aws

サービス認可リファレンス

サービス認可リファレンス



Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

サービス認可リファレンス: サービス認可リファレンス

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスはAmazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

リファレンス 1
アクション、リソース、および条件キー 1
アクションテーブル 1
リソースタイプテーブル 2
条件キーテーブル 3
AWS アカウント管理 18
AWS アクティブ化 24
Amazon API オペレーション 27
Alexa for Business 39
AmazonMediaImport 56
AWS Amplify 58
AWS Amplify 管理者 67
AWS Amplify UI ビルダー 75
Amazon MSK クラスター用の Apache Kafka API 88
Amazon API Gateway 95
AWS App Mesh 98
AWS App Mesh プレビュー 109
AWS App Runner 117
AWS App Studio 133
AWS App2Container 136
AWS AppConfig 139
AWS AppFabric 154
Amazon AppFlow 164
Amazon アプリインテグレーション 172
AWS アプリケーションの Auto Scaling 188
AWS Application Cost Profiler サービス 196
Application Discovery Arsenal 199
AWS Application Discovery Service 201
AWS アプリケーション移行サービス 214
Amazon Application Recovery Controller - ゾーンシフト 283
AWS アプリケーション変換サービス 296
Amazon AppStream 2.0 299
AWS AppSync 322
Amazon ARC リージョンスイッチ 338

AWS アーティファクト 344
Amazon Athena 349
AWS Audit Manager 363
Amazon Aurora DSQL 377
AWS Auto Scaling 383
AWS B2B データ交換 385
AWS バックアップ 393
AWS バックアップゲートウェイ 413
AWS バックアップ検索 420
AWS バックアップストレージ 425
AWS バッチ 429
Amazon Bedrock 446
Amazon Bedrock AgentCore 499
AWS Billing 517
AWS Billing および コスト管理ダッシュボード 524
AWS Billing コスト管理データのエクスポート 527
AWS Billing コスト管理料金計算ツール 532
AWS Billing コスト管理の推奨アクション 540
AWS Billing Conductor 542
AWS Billing コンソール 551
Amazon Braket 554
AWS Budget サービス 559
AWS BugBust 565
AWS Certificate Manager 572
AWS チャットボット 580
Amazon Chime 590
AWS クリーンルーム 654
AWS クリーンルーム ML 688
AWS クラウド コントロール API 713
Amazon Cloud Directory 716
AWS クラウド マップ 730
AWS Cloud9 739
AWS CloudFormation 749
Amazon CloudFront 773
Amazon CloudFront KeyValueStore 799
AWS CloudHSM 802

Amazon CloudSearch 810
AWS CloudShell 816
AWS CloudTrail 820
AWS CloudTrail データ 840
Amazon CloudWatch 843
Amazon CloudWatch Application Insights 856
Amazon CloudWatch Application Signals 862
Amazon CloudWatch Evidently 867
Amazon CloudWatch Internet Monitor 875
Amazon CloudWatch Logs 880
Amazon CloudWatch Network Synthetic Monitor 900
Amazon CloudWatch Observability Access Manager 904
Amazon CloudWatch Observability 管理サービス 910
AWS CloudWatch RUM 916
Amazon CloudWatch Synthetics 922
AWS CodeArtifact 930
Amazon CodeCatalyst 940
AWS CodeCommit 951
AWS CodeConnections 969
AWS CodeDeploy 983
AWS CodeDeploy セキュアホストコマンドサービス 995
Amazon CodeGuru 997
Amazon CodeGuru Profiler 999
Amazon CodeGuru Reviewer 1005
Amazon CodeGuru Security 1012
AWS CodePipeline 1017
AWS CodeStar 1027
AWS CodeStar 接続 1034
AWS CodeStar 通知 1048
Amazon CodeWhisperer 1056
Amazon Cognito ID 1062
Amazon Cognito Sync 1070
Amazon Cognito ユーザープール 1075
Amazon Comprehend 1092
Amazon Comprehend Medical 1127
AWS Compute Optimizer 1133

AWS 設定 1144
Amazon Connect Cases 1169
Amazon Connect Customer Profiles 1179
Amazon Connect アウトバウンドキャンペーン 1196
Amazon Connect Voice ID 1204
AWS コネクタサービス 1211
AWS Management Console モバイルアプリ 1213
AWS 一括請求 1216
AWS コントロールカタログ 1218
AWS Control Tower 1221
AWS コストと使用状況レポート 1234
AWS Cost Explorer サービス 1239
AWS コスト最適化ハブ 1253
AWS カスタマー検証サービス 1256
AWS データ交換 1259
Amazon Data Lifecycle Manager 1270
AWS データパイプライン 1274
AWS データベース移行サービス 1284
Database Query Metadata Service 1316
AWS DataSync 1320
Amazon DataZone 1334
AWS Deadline クラウド 1359
AWS DeepComposer 1397
AWS DeepRacer 1403
Amazon Detective 1425
AWS Device Farm 1434
Amazon DevOps Guru 1452
AWS 診断ツール 1459
AWS Direct Connect 1463
AWS ディレクトリサービス 1478
AWS Directory サービスデータ 1507
Amazon DocumentDB Elastic Clusters 1517
Amazon DynamoDB 1537
Amazon DynamoDB Accelerator (DAX) 1560
Amazon EC2 Auto Scaling (日本語) 1568
Amazon EC2 Image Builder 1596

Amazon EC2 Instance Connect 1630
Amazon EKS Auth 1635
AWS Elastic Beanstalk 1637
Amazon Elastic Block Store 1657
Amazon Elastic Container Registry 1662
Amazon Elastic Container Registry Public 1673
Amazon Elastic Container Service 1679
AWS Elastic Disaster Recovery 1710
Amazon Elastic File System 1743
Amazon Elastic Kubernetes Service 1754
AWS Elastic Load Balancing 1776
AWS Elastic Load Balancing V2 1793
Amazon Elastic MapReduce 1825
Amazon Elastic Transcoder 1844
Amazon Elastic VMware サービス 1849
Amazon ElastiCache 1853
AWS Elemental アプライアンスとソフトウェア 1912
AWS Elemental Appliances and Software Activation Service 1916
AWS Elemental MediaConnect 1920
AWS Elemental MediaConvert 1929
AWS Elemental MediaLive 1939
AWS Elemental MediaPackage 1966
AWS Elemental MediaPackage V2 1972
AWS Elemental MediaPackage VOD 1983
AWS Elemental MediaStore 1989
AWS Elemental MediaTailor 1995
AWS Elemental Support ケース 2006
AWS Elemental Support コンテンツ 2011
Amazon EMR on EKS (EMR コンテナ) 2013
Amazon EMR Serverless 2022
AWS エンドユーザーメッセージング SMS と音声 V2 2027
AWS エンドユーザーメッセージングソーシャル 2047
AWS エンティティの解決 2054
Amazon EventBridge 2063
Amazon EventBridge Pipes 2082
Amazon EventBridge Scheduler 2087

Amazon EventBridge スキーマ 2093
AWS フォールトインジェクションサービス 2101
Amazon FinSpace 2110
Amazon FinSpace API 2124
AWS Firewall Manager 2126
Amazon Forecast 2138
Amazon Fraud Detector 2157
AWS 無料利用枠 2186
Amazon FreeRTOS 2189
Amazon FSx 2195
Amazon GameLift Servers 2216
Amazon GameLift Streams 2244
AWS Global Accelerator 2250
AWS Glue 2262
AWS Glue DataBrew 2313
AWS Ground Station 2323
Amazon GroundTruth Labeling 2332
Amazon GuardDuty 2336
AWS Health APIsと通知 2353
AWS HealthImaging 2358
AWS HealthLake 2365
AWS Omics 2371
Amazon Honeycode 2389
AWS IAM Access Analyzer 2396
AWS IAM アイデンティティセンター 2403
AWS IAM Identity Center ディレクトリ 2428
AWS IAM Identity Center OIDC サービス 2439
AWS Identity and Access Management (IAM) 2441
AWS Identity and Access Management Roles Anywhere 2477
AWS ID ストア 2483
AWS Identity Store 認証 2490
AWS ID 同期 2492
AWS エクスポートディスクサービスのインポート 2496
Amazon Inspector 2499
Amazon Inspector2 2507
Amazon InspectorScan 2524

Amazon Interactive Video Service 2526
Amazon Interactive Video Service Chat 2545
AWS 請求サービス 2550
AWS IoT 1-Click 2556
AWS IoT Analytics 2562
AWS IoT Core Device Advisor 2570
AWS IoT Device Tester 2574
AWS IoT イベント 2577
AWS IoT Fleet Hub for Device Management 2586
AWS IoT FleetWise 2590
AWS IoT Greengrass 2604
AWS IoT Greengrass V2 2625
AWS IoT Jobs DataPlane 2637
AWS IoT マネージド統合 2640
AWS IoT SiteWise 2656
AWS IoT TwinMaker 2676
AWS IoT Wireless 2687
AWS IQ 2711
AWS IQ アクセス許可 2721
Amazon Kendra 2724
Amazon Kendra インテリジェントランキング 2738
Amazon Keyspaces (for Apache Cassandra) 2743
Amazon Kinesis Analytics 2750
Amazon Kinesis Analytics V2 2754
Amazon Kinesis Data Streams 2761
Amazon Kinesis Firehose 2772
Amazon Kinesis Video Streams 2776
AWS Lake Formation 2785
AWS Lambda 2795
AWS 起動ウィザード 2812
Amazon Lex 2820
Amazon Lex V2 2830
AWS License Manager 2851
AWS License Manager Linux Subscriptions Manager 2861
AWS License Manager ユーザーサブスクリプション 2866
Amazon Lightsail 2873

Amazon Location 2906
Amazon Location Service Maps 2919
Amazon Location Service Places 2921
Amazon Location Service Routes 2925
Amazon Lookout for Equipment 2928
Amazon Lookout for Metrics 2940
Amazon Lookout for Vision 2947
Amazon Machine Learning 2953
Amazon Macie 2960
AWS Mainframe Modernization アプリケーションテスト 2976
AWS Mainframe Modernization サービス 2985
Amazon Managed Blockchain 2995
Amazon Managed Blockchain Query 3005
Amazon Managed Grafana 3008
Amazon Managed Service for Prometheus 3015
Amazon Managed Streaming for Apache Kafka 3031
Amazon Managed Streaming for Kafka Connect 3048
Amazon Managed Workflows for Apache Airflow 3057
AWS Marketplace 3063
AWS Marketplace カタログ 3069
AWS Marketplace Commerce Analytics サービス 3074
AWS Marketplace デプロイサービス 3076
AWS Marketplace 検出 3081
AWS Marketplace 使用権限管理サービス 3083
AWS Marketplace イメージ構築サービス 3085
AWS Marketplace 管理ポータル 3088
AWS Marketplace 計測サービス 3092
AWS Marketplace プライベートマーケットプレイス 3095
AWS Marketplace 調達システムの統合 3098
AWS Marketplace レポート 3101
AWS Marketplace 販売者レポート 3103
AWS Marketplace Vendor Insights 3106
Amazon Mechanical Turk 3114
Amazon MemoryDB 3122
Amazon Message Delivery Service 3145
Amazon Message Gateway Service 3149

AWS .NET 用マイクロサービスエクストラクタ 3152
AWS Migration Acceleration プログラムクレジット 3154
AWS Migration Hub 3157
AWS Migration Hub オーケストレーター 3166
AWS Migration Hub リファクタリングスペース 3174
AWS Migration Hub Strategy の推奨事項 3194
Amazon Mobile Analytics 3200
Amazon Monitron 3202
Amazon MQ 3213
マルチパーティー承認 3221
Amazon Neptune 3230
Amazon Neptune Analytics 3236
AWS Network Firewall 3251
Network Flow Monitor 3266
AWS Network Manager 3273
AWS Network Manager チャット 3297
Amazon Nimble Studio 3300
Amazon One Enterprise 3319
Amazon OpenSearch 3328
Amazon OpenSearch Ingestion 3331
Amazon OpenSearch Serverless 3338
Amazon OpenSearch Service 3346
AWS OpsWorks 3371
AWS OpsWorks 設定管理 3383
AWS 組織 3388
AWS Outposts 3402
AWS パノラマ 3409
AWS 並列コンピューティングサービス 3418
AWS パートナーセントラルアカウント管理 3430
AWS Partner Central の販売 3432
AWS Payment Cryptography 3448
AWS 支払い 3458
AWS Performance Insights 3464
Amazon Personalize 3469
Amazon Pinpoint 3481
Amazon Pinpoint E メールサービス 3508

Amazon Pinpoint SMS および音声サービス 3523
Amazon Polly 3526
AWS 料金表 3530
AWS Active Directory 用プライベート CA コネクタ 3532
AWS SCEP 用プライベート CA コネクタ 3541
AWS プライベート認証機関 3546
AWS PrivateLink 3553
AWS プロトン 3555
AWS 発注書コンソール 3582
Amazon Q 3588
Amazon Q Business 3599
Amazon Q Business Q アプリ 3621
Amazon Q Developer 3636
Amazon Q in Connect 3640
Amazon QLDB 3663
Amazon QuickSight 3671
Amazon RDS Data API 3716
Amazon RDS IAM 認証 3720
AWS ごみ箱 3722
Amazon Redshift 3729
Amazon Redshift Data API 3772
Amazon Redshift Serverless 3778
Amazon Rekognition 3796
AWS rePost プライベート 3811
AWS レジリエンスハブ 3816
AWS Resource Access Manager (RAM) 3833
AWS Resource Explorer 3851
Amazon リソースグループのタグ付け API 3858
AWS リソースグループ 3861
Amazon RHEL ナレッジベースポータル 3869
AWS RoboMaker 3871
Amazon Route 53 3885
Amazon Route 53 ドメイン 3899
Amazon Route 53 プロファイル 3906
Amazon Route 53 Recovery クラスター 3913
Amazon Route 53 Recovery コントロール 3916

Amazon Route 53 Recovery Readiness 3923
Amazon Route 53 Resolver 3931
Amazon S3 Express 3952
Amazon S3 Glacier 3988
Amazon S3 Object Lambda 3995
Amazon S3 on Outposts 4022
Amazon S3 Tables 4090
Amazon S3 Vectors 4100
Amazon SageMaker データサイエンスアシスタント 4105
Amazon SageMaker 地理空間機能 4107
Amazon SageMaker と MLflow 4115
AWS Savings Plans 4125
AWS Secrets Manager 4129
AWS Security Hub 4156
AWS セキュリティインシデント対応 4178
Amazon Security Lake 4185
AWS サーバー移行サービス 4214
AWS サーバーレスアプリケーションリポジトリ 4221
AWS サービス - Oracle Database@AWS 4226
AWS サービスカタログ 4241
AWS AWS Management Console ユーザーエクスペリエンス機能を管理するためのサービス。 4267
AWS マネージドプライベートネットワークを提供する サービス 4269
Service Quotas 4277
Amazon SES 4286
AWS シールド 4303
AWS Shield ネットワークセキュリティディレクター 4314
AWS 署名者 4317
AWS サインイン 4323
Amazon Simple Email Service – Mail Manager 4326
Amazon Simple Email Service v2 4344
Amazon Simple Workflow Service 4380
Amazon SimpleDB 4398
AWS SimSpace ウィーバー 4402
AWS Snow デバイス管理 4406
AWS Snowball 4411

Amazon SNS 4417
AWS SQL Workbench 4427
Amazon SQS 4443
AWS ステップ関数 4448
AWS Storage Gateway 4459
AWS サプライチェーン 4482
AWS サポート 4490
AWS サポート Slack のアプリ 4497
AWS サポート コンソール 4500
AWS サポート プラン 4504
AWS 持続可能性 4507
AWS Systems Manager 4509
AWS SAP 用 Systems Manager 4551
AWS Systems Manager GUI Connect 4558
AWS Systems Manager Incident Manager 4561
AWS Systems Manager Incident Manager の連絡先 4569
AWS Systems Manager の高速セットアップ 4578
タグエディタ 4583
AWS 税設定 4585
AWS 通信ネットワークビルダー 4589
Amazon Textract 4600
Amazon Timestream 4606
Amazon Timestream InfluxDB 4617
AWS トロス 4624
Amazon Transcribe 4626
AWS Transfer Family 4642
AWS 変換 4654
Amazon Translate 4657
AWS Trusted Advisor 4663
AWS ユーザー通知 4674
AWS ユーザー通知の連絡先 4682
AWS ユーザーサブスクリプション 4686
AWS 検証済みアクセス 4689
Amazon Verified Permissions 4692
Amazon VPC Lattice 4698
Amazon VPC Lattice Services 4730

AWS WAF 4736
AWS WAF リージョン 4749
AWS WAF V2 4763
AWS Well-Architected ツール 4784
AWS ウィッカー 4801
Amazon WorkDocs 4805
Amazon WorkLink 4815
Amazon WorkMail 4823
Amazon WorkMail Message Flow 4843
Amazon WorkSpaces 4846
Amazon WorkSpaces Application Manager 4867
AWS WorkSpaces マネージドインスタンス 4869
Amazon WorkSpaces セキュアブラウザ 4874
Amazon WorkSpaces シンクライアント 4892
AWS X-Ray 4900
関連リソース 4910
サービスリファレンス情報へのプログラムによるアクセス 4911
追加のフィールド定義 4915
..... mmmmcmxviii

リファレンス

サービス認可リファレンスは、各 AWS サービスでサポートされているアクション、リソース、および条件キーのリストを提供します。 AWS Identity and Access Management (IAM) ポリシーでアクション、リソース、および条件キーを指定して、リソースへのアクセス AWS を管理できます。

内容

- AWS サービスのアクション、リソース、および条件キー
- 関連リソース

AWS サービスのアクション、リソース、および条件キー

各 AWS サービスは、IAM ポリシーで使用するアクション、リソース、および条件コンテキストキーを定義できます。このトピックでは、各サービスの要素の概要について説明します。

各トピックは、利用可能なアクション、リソース、条件キーのリストを含むテーブルで構成されます。

アクションテーブル

[アクション] テーブルには、IAM ポリシーステートメントの `Action` 要素で使用できるアクションがすべて一覧表示されています。サービスによって定義された API オペレーションがすべて IAM ポリシーのアクションとして使用できるとは限りません。いくつかのサービスには、API オペレーションに直接対応しない許可限定のアクションが含まれています。これらのアクションには [Permission only] (許可のみ) と表示されます。IAM ポリシーで使用できるアクションを特定するには、このリストを使用します。`Action`、`Resource`、または`Condition` 要素の詳細については、「IAM JSON ポリシー要素のリファレンス」を参照してください。[アクション] テーブルおよび [説明] テーブル列は、自己記述式です。

- [アクセスレベル] 列では、アクションの指定方法 (リスト、読み取り、書き込み、アクセス許可管理、タグ付け) について説明します。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、「ポリシー概要内のアクセスレベルの概要について」を参照してください。
- [リソースタイプ] 列は、アクションがリソースレベルのアクセス許可をサポートしているかどうかを示します。列が空の場合、アクションはリソースレベルのアクセス許可をサポートしておらず、ポリシーですべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、ポリシーの `Resource` 要素でリソース ARN を指定できます。リソースの詳細につい

ては、[リソースタイプ] テーブルの該当する行を参照してください。1 つのステートメントに含まれるアクションやリソースはすべて、相互に互換性がある必要があります。アクションに対して有効でないリソースを指定した場合、そのアクションを使用するリクエストは失敗し、ステートメントの `Effect` は適用されません。

必須リソースは、アスタリスク (*) でテーブルに示されています。このアクションを使用してステートメントでリソースレベルのアクセス許可 ARN を指定する場合、このタイプである必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、一方を使用することはできますが、他方を使用することはできません。

- [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。条件キーは、アクション、またはアクションと特定のリソースでサポートされる場合があります。キーが特定のリソースタイプと同じ行にあるかどうかには細心の注意を払ってください。このテーブルには、アクションに使用可能な、または無関係な状況のグローバル条件キーは含まれていません。グローバル条件キーの詳細については、「AWS グローバル条件コンテキストキー」を参照してください。
- [依存アクション] 列には、アクションそのもののアクセス許可に加えて、アクションを適切に呼び出すために持っておくべき追加のアクセス許可が含まれています。これは、アクションで複数のリソースにアクセスする場合に必要です。

  依存アクションは、一部のシナリオで必要とならない場合があります。ユーザーへの詳細な権限の付与について詳しくは、個々のサービスに関する資料を参照してください。

リソースタイプテーブル

[リソースタイプ] テーブルには、`Resource` ポリシー要素で ARN として指定できるすべてのリソースタイプが一覧表示されます。すべてのアクションで、すべてのリソースタイプを指定できるわけではありません。一部のリソースタイプは、特定のアクションでのみ動作します。リソースタイプをサポートしないアクションを使用してステートメントでそのリソースタイプを指定する場合、ステートメントではアクセスが許可されません。`Resource` 要素の詳細については、「IAM JSON ポリシーの要素: リソース」を参照してください。

- [ARN] 列では、このタイプのリソースの参照に使用する Amazon リソースネーム (ARN) 形式を指定します。$ で始まる部分は、お客様の状況で実際の値に置き換える必要があります。例えば、ARN に `$user-name` と表示されている場合は、その文字列を実際のユーザー名か、ユーザー名を含むポリシー変数に置き換える必要があります。ARN の詳細については、「IAM ARN」を参照してください。

- [条件キー] 列では、このリソースと上の表にあるサポートするアクションの両方がステートメントに含まれている場合にのみ IAM ポリシーステートメントに含むことができる条件コンテキストキーを指定します。

条件キーテーブル

[条件キー] テーブルには、IAM ポリシーステートメントの Condition 要素で使用できる条件コンテキストキーがすべて一覧表示されています。すべてのアクションやリソースで、すべてのキーを指定できるとは限りません。特定のキーは特定のタイプのアクションとリソースでのみ機能します。Condition 要素の詳細については、「IAM JSON ポリシーの要素: 条件」を参照してください。

- [タイプ] 列では、条件キーのデータタイプを指定します。このデータタイプを使用して、リクエストの値と、ポリシーステートメントの値の比較に使用できる条件演算子を特定します。データタイプに適切な演算子を使用する必要があります。不適切な演算子を使用した場合、条件は一致しないため、ポリシーステートメントは適用されません。

  [タイプ] 列でシンプルなタイプの「リスト」を指定した場合、ポリシーで複数のキーおよび値を使用することができます。これは、演算子で条件設定プレフィックスを使用して行います。ForAllValues プレフィックスを使用して、リクエスト内のすべての値がポリシーステートメントの値と一致する必要があることを指定します。ForAnyValue プレフィックスを使用して、リクエスト内の少なくとも 1 つの値がポリシーステートメントの値の 1 つと一致することを指定します。

トピック

- AWS Account Management のアクション、リソース、および条件キー
- AWS Activate のアクション、リソース、および条件キー
- Amazon AI Operations のアクション、リソース、および条件キー
- Alexa for Business のアクション、リソース、および条件キー
- AmazonMediaImport のアクション、リソース、および条件キー
- AWS Amplify のアクション、リソース、および条件キー
- AWS Amplify Admin のアクション、リソース、および条件キー
- AWS Amplify UIのアクション、リソース、および条件キー
- Amazon MSK クラスター用の Apache Kafka API のアクション、リソース、および条件キー
- Amazon API Gateway のアクション、リソース、および条件キー

- AWS App Mesh のアクション、リソース、および条件キー
- AWS App Mesh Preview のアクション、リソース、および条件キー
- AWS App Runner のアクション、リソース、および条件キー
- AWS App Studio のアクション、リソース、および条件キー
- AWS App2Container のアクション、リソース、条件キー
- AWS AppConfig のアクション、リソース、および条件キー
- AWS AppFabric のアクション、リソース、および条件キー
- Amazon AppFlow のアクション、リソース、および条件キー
- Amazon AppIntegrations のアクション、リソース、および条件キー
- AWS Application Auto Scaling のアクション、リソース、および条件キー
- AWS Application Cost Profiler Service のアクション、リソース、および条件キー
- Application Discovery Arsenal のアクション、リソース、および条件キー
- AWS Application Discovery Service のアクション、リソース、および条件キー
- AWS Application Migration Service のアクション、リソース、および条件キー
- Amazon Application Recovery Controller のアクション、リソース、および条件キー - ゾーンシフト
- AWS アプリケーション変換サービスのアクション、リソース、条件キー
- Amazon AppStream 2.0 のアクション、リソース、および条件キー
- AWS AppSync のアクション、リソース、および条件キー
- Amazon ARC リージョンスイッチのアクション、リソース、および条件キー
- AWS Artifact のアクション、リソース、および条件キー
- Amazon Athena のアクション、リソース、および条件キー
- AWS Audit Manager のアクション、リソース、および条件キー
- Amazon Aurora DSQL のアクション、リソース、および条件キー
- AWS Auto Scaling のアクション、リソース、および条件キー
- AWS B2B Data Interchange のアクション、リソース、および条件キー
- AWS Backup のアクション、リソース、および条件キー
- AWS Backup ゲートウェイのアクション、リソース、および条件キー
- AWS Backup Search のアクション、リソース、および条件キー
- AWS Backup ストレージのアクション、リソース、および条件キー

- AWS Batch のアクション、リソース、および条件キー
- Amazon Bedrock のアクション、リソース、条件キー
- Amazon Bedrock Agentcore のアクション、リソース、および条件キー
- AWS Billingのアクション、リソース、および条件キー
- および コスト管理ダッシュボードのアクション、リソース AWS Billing 、および条件キー
- AWS Billing And Cost Management データエクスポートのアクション、リソース、および条件キー
- AWS Billing And Cost Management 料金計算ツールのアクション、リソース、および条件キー
- AWS Billing And Cost Management の推奨アクションのアクション、リソース、および条件キー
- AWS Billing Conductorのアクション、リソース、および条件キー
- AWS Billing コンソールのアクション、リソース、および条件キー
- Amazon Braket のアクション、リソース、および条件キー
- AWS Budget Service のアクション、リソース、および条件キー
- AWS BugBust のアクション、リソース、条件キー
- AWS Certificate Manager のアクション、リソース、および条件キー
- AWS Chatbot のアクション、リソース、および条件キー
- Amazon Chime のアクション、リソース、および条件キー
- AWS クリーンルームのアクション、リソース、および条件キー
- AWS Clean Rooms ML のアクション、リソース、および条件キー
- AWS クラウド Control API のアクション、リソース、および条件キー
- Amazon Cloud Directory のアクション、リソース、および条件キー
- AWS クラウド Map のアクション、リソース、および条件キー
- AWS Cloud9 のアクション、リソース、および条件キー
- AWS CloudFormation のアクション、リソース、および条件キー
- Amazon CloudFront のアクション、リソース、および条件キー
- Amazon CloudFront KeyValueStore のアクション、リソース、および条件キー
- AWS CloudHSM のアクション、リソース、および条件キー
- Amazon CloudSearch のアクション、リソース、および条件キー
- AWS CloudShell のアクション、リソース、および条件キー
- AWS CloudTrail のアクション、リソース、および条件キー
- AWS CloudTrail Data のアクション、リソース、および条件キー

- Amazon CloudWatch のアクション、リソース、および条件キー
- Amazon CloudWatch Application Insights のアクション、リソース、および条件キー
- Amazon CloudWatch Application Signals のアクション、リソース、および条件キー
- Amazon CloudWatch Evidentlyのアクション、リソース、および条件キー
- Amazon CloudWatch Internet Monitor のアクション、リソース、および条件キー
- Amazon CloudWatch Logs のアクション、リソース、および条件キー
- Amazon CloudWatch Network Synthetic Monitor のアクション、リソース、および条件キー
- Amazon CloudWatch Observability Access Manager のアクション、リソース、条件キー
- Amazon CloudWatch Observability Admin Service のアクション、リソース、および条件キー
- AWS CloudWatch RUMのアクション、リソース、および条件キー
- Amazon CloudWatch Synthetics のアクション、リソース、および条件キー
- AWS CodeArtifact のアクション、リソース、および条件キー
- Amazon CodeCatalyst のアクション、リソース、および条件キー
- AWS CodeCommit のアクション、リソース、および条件キー
- AWS CodeConnections のアクション、リソース、および条件キー
- AWS CodeDeploy のアクション、リソース、および条件キー
- AWS CodeDeploy セキュアホストコマンドサービスのアクション、リソース、および条件キー
- Amazon CodeGuru のアクション、リソース、および条件キー
- Amazon CodeGuru Profiler のアクション、リソース、および条件キー
- Amazon CodeGuru Reviewer のアクション、リソース、および条件キー
- Amazon CodeGuru Security のアクション、リソース、および条件キー
- AWS CodePipeline のアクション、リソース、および条件キー
- AWS CodeStar のアクション、リソース、および条件キー
- AWS CodeStar Connections のアクション、リソース、および条件キー
- AWS CodeStar Notifications のアクション、リソース、および条件キー
- Amazon CodeWhisperer のアクション、リソース、および条件キー
- Amazon Cognito ID のアクション、リソース、および条件キー
- Amazon Cognito Sync のアクション、リソース、および条件キー
- Amazon Cognito ユーザープールのアクション、リソース、および条件キー
- Amazon Comprehend のアクション、リソース、および条件キー

- Amazon Comprehend Medical のアクション、リソース、および条件キー
- AWS Compute Optimizer のアクション、リソース、条件キー
- AWS Config のアクション、リソース、および条件キー
- Amazon Connect Cases のアクション、リソース、および条件キー
- Amazon Connect Customer Profiles のアクション、リソース、および条件キー
- Amazon Connect アウトバウンドキャンペーンのアクション、リソース、および条件キー
- Amazon Connect Voice ID のアクション、リソース、および条件キー
- AWS Connector Service のアクション、リソース、および条件キー
- AWS Management Console Mobile App のアクション、リソース、および条件キー
- AWS 一括請求のアクション、リソース、および条件キー
- AWS Control Catalog のアクション、リソース、および条件キー
- AWS Control Tower のアクション、リソース、および条件キー
- AWS のコストと使用状況レポートのアクション、リソース、および条件キー
- AWS Cost Explorer のアクション、リソース、および条件キー
- AWS Cost Optimization Hub のアクション、リソース、および条件キー
- AWS Customer Verification Service のアクション、リソース、および条件キー
- AWS Data Exchange のアクション、リソース、および条件キー
- Amazon Data Lifecycle Manager のアクション、リソース、および条件キー
- AWS Data Pipeline のアクション、リソース、および条件キー
- AWS Database Migration Service のアクション、リソース、および条件キー
- Database Query Metadata Service のアクション、リソース、および条件キー
- AWS DataSync のアクション、リソース、および条件キー
- Amazon DataZone のアクション、リソース、および条件キー
- AWS Deadline Cloud のアクション、リソース、および条件キー
- AWS DeepComposer のアクション、リソース、および条件キー
- AWS DeepRacer のアクション、リソース、および条件キー
- Amazon Detective のアクション、リソース、および条件キー
- AWS Device Farm のアクション、リソース、および条件キー
- Amazon DevOps Guru のアクション、リソース、および条件キー
- AWS 診断ツールのアクション、リソース、条件キー

- AWS Direct Connect のアクション、リソース、および条件キー
- AWS Directory Service のアクション、リソース、および条件キー
- AWS Directory Service Data のアクション、リソース、および条件キー
- Amazon DocumentDB Elastic Clusters のアクション、リソース、および条件キー
- Amazon DynamoDB のアクション、リソース、および条件キー
- Amazon DynamoDB Accelerator (DAX) のアクション、リソース、および条件キー
- Amazon EC2 Auto Scaling のアクション、リソース、および条件キー
- Amazon EC2 Image Builder のアクション、リソース、および条件キー
- Amazon EC2 Instance Connect のアクション、リソース、および条件キー
- Amazon EKS Auth のアクション、リソース、および条件キー
- AWS Elastic Beanstalk のアクション、リソース、および条件キー
- Amazon Elastic Block Store のアクション、リソース、および条件キー
- Amazon Elastic Container Registry のアクション、リソース、および条件キー
- Amazon Elastic Container Registry Public のアクション、リソース、および条件キー
- Amazon Elastic Container Service のアクション、リソース、および条件キー
- AWS Elastic ディザスタリカバリに対するアクション、リソースおよび条件キー
- Amazon Elastic File System のアクション、リソース、条件キー
- Amazon Elastic Kubernetes Service のアクション、リソース、および条件キー
- AWS Elastic Load Balancing のアクション、リソース、および条件キー
- AWS Elastic Load Balancing V2 のアクション、リソース、条件キー
- Amazon Elastic MapReduce のアクション、リソース、および条件キー
- Amazon Elastic Transcoder のアクション、リソース、および条件キー
- Amazon Elastic VMware Service のアクション、リソース、および条件キー
- Amazon ElastiCache のアクション、リソース、および条件キー
- AWS Elemental アプライアンスとソフトウェアのアクション、リソース、および条件キー
- AWS Elemental Appliances and Software Activation Service のアクション、リソース、および条件キー
- AWS Elemental MediaConnect のアクション、リソース、および条件キー
- AWS Elemental MediaConvert のアクション、リソース、および条件キー
- AWS Elemental MediaLive のアクション、リソース、および条件キー

- AWS Elemental MediaPackage のアクション、リソース、および条件キー
- AWS Elemental MediaPackage V2 のアクション、リソース、および条件キー
- AWS Elemental MediaPackage VOD のアクション、リソース、および条件キー
- AWS Elemental MediaStore のアクション、リソース、および条件キー
- AWS Elemental MediaTailor のアクション、リソース、および条件キー
- AWS Elemental Support Cases のアクション、リソース、条件キー
- AWS Elemental Support Content のアクション、リソース、条件キー
- Amazon EMR on EKS (EMR コンテナ) のアクション、リソース、および条件キー
- Amazon EMR Serverless のアクション、リソース、および条件キー
- AWS エンドユーザーメッセージング SMS および音声 V2 のアクション、リソース、および条件キー
- AWS End User Messaging Social のアクション、リソース、および条件キー
- AWS Entity Resolution のアクション、リソース、および条件キー
- Amazon EventBridge のアクション、リソース、および条件キー
- Amazon EventBridge Pipes のアクション、リソース、および条件キー
- Amazon EventBridge Scheduler のアクション、リソース、および条件キー
- Amazon EventBridge スキーマのアクション、リソース、および条件キー
- AWS Fault Injection Service のアクション、リソース、および条件キー
- Amazon FinSpace のアクション、リソース、および条件キー
- Amazon FinSpace API のアクション、リソース、および条件キー
- AWS Firewall Manager のアクション、リソース、および条件キー
- Amazon Forecast のアクション、リソース、および条件キー
- Amazon Fraud Detector のアクション、リソース、および条件キー
- AWS 無料利用枠のアクション、リソース、および条件キー
- Amazon FreeRTOS のアクション、リソース、および条件キー
- Amazon FSx のアクション、リソース、および条件キー
- Amazon GameLift サーバーのアクション、リソース、および条件キー
- Amazon GameLift Streams のアクション、リソース、および条件キー
- AWS Global Accelerator のアクション、リソース、および条件キー
- AWS Glue のアクション、リソース、および条件キー

- AWS Glue DataBrew のアクション、リソース、および条件キー
- AWS Ground Station のアクション、リソース、および条件キー
- Amazon GroundTruth Labeling のアクション、リソース、および条件キー
- Amazon GuardDuty のアクション、リソース、および条件キー
- AWS Health APIs and Notifications のアクション、リソース、および条件キー
- AWS HealthImaging のアクション、リソース、および条件キー
- AWS HealthLake のアクション、リソース、および条件キー
- AWS HealthOmics のアクション、リソース、および条件キー
- Amazon Honeycode のアクション、リソース、および条件キー
- AWS IAM Access Analyzer のアクション、リソース、および条件キー
- AWS IAM Identity Center のアクション、リソース、および条件キー
- AWS IAM Identity Center ディレクトリのアクション、リソース、および条件キー
- AWS IAM Identity Center OIDC サービスのアクション、リソース、および条件キー
- AWS Identity and Access Management (IAM) のアクション、リソース、および条件キー
- AWS Identity and Access Management Roles Anywhere のアクション、リソース、条件キー
- AWS Identity Store のアクション、リソース、および条件キー
- AWS Identity Store Auth のアクション、リソース、条件キー
- AWS Identity Sync のアクション、リソース、および条件キー
- AWS Import Export Disk Service のアクション、リソース、および条件キー
- Amazon Inspector のアクション、リソース、および条件キー
- Amazon Inspector2 のアクション、リソース、および条件キー
- Amazon InspectorScan のアクション、リソース、および条件キー
- Amazon Interactive Video Service のアクション、リソース、および条件キー
- Amazon Interactive Video Service Chat のアクション、リソース、および条件キー
- AWS 請求サービスのアクション、リソース、および条件キー
- AWS IoT 1-Click のアクション、リソース、および条件キー
- AWS IoT Analytics のアクション、リソース、および条件キー
- AWS IoT Core Device Advisor のアクション、リソース、および条件キー
- AWS IoT Device Tester のアクション、リソース、および条件キー
- AWS IoT Events のアクション、リソース、および条件キー

- AWS IoT Fleet Hub for Device Management のアクション、リソース、および条件キー
- AWS IoT FleetWise のアクション、リソース、および条件キー
- AWS IoT Greengrass のアクション、リソース、および条件キー
- AWS IoT Greengrass V2 のアクション、リソース、および条件キー
- AWS IoT Jobs DataPlane のアクション、リソース、および条件キー
- AWS IoT Managed Integrations のアクション、リソース、および条件キー
- AWS IoT SiteWise のアクション、リソース、および条件キー
- AWS IoT TwinMakerの、アクション、リソース、および条件キー
- AWS IoT Wireless のアクション、リソース、および条件キー
- AWS IQ のアクション、リソース、および条件キー
- AWS IQ Permissions のアクション、リソース、および条件キー
- Amazon Kendra のアクション、リソース、および条件キー
- Amazon Kendra インテリジェントランキングのアクション、リソース、および条件キー
- Amazon Keyspaces (Apache Cassandra 向け) のアクション、リソース、および条件キー
- Amazon Kinesis Analytics のアクション、リソース、および条件キー
- Amazon Kinesis Analytics V2 のアクション、リソース、および条件キー
- Amazon Kinesis Data Streams のアクション、リソース、および条件キー
- Amazon Kinesis Firehose のアクション、リソース、および条件キー
- Amazon Kinesis Video Streams のアクション、リソース、および条件キー
- AWS Lake Formation のアクション、リソース、および条件キー
- AWS Lambda のアクション、リソース、および条件キー
- AWS Launch Wizard のアクション、リソース、および条件キー
- Amazon Lex のアクション、リソース、および条件キー
- Amazon Lex V2 のアクション、リソース、および条件キー
- AWS License Manager のアクション、リソース、および条件キー
- AWS License Manager Linux Subscriptions Manager のアクション、リソース、および条件キー
- AWS License Manager User Subscriptions のアクション、リソース、および条件キー
- Amazon Lightsailのアクション、リソース、および条件キー
- Amazon Location のアクション、リソース、および条件キー
- Amazon Location Service Maps のアクション、リソース、および条件キー

- Amazon Location Service Places のアクション、リソース、および条件キー
- Amazon Location Service Routes のアクション、リソース、および条件キー
- Amazon Lookout for Equipment のアクション、リソース、および条件キー
- Amazon Lookout for Metrics のアクション、リソース、および条件キー
- Amazon Lookout for Vision のアクション、リソース、および条件キー
- Amazon Machine Learning のアクション、リソース、および条件キー
- Amazon Macie のアクション、リソース、および条件キー
- AWS Mainframe Modernization アプリケーションテストのアクション、リソース、条件キー
- AWS Mainframe Modernization サービスのアクション、リソース、条件キー
- Amazon Managed Blockchain のアクション、リソース、および条件キー
- Amazon Managed Blockchain Query のアクション、リソース、および条件キー
- Amazon Managed Grafana のアクション、リソース、および条件キー
- Amazon Managed Service for Prometheus のアクション、リソース、および条件キー
- Amazon Managed Streaming for Apache Kafka のアクション、リソース、および条件キー
- Amazon Managed Streaming for Kafka Connect のアクション、リソース、および条件キー
- Amazon Managed Workflows for Apache Airflow のアクション、リソース、および条件キー
- AWS Marketplaceのアクション、リソース、および条件キー
- AWS Marketplace Catalog のアクション、リソース、および条件キー
- AWS Marketplace Commerce Analytics Service のアクション、リソース、および条件キー
- AWS Marketplace Deployment Service のアクション、リソース、および条件キー
- AWS Marketplace Discovery のアクション、リソース、および条件キー
- AWS Marketplace Entitlement Service のアクション、リソース、および条件キー
- AWS Marketplace Image Building Service のアクション、リソース、および条件キー
- AWS Marketplace Management Portal のアクション、リソース、および条件キー
- AWS Marketplace Metering Service のアクション、リソース、および条件キー
- AWS Marketplace Private Marketplace のアクション、リソース、および条件キー
- AWS Marketplace Procurement Systems Integration のアクション、リソース、および条件キー
- AWS Marketplace Reporting のアクション、リソース、および条件キー
- AWS Marketplace Seller Reporting のアクション、リソース、および条件キー
- AWS Marketplace Vendor Insights のアクション、リソース、および条件キー

- Amazon Mechanical Turk のアクション、リソース、および条件キー
- Amazon MemoryDB のアクション、リソース、および条件キー
- Amazon Message Delivery Service のアクション、リソース、および条件キー
- Amazon Message Gateway Service のアクション、リソース、および条件キー
- AWS .NET 用Microservice Extractorのアクション、リソースおよび条件キー
- AWS Migration Acceleration Program クレジットのアクション、リソース、および条件キー
- AWS Migration Hub のアクション、リソース、および条件キー
- AWS Migration Hub Orchestrator のアクション、リソース、および条件キー
- AWS Migration Hub Refactor Spacesのアクション、リソース、および条件キー
- AWS Migration Hub Strategy Recommendations のアクション、リソース、および条件キー
- Amazon Mobile Analytics のアクションとリソース、条件キー
- Amazon Monitron のアクション、リソース、および条件キー
- Amazon MQ のアクション、リソース、および条件キー
- マルチパーティー承認のアクション、リソース、および条件キー
- Amazon Neptune のアクション、リソース、および条件キー
- Amazon Neptune Analytics のアクション、リソース、および条件キー
- AWS Network Firewall のアクション、リソース、および条件キー
- Network Flow Monitor のアクション、リソース、および条件キー
- AWS Network Manager のアクション、リソース、条件キー
- AWS Network Manager Chat のアクション、リソース、条件キー
- Amazon Nimble Studio のアクション、リソース、条件キー
- Amazon One Enterprise のアクション、リソース、および条件キー
- Amazon OpenSearch のアクション、リソース、および条件キー
- Amazon OpenSearch Ingestion のアクション、リソース、および条件キー
- Amazon OpenSearch Serverless のアクション、リソース、および条件キー
- Amazon OpenSearch Service のアクション、リソース、および条件キー
- AWS OpsWorks のアクション、リソース、および条件キー
- AWS OpsWorks Configuration Management のアクション、リソース、および条件キー
- AWS Organizations のアクション、リソース、および条件キー
- AWS Outposts のアクション、リソース、および条件キー

- AWS Panorama のアクション、リソース、および条件キー
- AWS パラレルコンピューティングサービスのアクション、リソース、および条件キー
- AWS パートナーセントラルのアカウント管理用のアクション、リソース、および条件キー
- AWS Partner Central Selling のアクション、リソース、および条件キー
- AWS Payment Cryptography のアクション、リソース、および条件キー
- AWS 支払いのアクション、リソース、および条件キー
- AWS Performance Insights のアクション、リソース、および条件キー
- Amazon Personalize のアクション、リソース、および条件キー
- Amazon Pinpoint のアクション、リソース、および条件キー
- Amazon Pinpoint Email Service のアクション、リソース、および条件キー
- Amazon Pinpoint SMS and Voice Service のアクション、リソース、および条件キー
- Amazon Polly のアクション、リソース、および条件キー
- AWS Price List のアクション、リソース、および条件キー
- アクティブディレクトリ用の AWS プライベート CA コネクタのアクション、リソース、条件キー
- AWS Private CA Connector for SCEP のアクション、リソース、条件キー
- AWS Private Certificate Authority のアクション、リソース、条件キー
- AWS PrivateLink のアクション、リソース、および条件キー
- AWS Proton のアクション、リソース、および条件キー
- AWS Purchase Orders Console のアクション、リソース、条件キー
- Amazon Q のアクション、リソース、および条件キー
- Amazon Q Business のアクション、リソース、および条件キー
- Amazon Q Business Q Apps のアクション、リソース、および条件キー
- Amazon Q Developer のアクション、リソース、および条件キー
- Amazon Q in Connect のアクション、リソース、および条件キー
- Amazon QLDB のアクション、リソース、および条件キー
- Amazon QuickSight のアクション、リソース、および条件キー
- Amazon RDS Data API のアクション、リソース、および条件キー
- Amazon RDS IAM 認証のアクション、リソース、条件キー
- AWS ごみ箱 のアクション、リソース、および条件キー

- Amazon Redshift のアクション、リソース、および条件キー
- Amazon Redshift Data API のアクション、リソース、および条件キー
- Amazon Redshift Serverless のアクション、リソース、条件キー
- Amazon Rekognition のアクション、リソース、および条件キー
- AWS rePost Private のアクション、リソース、および条件キー
- AWS Resilience Hub のアクション、リソースおよび条件キー
- AWS Resource Access Manager (RAM) のアクション、リソース、および条件キー
- AWS Resource Explorer のアクション、リソース、および条件キー
- Amazon リソースグループのタグ付け API のアクション、リソース、および条件キー
- AWS Resource Groups のアクション、リソース、および条件キー
- Amazon RHEL ナレッジベースポータルのアクション、リソース、条件キー
- AWS RoboMaker のアクション、リソース、および条件キー
- Amazon Route 53 のアクション、リソース、および条件キー
- Amazon Route 53 Domains のアクション、リソース、および条件キー
- Amazon Route 53 プロファイルのアクション、リソース、および条件キー
- Amazon Route 53 Recovery クラスターのアクション、リソース、および条件キー
- Amazon Route 53 Recovery コントロールのアクション、リソース、および条件キー
- Amazon Route 53 Recovery Readiness のアクション、リソース、および条件キー
- Amazon Route 53 Resolver のアクション、リソース、および条件キー
- Amazon S3 Express のアクション、リソース、および条件キー
- Amazon S3 Glacier のアクション、リソース、および条件キー
- Amazon S3 Object Lambda のアクション、リソース、条件キー
- Amazon S3 on Outposts のアクション、リソース、条件キー
- Amazon S3 Tables のアクション、リソース、および条件キー
- Amazon S3 Vectors のアクション、リソース、および条件キー
- Amazon SageMaker データサイエンスアシスタントのアクション、リソース、および条件キー
- Amazon SageMaker 地理空間機能のアクション、リソース、および条件キー
- MLflow を使用した Amazon SageMaker のアクション、リソース、および条件キー
- AWS Savings Plans のアクション、リソース、および条件キー
- AWS Secrets Manager のアクション、リソース、および条件キー

- AWS Security Hub のアクション、リソース、および条件キー
- AWS セキュリティインシデント対応のアクション、リソース、および条件キー
- Amazon Security Lake のアクション、リソース、および条件キー
- AWS Server Migration Service のアクション、リソース、および条件キー
- AWS Serverless Application Repository のアクション、リソース、および条件キー
- AWS サービス - Oracle Database@ のアクション、リソース、および条件キーAWS
- AWS Service Catalog のアクション、リソース、および条件キー
- AWS Management Console ユーザーエクスペリエンス機能を管理するための AWS Service のアクション、リソース、および条件キー。
- AWS のサービスが提供するマネージドプライベートネットワークのアクション、リソース、および条件キー
- Service Quotas のアクション、リソース、および条件キー
- Amazon SES のアクション、リソース、および条件キー
- AWS Shield のアクション、リソース、および条件キー
- AWS Shield ネットワークセキュリティディレクターのアクション、リソース、および条件キー
- AWS Signer のアクション、リソース、および条件キー
- AWS Signin のアクション、リソース、および条件キー
- Amazon Simple Email Service – Mail Manager のアクション、リソース、および条件キー
- Amazon Simple Email Service v2 のアクション、リソース、および条件キー
- Amazon Simple Workflow Service のアクション、リソース、および条件キー
- Amazon SimpleDB のアクション、リソース、および条件キー
- AWS SimSpace Weaver のアクション、リソース、および条件キー
- AWS Snow Device Management のアクション、リソース、および条件キー
- AWS Snowball のアクション、リソース、および条件キー
- Amazon SNS のアクション、リソース、および条件キー
- AWS SQL Workbench のアクション、リソース、条件キー
- Amazon SQS のアクション、リソース、および条件キー
- AWS Step Functions のアクション、リソース、および条件キー
- AWS Storage Gateway のアクション、リソースおよび条件キー
- AWS Supply Chain のアクション、リソース、および条件キー

- AWS サポートのアクション、リソース、および条件キー
- AWS サポート App in Slack のアクション、リソース、条件キー
- AWS サポート コンソールのアクション、リソース、および条件キー
- AWS サポート Plans のアクション、リソース、および条件キー
- AWS サステナビリティのアクション、リソース、条件キー
- AWS Systems Manager のアクション、リソース、および条件キー
- AWS Systems Manager for SAP のアクション、リソース、および条件キー
- AWS Systems Manager GUI Connectのアクション、リソース、および条件キー
- AWS Systems Manager Incident Manager のアクション、リソース、および条件キー
- AWS Systems Manager Incident Manager Contacts のアクション、リソース、および条件キー
- AWS Systems Manager Quick Setup のアクション、リソース、および条件キー
- タグエディタ のアクション、リソース、および条件キー
- AWS Tax Settings のアクション、リソース、および条件キー
- AWS Telco Network Builder のアクション、リソース、条件キー
- Amazon Textract のアクション、リソース、および条件キー
- Amazon Timestream のアクション、リソース、および条件キー
- Amazon Timestream InfluxDB のアクション、リソース、および条件キー
- AWS Tiros のアクション、リソース、および条件キー
- Amazon Transcribe のアクション、リソース、および条件キー
- AWS Transfer Family のアクション、リソース、および条件キー
- AWS Transform のアクション、リソース、および条件キー
- Amazon Translate のアクション、リソース、および条件キー
- AWS Trusted Advisor のアクション、リソース、および条件キー
- AWS ユーザー通知のアクション、リソース、および条件キー
- AWS ユーザー通知のアクション、リソース、および条件キー
- AWS User Subscriptions のアクション、リソース、および条件キー
- AWS Verified Access のアクション、リソース、および条件キー
- Amazon Verified Permissions のアクション、リソース、条件キー
- Amazon VPC Lattice のアクション、リソース、および条件キー
- Amazon VPC Lattice Services のアクション、リソース、および条件キー

- AWS WAF のアクション、リソース、および条件キー
- AWS WAF Regional のアクション、リソース、および条件キー
- AWS WAF V2 のアクション、リソース、および条件キー
- AWS Well-Architected Tool のアクション、リソース、および条件キー
- AWS Wickr のアクション、リソース、および条件キー
- Amazon WorkDocs のアクション、リソース、および条件キー
- Amazon WorkLink のアクション、リソース、および条件キー
- Amazon WorkMail のアクション、リソース、および条件キー
- Amazon WorkMail Message Flow のアクション、リソース、および条件キー
- Amazon WorkSpaces のアクション、リソース、および条件キー
- Amazon WorkSpaces Application Manager のアクション、リソース、および条件キー
- AWS WorkSpaces マネージドインスタンスのアクション、リソース、および条件キー
- Amazon WorkSpaces Secure Browser のアクション、リソース、および条件キー
- Amazon WorkSpaces シンクライアントのアクション、リソース、および条件キー
- AWS X-Ray のアクション、リソース、および条件キー

AWS Account Management のアクション、リソース、および条件キー

AWS アカウント管理 (サービスプレフィックス: account) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Account Management で定義されているアクション
- AWS Account Management で定義されているリソースタイプ
- AWS Account Management の条件キー

AWS Account Management で定義されているアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AcceptPrimaryEmailUpdate	アカウントのプライマリ E メールアドレスを更新するプロセスを受け入れる許可を付与する	書き込み	accountInOrganization		
				account:EmailTargetDomain	
CloseAccount [アクセス許可のみ]	アカウント情報を閉じるアクセス許可を付与	書き込み	account		
DeleteAlternateContact	アカウントの代替連絡先を削除するためのアクセス許可を付与する	書き込み	account		
			accountInOrganization		
				account:AlternateContactTypes	
DisableRegion	リージョンを無効にするためのアクセス許可を付与する	書き込み	account		
			accountInOrganization		
				account:TargetRegion	
EnableRegion	リージョンを有効にするためのアクセス許可を付与する	書き込み	account		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			accountInOrganization		
				account:TargetRegion	
GetAccountInformation	アカウントのアカウント情報を取得するアクセス許可を付与	読み取り	account		
			accountInOrganization		
GetAlternateContact	アカウントの代替連絡先を取得するためのアクセス許可を付与する	読み取り	account		
			accountInOrganization		
				account:AlternateContactTypes	
GetContactInformation	アカウントの主な連絡先情報を取得する許可を付与	読み取り	account		
			accountInOrganization		
GetPrimaryEmail	アカウントのプライマリ E メールアドレスを取得する許可を付与する	読み取り	accountInOrganization		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetRegionOptStatus	リージョンのオプトインステータスを取得するための許可を付与します	読み取り	account		
			accountInOrganization		
				account:TargetRegion	
ListRegions	利用可能なリージョンを一覧表示するためのアクセス許可を付与する	リスト	account		
			accountInOrganization		
PutAccountName	アカウントの名前を更新するアクセス許可を付与します	書き込み	account		
			accountInOrganization		
PutAlternateContact	アカウントの代替連絡先を変更するためのアクセス許可を付与する	書き込み	account		
			accountInOrganization		
				account:AlternateContactTypes	
PutContactInformation	アカウントの主な連絡先情報を更新する許可を付与	書き込み	account		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			accountInOrganization		
StartPrimaryEmailUpdate	アカウントのプライマリ E メールアドレスを更新するプロセスを開始する許可を付与する	書き込み	accountInOrganization		
				account:EmailTargetDomain	

AWS Account Management で定義されているリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
account	`arn:${Partition}:account::${Account}:account`	
accountInOrganization	`arn:${Partition}:account::${ManagementAccountId}:account/o-${OrganizationId}/${MemberAccountId}`	

AWS Account Management の条件キー

AWS アカウント管理では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
account:AccountResourceOrgPaths	組織内のアカウントでのリソースパスによりアクセスをフィルタリングする	ArrayOfString
account:AccountResourceOrgTags/${TagKey}	組織内のアカウントでのリソースタグによりアクセスをフィルタリングする	String
account:AlternateContactTypes	代替連絡先のタイプによりアクセスをフィルタリングする	ArrayOfString
account:EmailTargetDomain	ターゲット E メールアドレスの E メールドメインによってアクセスをフィルタリングする	String
account:TargetRegion	リージョンのリストによりアクセスをフィルタリングする ここに示されたすべてのリージョンを有効または無効にする	String

AWS Activate のアクション、リソース、および条件キー

AWS Activate (サービスプレフィックス: activate) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Activate で定義されるアクション
- AWS Activate で定義されるリソースタイプ
- AWS Activate の条件キー

AWS Activate で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateForm	アクティブ化申請フォームを送信する権限を付与します	書き込み			
GetAccountContact	AWS アカウント 連絡先情報を取得するアクセス許可を付与します	読み取り			
GetContentInfo	アクティブ化技術投稿とオファー情報を取得する権限を付与します	読み取り			
GetCosts	AWS コスト情報を取得するアクセス許可を付与します	読み取り			
GetCredits	AWS クレジット情報を取得する許可を付与	読み取り			
GetMemberInfo	アクティブ化メンバー情報を取得する権限を付与します	Read			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetProgram	アクティブ化プログラムを取得する権限を付与します	Read			
PutMemberInfo	アクティブ化メンバー情報を作成または更新する権限を付与します	Write			

AWS Activate で定義されるリソースタイプ

AWS Activate は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Activate へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Activate の条件キー

Activate には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon AI Operations のアクション、リソース、および条件キー

Amazon AI Operations (サービスプレフィックス: `aiops`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon AI Operations で定義されるアクション

- Amazon AI Operations で定義されるリソースタイプ
- Amazon AI Operations の条件キー

Amazon AI Operations で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシーの概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateInvestigation	指定された調査グループに新しい調査を作成するアクセス許可を付与します	書き込み	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext
CreateInvestigationEvent	指定された調査グループに新しい調査イベントを作成するアクセス許可を付与します	書き込み	investigation-group*		cloudwatch:DescribeAlarmHistory cloudwatch:DescribeAlarms cloudwatch:GetInsightRuleReport cloudwatch:GetMetricData

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					kms:Decrypt kms:GenerateDataKey logs:GetQueryResults sts:SetContext

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateInvestigationGroup	新しい調査グループを作成するアクセス許可を付与します	書き込み		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	aiops:TagResource cloudtrail:DescribeTrails iam:PassRole kms:Decrypt kms:DescribeKey kms:GenerateDataKey sso:CreateApplication sso:DeleteApplication sso:PutApplicationAccessScope sso:PutApplication

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					AssignmentConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant sso:TagResource

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateInvestigationResource	指定された調査グループに調査リソースを作成するアクセス許可を付与します	書き込み	investigation-group*		cloudwatch:DescribeAlarmHistory cloudwatch:DescribeAlarms cloudwatch:GetInsightRuleReport cloudwatch:GetMetricData kms:GenerateDataKey logs:GetQueryResults
DeleteInvestigation	指定された調査グループの調査を削除するアクセス許可を付与します	書き込み	investigation-group*		sts:SetContext
DeleteInvestigationGroup	指定された調査グループを削除するアクセス許可を付与します	書き込み	investigation-group*		sso:DeleteApplication

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteInvestigationGroupPolicy	調査グループにアタッチされた調査グループポリシーを削除するアクセス許可を付与します	書き込み	investigation-group*		
GetInvestigation	指定された調査グループで調査を取得するアクセス許可を付与します	読み取り	investigation-group*		
GetInvestigationEvent	指定された調査グループの調査イベントを取得するアクセス許可を付与します	読み取り	investigation-group*		kms:Decrypt
GetInvestigationGroup	指定された調査グループを取得するアクセス許可を付与します	読み取り	investigation-group*		
GetInvestigationGroupPolicy	調査グループにアタッチされた調査グループポリシーを取得する許可を付与	読み取り	investigation-group*		
GetInvestigationResource	指定された調査グループ内の調査リソースを取得するアクセス許可を付与します	読み取り	investigation-group*		kms:Decrypt
ListInvestigationEvents	指定された調査グループ内のすべての調査イベントを一覧表示するアクセス許可を付与します	リスト	investigation-group*		
ListInvestigationGroups	リクエスト AWS アカウントを行う 内のすべての調査グループを一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListInvestigations	指定された調査グループ内のすべての調査を一覧表示するアクセス許可を付与します	リスト	investigation-group*		
ListTagsForResource	指定されたリソースのタグを一覧表示するためのアクセス許可を付与	リスト	investigation-group*		
PutInvestigationGroupPolicy	調査グループにアタッチされた調査グループポリシーを作成/更新するアクセス許可を付与します	書き込み	investigation-group*		
TagResource	指定されたリソースの指定されたタグを追加または更新する許可を付与	Tagging	investigation-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	指定されたリソースから指定されたタグを削除するためのアクセス許可を付与	Tagging	investigation-group*		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateInvestigation	指定された調査グループの調査を更新する許可を付与	書き込み	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext
UpdateInvestigationEvent	指定された調査グループの調査イベントを更新する許可を付与	書き込み	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateInvestigationGroup	指定された調査グループを更新する許可を付与	書き込み	investigation-group*		cloudtrail:DescribeTrails iam:PassRole kms:Decrypt kms:DescribeKey kms:GenerateDataKey sso:CreateApplication sso:DeleteApplication sso:PutApplicationAccessScope sso:PutApplicationAssignmentConfiguration

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant sso:TagResource
ValidateInvestigationGroup	指定された調査グループを検証するアクセス許可を付与します	読み取り	investigation-group*		

Amazon AI Operations で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
investigation-group	`arn:${Partition}:aiops:${Region}:${Account}:investigation-group/${InvestigationGroupId}`	aws:ResourceTag/${TagKey}

Amazon AI Operations の条件キー

Amazon AI Operations では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Alexa for Business のアクション、リソース、および条件キー

Alexa for Business (サービスプレフィックス: a4b) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Alexa for Business で定義されるアクション
- Alexa for Business で定義されるリソースタイプ
- Alexa for Business の条件キー

Alexa for Business で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ApproveSkill	顧客の でスキルと組織を関連付けるアクセス許可を付与します AWS アカウント	書き込み			
AssociateContactWithAddressBook	特定のアドレス帳に連絡先を関連付けるためのアクセス許可を付与	Write	addressbook*		
			contact*		
AssociateDeviceWithNetworkProfile	指定されたネットワークプロファイルとデバイスを関連付けるためのアクセス許可を付与	Write	device*		
			networkprofile*		
AssociateDeviceWithRoom	特定のルームにデバイスを関連付けるためのアクセス許可を付与	Write	device*		
			room*		
AssociateSkillGroupWithRoom	特定のスキルグループにデバイスを関連付けるためのアクセス許可を付与	Write	room*		
			skillgroup*		
AssociateSkillWithSkillGroup	スキルとスキルグループに関連付けるためのアクセス許可を付与	Write	skillgroup*		
AssociateSkillWithUsers	登録されたユーザーがデバイスで有効にするためにプライベートスキルを利用可能にする許可を付与	Write			
CompleteRegistration [ア	Alexa デバイスの登録オペレーションを完了する許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
クセス許可のみ]					
CreateAddressBook	指定された詳細情報を持つアドレス帳を作成する許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateBusinessReportSchedule	指定された S3 の場所に日次または週次の間隔で配信するために、使用状況レポートの定期的なスケジュールを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConferenceProvider	ユーザーの の下に新しい会議プロバイダーを追加するアクセス許可を付与します AWS アカウント	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateContact	指定された詳細情報を持つ連絡先を作成する許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateGatewayGroup	指定された詳細でゲートウェイグループを作成する許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNetworkProfile	指定された詳細でネットワークプロファイルを作成する許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfile	新しいプロファイルを作成する許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRoom	指定された詳細でルームを作成する許可を付与	Write	profile*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSkillGroup	指定した名前と説明でスキルグループを作成する許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateUser	ユーザーを作成する許可を付与	Write	user*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAddressBook	アドレス帳 ARN によってアドレス帳を削除する許可を付与	Write	addressbook*		
DeleteBusinessReportSchedule	指定されたスケジュール ARN を使用して定期的なレポート配信スケジュールを削除する許可を付与	Write	schedule*		
DeleteConferenceProvider	会議プロバイダーを削除する許可を付与	Write	conferenceprovider*		
DeleteContact	連絡先 ARN によって連絡先を削除する許可を付与	Write	contact*		
DeleteDevice	Alexa for Business からデバイスを削除する許可を付与	Write	device*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteDeviceUsageData	デバイスの以前の音声入力データおよび関連する応答データの履歴全体を削除する許可を付与	Write	device*		
DeleteGatewayGroup	ゲートウェイグループを削除する許可を付与	Write	gatewaygroup*		
DeleteNetworkProfile	ネットワークプロファイル ARN によってネットワークプロファイルを削除する許可を付与	Write	networkprofile*		
DeleteProfile	プロファイル ARN によってプロファイルを削除する許可を付与	Write	profile*		
DeleteRoom	ルームを削除する許可を付与	Write	room*		
DeleteRoomSkillParameter	スキルとルームからパラメータを削除する許可を付与	Write	room*		
DeleteSkillAuthorization	スキルからサードパーティーアカウントのリンクを解除する許可を付与	Write	room*		
DeleteSkillGroup	スキルグループ ARN を持つスキルグループを削除する許可を付与	Write	skillgroup*		
DeleteUser	ユーザーを削除する許可を付与	Write	user*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DisassociateContactFromAddressBook	特定のアドレス帳から連絡先の関連付けを解除する許可を付与	Write	addressbook*		
			contact*		
DisassociateDeviceFromRoom	現在のルームからデバイスの関連付けを解除する許可を付与	Write	device*		
DisassociateSkillFromSkillGroup	スキルグループからスキルの関連付けを解除する許可を付与	Write	skillgroup*		
DisassociateSkillFromUsers	登録されたユーザー向けにプライベートスキルを利用不可にし、それらのユーザーによってデバイスでそのスキルが有効にされるのを防ぐためのアクセス許可を付与	Write	user*		
DisassociateSkillGroupFromRoom	特定のルームからスキルグループの関連付けを解除する許可を付与	Write	room*		
			skillgroup*		
ForgetSmartHomeAppliances	ルームに関連付けられたスマート家電を忘れるためのアクセス許可を付与	Write	room*		
GetAddressBook	アドレス帳 ARN によってアドレス帳の詳細を取得する許可を付与	Read	addressbook*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetConferencePreference	既存の会議の詳細設定を取得する許可を付与	Read			
GetConferenceProvider	特定の会議プロバイダーの詳細を取得する許可を付与	Read	conferenceprovider*		
GetContact	連絡先 ARN によって連絡先の詳細を取得する許可を付与	Read	contact*		
GetDevice	デバイスの詳細を取得する許可を付与	Read	device*		
GetGateway	ゲートウェイの詳細を取得する許可を付与	Read	gateway*		
GetGatewayGroup	ゲートウェイグループの詳細を取得する許可を付与	Read	gatewaygroup*		
GetInvitationConfiguration	ユーザー登録の招待メールのテンプレート用に設定された値を取得する許可を付与	Read			
GetNetworkProfile	ネットワークプロファイル ARN によってネットワークプロファイルの詳細を取得する許可を付与	Read	networkprofile*		
GetProfile	プロファイル ARN で提供されている場合、プロファイルを取得する許可を付与	Read	profile*		
GetRoom	ルームの詳細を取得する許可を付与	Read	room*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetRoomSkillParameter	スキルやルームに設定されている既存のパラメータを取得する許可を付与	Read	room*		
GetSkillGroup	スキルグループ ARN でスキルグループの詳細を取得する許可を付与	Read	skillgroup*		
ListBusinessReportSchedules	ユーザーが設定したスケジュールの詳細を一覧表示する許可を付与	リスト			
ListConferenceProviders	特定の で会議プロバイダーを一覧表示する許可を付与 AWS アカウント	リスト			
ListDeviceEvents	デバイス接続ステータスなどのイベント履歴を最大 30 日間一覧表示する許可を付与	リスト	device*		
ListGatewayGroups	ゲートウェイグループの概要を一覧表示する許可を付与	リスト			
ListGateways	ゲートウェイの概要を一覧表示する許可を付与	リスト	gatewaygroup*		
ListSkills	スキルを一覧表示する許可を付与	リスト			
ListSkillsStoreCategories	Alexa スキルストア内のすべてのカテゴリを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListSkillsStoreSkillsByCategory	Alexa スキルストア内のすべてのスキルをカテゴリ別に一覧表示する許可を付与	リスト			
ListSmartHomeAppliances	ルームに関連付けられたすべてのスマート家電を一覧表示する許可を付与	リスト	room*		
ListTags	リソースのすべてのタグを一覧表示する許可を付与	Read	device		
			room		
			user		
PutConferencePreference	特定の会議プロバイダーの会議の設定をアカウントレベルで行うためのアクセス許可を付与	Write			
PutDeviceSetupEvents [アクセス許可のみ]	Alexa デバイスセットアップイベントを発行する許可を付与	Write			
PutInvitationConfiguration	ユーザー登録の招待メールのテンプレートを指定された属性で設定する許可を付与	Write			
PutRoomSkillParameter	スキルにルーム固有のパラメータを配置する許可を付与	Write	room*		
PutSkillAuthorization	ユーザーのアカウントをサードパーティーのスキルプロバイダーにリンクする許可を付与	Write	room*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RegisterAVSDevice	Alexa Voice Service (AVS) を使用して、相手先ブランド製造会社 (OEM) によって構築された Alexa 対応デバイスを登録する許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys	
RegisterDevice [アクセス許可のみ]	Alexa デバイスを登録する許可を付与	書き込み			
RejectSkill	ユーザーの の下にある組織からスキルの関連付けを解除するアクセス許可を付与しますAWS アカウント	書き込み			
ResolveRoom	ルーム情報を解決する許可を付与	Read			
RevokeInvitation	招待を撤回する許可を付与	Write	user*		
SearchAddressBooks	アドレス帳を検索し、一連のフィルターと並べ替え条件に合致するアドレス帳を一覧表示する許可を付与	リスト			
SearchContacts	連絡先を検索し、一連のフィルターと並べ替え条件に合致するアドレス帳を一覧表示する許可を付与	リスト			
SearchDevices	デバイスを検索する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SearchNetworkProfiles	ネットワークプロファイルを検索し、一連のフィルターと並べ替え条件に合致するアドレス帳を一覧表示する許可を付与	リスト			
SearchProfiles	プロファイルを検索する許可を付与	リスト			
SearchRooms	ルームを検索する許可を付与	リスト			
SearchSkillGroups	スキルグループを検索する許可を付与	リスト			
SearchUsers	ユーザーを検索する許可を付与	リスト			
SendAnnouncement	検索またはフィルターによって識別されたルームにテキスト、SSML、または音声アナウンスを送信する非同期フローをトリガーする許可を付与	Write			
SendInvitation	ユーザーに招待を送信する許可を付与	Write	user*		
StartDeviceSync	以前のユーザーが設定した情報や設定をすべて消去して、デバイスとそのアカウントを既知のデフォルト設定に復元する許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartSmartHomeApplianceDiscovery	ルームに関連付けられたスマートホームアプライアンスの検出を開始する許可を付与	Read	room*		
TagResource	リソースにメタデータタグを追加する許可を付与	タグ付け	device		
			room		
			user		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースからメタデータタグを削除する許可を付与	タグ付け	device		
			room		
			user		
UpdateAddressBook	アドレス帳 ARN によってアドレス帳の詳細を更新する許可を付与	Write	addressbook*		
UpdateBusinessReportSchedule	指定されたスケジュール ARN を使用してレポート配信スケジュールの設定を更新する許可を付与	Write	schedule*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateConferenceProvider	既存の会議プロバイダーの設定を更新する許可を付与	Write	conferenceprovider*		
UpdateContact	連絡先 ARN によって連絡先の詳細を更新する許可を付与	Write	contact*		
UpdateDevice	デバイス名を更新する許可を付与	Write	device*		
UpdateGateway	ゲートウェイの詳細を更新する許可を付与	Write	gateway*		
UpdateGatewayGroup	ゲートウェイグループの詳細を更新する許可を付与	Write	gatewaygroup*		
UpdateNetworkProfile	ネットワークプロファイル ARN によってネットワークプロファイルを更新する許可を付与	Write	networkprofile*		
UpdateProfile	既存のプロファイルを更新する許可を付与	Write	profile*		
UpdateRoom	ルームの詳細を更新する許可を付与	Write	room*		
UpdateSkillGroup	スキルグループ ARN を使用してスキルグループの詳細を更新する許可を付与	Write	skillgroup*		

Alexa for Business で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
profile	arn:${Partition}:a4b:${Region}:${Account}:profile/${ResourceId}	
room	arn:${Partition}:a4b:${Region}:${Account}:room/${ResourceId}	aws:ResourceTag/${TagKey}
device	arn:${Partition}:a4b:${Region}:${Account}:device/${ResourceId}	aws:ResourceTag/${TagKey}
skillgroup	arn:${Partition}:a4b:${Region}:${Account}:skill-group/${ResourceId}	
user	arn:${Partition}:a4b:${Region}:${Account}:user/${ResourceId}	aws:ResourceTag/${TagKey}
addressbook	arn:${Partition}:a4b:${Region}:${Account}:address-book/${ResourceId}	
conferenceprovider	arn:${Partition}:a4b:${Region}:${Account}:conference-provider/${ResourceId}	
contact	arn:${Partition}:a4b:${Region}:${Account}:contact/${ResourceId}	
schedule	arn:${Partition}:a4b:${Region}:${Account}:schedule/${ResourceId}	

リソースタイプ	ARN	条件キー
networkprofile	arn:${Partition}:a4b:${Region}:${Account}:network-profile/${ResourceId}	
gateway	arn:${Partition}:a4b:${Region}:${Account}:gateway/${ResourceId}	
gatewaygroup	arn:${Partition}:a4b:${Region}:${Account}:gateway-group/${ResourceId}	

Alexa for Business の条件キー

Alexa for Business では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
a4b:amazonId	リクエスト内の Amazon ID に基づいてフィルタリングします。	文字列
a4b:filters_deviceType	リクエスト内のデバイスタイプに基づいてフィルタリングします。	ArrayOfString
aws:RequestTag/${TagKey}	各タグで許可されている値のセットに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられている tag-value に基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエスト内の必須タグのプレゼンスに基づいてアクションをフィルタリングします	ArrayOfString

AmazonMediaImport のアクション、リソース、および条件キー

AmazonMediaImport (サービスプレフィックス: mediaimport) では、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されており、IAM アクセス許可ポリシーでの使用が可能です。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AmazonMediaImport で定義されているアクション
- AmazonMediaImport で定義されているリソースタイプ
- AmazonMediaImport の条件キー

AmazonMediaImport で定義されているアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateDatabaseBinarySnapshot [アクセス許可のみ]	データベースのバイナリスナップショットを作成するためのアクセス許可を、顧客の AWS アカウントに付与	書き込み			

AmazonMediaImport で定義されているリソースタイプ

AmazonMediaImport では、IAM ポリシーステートメントの Resource 要素でのリソース ARN の指定はサポートされていません。AmazonMediaImport へのアクセスを許可するには、ポリシーで "Resource": "*" を指定します。

AmazonMediaImport の条件キー

AmazonMediaImport には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Amplify のアクション、リソース、および条件キー

AWS Amplify (サービスプレフィックス: amplify) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Amplify で定義されるアクション
- AWS Amplify で定義されるリソースタイプ
- AWS Amplify の条件キー

AWS Amplify で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateWebACL	WebACL をリソースに関連付けるアクセス許可を付与します	書き込み	apps*		
CreateApp	新しい Amplify アプリケーションを作成するアクセス許可を付与	書き込み	apps*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBackendEnvironment	Amplify AppId に新しいバックエンド環境を作成するアクセス許可を付与	書き込み	apps*		
CreateBranch	Amplify アプリケーションの新しいブランチを作成するアクセス許可を付与	書き込み	branches*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeployment	アプリケーションの手動デプロイ用のデプロイを作成するアクセス許可を付与 (アプリケーションはリポジトリに接続されません)	書き込み	branches*		
CreateDomainAssociation	アプリケーションに新しい DomainAssociation を作成するアクセス許可を付与	書き込み	domains*		
CreateWebHook	アプリケーションに新しいウェブフックを作成するアクセス許可を付与	書き込み	branches*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteApp	appId で指定された既存の Amplify アプリケーションを削除するアクセス許可を付与	書き込み	apps*		
DeleteBackendEnvironment	Amplify アプリケーションのブランチを削除するアクセス許可を付与	書き込み	apps*		
DeleteBranch	Amplify アプリケーションのブランチを削除するアクセス許可を付与	書き込み	branches*		
DeleteDomainAssociation	DomainAssociation を削除するアクセス許可を付与	書き込み	domains*		
DeleteJob	Amplify アプリケーションの一部である Amplify ブランチのジョブを削除するアクセス許可を付与	書き込み	jobs*		
DeleteWebHook	id でウェブフックを削除するアクセス許可を付与	書き込み	webhooks*		
DisassociateWebACL	リソースから WebACL の関連付けを解除するアクセス許可を付与します	書き込み	apps*		
GenerateAccessLogs	署名付き URL を使用して、特定の時間範囲のウェブサイトアクセスログを生成するアクセス許可を付与	書き込み	apps*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetApp	appId で指定された既存の Amplify アプリケーションを取得するアクセス許可を付与	読み取り	apps*		
GetArtifactUrl	artifactId に対応するアーティファクト情報を取得するアクセス許可を付与	読み取り	apps*		
GetBackendEnvironment	Amplify アプリケーションのバックエンド環境を取得するアクセス許可を付与	読み取り	apps*		
GetBranch	Amplify アプリケーションのブランチを取得するアクセス許可を付与	読み取り	branches*		
GetDomainAssociation	appId および domainName に対応するドメイン情報を取得するアクセス許可を付与	読み取り	domains*		
GetJob	Amplify アプリケーションの一部である Amplify ブランチのジョブを取得するアクセス許可を付与	読み取り	jobs*		
GetWebACLForResource	リソースに関連付けられた WebACL を取得するアクセス許可を付与します	読み取り	apps*		
GetWebHook	webhookId に対応するウェブフック情報を取得するアクセス許可を付与	読み取り	webhooks*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListApps	既存の Amplify アプリケーションを一覧表示するアクセス許可を付与	リスト			
ListArtifacts	アプリケーション、ブランチ、ジョブ、およびアーティファクトタイプとともにアーティファクトを一覧表示するアクセス許可を付与	リスト	apps*		
ListBackendEnvironments	Amplify アプリケーションのバックエンド環境を一覧表示するアクセス許可を付与	リスト	apps*		
ListBranches	Amplify アプリケーションのブランチを一覧表示するアクセス許可を付与	リスト	apps*		
ListDomainAssociations	アプリケーションのドメインを一覧表示するアクセス許可を付与	リスト	apps*		
ListJobs	Amplify アプリケーションの一部である、ブランチのジョブを一覧表示するアクセス許可を付与	リスト	branches*		
ListResourcesForWebACL	WebACL に関連付けられたリソースを一覧表示するアクセス許可を付与します	リスト			
ListTagsForResource	Amplify AWS コンソールリソースのタグを一覧表示するアクセス許可を付与します	読み取り	apps branches		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			domains		
			webhooks		
ListWebHooks	アプリケーションのウェブフックを一覧表示するアクセス許可を付与	リスト	apps*		
StartDeployment	アプリケーションの手動デプロイ用のデプロイを開始するアクセス許可を付与 (アプリケーションはリポジトリに接続されません)	書き込み	branches*		
StartJob	Amplify アプリケーションの一部である、ブランチの新しいジョブを開始するアクセス許可を付与	書き込み	jobs*		
StopJob	Amplify アプリケーションの一部である、ブランチの進行中のジョブを停止するアクセス許可を付与	書き込み	jobs*		
TagResource	Amplify AWS コンソールリソースにタグを付けるアクセス許可を付与します	Tagging	apps		
			branches		
			domains		
			webhooks		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Amplify AWS コンソールリソースからタグを削除するアクセス許可を付与します	Tagging	apps		
			branches		
			domains		
			webhooks		
				aws:TagKeys	
UpdateApp	既存の Amplify アプリケーションを更新するアクセス許可を付与	書き込み	apps*		
UpdateBranch	Amplify アプリケーションのブランチを更新するアクセス許可を付与	書き込み	branches*		
UpdateDomainAssociation	アプリケーションで DomainAssociation を更新するアクセス許可を付与	書き込み	domains*		
UpdateWebHook	ウェブフックを更新するアクセス許可を付与	書き込み	webhooks*		

AWS Amplify で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
apps	arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}	aws:ResourceTag/${TagKey}
branches	arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}/branches/${BranchName}	aws:ResourceTag/${TagKey}
jobs	arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}/branches/${BranchName}/jobs/${JobId}	
domains	arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}/domains/${DomainName}	aws:ResourceTag/${TagKey}
webhooks	arn:${Partition}:amplify:${Region}:${Account}:webhooks/${WebhookId}	aws:ResourceTag/${TagKey}

AWS Amplify の条件キー

AWS Amplify は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグのキーと値でアクセスをフィルター	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグのキーでアクセスをフィルタリング	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Amplify Admin のアクション、リソース、および条件キー

AWS Amplify Admin (サービスプレフィックス: amplifybackend) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Amplify Admin で定義されるアクション
- AWS Amplify Admin で定義されるリソースタイプ
- AWS Amplify Admin の条件キー

AWS Amplify Admin で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CloneBackend	既存の Amplify Admin バックエンド環境を新しい Amplify Admin バックエンド環境にクローンとして複製するアクセス許可を付与	Write	backend*		
CreateBackend	Amplify AppId に新しい Amplify Admin バックエンド環境を作成するアクセス許可を付与	Write	created-backend*		
CreateBackendAPI	AppId と backendEnvironmentName を併用して、既存の Amplify Admin バックエンド環境の API を作成するアクセス許可を付与	Write	api*		
			backend*		
			environment*		
CreateBackendAuth	AppId と backendEnvironmentName を併用して、既存の Amplify Admin バックエンド環境の認証リソースを作成するアクセス許可を付与	Write	auth*		
			backend*		
			environment*		
CreateBackendConfig	Amplify AppId で新しい Amplify Admin バックエンド設定を作成するアクセス許可を付与	書き込み	config*		
CreateBackendStorage	バックエンドストレージリソースを作成する許可を付与	書き込み	backend*		
			environment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			storage*		
CreateToken	AppId で Amplify Admin チャレンジトークンを作成するアクセス許可を付与	Write	backend*		
			token*		
DeleteBackend	AppId と backendEnvironmentName を併用して、既存の Amplify Admin バックエンド環境を削除するアクセス許可を付与	Write	backend*		
			environment*		
DeleteBackendAPI	AppId と backendEnvironmentName を併用して、既存の Amplify Admin バックエンド環境の API を削除するアクセス許可を付与	Write	api*		
			backend*		
			environment*		
DeleteBackendAuth	AppId と backendEnvironmentName を併用して、既存の Amplify Admin バックエンド環境の認証リソースを削除するアクセス許可を付与	書き込み	auth*		
			backend*		
			environment*		
DeleteBackendStorage	バックエンドストレージリソースを削除する許可を付与	書き込み	backend*		
			environment*		
			storage*		
DeleteToken	AppId で Amplify Admin チャレンジトークンを削除するアクセス許可を付与	Write	backend*		
			token*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GenerateBackendAPIModels	AppId と backendEnvironmentName を併用して、既存の Amplify Admin バックエンド環境の API のモデルを生成するアクセス許可を付与	Write	api*		
			backend*		
			environment*		
GetBackend	AppId と backendEnvironmentName を併用して、既存の Amplify Admin バックエンド環境を取得するアクセス許可を付与	Read	backend*		
			environment*		
GetBackendAPI	AppId と backendEnvironmentName を併用して、既存の Amplify Admin バックエンド環境の API を取得するアクセス許可を付与	Read	api*		
			backend*		
			environment*		
GetBackendAPIModels	AppId と backendEnvironmentName を併用して、既存の Amplify Admin バックエンド環境の API のモデルを取得するアクセス許可を付与	Read	api*		
			backend*		
			environment*		
GetBackendAuth	AppId と backendEnvironmentName を併用して、既存の Amplify Admin バックエンド環境の認証リソースを取得するアクセス許可を付与	Read	auth*		
			backend*		
			environment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetBackendJob	AppId と backendEnvironmentName を併用して、既存の Amplify Admin バックエンド環境のジョブを取得するアクセス許可を付与	読み取り	backend*		
			job*		
GetBackendStorage	既存のバックエンドストレージリソースを取得する許可を付与	読み取り	backend*		
			environment*		
GetToken	AppId で Amplify Admin チャレンジトークンを取得するアクセス許可を付与	Read	backend*		
			token*		
ImportBackendAuth	AppId と backendEnvironmentName を併用して、既存の Amplify Admin バックエンド環境の認証リソースをインポートする許可を付与	書き込み	auth*		
			backend*		
			environment*		
ImportBackendStorage	既存のバックエンドストレージリソースをインポートする許可を付与	書き込み	backend*		
			environment*		
			storage*		
ListBackendJobs	AppId と backendEnvironmentName を併用して、既存の Amplify Admin バックエンド環境のジョブを取得するアクセス許可を付与	リスト	backend*		
			job*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListS3Buckets	S3 バケットを取得する許可を付与	リスト			s3:ListAllMyBuckets
RemoveAllBackends	AppId で既存の Amplify Admin バックエンド環境を削除するアクセス許可を付与	Write	backend*		
			environment*		
RemoveBackendConfig	Amplify AppId で Amplify Admin バックエンド設定を削除するアクセス許可を付与	Write	config*		
UpdateBackendAPI	AppId と backendEnvironmentName を併用して、既存の Amplify Admin バックエンド環境の API を更新するアクセス許可を付与	Write	api*		
			backend*		
			environment*		
UpdateBackendAuth	AppId と backendEnvironmentName を併用して、既存の Amplify Admin バックエンド環境の認証リソースを更新するアクセス許可を付与	Write	auth*		
			backend*		
			environment*		
UpdateBackendConfig	Amplify AppId で Amplify Admin バックエンド設定を更新するアクセス許可を付与	Write	config*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateBackendJob	AppId と backendEnvironmentName を併用して、既存の Amplify Admin バックエンド環境のジョブを更新するアクセス許可を付与	書き込み	backend*		
			job*		
UpdateBackendStorage	バックエンドストレージリソースを更新する許可を付与	書き込み	backend*		
			environment*		
			storage*		

AWS Amplify Admin で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
created-backend	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/*`	
backend	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/*`	
environment	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/environments/*`	

リソースタイプ	ARN	条件キー
api	arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/api/*	
auth	arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/auth/*	
job	arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/job/*	
config	arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/config/*	
token	arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/challenge/*	
storage	arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/storage/*	

AWS Amplify Admin の条件キー

Amplify Admin には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Amplify UIのアクション、リソース、および条件キー

AWS Amplify UI Builder (サービスプレフィックス: amplifyuibuilder) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Amplify UI Builderで定義されるアクション
- AWS Amplify UI Builderで定義されるリソースタイプ
- AWS Amplify UI Buikderの条件キー

AWS Amplify UI Builderで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateComponent	コンポーネントを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp amplifyuibuilder:GetComponent amplifyuibuilder:TagResource
CreateForm	フォームを作成する許可を付与	書き込み		aws:RequestTag/${TagKey}	amplify:GetApp

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:TagKeys	amplifyuibuilder:GetForm amplifyuibuilder:TagResource amplifyuibuilder:UntagResource
CreateTheme	テーマを作成するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp amplifyuibuilder:GetTheme amplifyuibuilder:TagResource
DeleteComponent	コンポーネントを削除する許可を付与	書き込み	ComponentResource*		amplify:GetApp amplifyuibuilder:UntagResource

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteForm	フォームを削除する許可を付与	書き込み	FormResource*		amplify:GetApp amplifyuibuilder:TagResource amplifyuibuilder:UntagResource
DeleteTheme	テーマを削除するアクセス許可を付与	書き込み	ThemeResource*		amplify:GetApp amplifyuibuilder:UntagResource
ExchangeCodeForToken	コードをトークンと交換する権限を付与します。	書き込み			
ExportComponents	コンポーネントをエクスポートするアクセス許可を付与します。	読み取り			
ExportForms	フォームをエクスポートする許可を付与	読み取り			
ExportThemes	テーマをエクスポートするアクセス許可を付与します。	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetCodegenJob	既存の codegen ジョブを取得する許可を付与	読み取り	CodegenJobResource*		amplify:GetApp
GetComponent	既存のコンポーネントを取得するためのアクセス許可を付与します。	読み取り	ComponentResource*		amplify:GetApp
GetForm	既存のフォームを取得する許可を付与	読み取り	FormResource*		amplify:GetApp
GetMetadata	既存のメタデータを取得する許可を付与	読み取り			
GetTheme	既存のテーマを取得する許可を付与します。	読み取り	ThemeResource*		amplify:GetApp
ListCodegenJobs	codegen ジョブを一覧表示する許可を付与	リスト			amplify:GetApp
ListComponents	コンポーネントを一覧表示する許可の付与	リスト			amplify:GetApp
ListForms	フォームを一覧表示する許可を付与	リスト			amplify:GetApp
ListTagsForResource	指定された Amazon リソースネーム (ARN) のタグを一覧表示する許可を付与する	リスト	CodegenJobResource		
			ComponentResource		
			FormResource		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			ThemeResource		
ListThemes	テーマを一覧表示する許可を付与	リスト			amplify:GetApp
PutMetadataFlag	既存のメタデータを配置する許可を付与	書き込み			
RefreshToken	アクセストークンを refresh する許可を付与します。	書き込み			
ResetMetadataFlag	既存のメタデータをリセットする許可を付与	書き込み			
StartCodegenJob	codegen ジョブを開始する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp
TagResource	タグキーと値でリソースにタグを付ける許可を付与する	Tagging	CodegenJobResource		
			ComponentResource		
			FormResource		
			ThemeResource		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	指定された Amazon リソースネーム (ARN) でリソースのタグを解除する許可を付与する	Tagging	CodegenJobResource		
			ComponentResource		
			FormResource		
			ThemeResource		
				aws:TagKeys	
UpdateComponent	コンポーネントを更新するアクセス許可の付与します	書き込み	ComponentResource*		amplify:GetApp amplifyuibuilder:TagResource amplifyuibuilder:UntagResource

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateForm	フォームを更新する許可を付与	書き込み	FormResource*		amplify:GetApp amplifyuibuilder:GetForm amplifyuibuilder:TagResource amplifyuibuilder:UntagResource
UpdateTheme	テーマを更新するアクセス許可を付与	書き込み	ThemeResource*		amplify:GetApp amplifyuibuilder:GetTheme amplifyuibuilder:TagResource amplifyuibuilder:UntagResource

AWS Amplify UI Builderで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
CodegenJobResource	`arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/codegen-jobs/${Id}`	amplifyuibuilder:CodegenJobResourceAppId amplifyuibuilder:CodegenJobResourceEnvironmentName amplifyuibuilder:CodegenJobResourceId aws:ResourceTag/${TagKey}
ComponentResource	`arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/components/${Id}`	amplifyuibuilder:ComponentResourceAppId amplifyuibuilder:ComponentResourceEnvironmentName amplifyuibuilder:ComponentResourceId aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
FormResource	arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/forms/${Id}	amplifyuibuilder:FormResourceAppId amplifyuibuilder:FormResourceEnvironmentName amplifyuibuilder:FormResourceId aws:ResourceTag/${TagKey}
ThemeResource	arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/themes/${Id}	amplifyuibuilder:ThemeResourceAppId amplifyuibuilder:ThemeResourceEnvironmentName amplifyuibuilder:ThemeResourceId aws:ResourceTag/${TagKey}

AWS Amplify UI Buikderの条件キー

AWS Amplify UI Builder では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
amplifyuibuilder:CodegenJobResourceAppId	アプリケーション ID でアクセスをフィルタリングします。	String
amplifyuibuilder:CodegenJobResourceEnvironmentName	バックエンド 環境名でアクセスをフィルタリングします。	String
amplifyuibuilder:CodegenJobResourceId	codegen ジョブ ID でアクセスをフィルタリングします。	String
amplifyuibuilder:ComponentResourceAppId	アプリケーション ID でアクセスをフィルタリングします。	String
amplifyuibuilder:ComponentResourceEnvironmentName	バックエンド 環境名でアクセスをフィルタリングします。	String
amplifyuibuilder:ComponentResourceId	コンポーネント ID でアクセスをフィルタリングします。	String
amplifyuibuilder:FormResourceAppId	アプリケーション ID でアクセスをフィルタリングします。	String

条件キー	説明	[Type] (タイプ)
amplifyuibuilder:FormResourceEnvironmentName	バックエンド 環境名でアクセスをフィルタリングします。	String
amplifyuibuilder:FormResourceId	フォーム ID によりアクセスをフィルタリング	String
amplifyuibuilder:ThemeResourceAppId	アプリケーション ID でアクセスをフィルタリングします。	String
amplifyuibuilder:ThemeResourceEnvironmentName	バックエンド 環境名でアクセスをフィルタリングします。	String
amplifyuibuilder:ThemeResourceId	テーマ ID でアクセスをフィルタリングします。	String
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon MSK クラスター用の Apache Kafka API のアクション、リソース、および条件キー

Amazon MSK クラスター用の Apache Kafka API (サービスプレフィックス: `kafka-cluster`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon MSK クラスター用の Apache Kafka API によって定義されたアクション
- Amazon MSK クラスター用の Apache Kafka API によって定義されたリソースタイプ
- Amazon MSK クラスター用の Apache Kafka API の条件キー

Amazon MSK クラスター用の Apache Kafka API によって定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AlterCluster	Apache Kafka の ALTER CLUSTER ACL に相当する、クラスターのさまざまな側面を変更するためのアクセス許可を付与	Write	cluster*		kafka-cluster:Connect kafka-cluster:DescribeCluster
AlterClusterDynami	Apache Kafka の ALTER_CONFIGS CLUSTER ACL に相当する、クラスター	Write	cluster*		kafka-cluster:Connect

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
cConfiguration	の動的設定を変更するためのアクセス許可を付与				kafka-cluster:DescribeClusterDynamicConfiguration
AlterGroup	Apache Kafka の READ GROUP ACL に相当する、クラスター上のグループに参加させるためのアクセス許可を付与	Write	group*		kafka-cluster:Connect kafka-cluster:DescribeGroup
AlterTopic	Apache Kafka の ALTER TOPIC ACL に相当する、クラスター上のトピックを変更するためのアクセス許可を付与	Write	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic
AlterTopicDynamicConfiguration	Apache Kafka の ALTER_CONFIGS TOPIC ACL に相当する、クラスターのトピックの動的設定を変更するためのアクセス許可を付与	Write	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopicDynamicConfiguration

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AlterTransactionalId	Apache Kafka の WRITE TRANSACTIONAL_ID ACL に相当する、クラスター上のトランザクション ID を変更するためのアクセス許可を付与	Write	transactional-id*		kafka-cluster:Connect kafka-cluster:DescribeTransactionalId kafka-cluster:WriteData
Connect	クラスターに接続して認証するためのアクセス許可を付与	Write	cluster*		
CreateTopic	Apache Kafka の CREATE CLUSTER/TOPIC ACL に相当する、クラスター上のトピックを作成するためのアクセス許可を付与	Write	topic*		kafka-cluster:Connect
DeleteGroup	Apache Kafka の DELETE GROUP ACL に相当する、クラスター上のグループを削除するためのアクセス許可を付与	Write	group*		kafka-cluster:Connect kafka-cluster:DescribeGroup

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteTopic	Apache Kafka の DELETE TOPIC ACL に相当する、クラスター上のトピックを削除するためのアクセス許可を付与	Write	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic
DescribeCluster	Apache Kafka の DESCRIBE CLUSTER ACL に相当する、クラスターのさまざまな側面を記述するためのアクセス許可を付与	リスト	cluster*		kafka-cluster:Connect
DescribeClusterDynamicConfiguration	Apache Kafka の DESCRIBE_CONFIGS CLUSTER ACL に相当する、クラスターの動的設定を記述するためのアクセス許可を付与	リスト	cluster*		kafka-cluster:Connect
DescribeGroup	Apache Kafka の DESCRIBE GROUP ACL に相当する、クラスター上のグループを記述するためのアクセス許可を付与	リスト	group*		kafka-cluster:Connect
DescribeTopic	Apache Kafka の DESCRIBE TOPIC ACL に相当する、クラスター上のトピックを記述するためのアクセス許可を付与	リスト	topic*		kafka-cluster:Connect

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeTopicDynamicConfiguration	Apache Kafka の DESCRIBE_CONFIGS TOPIC ACL に相当する、クラスターのトピックの動的設定を記述するためのアクセス許可を付与	リスト	topic*		kafka-cluster:Connect
DescribeTransactionalId	Apache Kafka の DESCRIBE TRANSACTIONAL_ID ACL に相当する、クラスター上のトランザクション ID を記述するためのアクセス許可を付与	リスト	transactional-id*		kafka-cluster:Connect
ReadData	Apache Kafka の READ TOPIC ACL に相当する、クラスター上のトピックからデータを読み取るためのアクセス許可を付与	Read	topic*		kafka-cluster:AlterGroup kafka-cluster:Connect kafka-cluster:DescribeTopic
WriteData	Apache Kafka の WRITE TOPIC ACL に相当する、クラスター上のトピックにデータを書き込むためのアクセス許可を付与	Write	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
WriteDataIdempotently	Apache Kafka の IDEMPOTENT_WRITE CLUSTER ACL に相当する、クラスター上でべき等的にデータを書き込むためのアクセス許可を付与	Write	cluster*		kafka-cluster:Connect kafka-cluster:WriteData

Amazon MSK クラスター用の Apache Kafka API によって定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
cluster	arn:${Partition}:kafka:${Region}:${Account}:cluster/${ClusterName}/${ClusterUuid}	aws:ResourceTag/${TagKey}
topic	arn:${Partition}:kafka:${Region}:${Account}:topic/${ClusterName}/${ClusterUuid}/${TopicName}	
group	arn:${Partition}:kafka:${Region}:${Account}:group/${ClusterName}/${ClusterUuid}/${GroupName}	
transactional-id	arn:${Partition}:kafka:${Region}:${Account}:transactional-id/${ClusterNa	

リソースタイプ	ARN	条件キー
	me}/${ClusterUuid}/${TransactionalId}	

Amazon MSK クラスター用の Apache Kafka API の条件キー

Amazon MSK クラスター用の Apache Kafka API では、IAM ポリシーの Condition 要素で使用できる次の条件キーが定義されます。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアに基づいてアクションをフィルタリングします。リソースタグコンテキストキーは、トピック、グループ、トランザクション ID ではなく、クラスターリソースにのみ適用されます。	文字列

Amazon API Gateway のアクション、リソース、および条件キー

Amazon API Gateway (サービスプレフィックス: execute-api) には、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon API Gateway で定義されるアクション
- Amazon API Gateway で定義されるリソースタイプ
- Amazon API Gateway の条件キー

Amazon API Gateway で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
InvalidateCache	クライアントリクエスト時に API キャッシュを無効にします。	Write	execute-api-general*		
Invoke	クライアントリクエスト時に API を呼び出します。	Write	execute-api-domain		
			execute-api-general		
ManageConnections	ManageConnections は @connections API へのアクセスを制御します	Write	execute-api-general*		

Amazon API Gateway で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
execute-api-general	arn:${Partition}:execute-api:${Region}:${Account}:${ApiId}/${Stage}/${Method}/${ApiSpecificResourcePath}	execute-api:viaDomainArn
execute-api-domain	arn:${Partition}:execute-api:${Region}:${Account}:/domainnames/${DomainName} ${DomainIdentifier}	

Amazon API Gateway の条件キー

Amazon API Gateway では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
execute-api:viaDomainArn	API が呼び出されるドメイン名 ARN でアクセスをフィルタリングします	String

AWS App Mesh のアクション、リソース、および条件キー

AWS App Mesh (サービスプレフィックス: appmesh) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS App Mesh で定義されるアクション
- AWS App Mesh で定義されるリソースタイプ
- AWS App Mesh の条件キー

AWS App Mesh で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateGatewayRoute	仮想ゲートウェイに関連付けられたゲートウェイルートを作成する許可を付与	書き込み	gatewayRoute*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualService		
CreateMesh	サービスメッシュを作成する許可を付与	書き込み	mesh*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRoute	仮想ルーターに関連付けられたルートを作成する許可を付与	書き込み	route*	aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			virtualNode		
CreateVirtualGateway	サービスメッシュ内に仮想ゲートウェイを作成する許可を付与	書き込み	virtualGateway*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateVirtualNode	サービスメッシュ内に仮想ノードを作成する許可を付与	書き込み	virtualNode*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualService		
CreateVirtualRouter	サービスメッシュ内に仮想ルーターを作成する許可を付与	書き込み	virtualRouter*		
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateVirtualService	サービスメッシュ内に仮想サービスを作成する許可を付与	書き込み	virtualService*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualNode		
			virtualRouter		
DeleteGatewayRoute	既存のゲートウェイルートを削除する許可を付与	書き込み	gatewayRoute*		
DeleteMesh	既存のサービスメッシュを削除する許可を付与	書き込み	mesh*		
DeleteMeshPolicy [アクセス許可のみ]	メッシュの RAM アクセス制御ポリシーを削除する許可を付与する	書き込み	mesh*		
DeleteRoute	既存のルートを削除する許可を付与	書き込み	route*		
DeleteVirtualGateway	既存の仮想ゲートウェイを削除する許可を付与	書き込み	virtualGateway*		
DeleteVirtualNode	既存の仮想ノードを削除する許可を付与	書き込み	virtualNode*		
DeleteVirtualRouter	既存の仮想ルーターを削除する許可を付与	書き込み	virtualRouter*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteVirtualService	既存の仮想サービスを削除する許可を付与	書き込み	virtualService*		
DescribeGatewayRoute	既存のゲートウェイルートを記述する許可を付与	読み込み	gatewayRoute*		
DescribeMesh	既存のサービスメッシュを記述する許可を付与	読み込み	mesh*		
DescribeRoute	既存のルートを記述する許可を付与	読み込み	route*		
DescribeVirtualGateway	既存の仮想ゲートウェイを記述する許可を付与	読み込み	virtualGateway*		
DescribeVirtualNode	既存の仮想ノードを記述する許可を付与	読み込み	virtualNode*		
DescribeVirtualRouter	既存の仮想ルーターを記述する許可を付与	読み込み	virtualRouter*		
DescribeVirtualService	既存の仮想サービスを記述する許可を付与	読み取り	virtualService*		
GetMeshPolicy [許可のみ]	メッシュの RAM アクセス制御ポリシーを読み取る許可を付与する	読み取り	mesh*		
ListGatewayRoutes	サービスメッシュ内の既存のゲートウェイルートを一覧表示する許可を付与	リスト	virtualGateway*		
ListMeshes	既存のサービスメッシュを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListRoutes	サービスメッシュ内の既存のルートを一覧表示する許可を付与	リスト	virtualRouter*		
ListTagsForResource	App Mesh リソースのタグを一覧表示する許可を付与	リスト	gatewayRoute		
			mesh		
			route		
			virtualGateway		
			virtualNode		
			virtualRouter		
			virtualService		
ListVirtualGateways	サービスメッシュ内の既存の仮想ゲートウェイを一覧表示する許可を付与	リスト	mesh*		
ListVirtualNodes	既存の仮想ノードを一覧表示する許可を付与	リスト	mesh*		
ListVirtualRouters	サービスメッシュ内の既存の仮想ルーターを一覧表示する許可を付与	リスト	mesh*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListVirtualServices	サービスメッシュ内の既存の仮想サービスを一覧表示する許可を付与	リスト	mesh*		
PutMeshPolicy [許可のみ]	メッシュの RAM アクセス制御ポリシーを定義する許可を付与する	書き込み	mesh*		
StreamAggregatedResources	App Mesh エンドポイント (VirtualNode/VirtualGateway) のストリームリソースを受信する許可を付与	読み込み	virtualGateway		
			virtualNode		
TagResource	指定された resourceArn でリソースにタグを付けるためのアクセス権限を付与します	Tagging	gatewayRoute		
			mesh		
			route		
			virtualGateway		
			virtualNode		
			virtualRouter		
			virtualService		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	リソースからタグを削除する許可を付与	Tagging	gatewayRoute		
			mesh		
			route		
			virtualGateway		
			virtualNode		
			virtualRouter		
			virtualService		
				aws:TagKeys	
UpdateGatewayRoute	指定されたサービスメッシュおよび仮想ゲートウェイの既存のゲートウェイルートを更新する許可を付与	書き込み	gatewayRoute*		
			virtualService		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateMesh	既存のサービスメッシュを更新する許可を付与	書き込み	mesh*		
UpdateRoute	指定されたサービスメッシュおよび仮想ルーターの既存のルートを更新する許可を付与	書き込み	route*		
			virtualNode		
UpdateVirtualGateway	指定されたサービスメッシュ内の既存の仮想ゲートウェイを更新する許可を付与	書き込み	virtualGateway*		
UpdateVirtualNode	指定されたサービスメッシュ内の既存の仮想ノードを更新する許可を付与	書き込み	virtualNode*		
UpdateVirtualRouter	指定されたサービスメッシュ内の既存の仮想ルーターを更新する許可を付与	書き込み	virtualRouter*		
UpdateVirtualService	指定されたサービスメッシュ内の既存の仮想サービスを更新する許可を付与	書き込み	virtualService*		
			virtualNode		
			virtualRouter		

AWS App Mesh で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
mesh	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}	aws:ResourceTag/${TagKey}
virtualService	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualService/${VirtualServiceName}	aws:ResourceTag/${TagKey}
virtualNode	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualNode/${VirtualNodeName}	aws:ResourceTag/${TagKey}
virtualRouter	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}	aws:ResourceTag/${TagKey}
route	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}/route/${RouteName}	aws:ResourceTag/${TagKey}
virtualGateway	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}	aws:ResourceTag/${TagKey}
gatewayRoute	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}/gatewayRoute/${GatewayRouteName}	aws:ResourceTag/${TagKey}

AWS App Mesh の条件キー

AWS App Mesh は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアのプレゼンスによってアクションをフィルタリングします。	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアによってアクションをフィルタリングします。	文字列
aws:TagKeys	リクエスト内のタグキーのプレゼンスによってアクションをフィルタリングします。	ArrayOfString

AWS App Mesh Preview のアクション、リソース、および条件キー

AWS App Mesh Preview (サービスプレフィックス: appmesh-preview) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS App Mesh Preview で定義されるアクション
- AWS App Mesh Preview で定義されるリソースタイプ

- AWS App Mesh Preview の条件キー

AWS App Mesh Preview で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateGatewayRoute	仮想ゲートウェイに関連付けられたゲートウェイルートを作成する許可を付与	書き込み	gatewayRoute*		
			virtualService		
CreateMesh	サービスメッシュを作成する許可を付与	書き込み	mesh*		
CreateRoute	仮想ルーターに関連付けられたルートを作成する許可を付与	書き込み	route*		
			virtualNode		
CreateVirtualGateway	サービスメッシュ内に仮想ゲートウェイを作成する許可を付与	書き込み	virtualGateway*		
CreateVirtualNode	サービスメッシュ内に仮想ノードを作成する許可を付与	書き込み	virtualNode*		
			virtualService		
CreateVirtualRouter	サービスメッシュ内に仮想ルーターを作成する許可を付与	書き込み	virtualRouter*		
CreateVirtualService	サービスメッシュ内に仮想サービスを作成する許可を付与	書き込み	virtualService*		
			virtualNode		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			virtualRouter		
DeleteGatewayRoute	既存のゲートウェイルートを削除する許可を付与	書き込み	gatewayRoute*		
DeleteMesh	既存のサービスメッシュを削除する許可を付与	書き込み	mesh*		
DeleteMeshPolicy [アクセス許可のみ]	メッシュの RAM アクセス制御ポリシーを削除する許可を付与する	書き込み	mesh*		
DeleteRoute	既存のルートを削除する許可を付与	書き込み	route*		
DeleteVirtualGateway	既存の仮想ゲートウェイを削除する許可を付与	書き込み	virtualGateway*		
DeleteVirtualNode	既存の仮想ノードを削除する許可を付与	書き込み	virtualNode*		
DeleteVirtualRouter	既存の仮想ルーターを削除する許可を付与	書き込み	virtualRouter*		
DeleteVirtualService	既存の仮想サービスを削除する許可を付与	書き込み	virtualService*		
DescribeGatewayRoute	既存のゲートウェイルートを記述する許可を付与	読み込み	gatewayRoute*		
DescribeMesh	既存のサービスメッシュを記述する許可を付与	読み込み	mesh*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeRoute	既存のルートを記述する許可を付与	読み込み	route*		
DescribeVirtualGateway	既存の仮想ゲートウェイを記述する許可を付与	読み込み	virtualGateway*		
DescribeVirtualNode	既存の仮想ノードを記述する許可を付与	読み込み	virtualNode*		
DescribeVirtualRouter	既存の仮想ルーターを記述する許可を付与	読み込み	virtualRouter*		
DescribeVirtualService	既存の仮想サービスを記述する許可を付与	読み取り	virtualService*		
GetMeshPolicy [許可のみ]	メッシュの RAM アクセス制御ポリシーを読み取る許可を付与する	読み取り	mesh*		
ListGatewayRoutes	サービスメッシュ内の既存のゲートウェイルートを一覧表示する許可を付与	リスト	virtualGateway*		
ListMeshes	既存のサービスメッシュを一覧表示する許可を付与	リスト			
ListRoutes	サービスメッシュ内の既存のルートを一覧表示する許可を付与	リスト	virtualRouter*		
ListVirtualGateways	サービスメッシュ内の既存の仮想ゲートウェイを一覧表示する許可を付与	リスト	mesh*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListVirtualNodes	既存の仮想ノードを一覧表示する許可を付与	リスト	mesh*		
ListVirtualRouters	サービスメッシュ内の既存の仮想ルーターを一覧表示する許可を付与	リスト	mesh*		
ListVirtualServices	サービスメッシュ内の既存の仮想サービスを一覧表示する許可を付与	リスト	mesh*		
PutMeshPolicy [許可のみ]	メッシュの RAM アクセス制御ポリシーを定義する許可を付与する	書き込み	mesh*		
StreamAggregatedResources	App Mesh エンドポイント (VirtualNode/VirtualGateway) のストリームリソースを受信する許可を付与	Read	virtualGateway		
			virtualNode		
UpdateGatewayRoute	指定されたサービスメッシュおよび仮想ゲートウェイの既存のゲートウェイルートを更新する許可を付与	書き込み	gatewayRoute*		
			virtualService		
UpdateMesh	既存のサービスメッシュを更新する許可を付与	書き込み	mesh*		
UpdateRoute	指定されたサービスメッシュおよび仮想ルーターの既存のルートを更新する許可を付与	書き込み	route*		
			virtualNode		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateVirtualGateway	指定されたサービスメッシュ内の既存の仮想ゲートウェイを更新する許可を付与	書き込み	virtualGateway*		
UpdateVirtualNode	指定されたサービスメッシュ内の既存の仮想ノードを更新する許可を付与	書き込み	virtualNode*		
UpdateVirtualRouter	指定されたサービスメッシュ内の既存の仮想ルーターを更新する許可を付与	書き込み	virtualRouter*		
UpdateVirtualService	指定されたサービスメッシュ内の既存の仮想サービスを更新する許可を付与	Write	virtualService*		
			virtualNode		
			virtualRouter		

AWS App Mesh Preview で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
mesh	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}	
virtualService	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualService/${VirtualServiceName}	
virtualNode	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualNode/${VirtualNodeName}	
virtualRouter	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}	
route	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}/route/${RouteName}	
virtualGateway	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}	
gatewayRoute	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}/gatewayRoute/${GatewayRouteName}	

AWS App Mesh Preview の条件キー

App Mesh Preview には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS App Runner のアクション、リソース、および条件キー

AWS App Runner (サービスプレフィックス: apprunner) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS App Runner で定義されるアクション
- AWS App Runner で定義されるリソースタイプ
- AWS App Runner の条件キー

AWS App Runner で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateCustomDomain	独自のドメイン名を AWS App Runner サービスの App Runner サブドメイン URL に関連付けるアクセス許可を付与します	書き込み	service*		
AssociateWebAcl [アクセス許可のみ]	サービスを AWS WAF ウェブ ACL に関連付けるアクセス許可を付与します	書き込み	service* webacl*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateAutoScalingConfiguration	AWS App Runner 自動スケーリング設定リソースを作成するアクセス許可を付与します	書き込み	autoscalingconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnection	AWS App Runner 接続リソースを作成するアクセス許可を付与します	書き込み	connection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateObservabilityConfiguration	AWS App Runner オブザーバビリティ設定リソースを作成するアクセス許可を付与します	書き込み	observabilityconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateService	AWS App Runner サービスリソースを作成するアクセス許可を付与します	書き込み	service*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			vpcconnector		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys apprunner:ConnectionArn apprunner:AutoScalingConfigurationArn apprunner:ObservabilityConfigurationArn apprunner:VpcConnectorArn	
CreateVpcConnector	AWS App Runner VPC コネクタリソースを作成するアクセス許可を付与します	書き込み	vpcconnector*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVpcIngressConnection	AWS App Runner VpcIngressConnection リソースを作成するアクセス許可を付与します	書き込み	vpcingressconnection*		
				aws:RequestTag/${TagKey} aws:TagKeys apprunner:ServiceArn apprunner:VpcId apprunner:VpcEndpointId	
DeleteAutoScalingConfiguration	AWS App Runner 自動スケーリング設定リソースを削除するアクセス許可を付与します	書き込み	autoscalingconfiguration*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteConnection	AWS App Runner 接続リソースを削除するアクセス許可を付与します	書き込み	connection*		
DeleteObservabilityConfiguration	AWS App Runner オブザーバビリティ設定リソースを削除するアクセス許可を付与します	書き込み	observabilityconfiguration*		
DeleteService	AWS App Runner サービスリソースを削除するアクセス許可を付与します	書き込み	service*		
DeleteVpcConnector	AWS App Runner VPC コネクタリソースを削除するアクセス許可を付与します	書き込み	vpcconnector*		
DeleteVpcIngressConnection	AWS App Runner VpcIngressConnection リソースを削除するアクセス許可を付与します	書き込み	vpcingressconnection*		
DescribeAutoScalingConfiguration	AWS App Runner 自動スケーリング設定リソースの説明を取得するアクセス許可を付与します	読み取り	autoscalingconfiguration*		
DescribeCustomDomains	AWS App Runner サービスに関連付けられたカスタムドメイン名の説明を取得するアクセス許可を付与します	読み取り	service*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeObservabilityConfiguration	AWS App Runner オブザーバビリティ設定リソースの説明を取得するアクセス許可を付与します	読み取り	observabilityconfiguration*		
DescribeOperation	AWS App Runner サービスで発生したオペレーションの説明を取得するアクセス許可を付与します	読み取り	service*		
DescribeService	AWS App Runner サービスリソースの説明を取得するアクセス許可を付与します	読み取り	service*		
DescribeVpcConnector	AWS App Runner VPC コネクタリソースの説明を取得するアクセス許可を付与します	読み取り	vpcconnector*		
DescribeVpcIngressConnection	AWS App Runner VpcIngressConnection リソースの説明を取得するアクセス許可を付与します	読み取り	vpcingressconnection*		
DescribeWebAclForService [許可のみ]	AWS App Runner サービスに関連付けられている AWS WAF ウェブ ACL を取得する許可を付与	読み取り	service*		
DisassociateCustomDomain	AWS App Runner サービスからカスタムドメイン名の関連付けを解除するアクセス許可を付与します	書き込み	service*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisassociateWebAcl [アクセス許可のみ]	サービスと AWS WAF ウェブ ACL の関連付けを解除するアクセス許可を付与します	書き込み	service*		
ListAssociatedServicesForWebAcl [アクセス許可のみ]	AWS WAF ウェブ ACL に関連付けられているサービスを一覧表示するアクセス許可を付与します	リスト	webacl*		
ListAutoScalingConfigurations	の AWS App Runner 自動スケーリング設定のリストを取得するアクセス許可を付与します AWS アカウント	リスト			
ListConnections	内の AWS App Runner 接続のリストを取得するアクセス許可を付与します AWS アカウント	リスト			
ListObservabilityConfigurations	の AWS App Runner オブザーバビリティ設定のリストを取得するアクセス許可を付与します AWS アカウント	リスト			
ListOperations	AWS App Runner サービスリソースで発生したオペレーションのリストを取得するアクセス許可を付与します	リスト	service*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListServices	で実行中の AWS App Runner サービスのリストを取得するアクセス許可を付与します AWS アカウント	リスト			
ListServicesForAutoScalingConfiguration	の App Runner 自動スケーリング設定の関連する AppRunner サービスのリストを取得するアクセス許可を付与します AWS AWS アカウント	リスト	autoscalingconfiguration*		
ListTagsForResource	AWS App Runner リソースに関連付けられたタグを一覧表示するアクセス許可を付与します	読み取り	autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			service		
			vpcconnector		
ListVpcConnectors	内の AWS App Runner VPC コネクタのリストを取得するアクセス許可を付与します AWS アカウント	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListVpcIngressConnections	の AWS App Runner VpcIngressConnections のリストを取得するアクセス許可を付与します AWS アカウント	リスト			
PauseService	アクティブな AWS App Runner サービスを一時停止するアクセス許可を付与します	書き込み	service*		
ResumeService	アクティブな AWS App Runner サービスを再開するアクセス許可を付与します	書き込み	service*		
StartDeployment	AWS App Runner サービスへの手動デプロイを開始するアクセス許可を付与します	書き込み	service*		
TagResource	AWS App Runner リソースにタグを追加またはタグ値を更新するアクセス許可を付与します	Tagging	autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			service		
			vpcconnector		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			vpcingressconnection		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	AWS App Runner リソースからタグを削除するアクセス許可を付与します	Tagging	autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			service		
			vpcconnector		
			vpcingressconnection		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateDefaultAutoScalingConfiguration	AWS App Runner 自動スケーリング設定を のデフォルトに更新するアクセス許可を付与します AWS アカウント	書き込み	autoscalingconfiguration*		
UpdateService	AWS App Runner サービスリソースを更新する許可を付与	書き込み	service*		
			autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			vpcconnector		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				apprunner:ConnectionArn apprunner:AutoScalingConfigurationArn apprunner:ObservabilityConfigurationArn apprunner:VpcConnectorArn	
UpdateVpcIngressConnection	AWS App Runner VpcIngressConnection リソースを更新する許可を付与	書き込み	vpcingressconnection*		
				apprunner:VpcId apprunner:VpcEndpointId	

AWS App Runner で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
service	arn:${Partition}:apprunner:${Region}:${Account}:service/${ServiceName}/${ServiceId}	aws:ResourceTag/${TagKey}
connection	arn:${Partition}:apprunner:${Region}:${Account}:connection/${ConnectionName}/${ConnectionId}	aws:ResourceTag/${TagKey}
autoscalingconfiguration	arn:${Partition}:apprunner:${Region}:${Account}:autoscalingconfiguration/${AutoscalingConfigurationName}/${AutoscalingConfigurationVersion}/${AutoscalingConfigurationId}	aws:ResourceTag/${TagKey}
observabilityconfiguration	arn:${Partition}:apprunner:${Region}:${Account}:observabilityconfiguration/${ObservabilityConfigurationName}/${ObservabilityConfigurationVersion}/${ObservabilityConfigurationId}	aws:ResourceTag/${TagKey}
vpcconnector	arn:${Partition}:apprunner:${Region}:${Account}:vpcconnector/${VpcConnectorName}/${VpcConnectorVersion}/${VpcConnectorId}	aws:ResourceTag/${TagKey}
vpcingressconnection	arn:${Partition}:apprunner:${Region}:${Account}:vpcingressconnection/${V	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
	pcIngressConnectionName}/${VpcIngressConnectionId}	
webacl	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}	

AWS App Runner の条件キー

AWS App Runner は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
apprunner:AutoScalingConfigurationArn	関連付けられた AutoScalingConfiguration リソースの ARN に基づいた CreateService アクションと UpdateService アクションによって、アクセスをフィルタリングします	ARN
apprunner:ConnectionArn	関連付けられた接続リソースの ARN に基づいた CreateService アクションと UpdateService アクションによって、アクセスをフィルタリングします	ARN
apprunner:ObservabilityConfigurationArn	関連付けられた ObservabilityConfiguration リソースの ARN に基づいた CreateService アクションと UpdateService アクションで、アクセスをフィルタリングします	ARN
apprunner:ServiceArn	関連付けられたサービスリソースの ARN に基づいた CreateVpcIngressConnection アクションでアクセスをフィルタリング	ARN

条件キー	説明	[Type] (タイプ)
apprunner:VpcConnectorArn	関連付けられた VpcConnector リソースの ARN に基づいた CreateService アクションと UpdateService アクションによって、アクセスをフィルタリングします	ARN
apprunner:VpcEndpointId	リクエスト内の VPC エンドポイントに基づいた CreateVpcIngressConnection アクションと UpdateVpcIngressConnection アクションでアクセスをフィルタリング	String
apprunner:VpcId	リクエスト内の VPC に基づいた CreateVpcIngressConnection アクションと UpdateVpcIngressConnection アクションでアクセスをフィルタリング	String
aws:RequestTag/${TagKey}	リクエスト内のタグキーおよび値のペアのプレゼンスに基づいてアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアに基づいてアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいたアクションでアクセスをフィルタリングします	ArrayOfString

AWS App Studio のアクション、リソース、および条件キー

AWS App Studio (サービスプレフィックス: `appstudio`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS App Studio で定義されるアクション
- AWS App Studio で定義されるリソースタイプ
- AWS App Studio の条件キー

AWS App Studio で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetAccountStatus [アクセス許可のみ]	アカウントの現在のステータスを記述する許可を付与する	読み取り			
GetEnablementJobStatus [許可のみ]	有効化ジョブのステータスを取得する許可を付与する	読み取り			
StartEnablementJob [許可のみ]	有効化ジョブを送信する許可を付与する	書き込み			
StartRollbackEnablementJob [アクセス許可のみ]	有効化ジョブをロールバックする許可を付与する	書き込み			
StartTeamDeployment [アクセス許可のみ]	チームデプロイを開始する許可を付与する	書き込み			

AWS App Studio で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
instance	`arn:${Partition}:appstudio:${Region}:${Account}:instance/${InstanceId}`	
application	`arn:${Partition}:appstudio:${Region}:${Account}:application/${ApplicationId}`	
connector	`arn:${Partition}:appstudio:${Region}:${Account}:connector/${ConnectionId}`	

AWS App Studio の条件キー

App Studio には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS App2Container のアクション、リソース、条件キー

AWS App2Container (サービスプレフィックス: a2c) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS App2Container によって定義されたアクション
- AWS App2Container で定義されるリソースタイプ
- AWS App2Container の条件キー

AWS App2Container によって定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetContainerizationJobDetails	すべてのコンテナ化ジョブの詳細を取得する許可を付与	読み取り			
GetDeploymentJobDetails	すべてのデプロイジョブの詳細を取得する許可を付与	読み取り			
StartContainerizationJob	コンテナ化ジョブを開始する許可を付与	書き込み			
StartDeploymentJob	デプロイジョブを開始する許可を付与	書き込み			

AWS App2Container で定義されるリソースタイプ

AWS App2Container は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS App2Container へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS App2Container の条件キー

App2Container には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS AppConfig のアクション、リソース、および条件キー

AWS AppConfig (サービスプレフィックス: appconfig) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS AppConfig で定義されるアクション
- AWS AppConfig で定義されるリソースタイプ
- AWS AppConfig の条件キー

AWS AppConfig で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateApplication	アプリケーションを作成する許可を付与。	Write		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateConfigurationProfile	設定プロファイルを作成する許可を付与。	Write	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeploymentStrategy	デプロイ戦略を作成する許可を付与。	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironment	環境を作成する許可を付与	書き込み	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExtension	拡張機能を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateExtensionAssociation	拡張機能の関連付けを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateHostedConfigurationVersion	ホストされた設定バージョンを作成する許可を付与。	Write	application*		
			configurationprofile*		
DeleteApplication	アプリケーションを削除する許可を付与	Write	application*		
DeleteConfigurationProfile	設定プロファイルを削除する許可を付与。	Write	application*		
			configurationprofile*		
DeleteDeploymentStrategy	デプロイ戦略を削除する許可を付与。	Write	deploymentstrategy*		
DeleteEnvironment	環境を削除する許可を付与します	書き込み	application*		
			environment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteExtension	拡張機能を削除する許可を付与	書き込み	extension*		
DeleteExtensionAssociation	拡張機能の関連付けを削除する許可を付与	書き込み	extensionassociation*		
DeleteHostedConfigurationVersion	ホストされた設定バージョンを削除する許可を付与。	書き込み	application*		
			configurationprofile*		
			hostedconfigurationversion*		
GetAccountSettings	アカウント全体の AppConfig 設定を表示する許可を付与する	読み取り			
GetApplication	アプリケーションの詳細を表示する許可を付与。	Read	application*		
				aws:ResourceTag/${TagKey}	
GetConfiguration	設定の詳細を表示する許可を付与。	Read	application*		
			configurationprofile*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			environment*		
				aws:ResourceTag/${TagKey}	
GetConfigurationProfile	設定プロファイルの詳細を表示する許可を付与。	Read	application*		
			configurationprofile*		
				aws:ResourceTag/${TagKey}	
GetDeployment	デプロイの詳細を表示する許可を付与。	Read	application*		
			deployment*		
			environment*		
				aws:ResourceTag/${TagKey}	
GetDeploymentStrategy	デプロイ戦略の詳細を表示する許可を付与。	Read	deploymentstrategy*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
GetEnvironment	環境の詳細を表示する許可を付与。	読み取り	application*		
			environment*		
				aws:ResourceTag/${TagKey}	
GetExtension	拡張機能に関する詳細を表示する許可を付与	読み取り	extension*		
				aws:ResourceTag/${TagKey}	
GetExtensionAssociation	拡張機能の関連付けに関する詳細を表示する許可を付与	読み取り	extensionassociation*		
				aws:ResourceTag/${TagKey}	
GetHostedConfigurationVersion	ホストされた設定バージョンの詳細を表示する許可を付与。	読み取り	application*		
			configurationprofile*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			hostedconfigurationversion*		
GetLatestConfiguration	セキュリティ設定を取得する許可を付与。	読み取り	configuration*		
				aws:ResourceTag/${TagKey}	
ListApplications	アカウントのアプリケーションを一覧表示する許可を付与。	リスト			
ListConfigurationProfiles	アプリケーションの設定プロファイルを一覧表示する許可を付与。	リスト	application*		
ListDeploymentStrategies	アカウントのデプロイ戦略を一覧表示する許可を付与。	リスト			
ListDeployments	環境のデプロイを一覧表示する許可を付与。	リスト	application*		
			environment*		
ListEnvironments	アプリケーションの環境を一覧表示する許可を付与。	リスト	application*		
ListExtensionAssociations	アカウント内の拡張機能の関連付けを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListExtensions	アカウントの拡張機能を一覧表示する許可を付与。	リスト			
ListHostedConfigurationVersions	設定プロファイルのホストされた設定バージョンを一覧表示する許可を付与。	リスト	application*		
			configurationprofile*		
ListTagsForResource	指定したリソースのリソースタグのリストを表示する許可を付与	読み取り	application		
			configurationprofile		
			deployment		
			deploymentstrategy		
			environment		
			extension		
			extensionassociation		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartConfigurationSession	設定セッションを開始するアクセス許可を付与します	書き込み	configuration*		
				aws:ResourceTag/${TagKey}	
StartDeployment	デプロイを開始する許可を付与。	Write	application*		
			configurationprofile*		
			deploymentstrategy*		
			environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StopDeployment	デプロイを停止する許可を付与。	書き込み	application*		
			deployment*		
			environment*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
TagResource	appconfig リソースにタグを付けるアクセス許可を付与します。	Tagging	application		
			configuration		
			configurationprofile		
			deployment		
			deploymentstrategy		
			environment		
			extension		
			extensionassociation		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	appconfig リソースのタグを解除する許可を付与します。	Tagging	application		
			configuration		
			configurationprofile		
			deployment		
			deploymentstrategy		
			environment		
			extension		
			extensionassociation		
				aws:TagKeys	
UpdateAccountSettings	アカウント全体の AppConfig 設定を変更する許可を付与する	書き込み			
UpdateApplication	アプリケーションを変更する許可を付与。	Write	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
UpdateConfigurationProfile	設定プロファイルを変更する許可を付与。	Write	application*		
			configurationprofile*		
				aws:ResourceTag/${TagKey}	
UpdateDeploymentStrategy	デプロイ戦略を変更する許可を付与。	Write	deploymentstrategy*		
				aws:ResourceTag/${TagKey}	
UpdateEnvironment	環境を変更する許可を付与。	書き込み	application*		
			environment*		
				aws:ResourceTag/${TagKey}	
UpdateExtension	拡張機能を変更する許可を付与	書き込み	extension*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
UpdateExtensionAssociation	拡張機能の関連付けを変更する許可を付与	書き込み	extensionassociation*		
				aws:ResourceTag/${TagKey}	
ValidateConfiguration	設定を検証する許可を付与。	Write	application*		
			configurationprofile*		

AWS AppConfig で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
application	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
environment	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}	aws:ResourceTag/${TagKey}
configurationprofile	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/configurationprofile/${ConfigurationProfileId}	aws:ResourceTag/${TagKey}
deploymentstrategy	arn:${Partition}:appconfig:${Region}:${Account}:deploymentstrategy/${DeploymentStrategyId}	aws:ResourceTag/${TagKey}
deployment	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}/deployment/${DeploymentNumber}	aws:ResourceTag/${TagKey}
hostedconfigurationversion	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/configurationprofile/${ConfigurationProfileId}/hostedconfigurationversion/${VersionNumber}	
configuration	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}/configuration/${ConfigurationProfileId}	aws:ResourceTag/${TagKey}
extension	arn:${Partition}:appconfig:${Region}:${Account}:extension/${ExtensionId}/${ExtensionVersionNumber}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
extension association	arn:${Partition}:appconfig:${Region}:${Account}:extensionassociation/${ExtensionAssociationId}	aws:ResourceTag/${TagKey}

AWS AppConfig の条件キー

AWS AppConfig は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	指定されたタグに許可された値のセットに基づいてアクセスをフィルタリングします。	String
aws:ResourceTag/${TagKey}	AWS リソースに割り当てられたタグキーと値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString

AWS AppFabric のアクション、リソース、および条件キー

AWS AppFabric (サービスプレフィックス: appfabric) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS AppFabric によって定義されたアクション
- AWS AppFabric で定義されるリソースタイプ
- AWS AppFabric の条件キー

AWS AppFabric によって定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchGetUserAccessTasks	複数のユーザーにユーザーアクセスタスクを開始するアクセス許可を付与します	書き込み	appbundle*		
ConnectAppAuthorization	アプリケーション権限を接続するための許可を付与します	書き込み	appauthorization*		
			appbundle*		
CreateAppAuthorization	アプリケーションバンドルにアプリケーション権限を作成するための許可を付与します	書き込み	appbundle*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateAppBundle	アカウントのアプリケーションバンドルを作成するための許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIngestion	アプリケーションバンドルのインジェストを作成するための許可を付与します	書き込み	appbundle*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIngestionDestination	アプリケーションバンドルのインジェスト先を作成するための許可を付与します	書き込み	appbundle*		
			ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAppAuthorization	アプリケーションバンドル内のアプリケーション権限を削除するための許可を付与します	書き込み	appauthorization*		
			appbundle*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteAppBundle	アカウントのアプリケーションバンドルを削除するための許可を付与します	書き込み	appbundle*		
DeleteIngestion	アプリケーションバンドル内のインジェストを削除するための許可を付与します	書き込み	appbundle*		
			ingestion*		
DeleteIngestionDestination	インジェスト内の宛先を削除するアクセス許可を付与します	書き込み	appbundle*		
			ingestion*		
			ingestiondestination*		
GetAppAuthorization	アプリケーション権限の詳細を表示するための許可を付与します	読み取り	appauthorization*		
			appbundle*		
				aws:ResourceTag/${TagKey}	
GetAppBundle	アプリケーションバンドルの詳細を表示するための許可を付与します	読み取り	appbundle*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
GetIngestion	インジェストの詳細を表示するアクセス許可を付与します	読み取り	appbundle*		
			ingestion*		
				aws:ResourceTag/${TagKey}	
GetIngestionDestination	インジェスト先の詳細を表示するアクセス許可を付与します	読み取り	appbundle*		
			ingestion*		
			ingestiondestination*		
				aws:ResourceTag/${TagKey}	
ListAppAuthorizations	アプリケーションバンドル内のアプリケーション権限のリストを取得するための許可を付与します	リスト	appbundle*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListAppBundles	アカウント内のアプリケーションバンドルのリストを取得するための許可を付与します	リスト			
ListIngestionDestinations	インジェスト内の宛先のリストを取得するアクセス許可を付与します	リスト	appbundle*		
			ingestion*		
ListIngestions	アプリケーションバンドル内のインジェストのリストを取得するための許可を付与します	リスト	appbundle*		
ListTagsForResource	AppFabric リソースのタグを一覧表示するための許可を付与します	読み取り	appauthorization		
			appbundle		
			ingestion		
			ingestiondestination		
StartIngestion	インジェストを開始するアクセス許可を付与します	書き込み	appbundle*		
			ingestion*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartUserAccessTasks	ユーザーアクセスタスクを開始するアクセス許可を付与します	書き込み	appbundle*		
StopIngestion	インジェストを中止するアクセス許可を付与します	書き込み	appbundle*		
			ingestion*		
TagResource	AppFabric リソースにタグを付けるアクセス許可を付与します	Tagging	appauthorization		
			appbundle		
			ingestion		
			ingestiondestination		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	AppFabric リソースのタグを解除するアクセス許可を付与します	Tagging	appauthorization		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			appbundle		
			ingestion		
			ingestion destination		
				aws:TagKeys	
UpdateAppAuthorization	アプリケーションバンドル内のアプリケーション権限を更新するための許可を付与します	書き込み	appauthorization*		
			appbundle*		
				aws:ResourceTag/${TagKey}	
UpdateIngestionDestination	インジェスト内の宛先を更新するアクセス許可を付与します	書き込み	appbundle*		
			ingestion*		
			ingestion destination*		
				aws:ResourceTag/${TagKey}	

AWS AppFabric で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
appbundle	arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppBundleIdentifier}	aws:ResourceTag/${TagKey}
appauthorization	arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppbundleId}/appauthorization/${AppAuthorizationIdentifier}	aws:ResourceTag/${TagKey}
ingestion	arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppbundleId}/ingestion/${IngestionIdentifier}	aws:ResourceTag/${TagKey}
ingestion destination	arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppbundleId}/ingestion/${IngestionIdentifier}/ingestiondestination/${IngestionDestinationIdentifier}	aws:ResourceTag/${TagKey}

AWS AppFabric の条件キー

AWS AppFabric では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon AppFlow のアクション、リソース、および条件キー

Amazon AppFlow (サービスプレフィックス: appflow) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon AppFlow で定義されるアクション
- Amazon AppFlow で定義されるリソースタイプ
- Amazon AppFlow の条件キー

Amazon AppFlow で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelFlowExecutions	Amazon AppFlow フローの進行中の実行をキャンセルする許可を付与	書き込み	flow*		
CreateConnectorProfile	Amazon AppFlow フローで使用するログインプロファイルを作成する許可を付与。	書き込み			
CreateFlow	Amazon AppFlow フローを作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConnectorProfile	Amazon AppFlow で設定されたログインプロファイルを削除する許可を付与。	書き込み	connectorprofile*		
DeleteFlow	Amazon AppFlow フローを削除する許可を付与。	書き込み	flow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeConnector	Amazon AppFlow に登録されたコネクタの詳細を取得する許可を付与	読み込み	connector*		
DescribeConnectorEntity	Amazon AppFlow で設定されたログインプロファイルにオ	読み込み	connectorprofile*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	ブジェクトのすべてのフィールドを記述する許可を付与。				
DescribeConnectorFields [許可のみ]	Amazon AppFlow で設定されたログインプロファイルにオブジェクトのすべてのフィールドを記述する許可を付与 (コンソールのみ)。	読み込み	connectorprofile*		
DescribeConnectorProfiles	Amazon AppFlow で設定されたすべてのログインプロファイルを記述する許可を付与。	読み込み			
DescribeConnectors	Amazon AppFlow によってサポートされているすべてのコネクタを記述する許可を付与。	読み込み			
DescribeFlow	Amazon AppFlow で設定された特定のフローを記述する許可を付与。	読み込み	flow*		
DescribeFlowExecution [許可のみ]	Amazon AppFlow で設定されたフローのすべてのフロー実行を記述する許可を付与 (コンソールのみ)。	読み込み	flow*		
DescribeFlowExecutionRecords	Amazon AppFlow で設定されたフローのすべてのフロー実行を記述する許可を付与。	読み込み	flow*		
DescribeFlows [許可のみ]	Amazon AppFlow で設定されたすべてのフローを記述するアクセス許可を付与 (コンソールのみ)。	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListConnectorEntities	Amazon AppFlow で設定されたログインプロファイルのすべてのオブジェクトを一覧表示する許可を付与。	リスト	connectorprofile*		
ListConnectorFields [許可のみ]	Amazon AppFlow で設定されたログインプロファイルのすべてのオブジェクトを一覧表示する許可を付与 (コンソールのみ)。	読み込み	connectorprofile*		
ListConnectors	Amazon AppFlow でサポートされているすべてのコネクタを一覧表示する許可を付与	リスト	connector*		
ListFlows	Amazon AppFlow で設定されたすべてのフローを一覧表示する許可を付与。	リスト	flow*		
ListTagsForResource	フローのタグをリストする許可を付与。	読み込み	flow*		
RegisterConnector	Amazon AppFlow コネクタを登録する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
ResetConnectorMetadataCache	Amazon AppFlow がキャッシュに保存したコネクタエンティティのメタデータをリセットするアクセス許可を付与します	書き込み	connectorprofile*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RunFlow [アクセス許可のみ]	Amazon AppFlow で設定されたフローを実行する許可を付与 (コンソールのみ)。	書き込み	flow*		
StartFlow	Amazon AppFlow で設定されたフローを有効化 (スケジュールされたフローおよびイベントでトリガーされるフローの場合) または実行 (オンデマンドフローの場合) する許可を付与。	書き込み	flow*		
StopFlow	Amazon AppFlow で設定されたスケジュールされたフローまたはイベントでトリガーされるフローを無効化する許可を付与。	書き込み	flow*		
TagResource	フローまたはコネクタにタグを付けるアクセス許可を付与します	Tagging	connector		
			flow		
				aws:TagKeys aws:RequestTag/${TagKey}	
UnRegisterConnector	Amazon AppFlow のコネクタを登録解除する許可を付与	書き込み	connector*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	フローまたはコネクタのタグを解除するアクセス許可を付与します	Tagging	connector		
			flow		
				aws:TagKeys	
UpdateConnectorProfile	Amazon AppFlow で設定されたログインプロファイルを更新する許可を付与。	書き込み	connectorprofile*		
UpdateConnectorRegistration	Amazon AppFlow に設定された登録コネクタを更新する許可を付与	書き込み	connector*		
UpdateFlow	Amazon AppFlow で設定されたフローを更新する許可を付与。	書き込み	flow*		
UseConnectorProfile [アクセス許可のみ]	Amazon AppFlow でフローを作成するときに、コネクタプロファイルを使用する許可を付与	書き込み	connectorprofile*		

Amazon AppFlow で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアク

ションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
connector profile	`arn:${Partition}:appflow:${Region}:${Account}:connectorprofile/${ProfileName}`	
flow	`arn:${Partition}:appflow:${Region}:${Account}:flow/${FlowName}`	aws:ResourceTag/${TagKey}
connector	`arn:${Partition}:appflow:${Region}:${Account}:connector/${ConnectorLabel}`	aws:ResourceTag/${TagKey}

Amazon AppFlow の条件キー

Amazon AppFlow では、IAM ポリシーの `Condition` 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	各タグの許可された値のセットでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値でアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内の必須タグが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

Amazon AppIntegrations のアクション、リソース、および条件キー

Amazon AppIntegrations (サービスプレフィックス: `app-integrations`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon AppIntegrations によって定義されたアクション
- Amazon AppIntegrations によって定義されたリソースタイプ
- Amazon AppIntegrations の条件キー

Amazon AppIntegrations によって定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateApplication	新しいアプリケーションを作成するアクセス許可を付与します	書き込み	application*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy
				aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
CreateApplicationAssociation [アクセス許可のみ]	ApplicationAssociation を作成する許可を付与	書き込み	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateDataIntegration	新しい DataIntegration を作成するアクセス許可を付与	書き込み	data-integration*		appflow:DeleteFlow appflow:DescribeConnectorProfiles iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy kms:CreateGrant profile:GetDomain profile:GetProfileObjectType s3:GetBucketNotification

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					s3:GetEncryptionConfiguration s3:PutBucketNotification
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateDataIntegrationAssociation	DataIntegrationAssociation を作成するアクセス許可を付与	書き込み	data-integration*		appflow:CreateFlow appflow:DeleteFlow appflow:DescribeConnectorEntity appflow:DescribeConnectorProfiles appflow:TagResource appflow:UseConnectorProfile profile:CreateSnapshot profile:GetSnapshot

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataIntegrationSchedule	データ統合スケジュールを作成するアクセス許可を付与します	書き込み	data-integration*		
CreateEventIntegration	新しい EventIntegration を作成するアクセス許可を付与	書き込み	event-integration*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventIntegrationAssociation [アクセス許可のみ]	EventIntegrationAssociation を作成するアクセス許可を付与	書き込み	event-integration*		events:PutRule events:PutTargets

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	アプリケーションを削除する許可を付与	書き込み	application*		
				aws:ResourceTag/${TagKey}	
DeleteApplicationAssociation [アクセス許可のみ]	ApplicationAssociation の割り当てを削除する許可を付与	書き込み	application-association*		
DeleteDataIntegration	DataIntegration を削除するアクセス許可を付与	書き込み	data-integration*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteDataIntegrationAssociation [アクセス許可のみ]	DataIntegrationAssociation を削除するアクセス許可を付与	書き込み	data-integration-association*		appflow:CreateFlow appflow:DeleteFlow appflow:DescribeConnectorEntity appflow:DescribeConnectorProfiles appflow:StopFlow appflow:TagResource appflow:UseConnectorProfile
DeleteEventIntegration	EventIntegration を削除するアクセス許可を付与	書き込み	event-integration*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteEventIntegrationAssociation [アクセス許可のみ]	EventIntegrationAssociation を削除するアクセス許可を付与	書き込み	event-integration-association*		events:DeleteRule events:ListTargetsByRule events:RemoveTargets
GetApplication	アプリケーションの詳細を表示するアクセス許可を付与します	読み取り	application*		
				aws:ResourceTag/${TagKey}	
GetDataIntegration	DataIntegrations の詳細を表示するアクセス許可を付与	読み取り	data-integration*		
				aws:ResourceTag/${TagKey}	
GetDataIntegrationExecution	データ統合の実行に関する詳細を取得するアクセス許可を付与します	読み取り	data-integration*		
GetDataIntegrationSchedule	データ統合スケジュールに関する詳細を取得するアクセス許可を付与します	読み取り	data-integration*		
GetEventIntegration	EventIntegrations の詳細を表示するアクセス許可を付与	読み取り	event-integration*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
ListApplicationAssociations	ApplicationAssociations を一覧表示する許可を付与	リスト			
ListApplications	アプリケーションを一覧表示するアクセス許可を付与します	リスト			
ListDataIntegrationAssociations	DataIntegrationAssociations を一覧表示するアクセス許可を付与	リスト			
ListDataIntegrationExecutions	データ統合の実行を一覧表示するアクセス許可を付与します	リスト	data-integration*		
ListDataIntegrationSchedules	データ統合スケジュールを一覧表示する許可を付与	リスト	data-integration*		
ListDataIntegrations	DataIntegrations を一覧表示するアクセス許可を付与	リスト			
ListEventIntegrationAssociations	EventIntegrationAssociations を一覧表示するアクセス許可を付与	読み込み			
ListEventIntegrations	EventIntegrations を一覧表示するアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTagsForResource	Amazon AppIntegration リソースのタグを一覧表示する許可を付与	読み取り	application		
			data-integration		
			data-integration-association		
			event-integration		
			event-integration-association		
				aws:ResourceTag/${TagKey}	
StartDataIntegrationExecution	データ統合の実行を開始するアクセス許可を付与します	書き込み	data-integration*		profile:CreateSegmentSnapshot profile:CreateSnapshot
TagResource	Amazon AppIntegration リソースにタグを付けるアクセス許可を付与	Tagging	application		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			application-association		
			data-integration		
			data-integration-association		
			event-integration		
			event-integration-association		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Amazon AppIntegration リソースのタグを解除するアクセス許可を付与	Tagging	application		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			application-association		
			data-integration		
			data-integration-association		
			event-integration		
			event-integration-association		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateApplication	アプリケーションを変更するアクセス許可を付与します	書き込み	application*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateDataIntegration	DataIntegration を変更するアクセス許可を付与	書き込み	data-integration*		
				aws:ResourceTag/${TagKey}	
UpdateDataIntegrationAssociation	DataIntegrationAssociation を変更する許可を付与する	書き込み	data-integration-association*		profile:CreateSnapshot profile:GetSnapshot
				aws:ResourceTag/${TagKey}	
UpdateDataIntegrationSchedule	データ統合スケジュールを更新する許可を付与	書き込み	data-integration*		
UpdateEventIntegration	EventIntegration を変更するアクセス許可を付与	書き込み	event-integration*		
				aws:ResourceTag/${TagKey}	

Amazon AppIntegrations によって定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアク

ションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
event-integration	arn:${Partition}:app-integrations:${Region}:${Account}:event-integration/${EventIntegrationName}	aws:ResourceTag/${TagKey}
event-integration-association	arn:${Partition}:app-integrations:${Region}:${Account}:event-integration-association/${EventIntegrationName}/${ResourceId}	aws:ResourceTag/${TagKey}
data-integration	arn:${Partition}:app-integrations:${Region}:${Account}:data-integration/${DataIntegrationId}	aws:ResourceTag/${TagKey}
data-integration-association	arn:${Partition}:app-integrations:${Region}:${Account}:data-integration-association/${DataIntegrationId}/${ResourceId}	aws:ResourceTag/${TagKey}
application	arn:${Partition}:app-integrations:${Region}:${Account}:application/${ApplicationId}	aws:ResourceTag/${TagKey}
application-association	arn:${Partition}:app-integrations:${Region}:${Account}:application-association/${ApplicationId}/${ApplicationAssociationId}	aws:ResourceTag/${TagKey}

Amazon AppIntegrations の条件キー

Amazon AppIntegrations では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストで渡されたタグによりアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグによりアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーによりアクセスをフィルタリングします	ArrayOfString

AWS Application Auto Scaling のアクション、リソース、および条件キー

AWS Application Auto Scaling (サービスプレフィックス: application-autoscaling) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Application Auto Scaling で定義されるアクション
- AWS Application Auto Scaling で定義されるリソースタイプ

- AWS Application Auto Scaling の条件キー

AWS Application Auto Scaling で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteScalingPolicy	スケーリングポリシーを削除する許可を付与	書き込み	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
DeleteScheduledAction	スケジュールされたアクションを削除する許可を付与	書き込み	ScalableTarget*		
				application-autoscaling:service-namespace application-autosc	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aling:scalable-dimension	
DeregisterScalableTarget	スケーラブルなターゲットの登録を解除する許可を付与	書き込み	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
DescribeScalableTargets	指定した名前空間内の 1 つまたは複数のスケーラブルなターゲットの詳細を取得する許可を付与	読み取り			
DescribeScalingActivities	指定した名前空間内のスケーリングアクティビティのセットまたはすべての詳細を取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeScalingPolicies	指定した名前空間内のスケーリングポリシーのセットまたはすべての詳細を取得する許可を付与	読み取り			
DescribeScheduledActions	指定した名前空間内のスケジュールされたアクションのセットまたはすべての詳細を取得する許可を付与	読み取り			
GetPredictiveScalingForecast	予測スケーリングポリシーの予測データを取得する許可を付与	リスト			
ListTagsForResource	スケーラブルなターゲットのタグを一覧表示するための許可を付与します	読み取り	ScalableTarget*		
PutScalingPolicy	スケーラブルなターゲットのスケーリングポリシーを作成および更新する許可を付与	書き込み	ScalableTarget*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
PutScheduledAction	スケーラブルなターゲットのスケジュールされたアクションを作成および更新する許可を付与	書き込み	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RegisterScalableTarget	Application Auto Scaling でスケーラブルターゲットとして AWS またはカスタムリソースを登録し、スケーラブルターゲットの管理に使用される設定パラメータを更新する許可を付与	書き込み	ScalableTarget*		application-autoscaling:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
TagResource	スケーラブルなターゲットにタグ付けするための許可を付与します	Tagging	ScalableTarget*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	スケーラブルなターゲットからタグを削除するための許可を付与します	Tagging	ScalableTarget*		
				aws:TagKeys	

AWS Application Auto Scaling で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
ScalableTarget	arn:${Partition}:application-autoscaling:${Region}:${Account}:scalable-target/${ResourceId}	aws:ResourceTag/${TagKey}

AWS Application Auto Scaling の条件キー

AWS Application Auto Scaling では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
application-autoscaling:scalable-dimension	リクエストで渡されたスケーラブルなディメンションによるアクセスをフィルタリングします	String
application-autoscaling:service-namespace	リクエストで渡されたサービスの名前空間でアクセスをフィルタリングします	String
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Application Cost Profiler Service のアクション、リソース、および条件キー

AWS Application Cost Profiler Service (サービスプレフィックス: `application-cost-profiler`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Application Cost Profiler Service で定義されるアクション
- AWS Application Cost Profiler Service で定義されるリソースタイプ
- AWS Application Cost Profiler Service の条件キー

AWS Application Cost Profiler Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteReportDefinition	特定の Application Cost Profiler Report を使用して設定を削除するためのアクセス許可を付与し、レポート生成を効果的に無効にします	Write			
GetReportDefinition	特定の Application Cost Profiler Report リクエストを使用して構成を取得するためのアクセス許可を付与	Read			
ImportApplicationUsage	S3 からアプリケーションの使用状況をインポートするためのアクセス許可を付与	Write			
ListReportDefinitions	作成したさまざまな Application Cost Profiler Report 設定のリストを取得するためのアクセス許可を付与	Read			
PutReportDefinition	Application Cost Profiler Report 設定を作成するためのアクセス許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateReportDefinition	既存の Application Cost Profiler Report 設定を更新するためのアクセス許可を付与	Write			

AWS Application Cost Profiler Service で定義されるリソースタイプ

AWS Application Cost Profiler Service は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Application Cost Profiler Service へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Application Cost Profiler Service の条件キー

Application Cost Profiler には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Application Discovery Arsenal のアクション、リソース、および条件キー

Application Discovery Arsenal (サービスプレフィックス: `arsenal`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Application Discovery Arsenal で定義されるアクション
- Application Discovery Arsenal で定義されるリソースタイプ
- Application Discovery Arsenal の条件キー

Application Discovery Arsenal で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RegisterOnPremisesAgent [アクセス許可のみ]	AWS 提供されたデータコレクターを Application Discovery Service に登録するアクセス許可を付与します	書き込み			

Application Discovery Arsenal で定義されるリソースタイプ

Application Discovery Arsenal では、IAM ポリシーステートメントの `Resource` 要素でのリソース ARN の指定はサポートされていません。Application Discovery Arsenal へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

Application Discovery Arsenal の条件キー

Application Discovery Arsenal には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Application Discovery Service のアクション、リソース、および条件キー

AWS Application Discovery Service (サービスプレフィックス: `discovery`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Application Discovery Service で定義されるアクション

- AWS Application Discovery Service で定義されるリソースタイプ
- AWS Application Discovery Service の条件キー

AWS Application Discovery Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateConfigurationItemsToApplication	AssociateConfigurationItemsToApplication API に許可を付与します。AssociateConfigurationItemsToApplication は、1 つ以上の構成項目をアプリケーションに関連付けます	書き込み			
BatchDeleteAgents	BatchDeleteAgents API にアクセス許可を付与します。BatchDeleteAgents は、アカウントに関連付けられた 1 つ以上のエージェント/データコレクターを、それぞれエージェント ID で識別して削除します。データコレクターを削除しても、以前に収集されたデータは削除されません。	書き込み			
BatchDeleteImportData	BatchDeleteImportData API に許可を付与します。BatchDeleteImportData は、インポート ID で識別される 1 つ以上の Migration Hub インポートタスクを削除します。各インポートタスクには、サーバーまたはアプリケーションを識	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	別できるレコードが多数あります。				
CreateApplication	CreateApplication API に許可を付与します。CreateApplication は、指定された名前と説明でアプリケーションを作成します	書き込み			
CreateTags	CreateTags API に許可を付与します。CreateTags は、設定項目のタグを 1 つ以上作成します。タグは、IT アセットの分類に役立つメタデータです。この API は、複数の設定項目のリストを受け入れます。	Tagging			
DeleteApplications	DeleteApplications API に許可をを付与します。DeleteApplications は、アプリケーションのリストと設定項目の関連付けを削除します	書き込み			
DeleteTags	DeleteTags API に許可を付与します。DeleteTags は、設定項目と 1 つ以上のタグの関連付けを削除します。この API は、複数の設定項目のリストを受け入れます。	Tagging		aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeAgents	DescribeAgents API に許可を付与します。DescribeAgents は、エージェント、またはコネクタを ID ごとに一覧表示します。ID が指定されなかった場合は、ユーザーに関連付けられているエージェントまたはコネクタをすべて一覧表示します	読み取り			
DescribeBatchDeleteConfigurationTask	DescribeBatchDeleteConfigurationTask API にアクセス許可を付与します。DescribeBatchDeleteConfigurationTask は、一連の設定項目を削除するための一括削除タスクに関する属性を返します。指定するタスク ID は、StartBatchDeleteConfigurationTask の出力から受け取ったタスク ID でなければなりません。	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeConfigurations	DescribeConfigurations API に許可を付与します。DescribeConfigurations は、設定項目 ID のリストの属性を取得します。提供される ID はすべて、アセットタイプ (サーバー、アプリケーション、プロセス、または接続) が同じである必要があります。出力フィールドは、選択されたアセットタイプに固有です。たとえば、サーバー設定項目の出力には、ホスト名、オペレーティングシステム、ネットワークカード数など、サーバーに関する属性のリストが含まれています。	読み取り			
DescribeContinuousExports	DescribeContinuousExports API に許可を付与します。DescribeContinuousExports は、ID で指定されたエクスポートを一覧表示します。パラメータを渡さずに DescribeContinuousExports をそのまま呼び出すと、ユーザーに関連付けられている連続したエクスポートをすべて一覧表示できます。	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeExportConfigurations	DescribeExportConfigurations API に許可を付与します。DescribeExportConfigurations は、指定されたエクスポートプロセスのステータスを取得します。ステータスは、最大 100 のプロセスから取得できます。	読み取り			
DescribeExportTasks	DescribeExportTasks API に許可を付与します。DescribeExportTasks は、1 つ以上のエクスポートタスクのステータスを取得します。最大 100 個のエクスポートタスクのステータスを取得できます。	読み取り			
DescribeImportTasks	DescribeImportTasks API に許可を付与します。DescribeImportTasks は、ステータス情報、時間、ID、インポートファイルの Amazon S3 オブジェクト URL など、ユーザーのインポートタスクの配列を返します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeTags	DescribeTags API に許可を付与します。DescribeTags は、特定のタグでタグ付けされている設定項目のリストを取得します。または、特定の設定項目に割り当てられたすべてのタグのリストを取得します。	読み取り			
DisassociateConfigurationItemsFromApplication	DisassociateConfigurationItemsFromApplication API に許可を付与します。DisassociateConfigurationItemsFromApplication は、1 つ以上の構成項目をアプリケーションから関連付け解除します。	書き込み			
ExportConfigurations	ExportConfigurations API に許可を付与します。ExportConfigurations は、データを表示して評価できるように、検出されたすべての設定データを Amazon S3 バケットまたはアプリケーションにエクスポートします。データには、タグ、タグの関連付け、プロセス、接続、サーバー、システムパフォーマンスなどがあります。	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetDiscoverySummary	GetDiscoverySummary API に許可を付与します。GetDiscoverySummary は、検出されたアセットの概要を取得します。	読み取り			
GetNetworkConnectionGraph	GetNetworkConnectionGraph API に許可を付与します。GetNetworkConnectionGraph は、IP アドレス、サーバー ID、ノード ID のいずれかの入力リストを受け入れます。お客様がネットワーク接続グラフを視覚化するのに役立つノードとエッジのリストを返します。この API は、MigrationHub のコンソールでネットワークグラフ機能を可視化するために使用されます。	読み取り			
ListConfigurations	ListConfigurations API に許可を付与します。ListConfigurations は、フィルターで指定された条件に従って、設定項目のリストを取得します。このフィルター条件に基づいて関係の要件が特定されます。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListServerNeighbors	ListServerNeighbors API に許可を付与します。ListServerNeighbors は、指定されたサーバーから 1 ネットワークホップ離れたサーバーのリストを取得します。	リスト			
StartBatchDeleteConfigurationTask	StartBatchDeleteConfigurationTask API にアクセス許可を付与します。StartBatchDeleteConfigurationTask は、設定項目の非同期での一括削除を開始します。提供される ID はすべて、アセットタイプ (サーバー、アプリケーション、プロセス、または接続) が同じである必要があります。出力は固有のタスク ID で、これを使用して削除の進行状況を確認できます。	書き込み			
StartContinuousExport	StartContinuousExport API に許可を付与します。StartContinuousExport は、エージェントの検出データの Amazon Athena への連続フローを開始します	書き込み			iam:AttachRolePolicy iam:CreatePolicy iam:CreateRole iam:CreateServiceLinkedRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartDataCollectionByAgentIds	StartDataCollectionByAgentIds API に許可を付与します。StartDataCollectionByAgentIds は、データの収集を開始するように、指定されたエージェントまたはコネクタに指示します。	書き込み			
StartExportTask	StartExportTask API に許可を付与します。StartExportTask は、検出された設定項目および関係に関する設定データを、指定された形式の S3 バケットにエクスポートします。	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartImportTask	StartImportTask API に許可を付与します。StartImportTask はインポートタスクを開始します。Migration Hub のインポート機能を使用すると、Discovery Connector や Discovery Agent などの Application Discovery Service (ADS) ツールを使用 AWS せずに、オンプレミス環境の詳細を に直接インポートできます。これにより、インポートしたデータから直接、移行の評価と計画を実行することができます。たとえば、デバイスをアプリケーションとしてグループ化して移行ステータスを追跡することができます。	書き込み			discovery:AssociateConfigurationItemsToApplication discovery:CreateApplication discovery:CreateTags discovery:GetDiscoverySummary discovery:ListConfigurations s3:GetObject
StopContinuousExport	StopContinuousExport API に許可を付与します。StopContinuousExport は、エージェントの検出データの Amazon Athena への連続フローを停止します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StopDataCollectionByAgentIds	StopDataCollectionByAgentIds API に許可を付与します。StopDataCollectionByAgentIds は、データの収集を停止するように、指定されたエージェントまたはコネクタに指示します。	書き込み			
UpdateApplication	UpdateApplication API に許可を付与します。UpdateApplication は、アプリケーションに関するメタデータを更新します	書き込み			

AWS Application Discovery Service で定義されるリソースタイプ

AWS Application Discovery Service は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Application Discovery Service へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

> **Note**
>
> アクセスを分離するには、個別の AWS アカウントを作成して使用します。

AWS Application Discovery Service の条件キー

AWS Application Discovery Service では、IAM ポリシーの `Condition`要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Application Migration Service のアクション、リソース、および条件キー

AWS Application Migration Service (サービスプレフィックス: mgn) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Application Migration Service で定義されるアクション
- AWS Application Migration Service で定義されるリソースタイプ
- AWS Application Migration Service の条件キー

AWS Application Migration Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にア

クションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ArchiveApplication	アプリケーションをアーカイブする許可を付与	書き込み	ApplicationResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ArchiveWave	ウェーブをアーカイブするアクセス許可を付与	書き込み	WaveResource*		
AssociateApplications	ウェーブにアプリケーションを関連付ける許可を付与	書き込み	ApplicationResource*		
			WaveResource*		
AssociateSourceServers	アプリケーションにソースサーバーを関連付ける許可を付与	書き込み	ApplicationResource*		
			SourceServerResource*		
BatchCreateVolumeSnapshotGroupForMgn [アクセス許可のみ]	ボリュームスナップショットグループを作成する許可を付与	書き込み	SourceServerResource*		
BatchDeleteSnapshotRequestForMgn [アクセス許可のみ]	スナップショットのリクエストを一括で削除する許可を付与。	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ChangeServerLifeCycleState	ソースサーバーのライフサイクル状態を変更する許可を付与	書き込み	SourceServerResource*		
CreateApplication	アプリケーションを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnector	コネクタを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLaunchConfigurationTemplate	起動設定テンプレートを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNetworkMigrationDefinition	ネットワーク移行定義を作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateReplicationConfigurationTemplate	レプリケーション構成テンプレートを作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateVcenterClientForMgn [アクセス許可のみ]	v c enter クライアントを作成するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWave	ウェーブを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	アプリケーションを削除する許可を付与	書き込み	ApplicationResource*		
DeleteConnector	コネクタを削除する許可を付与	書き込み	ConnectorResource*		
DeleteJob	ジョブを削除する許可を付与	書き込み	JobResource*		
DeleteLaunchConfigurationTemplate	起動設定テンプレートを削除する許可を付与	書き込み	LaunchConfigurationTemplateResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteNetworkMigrationDefinition	ネットワーク移行定義を削除するアクセス許可を付与します	書き込み	NetworkMigrationDefinitionResource*		
DeleteReplicationConfigurationTemplate	レプリケーション構成テンプレートを削除する許可を付与	書き込み	ReplicationConfigurationTemplateResource*		
DeleteSourceServer	ソースサーバーを削除する許可を付与	書き込み	SourceServerResource*		
DeleteVcenterClient	vcenter クライアントを削除するアクセス許可を付与	書き込み	VcenterClientResource*		
DeleteWave	ウェーブを削除する許可を付与	書き込み	WaveResource*		
DescribeJobLogItems	ジョブログ項目を説明する許可を付与	読み込み	JobResource*		
DescribeJobs	ジョブを記述する許可を付与	リスト			
DescribeLaunchConfigurationTemplates	起動設定テンプレートを記述する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeReplicationConfigurationTemplates	レプリケーション構成テンプレートを記述する許可を付与	リスト			
DescribeReplicationServerAssociationsForMgn [許可のみ]	レプリケーションサーバーの関連付けを記述する許可を付与	読み込み			
DescribeSnapshotRequestsForMgn [許可のみ]	スナップショットのリクエストを記述する許可を付与	読み込み			
DescribeSourceServers	ソースサーバーを記述する許可を付与	リスト			
DescribeVcenterClients	vcenter クライアントを記述するアクセス許可を付与	リスト			
DisassociateApplications	ウェーブからアプリケーションの関連付けを解除する許可を付与	書き込み	ApplicationResource*		
			WaveResource*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DisassociateSourceServers	アプリケーションからソースサーバーの関連付けを解除する許可を付与	書き込み	ApplicationResource*		
			SourceServerResource*		
DisconnectFromService	サービスからソースサーバーの接続を切るアクセス許可を付与	書き込み	SourceServerResource*		
FinalizeCutover	カットオーバーを確定する許可を付与	書き込み	SourceServerResource*		
GetAgentCommandForMgn [アクセス許可のみ]	エージェントコマンドを取得する許可を付与	読み込み	SourceServerResource*		
GetAgentConfirmedResumeInfoForMgn [許可のみ]	エージェントに確認済みの再開情報を取得する許可を付与	読み込み	SourceServerResource*		
GetAgentInstallationAssetsForMgn [許可のみ]	エージェントのインストールアセットを取得する許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetAgentReplicationInfoForMgn [許可のみ]	エージェントレプリケーション情報を取得する許可を付与	読み込み	SourceServerResource*		
GetAgentRuntimeConfigurationForMgn [許可のみ]	エージェントのランタイム設定を取得する許可を付与	読み込み	SourceServerResource*		
GetAgentSnapshotCreditsForMgn [許可のみ]	エージェントスナップショットのクレジットを取得する許可を付与	読み込み	SourceServerResource*		
GetChannelCommandsForMgn [許可のみ]	チャネルコマンドを取得する許可を付与	読み込み			
GetLaunchConfiguration	起動設定を取得する許可を付与。	読み取り	SourceServerResource*		
GetNetworkMigrationDefinition	ネットワーク移行定義を取得する許可を付与	読み取り	NetworkMigrationDefinitionResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetNetworkMigrationMapperSegmentConstruct	ネットワーク移行マッパーセグメントコンストラクトを取得する許可を付与	読み取り	NetworkMigrationDefinitionResource*		
GetReplicationConfiguration	レプリケーション構成を取得する許可を付与	読み込み	SourceServerResource*		
GetVcenterClientCommandsForMgn [許可のみ]	vcenter クライアントコマンドを取得するアクセス許可を付与	読み込み	VcenterClientResource*		
InitializeService	サービスを初期化する許可を付与	書き込み			iam:AddRoleToInstanceProfile iam:CreateInstanceProfile iam:CreateServiceLinkedRole iam:GetInstanceProfile

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
IssueClientCertificateForMgn [アクセス許可のみ]	クライアント証明書を発行する許可を付与	書き込み	SourceServerResource		
ListApplications	アプリケーションの概要を一覧表示する許可を付与	リスト			
ListConnectors	コネクタを一覧表示する許可を付与	読み取り			
ListExportErrors	エクスポートタスクのエラーを一覧表示するための許可を付与します	リスト	ExportResource*		
ListExports	エクスポートタスクを一覧表示するための許可を付与します	リスト			
ListImportErrors	インポートタスクのエラーを一覧表示するための許可を付与します	リスト	ImportResource*		
ListImports	インポートタスクを一覧表示するための許可を付与します	リスト			
ListManagedAccounts	管理アカウントを一覧表示する許可を付与します	リスト			
ListNetworkMigrationAnalyses	ネットワーク移行分析を一覧表示する許可を付与	リスト	NetworkMigrationDefinitionResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListNetworkMigrationAnalysisResults	ネットワーク移行分析結果を一覧表示するアクセス許可を付与します	リスト	NetworkMigrationDefinitionResource*		
ListNetworkMigrationCodeGenerationSegments	ネットワーク移行コード生成セグメントを一覧表示する許可を付与	リスト	NetworkMigrationDefinitionResource*		
ListNetworkMigrationCodeGenerations	ネットワーク移行コード生成を一覧表示する許可を付与	リスト	NetworkMigrationDefinitionResource*		
ListNetworkMigrationDefinitions	ネットワーク移行定義を一覧表示する許可を付与	リスト			
ListNetworkMigrationDeployedStacks	ネットワーク移行でデプロイされたスタックを一覧表示するアクセス許可を付与します	リスト	NetworkMigrationDefinitionResource*		
ListNetworkMigrationDeployedStacksDeletions	ネットワーク移行でデプロイされたスタックの削除を一覧表示するアクセス許可を付与します	リスト	NetworkMigrationDefinitionResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListNetworkMigrationDeployments	ネットワーク移行デプロイを一覧表示するアクセス許可を付与します	リスト	NetworkMigrationDefinitionResource*		
ListNetworkMigrationExecutions	ネットワーク移行実行を一覧表示するアクセス許可を付与します	リスト	NetworkMigrationDefinitionResource*		
ListNetworkMigrationMapperSegmentConstructs	ネットワーク移行マッパーセグメントコンストラクトを一覧表示する許可を付与	リスト	NetworkMigrationDefinitionResource*		
ListNetworkMigrationMapperSegments	ネットワーク移行マッパーセグメントを一覧表示する許可を付与	リスト	NetworkMigrationDefinitionResource*		
ListNetworkMigrationMappings	ネットワーク移行マッピングを一覧表示する許可を付与	リスト	NetworkMigrationDefinitionResource*		
ListSourceServerActions	ソースサーバーアクションドキュメントを一覧表示する許可を付与	リスト	SourceServerResource*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTemplateActions	起動設定テンプレートアクションドキュメントを一覧表示する許可を付与	リスト	LaunchConfigurationTemplateResource*		
ListWaves	ウェーブの概要を一覧表示する許可を付与	リスト			
MarkAsArchived	ソースサーバをアーカイブ済みとしてマークする許可を付与	書き込み	SourceServerResource*		
NotifyAgentAuthenticationForMgn [アクセス許可のみ]	エージェント認証を通知する許可を付与	書き込み	SourceServerResource*		
NotifyAgentConnectedForMgn [アクセス許可のみ]	エージェントが接続されていることを通知する許可を付与	書き込み	SourceServerResource*		
NotifyAgentDisconnectedForMgn [アクセス許可のみ]	エージェントの切断を通知する許可を付与	書き込み	SourceServerResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
NotifyAgentReplicationProgressForMgn [アクセス許可のみ]	エージェントのレプリケーションの進行状況を通知する許可を付与	書き込み	SourceServerResource*		
NotifyVcenterClientStartedForMgn [アクセス許可のみ]	vcenter クライアントが開始されたことを通知するアクセス許可を付与	書き込み	VcenterClientResource*		
PauseReplication	レプリケーションを一時停止する許可を付与します	書き込み	SourceServerResource*		
PutSourceServerAction	ソースサーバーアクションドキュメントを配置する許可を付与	書き込み	SourceServerResource*		
PutTemplateAction	起動設定テンプレートアクションドキュメントを配置する許可を付与	書き込み	LaunchConfigurationTemplateResource*		
RegisterAgentForMgn [アクセス許可のみ]	エージェントを登録する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RemoveSourceServerAction	ソースサーバーアクションドキュメントを削除する許可を付与	書き込み	SourceServerResource*		
RemoveTemplateAction	起動設定テンプレートアクションドキュメントを削除する許可を付与	書き込み	LaunchConfigurationTemplateResource*		
ResumeReplication	レプリケーションを再開する許可を付与します	書き込み	SourceServerResource*		
RetryDataReplication	レプリケーションを再試行する許可を付与	書き込み	SourceServerResource*		
SendAgentLogsForMgn [アクセス許可のみ]	エージェントログを送信する許可を付与。	書き込み	SourceServerResource*		
SendAgentMetricsForMgn [アクセス許可のみ]	エージェントメトリックを送信する許可を付与	書き込み	SourceServerResource*		
SendChannelCommandResultForMgn [アクセス許可のみ]	チャネルコマンドの結果を送信する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SendClientLogsForMgn [アクセス許可のみ]	クライアントログを送信する許可を付与	書き込み			
SendClientMetricsForMgn [アクセス許可のみ]	クライアントメトリックを送信する許可を付与	書き込み			
SendVcenterClientCommandResultForMgn [アクセス許可のみ]	vcenterクライアントコマンドの結果を送信する許可を付与	書き込み	VcenterClientResource*		
SendVcenterClientLogsForMgn [アクセス許可のみ]	vcenterクライアントログを送信する許可を付与	書き込み	VcenterClientResource*		
SendVcenterClientMetricsForMgn [アクセス許可のみ]	vcenterクライアントメトリックを送信する許可を付与	書き込み	VcenterClientResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartCutover	カットオーバーを開始する許可を付与	書き込み	SourceServerResource*		ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateSecurityGroup ec2:CreateSnapshot ec2:CreateTags ec2:CreateVolume

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DeleteLaunchTemplateVersions ec2:DeleteSnapshot ec2:DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstanceAttribute ec2:DescribeInstanceStatus

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets ec2:DescribeVolumes ec2:DetachVolume

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:ReportInstanceStatus ec2:RevokeSecurityGroupEgress ec2:RunInstances ec2:StartInstances ec2:StopInstances ec2:TerminateInstances iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					mgn:ListTagsForResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StartExport	エクスポートタスクを開始するための許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeLaunchTemplateVersions mgn:DescribeSourceServers mgn:GetLaunchConfiguration mgn:ListApplications mgn:ListWaves s3:PutObject

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartImport	インポートタスクを作成するための許可を付与します	書き込み			ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplateVersions ec2:ModifyLaunchTemplate mgn:DescribeSourceServers mgn:GetLaunchConfiguration mgn:ListApplications mgn:ListWaves mgn:TagResource mgn:UpdateLaunchCo

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					nfiguration s3:PutObject

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartNetworkMigrationAnalysis	ネットワーク移行分析を開始するアクセス許可を付与します	書き込み	NetworkMigrationDefinitionResource*		directconnect:DescribeConnections directconnect:DescribeDirectConnectGatewayAssociations directconnect:DescribeDirectConnectGatewayAttachments directconnect:DescribeDirectConnectGateways directconnect:DescribeVirtualGateways directconnect:DescribeVirtu

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					allInterfaces ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInsightsPath ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DeleteNetworkInsightsAnalysis ec2:DeleteNetworkInsightsPath

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup ec2:DeleteTags ec2:DescribeAvailabilityZones ec2:DescribeCustomerGateways ec2:DescribeInstances ec2:DescribeInternetGateways ec2:DescribeManagedPrefixLists

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeNetworkInsightsAnalyses ec2:DescribeNetworkInsightsPaths ec2:DescribeNetworkInterfaces ec2:DescribePrefixLists ec2:DescribeRegions ec2:DescribeRouteTables

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeTransitGatewayAttachments ec2:DescribeTransitGatewayConnects ec2:DescribeTransitGatewayPeeringAttachments ec2:DescribeTransitGatewayRouteTables ec2:DescribeTransitGatewayV

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					pcAttachments ec2:DescribeTransitGateways ec2:DescribeVpcEndpointServiceConfigurations ec2:DescribeVpcEndpoints ec2:DescribeVpcPeeringConnections ec2:DescribeVpcs ec2:DescribeVpnConnections ec2:DescribeVpnGateways ec2:GetManagedPref

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ixListEntries ec2:GetTransitGatewayRouteTablePropagations ec2:SearchTransitGatewayRoutes ec2:StartNetworkInsightsAnalysis elasticloadbalancing:DescribeListeners elasticloadbalancing:DescribeLoadBalancerAttributes elasticloadbalancing:Descri

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					beLoadBalancers elasticloadbalancing:DescribeRules elasticloadbalancing:DescribeTags elasticloadbalancing:DescribeTargetGroupAttributes elasticloadbalancing:DescribeTargetGroups elasticloadbalancing:DescribeTargetHealth globalaccelerator:

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ListAccelerators globalaccelerator:ListCustomRoutingAccelerators globalaccelerator:ListCustomRoutingEndpointGroups globalaccelerator:ListCustomRoutingListeners globalaccelerator:ListCustomRoutingPortMappings globalaccelerator:ListEndpointGroups

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					globalaccelerator:ListListeners network-firewall:DescribeFirewall network-firewall:DescribeFirewallPolicy network-firewall:DescribeResourcePolicy network-firewall:DescribeRuleGroup network-firewall:ListFirewallPolicies network-firewall:L

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					istFirewalls network-firewall:ListRuleGroups tiros:CreateQuery tiros:ExtendQuery tiros:GetQueryAnswer tiros:GetQueryExplanation tiros:GetQueryExtensionAccounts
StartNetworkMigrationCodeGeneration	ネットワーク移行コード生成を開始する許可を付与	書き込み	NetworkMigrationDefinitionResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartNetworkMigrationDeployedStacksDeletion	ネットワーク移行デプロイされたスタックの削除を開始するアクセス許可を付与します	書き込み	NetworkMigrationDefinitionResource*		ec2:AcceptTransitGatewayVpcAttachment ec2:AssociateNatGatewayAddress ec2:AssociateRouteTable ec2:AssociateSubnetCidrBlock ec2:AssociateTransitGatewayRouteTable ec2:AssociateVpcCidrBlock ec2:AttachInternetGateway

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:DeleteInternetGateway ec2:DeleteLaunchTemplate ec2:DeleteLaunchTemplateVersions ec2:DeleteNatGateway ec2:DeleteNetworkAcl

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DeleteNetworkAclEntry ec2:DeleteNetworkInsightsAnalysis ec2:DeleteNetworkInsightsPath ec2:DeleteNetworkInterface ec2:DeleteRoute ec2:DeleteRouteTable ec2:DeleteSecurityGroup ec2:DeleteSnapshot ec2:DeleteSubnet

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DeleteTransitGateway ec2:DeleteTransitGatewayRoute ec2:DeleteTransitGatewayRouteTable ec2:DeleteTransitGatewayVpcAttachment ec2:DeleteVolume ec2:DeleteVpc ec2:DetachInternetGateway ec2:DetachVolume ec2:DisableTransit

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					GatewayRouteTablePropagation ec2:DisassociateNatGatewayAddress ec2:DisassociateRouteTable ec2:DisassociateTransitGatewayRouteTable ec2:EnableTransitGatewayRouteTablePropagation ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:ModifySubnetAttribute ec2:ModifyTransitGateway ec2:ModifyTransitGatewayVpcAttachment ec2:ModifyVolume ec2:ModifyVpcAttribute ec2:RejectTransitGatewayVpcAttachment ec2:ReleaseAddress ec2:ReplaceNetworkAclAssociation

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:ReplaceNetworkAclEntry ec2:ReplaceRoute ec2:ReplaceTransitGatewayRoute ec2:RevokeSecurityGroupEgress ec2:RevokeSecurityGroupIngress ec2:SearchTransitGatewayRoutes

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartNetworkMigrationDeployment	ネットワーク移行のデプロイを開始するアクセス許可を付与します	書き込み	NetworkMigrationDefinitionResource*		ec2:AcceptTransitGatewayVpcAttachment ec2:AssociateNatGatewayAddress ec2:AssociateRouteTable ec2:AssociateSubnetCidrBlock ec2:AssociateTransitGatewayRouteTable ec2:AssociateVpcCidrBlock ec2:AttachInternetGateway

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNatGateway ec2:CreateNetworkAcl ec2:CreateNetworkAclEntry ec2:CreateNetworkInsightsPath ec2:CreateNetworkInterface

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:CreateRoute ec2:CreateRouteTable ec2:CreateSecurityGroup ec2:CreateSubnet ec2:CreateTags ec2:CreateTransitGatewayRoute ec2:CreateTransitGatewayRouteTable ec2:CreateTransitGatewayVpcAttachment

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DeleteInternetGateway ec2:DeleteLaunchTemplate ec2:DeleteLaunchTemplateVersions ec2:DeleteNatGateway ec2:DeleteNetworkAcl ec2:DeleteNetworkAclEntry ec2:DeleteNetworkInsightsAnalysis ec2:DeleteNetworkInsightsPath

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DeleteNetworkInterface ec2:DeleteRoute ec2:DeleteRouteTable ec2:DeleteSecurityGroup ec2:DeleteSnapshot ec2:DeleteSubnet ec2:DeleteTransitGateway ec2:DeleteTransitGatewayRoute ec2:DeleteTransitGatewayRouteTable

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DeleteTransitGatewayVpcAttachment ec2:DeleteVolume ec2:DeleteVpc ec2:DescribeAccountAttributes ec2:DescribeAddresses ec2:DescribeAvailabilityZones ec2:DescribeCustomerGateways ec2:DescribeEgressOnlyInter

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					netGateways ec2:DescribeHosts ec2:DescribeImages ec2:DescribeInstanceAttribute ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeInternetGateways ec2:DescribeLaunchTemplateVersions

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DescribeLaunchTemplates ec2:DescribeManagedPrefixLists ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeNetworkInsightsAnalyses ec2:DescribeNetworkInsightsPaths ec2:DescribeNetworkInterfaces ec2:DescribePrefixLists

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DescribeRegions ec2:DescribeRouteTables ec2:DescribeSecurityGroupRules ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets ec2:DescribeTransitGatewayAttachments ec2:DescribeTransitGatewayConnects

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DescribeTransitGatewayPeeringAttachments ec2:DescribeTransitGatewayRouteTables ec2:DescribeTransitGatewayVpcAttachments ec2:DescribeTransitGateways ec2:DescribeVolumes ec2:DescribeVpcEndpointServiceConfigurations ec2:DescribeVpcEndpoints

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DescribeVpcPeeringConnections ec2:DescribeVpcs ec2:DescribeVpnConnections ec2:DescribeVpnGateways ec2:DetachInternetGateway ec2:DetachVolume ec2:DisableTransitGatewayRouteTablePropagation ec2:DisassociateNatGatewayAddress

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DisassociateRouteTable ec2:DisassociateTransitGatewayRouteTable ec2:EnableTransitGatewayRouteTablePropagation ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault ec2:GetManagedPrefixListEntries ec2:GetTransitGatewayRouteTableAssociations

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:GetTransitGatewayRouteTablePropagations ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:ModifySubnetAttribute ec2:ModifyTransitGateway ec2:ModifyTransitGatewayVpcAttachment ec2:ModifyVolume ec2:ModifyVpcAttribute

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:RejectTransitGatewayVpcAttachment ec2:ReleaseAddress ec2:ReplaceNetworkAclAssociation ec2:ReplaceNetworkAclEntry ec2:ReplaceRoute ec2:ReplaceTransitGatewayRoute ec2:RevokeSecurityGroupEgress ec2:RevokeSecurityGroupIngress

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					ec2:SearchTransitGatewayRoutes ec2:StartNetworkInsightsAnalysis
StartNetworkMigrationMapping	ネットワーク移行マッピングを開始するアクセス許可を付与します	書き込み	NetworkMigrationDefinitionResource*		
StartReplication	レプリケーションを開始する許可を付与	書き込み	SourceServerResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartTest	テストを開始する許可を付与	書き込み	SourceServerResource*		ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateSecurityGroup ec2:CreateSnapshot ec2:CreateTags ec2:CreateVolume

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DeleteLaunchTemplateVersions ec2:DeleteSnapshot ec2:DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstanceAttribute ec2:DescribeInstanceStatus

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets ec2:DescribeVolumes ec2:DetachVolume

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:ReportInstanceStatus ec2:RevokeSecurityGroupEgress ec2:RunInstances ec2:StartInstances ec2:StopInstances ec2:TerminateInstances iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					mgn:ListTagsForResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StopReplication	レプリケーションを停止する許可を付与	書き込み	SourceServerResource*		
TagResource	リソースタグを割り当てるアクセス許可を付与	タグ付け	ApplicationResource		
			ConnectorResource		
			ExportResource		
			ImportResource		
			JobResource		
			LaunchConfigurationTemplateResource		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			ReplicationConfigurationTemplateResource		
			SourceServerResource		
			VcenterClientResource		
			WaveResource		
				aws:RequestTag/${TagKey} mgn:CreateAction aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TerminateTargetInstances	ターゲットインスタンスを終了する許可を付与	書き込み	SourceServerResource*		ec2:DeleteVolume ec2:DescribeInstances ec2:DescribeVolumes ec2:TerminateInstances
				aws:RequestTag/${TagKey} aws:TagKeys	
UnarchiveApplication	アプリケーションのアーカイブを解除する許可を付与	書き込み	ApplicationResource*		
UnarchiveWave	ウェーブのアーカイブを解除する許可を付与	書き込み	WaveResource*		
UntagResource	リソースのタグを解除する許可を付与	タグ付け	ApplicationResource		
			ConnectorResource		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			JobResource		
			LaunchConfigurationTemplateResource		
			ReplicationConfigurationTemplateResource		
			SourceServerResource		
			VcenterClientResource		
			WaveResource		
				aws:TagKeys	
UpdateAgentBacklogForMgn [アクセス許可のみ]	エージェントのバックログを更新する許可を付与	書き込み	SourceServerResource*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateAgentConversionInfoForMgn [アクセス許可のみ]	エージェント変換情報を更新する許可を付与	書き込み	SourceServerResource*		
UpdateAgentReplicationInfoForMgn [アクセス許可のみ]	エージェントレプリケーション情報を更新する許可を付与	書き込み	SourceServerResource*		
UpdateAgentReplicationProcessStateForMgn [アクセス許可のみ]	エージェントレプリケーションプロセスの状態を更新する許可を付与	書き込み	SourceServerResource*		
UpdateAgentSourcePropertiesForMgn [アクセス許可のみ]	エージェントのソースプロパティを更新する許可を付与。	書き込み	SourceServerResource*		
UpdateApplication	アプリケーションを更新する許可を付与	書き込み	ApplicationResource*		
UpdateConnector	コネクタを更新する許可を付与	書き込み	ConnectorResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateLaunchConfiguration	起動設定を更新する許可を付与	書き込み	SourceServerResource*		
UpdateLaunchConfigurationTemplate	起動設定を更新する許可を付与	書き込み	LaunchConfigurationTemplateResource*		
UpdateNetworkMigrationDefinition	ネットワーク移行定義を更新する許可を付与	書き込み	NetworkMigrationDefinitionResource*		
UpdateNetworkMigrationMapperSegment	ネットワーク移行マッパーセグメントを更新する許可を付与	書き込み	NetworkMigrationDefinitionResource*		
UpdateNetworkMigrationMapperSegmentConstruct	ネットワーク移行マッパーセグメント構造を更新する許可を付与	書き込み	NetworkMigrationDefinitionResource*		
UpdateReplicationConfiguration	レプリケーション構成を更新する許可を付与。	書き込み	SourceServerResource*		
UpdateReplicationConfigurationTemplate	レプリケーション構成テンプレートを更新する許可を付与	書き込み	ReplicationConfigurationTemplateResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateSourceServer	ソースサーバーを更新する許可を付与	書き込み	SourceServerResource*		
UpdateSourceServerReplicationType	ソースサーバーレプリケーションタイプを更新するためのアクセス許可を付与	書き込み	SourceServerResource*		
UpdateWave	ウェーブを更新する許可を付与	書き込み	WaveResource*		
VerifyClientRoleForMgn [アクセス許可のみ]	クライアントロールを確認する許可を付与	読み取り			

AWS Application Migration Service で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
JobResource	arn:${Partition}:mgn:${Region}:${Account}:job/${JobID}	aws:ResourceTag/${TagKey}
ReplicationConfigu	arn:${Partition}:mgn:${Region}:${Account}:replication-configuration-temp	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
rationTemplateResource	late/${ReplicationConfigurationTemplateID}	
LaunchConfigurationTemplateResource	arn:${Partition}:mgn:${Region}:${Account}:launch-configuration-template/${LaunchConfigurationTemplateID}	aws:ResourceTag/${TagKey}
VcenterClientResource	arn:${Partition}:mgn:${Region}:${Account}:vcenter-client/${VcenterClientID}	aws:ResourceTag/${TagKey}
SourceServerResource	arn:${Partition}:mgn:${Region}:${Account}:source-server/${SourceServerID}	aws:ResourceTag/${TagKey}
ApplicationResource	arn:${Partition}:mgn:${Region}:${Account}:application/${ApplicationID}	aws:ResourceTag/${TagKey}
WaveResource	arn:${Partition}:mgn:${Region}:${Account}:wave/${WaveID}	aws:ResourceTag/${TagKey}
ImportResource	arn:${Partition}:mgn:${Region}:${Account}:import/${ImportID}	aws:ResourceTag/${TagKey}
ExportResource	arn:${Partition}:mgn:${Region}:${Account}:export/${ExportID}	aws:ResourceTag/${TagKey}
ConnectorResource	arn:${Partition}:mgn:${Region}:${Account}:connector/${ConnectorID}	aws:ResourceTag/${TagKey}
NetworkMigrationDefinitionResource	arn:${Partition}:mgn:${Region}:${Account}:network-migration-definition/${NetworkMigrationDefinitionID}	aws:ResourceTag/${TagKey}

AWS Application Migration Service の条件キー

AWS Application Migration Service では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーおよび値のペアのプレゼンスによってアクションをフィルタリング	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーのプレゼンスによってアクセスをフィルタリング	ArrayOfString
mgn:CreateAction	リソース作成 API アクションの名前によってアクセスをフィルタリングします	String

Amazon Application Recovery Controller のアクション、リソース、および条件キー - ゾーンシフト

Amazon Application Recovery Controller - ゾーンシフト (サービスプレフィックス: arc-zonal-shift) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Application Recovery Controller で定義されるアクション - ゾーンシフト
- Amazon Application Recovery Controller で定義されるリソースタイプ - ゾーンシフト
- Amazon Application Recovery Controller の条件キー - ゾーンシフト

Amazon Application Recovery Controller で定義されるアクション - ゾーンシフト

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelPracticeRun	アクティブな練習実行をキャンセルするアクセス許可を付与します	書き込み	ALB*		
			NLB*		
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CancelZonalShift	アクティブなゾーンシフトをキャンセルする許可を付与	書き込み	ALB*		
			NLB*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreatePracticeRunConfiguration	プラクティス実行設定を作成するためのアクセス許可を付与	書き込み	ALB*		cloudwatch:DescribeAlarms iam:CreateServiceLinkedRole
			NLB*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeletePracticeRunConfiguration	プラクティス実行設定を削除するためのアクセス許可を付与	書き込み	ALB* NLB*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetAutoshiftObserverNotificationStatus	Autoshift オブザーバー通知ステータスを取得する許可を付与する	読み取り			
GetManagedResource	マネージドリソースに関する情報を取得する許可を付与	読み取り	ALB* NLB*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ListAutoshifts	アクティブな自動シフトと完了した自動シフトを一覧表示するためのアクセス許可を付与	リスト			
ListManagedResources	マネージドリソースを一覧表示する許可を付与	リスト			
ListZonalShifts	ゾーンシフトを一覧表示する許可を付与	リスト			
StartPracticeRun	練習実行を開始するアクセス許可を付与します	書き込み	ALB* NLB*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
StartZonalShift	ゾーンシフトを開始する許可を付与	書き込み	ALB*		
			NLB*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateAutoshiftObserverNotificationStatus	Autoshift オブザーバー通知ステータスを更新する許可を付与する	書き込み			
UpdatePracticeRunConfiguration	プラクティス実行設定を更新するためのアクセス許可を付与	書き込み	ALB*		cloudwatch:DescribeAlarms iam:CreateServiceLinkedRole
			NLB*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateZonalAutoshiftConfiguration	ゾーン自動シフトのステータスを更新するためのアクセス許可を付与	書き込み	ALB*		iam:CreateServiceLinkedRole
			NLB*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateZonalShift	既存のゾーンシフトを更新する許可を付与	書き込み	ALB*		
			NLB*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Amazon Application Recovery Controller で定義されるリソースタイプ - ゾーンシフト

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
ALB	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}	arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
		elasticloadbalancing:ResourceTag/${TagKey}
NLB	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/net/${LoadBalancerName}/${LoadBalancerId}	arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Amazon Application Recovery Controller の条件キー - ゾーンシフト

Amazon Application Recovery Controller - ゾーンシフトでは、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
arc-zonal-shift:ResourceIdentifier	マネージドリソースのリソース識別子でアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	マネージドリソースに関連付けられたタグでアクセスをフィルタリングします	String
elasticloadbalanci	マネージドリソースに関連付けられたタグでアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
ng:ResourceTag/${TagKey}		

AWS アプリケーション変換サービスのアクション、リソース、条件キー

AWS Application Transformation Service (サービスプレフィックス: `application-transformation`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS アプリケーション変換サービスによって定義されるアクション
- AWS アプリケーション変換サービスで定義されるリソースタイプ
- AWS アプリケーション変換サービスの条件キー

AWS アプリケーション変換サービスによって定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetContainerization	すべてのコンテナ化ジョブの詳細を取得する許可を付与	読み取り			
GetDeployment	すべてのデプロイジョブの詳細を取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetGroupingAssessment	グループ化評価オペレーションの詳細を取得するアクセス許可を付与します	読み取り			
GetPortingCompatibilityAssessment	移植互換性オペレーションを取得するアクセス許可を付与します	読み取り			
GetPortingRecommendationAssessment	移植推奨評価オペレーションの詳細を取得するアクセス許可を付与します	読み取り			
GetRuntimeAssessment	ランタイム評価オペレーションの詳細を取得するアクセス許可を付与します	読み取り			
PutLogData	ログをプッシュするアクセス許可を付与します (クライアントのみ)	書き込み			
PutMetricData	メトリクスデータをプッシュするアクセス許可を付与します (クライアントのみ)	書き込み			
StartContainerization	コンテナ化ジョブを開始する許可を付与	書き込み			
StartDeployment	デプロイジョブを開始するためのアクセス許可を付与	書き込み			
StartGroupingAssessment	グループ化評価オペレーションを開始するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartPortingCompatibilityAssessment	移植互換性オペレーションを開始するアクセス許可を付与します	書き込み			
StartPortingRecommendationAssessment	移植推奨評価オペレーションを開始するアクセス許可を付与します	書き込み			
StartRuntimeAssessment	ランタイム評価オペレーションを開始するアクセス許可を付与します	書き込み			

AWS アプリケーション変換サービスで定義されるリソースタイプ

AWS Application Transformation Service は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS アプリケーション変換サービスへのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS アプリケーション変換サービスの条件キー

アプリケーション変換サービスには、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon AppStream 2.0 のアクション、リソース、および条件キー

Amazon AppStream 2.0 (サービスプレフィックス: `appstream`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon AppStream 2.0 で定義されるアクション
- Amazon AppStream 2.0 で定義されるリソースタイプ
- Amazon AppStream 2.0 の条件キー

Amazon AppStream 2.0 で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateAppBlockBuilderAppBlock	指定された App Block ビルダー を App Block に関連付けるアクセス許可を付与します	書き込み	app-block*		
			app-block-builder*		
				aws:ResourceTag/${TagKey}	
AssociateApplicationFleet	指定しアプリケーションをフリートに関連付けるアクセス許可を付与します。	書き込み	application*		
			fleet*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateApplicationToEntitlement	指定したアプリケーションを指定した使用権限管理に関連付ける許可を付与	書き込み	stack*		
AssociateFleet	指定したフリートを指定したスタックに関連付けるアクセス許可を付与します。	Write	fleet*		
			stack*		
				aws:ResourceTag/${TagKey}	
BatchAssociateUserStack	指定したユーザーを指定したスタックに関連付けるアクセス許可を付与します。ユーザープール内のユーザーは、Active Directory ドメインに参加しているフリートを持つスタックに割り当てることはできません。	Write	stack*		
				aws:ResourceTag/${TagKey}	
BatchDisassociateUserStack	指定したスタックから指定したユーザーの関連付けを解除する許可を付与。	書き込み	stack*		
				aws:ResourceTag/${TagKey}	
CopyImage	同じリージョン内の指定されたイメージ、または同じリージョン内の新しいリージョンにコピーするアクセス許可を付与します AWS アカウント	書き込み	image*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateAppBlock	App Block を作成する権限を付与します。アプリケーションブロック は、S3 バケット内のアプリケーションのファイルを含む仮想ハードディスクに関する詳細を格納します。また、仮想ハードディスクのマウント方法に関する詳細を含むセットアップスクリプトも格納されます。アプリケーションブロックは Elastic フリートでのみサポートされます。	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateAppBlockBuilder	App Block ビルダーを作成するアクセス許可を付与します。App Block ビルダーは、App Block の作成に使用される仮想マシンです	書き込み	app-block-builder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAppBlockBuilderStreamingURL	App Block ビルダーストリーミングセッションを開始するための URL を作成するアクセス許可を付与します	書き込み	app-block-builder*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateApplication	カスタマーアカウント内でアプリケーションを作成するアクセス許可を付与します。アプリケーションには、ストリーミングインスタンスでアプリケーションを起動する方法の詳細が保存されます。これは Elastic フリートでのみサポートされています。	書き込み	app-block*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateDirectoryConfig	AppStream 2.0 で Directory Config オブジェクトを作成する許可を付与。このオブジェクトには、フリートおよび Image Builder を Microsoft Active Directory ドメインに参加させるために必要な設定情報が含まれます。	書き込み			
CreateEntitlement	ユーザー属性に基づいてアプリケーションへのアクセスを制御する使用権限管理を作成する許可を付与	書き込み	stack*		
CreateFleet	フリートを作成する許可を付与。フリートはストリーミングインスタンスのグループで、ここからアプリケーションが実行され、ユーザーにストリーミングされます。	Write	fleet*		
			image		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateImageBuilder	Image Builder を作成する許可を付与。Image Builder は、イメージの作成に使用される仮想マシンです。	Write	image* image-builder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateImageBuilderStreamingURL	イメージビルダーストリーミングセッションを開始するための URL を作成する許可を付与。	Write	image-builder*		
				aws:ResourceTag/${TagKey}	
CreateStack	ユーザーに対してストリーミングアプリケーションを開始するためのスタックを作成する許可を付与。スタックは、関連付けられたフリート、ユーザーアクセスポリシー、ストレージ設定で構成されます。	Write	stack*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateStreamingURL	指定したユーザーに対して AppStream 2.0 ストリーミングセッションを開始するための一時的な URL を作成する許可を付与。ストリーミング URL により、ユーザーのセットアップなしでアプリケーションのストリーミングをテストすることができます。	書き込み	fleet*		
			stack*		
				aws:ResourceTag/${TagKey}	
CreateThemeForStack	ユーザーに表示するカスタムロゴ、ウェブサイトリンク、その他のブランドを含むカスタムブランドテーマを作成する許可を付与する	書き込み	stack*		
CreateUpdatedImage	カスタマーアカウント内の既存のイメージを更新する許可を付与	書き込み	image*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateUsageReportSubscription	使用状況レポートのサブスクリプションを作成する許可を付与。使用状況レポートは毎日生成されます。	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateUser	ユーザープールに新しいユーザーを作成する許可を付与。	書き込み			
DeleteAppBlock	指定された App Block を削除する許可を付与します。	書き込み	app-block*		
				aws:ResourceTag/${TagKey}	
DeleteAppBlockBuilder	指定された App Block ビルダーとリリース容量を削除するアクセス許可を付与します	書き込み	app-block-builder*		
				aws:ResourceTag/${TagKey}	
DeleteApplication	指定されたアプリケーションを削除する許可を付与	書き込み	application*		
				aws:ResourceTag/${TagKey}	
DeleteDirectoryConfig	指定した Directory Config オブジェクトを AppStream 2.0 から削除する許可を付与。このオブジェクトには、フリートおよび Image Builder を Microsoft Active Directory ドメインに参加させるために必要な設定情報が含まれます。	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteEntitlement	指定した使用権限管理を削除する許可を付与	書き込み	stack*		
DeleteFleet	指定したフリートを削除する許可を付与。	Write	fleet*		
				aws:ResourceTag/${TagKey}	
DeleteImage	指定したイメージを削除する許可を付与。イメージは、使用中の場合は削除できません。	Write	image*		
				aws:ResourceTag/${TagKey}	
DeleteImageBuilder	指定した Image Builder を削除して容量を解放するアクセス権限を付与します。	Write	image-builder*		
				aws:ResourceTag/${TagKey}	
DeleteImagePermissions	指定したプライベートイメージのアクセス許可を削除する許可を付与。	Write	image*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteStack	指定したスタックを削除する許可を付与。スタックの削除後、ユーザーは、スタックによって提供されたアプリケーションストリーミング環境を利用できなくなります。また、スタックのアプリケーションストリーミングセッションに行われたすべての予約も解放されます。	書き込み	stack*		
				aws:ResourceTag/${TagKey}	
DeleteThemeForStack	ユーザーに表示するカスタムロゴ、ウェブサイトリンク、その他のブランドを含むカスタムブランドテーマを削除する許可を付与する	書き込み	stack*		
DeleteUsageReportSubscription	使用状況レポートの生成を無効にする許可を付与。	Write			
DeleteUser	ユーザープールからユーザーを削除する許可を付与。	書き込み			
DescribeAppBlockBuilderAppBlockAssociations	指定された App Block ビルダーもしくは App Block に関連付けられている関連付けを取得するアクセス許可を付与します	リスト	app-block		
			app-block-builder		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeAppBlockBuilders	App Block ビルダー名が設定されている場合、1 つ以上の指定された App Block ビルダーを記述するリストを取得するアクセス許可を付与します。それ以外の場合は、アカウントのすべての App Block ビルダーが記述されます	リスト			
DescribeAppBlocks	App Block が設定されている場合、1 つ以上の指定した App Block を記述するリストを取得する許可を付与します。それ以外の場合は、アカウントのすべてのアプリケーションブロックが記述されます。	リスト			
DescribeApplicationFleetAssociations	指定されたアプリケーションもしくはフリートに関連付けられている関連付けを取得するアクセス許可を付与します。	リスト	application		
			fleet		
DescribeApplications	アプリケーション ARN が設定されている場合、1 つ以上の指定したイメージを記述するリストを取得する許可を付与します。それ以外の場合は、アカウントのすべてのAccountingが記述されます。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeDirectoryConfigs	AppStream 2.0 の 1 つ以上の指定した Directory Config オブジェクトの名前が設定されている場合、それらのオブジェクトを記述するリストを取得する許可を付与。それ以外の場合は、アカウントのすべての Directory Config オブジェクトが記述されます。このオブジェクトには、フリートおよび Image Builder を Microsoft Active Directory ドメインに参加させるために必要な設定情報が含まれます。	リスト			
DescribeEntitlements	指定したスタックの 1 つまたはすべての使用権限管理を取得する許可を付与	リスト	stack*		
DescribeFleets	フリート名が設定されている場合、1 つ以上の指定したフリートを記述するリストを取得する許可を付与。それ以外の場合は、アカウントのすべてのフリートが記述されます。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeImageBuilders	イメージビルダー名が設定されている場合、1 つ以上の指定したイメージビルダーを記述するリストを取得する許可を付与。それ以外の場合は、アカウントのすべてのイメージビルダーが記述されます。	リスト			
DescribeImagePermissions	所有するプライベートイメージ上の AWS アカウント IDsのアクセス許可を記述するリストを取得するアクセス許可を付与します	読み取り	image*		
DescribeImages	イメージ名またはイメージ ARN が設定されている場合、1 つ以上の指定したイメージを記述するリストを取得する許可を付与。それ以外の場合は、アカウントのすべてのイメージが記述されます。	リスト			
DescribeSessions	指定したスタックおよびフリートのストリーミングセッションを記述するリストを取得する許可を付与。スタックとフリートに対してユーザー ID が設定されている場合は、そのユーザーのストリーミングセッションのみが記述されます。	リスト	fleet* stack*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeStacks	スタック名が設定されている場合、1 つ以上の指定したスタックを記述するリストを取得する許可を付与。それ以外の場合は、アカウントのすべてのスタックが記述されます。	リスト			
DescribeThemeForStack	ユーザーに表示するカスタムロゴ、ウェブサイトリンク、その他のブランドなど、カスタムブランドテーマ情報を取得する許可を付与する	読み取り	stack*		
DescribeUsageReportSubscriptions	1 つ以上の使用状況レポートのサブスクリプションを記述するリストを取得する許可を付与。	リスト			
DescribeUserStackAssociations	UserStackAssociation オブジェクトを記述するリストを取得する許可を付与。	リスト	stack		
DescribeUsers	ユーザープール内のユーザーを記述するリストを取得する許可を付与。	リスト			
DisableUser	ユーザープールで指定したユーザーを無効にする許可を付与。このアクションによりユーザーは削除されません。	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DisassociateAppBlockBuilderAppBlock	指定された App Block ビルダーと App Block の関連付けを解除するアクセス許可を付与します	書き込み	app-block*		
			app-block-builder*		
				aws:ResourceTag/${TagKey}	
DisassociateApplicationFleet	指定したフリートから指定したアプリケーションの関連付けを解除する許可を付与します。	書き込み	application*		
			fleet*		
				aws:ResourceTag/${TagKey}	
DisassociateApplicationFromEntitlement	指定した使用権限管理から指定したアプリケーションの関連付けを解除する許可を付与	書き込み	stack*		
DisassociateFleet	指定したスタックから指定したフリートの関連付けを解除する許可を付与。	Write	fleet*		
			stack*		
				aws:ResourceTag/${TagKey}	
EnableUser	ユーザープールのユーザーを有効にする許可を付与。	Write			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ExpireSession	指定したストリーミングセッションをすぐに停止する許可を付与。	Write			
ListAssociatedFleets	指定したスタックに関連付けられているフリートの名前を取得する許可を付与。	Read	stack*		
ListAssociatedStacks	指定したフリートが関連付けられているスタックの名前を取得する許可を付与。	読み取り	fleet*		
ListEntitledApplications	指定した使用権限管理に関連付けられているアプリケーションを取得する許可を付与	リスト	stack*		
ListTagsForResource	指定した AppStream 2.0 リソースのすべてのタグのリストを取得するアクセス権限を付与します。イメージビルダー、イメージ、フリート、およびスタックのリソースをタグ付けすることができます。	読み取り			
StartAppBlockBuilder	指定された App Block ビルダーを開始するアクセス許可を付与します	書き込み	app-block-builder*		
				aws:ResourceTag/${TagKey}	
StartFleet	指定されたフリートを開始する許可を付与。	Write	fleet*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
StartImageBuilder	指定したイメージビルダーを開始する許可を付与。	書き込み	image-builder*		
				aws:ResourceTag/${TagKey}	
StopAppBlockBuilder	指定された App Block ビルダーを中止するアクセス許可を付与します	書き込み	app-block-builder*		
				aws:ResourceTag/${TagKey}	
StopFleet	指定したフリートを停止する許可を付与。	Write	fleet*		
				aws:ResourceTag/${TagKey}	
StopImageBuilder	指定したイメージビルダーを停止するアクセス権限を付与します。	Write	image-builder*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
Stream	指定したスタックから既存の認証情報およびストリームアプリケーションを使用してサインインするアクセス許可をフェデレーティッドユーザーに付与します。	Write	stack*		
				appstream:userId	
TagResource	指定した AppStream 2.0 リソースの 1 つ以上のタグを追加または上書きする許可を付与。以下のリソースがタグ付けされます：イメージビルダー、イメージ、フリート、スタック、アプリケーションブロックおよびアプリケーション。	Tagging	app-block		
			app-block-builder		
			application		
			fleet		
			image		
			image-builder		
			stack		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
UntagResource	指定した AppStream 2.0 リソースから 1 つ以上のタグの関連付けを解除する許可を付与。	Tagging	app-block		
			app-block-builder		
			application		
			fleet		
			image		
			image-builder		
			stack		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateAppBlockBuilder	指定された App Block ビルダーを更新するアクセス許可を付与します。App Block ビルダーは、App Block の作成に使用される仮想マシンです	書き込み	app-block-builder*		
				aws:ResourceTag/${TagKey}	
UpdateApplication	指定したアプリケーションに対して指定したフィールドを更新する許可を付与します。	書き込み	application*		
			app-block		
				aws:ResourceTag/${TagKey}	
UpdateDirectoryConfig	AppStream 2.0 で指定した Directory Config オブジェクトを更新する許可を付与。このオブジェクトには、フリートおよび Image Builder を Microsoft Active Directory ドメインに参加させるために必要な設定情報が含まれます。	書き込み			
UpdateEntitlement	指定した使用権限管理の指定したフィールドを更新する許可を付与	書き込み	stack*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateFleet	指定したフリートを更新する許可を付与。フリートが停止状態である場合、フリート名を除くすべての属性を更新することができます。	Write	fleet*		
			image		
				aws:ResourceTag/${TagKey}	
UpdateImagePermissions	指定したプライベートイメージのアクセス許可を追加または更新する許可を付与。	Write	image*		
				aws:ResourceTag/${TagKey}	
UpdateStack	指定したスタックに対して指定したフィールドを更新する許可を付与。	書き込み	stack*		
				aws:ResourceTag/${TagKey}	
UpdateThemeForStack	ユーザーに表示するカスタムロゴ、ウェブサイトリンク、その他のブランドなど、カスタムブランドテーマ情報を更新する許可を付与する	書き込み	stack*		

Amazon AppStream 2.0 で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
fleet	arn:${Partition}:appstream:${Region}:${Account}:fleet/${FleetName}	aws:ResourceTag/${TagKey}
image	arn:${Partition}:appstream:${Region}:${Account}:image/${ImageName}	aws:ResourceTag/${TagKey}
image-builder	arn:${Partition}:appstream:${Region}:${Account}:image-builder/${ImageBuilderName}	aws:ResourceTag/${TagKey}
stack	arn:${Partition}:appstream:${Region}:${Account}:stack/${StackName}	aws:ResourceTag/${TagKey}
app-block	arn:${Partition}:appstream:${Region}:${Account}:app-block/${AppBlockName}	aws:ResourceTag/${TagKey}
application	arn:${Partition}:appstream:${Region}:${Account}:application/${ApplicationName}	aws:ResourceTag/${TagKey}
app-block-builder	arn:${Partition}:appstream:${Region}:${Account}:app-block-builder/${AppBlockBuilderName}	aws:ResourceTag/${TagKey}

Amazon AppStream 2.0 の条件キー

Amazon AppStream 2.0 では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
appstream:userId	AppStream 2.0 ユーザーの ID によってアクセスをフィルタリングします。	String
aws:RequestTag/${TagKey}	リクエスト内のタグキーおよび値のペアのプレゼンスによってアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

AWS AppSync のアクション、リソース、および条件キー

AWS AppSync (サービスプレフィックス: appsync) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS AppSync で定義されるアクション
- AWS AppSync で定義されるリソースタイプ
- AWS AppSync の条件キー

AWS AppSync で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateApi	AppSync でカスタムドメイン名に GraphQL API をアタッチする許可を付与	書き込み	domain*		
AssociateMergedGraphqlApi	マージされた API をソース API に関連付ける許可を付与	書き込み	graphqlapi*		
AssociateSourceGraphqlApi	ソース API をマージされた API に関連付ける許可を付与	書き込み	graphqlapi*		
CreateApi	API を作成するアクセス許可を付与します	書き込み		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole
CreateApiCache	AppSync で API キャッシュを作成する許可を付与	書き込み			
CreateApiKey	API を実行しているクライアントに配布できる一意のキーを作成する許可を付与	書き込み			
CreateChannelNamespace	チャネル名前空間を作成するアクセス許可を付与します	書き込み	channelNamespace*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	データソースを作成するアクセス許可を付与	書き込み			
CreateDomainName	AppSync でカスタムドメイン名を作成する許可を付与	書き込み		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunction	新しい関数を作成する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateGraphqlApi	最上位の AppSync リソースである GraphQL API を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys appsync:Visibility	iam:CreateServiceLinkedRole
CreateResolver	リゾルバーを作成するアクセス許可を付与。リゾルバーは、受信リクエストをデータソースが理解できる形式に変換し、データソースのレスポンスを GraphQL に変換	書き込み			
CreateType	タイプを作成するためのアクセス許可を付与	書き込み			
DeleteApi	API を削除するアクセス許可を付与します。これにより、その API より下の AppSync リソースもすべてクリーンアップ	書き込み	api*		
				aws:ResourceTag/${TagKey}	
DeleteApiCache	AppSync で API キャッシュを削除する許可を付与	書き込み			
DeleteApiKey	API キーを削除する許可を付与	書き込み			
DeleteChannelNamespace	チャネル名前空間を削除するアクセス許可を付与します	書き込み	channelNamespace*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
DeleteDataSource	データソースを削除するアクセス許可を付与	書き込み			
DeleteDomainName	AppSync でカスタムドメイン名を削除する許可を付与	書き込み	domain*		
				aws:ResourceTag/${TagKey}	
DeleteFunction	関数を削除する許可を付与	書き込み			
DeleteGraphqlApi	GraphQL API を削除する許可を付与。これにより、その API より下の AppSync リソースもすべてクリーンアップ	書き込み	graphqlapi*		
				aws:ResourceTag/${TagKey}	
DeleteResolver	Resolver を削除する許可を付与	書き込み			
DeleteResourcePolicy [アクセス許可のみ]	リソースポリシーを削除する許可を付与	書き込み			
DeleteType	タイプを削除する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DisassociateApi	AppSync でカスタムドメイン名への GraphQL API のアタッチを解除するアクセス許可を付与	書き込み	domain*		
DisassociateMergedGraphqlApi	ソース API によって識別されるマージされた API から、関連付けられたソース API を削除する許可を付与	書き込み	mergedApiAssociation*		
DisassociateSourceGraphqlApi	マージされた API によって識別されるマージされた API から、関連付けられたソース API を削除する許可を付与	書き込み	sourceApiAssociation*		
EvaluateCode	ランタイムとコンテキストを使用してコードを評価するアクセス許可を付与	読み取り			
EvaluateMappingTemplate	テンプレートマッピングを評価する許可を付与	読み取り			
EventConnect	イベント API に接続するアクセス許可を付与します	書き込み	api*		
EventPublish	チャネル名前空間にイベントを発行するアクセス許可を付与します	書き込み	channelNamespace*		
EventSubscribe	チャネル名前空間をサブスクライブするアクセス許可を付与します	書き込み	channelNamespace*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
FlushApiCache	AppSync で API キャッシュをフラッシュする許可を付与	書き込み			
GetApi	API を取得するアクセス許可を付与します	読み取り	api*		
				aws:ResourceTag/${TagKey}	
GetApiAssociation	AppSync でカスタムドメイン名と GraphQL API の関連付けの詳細を読み取る許可を付与	読み取り	domain*		
GetApiCache	AppSync の API キャッシュに関する情報を読み取るためのアクセス権限を付与	読み取り			
GetChannelNamespace	チャネル名前空間を取得するアクセス許可を付与します	読み取り	channelNamespace*		
				aws:ResourceTag/${TagKey}	
GetDataSource	データソースを取得する許可を付与	読み取り			
GetDataSourceIntrospection	データソースのイントロスペクションを取得するための許可を付与	読み取り			
GetDomainName	AppSync でカスタムドメイン名に関する情報を取得する許可を付与	読み取り	domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
GetFunction	関数を取得する許可を付与	読み取り			
GetGraphqlApi	Graphql API を取得する許可を付与	読み取り	graphqlapi*		
				aws:ResourceTag/${TagKey}	
GetGraphqlApiEnvironmentVariables	GraphQL API の環境変数を取得する許可を付与する	読み取り			
GetIntrospectionSchema	GraphQL API のイントロスペクションスキーマを取得する許可を付与	読み取り			
GetResolver	リゾルバーを取得する許可を付与	読み取り			
GetResourcePolicy [許可のみ]	リソースポリシーを読み取る許可の付与	読み取り			
GetSchemaCreationStatus	スキーマ作成オペレーションの現在のステータスを取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetSourceApiAssociation	マージされた API に関連付けられたソース API に関する情報を読み取る許可を付与	読み取り	sourceApiAssociation*		
GetType	タイプを取得する許可を付与	読み取り			
GraphQL [許可のみ]	GraphQL クエリを GraphQL API に送信する許可を付与	書き込み	field*		
			graphqlapi*		
ListApiKeys	特定の API の API キーを一覧表示する許可を付与	リスト			
ListApis	APIs を一覧表示する許可を付与	リスト		aws:ResourceTag/${TagKey}	
ListChannelNamespaces	チャネル名前空間を一覧表示するアクセス許可を付与します	リスト	api*		
				aws:ResourceTag/${TagKey}	
ListDataSources	特定の API のデータソースを一覧表示する許可を付与	リスト			
ListDomainNames	AppSync でカスタムドメイン名を列挙する許可を付与	リスト		aws:ResourceTag/${TagKey}	
ListFunctions	特定の API の関数を一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListGraphqlApis	GraphQL API を一覧表示する許可を付与	リスト			
ListResolvers	特定の API およびタイプのリゾルバーを一覧表示するアクセス権限を付与	リスト			
ListResolversByFunction	特定の関数に関連付けられたリゾルバーを一覧表示する許可を付与	リスト			
ListSourceApiAssociations	特定のマージされた API に関連付けられたソース API を一覧表示する許可を付与	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	api		
			channelNamespace		
			domain		
			graphqlapi		
				aws:ResourceTag/${TagKey}	
ListTypes	特定の API のタイプを一覧表示する許可を付与	リスト			
ListTypesByAssociation	特定のマージされた API とソース API の関連付けのタイプを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutGraphqlApiEnvironmentVariables	GraphQL API の環境変数を更新する許可を付与する	書き込み			
PutResourcePolicy [アクセス許可のみ]	ソースポリシーを設定する許可を付与	書き込み			
SetWebACL	ウェブ ACL を設定する許可を付与	権限の管理			
SourceGraphQL [許可のみ]	マージされた API のソース API に GraphQL クエリを送信する許可を付与	書き込み	field* graphqlapi*		
StartDataSourceIntrospection	データソースをイントロスペクトするための許可を付与	書き込み			
StartSchemaCreation	GraphQL API に新しいスキーマを追加する許可を付与 このオペレーションは、非同期です。いつ完了したかを GetSchemaCreationStatus で表示可能	書き込み			
StartSchemaMerge	特定のマージされた API および関連付けられたソース API のスキーママージを開始する許可を付与	書き込み	sourceApiAssociation*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	api		
			channelNamespace		
			domain		
			graphqlapi		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	リソースのタグを解除する許可を付与	Tagging	api		
			channelNamespace		
			domain		
			graphqlapi		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateApi	API を更新するアクセス許可を付与します	書き込み	api*		iam:CreateServiceLinkedRole
				aws:ResourceTag/${TagKey}	
UpdateApiCache	AppSync で API キャッシュを更新する許可を付与	書き込み			
UpdateApiKey	特定の API の API キーを更新する許可を付与	書き込み			
UpdateChannelNamespace	チャネル名前空間を更新する許可を付与	書き込み	channelNamespace*		
				aws:ResourceTag/${TagKey}	
UpdateDataSource	データソースを更新する権限を付与	書き込み			
UpdateDomainName	AppSync でカスタムドメイン名を更新する許可を付与	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
UpdateFunction	既存の関数を更新する許可を付与	書き込み			
UpdateGraphqlApi	GraphQL API を更新する許可を付与	書き込み	graphqlapi*		iam:CreateServiceLinkedRole
				aws:ResourceTag/${TagKey}	
UpdateResolver	リゾルバーを更新する許可を付与	書き込み			
UpdateSourceApiAssociation	マージされた API ソースの API 関連付けを更新する許可を付与	書き込み	sourceApiAssociation*		
UpdateType	タイプを更新する許可を付与	書き込み			

AWS AppSync で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
datasource	arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/datasources/${DatasourceName}	
domain	arn:${Partition}:appsync:${Region}:${Account}:domainnames/${DomainName}	aws:ResourceTag/${TagKey}
graphqlapi	arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}	aws:ResourceTag/${TagKey}
field	arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/types/${TypeName}/fields/${FieldName}	
type	arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/types/${TypeName}	
function	arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/functions/${FunctionId}	
sourceApiAssociation	arn:${Partition}:appsync:${Region}:${Account}:apis/${MergedGraphQLAPIId}/sourceApiAssociations/${Associationid}	
mergedApiAssociation	arn:${Partition}:appsync:${Region}:${Account}:apis/${SourceGraphQLAPIId}/mergedApiAssociations/${Associationid}	
api	arn:${Partition}:appsync:${Region}:${Account}:apis/${ApiId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
channelNamespace	arn:${Partition}:appsync:${Region}:${Account}:apis/${ApiId}/channelNamespace/${ChannelNamespaceName}	aws:ResourceTag/${TagKey}

AWS AppSync の条件キー

AWS AppSync は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
appsync:Visibility	API の可視性によりアクセスをフィルタリングします	String
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアによるアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

Amazon ARC リージョンスイッチのアクション、リソース、および条件キー

Amazon ARC リージョンスイッチ (サービスプレフィックス: arc-region-switch) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon ARC リージョンスイッチで定義されるアクション
- Amazon ARC リージョンスイッチで定義されるリソースタイプ
- Amazon ARC リージョンスイッチの条件キー

Amazon ARC リージョンスイッチで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ApprovePlanExecutionStep	計画実行ステップを承認するアクセス許可を付与します	書き込み	plan*		
CancelPlanExecution	プランの実行をキャンセルするアクセス許可を付与します	書き込み	plan*		
CreatePlan	プランを作成するアクセス許可を付与します	書き込み	plan*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePlan	プランを削除するアクセス許可を付与します	書き込み	plan*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteResourcePolicy [アクセス許可のみ]	プランの RAM アクセスコントロールポリシーを削除するアクセス許可を付与します	権限の管理			
GetPlan	コントロールプレーン AWS リージョン を使用してすべての のプランに関する情報を取得する許可を付与	読み取り	plan*		
GetPlanEvaluationStatus	プランの評価ステータスを取得する許可を付与	読み取り	plan*		
GetPlanExecution	計画実行の詳細とセットアップ情報を取得する許可を付与	読み取り	plan*		
GetPlanInRegion	リージョンスイッチリージョンデータプレーン AWS リージョン を使用して、特定の のプランに関する情報を取得するアクセス許可を付与します	読み取り	plan*		
GetResourcePolicy [許可のみ]	プランのリソースポリシーを取得するアクセス許可を付与します	権限の管理	plan*		
ListPlanExecutionEvents	計画実行イベントを一覧表示するアクセス許可を付与します	リスト	plan*		
ListPlanExecutions	計画実行を一覧表示するアクセス許可を付与します	リスト	plan*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListPlans	コントロールプレーン AWS リージョン を使用してすべての の計画を一覧表示する許可を付与	リスト			
ListPlansInRegion	リージョン切り替えリージョンデータプレーン AWS リージョン を使用して、特定の の計画を一覧表示するアクセス許可を付与します	リスト			
ListRoute53HealthChecks	Route 53 ヘルスチェックを一覧表示する許可を付与	リスト	plan*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み込み	plan*		
				aws:ResourceTag/${TagKey}	
PutResourcePolicy [許可のみ]	プランの RAM アクセスコントロールポリシーを定義するアクセス許可を付与します	権限の管理			
StartPlanExecution	プランの実行を開始するアクセス許可を付与します	書き込み	plan*		
TagResource	リソースにタグを付けるアクセス許可を付与	Tagging	plan*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	Tagging	plan*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdatePlan	プランを更新するアクセス許可を付与します	書き込み	plan*		
UpdatePlanExecution	プラン実行を更新するアクセス許可を付与します	書き込み	plan*		
UpdatePlanExecutionStep	計画実行ステップを更新する許可を付与	書き込み	plan*		

Amazon ARC リージョンスイッチで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
plan	arn:${Partition}:arc-region-switch:${Region}:${Account}:plan/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon ARC リージョンスイッチの条件キー

Amazon ARC リージョンスイッチは、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リクエスト内のタグのキーと値でアクセスをフィルター	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

AWS Artifact のアクション、リソース、および条件キー

AWS Artifact (サービスプレフィックス: artifact) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Artifact で定義されるアクション
- AWS Artifact で定義されるリソースタイプ
- AWS Artifact の条件キー

AWS Artifact で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptAgreement	顧客アカウントによってまだ承諾されていない AWS 契約を承諾するアクセス許可を付与します	書き込み	agreement*		
AcceptNdaForAgreement	特定の契約リソースの NDA ドキュメントの条件を受け入れるアクセス許可を付与します	書き込み	agreement*		
GetAccountSettings	アーティファクトのアカウント設定を取得する許可を付与	読み取り			
GetAgreement	顧客アカウントによってまだ承諾されていない AWS 契約を取得する許可を付与	読み取り	agreement*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetCustomerAgreement	顧客アカウントによって承諾された AWS 契約を取得するアクセス許可を付与します	読み取り	customer-agreement*		
GetNdaForAgreement	特定の契約リソースの NDA ドキュメントを取得するアクセス許可を付与します	読み取り	agreement*		
GetReport	レポートをダウンロードする許可を付与	読み取り	report*		
GetReportMetadata	レポートに関連付けられたメタデータをダウンロードする許可を付与	読み取り	report*		
GetTermForReport	レポートに関連付けられた用語をダウンロードする許可を付与	読み取り	report*		
ListAgreements	AWS 契約を一覧表示するアクセス許可を付与します	リスト			
ListCustomerAgreements	顧客アカウントによって承諾された顧客契約リソースを一覧表示するアクセス許可を付与します	リスト			
ListReports	アカウント内のレポートを一覧表示する許可を付与	リスト			
PutAccountSettings	アーティファクトのアカウント設定を配置する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
Terminate Agreement	顧客アカウントによって以前承諾された顧客契約を終了する許可を付与	書き込み	customer-agreement *		

AWS Artifact で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
customer-agreement	arn:${Partition}:artifact::${Account}:customer-agreement/*	
agreement	arn:${Partition}:artifact:::agreement/*	
report	arn:${Partition}:artifact:${Region}::report/${ReportId}:${Version}	artifact:ReportCategory artifact:ReportSeries

AWS Artifact の条件キー

AWS Artifact は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
artifact:ReportCategory	レポートがどのカテゴリに関連付けるかによってアクセスをフィルタリングします	String
artifact:ReportSeries	レポートがどのシリーズに関連付けるかによってアクセスをフィルタリングします	String

Amazon Athena のアクション、リソース、および条件キー

Amazon Athena (サービスプレフィックス: athena) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Athena で定義されるアクション
- Amazon Athena で定義されるリソースタイプ
- Amazon Athena の条件キー

Amazon Athena で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchGetNamedQuery	1 つまたは複数の名前付きクエリに関する情報を取得する許可を付与	読み取り	workgroup *		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchGetPreparedStatement	1 つ以上のプリペアドステートメントに関する情報を取得する許可を付与します	読み取り	workgroup*		
BatchGetQueryExecution	1 つまたは複数の名クエリ実行に関する情報を取得する許可を付与	読み取り	workgroup*		
CancelCapacityReservation	キャパシティ予約をキャンセルする許可を付与	書き込み	capacity-reservation*		
CancelQueryExecution	クエリの実行をキャンセルする許可を付与 廃止済み。1.1.0 より前の Athena JDBC ドライバーを使用する AWS サービスとプリンシパルにのみ適用されます。それ以外の場合は StopQueryExecution を使用します	書き込み	workgroup*		
CreateCapacityReservation	キャパシティ予約を作成する許可を付与	書き込み	capacity-reservation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataCatalog	データカタログを作成する許可を付与	書き込み	datacatalog*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNamedQuery	名前付きクエリを作成する許可を付与	書き込み	workgroup*		
CreateNotebook	ノートブックを作成する許可を付与	書き込み	workgroup*		
CreatePreparedStatement	準備済みステートメントを作成する許可を付与	書き込み	workgroup*		
CreatePresignedNotebookUrl	署名付きのノートブック URL を作成する許可を付与	書き込み	workgroup*		
CreateWorkGroup	ワークグループを作成する許可を付与	書き込み	workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCapacityReservation	キャパシティ予約を削除する許可を付与	書き込み	capacity-reservation*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteDataCatalog	データカタログを削除する許可を付与	書き込み	datacatalog*		
DeleteNamedQuery	指定した名前付きクエリを削除する許可を付与	書き込み	workgroup*		
DeleteNotebook	ノートブックを削除する許可を付与	書き込み	workgroup*		
DeletePreparedStatement	指定した準備済みステートメントを削除する許可を付与	書き込み	workgroup*		
DeleteWorkGroup	ワークグループを削除する許可を付与	書き込み	workgroup*		
ExportNotebook	ノートブックをエクスポートする許可を付与	書き込み	workgroup*		
GetCalculationExecution	計算を実行する許可を付与	読み取り	workgroup*		
GetCalculationExecutionCode	計算実行コードを取得する許可を付与	読み取り	workgroup*		
GetCalculationExecutionStatus	計算実行ステータスを取得する許可を付与	読み取り	workgroup*		
GetCapacityAssignmentConfiguration	キャパシティ予約のキャパシティ割り当て情報を取得する許可を付与	読み取り	capacity-reservation*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetCapacityReservation	キャパシティ予約を取得する許可を付与	読み取り	capacity-reservation*		
GetCatalogs	データベースおよびテーブルへのアクセス許可を付与します。Athena JDBC ドライバーバージョン 1.1.0 を使用する AWS サービス管理ポリシーとプリンシパルにのみ適用されます。	読み取り			
GetDataCatalog	データカタログを取得する許可を付与	読み取り	datacatalog*		
GetDatabase	特定のデータカタログのデータベースを取得する許可を付与	読み取り	datacatalog*		
GetExecutionEngine	指定したデータベースおよびテーブルへのアクセス許可を付与します。Athena JDBC ドライバーバージョン 1.1.0 を使用する AWS サービス管理ポリシーとプリンシパルにのみ適用されます。	読み取り			
GetExecutionEngines	データベースおよびテーブルへのアクセス許可を付与します。Athena JDBC ドライバーバージョン 1.1.0 を使用する AWS サービス管理ポリシーとプリンシパルにのみ適用されます。	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetNamedQuery	指定した名前付きクエリに関する情報を取得する許可を付与	読み取り	workgroup *		
GetNamespace	指定したデータベースおよびテーブルへのアクセス許可を付与します。Athena JDBC ドライバーバージョン 1.1.0 を使用する AWS サービス管理ポリシーとプリンシパルにのみ適用されます。	読み取り			
GetNamespaces	データベースおよびテーブルへのアクセス許可を付与します。Athena JDBC ドライバーバージョン 1.1.0 を使用する AWS サービス管理ポリシーとプリンシパルにのみ適用されます。	読み取り			
GetNotebookMetadata	ノートブックのメタデータを取得する許可を付与	読み取り	workgroup *		
GetPreparedStatement	指定した準備済みステートメントに関する情報を取得する許可を付与	読み取り	workgroup *		
GetQueryExecution	指定したクエリ実行に関する情報を取得する許可を付与	読み取り	workgroup *		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetQueryExecutions	クエリを実行する許可を付与します。廃止済み。1.1.0 より前の Athena JDBC ドライバーを使用する AWS サービスとプリンシパルにのみ適用されます。それ以外の場合は ListQueryExecutions を使用します	読み取り			
GetQueryResults	クエリ結果を取得する許可を付与	読み取り	workgroup *		
GetQueryResultsStream	クエリ結果のストリーミングを取得する許可を付与	読み取り	workgroup *		
GetQueryRuntimeStatistics	指定したクエリ実行のランタイムの統計を取得する許可を付与	読み取り	workgroup *		
GetSession	セッションを取得する許可を付与	読み取り	workgroup *		
GetSessionStatus	セッションステータスを取得する許可を付与	読み取り	workgroup *		
GetTable	指定したテーブルへのアクセス許可を付与します。Athena JDBC ドライバーバージョン 1.1.0 を使用する AWS サービス管理ポリシーとプリンシパルにのみ適用されます。	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetTableMetadata	特定のデータカタログのテーブルに関するメタデータを取得する許可を付与	読み取り	datacatalog*		
GetTables	テーブルへのアクセス許可を付与します。Athena JDBC ドライバーバージョン 1.1.0 を使用する AWS サービス管理ポリシーとプリンシパルにのみ適用されます。	読み取り			
GetWorkGroup	ワークグループを取得する許可を付与	読み取り	workgroup*		
ImportNotebook	ノートブックをインポートする許可を付与	書き込み	workgroup*		
ListApplicationDPUSizes	ApplicationRuntimeIds のリストを返す許可を付与	リスト			
ListCalculationExecutions	計算実行のリストを返す許可を付与	リスト	workgroup*		
ListCapacityReservations	指定された のキャパシティ予約のリストを返すアクセス許可を付与します AWS アカウント	リスト			
ListDataCatalogs	指定された のデータカタログのリストを返すアクセス許可を付与します AWS アカウント	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListDatabases	特定のデータカタログのデータベースのリストを返す許可を付与	リスト	datacatalog*		
ListEngineVersions	指定された の athena エンジンバージョンのリストを返すアクセス許可を付与します AWS アカウント	読み取り			
ListExecutors	実行者のリストを返す許可を付与	リスト			
ListNamedQueries	指定された の Amazon Athena の名前付きクエリのリストを返すアクセス許可を付与します AWS アカウント	リスト	workgroup*		
ListNotebookMetadata	特定のワークグループに関するノートブックのリストを返す許可を付与	リスト	workgroup*		
ListNotebookSessions	特定のノートブックに関するセッションのリストを返す許可を付与	リスト	workgroup*		
ListPreparedStatements	指定したワークグループの準備済みステートメントのリストを返す許可を付与	リスト	workgroup*		
ListQueryExecutions	指定された のクエリ実行のリストを返すアクセス許可を付与します AWS アカウント	読み取り	workgroup*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListSessions	特定のワークグループに関するセッションのリストを返す許可を付与	リスト	workgroup*		
ListTableMetadata	特定のデータカタログのデータベース内のテーブルに関するメタデータのリストを返す許可を付与	読み取り	datacatalog*		
ListTagsForResource	リソースのタグのリストを返す許可を付与	読み取り	capacity-reservation*		
			datacatalog*		
			workgroup*		
ListWorkGroups	指定された のワークグループのリストを返すアクセス許可を付与します AWS アカウント	リスト			
PutCapacityAssignmentConfiguration	キャパシティ予約からクエリにキャパシティを割り当てる許可を付与	書き込み	capacity-reservation*		
			workgroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RunQuery	クエリを実行する許可を付与 廃止済み。1.1.0 より前の Athena JDBC ドライバーを使用する AWS サービスとプリンシパルにのみ適用されます。それ以外の場合は StartQueryExecution を使用します	書き込み			
StartCalculationExecution	計算実行を開始する許可を付与	書き込み	workgroup*		
StartQueryExecution	文字列として指定された SQL クエリを使用してクエリの実行を開始する許可を付与	書き込み	workgroup*		
StartSession	セッションを開始する許可を付与	書き込み	workgroup*		
StopCalculationExecution	計算実行を停止する許可を付与	書き込み	workgroup*		
StopQueryExecution	指定したクエリ実行を停止する許可を付与	書き込み	workgroup*		
TagResource	リソースにタグを追加する許可を付与	Tagging	capacity-reservation*		
			datacatalog*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateSession	セッションを終了する許可を付与	書き込み	workgroup*		
UntagResource	リソースからタグを削除する許可を付与	Tagging	capacity-reservation*		
			datacatalog*		
			workgroup*		
				aws:TagKeys	
UpdateCapacityReservation	キャパシティ予約を更新する許可を付与	書き込み	capacity-reservation*		
UpdateDataCatalog	データカタログを更新する許可を付与	書き込み	datacatalog*		
UpdateNamedQuery	指定した名前付きクエリを更新する許可を付与	書き込み	workgroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateNotebook	ノートブックを更新する許可を付与	書き込み	workgroup *		
UpdateNotebookMetadata	ノートブックのメタデータを更新する許可を付与	書き込み	workgroup *		
UpdatePreparedStatement	準備済みステートメントを更新する許可を付与	書き込み	workgroup *		
UpdateWorkGroup	ワークグループを更新する許可を付与	書き込み	workgroup *		

Amazon Athena で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
datacatalog	arn:${Partition}:athena:${Region}:${Account}:datacatalog/${DataCatalogName}	aws:ResourceTag/${TagKey}
workgroup	arn:${Partition}:athena:${Region}:${Account}:workgroup/${WorkGroupName}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
capacity-reservation	arn:${Partition}:athena:${Region}:${Account}:capacity-reservation/${CapacityReservationName}	aws:ResourceTag/${TagKey}

Amazon Athena の条件キー

Amazon Athena では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングする	ArrayOfString

AWS Audit Manager のアクション、リソース、および条件キー

AWS Audit Manager (サービスプレフィックス: auditmanager) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Audit Manager で定義されるアクション
- AWS Audit Manager で定義されるリソースタイプ
- AWS Audit Manager の条件キー

AWS Audit Manager で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateAssessmentReportEvidenceFolder	AWS Audit Manager で証拠フォルダを評価レポートに関連付けるアクセス許可を付与します	書き込み	assessment*		
BatchAssociateAssessmentReportEvidence	AWS Audit Manager の評価レポートに証拠のリストを関連付ける許可を付与	書き込み	assessment*		
BatchCreateDelegationByAssessment	AWS Audit Manager で評価の委任を作成する許可を付与	書き込み	assessment*		
			assessmentControlSet*		
BatchDeleteDelegat	AWS Audit Manager で評価の委任を削除する許可を付与	書き込み	assessment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ionByAssessment			assessmentControlSet*		
BatchDisassociateAssessmentReportEvidence	AWS Audit Manager の評価レポートから証拠のリストの関連付けを解除する許可を付与	書き込み	assessment*		
BatchImportEvidenceToAssessmentControl	AWS Audit Manager の評価コントロールに証拠のリストをインポートするアクセス許可を付与します	書き込み	assessmentControlSet*		
CreateAssessment	AWS Audit Manager で使用する評価を作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateAssessmentFramework	AWS Audit Manager で使用するフレームワークを作成するアクセス許可を付与します	書き込み	control*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateAssessmentReport	AWS Audit Manager で評価レポートを作成するアクセス許可を付与します	書き込み	assessment*		
CreateControl	AWS Audit Manager で使用するコントロールを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteAssessment	AWS Audit Manager で評価を削除するアクセス許可を付与します	書き込み	assessment*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteAssessmentFramework	AWS Audit Manager で評価フレームワークを削除する許可を付与	書き込み	assessmentFramework*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAssessmentFrameworkShare	AWS Audit Manager でカスタムフレームワークの共有リクエストを削除する許可を付与	書き込み			
DeleteAssessmentReport	AWS Audit Manager で評価レポートを削除する許可を付与	書き込み	assessment*		
DeleteControl	AWS Audit Manager でコントロールを削除する許可を付与	書き込み	control*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeregisterAccount	AWS Audit Manager でアカウントを登録解除するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeregisterOrganizationAdminAccount	AWS Audit Manager の委任管理者アカウントの登録を解除する許可を付与	書き込み			
DisassociateAssessmentReportEvidenceFolder	AWS Audit Manager の評価レポートから証拠フォルダの関連付けを解除する許可を付与	書き込み	assessment*		
GetAccountStatus	AWS Audit Manager でアカウントのステータスを取得する許可を付与	読み取り			
GetAssessment	AWS Audit Manager で作成された評価を取得する許可を付与	読み取り	assessment*		
GetAssessmentFramework	AWS Audit Manager で評価フレームワークを取得する許可を付与	読み取り	assessmentFramework*		
GetAssessmentReportUrl	AWS Audit Manager で評価レポートの URL を取得する許可を付与	読み取り	assessment*		
GetChangeLogs	AWS Audit Manager で評価の変更ログを取得する許可を付与	読み取り	assessment*		
GetControl	AWS Audit Manager でコントロールを取得する許可を付与	読み取り	control*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetDelegations	AWS Audit Manager ですべての委任を取得する許可を付与	リスト			
GetEvidence	AWS Audit Manager から証拠を取得する許可を付与	読み取り	assessmentControlSet*		
GetEvidenceByEvidenceFolder	AWS Audit Manager の証拠フォルダからすべての証拠を取得する許可を付与	読み取り	assessmentControlSet*		
GetEvidenceFileUploadUrl	手作業による証拠としてファイルをアップロードするために使用できる、署名済みの Amazon S3 URL を取得する許可を付与します	読み取り			
GetEvidenceFolder	AWS Audit Manager から証拠フォルダを取得する許可を付与	読み取り	assessmentControlSet*		
GetEvidenceFoldersByAssessment	AWS Audit Manager の評価から証拠フォルダを取得する許可を付与	読み取り	assessment*		
GetEvidenceFoldersByAssessmentControl	AWS Audit Manager の評価コントロールから証拠フォルダを取得する許可を付与	読み取り	assessmentControlSet*		
GetInsights	アクティブなすべての評価の分析データを取得するアクセス許可を付与します。	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetInsightsByAssessment	特定のアクティブな評価の分析データを取得するアクセス許可を付与します。	読み取り			
GetOrganizationAdminAccount	AWS Audit Manager で委任管理者アカウントを取得する許可を付与	読み取り			
GetServicesInScope	AWS Audit Manager で評価の対象となるサービスを取得する許可を付与	読み取り			
GetSettings	AWS Audit Manager で設定されたすべての設定を取得するアクセス許可を付与します	読み取り			
ListAssessmentControlInsightsByControlDomain	特定のコントロールドメインおよびアクティブアセスメント内のコントロールの分析データを一覧表示する権限を付与します。	リスト			
ListAssessmentFrameworkShareRequests	AWS Audit Manager のカスタムフレームワークに対するすべての送受信された共有リクエストを一覧表示するアクセス許可を付与します	リスト			
ListAssessmentFrameworks	AWS Audit Manager のすべての評価フレームワークを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListAssessmentReports	AWS Audit Manager ですべての評価レポートを一覧表示するアクセス許可を付与します	リスト			
ListAssessments	AWS Audit Manager ですべての評価を一覧表示するアクセス許可を付与します	リスト			
ListControlDomainInsights	すべてのアクティブな評価でコントロールドメインの分析データを一覧表示する権限を付与します。	リスト			
ListControlDomainInsightsByAssessment	特定のアクティブな評価でコントロールドメインの分析データを一覧表示する権限を付与します。	リスト			
ListControlInsightsByControlDomain	すべてのアクティブな評価で、特定のコントロールドメイン内のコントロールの分析データを一覧表示する権限を付与します。	リスト			
ListControls	AWS Audit Manager 内のすべてのコントロールを一覧表示するアクセス許可を付与します	リスト			
ListKeywordsForDataSource	AWS Audit Manager のすべてのデータソースキーワードを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListNotifications	AWS Audit Manager ですべての通知を一覧表示するアクセス許可を付与します	リスト			
ListTagsForResource	AWS Audit Manager リソースのタグを一覧表示する許可を付与	読み取り	assessment		
			control		
RegisterAccount	AWS Audit Manager にアカウントを登録する許可を付与	書き込み			
RegisterOrganizationAdminAccount	AWS Audit Manager の委任管理者として組織内のアカウントを登録する許可を付与	書き込み			
StartAssessmentFrameworkShare	AWS Audit Manager でカスタムフレームワークの共有リクエストを作成する許可を付与	書き込み	assessmentFramework*		
TagResource	AWS Audit Manager リソースにタグを付けるアクセス許可を付与します	Tagging	assessment		
			assessmentFramework		
			control		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	AWS Audit Manager リソースのタグを解除する許可を付与	Tagging	assessment	aws:ResourceTag/${TagKey}	
			assessmentFramework	aws:ResourceTag/${TagKey}	
			control	aws:ResourceTag/${TagKey}	
				aws:TagKeys	
UpdateAssessment	AWS Audit Manager で評価を更新する許可を付与	書き込み	assessment*		
UpdateAssessmentControl	AWS Audit Manager で評価コントロールを更新する許可を付与	書き込み	assessmentControlSet*		
UpdateAssessmentControlSetStatus	AWS Audit Manager の評価コントロールセットのステータスを更新する許可を付与	書き込み	assessmentControlSet*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateAssessmentFramework	AWS Audit Manager で評価フレームワークを更新する許可を付与	書き込み	assessmentFramework*		
			control*		
UpdateAssessmentFrameworkShare	AWS Audit Manager でカスタムフレームワークの共有リクエストを更新する許可を付与	書き込み	assessmentFramework*		
UpdateAssessmentStatus	AWS Audit Manager で評価のステータスを更新する許可を付与	書き込み	assessment*		
UpdateControl	AWS Audit Manager でコントロールを更新する許可を付与	書き込み	control*		
UpdateSettings	AWS Audit Manager の設定を更新する許可を付与	書き込み			
ValidateAssessmentReportIntegrity	AWS Audit Manager で評価レポートの整合性を検証するアクセス許可を付与します	読み取り			

AWS Audit Manager で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
assessment	arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${AssessmentId}	aws:ResourceTag/${TagKey}
assessmentFramework	arn:${Partition}:auditmanager:${Region}:${Account}:assessmentFramework/${AssessmentFrameworkId}	aws:ResourceTag/${TagKey}
assessmentControlSet	arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${AssessmentId}/controlSet/${ControlSetId}	
control	arn:${Partition}:auditmanager:${Region}:${Account}:control/${ControlId}	aws:ResourceTag/${TagKey}

AWS Audit Manager の条件キー

AWS Audit Manager は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列

条件キー	説明	タイプ
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon Aurora DSQL のアクション、リソース、および条件キー

Amazon Aurora DSQL (サービスプレフィックス: dsql) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Aurora DSQL で定義されるアクション
- Amazon Aurora DSQL で定義されるリソースタイプ
- Amazon Aurora DSQL の条件キー

Amazon Aurora DSQL で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddPeerCluster [アクセス許可のみ]	マルチリージョンクラスターにピアクラスターを追加する許可を付与	書き込み	Cluster*		dsql:PutMultiRegionProperties
CreateCluster	新しいクラスターを作成するアクセス許可を付与します	書き込み	Cluster*		iam:CreateServiceLinkedRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys dsql:WitnessRegion	
DbConnect	データベースに接続するアクセス許可を付与します	書き込み	Cluster*		
DbConnectAdmin	管理者ロールを使用してデータベースに接続するアクセス許可を付与します。他のロールに接続するには、DbConnect アクセス許可が必要です	書き込み	Cluster*		
DeleteCluster	クラスターとそのすべてのデータを削除するアクセス許可を付与します	書き込み	Cluster*		
GetBackupJob	Aurora DSQL クラスターバックアップジョブのステータスを取得する許可を付与	読み取り	Cluster*		
GetCluster	クラスターに関する情報を取得するアクセス許可を付与します	読み取り	Cluster*		
GetRestoreJob	Aurora DSQL クラスター復元ジョブのステータスを取得する許可を付与	読み取り	Cluster*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetVpcEndpointServiceName	クラスターの VPC エンドポイントサービス名を取得する許可を付与	読み取り	Cluster*		
ListClusters	クラスターのリストを取得するアクセス許可を付与します	リスト			
ListTagsForResource	Aurora DSQL リソースのすべてのタグを一覧表示するアクセス許可を付与します	読み取り	Cluster*		
PutMultiRegionProperties [許可のみ]	クラスターのマルチリージョンプロパティを更新する許可を付与	書き込み	Cluster*		
PutWitnessRegion [アクセス許可のみ]	マルチリージョンクラスターの監視リージョンを設定および更新するアクセス許可を付与します	書き込み	Cluster*		dsql:PutMultiRegionProperties
				dsql:WitnessRegion	
RemovePeerCluster [アクセス許可のみ]	マルチリージョンクラスターからピアクラスターを削除するアクセス許可を付与します	書き込み	Cluster*		dsql:PutMultiRegionProperties
StartBackupJob	Aurora DSQL クラスターのバックアップジョブを開始する許可を付与	書き込み	Cluster*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartRestoreJob	Aurora DSQL クラスターの復元ジョブを開始する許可を付与	書き込み	Cluster*		dsql:CreateCluster iam:CreateServiceLinkedRole
StopBackupJob	Aurora DSQL クラスターのバックアップジョブを停止する許可を付与	書き込み	Cluster*		
StopRestoreJob	Aurora DSQL クラスターの復元ジョブを停止する許可を付与	書き込み	Cluster*		
TagResource	Aurora DSQL リソースにタグを追加する許可を付与	Tagging	Cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Aurora DSQL リソースからタグを削除するアクセス許可を付与します	Tagging	Cluster*		
				aws:TagKeys	
UpdateCluster	クラスター属性を変更するアクセス許可を付与します	書き込み	Cluster*		
				dsql:WitnessRegion	

Amazon Aurora DSQL で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Cluster	arn:${Partition}:dsql:${Region}:${Account}:cluster/${Identifier}	aws:ResourceTag/${TagKey}

Amazon Aurora DSQL の条件キー

Amazon Aurora DSQL では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	String
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString
dsql:WitnessRegion	マルチリージョンクラスターの監視リージョンでアクセスをフィルタリングします	String

AWS Auto Scaling のアクション、リソース、および条件キー

AWS Auto Scaling (サービスプレフィックス: autoscaling-plans) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Auto Scaling で定義されるアクション
- AWS Auto Scaling で定義されるリソースタイプ
- AWS Auto Scaling の条件キー

AWS Auto Scaling で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateScalingPlan	スケーリングプランを作成します。	Write			
DeleteScalingPlan	指定されたスケーリングプランを削除します。	Write			
DescribeScalingPlanResources	指定されたスケーリングプラン内のスケーラブルなリソースについて説明します。	Read			
DescribeScalingPlans	指定されたスケーリングプラン、またはすべてのスケーリ	Read			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	ングプランの説明を表示します。				
GetScalingPlanResourceForecastData	スケーラブルなリソースの予測データを取得します。	Read			
UpdateScalingPlan	スケーリングプランを更新します。	Write			

AWS Auto Scaling で定義されるリソースタイプ

AWS Auto Scaling は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Auto Scaling へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Auto Scaling の条件キー

Auto Scaling には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS B2B Data Interchange のアクション、リソース、および条件キー

AWS B2B Data Interchange (サービスプレフィックス: `b2bi`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS B2B Data Interchange で定義されるアクション
- AWS B2B Data Interchange によって定義されるリソースタイプ
- AWS B2B Data Interchange の条件キー

AWS B2B Data Interchange で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateCapability	機能を作成するためのアクセス許可を付与	書き込み	transformer		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePartnership	パートナーシップを作成するためのアクセス許可を付与	書き込み	capability*		
			profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateProfile	プロファイルを作成する許可の付与	書き込み		aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey}	
CreateStarterMappingTemplate	スターター JSONATA/XSLT テンプレートを生成する許可を付与する	書き込み	transformer*		
CreateTransformer	トランスフォーマーを作成するためのアクセス許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteCapability	機能を削除するためのアクセス許可を付与	書き込み	capability*		
DeletePartnership	パートナーシップを削除するためのアクセス許可を付与	書き込み	partnership*		
DeleteProfile	プロファイルを削除する権限を付与します	書き込み	profile*		
DeleteTransformer	トランスフォーマーを削除するためのアクセス許可を付与	書き込み	transformer*		
GenerateMapping	Amazon Bedrock からスターター JSONATA/XSLT マッピングテンプレートを生成するアクセス許可を付与します	書き込み	transformer*		
GetCapability	機能を取得するためのアクセス許可を付与	読み取り	capability*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetPartnership	パートナーシップを取得するためのアクセス許可を付与	読み取り	partnership*		
GetProfile	プロファイルを取得する許可の付与	読み取り	profile*		
GetTransformer	トランスフォーマーを取得するためのアクセス許可を付与	読み取り	transformer*		
GetTransformerJob	トランスフォーマージョブを取得するためのアクセス許可を付与	読み取り	transformer*		
ListCapabilities	すべての機能を一覧表示するためのアクセス許可を付与	リスト			
ListPartnerships	すべてのパートナーシップを一覧表示するためのアクセス許可を付与	リスト			
ListProfiles	すべてのプロファイルを一覧表示するためのアクセス許可を付与	リスト			
ListTagsForResource	B2Bi リソースのタグを一覧表示するためのアクセス許可を付与	読み取り	capability		
			partnership		
			profile		
			transformer		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTransformers	すべてのトランスフォーマーを一覧表示するためのアクセス許可を付与	リスト			
StartTransformerJob	ドキュメントを変換するためのアクセス許可を付与	書き込み	transformer*		
TagResource	B2Bi リソースにタグを付けるためのアクセス許可を付与	Tagging	capability		
			partnership		
			profile		
			transformer		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestConversion	JSON/XML を edi ドキュメントに変換する許可を付与する	書き込み	transformer*		
TestMapping	サンプルファイルをマップするためのアクセス許可を付与	書き込み	transformer*		
TestParsing	EDI ドキュメントを解析するためのアクセス許可を付与	書き込み	transformer*		
UntagResource	B2Bi リソースのタグを解除するためのアクセス許可を付与	Tagging	capability		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			partnership		
			profile		
			transformer		
				aws:TagKeys	
UpdateCapability	機能を更新するためのアクセス許可を付与	書き込み	capability*		
			transformer		
UpdatePartnership	パートナーシップを更新するためのアクセス許可を付与	書き込み	partnership*		
			capability		
UpdateProfile	プロファイルを更新する許可の付与	書き込み	profile*		
UpdateTransformer	トランスフォーマーを更新するためのアクセス許可を付与	書き込み	transformer*		

AWS B2B Data Interchange によって定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
profile	arn:${Partition}:b2bi:${Region}:${Account}:profile/${ResourceId}	aws:ResourceTag/${TagKey}
capability	arn:${Partition}:b2bi:${Region}:${Account}:capability/${ResourceId}	aws:ResourceTag/${TagKey}
partnership	arn:${Partition}:b2bi:${Region}:${Account}:partnership/${ResourceId}	aws:ResourceTag/${TagKey}
transformer	arn:${Partition}:b2bi:${Region}:${Account}:transformer/${ResourceId}	aws:ResourceTag/${TagKey}

AWS B2B Data Interchange の条件キー

AWS B2B データ交換では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Backup のアクション、リソース、および条件キー

AWS Backup (サービスプレフィックス: backup) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Backup で定義されるアクション
- AWS Backup で定義されるリソースタイプ
- AWS Backup の条件キー

AWS Backup で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリス

ク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateBackupVaultMpaApprovalTeam	MPA 承認チームをバックアップボールトに関連付けるアクセス許可を付与します	書き込み	backupVault*		
				backup:MpaApprovalTeamArn	
CancelLegalHold	リーガルホールドをキャンセルする許可を付与	書き込み	legalHold*		
CopyFromBackupVault [アクセス許可のみ]	バックアップボールトからコピーするアクセス許可を付与	書き込み	recoveryPoint*		
				backup:CopyTargets	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				backup:CopyTargetOrgPaths	
CopyIntoBackupVault [アクセス許可のみ]	バックアップボールトにコピーするアクセス許可を付与	書き込み	backupVault*		
				aws:RequestTag/${TagKey}	
CreateBackupPlan	新しいバックアッププランを作成するアクセス許可を付与	書き込み	backupPlan*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBackupSelection	バックアッププランで新しいリソース割り当てを作成するアクセス許可を付与	書き込み	backupPlan*		iam:PassRole
CreateBackupVault	新しいバックアップボールトを作成するアクセス許可を付与	書き込み	backupVault*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateFramework	新しいフレームワークを作成する許可を付与	書き込み	framework*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLegalHold	新しいリーガルホールドを作成する許可を付与	書き込み	legalHold*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLogicallyAirGappedBackupVault	バックアップが保存される論理コンテナである、論理的に工アギャップされた新しいバックアップボールトを作成する許可を付与	書き込み	backupVault*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys backup:MinRetentionDays backup:MaxRetentionDays	
CreateReportPlan	新しいレポートプランを作成する許可を付与	書き込み	reportPlan*		
				aws:RequestTag/${TagKey} aws:TagKeys backup:FrameworkArns	
CreateRestoreAccessBackupVault	復元アクセスバックアップボールトを作成するアクセス許可を付与します	書き込み	backupVault*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRestoreTestingPlan	新しい復元テストプランを作成するためのアクセス許可を付与	書き込み	restoreTestingPlan*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRestoreTestingSelection	復元テストプランで新しいリソース割り当てを作成するためのアクセス許可を付与	書き込み	restoreTestingPlan*		iam:PassRole
DeleteBackupPlan	バックアッププランを削除するアクセス許可を付与	書き込み	backupPlan*		
DeleteBackupSelection	バックアッププランからリソース割り当てを削除するアクセス許可を付与	書き込み	backupPlan*		
DeleteBackupVault	バックアップボールトを削除するアクセス許可を付与	書き込み	backupVault*		
DeleteBackupVaultAccessPolicy	バックアップボールトアクセスポリシーを削除するアクセス許可を付与	権限の管理	backupVault*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteBackupVaultLockConfiguration	バックアップボールトからロック設定を削除するためのアクセス許可を付与	書き込み	backupVault*		
DeleteBackupVaultNotifications	バックアップボールトから通知を削除するためのアクセス許可を付与	書き込み	backupVault*		
DeleteBackupVaultSharingPolicy [アクセス許可のみ]	バックアップボールト共有ポリシーを削除する許可を付与	権限の管理	backupVault*		
DeleteFramework	フレームワークを削除する許可を付与	書き込み	framework*		
DeleteRecoveryPoint	バックアップボールトからリカバリポイントを削除するアクセス許可を付与	書き込み	recoveryPoint*		
DeleteReportPlan	レポートプランを削除する許可を付与	書き込み	reportPlan*		
DeleteRestoreTestingPlan	復元テストプランを削除するためのアクセス許可を付与	書き込み	restoreTestingPlan*		
DeleteRestoreTestingSelection	復元テストプランからリソース割り当てを削除するためのアクセス許可を付与	書き込み	restoreTestingPlan*		
DescribeBackupJob	バックアップジョブを記述するアクセス許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeBackupVault	指定された名前の新しいバックアップボールトを記述するアクセス許可を付与	読み込み	backupVault*		
DescribeCopyJob	コピージョブを記述するアクセス許可を付与	読み込み			
DescribeFramework	指定された名前のフレームワークを記述する許可を付与	読み込み	framework*		
DescribeGlobalSettings	グローバル設定を記述するアクセス許可を付与	読み込み			
DescribeProtectedResource	保護されたリソースを記述するアクセス許可を付与	読み込み			
DescribeRecoveryPoint	リカバリポイントを記述するアクセス許可を付与	読み込み	recoveryPoint*		
DescribeRegionSettings	リージョン設定を記述するアクセス許可を付与	読み込み			
DescribeReportJob	レポートジョブを記述する許可を付与	読み込み			
DescribeReportPlan	指定された名前のレポートプランを記述する許可を付与	読み込み	reportPlan*		
DescribeRestoreJob	復元ジョブを記述するアクセス許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisassociateBackupVaultMpaApprovalTeam	バックアップボールトから MPA 承認チームの関連付けを解除するアクセス許可を付与します	書き込み	backupVault*		
DisassociateRecoveryPoint	バックアップボールトからリカバリポイントの関連付けを解除するアクセス許可を付与	書き込み	recoveryPoint*		
DisassociateRecoveryPointFromParent	親からリカバリポイントの関連付けを解除する許可を付与	書き込み	recoveryPoint*		
ExportBackupPlanTemplate	バックアッププランを JSON として エクスポートするアクセス許可を付与	読み込み			
GetBackupPlan	バックアッププランを取得するアクセス許可を付与	読み込み	backupPlan*		
GetBackupPlanFromJSON	JSON をバックアッププランに変換するアクセス許可を付与	読み込み			
GetBackupPlanFromTemplate	テンプレートをバックアッププランに変換するアクセス許可を付与	読み込み			
GetBackupSelection	バックアッププランのリソース割り当てを取得するアクセス許可を付与	読み込み	backupPlan*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetBackupVaultAccessPolicy	バックアップボールトアクセスポリシーを取得するアクセス許可を付与	読み込み	backupVault*		
GetBackupVaultNotifications	バックアップボールト通知を取得するアクセス許可を付与	読み取り	backupVault*		
GetBackupVaultSharingPolicy [許可のみ]	バックアップボールト共有ポリシーを取得する許可を付与	読み取り	backupVault*		
GetLegalHold	リーガルホールドを取得する許可を付与	読み取り	legalHold*		
GetRecoveryPointIndexDetails	復旧ポイントのインデックス作成の詳細を取得するアクセス許可を付与します	読み取り	recoveryPoint*		
GetRecoveryPointRestoreMetadata	リカバリポイント復元メタデータを取得するアクセス許可を付与	読み取り	recoveryPoint*		
GetRestoreJobMetadata	復元ジョブに関連付けられた復元メタデータを取得するためのアクセス許可を付与	読み取り			
GetRestoreTestingInferredMetadata	復元テストによって生成された推測されるメタデータを取得するためのアクセス許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetRestoreTestingPlan	復元テストプランを取得するためのアクセス許可を付与	読み取り	restoreTestingPlan*		
GetRestoreTestingSelection	復元テストプランのリソース割り当てを取得するためのアクセス許可を付与	読み取り	restoreTestingPlan*		
GetSupportedResourceTypes	サポートされているリソースタイプを取得するアクセス許可を付与	読み取り			
ListBackupJobSummaries	バックアップジョブの概要を一覧表示する許可を付与	リスト			
ListBackupJobs	バックアップジョブを一覧表示するアクセス許可を付与	リスト			
ListBackupPlanTemplates	AWS Backup が提供するバックアッププランテンプレートを一覧表示する許可を付与	リスト			
ListBackupPlanVersions	バックアッププランのバージョンを一覧表示するアクセス許可を付与	リスト	backupPlan*		
ListBackupPlans	バックアッププランを一覧表示する許可を付与	リスト			
ListBackupSelections	特定のバックアッププランのリソース割り当てを一覧表示するアクセス許可を付与	リスト	backupPlan*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListBackupVaults	バックアップボールトを一覧表示する許可を付与	リスト			
ListCopyJobSummaries	コピージョブの概要を一覧表示する許可を付与	リスト			
ListCopyJobs	コピージョブを一覧表示するアクセス許可を付与	リスト			
ListFrameworks	フレームワークを一覧表示する許可を付与	リスト			
ListIndexedRecoveryPoints	インデックスが付けられた復旧ポイントのリストを取得するアクセス許可を付与します	リスト			
ListIndexedRecoveryPointsForSearch [許可のみ]	検索するインデックス付き復旧ポイントを一覧表示するアクセス許可を付与します	権限の管理			
ListLegalHolds	リーガルホールドー覧表示する許可を付与	リスト			
ListProtectedResources	AWS Backup で保護されたリソースを一覧表示するアクセス許可を付与します	リスト			
ListProtectedResourcesByBackupVault	バックアップボールト内の保護されたリソースを一覧表示する許可を付与	リスト	backupVault*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListRecoveryPointsByBackupVault	バックアップボールト内のリカバリポイントを一覧表示するアクセス許可を付与	リスト	backupVault*		
ListRecoveryPointsByLegalHold	リーガルホールドによるリカバリポイントを一覧表示する許可を付与	リスト	legalHold*		
ListRecoveryPointsByResource	リソースのリカバリポイントを一覧表示するアクセス許可を付与	リスト			
ListReportJobs	レポートジョブを一覧表示するための許可を付与	リスト			
ListReportPlans	レポートプランを一覧表示するための許可を付与	リスト			
ListRestoreAccessBackupVaults	バックアップボールトに関連付けられた復元アクセスバックアップボールトを一覧表示するアクセス許可を付与します	リスト	backupVault*		
ListRestoreJobSummaries	復元ジョブの概要を一覧表示する許可を付与	リスト			
ListRestoreJobs	復元ジョブを一覧表示するためのアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListRestoreJobsByProtectedResource	保護されたリソースの復元ジョブを一覧表示するためのアクセス許可を付与	リスト			
ListRestoreTestingPlans	復元テストプランを一覧表示するためのアクセス許可を付与	リスト			
ListRestoreTestingSelections	特定の復元テストプランのリソース割り当てを一覧表示するためのアクセス許可を付与	リスト	restoreTestingPlan*		
ListTags	リソースのタグを一覧表示する許可を付与	読み込み	backupPlan		
			backupVault		
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		
PutBackupVaultAccessPolicy	バックアップボールトにアクセスポリシーを追加するアクセス許可を付与	権限の管理	backupVault*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutBackupVaultLockConfiguration	バックアップボールトにロック設定を追加するためのアクセス許可を付与	書き込み	backupVault*		
				backup:ChangeableForDays backup:MinRetentionDays backup:MaxRetentionDays	
PutBackupVaultNotifications	バックアップボールトに SNS トピックを追加するアクセス許可を付与	書き込み	backupVault*		
PutBackupVaultSharingPolicy [アクセス許可のみ]	バックアップボールトに共有ポリシーを追加する許可を付与	権限の管理	backupVault*		
PutRestoreValidationResult	復元の検証結果を入力するためのアクセス許可を付与	書き込み			
RevokeRestoreAccessBackupVault	復元アクセスバックアップボールトを取り消すアクセス許可を付与します	書き込み	backupVault*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SearchRecoveryPoint [アクセス許可のみ]	復旧ポイントを検索するアクセス許可を付与します	権限の管理	recoveryPoint*		
StartBackupJob	新しいバックアップジョブを開始するアクセス許可を付与	書き込み	backupVault*		iam:PassRole
StartCopyJob	バックアップ元ボールトからバックアップ先ボールトにバックアップデータをコピーするアクセス許可を付与	書き込み	recoveryPoint*		iam:PassRole
StartReportJob	新しいレポートジョブを開始するための許可を付与	書き込み	reportPlan*		
StartRestoreJob	新しい復元ジョブを開始するアクセス許可を付与	書き込み	recoveryPoint*		iam:PassRole
StopBackupJob	バックアップジョブを停止するアクセス許可を付与	書き込み			
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	backupPlan		
			backupVault		
			framework		
			legalHold		
			recoveryPoint		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			reportPlan		
			restoreTestingPlan		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースのタグを解除する許可を付与	タグ付け	backupPlan		
			backupVault		
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateBackupPlan	バックアッププランを更新するアクセス許可を付与	書き込み	backupPlan*		
UpdateFramework	フレームワークを更新するための許可を付与	書き込み	framework*		
UpdateGlobalSettings	AWS アカウントの現在のグローバル設定を更新するアクセス許可を付与します	書き込み			
UpdateRecoveryPointIndexSettings	復旧ポイントインデックス設定を更新するアクセス許可を付与します	書き込み	recoveryPoint*		
				backup:Index	
UpdateRecoveryPointLifecycle	リカバリポイントのライフサイクルを更新するアクセス許可を付与	書き込み	recoveryPoint*		
UpdateRegionSettings	リージョンの現在のサービスオプトイン設定を更新するアクセス許可を付与	書き込み			
UpdateReportPlan	レポートプランを更新するための許可を付与	書き込み	reportPlan*		
				backup:FrameworkArns	
UpdateRestoreTestingPlan	復元テストプランを更新するためのアクセス許可を付与	書き込み	restoreTestingPlan*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateRestoreTestingSelection	復元テストプランで新しいリソース割り当てを更新するためのアクセス許可を付与	書き込み	restoreTestingPlan *		iam:PassRole

AWS Backup で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
backupVault	arn:${Partition}:backup:${Region}:${Account}:backup-vault:${BackupVaultName}	aws:ResourceTag/${TagKey}
backupPlan	arn:${Partition}:backup:${Region}:${Account}:backup-plan:${BackupPlanId}	aws:ResourceTag/${TagKey}
recoveryPoint	arn:${Partition}:${Vendor}:${Region}:*:${ResourceType}:${RecoveryPointId}	aws:ResourceTag/${TagKey}
framework	arn:${Partition}:backup:${Region}:${Account}:framework:${FrameworkName}-${FrameworkId}	aws:ResourceTag/${TagKey}
reportPlan	arn:${Partition}:backup:${Region}:${Account}:report-plan:${ReportPlanName}-${ReportPlanId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
legalHold	arn:${Partition}:backup:${Region}:${Account}:legal-hold:${LegalHoldId}	aws:ResourceTag/${TagKey}
restoreTestingPlan	arn:${Partition}:backup:${Region}:${Account}:restore-testing-plan:${RestoreTestingPlanName}-${RestoreTestingPlanId}	aws:ResourceTag/${TagKey}

AWS Backup の条件キー

AWS Backup では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	各タグの許可された値のセットでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエスト内の必須タグの存在でアクセスをフィルタリングします	ArrayOfString
backup:ChangeableForDays	ChangeableForDays パラメータの値によりアクセスをフィルタリングします	数値

条件キー	説明	タイプ
backup:CopyTargetOrgPaths	組織単位でアクセスをフィルタリングします	ArrayOfString
backup:CopyTargets	バックアップボールトの ARN でアクセスをフィルタリングします	ArrayOfARN
backup:FrameworkArns	フレームワーク ARN によりアクセスをフィルタリングします	ArrayOfARN
backup:Index	Index パラメータの値でアクセスをフィルタリングします	String
backup:MaxRetentionDays	MaxRetentionDays パラメータの値によりアクセスをフィルタリングします	数値
backup:MinRetentionDays	MinRetentionDays パラメータの値によりアクセスをフィルタリングします	数値
backup:MpaApprovalTeamArn	バックアップボールトの MPA 承認チーム ARN でアクセスをフィルタリングします	ARN

AWS Backup ゲートウェイのアクション、リソース、および条件キー

AWS Backup Gateway (サービスプレフィックス: `backup-gateway`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- バックアップ AWS ゲートウェイで定義されるアクション
- AWS Backup で定義されるリソースタイプ
- AWS Backup の条件キー

バックアップ AWS ゲートウェイで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateGatewayToServer	GateWayToServerに関連付けるアクセス許可を付与します	書き込み	gateway*		
			hypervisor*		
Backup	バックアップジョブを一覧表示するアクセス権限を付与します	書き込み	virtualmachine*		
CreateGateway	CreateGateWay にアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGateway	DeleteGateWay にアクセス許可を付与	書き込み	gateway*		
DeleteHypervisor	DeleteHypervisor を実行するアクセス許可を付与します	書き込み	hypervisor*		
DisassociateGatewayFromServer	サーバーからゲートウェイの関連付けを解除するアクセス許可を付与します	書き込み	gateway*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetBandwidthRateLimitSchedule	GetBandwidthRateLimitSchedule に許可を付与	読み取り	gateway*		
GetGateway	GetGateway に許可を付与します	読み取り	gateway*		
GetHypervisor	GetHypervisor に許可を付与	読み取り	hypervisor*		
GetHypervisorPropertyMappings	GetHypervisorPropertyMappings に許可を付与	読み取り	hypervisor*		
GetVirtualMachine	GetVirtualMachine に許可を付与します	読み取り	virtualmachine*		
ImportHypervisorConfiguration	ImporthypervisorConfiguration をインポートするアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
ListGateways	ListGateways にアクセス許可を付与	読み込み			
ListHypervisors	ListHypervisors にアクセス許可を付与	読み込み			
ListTagsForResource	タグを一覧表示するアクセス許可を付与します	読み込み	gateway hypervisor		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			virtualmachine		
ListVirtualMachines	仮想マシンを一覧表示するアクセス許可を付与します	読み取り			
PutBandwidthRateLimitSchedule	PutBandwidthRateLimitSchedule に許可を付与	書き込み	gateway*		
PutHypervisorPropertyMappings	PutHypervisorPropertyMappings に許可を付与	書き込み	hypervisor*		iam:PassRole
PutMaintenanceStartTime	MaintenNCEStartTime を配置するアクセス許可を付与します	書き込み	gateway*		
Restore	復元ジョブを一覧表示するアクセス権限を付与します	書き込み	hypervisor*		
StartVirtualMachinesMetadataSync	StartVirtualMachinesMetadataSync に許可を付与	書き込み	hypervisor*		iam:PassRole
TagResource	リソースにタグを付けるアクセス許可を付与します	Tagging	gateway		
			hypervisor		
			virtualmachine		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
TestHypervisorConfiguration	Testhypervisor 設定にアクセス権限を付与します	書き込み	gateway*		
UntagResource	リソースのタグを解除するアクセス許可を付与します	Tagging	gateway		
			hypervisor		
			virtualmachine		
				aws:TagKeys	
UpdateGatewayInformation	UpdateGatewayInformation するアクセス許可を付与します	書き込み	gateway*		
UpdateGatewaySoftwareNow	UpdateGatewaySoftwareNow に権限を付与します	書き込み	gateway*		
UpdateHypervisor	UpdateHypervisor のアクセス許可を付与します	書き込み	gateway*		

AWS Backup で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
gateway	`arn:${Partition}:backup-gateway:${Region}:${Account}:gateway/${GatewayId}`	aws:ResourceTag/${TagKey}
hypervisor	`arn:${Partition}:backup-gateway:${Region}:${Account}:hypervisor/${HypervisorId}`	aws:ResourceTag/${TagKey}
virtualmachine	`arn:${Partition}:backup-gateway:${Region}:${Account}:vm/${VirtualmachineId}`	aws:ResourceTag/${TagKey}

AWS Backup の条件キー

AWS Backup Gateway では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	各タグの許可された値のセットでアクセスをフィルタリングします	String

条件キー	説明	タイプ
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値でアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内の必須タグの存在でアクセスをフィルタリングします	ArrayOfString

AWS Backup Search のアクション、リソース、および条件キー

AWS Backup Search (サービスプレフィックス: backup-search) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Backup Search で定義されるアクション
- AWS Backup Search で定義されるリソースタイプ
- AWS バックアップ検索の条件キー

AWS Backup Search で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetSearchJob	検索ジョブの詳細を取得するアクセス許可を付与します	読み取り	searchJob*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetSearchResultExportJob	検索結果のエクスポートジョブの詳細を取得するアクセス許可を付与します	読み取り	searchExportJob*		
ListSearchJobBackups	検索ジョブの範囲内のバックアップを一覧表示するアクセス許可を付与します	読み取り	searchJob*		
ListSearchJobResults	検索ジョブの結果を一覧表示するアクセス許可を付与します	読み取り	searchJob*		
ListSearchJobs	検索ジョブを一覧表示するアクセス許可を付与します	リスト			
ListSearchResultExportJobs	検索結果のエクスポートジョブを一覧表示するアクセス許可を付与します	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	searchExportJob		
			searchJob		
StartSearchJob	検索ジョブを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartSearchResultExportJob	既存の検索ジョブのエクスポートジョブを開始する許可を付与	書き込み	searchJob*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
StopSearchJob	進行中の検索ジョブを停止するアクセス許可を付与します	書き込み	searchJob*		
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	searchExportJob		
			searchJob		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースのタグを解除する許可を付与	Tagging	searchExportJob		
			searchJob		
				aws:TagKeys	

AWS Backup Search で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
searchJob	arn:${Partition}:backup-search:${Region}:${Account}:search-job/${ResourceId}	aws:ResourceTag/${TagKey}
searchExportJob	arn:${Partition}:backup-search:${Region}:${Account}:search-export-job/${ResourceId}	aws:ResourceTag/${TagKey}

AWS バックアップ検索の条件キー

AWS Backup Search では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	各タグの許可された値のセットでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列

条件キー	説明	タイプ
aws:TagKeys	リクエスト内の必須タグの存在でアクセスをフィルタリングします	ArrayOfString

AWS Backup ストレージのアクション、リソース、および条件キー

AWS バックアップストレージ (サービスプレフィックス: backup-storage) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Backup ストレージで定義されるアクション
- AWS Backup ストレージで定義されるリソースタイプ
- AWS Backup ストレージの条件キー

AWS Backup ストレージで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CommitBackupJob [アクセス許可のみ]	バックアップジョブを実行する許可を付与	書き込み			
DeleteObjects [アクセス許可のみ]	オブジェクトを削除する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeBackupJob [アクセス許可のみ]	バックアップジョブを記述する許可を付与	書き込み			
GetBaseBackup [アクセス許可のみ]	ベースバックアップを取得する許可を付与	書き込み			
GetChunk [アクセス許可のみ]	復元ジョブのリカバリポイントからデータを取得する許可の付与	書き込み			
GetIncrementalBaseBackup [アクセス許可のみ]	増分ベースバックアップを取得する許可を付与	書き込み			
GetObjectMetadata [アクセス許可のみ]	復元ジョブのリカバリポイントからメタデータを取得する許可の付与	書き込み			
ListChunks [アクセス許可のみ]	復元ジョブのリカバリポイントからデータを一覧表示する許可の付与	書き込み			
ListObjects [アクセス許可のみ]	復元ジョブのリカバリポイントからデータを一覧表示する許可の付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
MountCapsule [アクセス許可のみ]	KMS キーをバックアップボールトに関連付けます。	書き込み			
NotifyObjectComplete [アクセス許可のみ]	アップロードされたデータをバックアップジョブの完了としてマークする許可を付与	書き込み			
PutChunk [アクセス許可のみ]	バックアップジョブの AWS バックアップマネージドリカバリポイントにデータをアップロードするアクセス許可を付与します	書き込み			
PutObject [アクセス許可のみ]	オブジェクトを配置する許可を付与	書き込み			
StartObject [アクセス許可のみ]	バックアップジョブの AWS バックアップマネージドリカバリポイントにデータをアップロードするアクセス許可を付与します	書き込み			
UpdateObjectComplete [アクセス許可のみ]	オブジェクトを完了に更新する許可を付与	書き込み			

AWS Backup ストレージで定義されるリソースタイプ

AWS バックアップストレージは、IAM ポリシーステートメントの Resource要素でのリソース ARN の指定をサポートしていません。 AWS Backup ストレージへのアクセスを許可するには、ポリシーで "Resource": "*" を指定します。

AWS Backup ストレージの条件キー

バックアップストレージには、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Batch のアクション、リソース、および条件キー

AWS バッチ (サービスプレフィックス: batch) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Batch で定義されるアクション
- AWS Batch で定義されるリソースタイプ
- AWS Batch の条件キー

AWS Batch で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelJob	アカウントの AWS バッチジョブキューでジョブをキャ	書き込み	job*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	ンセルするアクセス許可を付与します				
CreateComputeEnvironment	アカウントに AWS バッチコンピューティング環境を作成するアクセス許可を付与します	書き込み	compute-environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConsumableResource	アカウントに AWS バッチ消費リソースを作成するアクセス許可を付与します	書き込み	consumable-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJobQueue	アカウントに AWS バッチジョブキューを作成するアクセス許可を付与します	書き込み	job-queue*	aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			compute-environment		
			scheduling-policy		
			service-environment		
CreateSchedulingPolicy	アカウントに AWS バッチスケジューリングポリシーを作成するアクセス許可を付与します	書き込み	scheduling-policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateServiceEnvironment	アカウントに AWS バッチサービス環境を作成するアクセス許可を付与します	書き込み	service-environment*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteComputeEnvironment	アカウントの AWS バッチコンピューティング環境を削除するアクセス許可を付与します	書き込み	compute-environment*		
DeleteConsumableResource	アカウントの AWS バッチ消費リソースを削除するアクセス許可を付与します	書き込み	consumable-resource*		
DeleteJobQueue	アカウントの AWS バッチジョブキューを削除するアクセス許可を付与します	書き込み	job-queue*		
DeleteSchedulingPolicy	アカウントの AWS バッチスケジューリングポリシーを削除するアクセス許可を付与します	書き込み	scheduling-policy*		
DeleteServiceEnvironment	アカウントの AWS バッチサービス環境を削除するアクセス許可を付与します	書き込み	service-environment*		
DeregisterJobDefinition	アカウントで AWS バッチジョブ定義の登録を解除するアクセス許可を付与します	書き込み	job-definition-revision*		
DescribeComputeEnvironments	アカウント内の 1 つ以上の AWS バッチコンピューティング環境を記述するアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeConsumableResource	アカウント内の 1 つ以上の AWS バッチ消費リソースを記述するアクセス許可を付与します	読み取り	consumable-resource*		
DescribeJobDefinitions	アカウント内の 1 つ以上の AWS バッチジョブ定義を記述するアクセス許可を付与します	読み取り			
DescribeJobQueues	アカウント内の 1 つ以上の AWS バッチジョブキューを記述するアクセス許可を付与します	読み取り			
DescribeJobs	アカウントの AWS バッチジョブのリストを記述するアクセス許可を付与します	読み取り			
DescribeSchedulingPolicies	アカウント内の 1 つ以上の AWS バッチスケジューリングポリシーを記述するアクセス許可を付与します	読み取り			
DescribeServiceEnvironments	アカウント内の 1 つ以上の AWS バッチサービス環境を記述するアクセス許可を付与します	読み取り			
DescribeServiceJob	アカウントの AWS バッチサービスジョブを記述するアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetJobQueueSnapshot	アカウント内の AWS バッチジョブキューのスナップショットを取得するアクセス許可を付与します	読み取り	job-queue*		
ListConsumableResources	アカウントの AWS バッチ消費リソースを一覧表示するアクセス許可を付与します	リスト			
ListJobs	アカウント内の指定された AWS バッチジョブキューのジョブを一覧表示するアクセス許可を付与します	リスト			
ListJobsByConsumableResource	アカウント内の特定の消耗リソースを必要とする AWS バッチジョブを一覧表示する許可を付与	リスト	consumable-resource*		
ListSchedulingPolicies	アカウントの AWS バッチスケジューリングポリシーを一覧表示するアクセス許可を付与します	読み取り			
ListServiceJobs	アカウント内の指定された AWS バッチジョブキューのサービスジョブを一覧表示するアクセス許可を付与します	リスト			
ListTagsForResource	アカウントの AWS バッチリソースのタグを一覧表示するアクセス許可を付与します	読み取り	compute-environment		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			consumable-resource		
			job		
			job-definition-revision		
			job-queue		
			scheduling-policy		
			service-environment		
			service-job		
RegisterJobDefinition	アカウントに AWS バッチ ジョブ定義を登録するアクセス許可を付与します	書き込み	job-definition*		
			consumable-resource		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				batch:User batch:Privileged batch:Image batch:LogDriver batch:AWSLogsGroup batch:AWSLogsRegion batch:AWSLogsStreamPrefix batch:AWSLogsCreateGroup batch:EKSServiceAccountName batch:EKSImage batch:EKSRunAsUser	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				batch:EKSRunAsGroup batch:EKSPrivileged batch:EKSNamespace aws:RequestTag/${TagKey} aws:TagKeys	
SubmitJob	アカウントのジョブ定義から AWS バッチジョブを送信する許可を付与	書き込み	job*	batch:ShareIdentifier batch:EKSImage batch:EKSNamespace aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			job-definition*		
			job-queue*		
			consumable-resource		
SubmitServiceJob	AWS バッチサービスジョブを送信する許可を付与	書き込み	job-queue*		
			service-job*	batch:ShareIdentifier aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	アカウントの AWS バッチリソースにタグを付けるアクセス許可を付与します	Tagging	compute-environment		
			consumable-resource		
			job		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			job-definition-revision		
			job-queue		
			scheduling-policy		
			service-environment		
			service-job		
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateJob	アカウントの AWS バッチジョブキューでジョブを終了するアクセス許可を付与します	書き込み	job*		
TerminateServiceJob	アカウントの AWS バッチジョブキューでサービスジョブを終了するアクセス許可を付与します	書き込み	service-job*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	アカウントの AWS バッチリソースのタグを解除するアクセス許可を付与します	Tagging	compute-environment		
			consumable-resource		
			job		
			job-definition-revision		
			job-queue		
			scheduling-policy		
			service-environment		
			service-job		
				aws:TagKeys	
UpdateComputeEnvironment	アカウントの AWS バッチコンピューティング環境を更新する許可を付与	書き込み	compute-environment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateConsumableResource	アカウントの AWS バッチ消費リソースを更新するアクセス許可を付与します	書き込み	consumable-resource*		
UpdateJobQueue	アカウントの AWS バッチジョブキューを更新する許可を付与	書き込み	job-queue*		
			compute-environment		
			scheduling-policy		
UpdateSchedulingPolicy	アカウントの AWS バッチスケジューリングポリシーを更新する許可を付与	書き込み	scheduling-policy*		
UpdateServiceEnvironment	アカウントの AWS バッチサービス環境を更新するアクセス許可を付与します	書き込み	service-environment*		

AWS Batch で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
compute-environment	arn:${Partition}:batch:${Region}:${Account}:compute-environment/${ComputeEnvironmentName}	aws:ResourceTag/${TagKey}
job-queue	arn:${Partition}:batch:${Region}:${Account}:job-queue/${JobQueueName}	aws:ResourceTag/${TagKey}
job-definition	arn:${Partition}:batch:${Region}:${Account}:job-definition/${JobDefinitionName}	
job-definition-revision	arn:${Partition}:batch:${Region}:${Account}:job-definition/${JobDefinitionName}:${Revision}	aws:ResourceTag/${TagKey}
job	arn:${Partition}:batch:${Region}:${Account}:job/${JobId}	aws:ResourceTag/${TagKey}
scheduling-policy	arn:${Partition}:batch:${Region}:${Account}:scheduling-policy/${SchedulingPolicyName}	aws:ResourceTag/${TagKey}
service-environment	arn:${Partition}:batch:${Region}:${Account}:service-environment/${ServiceEnvironmentName}	aws:ResourceTag/${TagKey}
service-job	arn:${Partition}:batch:${Region}:${Account}:service-job/${JobId}	aws:ResourceTag/${TagKey}
consumable-resource	arn:${Partition}:batch:${Region}:${Account}:consumable-resource/${ConsumableResourceName}	aws:ResourceTag/${TagKey}

AWS Batch の条件キー

AWS Batch では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
batch:AWSLogsCreateGroup	指定したロギングドライバーに基づいてアクセスをフィルタリングし、awslogs グループがログに対して作成されるかどうかを決定	Bool
batch:AWSLogsGroup	ログが配置されている awslogs グループに基づいてアクセスをフィルタリング	String
batch:AWSLogsRegion	ログが送信されるリージョンに基づいてアクセスをフィルタリング	String
batch:AWSLogsStreamPrefix	awslogs ログストリームプレフィックスに基づいてアクセスをフィルタリング	String
batch:EKSImage	Amazon EKS ジョブのコンテナ開始に使用するイメージでアクセスをフィルタリング	String

条件キー	説明	タイプ
batch:EKSNamespace	Amazon EKS ジョブのポッドを実行するために使用されるクラスターの名前空間でアクセスをフィルタリングします	String
batch:EKSPrivileged	Amazon EKS ジョブのホストコンテナインスタンス (ルートユーザーと同様) に対する昇格された特権がコンテナに付与されたかどうかを特定する、指定された特権パラメータ値でアクセスをフィルタリング	Bool
batch:EKSRunAsGroup	Amazon EKS ジョブのコンテナ開始に使用する、指定されたグループ数値 ID (gid) でアクセスをフィルタリング	数値
batch:EKSRunAsUser	Amazon EKS ジョブのコンテナ開始に使用する、指定されたユーザー数値 ID (uid) でアクセスをフィルタリング	数値
batch:EKSServiceAccountName	Amazon EKS ジョブのポッド実行に使用するサービスアカウント名でアクセスをフィルタリング	String
batch:Image	コンテナ開始に使用するイメージでアクセスをフィルタリング	String
batch:LogDriver	コンテナに使用されるログドライバーに基づいてアクセスをフィルタリング	String
batch:Privileged	コンテナに、ホストコンテナインスタンスに対する昇格された権限 (ルートユーザーと同様) が付与されたかどうかを決定する指定されたパラメータ値に基づいてアクセスをフィルタリング	Bool
batch:ShareIdentifier	送信ジョブ内で使用される ShareIdentifier によるアクセスをフィルタリングします。	String
batch:User	コンテナ内で使用されるユーザー名または数値 uid に基づいてアクセスをフィルタリング	String

Amazon Bedrock のアクション、リソース、条件キー

Amazon Bedrock (サービスプレフィックス: bedrock) には、IAM 許可ポリシーで使用できる次のサービス固有のリソース、アクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Bedrock によって定義されたアクション
- Amazon Bedrock によって定義されたリソースタイプ
- Amazon Bedrock の条件キー

Amazon Bedrock によって定義されたアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリス

ク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AllowVendedLogDeliveryForResource [アクセス許可のみ]	ナレッジベースの vended log 配信を設定する許可を付与する	権限の管理	knowledge-base		
ApplyGuardrail	ガードレールを適用する許可を付与する	読み取り	guardrail*		
			guardrail-profile		
AssociateAgentCollaborator	別の既存のエージェントを共同作業者として既存のエー	書き込み	agent*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	ジェントに関連付けるアクセス許可を付与します				
AssociateAgentKnowledgeBase	ナレッジベースをエージェントに関連付ける許可を付与	書き込み	agent*		
			knowledge-base*		
AssociateThirdPartyKnowledgeBase [アクセス許可のみ]	サードパーティのプラットフォームを使用してナレッジデータを保存する許可を付与	書き込み		bedrock:ThirdPartyKnowledgeBaseCredentialsSecretArn	
BatchDeleteEvaluationJob	bedrock 評価ジョブのリストをバッチ削除する許可を付与する	書き込み	evaluation-job*		
CallWithBearerToken	ベアラートークンを使用するアクセス許可を付与します	読み取り			
CancelAutomatedReasoningPolicyBuildWorkflow	自動推論ポリシーのビルドワークフローをキャンセルするアクセス許可を付与します	書き込み	automated-reasoning-policy*		
CreateAgent	ドラフトエージェントバージョンを指す新しいエージェントとテストエージェントのエイリアスを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateAgentActionGroup	既存のエージェントに新しいアクショングループを作成する許可を付与	書き込み	agent*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAgentAlias	エージェントの新しいエイリアスを作成する許可を付与	書き込み	agent*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAutomatedReasoningPolicy	新しい自動推論ポリシーを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAutomatedReasoningPolicyTestCase	自動推論ポリシーのテストケースを作成するアクセス許可を付与します	書き込み	automated-reasoning-policy*		
CreateAutomatedReasoningPolicyVersion	新しい自動推論ポリシーバージョンを作成するアクセス許可を付与します	書き込み	automated-reasoning-policy*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBlueprint	データ自動化からのカスタム出力のブループリントを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateBlueprintVersion	既存のブループリントの新しいバージョンを作成するアクセス許可を付与します	書き込み	blueprint*		
CreateCustomModel	Bedrock にカスタムモデルを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomModelDeployment	カスタムモデルのカスタムモデルデプロイを作成するアクセス許可を付与します	書き込み	custom-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateDataAutomationProject	データ自動化プロジェクトを作成するアクセス許可を付与します	書き込み	blueprint		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	データソースを作成するアクセス許可を付与	書き込み	knowledge-base*		
CreateEvaluationJob	基盤モデルまたはカスタムモデルの評価ジョブを作成するためのアクセス許可を付与	書き込み	custom-model*		
			default-prompt-router*		
			foundation-model*		
			prompt-router*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateFlow	プロンプトフローを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFlowAlias	プロンプトフローのエイリアスを作成する許可を付与する	書き込み	flow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFlowVersion	プロンプトフローのイミュータブルバージョンを作成する許可を付与する	書き込み	flow*		
CreateFoundationModelAgreement	新しい基盤モデル契約を作成する許可を付与	書き込み			
CreateGuardrail	新しいガードレールを作成するためのアクセス許可を付与	書き込み	automated-reasoning-policy		
			automated-reasoning-policy-version		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			guardrail-profile		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateGuardrailVersion	新しいガードレールバージョンを作成するためのアクセス許可を付与	書き込み	guardrail*		
CreateInferenceProfile	推論プロファイルを作成するアクセス許可を付与します	書き込み	application-inference-profile*		
			foundation-model*		
			inference-profile*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInvocation	既存のセッションで新しい呼び出しを作成するアクセス許可を付与します	書き込み	session*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateKnowledgeBase	ナレッジベースを作成するためのアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMarketplaceModelEndpoint	マーケットプレイスモデルエンドポイントを作成するアクセス許可を付与します	書き込み			
CreateModelCopyJob	リージョン間またはアカウント間でカスタムモデルをコピーするためのジョブを作成する許可を付与する	書き込み	custom-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelCustomizationJob	カスタムトレーニングデータを使用してモデルをカスタマイズするジョブを作成するための許可を付与します	書き込み	custom-model*		
			foundation-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateModelEvaluationJob	基盤モデルまたはカスタムモデルの評価ジョブを作成するためのアクセス許可を付与	書き込み	custom-model*		
			foundation-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelImportJob	Bedrock にモデルをインポートするためのジョブを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelInvocationJob	新しいモデル呼び出しジョブを作成するためのアクセス許可を付与	書き込み	custom-model*		
			foundation-model*		
			model-invocation-job*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePrompt	プロンプトを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePromptRouter	カスタムプロンプトルーターを作成するアクセス許可を付与します	書き込み	application-inference-profile*		
			foundation-model*		
			inference-profile*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePromptVersion	プロンプトのバージョンを作成する許可を付与する	書き込み	prompt*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProvisionedModelThroughput	新しいプロビジョニングされたモデルスループットを作成する許可を付与	書き込み	custom-model*		
			foundation-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSession	新しいセッションを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAgent	以前に作成したエージェントを削除するためのアクセス許可を付与	書き込み	agent*		
DeleteAgentActionGroup	以前に作成したアクショングループを削除するためのアクセス許可を付与	書き込み	agent*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteAgentAlias	以前に作成したエージェントエイリアスを削除するためのアクセス許可を付与	書き込み	agent-alias*		
DeleteAgentMemory	エイリアスの既存のメモリを削除する許可を付与する	書き込み	agent-alias*		
DeleteAgentVersion	以前に作成したエージェントバージョンを削除するためのアクセス許可を付与	書き込み	agent*		
DeleteAutomatedReasoningPolicy	自動推論ポリシーまたはそのバージョンを削除するアクセス許可を付与します	書き込み	automated-reasoning-policy*		
			automated-reasoning-policy-version*		
DeleteAutomatedReasoningPolicyBuildWorkflow	自動推論ポリシーのビルドワークフローを削除する許可を付与	書き込み	automated-reasoning-policy*		
DeleteAutomatedReasoningPolicyTestCase	自動推論ポリシーのテストケースを削除する許可を付与	書き込み	automated-reasoning-policy*		
DeleteBlueprint	データ自動化のブループリントを削除するアクセス許可を付与します	書き込み	blueprint*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteCustomModel	以前に作成したカスタムモデルを削除するための許可を付与します	書き込み	custom-model*		
DeleteCustomModelDeployment	前に作成したカスタムモデルデプロイを削除するアクセス許可を付与します	書き込み	custom-model-deployment*		
DeleteDataAutomationProject	データ自動化プロジェクトを削除するアクセス許可を付与します	書き込み	data-automation-project*		
DeleteDataSource	データソースを削除するアクセス許可を付与	書き込み	knowledge-base*		
DeleteFlow	保存されたプロンプトを削除するための許可を付与する	書き込み	flow*		
DeleteFlowAlias	プロンプトフローのエイリアスを削除する許可を付与する	書き込み	flow-alias*		
DeleteFlowVersion	プロンプトフローのバージョンを削除する許可を付与する	書き込み	flow*		
DeleteFoundationModelAgreement	以前に作成した基盤モデル契約を削除する許可を付与	書き込み			
DeleteGuardrail	ガードレールまたはそのバージョンを削除するためのアクセス許可を付与	書き込み	guardrail*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteImportedModel	以前に作成した Bedrock のインポート済みモデルを削除する許可を付与する	書き込み	imported-model*		
DeleteInferenceProfile	推論プロファイルを削除するアクセス許可を付与します	書き込み	application-inference-profile*		
DeleteKnowledgeBase	ナレッジベースを削除するためのアクセス許可を付与	書き込み	knowledge-base*		
DeleteKnowledgeBaseDocuments	ナレッジベースからドキュメントを削除するアクセス許可を付与します	書き込み	knowledge-base*		
DeleteMarketplaceModelAgreement	Bedrock Marketplace 対応 AWS マーケットプレイスモデルからサブスクリプションを解除する許可を付与	書き込み			
DeleteMarketplaceModelEndpoint	マーケットプレイスモデルエンドポイントを削除するアクセス許可を付与します	書き込み	bedrock-marketplace-model-endpoint*		
DeleteModelInvocationLoggingConfiguration	既存の呼び出しログ記録設定を削除する許可を付与	書き込み			
DeletePrompt		書き込み	prompt*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	プロンプトまたはそのバージョンを削除する許可を付与する		prompt-version*		
DeletePromptRouter	カスタムプロンプトルーターを削除するアクセス許可を付与します	書き込み	prompt-router*		
DeleteProvisionedModelThroughput	以前に作成したプロビジョニングされたモデルスループットを削除する許可を付与	書き込み	provisioned-model*		
DeleteResourcePolicy [アクセス許可のみ]	以前に作成した Bedrock リソースポリシーを削除する	書き込み	custom-model*		
DeleteSession	前に作成したセッションを削除するアクセス許可を付与します	書き込み	session*		
DeregisterMarketplaceModelEndpoint	Bedrock Marketplace で使用できないように、マーケットプレイスモデルエンドポイントの登録を解除するアクセス許可を付与します	書き込み	bedrock-marketplace-model-endpoint*		
DetectGeneratedContent	提供されたコンテンツが Amazon Bedrock を使用して生成されたかどうかを検出する許可を付与する	読み取り	foundation-model*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DisassociateAgentCollaborator	以前に関連付けた共同作業者の関連付けを解除するアクセス許可を付与します	書き込み	agent*		
DisassociateAgentKnowledgeBase	エージェントからナレッジベースの関連付けを解除する許可を付与	書き込み	agent*		
			knowledge-base*		
EndSession	前に作成したセッションを終了するアクセス許可を付与します	書き込み	session*		
ExportAutomatedReasoningPolicyVersion	自動推論ポリシーバージョンアーティファクトを取得する許可を付与	読み取り	automated-reasoning-policy*		
			automated-reasoning-policy-version*		
GenerateQuery	ユーザー入力に関連付けられたクエリを生成するアクセス許可を付与します	読み取り			
GetAgent	既存のエージェントを取得する許可を付与	読み取り	agent*		
GetAgentActionGroup	既存のアクショングループを取得する許可を付与	読み取り	agent*		
GetAgentAlias	既存のエイリアスを取得する許可を付与	読み取り	agent-alias*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetAgentCollaborator	既存の共同作業者を取得するアクセス許可を付与します	読み取り	agent*		
GetAgentKnowledgeBase	エージェントに関連付けられたナレッジベースを記述する許可を付与	読み取り	agent*		
			knowledge-base*		
GetAgentMemory	既存のエイリアスのメモリを取得する許可を付与する	読み取り	agent-alias*		
GetAgentVersion	エージェントの既存のバージョンを取得する許可を付与	読み取り	agent*		
GetAsyncInvoke	送信した非同期呼び出しに関連付けられたプロパティを取得するアクセス許可を付与します	読み取り	async-invoke*		
GetAutomatedReasoningPolicy	自動推論ポリシーまたはそのバージョンを取得する許可を付与	読み取り	automated-reasoning-policy*		
			automated-reasoning-policy-version*		
GetAutomatedReasoningPolicyAnnotations	自動推論ポリシーのビルドワークフローの注釈を取得する許可を付与	読み取り	automated-reasoning-policy*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetAutomatedReasoningPolicyBuildWorkflow	自動推論ポリシーのビルドワークフローを取得する許可を付与	読み取り	automated-reasoning-policy*		
GetAutomatedReasoningPolicyBuildWorkflowResultAssets	自動推論ポリシーのビルドワークフローのアセットを取得する許可を付与	読み取り	automated-reasoning-policy*		
GetAutomatedReasoningPolicyNextScenario	自動推論ポリシーのビルドワークフローについて、次にレビューされていない生成シナリオを取得するアクセス許可を付与します	読み取り	automated-reasoning-policy*		
GetAutomatedReasoningPolicyTestCase	自動推論ポリシーのテストケースを取得する許可を付与	読み取り	automated-reasoning-policy*		
GetAutomatedReasoningPolicyTestResult	自動推論ポリシーのテストケースの結果を取得する許可を付与	読み取り	automated-reasoning-policy*		
GetBlueprint	データ自動化用の既存のブループリントを取得する許可を付与	読み取り	blueprint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetBlueprintRecommendation [許可のみ]	ブループリントレコメンデーションを取得するアクセス許可を付与します	読み取り			
GetCustomModel	作成した Bedrock カスタムモデルに関連付けられたプロパティを取得するための許可を付与します	読み取り	custom-model*		
GetCustomModelDeployment	カスタムモデルのデプロイに関連付けられたプロパティを取得するアクセス許可を付与します。このオペレーションを使用して、カスタムモデルデプロイのステータスを取得します。	読み取り	custom-model-deployment*		
GetDataAutomationProject	既存のデータ自動化プロジェクトを取得する許可を付与	読み取り	data-automation-project*		
GetDataAutomationStatus	データ自動化呼び出しジョブのステータスを取得するアクセス許可を付与します	読み取り	data-automation-invocation-job*		
GetDataSource	既存のデータソースを取得する許可を付与	読み取り	knowledge-base*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetEvaluationJob	評価ジョブに関連付けられたプロパティを取得するための許可を付与します。このオペレーションを使用して、評価ジョブのステータスを取得する	読み取り	evaluation-job*		
GetExecutionFlowSnapshot	フロー実行のフロー定義を取得する許可を付与	読み取り	flow*		
			flow-alias*		
			flow-execution*		
GetFlow	既存のプロンプトフローを取得する許可を付与する	読み取り	flow*		
GetFlowAlias	プロンプトフローの既存のエイリアスを取得する許可を付与する	読み取り	flow-alias*		
GetFlowExecution	フローエイリアスの既存の実行を取得する許可を付与	読み取り	flow*		
			flow-alias*		
			flow-execution*		
GetFlowVersion	プロンプトフローの既存のバージョンを取得する許可を付与する	読み取り	flow*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetFoundationModel	Bedrock の基盤モデルに関連付けられたプロパティを取得する許可を付与	読み取り	foundation-model*		
GetFoundationModelAvailability	基盤モデルの可用性を取得する許可を付与	読み取り			
GetGuardrail	ガードレールまたはそのバージョンを取得するためのアクセス許可を付与	読み取り	guardrail*		
GetImportedModel	Bedrock のインポート済みモデルに関連付けられたプロパティを取得する許可を付与する	読み取り	imported-model*		
GetInferenceProfile	推論プロファイルに関連付けられたプロパティを取得する許可を付与する	読み取り	application-inference-profile*		
			inference-profile*		
GetIngestionJob	既存の取り込みジョブを取得する許可を付与	読み取り	knowledge-base*		
GetInvocationStep	セッションから呼び出しステップを取得するアクセス許可を付与します	読み取り	session*		
GetKnowledgeBase	既存のナレッジベースを取得する許可を付与	読み取り	knowledge-base*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetKnowledgeBaseDocuments	ナレッジベースのドキュメントの詳細を取得するアクセス許可を付与します	読み取り	knowledge-base*		
GetMarketplaceModelEndpoint	マーケットプレイスモデルエンドポイントのプロパティを取得する許可を付与	読み取り	bedrock-marketplace-model-endpoint*		
GetModelCopyJob	モデルコピージョブに関連付けられたプロパティを取得するための許可を付与します。このオペレーションを使用して、モデルコピージョブのステータスを取得する	読み取り	model-copy-job*		
GetModelCustomizationJob	モデルカスタマイズジョブに関連付けられたプロパティを取得するための許可を付与します。このオペレーションを使用して、モデルカスタマイズジョブのステータスを取得します	読み取り	model-customization-job*		
GetModelEvaluationJob	モデル評価ジョブに関連付けられたプロパティを取得するためのアクセス許可を付与 このオペレーションを使用して、モデル評価ジョブのステータスを取得します	読み取り	model-evaluation-job*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetModelImportJob	モデルインポートジョブに関連付けられたプロパティを取得する許可を付与し、モデルインポートジョブのステータスを取得するために使用する	読み取り	model-import-job*		
GetModelInvocationJob	モデル呼び出しジョブを取得するためのアクセス許可を付与	読み取り	model-invocation-job*		
GetModelInvocationLoggingConfiguration	既存の呼び出しログ記録設定を取得するための許可を付与	読み取り			
GetPrompt	既存のプロンプトまたはそのバージョンを取得する許可を付与する	読み取り	prompt*		
			prompt-version*		
GetPromptRouter	プロンプトルーターに関連付けられたプロパティを取得するアクセス許可を付与します	読み取り	default-prompt-router*		
			prompt-router*		
GetProvisionedModelThroughput	プロビジョニングされたモデルスループットを取得する許可を付与	読み取り	provisioned-model*		
GetResourcePolicy [許可のみ]	Bedrock リソースのリソースポリシードキュメントを取得する	読み取り	custom-model*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetSession	既存のセッションを取得するアクセス許可を付与します	読み取り	session*		
GetUseCaseForModelAccess	モデルアクセスのユースケースを取得する許可を付与	読み取り			
IngestKnowledgeBaseDocuments	ドキュメントをナレッジベースに直接取り込むアクセス許可を付与します	書き込み	knowledge-base*		
InvokeAgent	ユーザー入力 (テキストのみ) を Bedrock のエージェントのエイリアスに送信する許可を付与	読み取り	agent-alias*		
InvokeAutomatedReasoningPolicy [許可のみ]	自動推論ポリシーを呼び出すアクセス許可を付与します	読み取り	automated-reasoning-policy*		
			automated-reasoning-policy-version*		
InvokeBlueprintRecommendationAsync [許可のみ]	ブループリントレコメンデーションを非同期的に呼び出すアクセス許可を付与します	書き込み	data-automation-profile*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
InvokeBuilder [アクセス許可のみ]	サポートされている Bedrock リソースの構築に役立つ会話ビルダーを使用する許可を付与する	書き込み			
InvokeDataAutomationAsync	Bedrock データ自動化ジョブを呼び出すアクセス許可を付与します	書き込み	blueprint*		
			data-automation-profile*		
			data-automation-project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
InvokeFlow	ユーザー入力でプロンプトフローを呼び出す許可を付与する	読み取り	flow-alias*		
InvokeInlineAgent	Bedrock のインラインエージェントにユーザー入力 (テキストのみ) を送信する許可を付与	読み取り		bedrock:InlineAgentName	
InvokeModel	リクエスト本文で提供された入力を使用して推論を実行するために、指定された Bedrock モデルを呼び出すための許可を付与します	読み取り	application-inference-profile*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			async-invoke*		
			bedrock-marketplace-model-endpoint*		
			custom-model-deployment*		
			default-prompt-router*		
			foundation-model*		
			imported-model*		
			inference-profile*		
			prompt-router*		
			provisioned-model*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				bedrock:InferenceProfileArn bedrock:PromptRouterArn aws:RequestTag/${TagKey} aws:TagKeys bedrock:GuardrailIdentifier	
InvokeModelWithResponseStream	ストリーミングレスポンスとともにリクエスト本文で提供された入力を使用して推論を実行するために、指定された Bedrock モデルを呼び出すための許可を付与します	読み取り	application-inference-profile*		
			bedrock-marketplace-model-endpoint*		
			custom-model-deployment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			default-prompt-router*		
			foundation-model*		
			imported-model*		
			inference-profile*		
			prompt-router*		
			provisioned-model*		
				bedrock:InferenceProfileArn bedrock:PromptRouterArn bedrock:GuardrailIdentifier	
ListAgentActionGroups	エージェント内のアクショングループを一覧表示する許可を付与	リスト	agent*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListAgentAliases	エージェントのエイリアスを一覧表示する許可を付与	リスト	agent*		
ListAgentCollaborators	エージェントの共同作業者を一覧表示するアクセス許可を付与します	リスト	agent*		
ListAgentKnowledgeBases	エージェントに関連付けられたナレッジベースを一覧表示する許可を付与	リスト	agent*		
ListAgentVersions	エージェントの既存のバージョンを一覧表示する許可を付与	リスト	agent*		
ListAgents	既存のエージェントを一覧表示する許可を付与	リスト			
ListAsyncInvokes	送信した非同期呼び出しのリストを取得するアクセス許可を付与します	リスト			
ListAutomatedReasoningPolicies	自動推論ポリシーまたはそのバージョンを一覧表示する許可を付与	リスト	automated-reasoning-policy		
ListAutomatedReasoningPolicyBuildWorkflows	自動推論ポリシーのビルドワークフローを一覧表示する許可を付与	リスト	automated-reasoning-policy*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListAutomatedReasoningPolicyTestCases	自動推論ポリシーのテストケースを一覧表示する許可を付与	リスト	automated-reasoning-policy*		
ListAutomatedReasoningPolicyTestResults	自動推論ポリシーのテスト結果を一覧表示する許可を付与	リスト	automated-reasoning-policy*		
ListBlueprints	データ自動化の既存のブループリントを一覧表示する許可を付与	リスト	data-automation-project		
ListCustomModelDeployments	送信したカスタムモデルデプロイのリストを取得するアクセス許可を付与します	リスト			
ListCustomModels	作成した Bedrock カスタムモデルのリストを取得するための許可を付与します	リスト			
ListDataAutomationProjects	既存のデータ自動化プロジェクトを一覧表示する許可を付与	リスト	blueprint		
ListDataSources	ナレッジベース内の既存のデータソースを一覧表示する許可を付与	リスト	knowledge-base*		
ListEvaluationJobs	送信した評価ジョブのリストを取得する許可を付与する	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListFlowAliases	プロンプトフローの既存のエイリアスを一覧表示する許可を付与する	リスト	flow*		
ListFlowExecutionEvents	フロー実行のイベントを取得するアクセス許可を付与します	リスト	flow*		
			flow-alias*		
			flow-execution*		
ListFlowExecutions	フローまたはフローエイリアスの実行を一覧表示する許可を付与	リスト	flow*		
			flow-alias		
ListFlowVersions	プロンプトフローの既存のバージョンを一覧表示する許可を付与する	リスト	flow*		
ListFlows	既存のプロンプトフローを一覧表示する許可を付与する	リスト			
ListFoundationModelAgreementOffers	基盤モデル契約のオファーのリストを取得する許可を付与	リスト			
ListFoundationModels	使用できる Bedrock の基盤モデルを一覧表示するための許可を付与します	リスト			
ListGuardrails	ガードレールまたはそのバージョンを一覧表示するためのアクセス許可を付与	リスト	guardrail		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListImportedModels	Bedrock のインポート済みモデルのリストを取得する許可を付与する	リスト			
ListInferenceProfiles	使用できる推論プロファイルを一覧表示する許可を付与する	リスト			
ListIngestionJobs	データソース内の取り込みジョブを一覧表示する許可を付与	リスト	knowledge-base*		
ListInvocationSteps	セッションから呼び出しステップのリストを取得するアクセス許可を付与します	リスト	session*		
ListInvocations	セッション内の呼び出しを一覧表示するアクセス許可を付与します	リスト	session*		
ListKnowledgeBaseDocuments	ナレッジベースのドキュメントを一覧表示するアクセス許可を付与します	リスト	knowledge-base*		
ListKnowledgeBases	既存のナレッジベースを一覧表示する許可を付与	リスト			
ListMarketplaceModelEndpoints	使用できるマーケットプレイスモデルエンドポイントを一覧表示するアクセス許可を付与します	読み取り			
ListModelCopyJobs	送信したモデルコピージョブのリストを取得するための許可を付与する	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListModelCustomizationJobs	送信したモデルカスタマイズジョブのリストを取得するための許可を付与します	リスト			
ListModelEvaluationJobs	送信したモデル評価ジョブのリストを取得するためのアクセス許可を付与	リスト			
ListModelImportJobs	モデルインポートジョブのリストを取得する許可を付与する	リスト			
ListModelInvocationJobs	以前に作成したモデル呼び出しジョブを一覧表示するためのアクセス許可を付与	リスト			
ListPromptRouters	使用できるプロンプトルーターを一覧表示するアクセス許可を付与します	リスト			
ListPrompts	既存のプロンプトを一覧表示する許可を付与する	リスト	prompt		
ListProvisionedModelThroughputs	以前に作成したプロビジョニングされたモデルスループットを一覧表示する許可を付与	リスト			
ListSessions	既存のセッションを一覧表示するアクセス許可を付与します	リスト			
ListTagsForResource	Bedrock リソースのタグを一覧表示するための許可を付与します	読み取り	agent*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			agent-alias*		
			application-inference-profile*		
			async-invoke*		
			automated-reasoning-policy*		
			automated-reasoning-policy-version*		
			blueprint*		
			custom-model*		
			custom-model-deployment*		
			data-automation-invocation-job*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			data-automation-project*		
			evaluation-job*		
			flow*		
			flow-alias*		
			guardrail*		
			imported-model*		
			knowledge-base*		
			model-copy-job*		
			model-customization-job*		
			model-evaluation-job*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			model-import-job*		
			model-invocation-job*		
			prompt*		
			prompt-router*		
			prompt-version*		
			provisioned-model*		
			session*		
OptimizePrompt	ユーザー入力でプロンプトを最適化するアクセス許可を付与します	読み取り			
PrepareAgent	ランタイムリクエストを受信する既存のエージェントを準備するためのアクセス許可を付与	書き込み	agent*		
PrepareFlow	プロンプトフローに行われた最新の変更を適用して、実行時に反映する許可を付与する	書き込み	flow*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutFoundationModelEntitlement	基盤モデルにアクセスするための使用権限を付与する許可を付与	書き込み			
PutInvocationStep	呼び出しステップをセッションの呼び出しに配置するアクセス許可を付与します	書き込み	session*		
PutModelInvocationLoggingConfiguration	既存の呼び出しログ記録設定を作成する許可を付与	書き込み			
PutResourcePolicy [アクセス許可のみ]	Bedrock リソースのリソースポリシーを追加する	書き込み	custom-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutUseCaseForModelAccess	モデルアクセスのユースケースを提供する許可を付与	書き込み			
RegisterMarketplaceModelEndpoint	Sagemaker エンドポイントをマーケットプレイスモデルエンドポイントとして登録する許可を付与	書き込み	bedrock-marketplace-model-endpoint*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RenderPrompt [アクセス許可のみ]	既存のプロンプトまたはそのバージョンをレンダリングするアクセス許可を付与します	読み取り	prompt*		
			prompt-version*		
Rerank	ユーザー入力に基づいてドキュメントをランク付けするアクセス許可を付与します	書き込み			
Retrieve	ナレッジベースから取り込まれたデータを取得するためのアクセス許可を付与	読み取り	knowledge-base*		
RetrieveAndGenerate	ユーザー入力を送信して取得と生成を実行するためのアクセス許可を付与	書き込み			
StartAutomatedReasoningPolicyBuildWorkflow	自動推論ポリシーのビルドワークフローを開始する許可を付与	書き込み	automated-reasoning-policy*		
StartAutomatedReasoningPolicyTestWorkflow	自動推論ポリシーのテストワークフローを開始する許可を付与	書き込み	automated-reasoning-policy*		
StartFlowExecution	フローエイリアスの実行を開始する許可を付与	書き込み	flow*		
			flow-alias*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartIngestionJob	取り込みジョブを開始する許可を付与	書き込み	knowledge-base*		
StopEvaluationJob	進行中の評価ジョブを停止する許可を付与する	書き込み	evaluation-job*		
StopFlowExecution	フローエイリアスの実行を停止するアクセス許可を付与します	書き込み	flow*		
			flow-alias*		
			flow-execution*		
StopIngestionJob	取り込みジョブを停止する許可を付与する	書き込み	knowledge-base*		
StopModelCustomizationJob	進行中の Bedrock モデルカスタマイズジョブを停止するための許可を付与します	書き込み	model-customization-job*		
StopModelInvocationJob	以前に開始したモデル呼び出しジョブを停止するためのアクセス許可を付与	書き込み	model-invocation-job*		
TagResource	Bedrock リソースをタグ付けするための許可を付与します	Tagging	agent		
			agent-alias		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			application-inference-profile		
			async-invoke		
			automated-reasoning-policy		
			automated-reasoning-policy-version		
			blueprint		
			custom-model		
			custom-model-deployment		
			data-automation-invocation-job		
			data-automation-project		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			evaluation-job		
			flow		
			flow-alias		
			guardrail		
			imported-model		
			knowledge-base		
			model-copy-job		
			model-customization-job		
			model-evaluation-job		
			model-import-job		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			model-invocation-job		
			prompt		
			prompt-router		
			prompt-version		
			provisioned-model		
			session		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Bedrock リソースのタグを解除するための許可を付与します	Tagging	agent		
			agent-alias		
			application-inference-profile		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			async-invoke		
			automated-reasoning-policy		
			automated-reasoning-policy-version		
			blueprint		
			custom-model		
			custom-model-deployment		
			data-automation-invocation-job		
			data-automation-project		
			evaluation-job		
			flow		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			flow-alias		
			guardrail		
			imported-model		
			knowledge-base		
			model-copy-job		
			model-customization-job		
			model-evaluation-job		
			model-import-job		
			model-invocation-job		
			prompt		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			prompt-router		
			prompt-version		
			provisioned-model		
			session		
				aws:TagKeys	
UpdateAgent	既存のエージェントを更新する許可を付与	書き込み	agent*		
UpdateAgentActionGroup	既存のアクショングループを更新する許可を付与	書き込み	agent*		
UpdateAgentAlias	既存のエイリアスを更新する許可を付与	書き込み	agent-alias*		
UpdateAgentCollaborator	既存の共同作業者を更新する許可を付与	書き込み	agent*		
UpdateAgentKnowledgeBase	エージェントに関連付けられたナレッジベースを更新する許可を付与	書き込み	agent*		
			knowledge-base*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateAutomatedReasoningPolicy	自動推論ポリシーを更新する許可を付与	書き込み	automated-reasoning-policy*		
UpdateAutomatedReasoningPolicyAnnotations	自動推論ポリシーのビルドワークフローの注釈を更新する許可を付与	書き込み	automated-reasoning-policy*		
UpdateAutomatedReasoningPolicyTestCase	自動推論ポリシーのテストケースを更新する許可を付与	書き込み	automated-reasoning-policy*		
UpdateBlueprint	データ自動化のブループリントを更新する許可を付与	書き込み	blueprint*		
UpdateDataAutomationProject	データ自動化プロジェクトを更新する許可を付与	書き込み	data-automation-project*		
			blueprint		
UpdateDataSource	データソースを更新する権限を付与	書き込み	knowledge-base*		
UpdateFlow	プロンプトフローを更新する許可を付与する	書き込み	flow*		
UpdateFlowAlias	プロンプトフローのエイリアスの設定を更新する許可を付与する	書き込み	flow-alias*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateGuardrail	ガードレールを更新するためのアクセス許可を付与	書き込み	guardrail*		
			automated-reasoning-policy		
			automated-reasoning-policy-version		
			guardrail-profile		
UpdateKnowledgeBase	ナレッジベースを更新する許可を付与	書き込み	knowledge-base*		
UpdateMarketplaceModelEndpoint	マーケットプレイスモデルエンドポイントを更新する許可を付与	書き込み	bedrock-marketplace-model-endpoint*		
UpdatePrompt	プロンプトを更新する許可を付与する	書き込み	prompt*		
UpdateProvisionedModelThroughput	以前に作成したプロビジョニングされたモデルスループットを更新する許可を付与	書き込み	custom-model*		
			foundation-model*		
			provisioned-model*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateSession	既存のセッションを更新するアクセス許可を付与します	書き込み	session*		
ValidateFlowDefinition	プロンプトフロー定義を検証するアクセス許可を付与します	読み取り			

Amazon Bedrock によって定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
foundation-model	arn:${Partition}:bedrock:${Region}::foundation-model/${ResourceId}	
async-invoke	arn:${Partition}:bedrock:${Region}:${Account}:async-invoke/${ResourceId}	aws:ResourceTag/${TagKey}
inference-profile	arn:${Partition}:bedrock:${Region}:${Account}:inference-profile/${ResourceId}	
default-prompt-router	arn:${Partition}:bedrock:${Region}:${Account}:default-prompt-router/${ResourceId}	

リソースタイプ	ARN	条件キー
prompt-router	arn:${Partition}:bedrock:${Region}:${Account}:prompt-router/${ResourceId}	
application-inference-profile	arn:${Partition}:bedrock:${Region}:${Account}:application-inference-profile/${ResourceId}	aws:ResourceTag/${TagKey}
custom-model	arn:${Partition}:bedrock:${Region}:${Account}:custom-model/${ResourceId}	aws:ResourceTag/${TagKey}
provisioned-model	arn:${Partition}:bedrock:${Region}:${Account}:provisioned-model/${ResourceId}	aws:ResourceTag/${TagKey}
model-customization-job	arn:${Partition}:bedrock:${Region}:${Account}:model-customization-job/${ResourceId}	aws:ResourceTag/${TagKey}
agent	arn:${Partition}:bedrock:${Region}:${Account}:agent/${AgentId}	aws:ResourceTag/${TagKey}
agent-alias	arn:${Partition}:bedrock:${Region}:${Account}:agent-alias/${AgentId}/${AgentAliasId}	aws:ResourceTag/${TagKey}
knowledge-base	arn:${Partition}:bedrock:${Region}:${Account}:knowledge-base/${KnowledgeBaseId}	aws:ResourceTag/${TagKey}
model-evaluation-job	arn:${Partition}:bedrock:${Region}:${Account}:model-evaluation-job/${ResourceId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
evaluation-job	arn:${Partition}:bedrock:${Region}:${Account}:evaluation-job/${ResourceId}	aws:ResourceTag/${TagKey}
model-invocation-job	arn:${Partition}:bedrock:${Region}:${Account}:model-invocation-job/${JobIdentifier}	aws:ResourceTag/${TagKey}
guardrail	arn:${Partition}:bedrock:${Region}:${Account}:guardrail/${GuardrailId}	aws:ResourceTag/${TagKey}
guardrail-profile	arn:${Partition}:bedrock:${Region}:${Account}:guardrail-profile/${ResourceId}	
automated-reasoning-policy	arn:${Partition}:bedrock:${Region}:${Account}:automated-reasoning-policy/${AutomatedReasoningPolicyId}	aws:ResourceTag/${TagKey}
automated-reasoning-policy-version	arn:${Partition}:bedrock:${Region}:${Account}:automated-reasoning-policy/${AutomatedReasoningPolicyId}:${AutomatedReasoningPolicyVersion}	aws:ResourceTag/${TagKey}
flow	arn:${Partition}:bedrock:${Region}:${Account}:flow/${FlowId}	aws:ResourceTag/${TagKey}
flow-alias	arn:${Partition}:bedrock:${Region}:${Account}:flow/${FlowId}/alias/${FlowAliasId}	aws:ResourceTag/${TagKey}
flow-execution	arn:${Partition}:bedrock:${Region}:${Account}:flow/${FlowId}/alias/${FlowAliasId}/execution/${FlowExecutionId}	

リソースタイプ	ARN	条件キー
model-copy-job	arn:${Partition}:bedrock:${Region}:${Account}:model-copy-job/${ResourceId}	aws:ResourceTag/${TagKey}
prompt	arn:${Partition}:bedrock:${Region}:${Account}:prompt/${PromptId}	aws:ResourceTag/${TagKey}
prompt-version	arn:${Partition}:bedrock:${Region}:${Account}:prompt/${PromptId}:${PromptVersion}	aws:ResourceTag/${TagKey}
model-import-job	arn:${Partition}:bedrock:${Region}:${Account}:model-import-job/${ResourceId}	aws:ResourceTag/${TagKey}
imported-model	arn:${Partition}:bedrock:${Region}:${Account}:imported-model/${ResourceId}	aws:ResourceTag/${TagKey}
bedrock-marketplace-model-endpoint	arn:${Partition}:bedrock:${Region}:${Account}:marketplace/model-endpoint/all-access	
data-automation-project	arn:${Partition}:bedrock:${Region}:${Account}:data-automation-project/${ProjectId}	aws:ResourceTag/${TagKey}
blueprint	arn:${Partition}:bedrock:${Region}:${Account}:blueprint/${BlueprintId}	aws:ResourceTag/${TagKey}
data-automation-invocation-job	arn:${Partition}:bedrock:${Region}:${Account}:data-automation-invocation/${JobId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
data-automation-profile	arn:${Partition}:bedrock:${Region}:${Account}:data-automation-profile/${ProfileId}	
session	arn:${Partition}:bedrock:${Region}:${Account}:session/${SessionId}	aws:ResourceTag/${TagKey}
custom-model-deployment	arn:${Partition}:bedrock:${Region}:${Account}:custom-model/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon Bedrock の条件キー

Amazon Bedrock では、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	必須の各タグで許可されている値のセットに基づく作成リクエストでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値に基づくアクションの有無でアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内の必須のタグの存在に基づく作成リクエストでアクセスをフィルタリングします	ArrayOfString
bedrock:GuardrailIdentifier	GuardrailArn または GuardrailArn:NumericVersion を含む GuardrailIdentifier でアクセスをフィルタリングします GuardrailArn GuardrailArn NumericVersion	ARN

条件キー	説明	[Type] (タイプ)
bedrock:InferenceProfileArn	指定された推論プロファイルによってアクセスをフィルタリングする	ARN
bedrock:InlineAgentName	インラインエージェント名でアクセスをフィルタリングします。これは InvokeInlineAgent API 名で使用されます。	String
bedrock:PromptRouterArn	指定されたプロンプトルーターでアクセスをフィルタリングします	ARN
bedrock:ThirdPartyKnowledgeBaseCredentialsSecretArn	サードパーティのプラットフォームの認証情報を含む secretArn でアクセスをフィルタリングします	ARN

Amazon Bedrock Agentcore のアクション、リソース、および条件キー

Amazon Bedrock Agentcore (サービスプレフィックス: `bedrock-agentcore`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Bedrock Agentcore で定義されるアクション
- Amazon Bedrock Agentcore で定義されるリソースタイプ
- Amazon Bedrock Agentcore の条件キー

Amazon Bedrock Agentcore で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AllowVendedLogDeliveryForResource [アクセス許可のみ]	リソースに提供されたテレメトリを設定するアクセス許可を付与します	権限の管理	memory*		
ConnectBrowserAutomationStream	ブラウザ自動化ストリームに接続するアクセス許可を付与します	読み取り			
ConnectBrowserLiveViewStream	ブラウザのライブビューストリームに接続する許可を付与	読み取り			
CreateAgentRuntime	新しいエージェントランタイムを作成するアクセス許可を付与します	書き込み			iam:PassRole
CreateAgentRuntimeEndpoint	新しいエージェントランタイムエンドポイントを作成するアクセス許可を付与します	書き込み			
CreateApiKeyCredentialProvider	新しい API キー認証情報プロバイダーを作成するアクセス許可を付与します	書き込み	apikeycredentialprovider*		
			token-vault*		
CreateBrowser	新しいカスタムブラウザを作成するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateCodeInterpreter	新しいカスタムコードインタプリタを作成するアクセス許可を付与します	書き込み			
CreateEvent	イベントを作成するアクセス許可を付与します	書き込み	memory*		
				bedrock-agentcore:sessionId bedrock-agentcore:actorId	
CreateGateway	新しいゲートウェイを作成するアクセス許可を付与します	書き込み			iam:PassRole
CreateGatewayTarget	既存のゲートウェイに新しいターゲットを作成するアクセス許可を付与します	書き込み	gateway*		
CreateMemory	メモリリソースを作成するアクセス許可を付与します	書き込み			iam:PassRole
CreateOauth2CredentialProvider	OAuth2 プロトコルを使用して外部リソースにアクセスするための新しい認証情報プロバイダーを作成するアクセス許可を付与します	書き込み	oauth2credentialprovider*		
			token-vault*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateWorkloadIdentity	新しいワークロード ID を作成するアクセス許可を付与します	書き込み	workload-identity*		
			workload-identity-directory*		
DeleteAgentRuntime	エージェントランタイムを削除するアクセス許可を付与します	書き込み	runtime*		
DeleteAgentRuntimeEndpoint	エージェントランタイムエンドポイントを削除するアクセス許可を付与します	書き込み	runtime*		
			runtime-endpoint*		
DeleteApiKeyCredentialProvider	登録された API キー認証情報プロバイダーを削除するアクセス許可を付与します	書き込み	apikeycredentialprovider*		
			token-vault*		
DeleteBrowser	カスタムブラウザを削除するアクセス許可を付与します	書き込み	browser-custom*		
DeleteCodeInterpreter	カスタムコードインタプリタを削除するアクセス許可を付与します	書き込み	code-interpreter-custom*		
DeleteEvent	イベントを削除するアクセス許可を付与します	書き込み	memory*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				bedrock-agentcore:sessionId bedrock-agentcore:actorId	
DeleteGateway	既存のゲートウェイを削除するアクセス許可を付与します	書き込み	gateway*		
DeleteGatewayTarget	既存のゲートウェイターゲットを削除するアクセス許可を付与します	書き込み	gateway*		
DeleteMemory	メモリリソースを削除するアクセス許可を付与します	書き込み	memory*		
DeleteMemoryRecord	メモリレコードを削除するアクセス許可を付与します	書き込み	memory*		
DeleteOauth2CredentialProvider	登録された OAuth2 認証情報プロバイダーを削除するアクセス許可を付与します	書き込み	oauth2credentialprovider*		
			token-vault*		
DeleteWorkloadIdentity	登録されたワークロード ID を削除するアクセス許可を付与します	書き込み	workload-identity*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			workload-identity-directory*		
GetAgentRuntime	エージェントランタイムの詳細を取得するアクセス許可を付与します	読み取り	runtime*		
GetAgentRuntimeEndpoint	エージェントランタイムエンドポイントの詳細を取得するアクセス許可を付与します	読み取り	runtime*		
			runtime-endpoint*		
GetApiKeyCredentialProvider	登録された API キー認証情報プロバイダーを名前で取得するアクセス許可を付与します	読み取り	apikeycredentialprovider*		
			token-vault*		
GetBrowser	ブラウザの詳細を取得するアクセス許可を付与します	読み取り	browser-custom*		
GetBrowserSession	ブラウザセッションの詳細を取得するアクセス許可を付与します	読み取り	browser*		
			browser-custom*		
GetCodeInterpreter	コードインタープリタの詳細を取得するアクセス許可を付与します	読み取り	code-interpreter-custom*		
GetCodeInterpreterSession	コードインタープリタセッションの詳細を取得するアクセス許可を付与します	読み取り	code-interpreter*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			code-interpreter-custom*		
GetEvent	イベントを取得するアクセス許可を付与します	読み取り	memory*		
				bedrock-agentcore:sessionId bedrock-agentcore:actorId	
GetGateway	既存のゲートウェイを取得するアクセス許可を付与します	読み取り	gateway*		
GetGatewayTarget	既存のゲートウェイターゲットを取得するアクセス許可を付与します	読み取り	gateway*		
GetMemory	メモリリソースの詳細を取得するアクセス許可を付与します	読み取り	memory*		
GetMemoryRecord	メモリレコードを取得するアクセス許可を付与します	読み取り	memory*		
GetOauth2CredentialProvider	登録された OAuth2 認証情報プロバイダーを名前で取得するアクセス許可を付与します	読み取り	oauth2credentialprovider*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			token-vault*		
GetResourceApiKey	Api キー認証情報プロバイダーに関連付けられた API キーを取得するアクセス許可を付与します	読み取り	apikeycredentialprovider*		
			token-vault*		
			workload-identity*		
			workload-identity-directory*		
GetResourceOauth2Token	OAuth2 2LO または 3LO フローでアクセストークンを取得して外部リソースにアクセスする許可を付与	読み取り	oauth2credentialprovider*		
			token-vault*		
			workload-identity*		
			workload-identity-directory*		
GetTokenVault	暗号化設定を含む TokenVault の現在の設定を取得する許可を付与	読み取り	token-vault*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetWorkloadAccessToken	ユーザーに代わって動作しないエージェントワークロードのワークロードアクセストークンを取得する許可を付与	書き込み	workload-identity*		
			workload-identity-directory*		
GetWorkloadAccessTokenForJWT	JWT トークンを持つユーザーに代わって動作するエージェントワークロードのワークロードアクセストークンを取得する許可を付与	書き込み	workload-identity*		
			workload-identity-directory*		
GetWorkloadAccessTokenForUserId	ユーザー ID を持つユーザーに代わって動作するエージェントワークロードのワークロードアクセストークンを取得する許可を付与	書き込み	workload-identity*		
			workload-identity-directory*		
GetWorkloadIdentity	名前や許可された OAuth2 リターン URLs	読み取り	workload-identity*		
			workload-identity-directory*		
InvokeAgentRuntime	エージェントランタイムエンドポイントを呼び出すアクセス許可を付与します	書き込み	runtime*		
			runtime-endpoint*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
InvokeCodeInterpreter	コードインタープリタセッションを呼び出すアクセス許可を付与します	書き込み	code-interpreter*		
			code-interpreter-custom*		
ListActors	アクターを一覧表示するアクセス許可を付与します	リスト	memory*		
ListAgentRuntimeEndpoints	エージェントランタイムエンドポイントを一覧表示するアクセス許可を付与します	リスト			
ListAgentRuntimeVersions	エージェントランタイムバージョンを一覧表示するアクセス許可を付与します	リスト			
ListAgentRuntimes	エージェントランタイムを一覧表示するアクセス許可を付与します	リスト			
ListApiKeyCredentialProviders	トークンボールト内のすべての API キー認証情報プロバイダーを一覧表示するアクセス許可を付与します	読み取り	apikeycredentialprovider*		
			token-vault*		
ListBrowserSessions	ブラウザセッションを一覧表示する許可を付与	リスト			
ListBrowsers	ブラウザを一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListCodeInterpreterSessions	コードインタープリタセッションを一覧表示する許可を付与	リスト	code-interpreter*		
			code-interpreter-custom*		
ListCodeInterpreters	コードインタプリタを一覧表示するアクセス許可を付与します	リスト			
ListEvents	イベントを一覧表示するアクセス許可を付与します	リスト	memory*		
				bedrock-agentcore:sessionId bedrock-agentcore:actorId	
ListGatewayTargets	既存のゲートウェイターゲットを一覧表示するアクセス許可を付与します	リスト	gateway*		
ListGateways	既存のゲートウェイを一覧表示するアクセス許可を付与します	リスト			
ListMemories	メモリリソースを一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListMemoryRecords	メモリレコードを一覧表示するアクセス許可を付与します	リスト	memory*		
				bedrock-agentcore:namespace	
				bedrock-agentcore:strategyId	
ListOauth2CredentialProviders	トークンボールト内のすべての OAuth2 認証情報プロバイダーを一覧表示するアクセス許可を付与します	読み取り	oauth2credentialprovider*		
			token-vault*		
ListSessions	セッションを一覧表示するアクセス許可を付与します	リスト	memory*		
				bedrock-agentcore:actorId	
ListWorkloadIdentities	発信者のすべてのワークロード ID を一覧表示するアクセス許可を付与します AWS アカウント	読み取り	workload-identity*		
			workload-identity-directory*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RetrieveMemoryRecords	セマティッククエリを介してメモリレコードを取得するアクセス許可を付与します	リスト	memory*		
				bedrock-agentcore:namespace bedrock-agentcore:strategyId	
SetTokenVaultCMK	カスタマーマネージドキー (CMK) またはサービスマネージドキーを特定の TokenVault に関連付けるアクセス許可を付与します	読み取り	token-vault*		
StartBrowserSession	新しいブラウザセッションを開始するアクセス許可を付与します	書き込み	browser*		
			browser-custom*		
StartCodeInterpreterSession	新しいコードインタプリタセッションを開始するアクセス許可を付与します	書き込み	code-interpreter*		
			code-interpreter-custom*		
StopBrowserSession	ブラウザセッションを停止するアクセス許可を付与します	書き込み	browser*		
			browser-custom*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StopCodeInterpreterSession	コードインタープリタセッションを停止するアクセス許可を付与します	書き込み	code-interpreter*		
			code-interpreter-custom*		
SynchronizeGatewayTargets [アクセス許可のみ]	ゲートウェイで検索を有効にするアクセス許可を付与します	権限の管理	gateway*		
UpdateAgentRuntime	エージェントランタイムを更新するアクセス許可を付与します	書き込み	runtime*		iam:PassRole
UpdateAgentRuntimeEndpoint	エージェントランタイムエンドポイントを更新するアクセス許可を付与します	書き込み	runtime*		
			runtime-endpoint*		
UpdateApiKeyCredentialProvider	既存の API キー認証情報プロバイダーを更新する許可を付与	書き込み	apikeycredentialprovider*		
			token-vault*		
UpdateBrowserStream	ブラウザセッションストリームのステータスを更新するアクセス許可を付与します	書き込み	browser*		
			browser-custom*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateGateway	既存のゲートウェイを更新するアクセス許可を付与します	書き込み	gateway*		iam:PassRole
UpdateGatewayTarget	既存のゲートウェイターゲットを更新するアクセス許可を付与します	書き込み	gateway*		
UpdateMemory	メモリリソースを更新するアクセス許可を付与します	書き込み	memory*		iam:PassRole
UpdateOauth2CredentialProvider	既存の OAuth2 認証情報プロバイダーを更新する許可を付与	書き込み	oauth2credentialprovider*		
			token-vault*		
UpdateWorkloadIdentity	既存のワークロード ID のメタデータを更新する許可を付与	書き込み	workload-identity*		
			workload-identity-directory*		

Amazon Bedrock Agentcore で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
memory	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:memory/${MemoryId}	
gateway	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:gateway/${GatewayId}	
workload-identity	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:workload-identity-directory/${DirectoryId}/workload-identity/${WorkloadIdentityName}	
oauth2credentialprovider	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:token-vault/${TokenVaultId}/oauth2credentialprovider/${Name}	
apikeycredentialprovider	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:token-vault/${TokenVaultId}/apikeycredentialprovider/${Name}	
runtime	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:runtime/${RuntimeId}	
runtime-endpoint	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:runtime/${RuntimeId}/runtime-endpoint/${Name}	
code-interpreter-custom	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:code-interpreter-custom/${CodeInterpreterId}	

リソースタイプ	ARN	条件キー
code-interpreter	arn:${Partition}:bedrock-agentcore:${Region}:aws:code-interpreter/${CodeInterpreterId}	
browser-custom	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:browser-custom/${BrowserId}	
browser	arn:${Partition}:bedrock-agentcore:${Region}:aws:browser/${BrowserId}	
workload-identity-directory	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:workload-identity-directory/${DirectoryId}	
token-vault	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:token-vault/${TokenVaultId}	

Amazon Bedrock Agentcore の条件キー

Amazon Bedrock エージェントコアは、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
bedrock-agentcore:actorId	アクター ID でアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
bedrock-agentcore:namespace	名前空間でアクセスをフィルタリングします	String
bedrock-agentcore:sessionId	セッション ID でアクセスをフィルタリングします	String
bedrock-agentcore:strategyId	メモリ戦略 ID でアクセスをフィルタリングします	String

AWS Billingのアクション、リソース、および条件キー

AWS Billing (サービスプレフィックス: billing) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Billingで定義されるアクション
- AWS Billingで定義されるリソースタイプ
- AWS Billingの条件キー

AWS Billingで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateBillingView	請求ビューを作成するアクセス許可を付与します	書き込み	billingview*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBillingView	請求ビューを削除するアクセス許可を付与します	書き込み	billingview*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy [アクセス許可のみ]	請求ビューリソースポリシーを削除するアクセス許可を付与します	権限の管理	billingview*		
				aws:ResourceTag/${TagKey}	
GetBillingData [許可のみ]	請求情報に関するクエリを実行するアクセス許可を付与	読み取り			
GetBillingDetails [許可のみ]	詳細な項目の請求情報を表示するアクセス許可を付与	読み取り			
GetBillingNotifications [許可のみ]	アカウント請求情報 AWS に関連して によって送信された	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	通知を表示するアクセス許可を付与します				
GetBillingPreferences [許可のみ]	リザーブドインスタンス、Savings Plans、クレジット共有などの請求設定を表示するアクセス許可を付与	読み取り			
GetBillingView	指定された請求ビューのメタデータを取得する許可を付与	読み取り	billingview*		
				aws:ResourceTag/${TagKey}	
GetBillingViewData [許可のみ]	指定された請求ビューのコストと使用状況データを取得する許可を付与	読み取り	billingview*		
GetContractInformation [許可のみ]	契約番号、エンドユーザーの組織名、PO 番号、アカウントが公共機関の顧客へのサービスに使用されているかどうかなど、アカウントの契約情報を表示するアクセス許可を付与	読み取り			
GetCredits [許可のみ]	引き換えられたクレジットを表示するアクセス許可を付与	読み取り			
GetIAMAccessPreference [許可のみ]	請求設定の「IAM アクセス許可を付与する」状態を取得するアクセス許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetResourcePolicy	リソースポリシーで指定された請求ビューを取得する許可を付与	権限の管理	billingview*		
				aws:ResourceTag/${TagKey}	
GetSellerOfRecord [許可のみ]	アカウントのデフォルトの登録販売者を取得するアクセス許可を付与	読み取り			
ListBillingViews	利用可能なすべての請求ビューのリストを取得するアクセス許可を付与します	読み取り			
ListSourceViewsForBillingView	指定された請求ビューのソースビューのリストを取得するアクセス許可を付与します	リスト	billingview*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	指定された請求ビューのタグのリストを取得するアクセス許可を付与します	読み取り	billingview*		
				aws:ResourceTag/${TagKey}	
PutContractInformation [許可のみ]	アカウントの契約情報、エンドユーザーの組織名、およびアカウントが公共部門の顧客にサービスを提供するために使用されるかどうかを設定するアクセス許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutResourcePolicy [アクセス許可のみ]	請求ビューリソースポリシーを配置するアクセス許可を付与します	権限の管理	billingview*		
				aws:ResourceTag/${TagKey}	
RedeemCredits [許可のみ]	AWS クレジットを引き換える許可を付与	書き込み			
TagResource	指定された請求ビューにタグを追加するアクセス許可を付与します	Tagging	billingview*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	指定された請求ビューからタグを削除するアクセス許可を付与します	Tagging	billingview*		
				aws:TagKeys aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateBillingPreferences [アクセス許可のみ]	リザーブドインスタンス、Savings Plans、クレジット共有などの請求設定を更新するアクセス許可を付与	書き込み			
UpdateBillingView	請求ビューを更新するアクセス許可を付与します	書き込み	billingview*		
				aws:ResourceTag/${TagKey}	
UpdateIAMAccessPreference [アクセス許可のみ]	請求設定の「IAM アクセス許可を付与する」状態を更新するアクセス許可を付与	書き込み			

AWS Billingで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
billingview	`arn:${Partition}:billing::${Account}:billingview/${ResourceId}`	aws:ResourceTag/${TagKey}

AWS Billingの条件キー

AWS Billing は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

および コスト管理ダッシュボードのアクション、リソース AWS Billing 、および条件キー

AWS Billing および コスト管理ダッシュボード (サービスプレフィックス: bcm-dashboards) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Billing および コスト管理ダッシュボードで定義されるアクション

- AWS Billing および コスト管理ダッシュボードで定義されるリソースタイプ
- AWS Billing および コスト管理ダッシュボードの条件キー

AWS Billing および コスト管理ダッシュボードで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateDashboard	ダッシュボードを作成するアクセス許可を付与します	書き込み			
DeleteDashboard	ダッシュボードを削除する許可を付与	書き込み			
GetDashboard	ダッシュボード情報を取得する許可を付与	読み取り			
GetResourcePolicy	ダッシュボードのリソースポリシーを取得する許可を付与	読み取り			
ListDashboards	ユーザーのすべてのダッシュボードに関する情報を一覧表示するアクセス許可を付与します	読み取り			
ListTagsForResource	リソースのすべてのタグを一覧表示するアクセス許可を付与します	読み取り			
TagResource	リソースのタグを作成するアクセス許可を付与します	書き込み			
UntagResource	リソースのタグを削除するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateDashboard	既存のダッシュボードを更新するアクセス許可を付与します	書き込み			

AWS Billing および コスト管理ダッシュボードで定義されるリソースタイプ

AWS Billing および コスト管理ダッシュボードでは、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定はサポートされていません。 AWS Billing および コスト管理ダッシュボードへのアクセスを許可するには、ポリシー`"Resource": "*"`で を指定します。

AWS Billing および コスト管理ダッシュボードの条件キー

Billing and Cost Management Dashboards には、ポリシーステートメントの `Condition`要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Billing And Cost Management データエクスポートのアクション、リソース、および条件キー

AWS Billing また、コスト管理データのエクスポート (サービスプレフィックス: `bcm-data-exports`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Billing And Cost Management データエクスポートで定義されるアクション
- AWS Billing And Cost Management データエクスポートで定義されるリソースタイプ
- AWS Billing And Cost Management データエクスポートの条件キー

AWS Billing And Cost Management データエクスポートで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateExport	エクスポートを作成するためのアクセス許可を付与	書き込み	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteExport	エクスポートを削除するためのアクセス許可を付与	書き込み	export*		
				aws:ResourceTag/${TagKey}	
GetExecution	エクスポートの実行を取得するためのアクセス許可を付与	読み取り	export*		
				aws:ResourceTag/${TagKey}	
GetExport	エクスポートを取得するためのアクセス許可を付与	読み取り	export*		
				aws:ResourceTag/${TagKey}	
GetTable	テーブルの詳細を取得するためのアクセス許可を付与	読み取り	table*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListExecutions	エクスポートのすべての実行を一覧表示するためのアクセス許可を付与	リスト	export*		
				aws:ResourceTag/${TagKey}	
ListExports	すべてのエクスポートを一覧表示するためのアクセス許可を付与	リスト			
ListTables	利用可能なすべてのテーブルを一覧表示するためのアクセス許可を付与	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	export*		
				aws:ResourceTag/${TagKey}	
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	export*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	リソースのタグを解除する許可を付与	Tagging	export*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateExport	エクスポートを更新するためのアクセス許可を付与	書き込み	export*		
			table*		
				aws:ResourceTag/${TagKey}	

AWS Billing And Cost Management データエクスポートで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
export	arn:${Partition}:bcm-data-exports:${Region}:${Account}:export/${Identifier}	aws:ResourceTag/${TagKey}
table	arn:${Partition}:bcm-data-exports:${Region}:${Account}:table/${Identifier}	

AWS Billing And Cost Management データエクスポートの条件キー

AWS Billing また、コスト管理データエクスポートでは、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Billing And Cost Management 料金計算ツールのアクション、リソース、および条件キー

AWS Billing また、コスト管理料金計算ツール (サービスプレフィックス: bcm-pricing-calculator) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Billing And Cost Management 料金計算ツールで定義されるアクション
- AWS Billing And Cost Management 料金計算ツールで定義されるリソースタイプ
- AWS Billing And Cost Management 料金計算ツールの条件キー

AWS Billing And Cost Management 料金計算ツールで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateBillEstimate	新しい請求書見積りを作成するアクセス許可を付与します。請求見積りが成功すると料金が発生します	書き込み	bill-scenario		
CreateBillScenario	新しい請求シナリオを作成するアクセス許可を付与します	書き込み			
CreateBillScenarioCommitmentModification	指定された請求シナリオから新しいコミットメントを作成または既存のコミットメントを削除するアクセス許可を付与します	書き込み	bill-scenario*		
CreateBillScenarioUsageModification	指定された請求シナリオで使用量を作成するアクセス許可を付与します	書き込み	bill-scenario*		
CreateWorkloadEstimate	新しいワークロード見積りを作成するアクセス許可を付与します	書き込み			
CreateWorkloadEstimateUsage	指定されたワークロード見積もりで使用量を作成するアクセス許可を付与します	書き込み	workload-estimate*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteBillEstimate	請求書見積りを削除するアクセス許可を付与します	書き込み	bill-estimate*		
DeleteBillScenario	請求シナリオを削除するアクセス許可を付与します	書き込み	bill-scenario*		
DeleteBillScenarioCommitmentModification	指定された請求シナリオから新しく追加されたコミットメントを削除するアクセス許可を付与します	書き込み	bill-scenario*		
DeleteBillScenarioUsageModification	指定された請求シナリオから新しく追加された使用量を削除するアクセス許可を付与します	書き込み	bill-scenario*		
DeleteWorkloadEstimate	指定されたワークロード見積もりを削除するアクセス許可を付与します	書き込み	workload-estimate*		
DeleteWorkloadEstimateUsage	指定されたワークロード見積りから新しく追加された使用量を削除するアクセス許可を付与します	書き込み	workload-estimate*		
GetBillEstimate	推定コストを含む請求見積りの詳細を取得するアクセス許可を付与します	読み取り	bill-estimate*		
GetBillScenario	請求シナリオに関連付けられた情報を取得するアクセス許可を付与します	読み取り	bill-scenario*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetPreferences	アカウントに適用可能なレートタイプの設定を取得するアクセス許可を付与します	読み取り			
GetWorkloadEstimate	ワークロードの見積もりに関連する情報を取得するアクセス許可を付与します	読み取り	workload-estimate*		
ListBillEstimateCommitments	指定された請求見積りに関連付けられたコミットメントを一覧表示するアクセス許可を付与します	リスト	bill-estimate*		
ListBillEstimateInputCommitmentModifications	指定された請求見積りに対する追加または削除されたコミットメントを一覧表示するアクセス許可を付与します	リスト	bill-estimate*		
ListBillEstimateInputUsageModifications	指定された請求見積りの追加または変更された使用量を一覧表示するアクセス許可を付与します	リスト	bill-estimate*		
ListBillEstimateLineItems	指定された請求見積りの結果明細項目を一覧表示するアクセス許可を付与します	リスト	bill-estimate*		
ListBillEstimates	請求見積りを一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListBillScenarioCommitmentModifications	請求シナリオに含まれるコミットメントを一覧表示する許可を付与	リスト	bill-scenario*		
ListBillScenarioUsageModifications	指定された請求シナリオの使用行を一覧表示するアクセス許可を付与します	リスト	bill-scenario*		
ListBillScenarios	請求シナリオを一覧表示する許可を付与	リスト			
ListTagsForResource	リソースのタグのリストを返す許可を付与	Tagging			
ListWorkloadEstimateUsage	指定されたワークロード見積もりの使用行を一覧表示するアクセス許可を付与します	リスト	workload-estimate*		
ListWorkloadEstimates	ワークロードの見積もりを一覧表示するアクセス許可を付与します	リスト			
TagResource	リソースにタグを追加する許可を付与	タグ付け		aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	Tagging		aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateBillEstimate	請求書見積り名と有効期限日時を更新するアクセス許可を付与します	書き込み	bill-estimate*		
UpdateBillScenario	指定された請求シナリオの名前と有効期限日時を更新するアクセス許可を付与します	書き込み	bill-scenario*		
UpdateBillScenarioCommitmentModification	指定された請求シナリオでコミットメントのコミットメントグループを更新する許可を付与	書き込み	bill-scenario*		
UpdateBillScenarioUsageModification	指定された請求シナリオで使用量、使用時間、および使用グループを更新するアクセス許可を付与します	書き込み	bill-scenario*		
UpdatePreferences	アカウントのレートタイプの設定を更新するアクセス許可を付与します	書き込み			
UpdateWorkloadEstimate	指定されたワークロード見積もりの名前と有効期限日時を更新するアクセス許可を付与します	書き込み	workload-estimate*		
UpdateWorkloadEstimateUsage	使用量 ID に基づいて、指定されたワークロード見積もりの使用量と使用量グループを更新するアクセス許可を付与します	書き込み	workload-estimate*		

AWS Billing And Cost Management 料金計算ツールで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
bill-estimate	`arn:${Partition}:bcm-pricing-calculator:${Region}:${Account}:bill-estimate/${BillEstimateId}`	
bill-scenario	`arn:${Partition}:bcm-pricing-calculator:${Region}:${Account}:bill-scenario/${BillScenarioId}`	
workload-estimate	`arn:${Partition}:bcm-pricing-calculator:${Region}:${Account}:workload-estimate/${WorkloadEstimateId}`	

AWS Billing And Cost Management 料金計算ツールの条件キー

AWS Billing また、コスト管理料金計算ツールでは、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列

条件キー	説明	タイプ
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Billing And Cost Management の推奨アクションのアクション、リソース、および条件キー

AWS Billing また、コスト管理の推奨アクション (サービスプレフィックス: `bcm-recommended-actions`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Billing And Cost Management の推奨アクションで定義されるアクション
- AWS Billing And Cost Management の推奨アクションで定義されるリソースタイプ
- AWS Billing およびコスト管理の推奨アクションの条件キー

AWS Billing And Cost Management の推奨アクションで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーショ

ンへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListRecommendedActions	すべての推奨アクションを一覧表示するアクセス許可を付与します	リスト			

AWS Billing And Cost Management の推奨アクションで定義されるリソースタイプ

AWS Billing また、コスト管理の推奨アクションでは、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定はサポートされていません。 AWS Billing And Cost Management の推奨アクションへのアクセスを許可するには、ポリシー`"Resource": "*"`で を指定します。

AWS Billing およびコスト管理の推奨アクションの条件キー

BillingAndCostManagementRecommendedActions には、ポリシーステートメントの `Condition`要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Billing Conductorのアクション、リソース、および条件キー

AWS Billing Conductor （ サービスプレフィックス: `billingconductor`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Billing Conductorで定義されるアクション
- AWS Billing Conductorで定義されるリソースタイプ

- AWS Billing Conductorの条件キー

AWS Billing Conductorで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateAccounts	1 ~ 30 のアカウントを 1 つの請求グループに関連付ける許可を付与	書き込み	billinggroup*		
AssociatePricingRules	料金設定ルールを関連付ける許可を付与	書き込み	pricingplan*		
			pricingrule*		
BatchAssociateResourcesToCustomLineItem	リソースをパーセンテージカスタム明細項目にバッチで関連付ける許可を付与	書き込み	customlineitem*		
BatchDisassociateResourcesFromCustomLineItem	リソースをパーセンテージカスタム明細項目からバッチで関連付け解除する許可を付与	書き込み	customlineitem*		
CreateBillingGroup	請求グループを作成する許可を付与	書き込み	pricingplan*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateCustomLineItem	カスタム明細項目を作成する許可を付与	書き込み	billinggroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePricingPlan	料金設定プランを作成する許可を付与	書き込み	pricingrule*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePricingRule	料金設定ルールを作成する許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteBillingGroup	請求グループを削除する許可を付与	書き込み	billinggroup*		
DeleteCustomLineItem	カスタム明細項目を削除する許可を付与	書き込み	customlineitem*		
DeletePricingPlan	料金設定プランを削除する許可を付与	書き込み	pricingplan*		
DeletePricingRule	料金設定ルールを削除する許可を付与	書き込み	pricingrule*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DisassociateAccounts	1 ~ 30 のアカウントを請求グループからデタッチする許可を付与	書き込み	billinggroup*		
DisassociatePricingRules	料金設定ルールの関連付けを解除する許可を付与	書き込み	pricingplan*		
			pricingrule*		
GetBillingGroupCostReport	指定した請求グループのコストレポートを表示する許可を付与	読み取り	billinggroup*		
ListAccountAssociations	連結アカウントが属する請求グループを表示しながら特定の請求期間の支払人アカウントの連結アカウントを一覧表示する許可を付与	リスト			
ListBillingGroupCostReports	請求グループのコストレポートを表示する許可を付与	読み込み			
ListBillingGroups	請求グループの詳細を表示する許可を付与	読み取り			
ListCustomLineItemVersions	カスタム明細項目バージョンを表示する許可を付与	読み取り	customlineitem*		
ListCustomLineItems	カスタム明細項目を表示する許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListPricingPlans	料金プランの詳細を表示する許可を付与	読み込み			
ListPricingPlansAssociatedWithPricingRule	価格設定ルールに関連付けられた価格プランを一覧表示する許可を付与	リスト	pricingrule*		
ListPricingRules	料金ルールの詳細を表示する許可を付与	読み込み			
ListPricingRulesAssociatedToPricingPlan	価格設定プランに関連付けられた価格ルールを一覧表示する許可を付与	リスト	pricingplan*		
ListResourcesAssociatedToCustomLineItem	パーセンテージカスタム明細項目に関連付けられたリソースを一覧表示する許可を付与	リスト	customlineitem*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与。	読み込み	billinggroup		
			customlineitem		
			pricingplan		
			pricingrule		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	billinggroup		
			customlineitem		
			pricingplan		
			pricingrule		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	リソースのタグを解除する許可を付与	Tagging	billinggroup		
			customlineitem		
			pricingplan		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			pricingrule		
				aws:TagKeys	
UpdateBillingGroup	請求グループを更新する許可を付与	書き込み	billinggroup*		
UpdateCustomLineItem	カスタム明細項目を更新する許可を付与	書き込み	customlineitem*		
UpdatePricingPlan	料金設定プランを更新する許可を付与	書き込み	pricingplan*		
UpdatePricingRule	料金設定ルールを更新する許可を付与	書き込み	pricingrule*		

AWS Billing Conductorで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
billinggroup	arn:${Partition}:billingconductor::${Account}:billinggroup/${BillingGroupId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
pricingplan	arn:${Partition}:billingconductor::${Account}:pricingplan/${PricingPlanId}	aws:ResourceTag/${TagKey}
pricingrule	arn:${Partition}:billingconductor::${Account}:pricingrule/${PricingRuleId}	aws:ResourceTag/${TagKey}
customlineitem	arn:${Partition}:billingconductor::${Account}:customlineitem/${CustomLineItemId}	aws:ResourceTag/${TagKey}

AWS Billing Conductorの条件キー

AWS Billing Conductor は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Billing コンソールのアクション、リソース、および条件キー

AWS Billing コンソール (サービスプレフィックス: aws-portal) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Billing コンソールで定義されるアクション
- AWS Billing コンソールで定義されるリソースタイプ
- AWS Billing コンソールの条件キー

AWS Billing コンソールで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetConsoleActionSetEnforced [アクセス許可のみ]	Billing、Cost Management、および Account コンソールに対する承認を制御するために、既存またはきめ細かい IAM アクションを使用するかどうかを表示するための許可を付与します	読み取り			
ModifyAccount [許可のみ]	アカウント設定を変更するアクセス許可を IAM ユーザーに付与するか拒否します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ModifyBilling [アクセス許可のみ]	請求設定を変更するアクセス許可を IAM ユーザーに付与するか拒否します	書き込み			
ModifyPaymentMethods [アクセス許可のみ]	支払い方法を変更するアクセス許可を IAM ユーザーに付与するか拒否します	書き込み			
UpdateConsoleActionSetEnforced [アクセス許可のみ]	Billing、Cost Management、および Account コンソールに対する承認を制御するために、既存またはきめ細かい IAM アクションを使用するかどうかを変更するための許可を付与します	書き込み			
ViewAccount [アクセス許可のみ]	アカウント設定を表示するアクセス許可を IAM ユーザーに付与するか拒否します	読み取り			
ViewBilling [許可のみ]	コンソールの請求ページを表示するアクセス許可を IAM ユーザーに付与するか拒否します	読み取り			
ViewPaymentMethods [許可のみ]	支払い方法を表示するアクセス許可を IAM ユーザーに付与するか拒否します	読み取り			
ViewUsage [許可のみ]	AWS 使用状況レポートを表示するアクセス許可を IAM ユーザーに許可または拒否する	読み取り			

AWS Billing コンソールで定義されるリソースタイプ

AWS Billing コンソールは、IAM ポリシーステートメントの Resource要素でのリソース ARN の指定をサポートしていません。 AWS Billing コンソールへのアクセスを許可するには、ポリシーで "Resource": "*" を指定します。

AWS Billing コンソールの条件キー

請求コンソールには、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Braket のアクション、リソース、および条件キー

Amazon Braket (サービスプレフィックス: braket) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Braket で定義されるアクション
- Amazon Braket で定義されるリソースタイプ
- Amazon Braket の条件キー

Amazon Braket で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptUserAgreement	Amazon Braket ユーザー契約に同意するアクセス許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
[アクセス許可のみ]					
CancelJob	ジョブをキャンセルする許可を付与	書き込み	job*		
CancelQuantumTask	量子タスクをキャンセルする許可を付与。	書き込み	quantum-task*		
CreateJob	ジョブを作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateQuantumTask	量子タスクを作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
GetDevice	Amazon Braket で利用可能なデバイスに関する情報を取得する許可を付与。	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetJob	ジョブを取得する許可を付与。	読み取り	job*		
GetQuantumTask	量子タスクを取得する許可を付与。	読み取り	quantum-task*		
GetServiceLinkedRoleStatus [許可のみ]	Amazon Braket サービスにリンクされたロールが作成されているかどうかを確認するアクセス許可を付与	読み取り			
GetUserAgreementStatus [許可のみ]	アカウントが Amazon Braket ユーザー契約に同意したかどうかを確認するアクセス許可を付与	読み取り			
ListTagsForResource	量子タスクリソースまたはジョブに適用されているタグを一覧表示するアクセス許可を付与します	読み取り	job		
			quantum-task		
SearchDevices	Amazon Braket で利用可能なデバイスを検索する許可を付与。	読み取り			
SearchJobs	ルームを検索する許可を付与	読み取り			
SearchQuantumTasks	量子タスクを検索する許可を付与。	読み取り			
TagResource	量子タスクまたはハイブリッドジョブに 1 つ以上のタグを追加するアクセス許可を付与	Tagging	job		
			quantum-task		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースから 1 つ以上のタグを削除する許可を付与。タグは、キーと値のペアから構成されます。	タグ付け	job		
			quantum-task		
				aws:TagKeys	

Amazon Braket で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
quantum-task	arn:${Partition}:braket:${Region}:${Account}:quantum-task/${RandomId}	aws:ResourceTag/${TagKey}
job	arn:${Partition}:braket:${Region}:${Account}:job/${JobName}	aws:ResourceTag/${TagKey}

Amazon Braket の条件キー

Amazon Braket では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

AWS Budget Service のアクション、リソース、および条件キー

AWS Budget Service (サービスプレフィックス: budgets) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Budget Service で定義されるアクション
- AWS Budget Service で定義されるリソースタイプ

- AWS Budget Service の条件キー

AWS Budget Service で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

> **Note**
>
> このテーブルのアクションは APIs ではなく、予算にアクセスする AWS Billing and Cost Management APIs へのアクセスを許可するアクセス許可です。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateBudgetAction	予算が特定の予算しきい値を超えた場合に実行される応答を構成する許可を付与します。タグを使用して予算アクションを作成するには、「budgets:TagResource」の許可も必要です	書き込み	budgetAction*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteBudgetAction	特定の予算に関連付けられているアクションを削除する許可を付与	書き込み	budgetAction*		
DescribeBudgetAction	予算に関連付けられた特定の予算アクションの詳細を取得する許可を付与	読み取り	budgetAction*		
DescribeBudgetActionHistories	特定の予算アクションに関連付けられた予算アクションステータスの履歴ビューを取得するためのアクセス許可を付与します。これらのステー	読み取り	budgetAction*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	タスには、「スタンバイ」、「保留中」、「実行済み」などの像が含まれます				
DescribeBudgetActionsForAccount	アカウントに関連付けられているすべての予算アクションの詳細を取得する許可を付与	読み取り			
DescribeBudgetActionsForBudget	予算に関連付けられているすべての予算アクションの詳細を取得する許可を付与	読み取り	budget*		
ExecuteBudgetAction	保留中の予算アクションを開始し、以前に実行された予算アクションを取り消す許可を付与	書き込み	budgetAction*		
ListTagsForResource	予算または予算アクションのリソースタグを表示する許可を付与する	読み取り	budget		
			budgetAction		
ModifyBudget	予算を作成および変更し、予算の詳細を編集する許可を付与します。タグを使用して予算を作成するには、「budgets:TagResource」の許可も必要です	書き込み	budget*		iam:CreateServiceLinkedRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagResource	予算または予算アクションにリソースタグを適用する許可を付与します。タグを使用して予算または予算アクションを作成するのにも必要です	Tagging	budget		
			budgetAction		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	予算または予算アクションからリソースタグを削除する許可を付与する	Tagging	budget		
			budgetAction		
				aws:TagKeys	
UpdateBudgetAction	予算に関連付けられた特定の予算アクションの詳細を更新する許可を付与	書き込み	budgetAction*		iam:PassRole
ViewBudget	予算と予算の詳細を表示する許可を付与	読み取り	budget*		billing:GetBillingViewData

AWS Budget Service で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
budget	arn:${Partition}:budgets::${Account}:budget/${BudgetName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
budgetAction	arn:${Partition}:budgets::${Account}:budget/${BudgetName}/action/${ActionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

AWS Budget Service の条件キー

AWS Budget Service では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられているタグに基づいてアクションをフィルタリングします	文字列

条件キー	説明	タイプ
aws:TagKeys	リクエストで渡されたタグキーに基づいてアクションをフィルタリングします	ArrayOfString

AWS BugBust のアクション、リソース、条件キー

AWS BugBust (サービスプレフィックス: bugbust) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS BugBust で定義されるアクション
- AWS BugBust で定義されるリソースタイプ
- AWS BugBust の条件キー

AWS BugBust で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateEvent [アクセス許可のみ]	BugBust イベントを作成する許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
EvaluateProfilingGroups [アクセス許可のみ]	チェックインされたプロファイルグループを評価する許可を付与	書き込み	Event*		
				aws:ResourceTag/${TagKey}	
GetEvent [アクセス許可のみ]	イベントの顧客詳細を表示する許可を付与	読み込み	Event*		
				aws:ResourceTag/${TagKey}	
GetJoinEventStatus [許可のみ]	BugBust イベントに参加しようとする BugBust プレイヤーの状態を表示する許可を付与	読み込み	Event*		
				aws:ResourceTag/${TagKey}	
JoinEvent [許可のみ]	イベントに参加する許可を付与	書き込み	Event*		
				aws:ResourceTag/${TagKey}	
ListBugs [アクセス許可のみ]	イベントにインポートされたバグを表示するアクセス許可を付与し、プレイヤーが作業できるようにします。	読み込み	Event*		codeguru-reviewer:DescribeCodeReview codeguru-reviewer:ListRecommendations

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
ListEventParticipants [許可のみ]	イベントの参加者を表示する許可を付与	読み込み	Event*		
				aws:ResourceTag/${TagKey}	
ListEventScores [許可のみ]	イベントのプレイヤーのスコアを表示する許可を付与	読み込み	Event*		
				aws:ResourceTag/${TagKey}	
ListEvents [許可のみ]	BugBust イベントの一覧を表示する許可を付与	リスト		aws:ResourceTag/${TagKey}	
ListProfilingGroups [許可のみ]	イベントにインポートされたプロファイルグループを表示するアクセス許可を付与し、プレイヤーが操作できるようにします。	読み込み	Event*		
				aws:ResourceTag/${TagKey}	
ListPullRequests [許可のみ]	イベントでクレームされたバグに対する修正を送信するためにプレイヤーが使用するプルリクエストを表示する許可を付与	読み込み	Event*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource [許可のみ]	Bugbust リソースのタグを一覧表示する許可を付与	読み込み	Event*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
TagResource [許可のみ]	Bugbust リソースにタグ付けする許可を付与	タグ付け	Event*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [アクセス許可のみ]	Bugbust リソースのタグ付けを解除する許可を付与	タグ付け	Event*		
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateEvent [アクセス許可のみ]	BugBust イベントを更新するためのアクセス許可を付与	書き込み	Event*		codeguru-profiler:DescribeProfilingGroup codeguru-profiler:ListProfilingGroups codeguru-reviewer:DescribeCodeReview codeguru-reviewer:ListCodeReviews codeguru-reviewer:ListRecommendations codeguru-reviewer:TagResource

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					codeguru-reviewer:UnTagResource
				aws:ResourceTag/${TagKey}	
UpdateWorkItem [アクセス許可のみ]	クレーム済みまたはクレームされていない (バグまたはプロファイリンググループ) として作業項目を更新する許可を付与	書き込み	Event*		codeguru-reviewer:ListRecommendations
				aws:ResourceTag/${TagKey}	
UpdateWorkItemAdmin [アクセス許可のみ]	イベントの作業項目 (バグまたはプロファイリンググループ) を更新する許可を付与	書き込み	Event*		codeguru-reviewer:ListRecommendations
				aws:ResourceTag/${TagKey}	

AWS BugBust で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Event	arn:${Partition}:bugbust:${Region}:${Account}:events/${EventId}	aws:ResourceTag/${TagKey}

AWS BugBust の条件キー

AWS BugBust は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられているタグに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーに基づいてアクションをフィルタリングします	ArrayOfString

AWS Certificate Manager のアクション、リソース、および条件キー

AWS Certificate Manager (サービスプレフィックス: acm) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Certificate Manager で定義されるアクション
- AWS Certificate Manager で定義されるリソースタイプ
- AWS Certificate Manager の条件キー

AWS Certificate Manager で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddTagsToCertificate	証明書に 1 つ以上のタグを追加するアクセス権限を付与します	タグ付け	certificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCertificate	証明書と関連付けられた秘密キーを削除するアクセス権限を付与します	書き込み	certificate*		
DescribeCertificate	証明書とそのメタデータを取得するアクセス権限を付与します	読み取り	certificate*		
ExportCertificate	エクスポート可能な証明書をエクスポートしてどこでも使	読み取り	certificate*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	用するためのアクセス許可を付与します			acm:DomainNames	
GetAccountConfiguration	AWS Certificate Manager からアカウントレベルの設定を取得する許可を付与	読み取り			
GetCertificate	証明書 ARN の証明書と証明書チェーンを取得するアクセス権限を付与します	読み取り	certificate*		
ImportCertificate	サードパーティー証明書を AWS Certificate Manager (ACM) にインポートする許可を付与	書き込み	certificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListCertificates	証明書の ARN のリストと各 ARN のドメイン名を取得するアクセス権限を付与します	リスト			
ListTagsForCertificate	証明書に関連付けられているタグを一覧表示するアクセス権限を付与します	読み取り	certificate*		
PutAccountConfiguration	AWS Certificate Manager でアカウントレベルの設定を更新する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RemoveTagsFromCertificate	証明書から 1 つ以上のタグを削除するアクセス権限を付与します	タグ付け	certificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RenewCertificate	適格なプライベート証明書を更新するアクセス権限を付与します	書き込み	certificate*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RequestCertificate	パブリック証明書またはプライベート証明書をリクエストするアクセス権限を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys acm:DomainNames acm:CertificateTransparencyLogging acm:ValidationMethod acm:KeyAlgorithm acm:CertificateAuthority acm:Export	
ResendValidationEmail	ドメイン所有権の検証をリクエストするメールを再送信するアクセス権限を付与します	書き込み	certificate*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RevokeCertificate	エクスポート可能な証明書を取り消すアクセス許可を付与します	書き込み	certificate*		
				acm:DomainNames	
UpdateCertificateOptions	証明書の設定を更新するアクセス権限を付与します。証明書の透過性の記録をオプトインするかオプトアウトするかを指定するためにこれを使用します	書き込み	certificate*		

AWS Certificate Manager で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
certificate	`arn:${Partition}:acm:${Region}:${Account}:certificate/${CertificateId}`	aws:ResourceTag/${TagKey}

AWS Certificate Manager の条件キー

AWS Certificate Manager は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
acm:CertificateAuthority	リクエスト内の certificateAuthority でアクセスをフィルタリングします。証明書を発行できる認証機関を制限するために使用できます。	String
acm:CertificateTransparencyLogging	リクエスト内の certificateTransparencyLogging オプションでアクセスをフィルタリングします。リクエスト内にキーが存在しない場合はデフォルトは「ENABLED」です。	String
acm:DomainNames	リクエスト内の domainNames でアクセスをフィルタリングします。このキーを使用して、証明書リクエストに含めることができるドメインを制限できます。	ArrayOfString
acm:Export	リクエストのエクスポートオプションでアクセスをフィルタリングします。エクスポートできる証明書の作成を制限するために使用できます	String
acm:KeyAlgorithm	リクエスト内の keyAlgorithm でアクセスをフィルタリングします。	String
acm:ValidationMethod	リクエスト内の validationMethod でアクセスをフィルタリングします。リクエスト内にキーがない場合はデフォルトは「EMAIL」です。	String
aws:RequestTag/${TagKey}	リクエスト内のタグキーおよび値のペアのプレゼンスによってアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

AWS Chatbot のアクション、リソース、および条件キー

AWS Chatbot (サービスプレフィックス: chatbot) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Chatbot で定義されるアクション
- AWS Chatbot で定義されるリソースタイプ
- AWS Chatbot の条件キー

AWS Chatbot で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリス

ク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateToConfiguration	リソースを設定に関連付けるアクセス許可を付与します	書き込み	ChatbotConfiguration*		
			custom-action*		
				aws:ResourceTag/${TagKey}	
CreateChimeWebhookConfiguration	AWS Chatbot Chime ウェブフック設定を作成するアクセス許可を付与します	書き込み		aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey}	
CreateCustomAction	カスタムアクションを作成するアクセス許可を付与します	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateMicrosoftTeamsChannelConfiguration	AWS Chatbot Microsoft Teams チャネル設定を作成するアクセス許可を付与します	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateSlackChannelConfiguration	AWS Chatbot Slack チャネル設定を作成するアクセス許可を付与します	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChimeWebhookConfiguration	AWS Chatbot Chime ウェブフック設定を削除するアクセス許可を付与します	書き込み	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	
DeleteCustomAction	カスタムアクションを削除する許可を付与	書き込み	custom-action*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
DeleteMicrosoftTeamsChannelConfiguration	AWS Chatbot Microsoft Teams チャネル設定を削除する許可を付与	書き込み	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	
DeleteMicrosoftTeamsConfiguredTeam	で AWS Chatbot で設定された Microsoft Teams を削除する許可を付与 AWS アカウント	書き込み			
DeleteMicrosoftTeamsUserIdentity	AWS Chatbot Microsoft Teams ユーザー ID を削除するアクセス許可を付与します	書き込み			
DeleteSlackChannelConfiguration	AWS Chatbot Slack チャネル設定を削除する許可を付与	書き込み	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	
DeleteSlackUserIdentity	AWS Chatbot Slack ユーザー ID を削除するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteSlackWorkspaceAuthorization	AWS に関連付けられた AWS アカウント Chatbot を用いて Slack ワークスペース認可を削除する許可を付与	書き込み			
DescribeChimeWebhookConfigurations	AWS アカウント内のすべての AWS Chatbot Chime Webhook 設定を一覧表示するアクセス許可を付与します	読み取り			
DescribeSlackChannelConfigurations	内のすべての AWS Chatbot Slack チャネル設定を一覧表示するアクセス許可を付与します AWS アカウント	読み取り			
DescribeSlackChannels	AWS Chatbot サービスでオンボーディングされた AWS アカウントに接続されている Slack ワークスペース内のすべてのパブリック Slack チャネルを一覧表示するアクセス許可を付与します	読み取り			
DescribeSlackUserIdentities	AWS Chatbot Slack ユーザー ID を記述する許可を付与	読み取り			
DescribeSlackWorkspaces	AWS Chatbot サービスでオンボーディングされた AWS アカウントに接続されているすべての承認された Slack ワークスペースを一覧表示するアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DisassociateFromConfiguration	設定からリソースの関連付けを解除するアクセス許可を付与します	書き込み	ChatbotConfiguration*		
			custom-action*		
				aws:ResourceTag/${TagKey}	
GetAccountPreferences	AWS Chatbot アカウント設定を取得するアクセス許可を付与します	読み取り			
GetCustomAction	カスタムアクションを取得するアクセス許可を付与します	読み取り	custom-action*		
				aws:ResourceTag/${TagKey}	
GetMicrosoftTeamsChannelConfiguration	で 1 つの AWS Chatbot Microsoft Teams チャネル設定を取得する許可を付与 AWS アカウント	読み取り		aws:ResourceTag/${TagKey}	
GetMicrosoftTeamsOauthParameters	AWS Chatbot サービスで使用される Microsoft Teams OAuth コードをリクエストする OAuth パラメータを生成するアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetSlackOauthParameters	AWS Chatbot サービスで使用される Slack OAuth コードをリクエストする OAuth パラメータを生成するアクセス許可を付与します	読み取り			
ListAssociations	設定に関連付けられたリソースを一覧表示するアクセス許可を付与します	読み取り	ChatbotConfiguration*		
ListCustomActions	カスタムアクションを一覧表示するアクセス許可を付与します	リスト			
ListMicrosoftTeamsChannelConfigurations	内のすべての AWS Chatbot Microsoft Teams チャネル設定を一覧表示するアクセス許可を付与します AWS アカウント	読み取り			
ListMicrosoftTeamsConfiguredTeams	AWS Chatbot サービスでオンボーディングされた AWS アカウントに接続されているすべての Microsoft Teams を一覧表示するアクセス許可を付与します	読み取り			
ListMicrosoftTeamsUserIdentities	AWS Chatbot Microsoft Teams ユーザー ID を記述する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTagsForResource	AWS Chatbot チャネル設定に関連付けられているすべてのタグを一覧表示するアクセス許可を付与します	読み取り			
RedeemMicrosoftTeamsOauthCode	以前に生成されたパラメータを Microsoft APIsと引き換え、 AWS Chatbot サービスで使用する OAuth トークンを取得するアクセス許可を付与します	書き込み			
RedeemSlackOauthCode	AWS Chatbot サービスで使用する OAuth トークンを取得するために、以前に生成されたパラメータを Slack API と引き換えるアクセス許可を付与します	書き込み			
TagResource	AWS Chatbot チャネル設定でタグを作成するアクセス許可を付与します	Tagging	ChatbotConfiguration		
			custom-action		
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	AWS Chatbot チャネル設定のタグを削除するアクセス許可を付与します	Tagging	ChatbotConfiguration		
			custom-action		
				aws:TagKeys	
UpdateAccountPreferences	AWS Chatbot アカウント設定を更新する許可を付与	書き込み			
UpdateChimeWebhookConfiguration	AWS Chatbot Chime ウェブフック設定を更新する許可を付与	書き込み	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	
UpdateCustomAction	カスタムアクションを更新するアクセス許可を付与します	書き込み	custom-action*		
				aws:ResourceTag/${TagKey}	
UpdateMicrosoftTeamsChannelConfiguration	AWS Chatbot Microsoft Teams チャネル設定を更新する許可を付与	書き込み	ChatbotConfiguration*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
UpdateSlackChannelConfiguration	AWS Chatbot Slack チャネル設定を更新する許可を付与	書き込み	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	

AWS Chatbot で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
ChatbotConfiguration	`arn:${Partition}:chatbot::${Account}:chat-configuration/${ConfigurationType}/${ChatbotConfigurationName}`	aws:ResourceTag/${TagKey}
custom-action	`arn:${Partition}:chatbot::${Account}:custom-action/${ActionName}`	aws:ResourceTag/${TagKey}

AWS Chatbot の条件キー

AWS Chatbot は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon Chime のアクション、リソース、および条件キー

Amazon Chime (サービスプレフィックス: chime) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Chime で定義されるアクション
- Amazon Chime で定義されるリソースタイプ

- Amazon Chime の条件キー

Amazon Chime で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AcceptDelegate	Amazon Chime アカウントの管理を別の AWS アカウントと共有するための代理招待を受け入れるアクセス許可を付与します	書き込み			
ActivateUsers	Amazon Chime エンタープライズアカウントでユーザーをアクティブ化するアクセス許可を付与	Write			
AddDomain	ドメインを Amazon Chime アカウントに追加するアクセス許可を付与	Write			
AddOrUpdateGroups	新規あるいは更新された既存の Active Directory あるいは Amazon Chime エンタープライズアカウントに関連付けられた Okta ユーザーグループを追加するアクセス許可を付与	書き込み			
AssociateChannelFlow	フローとチャネルを関連付けるためのアクセス許可を付与	書き込み	app-instance-bot*		
			app-instance-user*		
			channel*		
			channel-flow*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociatePhoneNumberWithUser	Amazon Chime ユーザーに電話番号を関連付けるアクセス許可を付与	Write			
AssociatePhoneNumbersWithVoiceConnector	複数の電話番号を Amazon Chime Voice Connector を関連付けるアクセス許可を付与	Write	voice-connector*		
AssociatePhoneNumbersWithVoiceConnectorGroup	複数の電話番号を Amazon Chime Voice Connector Group を関連付けるアクセス許可を付与	書き込み			
AssociateSigninDelegateGroupsWithAccount	指定されたサインイン代理グループを、指定された Amazon Chime アカウントに関連付ける許可を付与	書き込み			
AssociateVoiceConnectorConnect [アクセス許可のみ]	指定された Amazon Connect インスタンスを Amazon Chime Voice Connector に関連付けるアクセス許可を付与します	書き込み			
AuthorizeDirectory	Amazon Chime エンタープライズアカウントに Active Directory を承認するアクセス許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchCreateAttendee	アクティブな Amazon Chime SDK 会議の新しい参加者を作成する許可を付与	書き込み	meeting*		
BatchCreateChannelMembership	チャネルに複数のユーザーおよびボットを追加するための許可を付与します	書き込み	app-instance-bot*		
			app-instance-user*		
			channel*		
BatchCreateRoomMembership	ルームメンバーをバッチ追加する許可を付与	Write			
BatchDeletePhoneNumber	最大で 50 までの電話番号を削除キューに移動するアクセス許可を付与	Write			
BatchSuspendUser	チームあるいは EnterpriseLWA Amazon Chime アカウントから最大で 50 人までのユーザーを停止するアクセス許可を付与	Write			
BatchUnsuspendUser	指定した Amazon Chime EnterpriseLWA アカウントで以前に停止されたユーザーから、最大で 50 人までの停止を解除するアクセス許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchUpdateAttendeeCapabilitiesExcept	ExcludedAttendeeIds 表に一覧表示されている機能を除き、AttendeeCapabilities を更新する権限の付与	書き込み	meeting*		
BatchUpdatePhoneNumber	最大で 50 までの電話番号に対して、UpdatePhoneNumberRequestItem オブジェクト内で電話番号の詳細を更新するアクセス許可を付与	Write			
BatchUpdateUser	指定した Amazon Chime アカウントの 20 人までのユーザーの UpdateUserRequestItem オブジェクト内のユーザー詳細を更新するアクセス許可を付与	書き込み			
ChannelFlowCallback	チャンネル上のメッセージにコールバックするためのアクセス許可を付与	書き込み	channel*		
Connect	メッセージングセッションエンドポイントへのアプリケーションインスタンスユーザーのウェブソケット接続を確立するためのアクセス許可を付与	Write	app-instance-user*		
ConnectDirectory	Amazon Chime エンタープライズアカウントに Active Directory を接続するアクセス許可を付与	書き込み			ds:ConnectDirectory

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateAccount	管理者の で Amazon Chime アカウントを作成するアクセス許可を付与します AWS アカウント	書き込み			
CreateApiKey	Amazon Chime アカウントおよび Okta 設定用の新しい SCIM アクセスキーを生成するアクセス許可を付与	書き込み			
CreateAppInstance	でアプリケーションインスタンスを作成するアクセス許可を付与します AWS アカウント（タグベースのアクセスコントロールは identity-chime.<region>.amazonaws.com エンドポイントでのみサポートされています）。	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAppInstanceAdmin	ユーザーまたはボットを AppInstanceAdmin に昇格させるための許可を付与します	書き込み	app-instance*		
			app-instance-bot*		
			app-instance-user*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateAppInstanceBot	AppInstance 内にボットを作成する許可を付与する (タグベースのアクセスコントロールは identity-chime.<region>.amazonaws.com エンドポイントでのみサポートされる)	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAppInstanceUser	AppInstance 内にユーザーを作成する許可を付与する (タグベースのアクセスコントロールは identity-chime.<region>.amazonaws.com エンドポイントでのみサポートされる)	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAttendee	アクティブな Amazon Chime SDK 会議の新しい参加者を作成する許可を付与	Write	meeting*		
CreateBot	Amazon Chime エンタープライズアカウントのボットを作成するアクセス許可を付与	書き込み			
CreateCDRBucket	新しい通話詳細レコードの S3 バケットを作成するアクセス許可を付与	書き込み			s3:CreateBucket s3:ListAllMyBuckets

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateChannel	でアプリケーションインスタンスのチャネルを作成するアクセス許可を付与します AWS アカウント （タグベースのアクセスコントロールは messaging-chime でのみサポートされています。<region>.amazonaws.com エンドポイント）	書き込み	app-instance-bot*		
			app-instance-user*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateChannelBan	ユーザーまたはボットによるチャネルへのアクセスを禁止するための許可を付与します	書き込み	app-instance-bot*		
			app-instance-user*		
			channel*		
CreateChannelFlow	でアプリケーションインスタンスのチャネルフローを作成するアクセス許可を付与します AWS アカウント （タグベースのアクセスコントロールは messaging-chime でのみサポートされています。<region>.amazonaws.com エンドポイント）	書き込み	app-instance*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateChannelMembership	ユーザーまたはボットをチャネルに追加するための許可を付与します	書き込み	app-instance-bot*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			app-instance-user*		
			channel*		
CreateChannelModerator	チャネルモデレーターを作成するアクセス許可を付与	書き込み	app-instance-bot*		
			app-instance-user*		
			channel*		
CreateConnectAnalyticsConnector [アクセス許可のみ]	で Amazon Connect Analytics Connector を作成するアクセス許可を付与します AWS アカウント（タグベースのアクセスコントロールは voice-chime でのみサポートされています。<region>.amazonaws.com エンドポイント）	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	chime:CreateVoiceConnector
CreateConnectCallTransferConnector [アクセス許可のみ]	で Amazon Connect Call Transfer Connector を作成するアクセス許可を付与します AWS アカウント（タグベースのアクセスコントロールは voice-chime でのみサポートされます。<region>.amazonaws.com エンドポイント）	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	chime:CreateVoiceConnector

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateMediaCapturePipeline	メディアキャプチャパイプラインを作成する許可を付与する (タグベースのアクセスコントロールは media-pipelines-chime.<region>.amazonaws.com エンドポイントでのみサポートされる)	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	s3:GetBucketPolicy
CreateMediaConcatenationPipeline	メディア連結パイプラインを作成する許可を付与する (タグベースのアクセスコントロールは media-pipelines-chime.<region>.amazonaws.com エンドポイントでのみサポートされる)	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	s3:GetBucketPolicy
CreateMediaInsightsPipeline	メディアインサイトパイプラインを作成する許可を付与する (タグベースのアクセスコントロールは media-pipelines-chime.<region>.amazonaws.com エンドポイントでのみサポートされる)	書き込み	media-insights-pipeline-configuration*		chime:TagResource kinesisvideo:DescribeStream
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateMediaInsightsPipelineConfiguration	メディアインサイトパイプライン設定を作成する許可を付与する (タグベースのアクセスコントロールは media-pipelines-chime.<region>.amazonaws.com エンドポイントでのみサポートされる)	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	chime:TagResource iam:PassRole kinesis:DescribeStream s3:ListBucket
CreateMediaLiveConnectorPipeline	メディアライブコネクタパイプラインを作成する許可を付与する (タグベースのアクセスコントロールは media-pipelines-chime.<region>.amazonaws.com エンドポイントでのみサポートされる)	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateMediaPipelineKinesisVideoStreamPool	kinesis ビデオストリームプールを作成する許可を付与する (タグベースのアクセスコントロールは media-pipelines-chime.<region>.amazonaws.com エンドポイントでのみサポートされる)	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	kinesis:DescribeStream kinesisvideo:CreateStream kinesisvideo:GetDataEndpoint kinesisvideo:ListStreams
CreateMediaStreamPipeline	メディアストリームパイプラインを作成する許可を付与する (タグベースのアクセスコントロールは media-pipelines-chime.<region>.amazonaws.com エンドポイントでのみサポートされる)	書き込み	media-pipeline-kinesis-video-stream-pool*		kinesisvideo:DescribeStream kinesisvideo:GetDataEndpoint kinesisvideo:PutMedia

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateMeeting	指定されたメディアリージョンで、最初の参加者なしで新しいミーティングを作成する許可を付与する (タグベースのアクセス制御は meetings-chime.<region>.amazonaws.com エンドポイントでのみサポートされる)	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMeetingDialOut	指定した Amazon Chime SDK ミーティングに参加する電話番号に発信するアクセス許可を付与	書き込み	meeting*		
CreateMeetingWithAttendees	指定されたメディアリージョンで、一連の参加者を含む新しいミーティングを作成する許可を付与する (タグベースのアクセス制御は meetings-chime.<region>.amazonaws.com エンドポイントでのみサポートされる)	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePhoneNumberOrder	キャリアで電話番号の注文を作成するアクセス許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateProxySession	指定された Amazon Chime Voice Connector のプロキシセッションを作成する許可を付与。	Write	voice-connector*		
CreateRoom	ルームを作成する許可を付与	Write			
CreateRoomMembership	ルームメンバーを追加する許可を付与	書き込み			
CreateSipMediaApplication	で Amazon Chime SIP メディアアプリケーションを作成するアクセス許可を付与します AWS アカウント （タグベースのアクセスコントロールは voice-chime でのみサポートされています。<region>.amazonaws.com エンドポイント）	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateSipMediaApplicationCall	管理者の で Amazon Chime SIP メディアアプリケーションのアウトバウンドコールを作成するアクセス許可を付与します AWS アカウント	書き込み	sip-media-application*		
CreateSipRule	管理者の で Amazon Chime SIP ルールを作成するアクセス許可を付与します AWS アカウント	書き込み	sip-media-application		
CreateUser	指定された Amazon Chime アカウントのユーザーを作成する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateVoiceConnector	で Voice Connector を作成するアクセス許可を付与しますAWS アカウント（タグベースのアクセスコントロールは voice-chime.<region>.amazonaws.com エンドポイントでのみサポートされています）。	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	chime:CreateConnectAnalyticsConnector chime:CreateConnectCallTransferConnector
CreateVoiceConnectorGroup	管理者の の下に Amazon Chime Voice Connector グループを作成するアクセス許可を付与します AWS アカウント	書き込み	voice-connector		
CreateVoiceProfile	音声プロファイルを作成するための許可を付与します	書き込み			
CreateVoiceProfileDomain	音声プロファイルドメインを作成する許可を付与する (タグベースのアクセスコントロールは voice-chime.<region>.amazonaws.com エンドポイントでのみサポートされる)	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	chime:TagResource kms:CreateGrant kms:DescribeKey
DeleteAccount	指定した Amazon Chime アカウントを削除するアクセス許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteAccountOpenIdConfig	Amazon Chime アカウントから OpenIdConfig 属性を削除するアクセス許可を付与	Write			
DeleteApiKey	Amazon Chime アカウントおよび Okta 設定に関連付けられた指定の SCIM アクセスキーを削除するアクセス許可を付与	Write			
DeleteAppInstance	AppInstance を削除するアクセス許可を付与	書き込み	app-instance*		
DeleteAppInstanceAdmin	AppInstanceAdmin をユーザーまたはボットに降格するための許可を付与します	書き込み	app-instance*		
			app-instance-bot*		
			app-instance-user*		
DeleteAppInstanceBot	AppInstanceBot を削除するための許可を付与します	書き込み	app-instance-bot*		
DeleteAppInstanceStreamingConfigurations	アプリケーションインスタンスのデータストリーミングを無効にするアクセス許可を付与	Write	app-instance*		
DeleteAppInstanceUser	AppInstanceUser を削除するアクセス許可を付与	Write	app-instance-user*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteAttendee	指定した参加者を Amazon Chime SDK 会議から削除する許可を付与	Write	meeting*		
DeleteCDRBucket	通話詳細レコードの S3 バケットをAmazon Chime アカウントから削除するアクセス許可を付与	Write			s3:DeleteBucket
DeleteChannel	チャネルを削除する許可を付与。	書き込み	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelBan	チャネルの禁止リストからユーザーまたはボットを削除するための許可を付与します	書き込み	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelFlow	チャネルフローを削除するためのアクセス許可を付与	書き込み	channel*		
DeleteChannelMembership	チャネルからメンバーを削除するアクセス許可を付与	Write	app-instance-bot*		
			app-instance-user*		
			channel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteChannelMessage	チャネルメッセージを削除するアクセス許可を付与	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelModerator	モデレーターを削除するアクセス許可を付与	書き込み	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteDelegate	Amazon Chime アカウントから委任 AWS アカウント 管理を削除するアクセス許可を付与します	書き込み			
DeleteDomain	Amazon Chime アカウントからドメインを削除するアクセス許可を付与	Write			
DeleteEventsConfiguration	送信イベントを受信するためにボットのイベント設定を削除するアクセス許可を付与	Write			
DeleteGroups	Amazon Chime エンタープライズアカウントから Active Directory または Okta ユーザーグループを削除するアクセス許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteMediaCapturePipeline	メディアキャプチャパイプラインを削除する許可を付与	書き込み	media-pipeline*		
DeleteMediaInsightsPipelineConfiguration	メディアインサイトパイプライン設定を削除するための許可を付与します	書き込み	media-insights-pipeline-configuration*		chime:ListVoiceConnectors
DeleteMediaPipeline	メディアパイプラインを削除するアクセス許可を付与	書き込み	media-pipeline*		
DeleteMediaPipelineKinesisVideoStreamPool	Kinesis 動画ストリームプールを削除するアクセス許可を付与します	書き込み	media-pipeline-kinesis-video-stream-pool*		
DeleteMeeting	指定した Amazon Chime SDK アカウントを削除する許可を付与	書き込み	meeting*		
DeleteMessagingStreamingConfigurations	AppInstance のデータストリーミング設定を削除するための許可を付与します	書き込み	app-instance*		
DeletePhoneNumber	1 つの電話番号を削除キューに移動するアクセス許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteProxySession	指定された Amazon Chime Voice Connector のプロキシセッションを削除する許可を付与。	Write	voice-connector*		
DeleteRoom	ルームを削除する許可を付与	Write			
DeleteRoomMembership	ルームメンバーを削除する許可を付与	書き込み			
DeleteSipMediaApplication	管理者の で Amazon Chime SIP メディアアプリケーションを削除するアクセス許可を付与します AWS アカウント	書き込み	sip-media-application*		
DeleteSipRule	管理者の で Amazon Chime SIP ルールを削除するアクセス許可を付与します AWS アカウント	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteVoiceConnector	指定した Amazon Chime Voice Connector を削除するアクセス許可を付与	Write	voice-connector*		logs:CreateLogDelivery logs:DeleteLogDelivery logs:GetLogDelivery logs:ListLogDeliveries
DeleteVoiceConnectorEmergencyCallingConfiguration	指定した Amazon Chime Voice Connector のエマージェンシーコール設定を削除する許可を付与	書き込み	voice-connector*		
DeleteVoiceConnectorExternalSystemsConfiguration	指定された Amazon Chime Voice Connector に接続されている外部システムの設定を削除するアクセス許可を付与します	書き込み	voice-connector*		
DeleteVoiceConnectorGroup	指定した Amazon Chime Voice Connector Group を削除するアクセス許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteVoiceConnectorOrigination	指定した Amazon Chime Voice Connector の発信設定を削除するアクセス許可を付与	Write	voice-connector*		
DeleteVoiceConnectorProxy	指定した Amazon Chime Voice Connector のプロキシ設定を削除する許可を付与。	Write	voice-connector*		
DeleteVoiceConnectorStreamingConfiguration	指定した Amazon Chime Voice Connector のストリーミング設定を削除するアクセス許可を付与	Write	voice-connector*		
DeleteVoiceConnectorTermination	指定した Amazon Chime Voice Connector の終了設定を削除するアクセス許可を付与	Write	voice-connector*		
DeleteVoiceConnectorTerminationCredentials	指定した Amazon Chime Voice Connector の SIP 終了認証情報を削除するアクセス許可を付与	書き込み	voice-connector*		
DeleteVoiceProfile	音声プロファイルを削除するための許可を付与します	書き込み	voice-profile*		
DeleteVoiceProfileDomain	音声プロファイルドメインを削除するための許可を付与します	書き込み	voice-profile-domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeregisterAppInstanceUserEndpoint	アプリケーションインスタンスユーザーのエンドポイントを登録解除するアクセス許可を付与	書き込み	app-instance-user*		
DescribeAppInstance	AppInstance の全詳細を取得するアクセス許可を付与	Read	app-instance*		
DescribeAppInstanceAdmin	AppInstanceAdmin の全詳細を取得するアクセス許可を付与	読み取り	app-instance*		
			app-instance-bot*		
			app-instance-user*		
DescribeAppInstanceBot	AppInstanceBot の全詳細を取得するための許可を付与します	読み取り	app-instance-bot*		
DescribeAppInstanceUser	AppInstanceUser の全詳細を取得するアクセス許可を付与	読み取り	app-instance-user*		
DescribeAppInstanceUserEndpoint	アプリケーションインスタンスユーザーに登録されたエンドポイントを記述するアクセス許可を付与	読み取り	app-instance-user*		
DescribeChannel	チャネルの全詳細を取得するアクセス許可を付与	Read	app-instance-bot*		
			app-instance-user*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			channel*		
DescribeChannelBan	チャネル禁止の全詳細を取得するアクセス許可を付与	読み取り	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelFlow	チャネルフローの完全な詳細を取得するためのアクセス許可を付与	読み取り	channel-flow*		
DescribeChannelMembership	チャネルメンバーシップの全詳細を取得するアクセス許可を付与	読み取り	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelMembershipForAppInstanceUser	指定したユーザーまたはボットのメンバーシップに基づいてチャネルの詳細を取得するための許可を付与します	読み取り	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelModeratedByAppInstanceUser	指定したユーザーまたはボットによってモデレートされたチャネルの全詳細を取得するための許可を付与します	読み取り	app-instance-bot*		
			app-instance-user*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			channel*		
DescribeChannelModerator	単一の ChannelModerator の全詳細を取得するアクセス許可を付与	読み取り	app-instance-bot*		
			app-instance-user*		
			channel*		
DisassociateChannelFlow	チャネルとフローの関連付けを解除するためのアクセス許可を付与	書き込み	app-instance-bot*		
			app-instance-user*		
			channel*		
			channel-flow*		
DisassociatePhoneNumberFromUser	指定した Amazon Chime ユーザーからプライマリでプロビジョニングされた番号の関連付けを解除するアクセス許可を付与	Write			
DisassociatePhoneNumbersFromVoiceConnector	指定した Amazon Chime Voice Connector から複数の電話番号の関連付けを解除するアクセス許可を付与	Write	voice-connector*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisassociatePhoneNumbersFromVoiceConnectorGroup	指定した Amazon Chime Voice Connector Group から複数の電話番号の関連付けを解除するアクセス許可を付与	書き込み			
DisassociateSigninDelegateGroupsFromAccount	指定されたサインイン代理グループを、指定された Amazon Chime アカウントから関連付けを解除する許可を付与	書き込み			
DisassociateVoiceConnectorConnect [アクセス許可のみ]	指定された Amazon Chime Voice Connector から Amazon Connect インスタンスの関連付けを解除するアクセス許可を付与します	書き込み			
DisconnectDirectory	Amazon Chime エンタープライズアカウントから Active Directory の接続を解除するアクセス許可を付与	Write			
GetAccount	指定した Amazon Chime アカウントの詳細を取得するアクセス許可を付与	Read			
GetAccountResource	Amazon Chime アカウントに関連付けられているアカウントリソースの詳細を取得するアクセス許可を付与	Read			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetAccountSettings	指定した Amazon Chime アカウント ID のアカウント設定を取得するアクセス許可を付与	Read			
GetAccountWithOpenIdConfig	Amazon Chime アカウントのアカウント詳細および OpenIdConfig 属性を取得するアクセス許可を付与	Read			
GetAppInstanceRetentionSettings	アプリケーションインスタンスの保持設定を取得するアクセス許可を付与	Read	app-instance*		
GetAppInstanceStreamingConfigurations	アプリケーションインスタンスのストリーミング設定を取得するアクセス許可を付与	Read	app-instance*		
GetAttendee	指定された会議 ID と参加者 ID の参加者詳細を取得する許可を付与	Read	meeting*		
GetBot	指定したボットの詳細を取得するアクセス許可を付与	Read			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetCDRBucket	Amazon Chime アカウントに関連付けられた通話詳細レコードの S3 バケットの詳細を取得するアクセス許可を付与	読み取り			s3:GetBucketAcl s3:GetBucketLocation s3:GetBucketLogging s3:GetBucketVersioning s3:GetBucketWebsite
GetChannelMembershipPreferences	チャネルメンバーシップの優先権を取得するアクセス許可を付与	読み取り	app-instance-bot*		
			app-instance-user*		
			channel*		
GetChannelMessage	チャネルメッセージの全詳細を取得するアクセス許可を付与	読み取り	app-instance-bot*		
			app-instance-user*		
			channel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetChannelMessageStatus	チャネルメッセージのステータスを取得するためのアクセス許可を付与	読み取り	app-instance-bot*		
			app-instance-user*		
			channel*		
GetDomain	Amazon Chime アカウントに関連付けられたドメインのドメイン詳細を取得するアクセス許可を付与	Read			
GetEventsConfiguration	送信イベントを受信するためにボットのイベント設定の詳細を取得するアクセス許可を付与	読み取り			
GetGlobalSettings	の Amazon Chime に関連するグローバル設定を取得する許可を付与 AWS アカウント	読み取り			
GetMediaCapturePipeline	既存のメディアキャプチャパイプラインを取得する許可を付与	読み取り	media-pipeline*		
GetMediaInsightsPipelineConfiguration	メディアインサイトパイプライン設定を取得するための許可を付与します	読み取り	media-insights-pipeline-configuration*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetMediaPipeline	既存のメディアパイプラインを取得するアクセス許可を付与	読み取り	media-pipeline*		
GetMediaPipelineKinesisVideoStreamPool	既存のメディアパイプラインを取得するアクセス許可を付与	読み取り	media-pipeline-kinesis-video-stream-pool*		
GetMeeting	指定された会議 ID の会議レコードを取得する許可を付与	Read	meeting*		
GetMeetingDetail	参加者、接続、およびその他のミーティングの詳細を取得するアクセス許可を付与	Read			
GetMessagingSessionEndpoint	メッセージングセッションのエンドポイントを取得するアクセス許可を付与	読み取り			
GetMessagingStreamingConfigurations	AppInstance のデータストリーミング設定を取得するための許可を付与します	読み取り	app-instance*		
GetPhoneNumber	指定した電話番号の詳細を取得するアクセス許可を付与	Read			
GetPhoneNumberOrder	指定した電話番号注文の詳細を取得するアクセス許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetPhoneNumberSettings	の Amazon Chime に関連する電話番号設定を取得する許可を付与 AWS アカウント	読み取り			
GetProxySession	指定した Amazon Chime Voice Connector の指定したプロキシセッションの詳細を取得する許可を付与。	読み取り	voice-connector*		
GetRetentionSettings	指定された Amazon Chime アカウントの保持設定を取得する許可を付与	読み取り			
GetRoom	ルームを取得する許可を付与	読み取り			
GetSipMediaApplication	管理者の で Amazon Chime SIP メディアアプリケーションの詳細を取得するアクセス許可を付与します AWS アカウント	読み取り	sip-media-application*		
GetSipMediaApplicationAlexaSkillConfiguration	管理者の で Amazon Chime SIP メディアアプリケーションの Alexa スキル設定を取得するアクセス許可を付与します AWS アカウント	読み取り	sip-media-application*		
GetSipMediaApplicationLoggingConfiguration	管理者の で Amazon Chime SIP メディアアプリケーションのログ記録設定を取得するアクセス許可を付与します AWS アカウント	読み取り	sip-media-application*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetSipRule	管理者の で Amazon Chime SIP ルールの詳細を取得する許可を付与 AWS アカウント	読み取り			
GetSpeakerSearchTask	指定された Amazon Chime リソースでスピーカー検索タスクを取得するアクセス許可を付与します	読み取り	media-pipeline		
			voice-connector		
GetTelephonyLimits	のテレフォニー制限を取得するアクセス許可を付与します AWS アカウント	読み取り			
GetUser	指定したユーザー ID の詳細を取得するアクセス許可を付与	Read			
GetUserActivityReportData	[User details (ユーザー詳細)] ページでユーザーアクティビティの要約を取得するアクセス許可を付与	Read			
GetUserByEmail	Amazon Chime のエンタープライズアカウントまたはチームアカウントの E メールアドレスに基づき、Amazon Chime ユーザーのユーザー詳細を取得するアクセス許可を付与	Read			
GetUserSettings	指定した Amazon Chime ユーザーに関連するユーザー設定を取得するアクセス許可を付与	Read			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetVoiceConnector	指定した Amazon Chime Voice Connector の詳細を取得するアクセス許可を付与	Read	voice-connector*		
GetVoiceConnectorEmergencyCallingConfiguration	指定した Amazon Chime Voice Connector のエマージェンシーコール設定の詳細を取得する許可を付与	読み取り	voice-connector*		
GetVoiceConnectorExternalSystemsConfiguration	指定された Amazon Chime Voice Connector に接続されている外部システムの設定を取得するアクセス許可を付与します	読み取り	voice-connector*		
GetVoiceConnectorGroup	指定した Amazon Chime Voice Connector Group の詳細を取得するアクセス許可を付与	Read			
GetVoiceConnectorLoggingConfiguration	指定した Amazon Chime Voice Connector のログ記録設定の詳細を取得するアクセス許可を付与	Read	voice-connector*		
GetVoiceConnectorOrigination	指定した Amazon Chime Voice Connector の発信設定の詳細を取得するアクセス許可を付与	Read	voice-connector*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetVoiceConnectorProxy	指定した Amazon Chime Voice Connector のプロキシ設定の詳細を取得する許可を付与。	Read	voice-connector*		
GetVoiceConnectorStreamingConfiguration	指定した Amazon Chime Voice Connector のストリーミング設定の詳細を取得するアクセス許可を付与	Read	voice-connector*		
GetVoiceConnectorTermination	指定した Amazon Chime Voice Connector の終了設定の詳細を取得するアクセス許可を付与	Read	voice-connector*		
GetVoiceConnectorTerminationHealth	指定した Amazon Chime Voice Connector の終了ヘルスの詳細を取得するアクセス許可を付与	読み取り	voice-connector*		
GetVoiceProfile	音声プロファイルを取得するための許可を付与します	読み取り	voice-profile*		
GetVoiceProfileDomain	音声プロファイルドメインを取得するための許可を付与します	読み取り	voice-profile-domain*		
GetVoiceToneAnalysisTask	指定された Amazon Chime リソースで音声トーン分析タスクを取得するアクセス許可を付与します	読み取り	media-pipeline		
			voice-connector		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
InviteDelegate	Amazon Chime アカウントの AWS アカウント 委任リクエストを受け入れる招待を送信するアクセス許可を付与します	書き込み			
InviteUsers	指定した Amazon Chime アカウントに最大で 50 人までのユーザーを招待するアクセス許可を付与	Write			
InviteUsersFromProvider	サードパーティープロバイダーから Amazon Chime アカウントにユーザーを招待する許可を付与。	Write			
ListAccountUsageReportData	Amazon Chime アカウントの使用状況レポートデータのリストを取得するアクセス許可を付与	リスト			
ListAccounts	管理者の で Amazon Chime アカウントを一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListApiKeys	Amazon Chime アカウントおよび Okta 設定で定義された SCIM アクセスキーのリストを取得するアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListAppInstanceAdmins	アプリケーションインスタンス内の管理者の一覧を表示するアクセス許可を付与	リスト	app-instance*		
			app-instance-bot*		
			app-instance-user*		
ListAppInstanceBots	単一のアプリケーションインスタンスで作成されたすべての AppInstanceBots を一覧表示するための許可を付与します	リスト	app-instance-bot*		
ListAppInstanceUserEndpoints	アプリケーションインスタンスユーザーに登録されたエンドポイントを一覧表示するアクセス許可を付与	リスト	app-instance-user*		
ListAppInstanceUsers	単一のアプリケーションインスタンスで作成されたすべての AppInstanceUsers を一覧表示するアクセス許可を付与	リスト	app-instance-user*		
ListAppInstances	1 つの で作成されたすべての Amazon Chime アプリケーションインスタンスを一覧表示するアクセス許可を付与します AWS アカウント	リスト	app-instance*		
ListAttendeeTags	Amazon Chime SDK 参加者リソースに適用されたタグを一覧表示する許可を付与。	リスト	meeting*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListAttendees	指定された Amazon Chime SDK 会議に対して、最大 100 人の参加者をリストする許可を付与	リスト	meeting*		
ListAvailableVoiceConnectorRegions	Amazon Chime SDK Voice Connector AWS リージョンを作成できる を一覧表示する許可を付与	リスト			
ListBots	Amazon Chime エンタープライズアカウントに関連付けられたボットを一覧表示するアクセス許可を付与	リスト			
ListCDRBucket	通話詳細レコードの S3 バケットを一覧表示するアクセス許可を付与	リスト			s3:ListAllMyBuckets s3:ListBucket
ListCallingRegions	管理者の で使用できる呼び出しリージョンを一覧表示するアクセス許可を付与しますAWS アカウント	リスト			
ListChannelBans	特定のチャネルへのアクセスを禁止されているすべてのユーザーおよびボットを一覧表示するための許可を付与します	リスト	app-instance-bot*		
			app-instance-user*		
			channel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListChannelFlows	単一の Chime AppInstance で作成されたすべてのチャネルフローをリストするためのアクセス許可を付与	リスト	channel-flow*		
ListChannelMemberships	チャネル内のすべてのチャネルメンバーシップを一覧表示するアクセス許可を付与	リスト	app-instance-bot*		
			app-instance-user*		
			channel*		
ListChannelMembershipsForAppInstanceUser	特定のユーザーまたはボットが所属しているすべてのチャネルを一覧表示するための許可を付与します	リスト	app-instance-bot*		
			app-instance-user*		
ListChannelMessages	チャネル内のすべてのメッセージを一覧表示するアクセス許可を付与	読み取り	app-instance-bot*		
			app-instance-user*		
			channel*		
ListChannelModerators	チャネルのすべてのモデレーターを一覧表示するアクセス許可を付与	リスト	app-instance-bot*		
			app-instance-user*		
			channel*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListChannels	単一の Chime AppInstance で作成されたすべての AppInstanceUsers を一覧表示するアクセス許可を付与	リスト	app-instance-bot*		
			app-instance-user*		
ListChannelsAssociatedWithChannelFlow	単一の Chime Channel Flow に関連付けられたすべての Channel を一覧表示するアクセス許可を付与	リスト	channel-flow*		
ListChannelsModeratedByAppInstanceUser	ユーザーまたはボットによってモデレートされたすべてのチャネルを一覧表示するための許可を付与します	リスト	app-instance-bot*		
			app-instance-user*		
ListDelegates	Amazon Chime アカウントに関連付けられたアカウント委任情報のリストを取得するアクセス許可を付与	リスト			
ListDirectories	の Directory Service でホストされているアクティブな Active Directory を一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListDomains	Amazon Chime アカウントに関連付けられたドメインのリストを取得するアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListGroups	Amazon Chime エンタープライズアカウントに関連付けられた Active Directory または Okta ユーザーグループのリストを取得するアクセス許可を付与	リスト			
ListMediaCapturePipelines	メディアキャプチャパイプラインを一覧表示する許可を付与	リスト			
ListMediaInsightsPipelineConfigurations	すべてのメディアインサイトパイプライン設定を一覧表示するための許可を付与します	リスト			
ListMediaPipelineKinesisVideoStreamPools	メディアパイプラインを一覧表示するアクセス許可を付与	リスト			
ListMediaPipelines	メディアパイプラインを一覧表示するアクセス許可を付与	リスト			
ListMeetingEvents	指定したミーティングで発生したすべてのイベントのリストを取得するアクセス許可を付与	リスト			
ListMeetingTags	Amazon Chime SDK ミーティングリソースに適用されたタグを一覧表示する許可を付与	リスト	meeting*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListMeetings	最大 100 件のアクティブな Amazon Chime SDK 会議を一覧表示する許可を付与	リスト			
ListMeetingsReportData	指定した日付範囲内に終了したミーティングのリストを取得するアクセス許可を付与	リスト			
ListPhoneNumberOrders	管理者の で電話番号の注文を一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListPhoneNumbers	管理者の の電話番号を一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListProxySessions	指定された Amazon Chime Voice Connector のプロキシセッションを一覧表示する許可を付与。	リスト	voice-connector*		
ListRoomMemberships	すべてのルームメンバーを一覧表示する許可を付与	リスト			
ListRooms	ルームを一覧表示する許可を付与	リスト			
ListSipMediaApplications	管理者の ですべての Amazon Chime SIP メディアアプリケーションを一覧表示するアクセス許可を付与します AWS アカウント	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListSipRules	管理者の にあるすべての Amazon Chime SIP ルールを一覧表示するアクセス許可を付与します AWS アカウント	リスト	sip-media-application		
ListSubChannels	単一 Channel 内のすべての SubChannel を一覧表示するアクセス許可を付与	リスト	app-instance-bot*		
			app-instance-user*		
			channel*		
ListSupportedPhoneNumberCountries	でサポートされている電話番号の国を一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListTagsForResource	Amazon Chime リソースに適用されたタグを一覧表示する許可を付与	読み取り	app-instance		
			app-instance-bot		
			app-instance-user		
			channel		
			channel-flow		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			media-insights-pipeline-configuration		
			media-pipeline		
			media-pipeline-kinesis-video-stream-pool		
			meeting		
			sip-media-application		
			voice-connector		
			voice-profile-domain		
ListUsers	指定した Amazon Chime アカウントに所属するユーザーのリストを取得するアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListVoiceConnectorGroups	管理者の の下に Amazon Chime Voice Connector グループを一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListVoiceConnectorTerminationCredentials	指定した Amazon Chime Voice Connector の SIP 終了認証情報のリストを取得するアクセス許可を付与	リスト	voice-connector*		
ListVoiceConnectors	管理者の の下に Amazon Chime Voice Connector を一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListVoiceProfileDomains	音声プロファイルドメインを一覧表示するための許可を付与します	リスト			
ListVoiceProfiles	音声プロファイルを一覧表示するための許可を付与します	リスト	voice-profile-domain*		
LogoutUser	現在ユーザーがログインしているすべてのデバイスから、指定したユーザーをログアウトするアクセス許可を付与	Write			
PutAppInstanceRetentionSettings	アプリケーションインスタンスのデータ保持を有効にするアクセス許可を付与	Write	app-instance*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutAppInstanceStreamingConfigurations	アプリケーションインスタンスのデータストリーミングを設定するアクセス許可を付与	書き込み	app-instance*		
PutAppInstanceUserExpirationSettings	AppInstanceUser の有効期限の設定を PUT するための許可を付与します	書き込み	app-instance-user*		
PutChannelExpirationSettings	チャネルの有効期限の設定を PUT するための許可を付与します	書き込み	app-instance-user*		
			channel*		
PutChannelMembershipPreferences	チャンネルメンバーシップの優先権を設定するアクセス許可を付与	書き込み	app-instance-bot*		
			app-instance-user*		
			channel*		
PutEventsConfiguration	送信イベントを受信するためにボットのイベント設定の詳細を更新するアクセス許可を付与	書き込み			
PutMessagingStreamingConfigurations	AppInstance のデータストリーミング設定を PUT するための許可を付与します	書き込み	app-instance*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutRetentionSettings	指定された Amazon Chime アカウントの保持設定を作成または更新する許可を付与	書き込み			
PutSipMediaApplicationAlexaSkillConfiguration	管理者の で Amazon Chime SIP メディアアプリケーションの Alexa スキル設定を更新するアクセス許可を付与します AWS アカウント	書き込み	sip-media-application*		
PutSipMediaApplicationLoggingConfiguration	管理者の で Amazon Chime SIP メディアアプリケーションのログ記録設定を更新するアクセス許可を付与します AWS アカウント	書き込み	sip-media-application*		
PutVoiceConnectorEmergencyCallingConfiguration	指定した Amazon Chime Voice Connector のエマージェンシーコール設定を追加する許可を付与	書き込み	voice-connector*		
PutVoiceConnectorExternalSystemsConfiguration	指定された Amazon Chime Voice Connector に接続されている外部システムの設定を更新するアクセス許可を付与します	書き込み	voice-connector*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutVoiceConnectorLoggingConfiguration	指定した Amazon Chime Voice Connector のログ記録設定を追加する許可を付与。	Write	voice-connector*		logs:CreateLogDelivery logs:CreateLogGroup logs:DeleteLogDelivery logs:DescribeLogGroups logs:GetLogDelivery logs:ListLogDeliveries
PutVoiceConnectorOrigination	指定した Amazon Chime Voice Connector の発信設定を更新するアクセス許可を付与	Write	voice-connector*		
PutVoiceConnectorProxy	指定した Amazon Chime Voice Connector のプロキシ設定を追加する許可を付与。	Write	voice-connector*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutVoiceConnectorStreamingConfiguration	指定した Amazon Chime Voice Connector のストリーミング設定を追加するアクセス許可を付与	Write	voice-connector*		chime:GetMediaInsightsPipelineConfiguration
			media-insights-pipeline-configuration		
PutVoiceConnectorTermination	指定した Amazon Chime Voice Connector の終了設定を更新するアクセス許可を付与	Write	voice-connector*		
PutVoiceConnectorTerminationCredentials	指定した Amazon Chime Voice Connector の SIP 終了認証情報を追加するアクセス許可を付与	Write	voice-connector*		
RedactChannelMessage	メッセージの内容を編集するアクセス許可を付与	書き込み	app-instance-bot*		
			app-instance-user*		
			channel*		
RedactConversationMessage	指定した Chime 会話メッセージを編集する許可を付与	書き込み			
RedactRoomMessage	指定した Chime ルームメッセージを編集する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RegenerateSecurityToken	指定したボットのセキュリティトークンを再生成するアクセス許可を付与	書き込み			
RegisterAppInstanceUserEndpoint	アプリケーションインスタンスユーザーのエンドポイントを登録するアクセス許可を付与	書き込み	app-instance-user*		mobiletargeting:GetApp
RenameAccount	Amazon Chime エンタープライズあるいはチームアカウントのアカウント名を変更するアクセス許可を付与	Write			
RenewDelegate	Amazon Chime アカウントに関連付けられた委任リクエストを更新するアクセス許可を付与	Write			
ResetAccountResource	Amazon Chime アカウントのアカウントリソースをリセットするアクセス許可を付与	Write			
ResetPersonalPIN	Amazon Chime アカウントの指定したユーザーの個人ミーティング PIN をリセットするアクセス許可を付与	Write			
RestorePhoneNumber	指定した電話番号を削除キューから電話番号インベントリに戻して復元するアクセス許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RetrieveDataExports	「Request attachments」(添付ファイルのリクエスト) アクションの一部として返された、すべてのユーザー添付ファイルへのリンクを含むファイルをダウンロードするアクセス許可を付与	読み取り			
SearchAvailablePhoneNumbers	キャリアから注文できる電話番号を検索するアクセス許可を付与	読み取り			
SearchChannels	AppInstanceUser が属するチャンネルを検索する権限、または AppInstaceAdmin の AppInstance にわたるチャンネルを検索するアクセス許可を付与	リスト	app-instance-bot*		
			app-instance-user*		
SendChannelMessage	メンバーが所属している特定のチャネルにメッセージを送信するアクセス許可を付与	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
StartDataExport	「Request attachments」(添付ファイルのリクエスト) リクエストを送信するアクセス許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartMeetingTranscription	会議の文字起こしを開始する許可を付与	書き込み			
StartSpeakerSearchTask	指定された Amazon Chime リソースでスピーカー検索タスクを開始するアクセス許可を付与します	書き込み	media-pipeline		
			voice-connector		
StartVoiceToneAnalysisTask	指定された Amazon Chime リソースで音声トーン分析タスクを開始するアクセス許可を付与します	書き込み	media-pipeline		
			voice-connector		
StopMeetingTranscription	会議のトランスクリプションを停止するアクセス許可を付与	書き込み			
StopSpeakerSearchTask	指定された Amazon Chime リソースでスピーカー検索タスクを停止するアクセス許可を付与します	書き込み	media-pipeline		
			voice-connector		
StopVoiceToneAnalysisTask	指定された Amazon Chime リソースで音声トーン分析タスクを停止するアクセス許可を付与します	書き込み	media-pipeline		
			voice-connector		
SubmitSupportRequest	カスタマーサービスサポートリクエストを送信するアクセス許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SuspendUsers	Amazon Chime エンタープライズアカウントからユーザーを停止するアクセス許可を付与	Write			
TagAttendee	指定したタグを指定された Amazon Chime SDK の参加者に適用する許可を付与。	Tagging	meeting*		
TagMeeting	指定されたタグを指定された Amazon Chime SDK ミーティングに適用する許可を付与	Tagging	meeting*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
TagResource	指定されたタグを指定されたリソースに適用する許可を付与する (タグベースのアクセスコントロールは *-chime.<region>.amazonaws.com エンドポイントでのみサポートされる)	Tagging	app-instance		
			app-instance-bot		
			app-instance-user		
			channel		
			channel-flow		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			media-insights-pipeline-configuration		
			media-pipeline		
			media-pipeline-kinesis-video-stream-pool		
			meeting		
			sip-media-application		
			voice-connector		
			voice-profile-domain		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UnauthorizeDirectory	Amazon Chime エンタープライズアカウントから Active Directory を承認解除するアクセス許可を付与	書き込み			
UntagAttendee	指定された Amazon Chime SDK 参加者から指定したタグを解除する許可を付与	Tagging	meeting*		
UntagMeeting	指定された Amazon Chime SDK ミーティングから指定したタグを解除する許可を付与	Tagging	meeting*		
UntagResource	指定されたリソースから指定されたタグのタグを解除する許可を付与する (タグベースのアクセスコントロールは *-chime.<region>.amazonaws.com エンドポイントでのみサポートされる)	Tagging	app-instance		
			app-instance-bot		
			app-instance-user		
			channel		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			channel-flow		
			media-insights-pipeline-configuration		
			media-pipeline		
			media-pipeline-kinesis-video-stream-pool		
			meeting		
			sip-media-application		
			voice-connector		
			voice-profile-domain		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateAccount	指定した Amazon Chime アカウントのアカウント詳細を更新するアクセス許可を付与	Write			
UpdateAccountOpenIdConfig	Amazon Chime アカウントから OpenIdConfig 属性を更新するアクセス許可を付与	Write			
UpdateAccountResource	Amazon Chime アカウントのアカウントリソースを更新するアクセス許可を付与	Write			
UpdateAccountSettings	指定した Amazon Chime アカウントの設定を更新するアクセス許可を付与	Write			
UpdateAppInstance	AppInstance メタデータを更新するアクセス許可を付与	書き込み	app-instance*		
UpdateAppInstanceBot	AppInstanceBot の詳細を更新するための許可を付与します	書き込み	app-instance-bot*		
UpdateAppInstanceUser	AppInstanceUser の詳細を更新するアクセス許可を付与	書き込み	app-instance-user*		
UpdateAppInstanceUserEndpoint	アプリケーションインスタンスユーザーに登録されたエンドポイントを更新するアクセス許可を付与	書き込み	app-instance-user*		
UpdateAttendeeCapabilities	更新する機能に許可の付与	書き込み	meeting*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateBot	指定したボットのステータスを更新するアクセス許可を付与	Write			
UpdateCDRSettings	通話詳細レコードの S3 バケットを更新するアクセス許可を付与	Write			s3:CreateBucket s3:DeleteBucket s3:ListAllMyBuckets
UpdateChannel	チャネルの属性を更新するアクセス許可を付与	書き込み	app-instance-bot*		
			app-instance-user*		
			channel*		
UpdateChannelFlow	チャネルフローを更新するためのアクセス許可を付与	書き込み	channel-flow*		
UpdateChannelMessage	メッセージの内容を更新するアクセス許可を付与	Write	app-instance-bot*		
			app-instance-user*		
			channel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateChannelReadMarker	ユーザーがチャネル内のメッセージを最後に読んだ時点にタイムスタンプを設定するアクセス許可を付与	書き込み	app-instance-bot*		
			app-instance-user*		
			channel*		
UpdateGlobalSettings	の Amazon Chime に関連するグローバル設定を更新する許可を付与 AWS アカウント	書き込み			
UpdateMediaInsightsPipelineConfiguration	メディアインサイトパイプライン設定のステータスを更新するための許可を付与します	書き込み	media-insights-pipeline-configuration*		chime:ListVoiceConnectors iam:PassRole kinesis:DescribeStream s3:ListBucket
UpdateMediaInsightsPipelineStatus	メディアインサイトパイプラインのステータスを更新するための許可を付与します	書き込み	media-pipeline*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateMediaPipelineKinesisVideoStreamPool	Kinesis 動画ストリームプールを更新するアクセス許可を付与します	書き込み	media-pipeline-kinesis-video-stream-pool*		
UpdatePhoneNumber	指定した電話番号の電話番号詳細を更新するアクセス許可を付与	書き込み			
UpdatePhoneNumberSettings	の Amazon Chime に関連する電話番号設定を更新する許可を付与 AWS アカウント	書き込み			
UpdateProxySession	指定された Amazon Chime Voice Connector のプロキシセッションを更新する許可を付与。	Write	voice-connector*		
UpdateRoom	ルームを更新する許可を付与	Write			
UpdateRoomMembership	ルームメンバーシップロールを更新する許可を付与	書き込み			
UpdateSipMediaApplication	管理者の で Amazon Chime SIP メディアアプリケーションのプロパティを更新するアクセス許可を付与します AWS アカウント	書き込み	sip-media-application*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateSipMediaApplicationCall	管理者の で Amazon Chime SIP メディアアプリケーションの呼び出しを更新するアクセス許可を付与します AWS アカウント	書き込み	sip-media-application*		
UpdateSipRule	管理者の で Amazon Chime SIP ルールのプロパティを更新する許可を付与 AWS アカウント	書き込み	sip-media-application		
UpdateSupportedLicenses	Amazon Chime アカウントのユーザーが利用できる、サポートされているライセンス層を更新するアクセス許可を付与	Write			
UpdateUser	指定したユーザー ID のユーザー詳細を更新するアクセス許可を付与	Write			
UpdateUserLicenses	Amazon Chime ユーザーのライセンスを更新するアクセス許可を付与	Write			
UpdateUserSettings	指定した Amazon Chime ユーザーに関連するユーザー設定を更新するアクセス許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateVoiceConnector	指定した Amazon Chime Voice Connector の Amazon Chime Voice Connector の詳細を更新するアクセス許可を付与	Write	voice-connector*		
UpdateVoiceConnectorGroup	指定した Amazon Chime Voice Connector Group の Amazon Chime Voice Connector グループの詳細を更新するアクセス許可を付与	書き込み	voice-connector		
UpdateVoiceProfile	音声プロファイルを更新するための許可を付与します	書き込み	voice-profile*		
UpdateVoiceProfileDomain	音声プロファイルドメインを更新するための許可を付与します	書き込み	voice-profile-domain*		
ValidateAccountResource	Amazon Chime アカウントのアカウントリソースを検証するアクセス許可を付与	読み取り			
ValidateE911Address	Amazon Chime Voice Connector での公的機関への緊急通報に使用されるアドレスを検証するための許可を付与します	読み取り			

Amazon Chime で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
meeting	arn:${Partition}:chime::${AccountId}:meeting/${MeetingId}	aws:ResourceTag/${TagKey}
app-instance	arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}	aws:ResourceTag/${TagKey}
app-instance-user	arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/user/${AppInstanceUserId}	aws:ResourceTag/${TagKey}
app-instance-bot	arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/bot/${AppInstanceBotId}	aws:ResourceTag/${TagKey}
channel	arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/channel/${ChannelId}	aws:ResourceTag/${TagKey}
channel-flow	arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/channel-flow/${ChannelFlowId}	aws:ResourceTag/${TagKey}
media-pipeline	arn:${Partition}:chime:${Region}:${AccountId}:media-pipeline/${MediaPipelineId}	aws:ResourceTag/${TagKey}
media-insights-pipeline-configuration	arn:${Partition}:chime:${Region}:${AccountId}:media-insights-pipeline-configuration/${ConfigurationName}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
media-pipeline-kinesis-video-stream-pool	arn:${Partition}:chime:${Region}:${AccountId}:media-pipeline-kinesis-video-stream-pool/${PoolName}	aws:ResourceTag/${TagKey}
voice-profile-domain	arn:${Partition}:chime:${Region}:${AccountId}:voice-profile-domain/${VoiceProfileDomainId}	aws:ResourceTag/${TagKey}
voice-profile	arn:${Partition}:chime:${Region}:${AccountId}:voice-profile/${VoiceProfileId}	
voice-connector	arn:${Partition}:chime:${Region}:${AccountId}:vc/${VoiceConnectorId}	aws:ResourceTag/${TagKey}
sip-media-application	arn:${Partition}:chime:${Region}:${AccountId}:sma/${SipMediaApplicationId}	aws:ResourceTag/${TagKey}

Amazon Chime の条件キー

Amazon Chime では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグのキーと値でアクセスをフィルター	String

条件キー	説明	タイプ
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString

AWS クリーンルームのアクション、リソース、および条件キー

AWS クリーンルーム (サービスプレフィックス: `cleanrooms`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS クリーンルームで定義されるアクション
- AWS クリーンルームで定義されるリソースタイプ
- AWS クリーンルームの条件キー

AWS クリーンルームで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchGetCollaborat	コラボレーションに関連する分析テンプレートの詳細を表示するアクセス許可を付与	読み取り	analysistemplate*		cleanrooms:GetCollaboration

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ionAnalysisTemplate					AnalysisTemplate
			collaboration*		
BatchGetSchema	スキーマの詳細を表示するアクセス許可を付与	読み取り	collaboration*		cleanrooms:GetSchema
			configuredtableassociation		
			idmappingtable		
BatchGetSchemaAnalysisRule	スキーマ (複数可) に関連付けられている分析ルールを表示する許可を付与する	読み取り	collaboration*		cleanrooms:GetSchema
			configuredtableassociation		
			idmappingtable		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateAnalysisTemplate	新しい分析テンプレートを作成するアクセス許可を付与	書き込み	analysistemplate*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCollaboration	新しいコラボレーション、共有データコラボレーション環境を作成するアクセス許可を付与	書き込み	collaboration*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateConfiguredAudienceModelAssociation	新しい関連付けを作成して、Clean Rooms ML の設定済みオーディエンスモデルをコラボレーションにリンクするためのアクセス許可を付与	書き込み	configuredaudiencemodelassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	cleanrooms-ml:GetConfiguredAudienceModel cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateConfiguredTable	新しい設定済みテーブルを作成するアクセス許可を付与	書き込み	configuredtable*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	athena:GetTableMetadata glue:BatchGetPartition glue:GetDatabase glue:GetDatabases glue:GetPartition glue:GetPartitions glue:GetSchemaVersion glue:GetTable glue:GetTables
CreateConfiguredTableAnalysisRule	設定済みテーブルの分析ルールを作成するアクセス許可を付与	書き込み	configuredtable*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateConfiguredTableAssociation	新しいアソシエーションを作成して、設定済みテーブルをコラボレーションにリンクするアクセス許可を付与	書き込み	configuredtable*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:PassRole
			configuredtableassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateConfiguredTableAssociationAnalysisRule	設定済みテーブル関連付けの分析ルールを作成する許可を付与する	書き込み	configuredtableassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateIdMappingTable	新しい ID マッピングテーブルを作成して、ID マッピングワークフローをコラボレーションにリンクする許可を付与する	書き込み	idmappingtable*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	entityresolution:AddPolicyStatement entityresolution:GetIdMappingWorkflow
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateIdNamespaceAssociation	新しい関連付けを作成して、AWS エンティティ解決 ID 名前空間をコラボレーションにリンクするアクセス許可を付与します	書き込み	idnamespaceassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	entityresolution:AddPolicyStatement entityresolution:GetIdNamespace
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateMembership	メンバーシップを作成してコラボレーションに参加するアクセス許可を付与	書き込み	collaboration*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:PassRole logs:CreateLogDelivery logs:CreateLogGroup logs:DeleteLogDelivery logs:DescribeLogGroups logs:DescribeResourcePolicies logs:GetLogDelivery logs:ListLogDeliveries logs:PutResourcePolicy

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					logs:UpdateLogDelivery s3:GetBucketLocation
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreatePrivacyBudgetTemplate	新しいプライバシー予算テンプレートを作成するためのアクセス許可を付与	書き込み	membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			privacybudgettemplate*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteAnalysisTemplate	既存の分析テンプレートを削除するアクセス許可を付与	書き込み	analysistemplate*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteCollaboration	既存のコラボレーションを削除するアクセス許可を付与	書き込み	collaboration*		cleanrooms-ml:DeleteConfiguredAudienceModelPolicy cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteConfiguredAudienceModelAssociation	既存の設定済みオーディエンスモデルの関連付けを削除するためのアクセス許可を付与	書き込み	configuredaudiencemodelassociation*		cleanrooms-ml:DeleteConfiguredAudienceModelPolicy cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy
DeleteConfiguredTable	設定済みテーブルを削除するアクセス許可を付与	書き込み	configuredtable*		
DeleteConfiguredTableAnalysisRule	既存の分析ルールを削除するアクセス許可を付与	書き込み	configuredtable*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteConfiguredTableAssociation	コラボレーションから設定済みテーブルの関連付けを解除するアクセス許可を付与	書き込み	configuredtableassociation*		
DeleteConfiguredTableAssociationAnalysisRule	既存の設定済みテーブル関連分析ルールを削除する許可を付与する	書き込み	configuredtableassociation*		
DeleteIdMappingTable	コラボレーションから ID マッピングテーブルを削除する許可を付与する	書き込み	idmappingtable*		entityresolution:DeletePolicyStatement
			membership*		
DeleteIdNamespaceAssociation	コラボレーションから ID 名前空間の関連付けを削除する許可を付与する	書き込み	idnamespaceassociation*		entityresolution:DeletePolicyStatement
			membership*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteMember	コラボレーションからメンバーを削除するアクセス許可を付与	書き込み	collaboration*		cleanrooms-ml:DeleteConfiguredAudienceModelPolicy cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy
DeleteMembership	メンバーシップを削除してコラボレーションを終了するアクセス許可を付与	書き込み	membership*		
DeletePrivacyBudgetTemplate	既存のプライバシー予算テンプレートを削除するためのアクセス許可を付与	書き込み	privacybudgettemplate*		
GetAnalysisTemplate	分析テンプレートの詳細を表示するアクセス許可を付与	読み取り	analysistemplate*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetCollaboration	コラボレーションの詳細を表示するアクセス許可を付与	読み取り	collaboration*		
GetCollaborationAnalysisTemplate	コラボレーション内の分析テンプレートの詳細を表示するアクセス許可を付与	読み取り	analysistemplate*		
			collaboration*		
GetCollaborationConfiguredAudienceModelAssociation	コラボレーション内の設定済みオーディエンスモデルの関連付けの詳細を表示するためのアクセス許可を付与	読み取り	collaboration*		
			configuredaudiencemodelassociation*		
GetCollaborationIdNamespaceAssociation	コラボレーション内で ID 名前空間の関連付けを取得する許可を付与する	読み取り	collaboration*		
			idnamespaceassociation*		
GetCollaborationPrivacyBudgetTemplate	コラボレーション内のプライバシー予算テンプレートの詳細を表示するためのアクセス許可を付与	読み取り	collaboration*		
			privacybudgettemplate*		
GetConfiguredAudienceModelAssociation	設定済みオーディエンスモデルの関連付けの詳細を表示するためのアクセス許可を付与	読み取り	configuredaudiencemodelassociation*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetConfiguredTable	設定済みテーブルの詳細を表示するアクセス許可を付与	読み取り	configuredtable*		
GetConfiguredTableAnalysisRule	設定済みテーブルの分析ルールを表示するアクセス許可を付与	読み取り	configuredtable*		
GetConfiguredTableAssociation	設定済みテーブルの関連付けの詳細を表示するアクセス許可を付与	読み取り	configuredtableassociation*		
GetConfiguredTableAssociationAnalysisRule	設定済みテーブル関連付けの分析ルールを表示する許可を付与する	読み取り	configuredtableassociation*		
GetIdMappingTable	ID マッピングテーブルの詳細を表示する許可を付与する	読み取り	idmappingtable*		
			membership*		
GetIdNamespaceAssociation	ID 名前空間の関連付けの詳細を表示する許可を付与する	読み取り	idnamespaceassociation*		entityresolution:GetIdNamespace
			membership*		
GetMembership	メンバーシップに関する詳細を表示するアクセス許可を付与	読み取り	membership*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetPrivacyBudgetTemplate	プライバシー予算テンプレートの詳細を表示するためのアクセス許可を付与	読み取り	privacybudgettemplate*		
GetProtectedJob	保護されたジョブを表示するアクセス許可を付与します	読み取り	membership*		
GetProtectedQuery	プロジェクトクエリを表示するアクセス許可を付与	読み取り	membership*		
GetSchema	スキーマの詳細を表示するアクセス許可を付与	読み取り	collaboration*		
			configuredtableassociation*		
GetSchemaAnalysisRule	スキーマに関連付けられている分析ルールを表示するアクセス許可を付与	読み取り	collaboration*		cleanrooms:GetSchema
			configuredtableassociation*		
ListAnalysisTemplates	利用可能な分析テンプレートを一覧表示するアクセス許可を付与	リスト	analysistemplate*		
			membership*		
ListCollaborationAnalysisTemplates	コラボレーション内の利用可能な分析テンプレートを一覧表示するアクセス許可を付与	リスト	collaboration*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListCollaborationConfiguredAudienceModelAssociations	コラボレーション内の利用可能な設定済みオーディエンスモデルの関連付けを一覧表示するためのアクセス許可を付与	リスト	collaboration*		
ListCollaborationIdNamespaceAssociations	コラボレーション内の ID 名前空間を一覧表示する許可を付与する	リスト	collaboration*		
ListCollaborationPrivacyBudgetTemplates	コラボレーション内の利用可能なプライバシー予算テンプレートを一覧表示するためのアクセス許可を付与	リスト	collaboration*		
ListCollaborationPrivacyBudgets	コラボレーション内のプライバシー予算を一覧表示するためのアクセス許可を付与	リスト	collaboration*		
ListCollaborations	利用可能なコラボレーションを一覧表示するアクセス許可を付与	リスト			
ListConfiguredAudienceModelAssociations	メンバーシップに利用可能な設定済みオーディエンスモデルの関連付けを一覧表示するためのアクセス許可を付与	リスト	configuredaudiencemodelassociation*		
			membership*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListConfiguredTableAssociations	メンバーシップに利用可能な設定済みテーブル関連付けを一覧表示するアクセス許可を付与	リスト	configuredtableassociation*		
			membership*		
ListConfiguredTables	利用可能な設定済みテーブルを一覧表示するアクセス許可を付与	リスト			
ListIdMappingTables	メンバーシップに使用可能な ID マッピングテーブルを一覧表示する許可を付与する	リスト	idmappingtable*		
			membership*		
ListIdNamespaceAssociations	メンバーシップのエンティティ解決データ関連付けを一覧表示する許可を付与する	リスト	idnamespaceassociation*		
			membership*		
ListMembers	コラボレーションからメンバーを一覧表示するアクセス許可を付与	リスト	collaboration*		
ListMemberships	利用可能なメンバーシップを一覧表示するアクセス許可を付与	リスト			
ListPrivacyBudgetTemplates	利用可能なプライバシー予算テンプレートを一覧表示するためのアクセス許可を付与	リスト	membership*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			privacybudgettemplate*		
ListPrivacyBudgets	利用可能なプライバシー予算を一覧表示するためのアクセス許可を付与	リスト	membership*		
ListProtectedJobs	保護されたジョブを一覧表示する許可を付与	リスト	membership*		
ListProtectedQueries	保護されたクエリを一覧表示するアクセス許可を付与	リスト	membership*		
ListSchemas	コラボレーションで使用可能なスキーマを表示するアクセス許可を付与	リスト	collaboration*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与。	リスト	analysistemplate		
			collaboration		
			configuredaudiencemodelassociation		
			configuredtable		
			configuredtableassociation		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			membership		
			privacybudgettemplate		
PassCollaboration [許可のみ]	Clean Rooms ML カスタムモデルのコンテキストでコラボレーションにアクセスする許可を付与	読み取り	collaboration*		
PassMembership [許可のみ]	Clean Rooms ML カスタムモデルのコンテキストでメンバーシップにアクセスする許可を付与	読み取り	membership*		
PopulateIdMappingTable	AWS エンティティ解決で ID マッピングジョブを開始し、クリーンルームコラボレーションで ID マッピング結果を生成するアクセス許可を付与します。	書き込み	idmappingtable*		entityresolution:GetIdMappingWorkflow
			membership*		
PreviewPrivacyImpact	プライバシー予算テンプレートの設定をプレビューするためのアクセス許可を付与	読み取り	membership*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartProtectedJob	保護されたジョブを開始する許可を付与	書き込み	membership*		cleanrooms:GetCollaborationAnalysisTemplate cleanrooms:GetSchema
			analysistemplate		
			configuredtableassociation		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartProtectedQuery	保護されたクエリを開始するアクセス許可を付与	書き込み	membership*		cleanrooms:GetCollaborationAnalysisTemplate cleanrooms:GetSchema s3:GetBucketLocation s3:ListBucket s3:PutObject
			analysistemplate		
			configuredtableassociation		
			idmappingtable		
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	analysistemplate		
			collaboration		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			configuredaudiencemodelassociation		
			configuredtable		
			configuredtableassociation		
			idmappingtable		
			idnamespaceassociation		
			membership		
			privacybudgettemplate		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	リソースのタグを解除する許可を付与	Tagging	analysistemplate		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			collaboration		
			configuredaudiencemodelassociation		
			configuredtable		
			configuredtableassociation		
			idmappingtable		
			idnamespaceassociation		
			membership		
			privacybudgettemplate		
				aws:TagKeys	
UpdateAnalysisTemplate	分析テンプレートの詳細を更新するアクセス許可を付与	書き込み	analysistemplate*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateCollaboration	コラボレーションの詳細を更新するアクセス許可を付与	書き込み	collaboration*		
UpdateConfiguredAudienceModelAssociation	設定済みオーディエンスモデルの関連付けを更新するためのアクセス許可を付与	書き込み	configuredaudiencemodelassociation*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateConfiguredTable	既存の設定済みテーブルを更新するアクセス許可を付与	書き込み	configuredtable*		athena:GetTableMetadata cleanrooms:UpdateConfiguredTableAllowedColumns cleanrooms:UpdateConfiguredTableReference glue:BatchGetPartition glue:GetDatabase glue:GetDatabases glue:GetPartition glue:GetPartitions

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					glue:GetSchemaVersion glue:GetTable glue:GetTables
UpdateConfiguredTableAllowedColumns [アクセス許可のみ]	既存の設定済みテーブルの許可された列を更新する許可を付与	書き込み	configuredtable*		
UpdateConfiguredTableAnalysisRule	設定済みテーブルの分析ルールを更新するアクセス許可を付与	書き込み	configuredtable*		
UpdateConfiguredTableAssociation	設定済みテーブル関連付けを更新するアクセス許可を付与	書き込み	configuredtableassociation*		iam:PassRole
UpdateConfiguredTableAssociationAnalysisRule	設定済みテーブル関連付けの分析ルールを更新する許可を付与する	書き込み	configuredtableassociation*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateConfiguredTableReference [アクセス許可のみ]	既存の設定済みテーブルのテーブルリファレンスを更新する許可を付与	書き込み	configuredtable*		
UpdateIdMappingTable	ID マッピングテーブルを更新する許可を付与する	書き込み	idmappingtable*		
			membership*		
UpdateIdNamespaceAssociation	エンティティ解決入力関連付けを更新する許可を付与する	書き込み	idnamespaceassociation*		entityresolution:GetIdNamespace
			membership*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateMembership	メンバーシップの詳細を更新するアクセス許可を付与	書き込み	membership*		iam:PassRole logs:CreateLogDelivery logs:CreateLogGroup logs:DeleteLogDelivery logs:DescribeLogGroups logs:DescribeResourcePolicies logs:GetLogDelivery logs:ListLogDeliveries logs:PutResourcePolicy

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					logs:UpdateLogDelivery s3:GetBucketLocation
UpdatePrivacyBudgetTemplate	プライバシー予算テンプレートの詳細を更新するためのアクセス許可を付与	書き込み	privacybudgettemplate*		
UpdateProtectedJob	保護されたジョブを更新する許可を付与	書き込み	membership*		
UpdateProtectedQuery	保護されたクエリを更新するアクセス許可を付与	書き込み	membership*		

AWS クリーンルームで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
analysistemplate	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/analysistemplate/${AnalysisTemplateId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
collaboration	arn:${Partition}:cleanrooms:${Region}:${Account}:collaboration/${CollaborationId}	aws:ResourceTag/${TagKey}
configuredaudiencemodelassociation	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/configuredaudiencemodelassociation/${ConfiguredAudienceModelAssociationId}	aws:ResourceTag/${TagKey}
configuredtable	arn:${Partition}:cleanrooms:${Region}:${Account}:configuredtable/${ConfiguredTableId}	aws:ResourceTag/${TagKey}
configuredtableassociation	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/configuredtableassociation/${ConfiguredTableAssociationId}	aws:ResourceTag/${TagKey}
idmappingtable	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/idmappingtable/${IdMappingTableId}	aws:ResourceTag/${TagKey}
idnamespaceassociation	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/idnamespaceassociation/${IdNamespaceAssociationId}	aws:ResourceTag/${TagKey}
membership	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
privacybudgettemplate	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/privacybudgettemplate/${PrivacyBudgetTemplateId}	aws:ResourceTag/${TagKey}

AWS クリーンルームの条件キー

AWS クリーンルームでは、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Clean Rooms ML のアクション、リソース、および条件キー

AWS Clean Rooms ML (サービスプレフィックス: cleanrooms-ml) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Clean Rooms ML で定義されるアクション
- AWS Clean Rooms ML で定義されるリソースタイプ
- AWS Clean Rooms ML の条件キー

AWS Clean Rooms ML で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelTrainedModel	トレーニング済みモデルをキャンセルするアクセス許可を付与します	書き込み	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CancelTrainedModelInferenceJob	トレーニング済みモデル推論ジョブをキャンセルするアクセス許可を付与します	書き込み	TrainedModelInferenceJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateAudienceModel	オーディエンスモデルを作成するためのアクセス許可を付与	書き込み	trainingdataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguredAudienceModel	設定済みオーディエンスモデルを作成するためのアクセス許可を付与	書き込み	audiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguredModelAlgorithm	設定されたモデルアルゴリズムを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguredModelAlgorithmAssociation	設定されたモデルアルゴリズムの関連付けを作成するアクセス許可を付与します	書き込み	ConfiguredModelAlgorithm*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMLInputChannel	ML 入力チャネルを作成するアクセス許可を付与します	書き込み	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrainedModel	トレーニング済みモデルを作成するアクセス許可を付与します	書き込み	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateTrainingDataset	トレーニングデータセットまたはシードオーディエンスを作成するためのアクセス許可を付与 Clean Rooms ML では、TrainingDataSet は Glue テーブルにポイントするメタデータであり、AudienceModel の作成時にのみ読み込まれます。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAudienceGenerationJob	指定されたオーディエンス生成ジョブを削除し、ジョブに関連付けられているすべてのデータを削除するためのアクセス許可を付与	書き込み	audiencegenerationjob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAudienceModel	指定されたオーディエンス生成ジョブを削除し、ジョブに関連付けられているすべてのデータを削除するためのアクセス許可を付与	書き込み	audiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredAudienceModel	指定された設定済みオーディエンスモデルを削除するためのアクセス許可を付与	書き込み	configuredaudiencemodel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredAudienceModelPolicy	指定された設定済みオーディエンスモデルポリシーを削除するためのアクセス許可を付与	書き込み	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredModelAlgorithm	設定されたモデルアルゴリズムを削除するアクセス許可を付与します	書き込み	ConfiguredModelAlgorithm*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredModelAlgorithmAssociation	設定されたモデルアルゴリズムの関連付けを削除するアクセス許可を付与します	書き込み	ConfiguredModelAlgorithmAssociation*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMLConfiguration	ML 設定を削除するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMLInputChannelData	ML 入力チャネルに関連付けられているすべてのデータを削除するアクセス許可を付与します	書き込み	MLInputChannel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTrainedModelOutput	トレーニング済みモデルに関連付けられているすべての出力を削除するアクセス許可を付与します	書き込み	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteTrainingDataset	トレーニングデータセットを削除するためのアクセス許可を付与	書き込み	trainingdataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetAudienceGenerationJob	オーディエンス生成ジョブに関する情報を返すためのアクセス許可を付与	読み取り	audiencegenerationjob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetAudienceModel	オーディエンスモデルに関する情報を返すためのアクセス許可を付与	読み取り	audiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetCollaborationConfiguredModelAlgorithmAssociation	コラボレーションのメンバーによって作成された設定されたモデルアルゴリズムの関連付けに関する情報を返すアクセス許可を付与します	読み取り	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
GetCollaborationMLInputChannel	コラボレーションのメンバーによって作成された ML 入力チャネルに関する情報を返すアクセス許可を付与します	読み取り	MLInputChannel*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetCollaborationTrainedModel	コラボレーションのメンバーによって作成されたトレーニング済みモデルに関する情報を返すアクセス許可を付与します	読み取り	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
GetConfiguredAudienceModel	設定済みオーディエンスモデルに関する情報を返すためのアクセス許可を付与	読み取り	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetConfiguredAudienceModelPolicy	設定済みオーディエンスモデルポリシーに関する情報を返すためのアクセス許可を付与	読み取り	configuredaudiencemodel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
GetConfiguredModelAlgorithm	設定されたモデルアルゴリズムに関する情報を返すアクセス許可を付与します	読み取り	ConfiguredModelAlgorithm*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetConfiguredModelAlgorithmAssociation	設定されたモデルアルゴリズムの関連付けに関する情報を返すアクセス許可を付与します	読み取り	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetMLConfiguration	ML 設定に関する情報を返すアクセス許可を付与します	読み取り		aws:RequestTag/${TagKey} aws:TagKeys	
GetMLInputChannel	ML 入力チャネルに関する情報を返すアクセス許可を付与します	読み取り	MLInputChannel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetTrainedModel	トレーニング済みモデルに関する情報を返すアクセス許可を付与します	読み取り	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetTrainedModelInferenceJob	トレーニング済みモデル推論ジョブに関する情報を返すアクセス許可を付与します	読み取り	TrainedModelInferenceJob*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
GetTrainingDataset	トレーニングデータセットに関する情報を返すためのアクセス許可を付与	読み取り	trainingdataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListAudienceExportJobs	オーディエンスエクスポートジョブのリストを返すためのアクセス許可を付与	リスト	audiencegenerationjob		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListAudienceGenerationJobs	オーディエンス生成ジョブのリストを返すためのアクセス許可を付与	リスト	configuredaudiencemodel		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
ListAudienceModels	オーディエンスモデルのリストを返すためのアクセス許可を付与	リスト			
ListCollaborationConfiguredModelAlgorithmAssociations	コラボレーションのメンバーによって作成された設定済みモデルアルゴリズムのリストを返すアクセス許可を付与します	リスト		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
ListCollaborationMLInputChannels	コラボレーションのメンバーによって作成された ML 入力チャネルのリストを返すアクセス許可を付与します	リスト		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListCollaborationTrainedModelExportJobs	コラボレーションのメンバーによって開始されたトレーニング済みモデルエクスポートジョブのリストを返すアクセス許可を付与します	リスト	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
ListCollaborationTrainedModelInferenceJobs	コラボレーションのメンバーによって開始されたトレーニング済みモデル推論ジョブのリストを返すアクセス許可を付与します	リスト		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListCollaborationTrainedModels	コラボレーションのメンバーによって作成されたトレーニング済みモデルのリストを返すアクセス許可を付与します	リスト		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
ListConfiguredAudienceModels	設定済みオーディエンスモデルのリストを返すためのアクセス許可を付与	リスト			
ListConfiguredModelAlgorithmAssociations	設定されたモデルアルゴリズムの関連付けのリストを返すアクセス許可を付与します	リスト		aws:RequestTag/${TagKey} aws:TagKeys	
ListConfiguredModelAlgorithms	設定されたモデルアルゴリズムのリストを返すアクセス許可を付与します	リスト		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListMLInputChannels	ML 入力チャネルのリストを返すアクセス許可を付与します	リスト		aws:RequestTag/${TagKey} aws:TagKeys	
ListTagsForResource	指定されたリソースのタグのリストを返すためのアクセス許可を付与	リスト	audiencegenerationjob		
			audiencemodel		
			configuredaudiencemodel		
			trainingdataset		
				aws:TagKeys aws:ResourceTag/${TagKey}	
ListTrainedModelInferenceJobs	トレーニング済みモデル推論ジョブのリストを返すアクセス許可を付与します	リスト		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTrainedModelVersions	トレーニング済みモデルバージョンのリストを返すアクセス許可を付与します	リスト		aws:RequestTag/${TagKey} aws:TagKeys	
ListTrainedModels	トレーニング済みモデルのリストを返すアクセス許可を付与します	リスト		aws:RequestTag/${TagKey} aws:TagKeys	
ListTrainingDatasets	トレーニングデータセットのリストを返すためのアクセス許可を付与	リスト			
PutConfiguredAudienceModelPolicy	設定済みオーディエンスモデルのリソースポリシーを作成または更新するためのアクセス許可を付与	権限の管理	configuredaudiencemodel*		
PutMLConfiguration	ML 設定を配置するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
StartAudienceExportJob	オーディエンスを生成した後に、指定したサイズのオーディエンスをエクスポートするためのアクセス許可を付与	書き込み	audiencegenerationjob*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
StartAudienceGenerationJob	オーディエンス生成ジョブを開始するためのアクセス許可を付与	書き込み	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
StartTrainedModelExportJob	トレーニング済みモデルエクスポートジョブを開始するアクセス許可を付与します	書き込み	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartTrainedModelInferenceJob	トレーニング済みモデル推論ジョブを開始する許可を付与	書き込み	ConfiguredModelAlgorithmAssociation*		
			MLInputChannel*		
			TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	特定のリソースにタグを付けるためのアクセス許可を付与	Tagging	ConfiguredModelAlgorithm		
			ConfiguredModelAlgorithmAssociation		
			MLInputChannel		
			TrainedModel		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			TrainedModelInferenceJob		
			audiencegenerationjob		
			audiencemodel		
			configuredaudiencemodel		
			trainingdataset		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UnTagResource	特定のリソースのタグを解除するためのアクセス許可を付与	Tagging	ConfiguredModelAlgorithm		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			ConfiguredModelAlgorithmAssociation		
			MLInputChannel		
			TrainedModel		
			TrainedModelInferenceJob		
			audiencegenerationjob		
			audiencemodel		
			configuredaudiencemodel		
			trainingdataset		
				aws:TagKeys aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateConfiguredAudienceModel	設定済みオーディエンスモデルを更新するためのアクセス許可を付与	書き込み	configuredaudiencemodel*		
			audiencemodel		
				aws:RequestTag/${TagKey} aws:TagKeys	

AWS Clean Rooms ML で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
trainingdataset	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:training-dataset/${ResourceId}	aws:ResourceTag/${TagKey}
audiencemodel	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:audience-model/${ResourceId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
configuredaudiencemodel	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:configured-audience-model/${ResourceId}	aws:ResourceTag/${TagKey}
audiencegenerationjob	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:audience-generation-job/${ResourceId}	aws:ResourceTag/${TagKey}
ConfiguredModelAlgorithm	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:configured-model-algorithm/${ResourceId}	aws:ResourceTag/${TagKey}
ConfiguredModelAlgorithmAssociation	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:membership/${MembershipId}/configured-model-algorithm-association/${ResourceId}	aws:ResourceTag/${TagKey}
MLInputChannel	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:membership/${MembershipId}/ml-input-channel/${ResourceId}	aws:ResourceTag/${TagKey}
TrainedModel	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:membership/${MembershipId}/trained-model/${ResourceId}	aws:ResourceTag/${TagKey}
TrainedModelInferenceJob	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:membership/${MembershipId}/trained-model-inference-job/${ResourceId}	aws:ResourceTag/${TagKey}

AWS Clean Rooms ML の条件キー

AWS Clean Rooms ML では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString
cleanrooms-ml:CollaborationId	クリーンルームコラボレーション ID でアクセスをフィルタリングします	String

AWS クラウド Control API のアクション、リソース、および条件キー

AWS クラウド Control API (サービスプレフィックス: cloudformation) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS クラウド Control API で定義されているアクション
- AWS クラウド Control API で定義されているリソースタイプ
- AWS クラウド Control API の条件キー

AWS クラウド Control API で定義されているアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelResourceRequest	アカウント内のリソースリクエストをキャンセルするためのアクセス許可を付与	書き込み			
CreateResource	アカウント内にリソースを作成するためのアクセス許可を付与	書き込み			
DeleteResource	アカウント内のリソースを削除するためのアクセス許可を付与	書き込み			
GetResource	アカウント内のリソースを取得するためのアクセス許可を付与	読み取り			
GetResourceRequestStatus	アカウント内のリソースリクエストを取得するためのアクセス許可を付与	読み取り			
ListResourceRequests	アカウント内のリソースリクエストを一覧表示するためのアクセス許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListResources	アカウント内のリソースを一覧表示するためのアクセス許可を付与	読み取り			
UpdateResource	アカウント内のリソースを更新するためのアクセス許可を付与	書き込み			

AWS クラウド Control API で定義されているリソースタイプ

AWS クラウド Control API は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS クラウド Control API へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS クラウド Control API の条件キー

Cloud Control API には、ポリシーステートメントの `Condition` 要素で使用できるような、サービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Cloud Directory のアクション、リソース、および条件キー

Amazon Cloud Directory (サービスプレフィックス: `clouddirectory`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Cloud Directory で定義されるアクション
- Amazon Cloud Directory で定義されるリソースタイプ
- Amazon Cloud Directory の条件キー

Amazon Cloud Directory で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddFacetToObject	オブジェクトに新しいファセットを追加するアクセス許可を付与します	書き込み	directory*		
ApplySchema	入力された発行済みスキーマを、発行済みスキーマと同じ名前とバージョンでディレクトリにコピーするアクセス許可を付与します	書き込み	directory* publishedSchema*		
AttachObject	既存のオブジェクトを別の既存のオブジェクトにアタッチするアクセス許可を付与します	書き込み	directory*		
AttachPolicy	ポリシーオブジェクトを他のオブジェクトにアタッチするアクセス許可を付与します	書き込み	directory*		
AttachToIndex	指定されたオブジェクトを指定されたインデックスにアタッチするアクセス許可を付与します	書き込み	directory*		
AttachTypedLink	ソースとターゲットオブジェクトリファレンス間に型付きリンクをアタッチするアクセス許可を付与します	書き込み	directory*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchRead	バッチ内のすべての読み取りオペレーションを実行するアクセス許可を付与します。BatchRead 内の各オペレーションに明示的にアクセス許可を付与する必要があります	読み取り	directory*		
BatchWrite	バッチ内のすべての書き込みオペレーションを実行するアクセス許可を付与します。BatchWrite 内の各オペレーションに明示的にアクセス許可を付与する必要があります	書き込み	directory*		
CreateDirectory	発行済みスキーマをディレクトリにコピーしてディレクトリを作成するアクセス許可を付与します	書き込み	publishedSchema*		
CreateFacet	スキーマで新しいファセットを作成するアクセス許可を付与します	書き込み	appliedSchema*		
			developmentSchema*		
CreateIndex	インデックスオブジェクトを作成するアクセス許可を付与します	書き込み	directory*		
CreateObject	ディレクトリにオブジェクトを作成するアクセス許可を付与します	書き込み	directory*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSchema	開発状態の新しいスキーマを作成するアクセス許可を付与します	書き込み			
CreateTypedLinkFacet	スキーマで新しい型付きリンクファセットを作成するアクセス許可を付与します	書き込み	appliedSchema*		
			developmentSchema*		
DeleteDirectory	ディレクトリを削除するアクセス許可を付与します。無効のディレクトリのみを削除できます	書き込み	directory*		
DeleteFacet	特定のファセットを削除するアクセス許可を付与します。ファセットに関連付けられているすべての属性とルールが削除されます	書き込み	developmentSchema*		
DeleteObject	オブジェクトとそれに関連する属性を削除するアクセス許可を付与します	書き込み	directory*		
DeleteSchema	特定のスキーマを削除するアクセス許可を付与します	書き込み	developmentSchema*		
			publishedSchema*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteTypedLinkFacet	特定の TypedLink ファセットを削除するアクセス許可を付与します。ファセットに関連付けられているすべての属性とルールが削除されます	書き込み	developmentSchema*		
DetachFromIndex	指定されたインデックスから指定されたオブジェクトをデタッチするアクセス許可を付与します	書き込み	directory*		
DetachObject	親オブジェクトから特定のオブジェクトをデタッチするアクセス許可を付与します	書き込み	directory*		
DetachPolicy	オブジェクトからポリシーをデタッチするアクセス許可を付与します	書き込み	directory*		
DetachTypedLink	特定のソースとターゲットオブジェクトリファレンス間の特定の型付きリンクをデタッチするアクセス許可を付与します	書き込み	directory*		
DisableDirectory	指定されたディレクトリを無効にするアクセス許可を付与します	書き込み	directory*		
EnableDirectory	指定されたディレクトリを有効にするアクセス許可を付与します	書き込み	directory*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetAppliedSchemaVersion	使用中のマイナーバージョンを含む、現在適用されているスキーマバージョン ARN を返すアクセス許可を付与します	読み取り	appliedSchema*		
GetDirectory	ディレクトリに関するメタデータを取得するアクセス許可を付与します	読み取り	directory*		
GetFacet	ファセット名、属性、ルール、ObjectType など、ファセットの詳細を取得するアクセス許可を付与します	読み取り	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
GetLinkAttributes	型付きリンクに関連付けられている属性を取得するアクセス許可を付与します	読み取り	directory*		
GetObjectAttributes	オブジェクトに関連付けられているファセット内の属性を取得するアクセス許可を付与します	読み取り	directory*		
GetObjectInformation	オブジェクトに関するメタデータを取得するアクセス許可を付与します	読み取り	directory*		
GetSchemaAsJson	スキーマの JSON 表現を取得するアクセス許可を付与します	読み取り	appliedSchema*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			developmentSchema*		
			publishedSchema*		
GetTypedLinkFacetInformation	特定の型付きリンクのファセットに関連付けられているアイデンティティ属性の注文情報を返すアクセス許可を付与します	読み取り	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
ListAppliedSchemaArns	ディレクトリに適用されているスキーマを一覧表示するアクセス許可を付与します	リスト	directory*		
ListAttachedIndices	オブジェクトにアタッチされているインデックスを一覧表示するアクセス許可を付与します	読み取り	directory*		
ListDevelopmentSchemaArns	開発状態のスキーマの ARN を取得するアクセス許可を付与します	リスト			
ListDirectories	アカウント内で作成されたディレクトリを一覧表示するアクセス許可を付与します	リスト			
ListFacetAttributes	ファセットにアタッチされている属性を取得するアクセス許可を付与します	読み取り	appliedSchema*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			developmentSchema*		
			publishedSchema*		
ListFacetNames	スキーマに存在するファセット名を取得するアクセス許可を付与します	読み取り	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
ListIncomingTypedLinks	特定のオブジェクトに対するすべての着信 TypedLinks の、ページ分割されたリストを返すアクセス許可を付与します	読み取り	directory*		
ListIndex	指定されたインデックスにアタッチされているオブジェクトを一覧表示するアクセス許可を付与します	読み取り	directory*		
ListManagedSchemaArns	各マネージドスキーマのメジャーバージョンファミリーを一覧表示するアクセス許可を付与します。メジャーバージョン ARN が SchemaArn として提供されている場合は、そのファミリーのマイナーバージョンリビジョンが代わりに一覧表示されます	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListObjectAttributes	オブジェクトに関連付けられているすべての属性を一覧表示するアクセス許可を付与します	読み取り	directory*		
ListObjectChildren	特定のオブジェクトに関連付けられた子オブジェクトの、ページ分割されたリストを返すアクセス許可を付与します	読み取り	directory*		
ListObjectParentPaths	任意のオブジェクトタイプ (ノード、リーフノード、ポリシーノード、インデックスノードオブジェクトなど) で利用できる親パスをすべて取得するアクセス許可を付与します	読み取り	directory*		
ListObjectParents	特定のオブジェクトに関連付けられている親オブジェクトをページ分割した形で一覧表示するアクセス許可を付与します	読み取り	directory*		
ListObjectPolicies	オブジェクトにアタッチされているポリシーをページ分割した形で返すアクセス許可を付与します	読み取り	directory*		
ListOutgoingTypedLinks	特定のオブジェクトに対するすべての TypedLinks 送信の、ページ分割したリストを返すアクセス許可を付与します	読み取り	directory*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListPolicyAttachments	特定のポリシーがアタッチされているすべての ObjectIdentifier を返すアクセス許可を付与します	読み取り	directory*		
ListPublishedSchemaArns	発行されたスキーマ ARN を取得するアクセス許可を付与します	リスト			
ListTagsForResource	リソースのタグを返すアクセス許可を付与します	読み取り	directory*		
ListTypedLinkFacetAttributes	型付きリンクのファセットに関連付けられた属性を、ページ分割したリストとして返すアクセス許可を付与します	読み取り	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
ListTypedLinkFacetNames	スキーマに存在する型付きリンクのファセット名を、ページ分割したリストとして返すアクセス許可を付与します	読み取り	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
LookupPolicy	指定されたオブジェクトへのディレクトリのルートからすべてのポリシーを一覧表示するアクセス許可を付与します	読み取り	directory*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PublishSchema	開発スキーマをバージョンとともに発行するアクセス許可を付与します	書き込み	developmentSchema*		
PutSchemaFromJson	JSON アップロードを使用してスキーマを更新するアクセス許可を付与します。開発スキーマにのみ使用できます	書き込み			
RemoveFacetFromObject	指定されたオブジェクトから指定されたファセットを削除するアクセス許可を付与します	書き込み	directory*		
TagResource	リソースにタグを追加するアクセス許可を付与します	タグ付け	directory*		
UntagResource	リソースからタグを削除する許可を付与	Tagging	directory*		
UpdateFacet	ファセットの既存の属性、ルール、ObjectType を追加/更新/削除するアクセス許可を付与します	書き込み	appliedSchema*		
			developmentSchema*		
UpdateLinkAttributes	特定の型付きリンクの属性を更新するアクセス許可を付与します。更新する属性を、その IdentityAttributeOrder で定義された型付きリンクのアイデンティティに関与させないでください	書き込み	directory*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateObjectAttributes	特定のオブジェクトの属性を更新するアクセス許可を付与します	書き込み	directory*		
UpdateSchema	スキーマ名を新しい名前で更新するアクセス許可を付与します	書き込み	developmentSchema*		
UpdateTypedLinkFacet	TypedLink ファセットの既存の属性、ルール、アイデンティティ属性の順序を追加/更新/削除するアクセス許可を付与します	書き込み	developmentSchema*		
UpgradeAppliedSchema	MinorVersion で見つかったスキーマ更新で PublishedSchemaArn を使用して、単一のディレクトリをインプレースでアップグレードするアクセス許可を付与します。下位互換のマイナーバージョンアップグレードは、ディレクトリ内のすべてのオブジェクトのリーダーがすぐに利用できます	書き込み	directory* publishedSchema*		
UpgradePublishedSchema	DevelopmentSchemaArn の現在のコンテンツを使用して、新しいマイナーバージョンリビジョンで発行されたスキーマをアップグレードするアクセス許可を付与します	書き込み	developmentSchema* publishedSchema*		

Amazon Cloud Directory で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
appliedSchema	arn:${Partition}:clouddirectory:${Region}:${Account}:directory/${DirectoryId}/schema/${SchemaName}/${Version}	
developmentSchema	arn:${Partition}:clouddirectory:${Region}:${Account}:schema/development/${SchemaName}	
directory	arn:${Partition}:clouddirectory:${Region}:${Account}:directory/${DirectoryId}	
publishedSchema	arn:${Partition}:clouddirectory:${Region}:${Account}:schema/published/${SchemaName}/${Version}	

Amazon Cloud Directory の条件キー

Cloud Directory には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS「グローバル条件コンテキストキー」を参照してください。

AWS クラウド Map のアクション、リソース、および条件キー

AWS クラウド Map (サービスプレフィックス: servicediscovery) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS クラウド Map で定義されるアクション
- AWS クラウド Map で定義されるリソースタイプ
- AWS クラウド Map の条件キー

AWS クラウド Map で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateHttpNamespace	HTTP 名前空間を作成する権限を付与します。	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreatePrivateDnsNamespace	DNS に基づいてプライベート名前空間 (指定された Amazon VPC 内でのみ表示される名前空間) を作成する権限を付与します	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreatePublicDnsNamespace	DNS に基づいてパブリック名前空間 (インターネットで表示される名前空間) を作成する権限を付与します	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateService	サービスを作成する許可を付与	書き込み	namespace* service*		
				servicediscovery:NamespaceArn aws:TagKeys aws:RequestTag/${TagKey}	
DeleteNamespace	指定された名前空間を削除する権限を付与します	書き込み	namespace*		
DeleteResourcePolicy [アクセス許可のみ]	名前空間の RAM アクセスコントロールポリシーを削除するアクセス許可を付与します	書き込み	namespace*		
DeleteService	指定されたサービスを削除する権限を付与します	書き込み	service*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				servicediscovery:ServiceCreatedByAccount	
DeleteServiceAttributes	サービスから指定された属性を削除するアクセス許可を付与します	書き込み	service*		
				servicediscovery:ServiceCreatedByAccount	
DeregisterInstance	指定されたインスタンスについて Amazon Route 53 が作成したリソースとヘルスチェック (存在する場合) を削除します	書き込み	service*		
				servicediscovery:ServiceArn servicediscovery:ServiceCreatedByAccount	
DiscoverInstances	指定された名前空間とサービスの登録済みインスタンスを検出する権限を付与します	読み取り	namespace*		
			service*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				servicediscovery:NamespaceName servicediscovery:ServiceName	
DiscoverInstancesRevision	指定された名前空間とサービスのインスタンスのリビジョンを検出するための許可を付与します	読み取り	namespace*		
			service*		
				servicediscovery:NamespaceName servicediscovery:ServiceName	
GetInstance	指定されたインスタンスに関する情報を取得する権限を付与します	読み込み	service*		
				servicediscovery:ServiceArn	
GetInstancesHealthStatus	1 つまたは複数のインスタンスの現在の正常性ステータス (正常、異常、または不明) を取得する権限を付与します	読み込み	service*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				servicediscovery:ServiceArn	
GetNamespace	名前空間に関する情報を取得する権限を付与します	読み込み	namespace*		
GetOperation	オペレーションに関する情報を取得する権限を付与します	読み取り	namespace*		
			service		
GetResourcePolicy [許可のみ]	名前空間の RAM アクセスコントロールポリシーを読み取るアクセス許可を付与します	読み取り	namespace*		
GetService	指定されたサービスの設定を取得する権限を付与します	読み取り	service*		
GetServiceAttributes	指定されたサービスの属性を取得するアクセス許可を付与します	読み取り	service*		
ListInstances	指定されたサービスに登録されていたインスタンスに関する概要情報を取得する権限を付与します	読み込み	service*		
				servicediscovery:ServiceArn	
ListNamespaces	名前空間に関する情報を取得する権限を付与します	読み込み			
ListOperations	指定する基準に一致するオペレーションを一覧表示する権限を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListServices	指定されたフィルターに一致するすべてのサービスの設定を取得する権限を付与します	読み込み			
ListTagsForResource	指定されたリソースのタグを一覧表示する権限を付与します	読み取り			
PutResourcePolicy [許可のみ]	名前空間の RAM アクセスコントロールポリシーを定義するアクセス許可を付与します	書き込み	namespace*		
RegisterInstance	指定されたサービスの設定に基づいてインスタンスを登録する権限を付与します	書き込み	service*		
				servicediscovery:ServiceArn servicediscovery:ServiceCreatedByAccount	
TagResource	指定されたリソースに 1 つ以上のタグを追加する権限を付与します	タグ付け		aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	指定されたリソースから 1 つ以上のタグを削除する権限を付与します	Tagging		aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateHttpNamespace	HTTP 名前空間の設定を更新する許可を付与	書き込み	namespace*		
UpdateInstanceCustomHealthStatus	カスタムヘルスチェックが実行されるインスタンスの現在のヘルスステータスを更新する権限を付与します	書き込み	service*		
				servicediscovery:ServiceArn servicediscovery:ServiceCreatedByAccount	
UpdatePrivateDnsNamespace	プライベート DNS 名前空間の設定を更新する許可を付与	書き込み	namespace*		
UpdatePublicDnsNamespace	パブリック DNS 名前空間の設定を更新する許可を付与	書き込み	namespace*		
UpdateService	指定されたサービス内の設定を更新する権限を付与します	書き込み	service*		
				servicediscovery:ServiceCreatedByAccount	
UpdateServiceAttributes	指定されたサービスの属性を更新するアクセス許可を付与します	書き込み	service*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				servicediscovery:ServiceCreatedByAccount	

AWS クラウド Map で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
namespace	arn:${Partition}:servicediscovery:${Region}:${Account}:namespace/${NamespaceId}	aws:ResourceTag/${TagKey}
service	arn:${Partition}:servicediscovery:${Region}:${Account}:service/${ServiceId}	aws:ResourceTag/${TagKey}

AWS クラウド Map の条件キー

AWS クラウド Map では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします。	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられているタグに基づいてアクションをフィルタリングします。	文字列
aws:TagKeys	リクエストで渡されたタグキーに基づいてアクションをフィルタリングします。	ArrayOfString
servicediscovery:NamespaceArn	関連する名前空間の Amazon リソースネーム (ARN) を指定してアクセスをフィルタリングします	ARN
servicediscovery:NamespaceName	関連する名前空間の名前を指定してアクセスをフィルタリングします	文字列
servicediscovery:ServiceArn	関連サービスの Amazon リソースネーム (ARN) を指定してアクセスをフィルタリングします	ARN
servicediscovery:ServiceCreatedByAccount	関連するサービス作成者のアカウント ID を指定してアクセスをフィルタリングします	String
servicediscovery:ServiceName	関連サービスの名前を指定してアクセスをフィルタリングします	文字列

AWS Cloud9 のアクション、リソース、および条件キー

AWS Cloud9 (サービスプレフィックス: cloud9) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Cloud9 で定義されるアクション
- AWS Cloud9 で定義されるリソースタイプ
- AWS Cloud9 の条件キー

AWS Cloud9 で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ActivateEC2Remote [アクセス許可のみ]	AWS Cloud9 IDE が接続する Amazon EC2 インスタンスを起動するアクセス許可を付与します	書き込み	environment*		
CreateEnvironmentEC2	AWS Cloud9 開発環境を作成し、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを起動して、インスタンスで環境をホストするアクセス許可を付与します	書き込み		cloud9:EnvironmentName cloud9:InstanceType cloud9:SubnetId cloud9:UserArn	ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				cloud9:OwnerArn aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironmentMembership	AWS Cloud9 開発環境に環境メンバーを追加する許可を付与	書き込み	environment*		
				cloud9:UserArn cloud9:EnvironmentId cloud9:Permissions	
CreateEnvironmentSSH [アクセス許可のみ]	AWS Cloud9 SSH 開発環境を作成する許可を付与	書き込み		cloud9:EnvironmentName cloud9:OwnerArn aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateEnvironmentToken [アクセス許可のみ]	AWS Cloud9 IDE とユーザーの環境間の接続を許可する認証トークンを作成するアクセス許可を付与します	読み取り	environment*		
DeleteEnvironment	AWS Cloud9 開発環境を削除するアクセス許可を付与します。環境が Amazon Elastic Compute Cloud (Amazon EC2) インスタンスでホストされている場合は、インスタンスも終了します。	書き込み	environment*		iam:CreateServiceLinkedRole
DeleteEnvironmentMembership	AWS Cloud9 開発環境から環境メンバーを削除するアクセス許可を付与します	書き込み	environment*		
				cloud9:UserArn cloud9:EnvironmentId	
DescribeEC2Remote [アクセス許可のみ]	ホスト、ユーザー、ポートを含む、EC2 開発環境への接続に関する詳細を取得する許可を付与	読み取り	environment*		
DescribeEnvironmentMemberships	AWS Cloud9 開発環境の環境メンバーに関する情報を取得する許可を付与	読み取り	environment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				cloud9:UserArn cloud9:EnvironmentId	
DescribeEnvironmentStatus	AWS Cloud9 開発環境のステータス情報を取得する許可を付与	読み取り	environment*		
DescribeEnvironments	AWS Cloud9 開発環境に関する情報を取得する許可を付与	読み取り	environment*		
DescribeSSHRemote [許可のみ]	ホスト、ユーザー、ポートを含む、SSH 開発環境への接続に関する詳細を取得する許可を付与	読み込み	environment*		
GetEnvironmentConfig [許可のみ]	AWS Cloud9 IDE の初期化に使用される設定情報を取得する許可を付与	読み取り	environment*		
GetEnvironmentSettings [許可のみ]	指定された開発環境の AWS Cloud9 IDE 設定を取得する許可を付与	読み取り	environment*		
GetMembershipSettings [許可のみ]	指定された環境メンバーの AWS Cloud9 IDE 設定を取得する許可を付与	読み取り	environment*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetMigrationExperiences [許可のみ]	Cloud9 ユーザーの移行エクスペリエンスを取得する許可を付与	読み取り			
GetUserPublicKey [許可のみ]	Cloud AWS Cloud9 が SSH 開発環境に接続するために使用する、ユーザーのパブリック SSH キーを取得するアクセス許可を付与します	読み取り		cloud9:UserArn	
GetUserSettings [許可のみ]	指定されたユーザーの AWS Cloud9 IDE 設定を取得する許可を付与	読み取り			
ListEnvironments	AWS Cloud9 開発環境識別子のリストを取得する許可を付与	読み取り			
ListTagsForResource	Cloud9 環境のタグを一覧表示する許可を付与	読み込み	environment*		
ModifyTemporaryCredentialsOnEnvironmentEC2 [許可のみ]	AWS Cloud9 統合開発環境 (IDE) で使用される Amazon EC2 インスタンスに AWS マネージドー時認証情報を設定するアクセス許可を付与します	書き込み	environment*		
TagResource	Cloud9 環境にタグを追加する許可を付与	Tagging	environment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Cloud9 環境からタグを削除する許可を付与	Tagging	environment*		
				aws:TagKeys	
UpdateEnvironment	既存の AWS Cloud9 開発環境の設定を変更するアクセス許可を付与します	書き込み	environment*		
UpdateEnvironmentMembership	AWS Cloud9 開発環境の既存の環境メンバーの設定を変更するアクセス許可を付与します	書き込み	environment*		
				cloud9:UserArn cloud9:EnvironmentId cloud9:Permissions	
UpdateEnvironmentSettings [アクセス許可のみ]	指定された開発環境の AWS Cloud9 IDE 設定を更新する許可を付与	書き込み	environment*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateMembershipSettings [アクセス許可のみ]	指定された環境メンバーの AWS Cloud9 IDE 設定を更新する許可を付与	書き込み	environment*		
UpdateSSHRemote [アクセス許可のみ]	ホスト、ユーザー、ポートを含む、SSH 開発環境への接続に関する詳細を更新する許可を付与	書き込み	environment*		
UpdateUserSettings [アクセス許可のみ]	AWS Cloud9 ユーザーの IDE 固有の設定を更新する許可を付与	書き込み			

AWS Cloud9 で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
environment	`arn:${Partition}:cloud9:${Region}:${Account}:environment:${ResourceId}`	aws:ResourceTag/${TagKey}

AWS Cloud9 の条件キー

AWS Cloud9 では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString
cloud9:EnvironmentId	AWS Cloud9 環境 ID でアクセスをフィルタリングします	String
cloud9:EnvironmentName	AWS Cloud9 環境名でアクセスをフィルタリングします	String
cloud9:InstanceType	AWS Cloud9 環境の Amazon EC2 インスタンスのインスタンスタイプでアクセスをフィルタリングします	String
cloud9:OwnerArn	指定されたオーナー ARN でアクセスをフィルタリングします。	ARN
cloud9:Permissions	AWS Cloud9 アクセス許可のタイプでアクセスをフィルタリングします	String
cloud9:SubnetId	AWS Cloud9 環境が作成されるサブネット ID でアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
cloud9:UserArn	指定されたユーザー ARN でアクセスをフィルタリングします。	ARN

AWS CloudFormation のアクション、リソース、および条件キー

AWS CloudFormation (サービスプレフィックス: `cloudformation`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS CloudFormation で定義されるアクション
- AWS CloudFormation で定義されるリソースタイプ
- AWS CloudFormation の条件キー

AWS CloudFormation で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ActivateOrganizationsAccess	StackSet と Organization 間の信頼できるアクセスを有効にする許可を付与します。StackSet と Organization 間の信頼されたアクセスが有効になっていると、管理アカウントには、組織の StackSets を	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	作成および管理するためのアクセス許可が与えられます。				
ActivateType	公開されたサードパーティー拡張機能をアクティブ化するためのアクセス許可を付与し、スタックテンプレートで使用できるようにする	書き込み			
BatchDescribeTypeConfigurations	指定した CloudFormation 拡張機能の設定データを返すためのアクセス許可を付与	読み取り			
CancelUpdateStack	指定されたスタックの更新をキャンセルするアクセス許可を付与	Write	stack*		
ContinueUpdateRollback	UPDATE_ROLLBACK_FAILED 状態のスタックについて、UPDATE_ROLLBACK_COMPLETE 状態になるようロールバックを続けるアクセス許可を付与	Write	stack*		
				cloudformation:RoleArn	
CreateChangeSet	スタックの変更のリストを作成するアクセス許可を付与	書き込み	stack*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				cloudformation:ChangeSetName cloudformation:ResourceTypes cloudformation:ImportResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateGeneratedTemplate	CloudFormation でまだ管理されていない既存のリソースからテンプレートを作成する許可を付与する	書き込み			
CreateStack	テンプレートで指定されたスタックを作成するアクセス許可を付与	Write	stack*	cloudformation:ResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateStackInstances	指定されたリージョン内で指定されたアカウントのスタックインスタンスを作成するアクセス許可を付与	書き込み	stackset*		
			stackset-target		
			type		
				aws:TagKeys cloudformation:TargetRegion	
CreateStackRefactor	スタックリファクタリングを作成するアクセス許可を付与します	書き込み	stack*		
CreateStackSet	テンプレートで指定されたスタックセットを作成するアクセス許可を付与	Write		cloudformation:RoleArn cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateUploadBucket [アクセス許可のみ]	Amazon S3 バケットにテンプレートをアップロードするアクセス許可を付与 AWS CloudFormation コンソールでのみ使用され、API リファレンスには記載されていません	書き込み			
DeactivateOrganizationsAccess	StackSet と Organization 間の信頼できるアクセスを無効にする許可を付与します。信頼できるアクセスが無効化されている場合、管理アカウントには組織のサービス管理のスタックセットを作成および管理する権限がありません。	書き込み			
DeactivateType	アカウントとリージョン内で先にアクティブ化されている、公開拡張機能を非アクティブ化するためのアクセス許可を付与	書き込み			
DeleteChangeSet	指定された変更セットを削除するアクセス許可を付与 変更セットを削除することで、誤った変更セットの実行が防止されます。	書き込み	stack*		
				cloudformation:ChangeSetName	
DeleteGeneratedTemplate	生成されたテンプレートを削除する許可を付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteStack	指定されたスタックを削除するアクセス許可を付与	Write	stack*		
				cloudformation:RoleArn	
DeleteStackInstances	指定されたリージョン内で指定されたアカウントのスタックインスタンスを削除するアクセス許可を付与	Write	stackset*		
			stackset-target		
			type		
				cloudformation:TargetRegion	
DeleteStackSet	指定されたスタックセットを削除するアクセス許可を付与	Write	stackset*		
DeregisterType	既存の CloudFormation タイプまたはタイプバージョンの登録を解除するアクセス許可を付与	書き込み			
DescribeAccountLimits	アカウントの AWS CloudFormation 制限を取得するアクセス許可を付与します	読み取り			
DescribeChangeSet	指定された変更セットの説明を返すアクセス許可を付与	読み取り	stack*		
				cloudformation:ChangeSetName	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeChangeSetHooks	指定した変更セットのフック呼び出し情報を返す許可を付与	読み取り	stack*		
				cloudformation:ChangeSetName	
DescribeGeneratedTemplate	生成されたテンプレートを記述する許可を付与します。出力には、生成されたテンプレートの作成の進行状況に関する詳細が含まれます	読み取り			
DescribeOrganizationsAccess	アカウントの OrganizationAccess ステータスに関する情報を返す許可を付与します	読み取り			
DescribePublisher	CloudFormation 拡張機能のパブリッシャーに関する情報を返すためのアクセス許可を付与	読み取り			
DescribeResourceScan	リソーススキャンの詳細を記述する許可を付与する	読み取り			
DescribeStackDriftDetectionStatus	スタックドリフト検出オペレーションに関する情報を返すアクセス許可を付与	Read			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeStackEvents	指定されたスタックについて、スタック関連のすべてのイベントを返すアクセス許可を付与	読み取り	stack*		
DescribeStackInstance	指定されたスタックセット、AWS アカウント、リージョンに関連付けられているスタックインスタンスを返すアクセス許可を付与します	読み取り	stackset*		
DescribeStackRefactor	指定されたスタックリファクタリングの説明を返すアクセス許可を付与します	読み取り	stack*		
DescribeStackResource	指定のスタック内にある指定のリソースの説明を返すアクセス許可を付与	Read	stack*		
DescribeStackResourceDrifts	指定されたスタック内でドリフトが確認されたリソースのドリフト情報を返すアクセス許可を付与	読み取り	stack*		
DescribeStackResources	実行中および削除されたスタックの AWS リソースの説明を返すアクセス許可を付与します	読み取り	stack*		
DescribeStackSet	指定されたスタックセットの説明を返すアクセス許可を付与	Read	stackset*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeStackSetOperation	指定されたスタックセットオペレーションの説明を返すアクセス許可を付与	読み取り	stackset*		
DescribeStacks	指定されたスタックの説明、および ListStacks アクションと組み合わせて使用した場合はすべてのスタックの説明を返す許可を付与	リスト	stack		cloudformation:ListStacks
DescribeType	リクエストされた CloudFormation タイプに関する情報を返すアクセス許可を付与	Read			
DescribeTypeRegistration	CloudFormation タイプの登録プロセスに関する情報を返すアクセス許可を付与	Read			
DetectStackDrift	スタックの実際の設定が、スタックテンプレートおよびテンプレートパラメータとして指定された値で定義されている、意図された設定と異なるかどうかを検出するアクセス許可を付与	Read	stack*		
DetectStackResourceDrift	リソースの実際の設定が、スタックテンプレートおよびテンプレートパラメータとして指定された値で定義されている、意図された設定と異なるか、またはドリフトしているかについての情報を返すアクセス許可を付与	Read	stack*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DetectStackSetDrift	ユーザーがスタックセットとそのスタックセットに属するスタックインスタンスのドリフトを検出できるようにアクセス許可を付与	Read	stackset*		
EstimateTemplateCost	テンプレートの推定月額コストを返すアクセス許可を付与	Read		cloudformation:TemplateUrl	
ExecuteChangeSet	指定された変更セットの作成時に提供された入力情報を使い、スタックを更新するアクセス許可を付与	書き込み	stack*		
				cloudformation:ChangeSetName	
ExecuteStackRefactor	指定されたスタックリファクタリングの作成時に提供された入力情報を使用してスタックリファクタリングを実行するアクセス許可を付与します	書き込み	stack*		
GetGeneratedTemplate	生成されたテンプレートを取得する許可を付与する	読み取り			
GetStackPolicy	指定されたスタックのスタックポリシーを返すアクセス許可を付与	Read	stack*		
GetTemplate	指定されたスタックのテンプレート本文を返すアクセス許可を付与	Read	stack*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetTemplateSummary	承認ルールテンプレートに関する情報を返すアクセス許可を付与	読み取り	stack		
			stackset		
				cloudformation:TemplateUrl	
ImportStacksToStackSet	ユーザーが既存のスタックを新規または既存のスタックセットにインポートできるようにする許可を付与	書き込み	stackset*		
ListChangeSets	スタックのアクティブな変更セットごとに、ID とステータスを返すアクセス許可を付与 例えば、AWS CloudFormation は CREATE_IN_PROGRESS または CREATE_PENDING 状態にある変更セットを一覧表示します。	リスト	stack*		
ListExports	このアクションを呼び出すアカウントおよびリージョンにあるエクスポートされた出力値を一覧表示するアクセス許可を付与	リスト			
ListGeneratedTemplates	このリージョンで生成されたテンプレートを一覧表示する許可を付与する	リスト			
ListHookResults		リスト	stack		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	指定されたターゲットのフック呼び出し結果情報を返すアクセス許可を付与します			cloudformation:ChangeSetName	
ListImports	エクスポートされた出力値をインポートしているスタックを一覧表示するアクセス許可を付与	リスト			
ListResourceScanRelatedResources	リソーススキャンからのリソースのリストに関連するリソースを一覧表示する許可を付与します。レスポンスは、返された各リソースが CloudFormation によって既に管理されているかどうかを示します	リスト			
ListResourceScanResources	リソーススキャンからリソースを一覧表示する許可を付与します。結果は、リソース識別子、リソースタイプのプレフィックス、タグキー、タグ値でフィルタリングできます	リスト			
ListResourceScans	リソーススキャンを最新のものから古いものまで一覧表示する許可を付与します。デフォルトでは、最大 10 回リソーススキャンが返されます	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListStackInstanceResourceDrifts	指定されたスタックインスタンス内でドリフトが確認されたリソースのドリフト情報を返すアクセス許可を付与します	リスト	stackset*		
ListStackInstances	指定されたスタックセットに関連付けられているスタックインスタンスについて要約情報を返すアクセス許可を付与	リスト	stackset*		
ListStackRefactorActions	指定されたスタックリファクタリングのアクションのリストを返すアクセス許可を付与します	リスト	stack*		
ListStackRefactors	アクティブな各スタックリファクタリングの ID とステータスを返すアクセス許可を付与します	リスト	stack*		
ListStackResources	指定されたスタックのすべてのリソースの説明を返すアクセス許可を付与	リスト	stack*		
ListStackSetAutoDeploymentTargets	StackSet 自動デプロイメントターゲットに関する概要情報を返す許可を付与する	リスト	stackset*		
ListStackSetOperationResults	スタックセットオペレーションの結果に関する要約情報を返すアクセス許可を付与	リスト	stackset*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListStackSetOperations	スタックセットで実行されたオペレーションに関する概要情報を返すアクセス許可を付与	リスト	stackset*		
ListStackSets	ユーザーに関連付けられたスタックセットに関する概要情報を返すアクセス許可を付与	リスト			
ListStacks	指定された StackStatusFilter に一致するステータスを持つスタックに関する概要情報を返す許可を付与します。DescribeStacks アクションと組み合わせて、スタックの説明を一覧表示する許可を付与	リスト			
ListTypeRegistrations	CloudFormation タイプの登録試行を一覧表示するアクセス許可を付与	リスト			
ListTypeVersions	特定の CloudFormation タイプのバージョンを一覧表示するアクセス許可を付与	リスト			
ListTypes	利用可能な CloudFormation タイプを一覧表示するアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PublishType	指定された拡張機能をこのリージョンで公開するために、CloudFormation レジストリに対し公開するためのアクセス許可を付与	書き込み			
RecordHandlerProgress	ハンドラーの進行状況を記録する許可を付与	書き込み	stack*		
RegisterPublisher	アカウントを、CloudFormation レジストリ内で公開拡張機能のパブリッシャーとして登録するための、アクセス許可を付与	書き込み			
RegisterType	新しい CloudFormation タイプを登録するアクセス許可を付与	書き込み			
RollbackStack	スタックを最後の安定状態にロールバックするアクセス許可を付与	書き込み	stack*		
				cloudformation:RoleArn	
SetStackPolicy	指定されたスタックのスタックポリシーを設定するアクセス許可を付与	権限の管理	stack*		
				cloudformation:StackPolicyUrl	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SetTypeConfiguration	指定されたアカウントおよびリージョンで、登録済みの CloudFormation 拡張機能に対し設定データを設定するためのアクセス許可を付与	書き込み			
SetTypeDefaultVersion	CloudFormation オペレーションに適用する CloudFormation タイプのバージョンを設定するアクセス許可を付与	Write			
SignalResource	成功または失敗のステータスを持つ指定のリソースにシグナルを送信するアクセス許可を付与	書き込み	stack*		
StartResourceScan	このリージョンのこのアカウントのリソースのスキャンを開始する許可を付与する	書き込み			
StopStackSetOperation	スタックセットおよびそれに関連付けられているスタックインスタンスで進行中のオペレーションを停止するアクセス許可を付与	Write	stackset*		
TagResource	クラウドフォーメーションリソースにタグを付けるアクセス許可を付与	Tagging	changeset		
			stack		
			stackset		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey} cloudformation:CreateAction	
TestType	登録済みの拡張機能をテストし、CloudFormation レジストリ内での公開に必要な、すべての要件を満たしていることを確認するためのアクセス許可を付与	書き込み			
UntagResource	クラウドフォーメーションリソースのタグを解除するアクセス許可を付与	Tagging	changeset		
			stack		
			stackset		
				aws:TagKeys cloudformation:CreateAction	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateGeneratedTemplate	生成されたテンプレートを更新する許可を付与します。これは、名前の変更、リソースの追加と削除、リソースの更新、および DeletionPolicy と UpdateReplacePolicy の設定の変更に使用できます	書き込み			
UpdateStack	テンプレートで指定されたスタックを更新するアクセス許可を付与	Write	stack*	cloudformation:ResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateStackInstances	指定されたリージョン内で指定されたアカウントのスタックインスタンスのパラメータ値を更新するアクセス許可を付与	Write	stackset*		
			stackset-target		
			type		
				cloudformation:TargetRegion	
UpdateStackSet	テンプレートで指定されたスタックセットを更新するアクセス許可を付与	Write	stackset*		
			stackset-target		
			type		
				cloudformation:RoleArn cloudformation:TemplateUrl cloudformation:TargetRegion aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateTerminationProtection	指定されたスタックの終了保護を更新するアクセス許可を付与	Write	stack*		
ValidateTemplate	指定されたテンプレートを検証するアクセス許可を付与	Read		cloudformation:TemplateUrl	

AWS CloudFormation で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
changeset	arn:${Partition}:cloudformation:${Region}:${Account}:changeSet/${ChangeSetName}/${Id}	aws:ResourceTag/${TagKey}
stack	arn:${Partition}:cloudformation:${Region}:${Account}:stack/${StackName}/${Id}	aws:ResourceTag/${TagKey}
stackset	arn:${Partition}:cloudformation:${Region}:${Account}:stackset/${StackSetName}:${Id}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
stackset-target	arn:${Partition}:cloudformation:${Region}:${Account}:stackset-target/${StackSetTarget}	
type	arn:${Partition}:cloudformation:${Region}:${Account}:type/resource/${Type}	
generated template	arn:${Partition}:cloudformation:${Region}:${Account}:generatedTemplate/${Id}	
resources can	arn:${Partition}:cloudformation:${Region}:${Account}:resourceScan/${Id}	

AWS CloudFormation の条件キー

AWS CloudFormation では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

条件キー	説明	タイプ
cloudformation:ChangeSetName	AWS CloudFormation 変更セット名でアクセスをフィルタリングします。IAM ユーザーがどの変更セットを実行または削除できるかを制御するために使用します。	String
cloudformation:CreateAction	リソース変更 API アクションの名前でアクセスをフィルタリングします。を使用して、IAM ユーザーがスタックまたはスタックセットのタグの追加または削除に使用できる APIs を制御します。	String
cloudformation:ImportResourceTypes	AWS::EC2::Instance などのテンプレートリソースタイプでアクセスをフィルタリングします。IAM ユーザーがスタックにリソースをインポートする際に操作できるリソースタイプを制御するために使用します。	String
cloudformation:ResourceTypes	AWS::EC2::Instance などのテンプレートリソースタイプでアクセスをフィルタリングします。IAM ユーザーがスタックの作成または更新時に操作できるリソースタイプを制御するために使用します。	ArrayOfString
cloudformation:RoleArn	IAM サービスロールの ARN によりアクセスをフィルタリングする IAM ユーザーがスタックまたは変更セットの操作にどのサービスロールを使用できるかを制御するために使用します。	ARN
cloudformation:StackPolicyUrl	Amazon S3 のスタックポリシー URL によりアクセスをフィルタリングする IAM ユーザーがスタックアクションの作成または更新アクション時にスタックにどのスタックポリシーを関連付けられるかを制御するために使用します。	String
cloudformation:TargetRegion	スタックセットのターゲットリージョンによりアクセスをフィルタリングする スタックセットを作成または更新する IAM ユーザーが使用可能なリージョンを、制御するために使用します。	ArrayOfString

条件キー	説明	タイプ
cloudformation:TemplateUrl	Amazon S3 のテンプレート URL によりアクセスをフィルタリングする IAM ユーザーがスタックの作成または更新時にどのテンプレートを使用できるかを制御するために使用します。	文字列

Amazon CloudFront のアクション、リソース、および条件キー

Amazon CloudFront (サービスプレフィックス: `cloudfront`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CloudFront で定義されるアクション
- Amazon CloudFront で定義されるリソースタイプ
- Amazon CloudFront の条件キー

Amazon CloudFront で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にア

クションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AllowVendedLogDeliveryForResource [アク	ディストリビューションの販売ログ配信を設定するアクセス許可を付与します	権限の管理	distribution		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
セス許可のみ]					
AssociateAlias	CloudFront ディストリビューションにエイリアスを関連付ける許可を付与	書き込み	distribution*		
AssociateDistributionTenantWebACL	ディストリビューションテナントを AWS WAF ウェブ ACL に関連付けるアクセス許可を付与します	書き込み	distribution-tenant*		
AssociateDistributionWebACL	ディストリビューションを AWS WAF ウェブ ACL に関連付けるアクセス許可を付与します	書き込み	distribution*		
CopyDistribution	既存のディストリビューションをコピーしたり、新しいウェブディストリビューションを作成したりするための許可を付与します	書き込み	distribution*		cloudfront:CopyDistribution cloudfront:CreateDistribution cloudfront:GetDistribution
CreateAnycastIpList	エニーキャスト静的 IP リストを作成するアクセス許可を付与します	書き込み	anycast-ip-list*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCachePolicy	CloudFront に新しいキャッシュポリシーを追加する許可を付与	Write	cache-policy*		
CreateCloudFrontOriginAccessIdentity	新しい CloudFront オリジンアクセスアイデンティティを作成する許可を付与	書き込み	origin-access-identity*		
CreateConnectionGroup	接続グループを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateContinuousDeploymentPolicy	CloudFront に新しい継続的デプロイポリシーを追加するための許可を付与します	書き込み	continuous-deployment-policy*		
CreateDistribution	新しいウェブディストリビューションを作成する許可を付与	書き込み	distribution*		cloudfront:CreateConnectionGroup

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateDistributionTenant	ディストリビューションテナントを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFieldLevelEncryptionConfig	新しいフィールドレベル暗号化設定を作成する許可を付与	Write			
CreateFieldLevelEncryptionProfile	フィールドレベル暗号化プロファイルを作成する許可を付与	Write			
CreateFunction	CloudFront 関数を作成する許可を付与	Write	function*		
CreateInvalidation	新しい無効化バッチリクエストを作成する許可を付与	書き込み	distribution*		
CreateInvalidationForDistributionTenant	ディストリビューションテナントの無効化を作成するアクセス許可を付与します	書き込み	distribution-tenant*		
CreateKeyGroup	CloudFront に新しいキーグループを追加する許可を付与	書き込み			
CreateKeyValueStore	CloudFront KeyValueStore を作成する許可を付与	書き込み	key-value-store*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateMonitoringSubscription	指定された CloudFront ディストリビューションの追加の CloudWatch メトリクスを有効にする許可を付与。追加のメトリクスには追加コストが発生します	書き込み			
CreateOriginAccessControl	新しいオリジンアクセスコントロールを作成する権限を付与する	書き込み			
CreateOriginRequestPolicy	CloudFront に新しいオリジンリクエストポリシーを追加する許可を付与	Write	origin-request-policy*		
CreatePublicKey	CloudFront に新しいパブリックキーを追加する許可を付与	Write			
CreateRealtimeLogConfig	リアルタイムログ設定を作成する許可を付与	書き込み	realtime-log-config*		
CreateResponseHeadersPolicy	CloudFront に新しいレスポンスヘッダーポリシーを追加する許可を付与	書き込み	response-headers-policy*		
CreateSavingsPlan [アクセス許可のみ]	新しい Savings Plans を作成する権限を付与する	書き込み			
CreateStreamingDistribution	新しい RTMP ディストリビューションを作成する許可を付与	Write	streaming-distribution*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateStreamingDistributionWithTags	新しい RTMP ディストリビューションをタグ付きで作成する許可を付与	書き込み	streaming-distribution*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVpcOrigin	VPC オリジンを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAnycastIpList	エニーキャスト静的 IP リストを削除する許可を付与	書き込み	anycast-ip-list*		
DeleteCachePolicy	キャッシュポリシーを削除する許可を付与	Write	cache-policy*		
DeleteCloudFrontOriginAccessIdentity	CloudFront オリジンアクセスアイデンティティを削除する許可を付与	書き込み	origin-access-identity*		
DeleteConnectionGroup	接続グループを削除するアクセス許可を付与します	書き込み	connection-group*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteContinuousDeploymentPolicy	継続的デプロイポリシーを削除するための許可を付与します	書き込み	continuous-deployment-policy*		
DeleteDistribution	ウェブディストリビューションを削除する許可を付与	書き込み	distribution*		
DeleteDistributionTenant	ディストリビューションテナントを削除するアクセス許可を付与します	書き込み	distribution-tenant*		
DeleteFieldLevelEncryptionConfig	フィールドレベル暗号化の設定を削除する許可を付与	Write	field-level-encryption-config*		
DeleteFieldLevelEncryptionProfile	フィールドレベル暗号化プロファイルを削除する許可を付与	Write	field-level-encryption-profile*		
DeleteFunction	CloudFront 関数を削除する許可を付与	Write	function*		
DeleteKeyGroup	キーグループを削除する許可を付与	書き込み			
DeleteKeyValueStore	CloudFront KeyValueStore を削除する許可を付与	書き込み	key-value-store*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteMonitoringSubscription	指定された CloudFront ディストリビューションの追加の CloudWatch メトリクスを無効にする許可を付与	書き込み			
DeleteOriginAccessControl	オリジンアクセスコントロールを削除する権限を付与する	書き込み	origin-access-control*		
DeleteOriginRequestPolicy	オリジンリクエストポリシーを削除する許可を付与	Write	origin-request-policy*		
DeletePublicKey	CloudFront から公開鍵を削除する許可を付与	Write			
DeleteRealtimeLogConfig	リアルタイムログ設定を削除する許可を付与	書き込み	realtime-log-config*		
DeleteResponseHeadersPolicy	リソースヘッダーポリシを削除する許可を付与	書き込み	response-headers-policy*		
DeleteStreamingDistribution	RTMP ディストリビューションを削除する許可を付与	書き込み	streaming-distribution*		
DeleteVpcOrigin	VPC オリジンを削除するアクセス許可を付与します	書き込み	vpcorigin*		
DescribeFunction	CloudFront 関数概要を取得する許可を付与	読み取り	function*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeKeyValueStore	CloudFront KeyValueStore 概要を取得する許可を付与	読み取り	key-value-store*		
DisassociateDistributionTenantWebACL	AWS WAF ウェブ ACL からディストリビューションテナントの関連付けを解除する許可を付与	書き込み	distribution-tenant*		
DisassociateDistributionWebACL	AWS WAF ウェブ ACL からディストリビューションの関連付けを解除する許可を付与	書き込み	distribution*		
GetAnycastIpList	エニーキャスト静的 IP リストを取得する許可を付与	読み取り	anycast-ip-list*		
GetCachePolicy	キャッシュポリシーを取得する許可を付与	Read	cache-policy*		
GetCachePolicyConfig	キャッシュポリシー設定を取得する許可を付与	Read	cache-policy*		
GetCloudFrontOriginAccessIdentity	CloudFront オリジンアクセスアイデンティティに関する情報を取得する許可を付与	Read	origin-access-identity*		
GetCloudFrontOriginAccessIdentityConfig	CloudFront オリジンアクセスアイデンティティに関する設定情報を取得する許可を付与	読み取り	origin-access-identity*		
GetConnectionGroup	接続グループに関する情報を取得するアクセス許可を付与します	読み取り	connection-group*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetConnectionGroupByRoutingEndpoint	指定されたルーティングエンドポイントによって接続グループに関する情報を取得するアクセス許可を付与します	読み取り	connection-group*		
GetContinuousDeploymentPolicy	継続的デプロイポリシーを取得するための許可を付与します	読み取り	continuous-deployment-policy*		
GetContinuousDeploymentPolicyConfig	継続的デプロイポリシー設定を取得するための許可を付与します	読み取り	continuous-deployment-policy*		
GetDistribution	ウェブディストリビューションに関する情報を取得する許可を付与	Read	distribution*		
GetDistributionConfig	ディストリビューションに関する設定情報を取得する許可を付与	読み取り	distribution*		
GetDistributionTenant	ディストリビューションテナントに関する情報を取得する許可を付与	読み取り	distribution-tenant*		
GetDistributionTenantByDomain	関連付けられたドメインによってディストリビューションテナントに関する情報を取得するアクセス許可を付与します	読み取り	distribution-tenant*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetFieldLevelEncryption	フィールドレベル暗号化設定情報を取得する許可を付与	Read	field-level-encryption-config*		
GetFieldLevelEncryptionConfig	フィールドレベル暗号化設定情報を取得する許可を付与	Read	field-level-encryption-config*		
GetFieldLevelEncryptionProfile	フィールドレベル暗号化設定情報を取得する許可を付与	Read	field-level-encryption-profile*		
GetFieldLevelEncryptionProfileConfig	フィールドレベル暗号化プロファイル設定情報を取得する許可を付与	Read	field-level-encryption-profile*		
GetFunction	CloudFront 関数のコードを取得する許可を付与	Read	function*		
GetInvalidation	無効化に関する情報を取得する許可を付与	読み取り	distribution*		
GetInvalidationForDistributionTenant	ディストリビューションテナントの無効化に関する情報を取得するアクセス許可を付与します	読み取り	distribution-tenant*		
GetKeyGroup	キーグループを取得する許可を付与	Read			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetKeyGroupConfig	キーグループ設定を取得する許可を付与	読み取り			
GetManagedCertificateDetails	CloudFront マネージド証明書の詳細を取得する許可を付与	読み取り	distribution-tenant*		
GetMonitoringSubscription	指定された CloudFront ディストリビューションで追加の CloudWatch メトリクスが有効になっているかどうかに関する情報を取得する許可を付与	読み取り			
GetOriginAccessControl	オリジンアクセスコントロールを取得する権限を付与する	読み取り	origin-access-control*		
GetOriginAccessControlConfig	オリジンアクセスコントロール設定を取得する権限を付与する	読み取り	origin-access-control*		
GetOriginRequestPolicy	オリジンリクエストポリシーを取得する許可を付与	Read	origin-request-policy*		
GetOriginRequestPolicyConfig	オリジンリクエストポリシー設定を取得する許可を付与	Read	origin-request-policy*		
GetPublicKey	公開鍵情報を取得する許可を付与	Read			
GetPublicKeyConfig	公開鍵設定情報を取得する許可を付与	Read			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetRealtimeLogConfig	リアルタイムログ設定を取得する許可を付与	読み取り	realtime-log-config*		
GetResponseHeadersPolicy	レスポンスヘッダーポリシーを取得するアクセス許可を付与	読み取り	response-headers-policy*		
GetResponseHeadersPolicyConfig	レスポンスヘッダーポリシー設定を取得する許可を付与	読み取り	response-headers-policy*		
GetSavingsPlan [許可のみ]	Savings Plans を取得する権限を付与する	読み取り			
GetStreamingDistribution	RTMP ディストリビューションに関する情報を取得する許可を付与	Read	streaming-distribution*		
GetStreamingDistributionConfig	ストリーミングディストリビューションに関する設定情報を取得する許可を付与	読み取り	streaming-distribution*		
GetVpcOrigin	VPC オリジンに関する情報を取得する許可を付与	読み取り	vpcorigin*		
ListAnycastIpLists	Anycast 静的 IP リストを一覧表示する許可を付与	リスト			
ListCachePolicies	このアカウントに対して CloudFront で作成されたすべてのキャッシュポリシーを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListCloudFrontOriginAccessIdentities	CloudFront オリジンアクセスアイデンティティを一覧表示する許可を付与	リスト			
ListConflictingAliases	CloudFront で指定したエイリアスと競合するすべてのエイリアスを一覧表示する許可を付与	リスト	distribution*		
ListConnectionGroups	内の接続グループを一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListContinuousDeploymentPolicies	アカウント内のすべての継続的デプロイポリシーを一覧表示するための許可を付与します	リスト			
ListDistributionTenants	のディストリビューションテナントを一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListDistributionTenantsByCustomization	指定したカスタマイズによってディストリビューションテナントを一覧表示するアクセス許可を付与します	リスト			
ListDistributions	に関連付けられているディストリビューションを一覧表示するアクセス許可を付与します AWS アカウント	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListDistributionsByAnycastIpListId	指定された AnycastIpListId に関連付けられているアカウントのディストリビューションを一覧表示するアクセス許可を付与します	リスト			
ListDistributionsByCachePolicyId	指定したキャッシュポリシーにキャッシュ動作が関連付けられているディストリビューションのディストリビューション ID を一覧表示する許可を付与	リスト			
ListDistributionsByConnectionMode	指定された接続モードでディストリビューションを一覧表示するアクセス許可を付与します	リスト			
ListDistributionsByKeyGroup	指定したキーグループにキャッシュ動作が関連付けられているディストリビューションのディストリビューション ID を一覧表示する許可を付与	リスト			
ListDistributionsByLambdaFunction [許可のみ]	Lambda 関数に関連付けられているディストリビューションを一覧表示するためのアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListDistributionsByOriginRequestPolicyId	指定したオリジンリクエストポリシーにキャッシュ動作が関連付けられているディストリビューションのディストリビューション ID を一覧表示する許可を付与	リスト			
ListDistributionsByRealtimeLogConfig	指定されたリアルタイムログ設定に関連付けられたキャッシュ動作を持つディストリビューションのリストを取得する許可を付与する	リスト			
ListDistributionsByResponseHeadersPolicyId	指定したレスポンスヘッダーポリシーにキャッシュ動作が関連付けられているディストリビューションのディストリビューション ID を一覧表示する許可を付与	リスト			
ListDistributionsByVpcOriginId	指定された VPC オリジンに関連付けられたディストリビューションIDs を一覧表示するアクセス許可を付与します	リスト			
ListDistributionsByWebACLId	特定の AWS WAF ウェブ ACL AWS アカウント を持つ に関連付けられたディストリビューションを一覧表示するアクセス許可を付与します	リスト			
ListDomainConflicts	指定されたドメインのドメイン競合を一覧表示するアクセス許可を付与します	リスト	distribution		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			distribution-tenant		
ListFieldLevelEncryptionConfigs	このアカウントの CloudFront で作成されたすべてのフィールドレベル暗号化設定を一覧表示する許可を付与	リスト			
ListFieldLevelEncryptionProfiles	このアカウントの CloudFront で作成されたすべてのフィールドレベル暗号化プロファイルを一覧表示する許可を付与	リスト			
ListFunctions	CloudFront 関数のリストを取得する許可を付与	リスト			
ListInvalidations	無効化バッチを一覧表示する許可を付与	リスト	distribution*		
ListInvalidationsForDistributionTenant	ディストリビューションテナントの無効化を一覧表示するアクセス許可を付与します	リスト	distribution-tenant*		
ListKeyGroups	このアカウントの CloudFront で作成されたすべてのキーグループを一覧表示する許可を付与	リスト			
ListKeyValueStores	CloudFront KeyValueStores のリストを取得する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListOriginAccessControls	アカウント内にあるすべてのオリジンアクセスコントロールを一覧表示する権限を付与する	リスト			
ListOriginRequestPolicies	このアカウントの CloudFront で作成されたすべてのオリジンリクエストポリシーを一覧表示する許可を付与	リスト			
ListPublicKeys	このアカウントの CloudFront に追加されたすべてのパブリックキーを一覧表示する許可を付与	リスト			
ListRateCards [許可のみ]	アカウントの CloudFront レートカードを一覧表示する権限を付与する	リスト			
ListRealtimeLogConfigs	リアルタイムログ設定を一覧表示する許可を付与	リスト			
ListResponseHeadersPolicies	このアカウントの CloudFront で作成されたすべてのレスポンスヘッダーポリシーを一覧表示する許可を付与	リスト			
ListSavingsPlans [許可のみ]	アカウント内に savings plans を一覧表示する権限を付与する	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListStreamingDistributions	RTMP ディストリビューションを一覧表示する許可を付与	リスト			
ListTagsForResource	CloudFront リソースのタグを一覧表示する許可を付与	読み取り	anycast-ip-list		
			connection-group		
			distribution		
			distribution-tenant		
			vpcorigin		
ListUsages [許可のみ]	CloudFront の使用状況を一覧表示する権限を付与する	リスト			
ListVpcOrigins	VPC オリジンを一覧表示する許可を付与	リスト			
PublishFunction	CloudFront 関数を発行する許可を付与	Write	function*		
TagResource	CloudFront リソースにタグを追加する許可を付与	タグ付け	anycast-ip-list		
			connection-group		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			distribution		
			distribution-tenant		
			streaming-distribution		
			vpcorigin		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestFunction	CloudFront 関数をテストする許可を付与	Write	function*		
UntagResource	CloudFrontリソースからタグを削除する許可を付与	タグ付け	anycast-ip-list		
			connection-group		
			distribution		
			distribution-tenant		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			streaming-distribution		
			vpcorigin		
				aws:TagKeys	
UpdateCachePolicy	キャッシュポリシーを更新する許可を付与	Write	cache-policy*		
UpdateCloudFrontOriginAccessIdentity	CloudFront オリジンアクセスアイデンティティの設定を設定する許可を付与	書き込み	origin-access-identity*		
UpdateConnectionGroup	接続グループを更新するアクセス許可を付与します	書き込み	connection-group*		
UpdateContinuousDeploymentPolicy	継続的デプロイポリシーを更新するための許可を付与します	書き込み	continuous-deployment-policy*		
UpdateDistribution	ウェブディストリビューション設定を更新する許可を付与	書き込み	distribution*		
UpdateDistributionTenant	ディストリビューションテナントを更新する許可を付与	書き込み	distribution-tenant*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateDistributionWithStagingConfig	ステージング Web ディストリビューションから対応するプライマリ Web ディストリビューションに設定をコピーする許可を付与する	書き込み	distribution*		
UpdateDomainAssociation	ドメインの関連付けを更新するアクセス許可を付与します	書き込み	distribution		
			distribution-tenant		
UpdateFieldLevelEncryptionConfig	フィールドレベル暗号化設定を更新する許可を付与	Write			
UpdateFieldLevelEncryptionProfile	フィールドレベル暗号化プロファイルを更新する許可を付与	Write	field-level-encryption-profile*		
UpdateFunction	CloudFront 関数を更新する許可を付与	Write	function*		
UpdateKeyGroup	キーグループを更新する許可を付与	書き込み			
UpdateKeyValueStore	CloudFront KeyValueStore を更新する許可を付与	書き込み	key-value-store*		
UpdateOriginAccessControl	オリジンアクセスコントロールを更新する権限を付与する	書き込み	origin-access-control*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateOriginRequestPolicy	オリジンリクエストポリシーを更新する許可を付与	Write	origin-request-policy*		
UpdatePublicKey	公開鍵情報を更新する許可を付与	Write			
UpdateRealtimeLogConfig	リアルタイムログ設定を更新する許可を付与	書き込み	realtime-log-config*		
UpdateResponseHeadersPolicy	データセットのリソースポリシーを更新するアクセス許可を付与	書き込み	response-headers-policy*		
UpdateSavingsPlan [アクセス許可のみ]	Savings Plans を更新する権限を付与する	書き込み			
UpdateStreamingDistribution	RTMP ディストリビューションの設定を更新する許可を付与	書き込み	streaming-distribution*		
UpdateVpcOrigin	VPC オリジンを更新する許可を付与	書き込み	vpcorigin*		
VerifyDnsConfiguration	指定されたドメインの DNS 設定を検証するアクセス許可を付与します	読み取り	distribution-tenant		

Amazon CloudFront で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
distribution	arn:${Partition}:cloudfront::${Account}:distribution/${DistributionId}	aws:ResourceTag/${TagKey}
streaming-distribution	arn:${Partition}:cloudfront::${Account}:streaming-distribution/${DistributionId}	aws:ResourceTag/${TagKey}
origin-access-identity	arn:${Partition}:cloudfront::${Account}:origin-access-identity/${Id}	
field-level-encryption-config	arn:${Partition}:cloudfront::${Account}:field-level-encryption-config/${Id}	
field-level-encryption-profile	arn:${Partition}:cloudfront::${Account}:field-level-encryption-profile/${Id}	
cache-policy	arn:${Partition}:cloudfront::${Account}:cache-policy/${Id}	
origin-request-policy	arn:${Partition}:cloudfront::${Account}:origin-request-policy/${Id}	
realtime-log-config	arn:${Partition}:cloudfront::${Account}:realtime-log-config/${Name}	

リソースタイプ	ARN	条件キー
function	arn:${Partition}:cloudfront::${Account}:function/${Name}	
key-value-store	arn:${Partition}:cloudfront::${Account}:key-value-store/${Name}	
response-headers-policy	arn:${Partition}:cloudfront::${Account}:response-headers-policy/${Id}	
origin-access-control	arn:${Partition}:cloudfront::${Account}:origin-access-control/${Id}	
continuous-deployment-policy	arn:${Partition}:cloudfront::${Account}:continuous-deployment-policy/${Id}	
anycast-ip-list	arn:${Partition}:cloudfront::${Account}:anycast-ip-list/${Id}	aws:ResourceTag/${TagKey}
vpcorigin	arn:${Partition}:cloudfront::${Account}:vpcorigin/${Id}	aws:ResourceTag/${TagKey}
distribution-tenant	arn:${Partition}:cloudfront::${Account}:distribution-tenant/${Id}	aws:ResourceTag/${TagKey}
connection-group	arn:${Partition}:cloudfront::${Account}:connection-group/${Id}	aws:ResourceTag/${TagKey}

Amazon CloudFront の条件キー

Amazon CloudFront は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

Amazon CloudFront KeyValueStore のアクション、リソース、および条件キー

Amazon CloudFront KeyValueStore (サービスプレフィックス: `cloudfront-keyvaluestore`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CloudFront KeyValueStore で定義されるアクション
- Amazon CloudFront KeyValueStore で定義されるリソースタイプ
- Amazon CloudFront KeyValueStore の条件キー

Amazon CloudFront KeyValueStore で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteKey	キーで指定されたキーと値のペアを削除するためのアクセス許可を付与	書き込み	key-value-store*		
DescribeKeyValueStore	キー値ストアに関するメタデータ情報を返すためのアクセス許可を付与	読み取り	key-value-store*		
GetKey	キーと値のペアを返すためのアクセス許可を付与	読み取り	key-value-store*		
ListKeys	キーと値のペアのリストを返すためのアクセス許可を付与	リスト	key-value-store*		
PutKey	新しいキーと値のペアを作成したり、既存のキー値を置き換えたりするためのアクセス許可を付与	書き込み	key-value-store*		
UpdateKeys	単一のオールオアナッシング操作で複数のキーと値のペアを配置または削除するためのアクセス許可を付与	書き込み	key-value-store*		

Amazon CloudFront KeyValueStore で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
key-value-store	arn:${Partition}:cloudfront::${Account}:key-value-store/${ResourceId}	

Amazon CloudFront KeyValueStore の条件キー

CloudFront KeyValueStore には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーがありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS CloudHSM のアクション、リソース、および条件キー

AWS CloudHSM (サービスプレフィックス: cloudhsm) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS CloudHSM で定義されるアクション
- AWS CloudHSM で定義されるリソースタイプ
- AWS CloudHSM の条件キー

AWS CloudHSM で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CopyBackupToRegion	指定されたリージョンにバックアップのコピーを作成するための許可を付与します	書き込み	backup*		cloudhsm:CopyBackupToRegion cloudhsm:TagResource cloudhsm:UntagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCluster	新しい AWS CloudHSM クラスターを作成するアクセス許可を付与します	書き込み	backup		cloudhsm:TagResource ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:RevokeSecurityGroupEgress iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateHsm	指定された AWS CloudHSM クラスターに新しいハードウェアセキュリティモジュール (HSM) を作成するアクセス許可を付与します	書き込み	cluster*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					ec2:RevokeSecurityGroupEgress
DeleteBackup	指定された CloudHSM バックアップを削除するための許可を付与します	書き込み	backup*		
DeleteCluster	指定された AWS CloudHSM クラスターを削除するアクセス許可を付与します	書き込み	cluster*		ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup
DeleteHsm	指定した HSM を削除するための許可を付与します	書き込み			ec2:DeleteNetworkInterface
DeleteResourcePolicy	CloudHSM リソースに添付されたポリシーを削除する許可を付与する	書き込み	backup*		
DescribeBackups	AWS CloudHSM クラスターのバックアップに関する情報を取得する許可を付与	読み取り			
DescribeClusters	AWS CloudHSM クラスターに関する情報を取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetResourcePolicy	AWS CloudHSM リソースにアタッチされたポリシーに関する情報を取得するアクセス許可を付与します	読み取り	backup*		
InitializeCluster	AWS CloudHSM クラスターをリクエストするアクセス許可を付与します	書き込み	cluster*		
ListTags	指定された AWS CloudHSM クラスターのタグのリストを取得するアクセス許可を付与します	読み取り	backup		
			cluster		
ModifyBackupAttributes	AWS CloudHSM バックアップの属性を変更する許可を付与	書き込み	backup*		
ModifyCluster	AWS CloudHSM クラスターを変更するアクセス許可を付与します	書き込み	cluster*		ec2:DescribeSubnets
PutResourcePolicy	AWS CloudHSM リソースにポリシーをアタッチするアクセス許可を付与します	書き込み	backup*		
RestoreBackup	指定された CloudHSM バックアップを復元するための許可を付与します	書き込み	backup*		
TagResource	指定された AWS CloudHSM クラスターの 1 つ以上のタグを追加または上書きするアクセス許可を付与します	Tagging	backup		
			cluster		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	指定された AWS CloudHSM クラスターから指定されたタグを削除するアクセス許可を付与します	Tagging	backup		
			cluster		
				aws:TagKeys	

AWS CloudHSM で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
backup	`arn:${Partition}:cloudhsm:${Region}:${Account}:backup/${CloudHsmBackupInstanceName}`	aws:ResourceTag/${TagKey}
cluster	`arn:${Partition}:cloudhsm:${Region}:${Account}:cluster/${CloudHsmClusterInstanceName}`	aws:ResourceTag/${TagKey}

AWS CloudHSM の条件キー

AWS CloudHSM では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

Amazon CloudSearch のアクション、リソース、および条件キー

Amazon CloudSearch (サービスプレフィックス: cloudsearch) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CloudSearch で定義されるアクション
- Amazon CloudSearch で定義されるリソースタイプ

- Amazon CloudSearch の条件キー

Amazon CloudSearch で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AddTags	Amazon CloudSearch ドメインにリソースタグをアタッチします	Tagging	domain*		
BuildSuggesters	検索候補インデックスを作成します	書き込み	domain*		
CreateDomain	新しい検索ドメインを作成します	書き込み	domain*		
DefineAnalysisScheme	テキストまたはテキスト配列のフィールドに適用可能な分析スキームを設定し、言語固有のテキスト処理オプションを定義します	書き込み	domain*		
DefineExpression	検索ドメインの Expression を設定します	書き込み	domain*		
DefineIndexField	検索ドメインの IndexField を設定します	書き込み	domain*		
DefineSuggester	ドメインのサジェスタを設定します	書き込み	domain*		
DeleteAnalysisScheme	分析スキームを削除します	書き込み	domain*		
DeleteDomain	検索ドメインとそのすべてのデータを完全に削除します	書き込み	domain*		
DeleteExpression	検索ドメインから Expression を削除します	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteIndexField	検索ドメインから IndexField を削除します	書き込み	domain*		
DeleteSuggester	サジェスタを削除します	書き込み	domain*		
DescribeAnalysisSchemes	ドメインに設定された分析スキームを取得します	読み取り	domain*		
DescribeAvailabilityOptions	ドメインに設定された可用性オプションを取得します	読み取り	domain*		
DescribeDomainEndpointOptions	ドメインに設定されたドメインエンドポイントオプションを取得します	読み取り	domain*		
DescribeDomains	このアカウントが所有する検索ドメインに関する情報を取得します	リスト	domain*		
DescribeExpressions	検索ドメインに設定された式を取得します	読み取り	domain*		
DescribeIndexFields	検索ドメインに設定されたインデックスフィールドに関する情報を取得します	読み取り	domain*		
DescribeScalingParameters	ドメインに設定されたスケーリングパラメータを取得します	読み取り	domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeServiceAccessPolicies	ドメインのドキュメントと検索エンドポイントへのアクセスを制御するアクセスポリシーに関する情報を取得します	読み取り	domain*		
DescribeSuggesters	ドメインに設定されたサジェスタを取得します	読み取り	domain*		
IndexDocuments	検索ドメインに、最新のインデックス作成オプションを使用してドキュメントのインデックス作成を開始するように指示します	書き込み	domain*		
ListDomainNames	アカウントが所有するすべての検索ドメインを一覧表示します	リスト	domain*		
ListTags	Amazon CloudSearch ドメインのすべてのリソースタグを表示します	読み取り	domain*		
RemoveTags	Amazon ES ドメインから指定したリソースタグを削除します	Tagging	domain*		
UpdateAvailabilityOptions	ドメインの可用性オプションを設定します	書き込み	domain*		
UpdateDomainEndpointOptions	ドメインのドメインエンドポイントオプションを設定します	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateScalingParameters	ドメインのスケーリングパラメータを設定します	書き込み	domain*		
UpdateServiceAccessPolicies	ドメインのドキュメントおよび検索エンドポイントへのアクセスを制御するアクセスルールを設定します	権限の管理	domain*		
document [許可のみ]	ドキュメントサービスオペレーションへのアクセスを許可します	書き込み	domain		
search [アクセス許可のみ]	検索オペレーションへのアクセスを許可します	読み取り	domain		
suggest [許可のみ]	提案オペレーションへのアクセスを許可します	読み取り	domain		

Amazon CloudSearch で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

> **Note**
>
> IAM ポリシーで Amazon CloudSearch のリソース ARN を使用する方法については、Amazon CloudSearch 開発者ガイドの「Amazon CloudSearch の ARN」を参照してください。

リソースタイプ	ARN	条件キー
domain	arn:${Partition}:cloudsearch:${Region}:${Account}:domain/${DomainName}	

Amazon CloudSearch の条件キー

CloudSearch には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS CloudShell のアクション、リソース、および条件キー

AWS CloudShell (サービスプレフィックス: cloudshell) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS CloudShell で定義されるアクション
- AWS CloudShell で定義されるリソースタイプ
- AWS CloudShell の条件キー

AWS CloudShell で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ApproveCommand [アクセス許可のみ]	別の AWS サービスによって送信されたコマンドを承認するアクセス許可を付与します	読み取り	Environment*		
CreateEnvironment [許可のみ]	CloudShell 環境を作成するアクセス許可を付与します	Write		cloudshell:SecurityGroupIds cloudshell:SubnetIds cloudshell:VpcIds	
CreateSession [アクセス許可のみ]	から CloudShell 環境に接続するアクセス許可を付与します AWS Management Console	書き込み	Environment*		
DeleteEnvironment [アクセス許可のみ]	CloudShell 環境を削除する許可を付与	Write	Environment*		
DescribeEnvironments [アクセス許可のみ]	既存のユーザーの環境の説明を返す許可を付与する	リスト			
GetEnvironmentStatus [許可のみ]	CloudShell 環境のステータスを読み取るアクセス許可を付与	Read	Environment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetFileDownloadUrls [許可のみ]	CloudShell 環境からファイルをダウンロードするアクセス許可を付与します	Write	Environment*		
GetFileUploadUrls [アクセス許可のみ]	CloudShell 環境にファイルをアップロードするアクセス許可を付与します	Write	Environment*		
PutCredentials [アクセス許可のみ]	コンソール認証情報を環境に転送するアクセス許可を付与します	Write	Environment*		
StartEnvironment [アクセス許可のみ]	停止した CloudShell 環境を開始する許可を付与	Write	Environment*		
StopEnvironment [アクセス許可のみ]	実行中の CloudShell 環境を停止する許可を付与	Write	Environment*		

AWS CloudShell で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Environment	arn:${Partition}:cloudshell:${Region}:${Account}:environment/${EnvironmentId}	

AWS CloudShell の条件キー

AWS CloudShell では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
cloudshell:SecurityGroupIds	セキュリティグループ ID によってアクセスをフィルターします。CreateEnvironment 操作中に使用できます	ArrayOfString
cloudshell:SubnetIds	サブネット ID でアクセスをフィルタリングします。CreateEnvironment 操作中に使用できます	ArrayOfString
cloudshell:VpcIds	VPC ID でアクセスをフィルタリングします。CreateEnvironment 操作中に使用できます	ArrayOfString

AWS CloudTrail のアクション、リソース、および条件キー

AWS CloudTrail (サービスプレフィックス: cloudtrail) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS CloudTrail で定義されるアクション
- AWS CloudTrail で定義されるリソースタイプ
- AWS CloudTrail の条件キー

AWS CloudTrail で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddTags	1 つ以上のタグを証跡、イベントデータストア、チャネル、またはダッシュボードに追加するアクセス許可を最大 50 個まで付与します	Tagging	channel		
			dashboard		
			eventdatastore		
			trail		
				aws:RequestTag/${TagKey} aws:TagKeys	
CancelQuery	実行中のクエリをキャンセルする許可を付与。	書き込み	eventdatastore*		
CreateChannel	チャネルを作成する許可を付与	書き込み	channel*		cloudtrail:AddTags

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			eventdatastore*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDashboard	ダッシュボードを作成するアクセス許可を付与します	書き込み	dashboard*		cloudtrail:AddTags cloudtrail:StartDashboardRefresh cloudtrail:StartQuery
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateEventDataStore	イベントデータストアを作成する許可を付与	書き込み	eventdatastore*		cloudtrail:AddTags iam:CreateServiceLinkedRole iam:GetRole kms:Decrypt kms:GenerateDataKey organizations:ListAWSServiceAccessForOrganization
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateServiceLinkedChannel [アクセス許可のみ]	への口グデータの配信設定を指定する AWS サービスにリンクされたチャネルを作成するアクセス許可を付与します	書き込み	channel*		
CreateTrail	Amazon S3 バケットに口グデータを配信するための設定を指定する証跡を作成する許可を付与。	書き込み	trail*		cloudtrail:AddTags iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	チャネルを削除する許可を付与。	書き込み	channel*		
DeleteDashboard	ダッシュボードを削除する許可を付与	書き込み	dashboard*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteEventDataStore	イベントデータストアを削除する許可を付与	書き込み	eventdatastore*		
DeleteResourcePolicy	指定されたリソースからリソースポリシーを削除するための許可を付与します	書き込み	channel		
			dashboard		
			eventdatastore		
DeleteServiceLinkedChannel [アクセス許可のみ]	サービスにリンクされたチャンネルを削除するアクセス許可を付与	書き込み	channel*		
DeleteTrail	証跡を削除する許可を付与。	書き込み	trail*		
DeregisterOrganizationDelegatedAdmin	AWS Organizations メンバーアカウントを委任管理者として登録解除する許可を付与	書き込み			organizations:DeregisterDelegatedAdministrator organizations:ListAWSServiceAccessForOrganization
DescribeQuery	クエリの詳細を一覧表示する許可を付与	読み込み	eventdatastore*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeTrails	アカウントに設定されている現在のリージョンに関連付けられている証跡の設定を一覧表示する許可を付与。	読み取り			
DisableFederation	AWS Glue データカタログを使用してイベントデータストアデータのフェデレーションを無効にするアクセス許可を付与します	書き込み	eventdatastore*		glue:DeleteDatabase glue:DeleteTable glue:PassConnection lakeformation:DeregisterResource lakeformation:RegisterResource

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
EnableFederation	AWS Glue データカタログを使用してイベントデータストアデータのフェデレーションを有効にするアクセス許可を付与します	書き込み	eventdatastore*		glue:CreateDatabase glue:CreateTable iam:GetRole iam:PassRole lakeformation:DeregisterResource lakeformation:RegisterResource
GenerateQuery	CloudTrail Lake クエリジェネレーターを使用して、指定されたイベントデータストアのクエリを生成する許可を付与する	書き込み	eventdatastore*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GenerateQueryResultsSummary [アクセス許可のみ]	CloudTrail 自然言語ジェネレーターを使用して、指定されたクエリの結果概要を生成するアクセス許可を付与します	読み取り	eventdatastore*		cloudtrail:GetQueryResults kms:Decrypt kms:GenerateDataKey
GetChannel	特定のチャネルについての情報を返すアクセス許可を付与	読み取り	channel*		
GetDashboard	ダッシュボードの設定を一覧表示するアクセス許可を付与します	読み取り	dashboard*		
GetEventConfiguration	イベントデータストア用に設定されたイベント設定を一覧表示するアクセス許可を付与します	読み取り	eventdatastore*		
GetEventDataStore	イベントデータストアの設定を一覧表示する許可を付与	読み取り	eventdatastore*		
GetEventDataStoreData	AWS Glue データカタログを使用してイベントデータストアからデータを取得する許可を付与	読み取り	eventdatastore*		kms:Decrypt kms:GenerateDataKey

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetEventSelectors	証跡用に設定されたイベントセレクタの設定を一覧表示する許可を付与。	読み取り	trail*		
GetImport	特定のインポートについての情報を返すアクセス許可を付与	読み取り			
GetInsightSelectors	証跡またはイベントデータストア用に設定されている CloudTrail Insights セレクタを一覧表示する許可を付与	読み取り	eventdatastore		
			trail		
GetQueryResults	完了したクエリの結果を取得する許可を付与	読み取り	eventdatastore*		kms:Decrypt kms:GenerateDataKey
GetResourcePolicy	指定されたリソースにアタッチされたリソースポリシーを取得するための許可を付与します	読み取り	channel		
			dashboard		
			eventdatastore		
GetServiceLinkedChannel [許可のみ]	サービスにリンクされたチャンネルの設定を一覧表示するアクセス許可を付与	読み取り	channel*		
GetTrail	証跡の設定を一覧表示する許可を付与。	読み込み	trail*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetTrailStatus	指定された証跡に関する情報が記載された JSON 形式のリストを取得する許可を付与。	読み取り	trail*		
ListChannels	現在のアカウントでチャンネル、およびそのソース名を一覧表示するアクセス許可を付与	リスト			
ListDashboards	アカウントの現在のリージョンに関連付けられているダッシュボードを一覧表示するアクセス許可を付与します	リスト			
ListEventDataStores	アカウントの現在のリージョンに関連付けられたイベントデータストアを一覧表示する許可を付与	リスト			
ListImportFailures	指定したインポートの失敗のリストを返すアクセス許可を付与	読み取り			
ListImports	ImportStatus または Destination 別にすべてのインポート情報、または特定のインポートセットに関する情報を返すアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListPublicKeys	指定された時間範囲内の、対応するプライベートキーが証跡ダイジェストファイルの署名に使用されたパブリックキーを一覧表示する許可を付与。	読み込み			
ListQueries	イベントデータストアに関連付けられたクエリを一覧表示する許可を付与	リスト	eventdatastore*		
ListServiceLinkedChannels [許可のみ]	指定されたアカウントの、現在のリージョンに関連付けられている、サービスにリンクされたチャンネルを一覧表示するアクセス許可を付与	リスト			
ListTags	現在のリージョンの証跡、イベントデータストア、チャネル、またはダッシュボードのタグを一覧表示するアクセス許可を付与します	読み取り	channel		
			dashboard		
			eventdatastore		
			trail		
ListTrails	アカウントに設定されている現在のリージョンに関連付けられている証跡を一覧表示する許可を付与。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
LookupEvents	CloudTrail でキャプチャされた API アクティビティイベントのメトリクスデータを検索して取得し、アカウントのリソースを作成、更新、または削除する許可を付与する	読み取り			
PutEventConfiguration	イベントデータストアのイベント設定を作成および更新するアクセス許可を付与します	書き込み	eventdatastore*		iam:CreateServiceLinkedRole iam:GetRole
PutEventSelectors	証跡のイベントセレクタを作成および更新する許可を付与。	書き込み	trail*		
PutInsightSelectors	証跡またはイベントデータストア用の CloudTrail Insights セレクタを作成および更新する許可を付与	書き込み	eventdatastore		
			trail		
PutResourcePolicy	指定されたリソースにリソースポリシーをアタッチするための許可を付与します	書き込み	channel		
			dashboard		
			eventdatastore		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RegisterOrganizationDelegatedAdmin	AWS Organizations メンバーアカウントを委任管理者として登録する許可を付与	書き込み			iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization organizations:RegisterDelegatedAdministrator
RemoveTags	証跡、イベントデータストア、チャネル、またはダッシュボードからタグを削除するアクセス許可を付与します	Tagging	channel		
			dashboard		
			eventdatastore		
			trail		
				aws:TagKeys	
RestoreEventDataStore	イベントデータストアを復元する許可を付与	書き込み	eventdatastore*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SearchSampleQueries	CloudTrail Lake サンプルクエリのセマンティック検索を実行するアクセス許可を付与します	読み取り			
StartDashboardRefresh	指定されたダッシュボードで更新を開始するアクセス許可を付与します	書き込み	dashboard*		cloudtrail:StartQuery
StartEventDataStoreIngestion	イベントデータストアで取り込みを開始する許可を付与	書き込み	eventdatastore*		
StartImport	ログに記録されたトレイルイベントのソース S3 バケットから宛先のイベントデータストアへのインポートを開始するアクセス許可を付与	書き込み			
StartLogging	証跡の AWS API コールとログファイル配信の記録を開始するアクセス許可を付与します	書き込み	trail*		
StartQuery	指定したイベントデータストアで新しいクエリを開始する許可を付与	書き込み	eventdatastore*		kms:Decrypt kms:GenerateDataKey
StopEventDataStoreIngestion	イベントデータストアで取り込みを停止する許可を付与	書き込み	eventdatastore*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StopImport	指定されたインポートを停止するアクセス許可を付与	書き込み			
StopLogging	証跡の AWS API コールとログファイルの配信の記録を停止するアクセス許可を付与します	書き込み	trail*		
UpdateChannel	チャネルを更新する許可を付与	書き込み	channel*		
UpdateDashboard	ダッシュボードを更新する許可を付与	書き込み	dashboard*		cloudtrail:StartDashboardRefresh cloudtrail:StartQuery

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateEventDataStore	イベントデータストアを更新する許可を付与	書き込み	eventdatastore*		iam:CreateServiceLinkedRole iam:GetRole kms:Decrypt kms:GenerateDataKey organizations:ListAWSServiceAccessForOrganization
UpdateServiceLinkedChannel [アクセス許可のみ]	サービスにリンクされたチャネル設定を更新して AWS サービスにログデータを配信するアクセス許可を付与します	書き込み	channel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateTrail	ログファイルの配信を指定する設定を更新する許可を付与。	書き込み	trail*		iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization

AWS CloudTrail で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

> **Note**
>
> CloudTrail アクションへのアクセスを制御するポリシーの場合、Resource 要素は常に "*" に設定します。IAM ポリシーでリソース ARNsAWS CloudTrail 「 ユーザーガイド」の「How AWS CloudTrail works with IAM」を参照してください。

リソースタイプ	ARN	条件キー
trail	arn:${Partition}:cloudtrail:${Region}:${Account}:trail/${TrailName}	aws:ResourceTag/${TagKey}
eventdatastore	arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/${EventDataStoreId}	aws:ResourceTag/${TagKey}
channel	arn:${Partition}:cloudtrail:${Region}:${Account}:channel/${ChannelId}	aws:ResourceTag/${TagKey}
dashboard	arn:${Partition}:cloudtrail:${Region}:${Account}:dashboard/${DashboardName}	aws:ResourceTag/${TagKey}

AWS CloudTrail の条件キー

AWS CloudTrail では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアによるアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされたタグでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString

AWS CloudTrail Data のアクション、リソース、および条件キー

AWS CloudTrail Data (サービスプレフィックス: `cloudtrail-data`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS CloudTrail Data によって定義されたアクション
- AWS CloudTrail Data で定義されるリソースタイプ
- AWS CloudTrail Data の条件キー

AWS CloudTrail Data によって定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutAuditEvents	アプリケーションイベントを CloudTrail Lake に取り込むための許可を付与します	書き込み	channel*		

AWS CloudTrail Data で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

> **Note**
>
> CloudTrail アクションへのアクセスを制御するポリシーの場合、Resource 要素は常に "*" に設定します。IAM ポリシーでリソース ARNs「 AWS CloudTrail ユーザーガイド」の「How AWS CloudTrail works with IAM」を参照してください。

リソースタイプ	ARN	条件キー
channel	`arn:${Partition}:cloudtrail:${Region}:${Account}:channel/${ChannelId}`	aws:ResourceTag/${TagKey}

AWS CloudTrail Data の条件キー

AWS CloudTrail Data では、IAM ポリシーの `Condition`要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグのキーと値でアクセスをフィルター	文字列
aws:ResourceTag/${TagKey}	リクエスト内のタグキーと値のペアのプレゼンスに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon CloudWatch のアクション、リソース、および条件キー

Amazon CloudWatch (サービスプレフィックス: cloudwatch) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CloudWatch で定義されるアクション
- Amazon CloudWatch で定義されるリソースタイプ
- Amazon CloudWatch の条件キー

Amazon CloudWatch で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchGetServiceLevelIndicatorReport	サービスレベル指標レポートを一括取得するためのアクセス許可を付与	読み取り			
BatchGetServiceLevelObjectiveBudgetReport	サービスレベル目標の予算レポートを一括取得するためのアクセス許可を付与	読み取り	slo*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateServiceLevelObjective	サービスレベル目標を作成するためのアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlarms	アラームのコレクションを削除する許可を付与。	書き込み	alarm*		
DeleteAnomalyDetector	指定した異常検出モデルをアカウントから削除する許可を付与。	書き込み			
DeleteDashboards	指定したすべての CloudWatch ダッシュボードを削除する許可を付与	書き込み	dashboard*		
DeleteInsightRules	インサイトルールのコレクションを削除する許可を付与。	書き込み	insight-rule*		
DeleteMetricStream	指定した CloudWatch メトリックストリームを削除する許可を付与。	書き込み	metric-stream*		
DeleteServiceLevelObjective	サービスレベル目標を削除するためのアクセス許可を付与	書き込み	slo*		
DescribeAlarmHistory	指定したアラームの履歴を取得する許可を付与。	読み込み	alarm*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeAlarms	ユーザーのアカウントが現在所有しているすべてのアラームを記述する許可を付与。	読み込み	alarm*		
DescribeAlarmsForMetric	ユーザーのアカウントが現在所有している、指定したメトリクスで設定されているすべてのアラームを記述する許可を付与。	読み込み			
DescribeAnomalyDetectors	アカウントで作成した異常検出モデルを一覧表示する許可を付与。	読み込み			
DescribeInsightRules	ユーザーのアカウントが現在所有しているすべてのインサイトルールを記述する許可を付与。	読み込み			
DisableAlarmActions	アラームのコレクションに対するアクションを無効にする許可を付与。	書き込み	alarm*		
DisableInsightRules	インサイトルールのコレクションを無効にする許可を付与。	書き込み	insight-rule*		
EnableAlarmActions	アラームのコレクションに対するアクションを有効にする許可を付与。	書き込み	alarm*		
EnableInsightRules	インサイトルールのコレクションを有効にする許可を付与。	書き込み	insight-rule*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
EnableTopologyDiscovery	CloudWatch トポロジ検出を有効にするためのアクセス許可を付与	書き込み			
GenerateQuery	自然言語プロンプトからメトリクスインサイトまたはログインサイトクエリ文字列を生成するためのアクセス許可を付与	読み取り			
GenerateQueryResultsSummary	生成 AI を使用して自然言語で CloudWatch LogInsights クエリ結果の概要を生成するアクセス許可を付与します	読み取り			
GetDashboard	指定した CloudWatch ダッシュボードの詳細を表示する許可を付与。	読み込み	dashboard*		
GetInsightRuleReport	特定のインサイトルールについて、時間範囲内で一意のコントリビュータの top-N レポートを返すアクセス許可を付与します。	読み込み	insight-rule*		
GetMetricData	CloudWatch メトリクスデータのバッチ容量を取得し、取得したデータで Metric Math を行うアクセス許可を付与します。	読み込み			
GetMetricStatistics	指定したメトリクスの統計を取得する許可を付与。	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetMetricStream	CloudWatch メトリックストリームの詳細を返すアクセス許可を付与します。	読み込み	metric-stream*		
GetMetricWidgetImage	メトリクスウィジェットのスナップショットを取得する許可を付与	読み取り			
GetService	サービスに関する情報を取得するためのアクセス許可を付与	読み取り	service*		
GetServiceData [許可のみ]	サービスデータを取得するためのアクセス許可を付与	読み取り	service*		
GetServiceLevelObjective	サービスレベル目標に関する情報を取得するためのアクセス許可を付与	読み取り	slo*		
GetTopologyDiscoveryStatus [許可のみ]	CloudWatch トポロジ検出ステータスを取得するためのアクセス許可を付与	読み取り			
GetTopologyMap	CloudWatch トポロジマップを取得するためのアクセス許可を付与	読み取り			
Link [許可のみ]	モニタリングアカウントに CloudWatch リソースを共有する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListDashboards	アカウント内のすべてのCloudWatch ダッシュボードのリストを返すアクセス許可を付与します。	リスト			
ListEntitiesForMetric [許可のみ]	特定のメトリクスを出力するすべてのエンティティを取得するアクセス許可を付与します	リスト			
ListManagedInsightRules	特定のリソース ARN で使用可能なマネージド型インサイトルールを一覧表示する許可を付与	読み取り		aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestManagedResourceARNs	
ListMetricStreams	アカウント内のすべてのCloudWatch メトリックストリームのリストを返すアクセス許可を付与します。	リスト			
ListMetrics	AWS アカウント 所有者に保存されている有効なメトリクスのリストを取得するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListServiceLevelObjectives	サービスレベル目標を一覧表示するためのアクセス許可を付与	リスト			
ListServices	サービスを一覧表示する許可を付与	リスト			
ListTagsForResource	Amazon CloudWatch リソースのタグを一覧表示する許可を付与。	リスト	alarm		
			insight-rule		
			slo		
	シナリオ: CloudWatch-Alarm		alarm*		
	シナリオ: CloudWatch-Insight Rule		insight-rule*		
	シナリオ: CloudWatch-ServiceLevelObjective		slo*		
PutAnomalyDetector	CloudWatch メトリクスの異常検出モデルを作成または更新する許可を付与。	書き込み			
PutCompositeAlarm	複合アラームを作成または更新する許可を付与。	書き込み	alarm*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:AlarmActions	
PutDashboard	CloudWatch ダッシュボードを作成したり、既存のダッシュボード (存在する場合) を更新したりする許可を付与。	書き込み	dashboard*		
PutInsightRule	新しいインサイトルールを作成したり、既存のインサイトルールを置き換えるアクセス許可を付与します。	書き込み	insight-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestInsightRuleLogGroups	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutManagedInsightRules	マネージド型インサイトルールを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestManagedResourceARNs	
PutMetricAlarm	アラームを作成または更新するアクセス許可を付与し、指定した Amazon CloudWatch メトリクスに関連付けます。	書き込み	alarm*	aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:AlarmActions	
PutMetricData	メトリクスデータポイントを Amazon CloudWatch に発行する許可を付与。	書き込み		cloudwatch:namespace	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutMetricStream	CloudWatch メトリックストリームを作成するアクセス許可を、既存のメトリックストリームがすでに存在する場合は、既存のメトリックストリームを更新する許可を付与。	書き込み	metric-stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
SetAlarmState	テスト目的でアラームの状態を一時的に設定する許可を付与。	書き込み	alarm*		
StartMetricStreams	指定したすべての CloudWatch メトリックストリームを開始する許可を付与。	書き込み	metric-stream*		
StopMetricStreams	指定したすべての CloudWatch メトリックストリームを停止する許可を付与。	書き込み	metric-stream*		
TagResource	Amazon CloudWatch リソースにタグを追加する許可を付与。	タグ付け	alarm		
			insight-rule		
			slo		
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	シナリオ: CloudWatch-Alarm		alarm*		
	シナリオ: CloudWatch-Insight Rule		insight-rule*		
	シナリオ: CloudWatch-ServiceLevelObjective		slo*		
UntagResource	Amazon CloudWatch リソースからタグを削除する許可を付与。	タグ付け	alarm		
			insight-rule		
			slo		
				aws:TagKeys	
	シナリオ: CloudWatch-Alarm		alarm*		
	シナリオ: CloudWatch-Insight Rule		insight-rule*		
	シナリオ: CloudWatch-ServiceLevelObjective		slo*		
UpdateServiceLevelObjective	サービスレベル目標を更新するためのアクセス許可を付与	書き込み	slo*		

Amazon CloudWatch で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
alarm	arn:${Partition}:cloudwatch:${Region}:${Account}:alarm:${AlarmName}	aws:ResourceTag/${TagKey}
dashboard	arn:${Partition}:cloudwatch::${Account}:dashboard/${DashboardName}	
insight-rule	arn:${Partition}:cloudwatch:${Region}:${Account}:insight-rule/${InsightRuleName}	aws:ResourceTag/${TagKey}
metric-stream	arn:${Partition}:cloudwatch:${Region}:${Account}:metric-stream/${MetricStreamName}	aws:ResourceTag/${TagKey}
slo	arn:${Partition}:cloudwatch:${Region}:${Account}:slo/${SloName}	aws:ResourceTag/${TagKey}
service	arn:${Partition}:cloudwatch:${Region}:${Account}:service/${ServiceName}-${UniqueAttributesHex}	aws:ResourceTag/${TagKey}

Amazon CloudWatch の条件キー

Amazon CloudWatch は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	各タグで許可されている値のセットに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられている tag-value に基づいてアクションをフィルタリングします。	文字列
aws:TagKeys	リクエスト内の必須タグのプレゼンスに基づいてアクションをフィルタリングします	ArrayOfString
cloudwatch:AlarmActions	定義されたアラームアクションに基づいてアクションをフィルターします	ArrayOfString
cloudwatch:namespace	オプションの名前空間値の存在に基づいてアクションをフィルタリングします。	String
cloudwatch:requestInsightRuleLogGroups	インサイトルールで指定されたロググループに基づいてアクションをフィルタリングします	ArrayOfString
cloudwatch:requestManagedResourceARNs	マネージド型インサイトルールで指定されたリソース ARN によってアクセスをフィルタリングします	ArrayOfARN

Amazon CloudWatch Application Insights のアクション、リソース、および条件キー

Amazon CloudWatch Application Insights (サービスプレフィックス: `applicationinsights`) では、IAM 許可ポリシーで使用できるように、次のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CloudWatch Application Insights で定義されるアクション
- Amazon CloudWatch Application Insights で定義されるリソースタイプ
- Amazon CloudWatch Application Insights の条件キー

Amazon CloudWatch Application Insights で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddWorkload	ワークロードを追加する許可を付与	書き込み			
CreateApplication	リソースグループからアプリケーションを作成する許可を付与	Write			
CreateComponent	リソースグループからコンポーネントを作成する許可を付与	Write			
CreateLogPattern	ログにパターンを作成する許可を付与	Write			
DeleteApplication	アプリケーションを削除する許可を付与	Write			
DeleteComponent	コンポーネントを削除する許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteLogPattern	ログパターンを削除する許可を付与	Write			
DescribeApplication	アプリケーションを記述する許可を付与	Read			
DescribeComponent	コンポーネントを記述する許可を付与	Read			
DescribeComponentConfiguration	コンポーネントの設定を記述する許可を付与	Read			
DescribeComponentConfigurationRecommendation	推奨されるアプリケーションコンポーネント設定を記述する許可を付与	Read			
DescribeLogPattern	ログパターンを記述する許可を付与	Read			
DescribeObservation	観測を記述する許可を付与	Read			
DescribeProblem	問題を記述する許可を付与	Read			
DescribeProblemObservations	問題内の観測を記述する許可を付与	読み取り			
DescribeWorkload	ワークロードを記述する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
Link [許可のみ]	モニタリングアカウントに Application Insights リソースを共有する許可を付与	書き込み			
ListApplications	すべてのアプリケーションを一覧表示する許可を付与	リスト			
ListComponents	アプリケーションのコンポーネントを一覧表示する許可を付与	リスト			
ListConfigurationHistory	設定履歴を一覧表示する許可を付与	リスト			
ListLogPatternSets	アプリケーションのログパターンセットを一覧表示する許可を付与	リスト			
ListLogPatterns	ログパターンを一覧表示する許可を付与	リスト			
ListProblems	アプリケーション内の問題を一覧表示する許可を付与	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り			
ListWorkloads	ワークロードを一覧表示する許可を付与	リスト			
RemoveWorkload	ワークロードを削除する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け		aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースのタグを解除する許可を付与	タグ付け		aws:TagKeys	
UpdateApplication	アプリケーションを更新する許可を付与	Write			
UpdateComponent	コンポーネントを更新するアクセス許可の付与します	Write			
UpdateComponentConfiguration	コンポーネントの設定を更新する許可を付与	Write			
UpdateLogPattern	ログパターンを更新する許可を付与	書き込み			
UpdateProblem	問題を更新する許可を付与	書き込み			
UpdateWorkload	ワークロードを更新する許可を付与	書き込み			

Amazon CloudWatch Application Insights で定義されるリソースタイプ

Amazon CloudWatch Application Insights では、IAM ポリシーステートメントの `Resource` 要素でのリソース ARN の指定はサポートされていません。Amazon CloudWatch Application Insights へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

Amazon CloudWatch Application Insights の条件キー

Amazon CloudWatch Application Insights は、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString

Amazon CloudWatch Application Signals のアクション、リソース、および条件キー

Amazon CloudWatch Application Signals (サービスプレフィックス: application-signals) では、IAM 許可ポリシーで使用できるように、次のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CloudWatch Application Signals で定義されるアクション
- Amazon CloudWatch Application Signals で定義されるリソースタイプ
- Amazon CloudWatch Application Signals の条件キー

Amazon CloudWatch Application Signals で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchGetServiceLevelObjectiveBudgetReport	サービスレベル目標の予算レポートを一括取得するためのアクセス許可を付与	読み取り	slo*		
BatchUpdateExclusionWindows	Amazon CloudWatch SLOs	書き込み	slo*		
CreateServiceLevelObjective	サービスレベル目標を作成するためのアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteServiceLevelObjective	サービスレベル目標を削除するためのアクセス許可を付与	書き込み	slo*		
GetService	サービスに関する情報を取得するためのアクセス許可を付与	読み取り			
GetServiceLevelObjective	サービスレベル目標に関する情報を取得するためのアクセス許可を付与	読み取り	slo*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
Link [許可のみ]	Application Signals リソースをモニタリングアカウントと共有するためのアクセス許可を付与します	書き込み			
ListObservedEntities	他のエンティティに関連付けられたエンティティを一覧表示するアクセス許可を付与します	リスト			
ListServiceDependencies	サービスの依存関係を一覧表示する許可を付与する	読み取り			
ListServiceDependents	サービスの依存関係を一覧表示する許可を付与する	読み取り			
ListServiceLevelObjectiveExclusionWindows	Amazon CloudWatch SLO の除外ウィンドウを一覧表示する許可を付与	リスト	slo*		
ListServiceLevelObjectives	サービスレベル目標を一覧表示するためのアクセス許可を付与	リスト			
ListServiceOperations	サービスオペレーションを一覧表示する許可を付与する	読み取り			
ListServices	サービスを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTagsForResource	Amazon CloudWatch SLO のタグを一覧表示する許可を付与する	読み取り	slo*		
StartDiscovery	CloudWatch 検出を有効にする許可を付与する	書き込み			
TagResource	Amazon CloudWatch SLO にタグを追加する許可を付与する	Tagging	slo*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Amazon CloudWatch SLO へのタグを解除する許可を付与する	Tagging	slo*		
				aws:TagKeys	
UpdateServiceLevelObjective	サービスレベル目標を更新するためのアクセス許可を付与	書き込み	slo*		

Amazon CloudWatch Application Signals で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
slo	arn:${Partition}:application-signals:${Region}:${Account}:slo/${SloName}	aws:ResourceTag/${TagKey}

Amazon CloudWatch Application Signals の条件キー

Amazon CloudWatch Application Signals は、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	各タグの許可された値のセットでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値でアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内の必須タグの存在でアクセスをフィルタリングします	ArrayOfString

Amazon CloudWatch Evidentlyのアクション、リソース、および条件キー

Amazon CloudWatch Evidently (サービスプレフィックス: evidently) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース,アクションおよび条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CloudWatch Evidentlyで定義されるアクション
- Amazon CloudWatch Evidentlyで定義されるリソースタイプ
- Amazon CloudWatch Evidentlyの条件キー

Amazon CloudWatch Evidentlyで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchEvaluateFeature	バッチ評価機能リクエストを送信するアクセス許可を付与	書き込み	Feature*		
CreateExperiment	実験を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFeature	特徴を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLaunch	起動を作成するためのアクセス許可を付与	書き込み		aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
CreateProject	プロジェクトを作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole iam:GetRole
CreateSegment	セグメントを作成するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteExperiment	実験を削除する許可を付与	書き込み	Experiment*		
DeleteFeature	特徴を削除する許可を付与	書き込み	Feature*		
DeleteLaunch	起動を削除するためのアクセス許可を付与	書き込み	Launch*		
DeleteProject	プロジェクトを削除する許可を付与	書き込み	Project*		
DeleteSegment	セグメントを削除するアクセス許可を付与	書き込み	Segment*		
EvaluateFeature	評価機能リクエストを送信するアクセス許可を付与	書き込み	Feature*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetExperiment	実験の詳細を取得する許可を付与	読み込み	Experiment*		
GetExperimentResults	実験結果を作成する許可を付与	読み込み	Experiment*		
GetFeature	特徴の詳細を取得する許可を付与	読み込み	Feature*		
GetLaunch	起動の詳細を取得する許可を付与	読み込み	Launch*		
GetProject	プロジェクトの詳細を取得する許可を付与	読み取り	Project*		
GetSegment	セグメントの詳細を取得するアクセス許可を付与	読み取り	Segment*		
ListExperiments	実験を一覧表示する許可を付与	読み込み			
ListFeatures	特徴を一覧表示する許可を付与	読み込み			
ListLaunches	起動を一覧表示するためのアクセス許可を付与	読み込み			
ListProjects	プロジェクトを一覧表示する許可を付与	読み取り			
ListSegmentReferences	セグメントを参照するリソースを一覧表示するアクセス許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListSegments	セグメントを一覧表示するアクセス許可を付与	読み取り			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み込み			
PutProjectEvents	パフォーマンスイベントを送信するアクセス許可を付与	書き込み	Project*		
StartExperiment	実験を開始する許可を付与	書き込み	Experiment*		
StartLaunch	起動を開始する許可を付与	書き込み	Launch*		
StopExperiment	実験を停止する許可を付与	書き込み	Experiment*		
StopLaunch	起動を停止する許可を付与	書き込み	Launch*		
TagResource	リソースにタグを付けるアクセス許可を付与	Tagging	Experiment		
			Feature		
			Launch		
			Project		
			Segment		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TestSegmentPattern	セグメントパターンをテストするアクセス許可を付与	読み取り			
UntagResource	リソースのタグを解除する許可を付与	Tagging	Experiment		
			Feature		
			Launch		
			Project		
			Segment		
				aws:TagKeys	
UpdateExperiment	実験を更新する許可を付与	書き込み	Experiment*		
UpdateFeature	特徴を更新するアクセス許可を付与	書き込み	Feature*		
UpdateLaunch	起動を更新するためのアクセス許可を付与	書き込み	Launch*		
UpdateProject	プロジェクトを更新する許可を付与	書き込み	Project*		iam:CreateServiceLinkedRole iam:GetRole
UpdateProjectDataDelivery	プロジェクトデータデリバリーを更新する許可を付与	書き込み	Project*		

Amazon CloudWatch Evidentlyで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Project	arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}	aws:ResourceTag/${TagKey}
Feature	arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}/feature/${FeatureName}	aws:ResourceTag/${TagKey}
Experiment	arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}/experiment/${ExperimentName}	aws:ResourceTag/${TagKey}
Launch	arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}/launch/${LaunchName}	aws:ResourceTag/${TagKey}
Segment	arn:${Partition}:evidently:${Region}:${Account}:segment/${SegmentName}	aws:ResourceTag/${TagKey}

Amazon CloudWatch Evidentlyの条件キー

Amazon CloudWatch Evidently は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義する許可を付与します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	IAM プリンシパルに代わってリクエストが渡されるタグによってアクセスをフィルタリングします。	String
aws:ResourceTag/${TagKey}	IAM プリンシパルに代わってリクエストを行うリソースに関連付けられているタグアクセスをフィルタリングします。	String
aws:TagKeys	IAMプリンシパルに代わってリクエストで渡されるタグキーでアクセスをフィルタリングします。	ArrayOfString

Amazon CloudWatch Internet Monitor のアクション、リソース、および条件キー

Amazon CloudWatch Internet Monitor (サービスプレフィックス: `internetmonitor`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース,アクションおよび条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CloudWatch Internet Monitor で定義されるアクション
- Amazon CloudWatch Internet Monitor で定義されるリソースタイプ
- Amazon CloudWatch Internet Monitor の条件キー

Amazon CloudWatch Internet Monitor で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateMonitor	モニターを作成するための許可を付与します	書き込み	Monitor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMonitor	モニターを削除するための許可を付与します	書き込み	Monitor*		
GetHealthEvent	指定されたモニターのヘルスイベントに関する情報を取得するための許可を付与します	読み取り	Monitor*		
GetInternetEvent	指定されたインターネットイベントに関する情報を取得する許可を付与する	読み取り	InternetEvent*		
GetMonitor	モニターに関する情報を取得するための許可を付与します	読み取り	Monitor*		
GetQueryResults	モニターのデータクエリの結果を取得するアクセス許可を付与します	読み取り	Monitor*		
GetQueryStatus	モニターのデータクエリのステータスを取得するアクセス許可を付与します	読み取り	Monitor*		
Link [許可のみ]	モニタリングアカウントとインターネットモニターリソースを共有する許可を付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListHealthEvents	モニターのすべてのヘルスイベントを一覧表示するための許可を付与します	リスト	Monitor*		
ListInternetEvents	すべてのインターネットイベントを一覧表示する許可を付与する	リスト			
ListMonitors	アカウント内のすべてのモニターとそのステータスを一覧表示するための許可を付与します	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	Monitor*		
StartQuery	モニターのデータクエリを開始するアクセス許可を付与します	読み取り	Monitor*		
StopQuery	モニターのデータクエリを停止するアクセス許可を付与します	読み取り	Monitor*		
TagResource	リソースにタグを追加する許可を付与	タグ付け	Monitor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	Tagging	Monitor*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
UpdateMonitor	モニターを更新するための許可を付与します	書き込み	Monitor*		

Amazon CloudWatch Internet Monitor で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
HealthEvent	arn:${Partition}:internetmonitor:${Region}:${Account}:monitor/${MonitorName}/health-event/${EventId}	aws:ResourceTag/${TagKey}
Monitor	arn:${Partition}:internetmonitor:${Region}:${Account}:monitor/${MonitorName}	aws:ResourceTag/${TagKey}
InternetEvent	arn:${Partition}:internetmonitor::${Account}:internet-event/${InternetEventId}	

Amazon CloudWatch Internet Monitor の条件キー

Amazon CloudWatch Internet Monitor では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに

絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon CloudWatch Logs のアクション、リソース、および条件キー

Amazon CloudWatch Logs (サービスプレフィックス: `logs`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CloudWatch Logs で定義されるアクション
- Amazon CloudWatch Logs で定義されるリソースタイプ
- Amazon CloudWatch Logs の条件キー

Amazon CloudWatch Logs で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateKmsKey	指定された AWS Key Management Service (AWS KMS) カスタマーマスターキー (CMK) を指定されたロググループに関連付けるアクセス許可を付与します	書き込み	log-group*		
CancelExportTask	保留中または実行中の状態の場合、エクスポートタスクをキャンセルする許可を付与	書き込み			
CreateDelivery	配信元を配信先に接続する配信を作成する許可を付与	書き込み	delivery*		
			delivery-destination*		
			delivery-source*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateExportTask	ロググループから Amazon S3 バケットにデータを効率的にエクスポートできる ExportTask を作成する許可を付与	書き込み	log-group*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateLogAnomalyDetector	ログの異常ディテクターを作成するためのアクセス許可を付与	書き込み	log-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLogDelivery [アクセス許可のみ]	ログ配信を作成する許可を付与	書き込み			
CreateLogGroup	指定された名前で新しいロググループを作成する許可を付与	書き込み	log-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLogStream	指定された名前で新しいログストリームを作成する許可を付与	書き込み	log-stream*		
DeleteAccountPolicy	アカウントポリシーを削除するアクセス許可を付与します	書き込み			
DeleteDataProtectionPolicy	ロググループにアタッチされたデータ保護ポリシーを削除する許可を付与	書き込み	log-group*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteDelivery	配信を削除する許可を付与	書き込み	delivery*		
DeleteDeliveryDestination	関連付けられた配信のすべてが削除された後で配信先を削除する許可を付与	書き込み	delivery-destination*		
DeleteDeliveryDestinationPolicy	配信先に関連付けられた配信先ポリシーを削除する許可を付与	書き込み	delivery-destination*		
DeleteDeliverySource	関連付けられた配信のすべてが削除された後で配信元を削除する許可を付与	書き込み	delivery-destination*		
DeleteDestination	指定された名前の送信先を削除する許可を付与	書き込み	destination*		
DeleteIndexPolicy	ロググループにアタッチされたインデックスポリシーを削除するアクセス許可を付与します	書き込み			
DeleteIntegration	統合を削除するアクセス許可を付与します	書き込み			
DeleteLogAnomalyDetector	ログの異常ディテクターを削除するためのアクセス許可を付与	書き込み	anomaly-detector*		
DeleteLogDelivery [アクセス許可のみ]	指定されたログ配信のログ配信情報を削除する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteLogGroup	指定された名前のロググループを削除する許可を付与	書き込み	log-group*		
DeleteLogStream	ログストリームを削除する許可を付与	書き込み	log-stream*		
DeleteMetricFilter	指定されたロググループに関連付けられたメトリクスフィルターを削除する許可を付与	書き込み	log-group*		
DeleteQueryDefinition	保存された CloudWatch Logs Insights のクエリ定義を削除する許可を付与	書き込み			
DeleteResourcePolicy	このアカウントからリソースポリシーを削除する許可を付与	権限の管理			
DeleteRetentionPolicy	指定されたロググループの保持ポリシーを削除する許可を付与	書き込み	log-group*		
DeleteSubscriptionFilter	指定されたロググループに関連付けられたサブスクリプションフィルターを削除する許可を付与	書き込み	log-group*		
DeleteTransformer	指定されたロググループに関連付けられたトランスフォーマーを削除するアクセス許可を付与します	書き込み	log-group*		
DescribeAccountPolicies	アカウントポリシーを取得するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeConfigurationTemplates	利用可能なログタイプの設定テンプレートのリストを取得する許可を付与する	リスト			
DescribeDeliveries	アカウント内の配信のリストを取得する許可を付与	リスト			
DescribeDeliveryDestinations	アカウント内の配信先のリストを取得する許可を付与	リスト			
DescribeDeliverySources	アカウント内の配信元のリストを取得する許可を付与	リスト			
DescribeDestinations	リクエスト AWS アカウントを行う に関連付けられているすべての送信先を返すアクセス許可を付与します	リスト			
DescribeExportTasks	リクエスト AWS アカウントを行う に関連付けられているすべてのエクスポートタスクを返すアクセス許可を付与します	リスト			
DescribeFieldIndexes	ロググループにアタッチされているすべてのインデックス作成属性を返すアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeIndexPolicies	ロググループにアタッチされているすべてのインデックスポリシーを返すアクセス許可を付与します	リスト			
DescribeLogGroups	リクエスト AWS アカウントを行う に関連付けられているすべてのロググループを返すアクセス許可を付与します	リスト			
DescribeLogStreams	指定されたロググループに関連付けられているすべてのログストリームを返す許可を付与	リスト	log-group *		
DescribeMetricFilters	指定されたロググループに関連付けられているすべてのメトリクスフィルターを返す許可を付与	リスト	log-group *		
DescribeQueries	このアカウントでスケジュールされている、実行されている、または最近実行された CloudWatch Logs Insights クエリのリストを返す許可を付与	リスト			
DescribeQueryDefinitions	保存した CloudWatch Logs Insights のクエリ定義のページ分割されたリストを返す許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeResourcePolicies	このアカウントのすべてのリソースポリシーを返す許可を付与	リスト			
DescribeSubscriptionFilters	指定されたロググループに関連付けられているすべてのサブスクリプションフィルターを返す許可を付与	リスト	log-group*		
DisassociateKmsKey	関連付けられた AWS Key Management Service (AWS KMS) カスタマーマスターキー (CMK) と指定されたロググループの関連付けを解除するアクセス許可を付与します	書き込み	log-group*		
FilterLogEvents	指定されたロググループから、オプションのフィルターパターンによってフィルタリングされたログイベントを取得する許可を付与	読み取り	log-group*		
GetDataProtectionPolicy	ロググループにアタッチされたデータ保護ポリシーを取得する許可を付与	読み取り	log-group*		
GetDelivery	単一の配信を取得する許可を付与	読み取り	delivery*		
GetDeliveryDestination	単一の配信先を取得する許可を付与	読み取り	delivery-destination*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetDeliveryDestinationPolicy	配信先にアタッチされている配信先ポリシーを取得する許可を付与	読み取り	delivery-destination*		
GetDeliverySource	単一の配信元を取得する許可を付与	読み取り	delivery-source*		
GetIntegration	単一の統合を取得するアクセス許可を付与します	読み取り			
GetLogAnomalyDetector	ログの異常ディテクターを取得するためのアクセス許可を付与	読み取り	anomaly-detector*		
GetLogDelivery [許可のみ]	指定されたログ配信のログ配信情報を取得する許可を付与	読み取り			
GetLogEvents	指定されたログストリームからログイベントを取得する許可を付与	読み取り	log-stream*		
GetLogGroupFields	指定されたロググループのログイベントに含まれているフィールドのリストを、各フィールドが含まれているログイベントの割合と一緒に返す許可を付与	読み取り	log-group*		
GetLogRecord	1 つのログイベントのすべてのフィールドおよび値を取得する許可を付与	読み取り	log-group*		
GetQueryResults	指定されたクエリの結果を返す許可を付与	読み取り	log-group*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetTransformer	指定されたロググループに関連付けられたトランスフォーマーを返すアクセス許可を付与します	読み取り	log-group *		
Link [許可のみ]	モニタリングアカウントに CloudWatch リソースを共有する許可を付与	書き込み			
ListAnomalies	リクエスト AWS アカウントを行う で検出されたすべての異常を一覧表示するアクセス許可を付与します	リスト	anomaly-detector		
ListEntitiesForLogGroup [許可のみ]	ロググループに関連付けられているすべてのエンティティを取得するアクセス許可を付与します	リスト			
ListIntegrations	リクエスト AWS アカウントを行う に関連付けられているすべての統合を一覧表示するアクセス許可を付与します	リスト			
ListLogAnomalyDetectors	リクエスト AWS アカウントを行う に関連付けられているすべての異常ディテクターを返すアクセス許可を付与します	リスト	anomaly-detector		
ListLogDeliveries [許可のみ]	指定されたアカウント/ログソースのすべてのログ配信を一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListLogGroups	リクエスト AWS アカウントを行う に関連付けられているすべてのロググループを返すアクセス許可を付与します	リスト			
ListLogGroupsForEntity [許可のみ]	エンティティに関連付けられているすべてのロググループを取得するアクセス許可を付与します	リスト			
ListLogGroupsForQuery	指定されたクエリに関連付けられているすべてのロググループを返すアクセス許可を付与します	リスト			
ListTagsForResource	指定されたリソースのタグを一覧表示するためのアクセス許可を付与	リスト	anomaly-detector		
			delivery		
			delivery-destination		
			delivery-source		
			destination		
			log-group		
ListTagsLogGroup	指定されたロググループのタグを一覧表示する許可を付与	リスト	log-group *		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutAccountPolicy	アカウントポリシーをアタッチするアクセス許可を付与します	書き込み			
PutDataProtectionPolicy	ログイベントから機密情報を検出して編集するためのデータ保護ポリシーをアタッチする許可を付与	書き込み	log-group*		
PutDeliveryDestination	配信先を作成または更新する許可を付与	書き込み	delivery-destination*		
				aws:TagKeys aws:RequestTag/${TagKey} logs:DeliveryDestinationResourceArn	
PutDeliveryDestinationPolicy	配信先に配信先ポリシーをアタッチする許可を付与	書き込み	delivery-destination*		
PutDeliverySource	配信元を作成または更新する許可を付与	書き込み	delivery-source*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey} logs:LogGeneratingResourceArns	
PutDestination	送信先を作成または更新する許可を付与	書き込み	destination*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	
PutDestinationPolicy	既存の送信先に関連付けられたアクセスポリシーを作成または更新する許可を付与	書き込み	destination*		
PutIndexPolicy	ロググループレベルでインデックスポリシーをアタッチして検索とクエリを最適化するアクセス許可を付与します	書き込み			
PutIntegration	CloudWatch Logs と Opensearch の統合を作成するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutLogEvents	ログイベントのバッチを指定されたログストリームにアップロードする許可を付与	書き込み	log-stream*		
PutMetricFilter	メトリクスフィルターの作成や更新の許可を付与し、それを指定されたロググループに関連付ける	書き込み	log-group*		
PutQueryDefinition	クエリ定義を作成または更新する許可を付与	書き込み			
PutResourcePolicy	リソースポリシーを作成または更新するアクセス許可を付与し、他の AWS サービスがこのアカウントにログイベントを配置できるようにします	権限の管理			
PutRetentionPolicy	指定されたロググループの保持期間を設定する許可を付与	書き込み	log-group*		
PutSubscriptionFilter	サブスクリプションフィルターの作成や更新の許可を付与し、それを指定されたロググループに関連付ける	書き込み	log-group*		iam:PassRole
			destination		
PutTransformer	トランスフォーマーを作成または更新するアクセス許可を付与し、指定したロググループに関連付けます	書き込み	log-group*		
StartLiveTail	CloudWatch Logs でライブテールセッションを開始する許可を付与	読み取り	log-group*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartQuery	CloudWatch Logs Insights を使用してロググループのクエリをスケジュールする許可を付与	読み取り	log-group *		
StopLiveTail [許可のみ]	進行中のライブテールセッションを停止する許可を付与	読み取り			
StopQuery	進行中の CloudWatch Logs Insights クエリを停止する許可を付与	読み取り			
TagLogGroup	指定されたロググループの指定されたタグを追加または更新する許可を付与	Tagging	log-group *		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource	指定されたリソースの指定されたタグを追加または更新する許可を付与	Tagging	anomaly-detector		
			delivery		
			delivery-destination		
			delivery-source		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			destination		
			log-group		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestMetricFilter	ログイベントメッセージのサンプルに対してメトリクスフィルターのフィルターパターンをテストする許可を付与	読み取り			
TestTransformer	ログイベントメッセージのサンプルに対してトランスフォーマーをテストするアクセス許可を付与します	読み取り			
Unmask [許可のみ]	データ保護ポリシーで編集されたマスクされていない状態のログイベントを取得する許可を付与	読み取り	log-group *		
UntagLogGroup	指定されたロググループから指定されたタグを削除する許可を付与	Tagging	log-group *		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	指定されたリソースから指定されたタグを削除するためのアクセス許可を付与	Tagging	anomaly-detector		
			delivery		
			delivery-destination		
			delivery-source		
			destination		
			log-group		
				aws:TagKeys	
UpdateAnomaly	ログの異常ディテクターによって報告された異常を更新するためのアクセス許可を付与	書き込み	anomaly-detector*		
UpdateDeliveryConfiguration	配信に関連する設定を更新する許可を付与する	書き込み	delivery*		
			delivery-destination*		
			delivery-source*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateLogAnomalyDetector	ログの異常ディテクターを更新するためのアクセス許可を付与	書き込み	anomaly-detector*		
UpdateLogDelivery [アクセス許可のみ]	指定されたログ配信のログ配信情報を更新する許可を付与	書き込み			

Amazon CloudWatch Logs で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
log-group	arn:${Partition}:logs:${Region}:${Account}:log-group:${LogGroupName}	aws:ResourceTag/${TagKey}
log-stream	arn:${Partition}:logs:${Region}:${Account}:log-group:${LogGroupName}:log-stream:${LogStreamName}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
destination	arn:${Partition}:logs:${Region}:${Account}:destination:${DestinationName}	aws:ResourceTag/${TagKey}
delivery-source	arn:${Partition}:logs:${Region}:${Account}:delivery-source:${DeliverySourceName}	aws:ResourceTag/${TagKey}
delivery	arn:${Partition}:logs:${Region}:${Account}:delivery:${DeliveryName}	aws:ResourceTag/${TagKey}
delivery-destination	arn:${Partition}:logs:${Region}:${Account}:delivery-destination:${DeliveryDestinationName}	aws:ResourceTag/${TagKey}
anomaly-detector	arn:${Partition}:logs:${Region}:${Account}:anomaly-detector:${DetectorId}	aws:ResourceTag/${TagKey}

Amazon CloudWatch Logs の条件キー

Amazon CloudWatch Logs は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義する許可を付与。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列

条件キー	説明	タイプ
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
logs:DeliveryDestinationResourceArn	リクエストで渡されたログの配信先 ARN でアクセスをフィルタリングします	ARN
logs:LogGenerating ResourceArns	リクエストで渡されたログ生成リソース ARN でアクセスをフィルタリングします	ArrayOfARN

Amazon CloudWatch Network Synthetic Monitor のアクション、リソース、および条件キー

Amazon CloudWatch Network Synthetic Monitor (サービスプレフィックス: `networkmonitor`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CloudWatch Network Synthetic Monitor で定義されるアクション
- Amazon CloudWatch Network Synthetic Monitor で定義されるリソースタイプ
- Amazon CloudWatch Network Synthetic Monitor の条件キー

Amazon CloudWatch Network Synthetic Monitor で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateMonitor	モニターを作成するための許可を付与します	書き込み	monitor*		
CreateProbe	プローブを作成する許可を付与	書き込み			
DeleteMonitor	モニターを削除するための許可を付与します	書き込み	monitor*		
DeleteProbe	プローブを削除する許可を付与	書き込み	probe*		
GetMonitor	モニターに関する情報を取得するための許可を付与します	読み取り	monitor*		
GetProbe	プローブに関する情報を取得する許可を付与	読み取り	probe*		
ListMonitors	アカウント内のすべてのモニターとそのステータスを一覧表示するための許可を付与します	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	monitor		
			probe		
TagResource	リソースにタグを追加する許可を付与	タグ付け	monitor		
			probe		
UntagResource	リソースからタグを削除する許可を付与	Tagging	monitor		
			probe		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
UpdateMonitor	モニターを更新するための許可を付与します	書き込み	monitor*		
UpdateProbe	プローブを更新する許可を付与	書き込み	probe*		

Amazon CloudWatch Network Synthetic Monitor で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
monitor	arn:${Partition}:networkmonitor:${Region}:${Account}:monitor/${MonitorName}	aws:ResourceTag/${TagKey}
probe	arn:${Partition}:networkmonitor:${Region}:${Account}:probe/${ProbeId}	aws:ResourceTag/${TagKey}

Amazon CloudWatch Network Synthetic Monitor の条件キー

Amazon CloudWatch Network Synthetic Monitor では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアによるアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon CloudWatch Observability Access Manager のアクション、リソース、条件キー

Amazon CloudWatch Observability Access Manager (サービスプレフィックス: oam) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクションおよび条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CloudWatch Observability Access Managerで定義されるアクション
- Amazon CloudWatch Observability Access Managerで定義されるリソースタイプ
- Amazon CloudWatch Observability Access Manager の条件キー

Amazon CloudWatch Observability Access Managerで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateLink	クロスアカウントのモニタリングのためのモニタリングアカウントとソースアカウント間のリンクを作成する許可を付与	書き込み	Sink*		oam:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys oam:ResourceTypes	
CreateSink	クロスアカウントのモニタリングのためのモニタリングアカウントとして使用できるよう、アカウントにシンクを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	oam:TagResource
DeleteLink	クロスアカウントのモニタリングのためのモニタリングアカウントとソースアカウント間のリンクを削除する許可を付与	書き込み	Link*		
				aws:ResourceTag/${TagKey}	
DeleteSink	モニタリングアカウント内のクロスアカウントモニタリングシンクを削除する許可を付与	書き込み	Sink*		
				aws:ResourceTag/${TagKey}	
GetLink	1 つのクロスアカウントモニタリングリンクに関する完全な情報を取得する許可を付与	読み取り	Link*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
GetSink	1 つのクロスアカウントモニタリングシンクに関する完全な情報を取得する許可を付与	読み取り	Sink*		
				aws:ResourceTag/${TagKey}	
GetSinkPolicy	クロスアカウントモニタリングシンクの IAM ポリシーについての完全な情報を取得する許可を付与	読み取り	Sink*		
				aws:ResourceTag/${TagKey}	
ListAttachedLinks	クロスアカウントモニタリングシンクにリンクされているリンクのリストを取得する許可を付与	読み取り	Sink*		
				aws:ResourceTag/${TagKey}	
ListLinks	このアカウントのクロスアカウントモニタリングリンクの ARN を取得する許可を付与	読み取り			
ListSinks	このアカウントのクロスアカウントモニタリングシンクの ARN を取得する許可を付与	読み取り			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	Link		
			Sink		
PutSinkPolicy		書き込み	Sink*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	クロスアカウントモニタリングシンクの IAM ポリシーを作成または更新する許可を付与			aws:ResourceTag/${TagKey}	
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	Link		
			Sink		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースのタグを解除する許可を付与	Tagging	Link		
			Sink		
				aws:TagKeys	
UpdateLink	モニタリングアカウントとソースアカウント間の既存のリンクを更新する許可を付与	書き込み	Link*		
				aws:ResourceTag/${TagKey} oam:ResourceTypes	

Amazon CloudWatch Observability Access Managerで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアク

ションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Link	`arn:${Partition}:oam:${Region}:${Account}:link/${ResourceId}`	aws:ResourceTag/${TagKey}
Sink	`arn:${Partition}:oam:${Region}:${Account}:sink/${ResourceId}`	aws:ResourceTag/${TagKey}

Amazon CloudWatch Observability Access Manager の条件キー

Amazon CloudWatch Observability Access Manager は、IAM ポリシーの `Condition` 要素で使用できる以下の条件キーを定義する許可を付与します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString
oam:ResourceTypes	リクエスト内のリソースタイプの有無でアクセスをフィルタリング	ArrayOfString

Amazon CloudWatch Observability Admin Service のアクション、リソース、および条件キー

Amazon CloudWatch Observability Admin Service (サービスプレフィックス: `observabilityadmin`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CloudWatch Observability Admin Service で定義されるアクション
- Amazon CloudWatch Observability Admin Service で定義されるリソースタイプ
- Amazon CloudWatch Observability Admin Service の条件キー

Amazon CloudWatch Observability Admin Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイ

プが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateTelemetryRule	アカウントの指定された名前で新しいテレメトリルールを作成するアクセス許可を付与します	書き込み	telemetry-rule*		
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateTelemetryRuleForOrganization	組織の指定された名前で新しい組織のテレメトリルールを作成するアクセス許可を付与します	書き込み	organization-telemetry-rule*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteTelemetryRule	アカウントの指定された名前のテレメトリルールを削除するアクセス許可を付与します	書き込み	telemetry-rule*		
DeleteTelemetryRuleForOrganization	組織の指定された名前の組織テレメトリルールを削除するアクセス許可を付与します	書き込み	organization-telemetry-rule*		
GetTelemetryEvaluationStatus	アカウントの Telemetry Config 機能のステータスを取得するアクセス許可を付与します	読み取り			
GetTelemetryEvaluationStatusForOrganization	組織の Telemetry Config 機能のステータスを取得するアクセス許可を付与します	読み取り			
GetTelemetryRule	アカウントの指定されたテレメトリルールを取得するアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetTelemetryRuleForOrganization	組織の指定された組織のテレメトリルールを取得するアクセス許可を付与します	読み取り			
ListResourceTelemetry	アカウントに関連付けられたリソースのテレメトリ設定を取得するアクセス許可を付与します	読み取り			
ListResourceTelemetryForOrganization	組織内のアカウントに関連付けられたリソースのテレメトリ設定を取得するアクセス許可を付与します	読み取り			
ListTagsForResource	指定されたリソースのタグを一覧表示するためのアクセス許可を付与	リスト	organization-telemetry-rule		
			telemetry-rule		
ListTelemetryRules	アカウントのテレメトリルールを一覧表示するアクセス許可を付与します	リスト			
ListTelemetryRulesForOrganization	組織のテレメトリルールを一覧表示する許可を付与	リスト			
StartTelemetryEvaluation	アカウントのテレメトリ設定機能を開始するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartTelemetryEvaluationForOrganization	組織のテレメトリ設定機能を開始するアクセス許可を付与します	書き込み			
StopTelemetryEvaluation	アカウントのテレメトリ設定機能を停止するアクセス許可を付与します	書き込み			
StopTelemetryEvaluationForOrganization	組織のテレメトリ設定機能を停止するアクセス許可を付与します	書き込み			
TagResource	指定されたリソースの指定されたタグを追加または更新する許可を付与	Tagging	organization-telemetry-rule		
			telemetry-rule		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	指定されたリソースから指定されたタグを削除するためのアクセス許可を付与	Tagging	organization-telemetry-rule		
			telemetry-rule		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
UpdateTelemetryRule	アカウントの指定されたテレメトリルールを更新するアクセス許可を付与します	書き込み	telemetry-rule*		
UpdateTelemetryRuleForOrganization	組織の指定された組織のテレメトリルールを取得するアクセス許可を付与します	書き込み	organization-telemetry-rule*		

Amazon CloudWatch Observability Admin Service で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
telemetry-rule	`arn:${Partition}:observabilityadmin:${Region}:${Account}:telemetry-rule:${TelemetryRuleName}`	aws:ResourceTag/${TagKey}
organization-telemetry-rule	`arn:${Partition}:observabilityadmin:${Region}:${Account}:organization-telemetry-rule:${TelemetryRuleName}`	aws:ResourceTag/${TagKey}

Amazon CloudWatch Observability Admin Service の条件キー

Amazon CloudWatch Observability Admin Service では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS CloudWatch RUMのアクション、リソース、および条件キー

AWS CloudWatch RUM (サービスプレフィックス: rum) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS CloudWatch RUMで定義されたアクション

- AWS CloudWatch RUMで定義されるリソースタイプ
- AWS CloudWatch RUMの条件キー

AWS CloudWatch RUMで定義されたアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchCreateRumMetricDefinitions	RUM メトリクス定義を作成する許可を付与	書き込み	AppMonitorResource*		
BatchDeleteRumMetricDefinitions	RUM メトリクス定義を削除する許可を付与	書き込み	AppMonitorResource*		
BatchGetRumMetricDefinitions	RUM メトリクス定義を取得する許可を付与	読み取り	AppMonitorResource*		
CreateAppMonitor	アプリケーションモニター メタデータを作成する権限を付与します。	書き込み	AppMonitorResource*		iam:CreateServiceLinkedRole iam:GetRole
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAppMonitor	アプリケーションモニター メタデータを削除する権限を付与します。	書き込み	AppMonitorResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteResourcePolicy	アプリケーションモニターにアタッチされたリソースポリシーを削除するアクセス許可を付与します	書き込み	AppMonitorResource*		
DeleteRumMetricsDestination	RUM メトリクス送信先を削除する許可を付与	書き込み	AppMonitorResource*		
GetAppMonitor	アプリケーションモニター メタデータを取得する権限を付与します。	読み取り	AppMonitorResource*		
GetAppMonitorData	AppMonitor データを取得するアクセス許可を付与します	読み取り	AppMonitorResource*		
GetResourcePolicy	アプリモニターにアタッチされたリソースポリシーを取得するアクセス許可を付与します	読み取り	AppMonitorResource*		
ListAppMonitors	アプリケーションモニター メタデータを一覧表示する権限を付与します。	リスト			
ListRumMetricsDestinations	RUM メトリクス送信先を一覧表示する許可を付与	読み取り	AppMonitorResource*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutResourcePolicy	リソースポリシーをアプリケーションモニターにアタッチするアクセス許可を付与します	書き込み	AppMonitorResource*		
PutRumEvents	アプリケーションモニター の RUM イベントを取得するアクセス許可を付与します。	書き込み	AppMonitorResource*		
PutRumMetricsDestination	RUM メトリクス送信先を配置する許可を付与	書き込み	AppMonitorResource*		
TagResource	リソースにタグを付けるアクセス許可を付与	Tagging	AppMonitorResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースのタグを解除する許可を付与します。	Tagging	AppMonitorResource*		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateAppMonitor	アプリケーションモニター メタデータを更新する権限を付与します。	書き込み	AppMonitorResource*		iam:CreateServiceLinkedRole iam:GetRole
UpdateRumMetricDefinition	RUM メトリクス定義を更新する許可を付与	書き込み	AppMonitorResource*		

AWS CloudWatch RUMで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
AppMonitorResource	`arn:${Partition}:rum:${Region}:${Account}:appmonitor/${Name}`	aws:ResourceTag/${TagKey}

AWS CloudWatch RUMの条件キー

AWS CloudWatch RUM では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	IAM プリンシパルに代わってリクエストが渡されるタグによってアクセスをフィルタリングします。	String
aws:ResourceTag/${TagKey}	IAM プリンシパルに代わってリクエストを行うリソースに関連付けられているタグアクセスをフィルタリングします。	String
aws:TagKeys	IAMプリンシパルに代わってリクエストで渡されるタグキーでアクセスをフィルタリングします。	ArrayOfString

Amazon CloudWatch Synthetics のアクション、リソース、および条件キー

Amazon CloudWatch Synthetics (サービスプレフィックス: `synthetics`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CloudWatch Synthetics で定義されるアクション
- Amazon CloudWatch Synthetics で定義されるリソースタイプ
- Amazon CloudWatch Synthetics の条件キー

Amazon CloudWatch Synthetics で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateResource	リソースをグループに関連付けるアクセス許可を付与	書き込み	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCanary	Canary を作成するアクセス権限を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGroup	グループを作成するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCanary	Canary を削除するためのアクセス許可を付与します。Amazon Synthetics は、Lambda 関数と CloudWatch アラーム (作成した場合) 以外のすべてのリソースを削除します	書き込み	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteGroup	グループを削除するアクセス許可を付与	書き込み	group*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeCanaries	すべての Canary の情報を一覧表示するアクセス権限を付与します	読み込み		synthetics:Names	
DescribeCanariesLastRun	すべての Canary に関連付けられている最後のテスト実行に関する情報を一覧表示するアクセス権限を付与します	読み込み		synthetics:Names	
DescribeRuntimeVersions	Synthetics Canary ランタイムバージョンに関する情報を一覧表示するためのアクセス許可を付与します	読み取り			
DisassociateResource	グループのリソースとの関連付けを解除するアクセス許可を付与	書き込み	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetCanary	Canary の詳細を表示するアクセス許可を付与	読み取り	canary*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetCanaryRuns	Canary に関連付けられたすべてのテスト実行に関する情報を一覧表示するアクセス権限を付与します	読み取り	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetGroup	グループの詳細を表示するアクセス許可を付与	読み取り	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListAssociatedGroups	関連付けられた canary のグループに関する情報を一覧表示するアクセス許可を付与	リスト	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListGroupResources		リスト	group*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	グループ内の canary に関する情報を一覧表示するアクセス許可を付与			aws:ResourceTag/${TagKey} aws:TagKeys	
ListGroups	すべてのグループの情報を一覧表示するアクセス許可を付与	リスト			
ListTagsForResource	リソースに関連付けられたすべてのタグと値を一覧表示するアクセス許可を付与	読み取り	canary		
			group		
StartCanary	Amazon CloudWatch Synthetics がウェブサイトのモニタリングを開始するように Canary を開始するアクセス権限を付与します	書き込み	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
StartCanaryDryRun	Amazon CloudWatch Synthetics が指定されたパラメータを使用して Canary のテスト実行を実行できるように、Canary ドライランを開始するアクセス許可を付与します	書き込み	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
StopCanary	Canary を停止するアクセス権限を付与します	書き込み	canary*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:TagKeys	
TagResource	リソースに 1 つ以上のタグを追加する許可を付与	タグ付け	canary		
			group		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースから 1 つ以上のタグを削除する許可を付与	Tagging	canary		
			group		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCanary	Canary を更新するアクセス権限を付与します	書き込み	canary*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:TagKeys	

Amazon CloudWatch Synthetics で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
canary	arn:${Partition}:synthetics:${Region}:${Account}:canary:${CanaryName}	aws:ResourceTag/${TagKey}
group	arn:${Partition}:synthetics:${Region}:${Account}:group:${GroupId}	aws:ResourceTag/${TagKey}

Amazon CloudWatch Synthetics の条件キー

Amazon CloudWatch Synthetics では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられているタグに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーに基づいてアクションをフィルタリングします	ArrayOfString
synthetics:Names	Canary 名に基づいて、アクセスをフィルタリングします	ArrayOfString

AWS CodeArtifact のアクション、リソース、および条件キー

AWS CodeArtifact (サービスプレフィックス: `codeartifact`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS CodeArtifact で定義されるアクション
- AWS CodeArtifact で定義されるリソースタイプ
- AWS CodeArtifact の条件キー

AWS CodeArtifact で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateExternalConnection	リポジトリに外部接続を追加する許可を付与	Write	repository*		
AssociateWithDownstreamRepository	既存のリポジトリをアップストリームリポジトリとして別のリポジトリに関連付けるアクセス許可を付与します	書き込み	repository*		
CopyPackageVersions	あるリポジトリから同じドメイン内の別のリポジトリにパッケージバージョンをコピーする許可を付与	書き込み	package* repository*		
CreateDomain	新しいドメインを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePackageGroup	パッケージグループを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRepository	新しいリポジトリを作成する許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteDomain	ドメインを削除する許可を付与	Write	domain*		
DeleteDomainPermissionsPolicy	ドメイン上のリソースポリシーセットを削除する許可を付与	権限の管理	domain*		
DeletePackage	パッケージを削除するための許可を付与します	書き込み	package*		
DeletePackageGroup	パッケージグループを削除する許可を付与する	書き込み	package-group*		
DeletePackageVersions	パッケージのバージョンを削除する許可を付与	Write	package*		
DeleteRepository	リポジトリを削除する許可を付与	Write	repository*		
DeleteRepositoryPermissionsPolicy	リポジトリ上のリソースポリシーセットを削除する許可を付与	Permissions management	repository*		
DescribeDomain	ドメインに関する情報を返すアクセス許可を付与します	読み取り	domain*		
DescribePackage	パッケージに関する情報を取得する許可を付与	読み取り	package*		
DescribePackageGroup	パッケージグループに関する詳細情報を返す許可を付与する	読み取り	package-group*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribePackageVersion	パッケージのバージョンに関する情報を返すアクセス許可を付与します	Read	package*		
DescribeRepository	リポジトリに関する詳細情報を返すアクセス許可を付与します	Read	repository*		
DisassociateExternalConnection	リポジトリからの外部接続の関連付けを解除する許可を付与	Write	repository*		
DisposePackageVersions	パッケージのバージョンのステータスを廃棄に設定し、アセットを削除する許可を付与	書き込み	package*		
GetAssociatedPackageGroup	パッケージの関連付けられたパッケージグループを返す許可を付与する	読み取り	package-group*		
GetAuthorizationToken	ドメイン内のリポジトリにアクセスするための一時認証トークンを生成する許可を付与	Read	domain*		
GetDomainPermissionsPolicy	ドメインのリソースポリシーを返すアクセス許可を付与します	Read	domain*		
GetPackageVersionAsset	パッケージのバージョンの一部であるアセット (またはファイル) を返すアクセス許可を付与します	Read	package*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetPackageVersionReadme	パッケージのバージョンの readme ファイルを返すアクセス許可を付与します	Read	package*		
GetRepositoryEndpoint	リポジトリのエンドポイントを返すアクセス許可を付与します	Read	repository*		
GetRepositoryPermissionsPolicy	リポジトリのリソースポリシーを返すアクセス許可を付与します	読み取り	repository*		
ListAllowedRepositoriesForGroup	パッケージグループの許可されたリポジトリを一覧表示する許可を付与する	リスト	package-group*		
ListAssociatedPackages	パッケージグループに関連付けられたパッケージを一覧表示する許可を付与する	リスト	package-group*		
ListDomains	現在のユーザーの のドメインを一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListPackageGroups	ドメイン内のパッケージグループを一覧表示する許可を付与する	リスト	domain*		
ListPackageVersionAssets	パッケージのバージョンのアセットを一覧表示する許可を付与	リスト	package*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListPackageVersionDependencies	パッケージバージョンの直接の依存関係を一覧表示する許可を付与	リスト	package*		
ListPackageVersions	パッケージのバージョンを一覧表示する許可を付与	リスト	package*		
ListPackages	リポジトリ内のパッケージを一覧表示する許可を付与	リスト	repository*		
ListRepositories	呼び出し元アカウントによって管理されているリポジトリを一覧表示する許可を付与	リスト			
ListRepositoriesInDomain	ドメイン内のリポジトリを一覧表示する許可を付与	リスト	domain*		
ListSubPackageGroups	親パッケージグループのサブパッケージグループを一覧表示する許可を付与する	リスト	package-group*		
ListTagsForResource	CodeArtifact リソースのタグを一覧表示する権限を付与します	リスト	domain		
			package-group		
			repository		
PublishPackageVersion	リポジトリエンドポイントにアセットとメタデータを公開する許可を付与	Write	package*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutDomainPermissionsPolicy	リソースポリシーをドメインにアタッチする許可を付与	Write	domain*		
PutPackageMetadata	リポジトリエンドポイントを使用してパッケージメタデータを追加、変更、または削除する許可を付与	書き込み	package*		
PutPackageOriginConfiguration	パッケージのオリジン設定を行う許可を付与	書き込み	package*		
PutRepositoryPermissionsPolicy	リソースポリシーをリポジトリにアタッチする許可を付与	Write	repository*		
ReadFromRepository	リポジトリエンドポイントからパッケージアセットとメタデータを返すアクセス許可を付与します	Read	repository*		
TagResource	CodeArtifact リソースにタグを付ける権限を付与します	タグ付け	domain		
			package-group		
			repository		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	CodeArtifact リソースからタグを削除する権限を付与します	Tagging	domain		
			package-group		
			repository		
				aws:TagKeys	
UpdatePackageGroup	パッケージグループのプロパティを変更する許可を付与する	書き込み	package-group*		
UpdatePackageGroupOriginConfiguration	パッケージグループのパッケージオリジン設定を変更する許可を付与する	書き込み	package-group*		
UpdatePackageVersionsStatus	パッケージの 1 つ以上のバージョンのステータスを変更する許可を付与	Write	package*		
UpdateRepository	リポジトリのプロパティを変更する許可を付与	Write	repository*		

AWS CodeArtifact で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

> **Note**
>
> パッケージグループリソースの ARN は、エンコードされたパッケージグループパターンを使用する必要があります。

リソースタイプ	ARN	条件キー
domain	arn:${Partition}:codeartifact:${Region}:${Account}:domain/${DomainName}	aws:ResourceTag/${TagKey}
repository	arn:${Partition}:codeartifact:${Region}:${Account}:repository/${DomainName}/${RepositoryName}	aws:ResourceTag/${TagKey}
package-group	arn:${Partition}:codeartifact:${Region}:${Account}:package-group/${DomainName}${EncodedPackageGroupPattern}	aws:ResourceTag/${TagKey}
package	arn:${Partition}:codeartifact:${Region}:${Account}:package/${DomainName}/${RepositoryName}/${PackageFormat}/${PackageNamespace}/${PackageName}	

AWS CodeArtifact の条件キー

AWS CodeArtifact は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

Amazon CodeCatalyst のアクション、リソース、および条件キー

Amazon CodeCatalyst (サービスプレフィックス: codecatalyst) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CodeCatalyst で定義されるアクション
- Amazon CodeCatalyst で定義されるリソースタイプ

- Amazon CodeCatalyst の条件キー

Amazon CodeCatalyst で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AcceptConnection [アクセス許可のみ]	このアカウントを Amazon CodeCatalyst スペースに接続するリクエストを受け入れるアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
AssociateIamRoleToConnection [アクセス許可のみ]	IAM ロールを接続に関連付けるアクセス許可を付与	書き込み	connections*		iam:PassRole
				aws:ResourceTag/${TagKey}	
AssociateIdentityCenterApplicationToSpace [アクセス許可のみ]	IAM アイデンティティセンターアプリケーションを Amazon CodeCatalyst スペースに関連付けるためのアクセス許可を付与	書き込み	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
AssociateIdentityToIdentityCenterApplication [アクセス許可のみ]	Amazon CodeCatalyst スペースの IAM アイデンティティセンターアプリケーションに ID を関連付けるためのアクセス許可を付与	書き込み	identity-center-applications*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchAssociateIdentitiesToIdentityCenterApplication [アクセス許可のみ]	Amazon CodeCatalyst スペースの IAM アイデンティティセンターアプリケーションに複数の ID を関連付けるためのアクセス許可を付与	書き込み	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
BatchDisassociateIdentitiesFromIdentityCenterApplication [アクセス許可のみ]	Amazon CodeCatalyst スペースの IAM アイデンティティセンターアプリケーションから複数の ID の関連付けを解除するためのアクセス許可を付与	書き込み	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
CreateIdentityCenterApplication [アクセス許可のみ]	IAM アイデンティティセンターアプリケーションを作成するためのアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSpace [アクセス許可のみ]	Amazon CodeCatalyst スペースを作成するためのアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSpaceAdminRoleAssignment [アクセス許可のみ]	特定の Amazon CodeCatalyst スペースと IAM アイデンティティセンターアプリケーションの管理者ロール割り当てを作成するためのアクセス許可を付与	書き込み	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
DeleteConnection [アクセス許可のみ]	接続を削除する許可を付与。	書き込み	connections*		
				aws:ResourceTag/${TagKey}	
DeleteIdentityCenterApplication [アクセス許可のみ]	IAM アイデンティティセンターアプリケーションを削除するためのアクセス許可を付与	書き込み	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
DisassociateIamRoleFromConnection [アクセス許可のみ]	IAM ロールを接続から関連付け解除するアクセス許可を付与	書き込み	connections*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DisassociateIdentityCenterApplicationFromSpace [アクセス許可のみ]	IAM アイデンティティセンターアプリケーションを Amazon CodeCatalyst スペースから関連付け解除するためのアクセス許可を付与	書き込み	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
DisassociateIdentityFromIdentityCenterApplication [アクセス許可のみ]	Amazon CodeCatalyst スペースの IAM アイデンティティセンターアプリケーションから ID の関連付けを解除するためのアクセス許可を付与	書き込み	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
GetBillingAuthorization [アクセス許可のみ]	接続に対する請求許可を説明するアクセス許可を付与	読み取り	connections*		
				aws:ResourceTag/${TagKey}	
GetConnection [許可のみ]	接続を取得するためアクセス許可を付与	読み取り	connections*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetIdentityCenterApplication [許可のみ]	IAM アイデンティティセンターアプリケーション関する情報を取得するためのアクセス許可を付与	読み取り	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
GetPendingConnection [許可のみ]	このアカウントを Amazon CodeCatalyst スペースに接続するリクエストで、保留中のものを取得するアクセス許可を付与	読み取り			
ListConnections [許可のみ]	保留中ではない接続を一覧表示するアクセス許可を付与	リスト			
ListIamRolesForConnection [許可のみ]	IAM ロールを接続に関連付けるアクセス許可を付与	リスト	connections*		
				aws:ResourceTag/${TagKey}	
ListIdentityCenterApplications [許可のみ]	アカウント内のすべての IAM アイデンティティセンターアプリケーションのリストを表示するためのアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListIdentityCenterApplicationsForSpace [許可のみ]	Amazon CodeCatalyst スペースで IAM アイデンティティセンターアプリケーションのリストを表示するためのアクセス許可を付与	リスト			
ListSpacesForIdentityCenterApplication [許可のみ]	IAM アイデンティティセンターアプリケーションで Amazon CodeCatalyst スペースのリストを表示するためのアクセス許可を付与	リスト	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource [許可のみ]	Amazon CodeCatalyst リソースのタグを一覧表示する許可を付与	読み取り	connections		
			identity-center-applications		
				aws:ResourceTag/${TagKey}	
PutBillingAuthorization [許可のみ]	接続に関する請求の認可を作成または更新するアクセス許可を付与	書き込み	connections*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RejectConnection [アクセス許可のみ]	このアカウントを Amazon CodeCatalyst スペースに接続するリクエストを拒否するアクセス許可を付与	書き込み			
SynchronizeIdentityCenterApplication [アクセス許可のみ]	IAM アイデンティティセンターアプリケーションをバッキングアイデンティティストアと同期するためのアクセス許可を付与	書き込み	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
TagResource [アクセス許可のみ]	Amazon CodeCatalyst リソースにタグ付けする許可を付与	Tagging	connections		
			identity-center-applications		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource [アクセス許可のみ]	Amazon CodeCatalyst リソースのタグを削除する許可を付与	Tagging	connections		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			identity-center-applications		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateIdentityCenterApplication [アクセス許可のみ]	IAM アイデンティティセンターアプリケーションを更新するためのアクセス許可を付与	書き込み	identity-center-applications*		
				aws:ResourceTag/${TagKey}	

Amazon CodeCatalyst で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
connections	arn:${Partition}:codecatalyst:${Region}:${Account}:/connections/${ConnectionId}	aws:ResourceTag/${TagKey}
identity-center-applications	arn:${Partition}:codecatalyst:${Region}:${Account}:/identity-center-applications/${IdentityCenterApplicationId}	aws:ResourceTag/${TagKey}
space	arn:${Partition}:codecatalyst:::space/${SpaceId}	
project	arn:${Partition}:codecatalyst:::space/${SpaceId}/project/${ProjectId}	

Amazon CodeCatalyst の条件キー

Amazon CodeCatalystでは、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義しています。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグのキーと値でアクセスをフィルター	String
aws:ResourceTag/${TagKey}	リクエスト内のタグキーおよび値のペアのプレゼンスによってアクションをフィルタリングします	String

条件キー	説明	タイプ
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString

AWS CodeCommit のアクション、リソース、および条件キー

AWS CodeCommit (サービスプレフィックス: codecommit) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS CodeCommit で定義されるアクション
- AWS CodeCommit で定義されるリソースタイプ
- AWS CodeCommit の条件キー

AWS CodeCommit で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateApprovalRuleTemplateWithRepository	承認ルールテンプレートをリポジトリに関連付けるアクセス許可を付与	Write	repository*		
BatchAssociateAppr	1 回のオペレーションで複数のリポジトリに承認ルールテ	Write	repository*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ovalRuleTemplateWithRepositories	ンプレートを関連付けるアクセス許可を付与				
BatchDescribeMergeConflicts	3 方向マージオプションまたはスカッシュマージオプションを使用して 2 つのコミットをマージしようとしたときに、複数のマージ競合に関する情報を取得する許可を付与。	Read	repository*		
BatchDisassociateApprovalRuleTemplateFromRepositories	1 回のオペレーションで承認ルールテンプレートと複数のリポジトリ間の関連付けを削除する許可を付与	書き込み	repository*		
BatchGetCommits	AWS CodeCommit リポジトリ内の 1 つ以上のコミットに関する情報を返すアクセス許可を付与します	読み取り	repository*		
BatchGetPullRequests [許可のみ]	AWS CodeCommit リポジトリ内の 1 つ以上のプルリクエストに関する情報を返すアクセス許可を付与します	読み取り	repository*		
BatchGetRepositories	複数のリポジトリに関する情報を取得する許可を付与。	Read	repository*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CancelUploadArchive [許可のみ]	AWS CodePipeline のパイプラインへのアーカイブのアップロードをキャンセルするアクセス許可を付与します	読み取り	repository*		
CreateApprovalRuleTemplate	承認ルールテンプレートを作成する許可を付与。このテンプレートで定義された条件と一致するプル要求で承認ルールを自動的に作成します。個々のプルリクエストの承認ルールを作成するアクセス許可は付与されません	書き込み			
CreateBranch	この API を使用して AWS CodeCommit リポジトリにブランチを作成するアクセス許可を付与します。Git ブランチ作成アクションは制御しません。	書き込み	repository*		
				codecommit:References	
CreateCommit	AWS CodeCommit リポジトリのブランチ内の単一または複数のファイルを追加、コピー、移動、または更新し、指定されたブランチの変更のコミットを生成するアクセス許可を付与します	書き込み	repository*		
				codecommit:References	
CreatePullRequest	指定されたリポジトリにプルリクエストを作成する許可を付与。	Write	repository*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreatePullRequestApprovalRule	個々のプルリクエストに固有の承認ルールを作成する許可を付与。承認ルールテンプレートを作成するアクセス許可は付与しません。	書き込み	repository*		
CreateRepository	AWS CodeCommit リポジトリを作成するアクセス許可を付与します	書き込み	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUnreferencedMergeCommit	3 方向またはスカッシュマージオプションを使用して 2 つのコミットをマージした結果を含む、参照されていないコミットを作成する (ただし Git マージアクションは管理しない) アクセス許可を付与	Write	repository*		
				codecommit:References	
DeleteApprovalRuleTemplate	承認ルールテンプレートを削除する許可を付与	書き込み			
DeleteBranch	この API を使用して AWS CodeCommit リポジトリ内のブランチを削除するアクセス許可を付与します。Git ブランチ削除アクションは制御しません。	書き込み	repository*		
				codecommit:References	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteCommentContent	リポジトリ内の変更、ファイル、またはコミットに対するコメントの内容を削除する許可を付与。	Write	repository*		
DeleteFile	指定されたブランチから指定されたファイルを削除する許可を付与。	Write	repository*		
				codecommit:References	
DeletePullRequestApprovalRule	ルールが承認ルールテンプレートによって作成されなかった場合に、プルリクエストに対して作成された承認ルールを削除する許可を付与	書き込み	repository*		
DeleteRepository	AWS CodeCommit リポジトリを削除するアクセス許可を付与します	書き込み	repository*		
DescribeMergeConflicts	3 方向またはスカッシュマージオプションを使用して 2 つのコミットをマージしようとしたときに、特定のマージ競合に関する情報を取得する許可を付与。	Read	repository*		
DescribePullRequestEvents	1 つ以上のプルリクエストイベントに関する情報を返すアクセス許可を付与	Read	repository*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DisassociateApprovalRuleTemplateFromRepository	承認規則テンプレートとリポジトリ間の関連付けを削除する許可を付与	Write	repository*		
EvaluatePullRequestApprovalRules	現在の承認状態と承認ルールの要件に基づいて、プルリクエストがマージ可能かどうかを評価する許可を付与	Read	repository*		
GetApprovalRuleTemplate	承認ルールテンプレートに関する情報を返すアクセス許可を付与	読み取り			
GetBlob	AWS CodeCommit AWS CodeCommit コンソールから CodeCommit リポジトリ内の個々のファイルのエンコードされたコンテンツを表示するアクセス許可を付与します	読み取り	repository*		
GetBranch	この API を使用して AWS CodeCommit リポジトリ内のブランチに関する詳細を取得するアクセス許可を付与します。Git ブランチアクションは制御しません。	読み取り	repository*		
GetComment	リポジトリ内の変更、ファイル、またはコミットに対するコメントの内容を取得する許可を付与。	Read	repository*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetCommentReactions	コメントに対する反応を取得する許可を付与	Read	repository*		
GetCommentsForComparedCommit	2 つのコミットの比較についてのコメントに関する情報を取得する許可を付与。	Read	repository*		
GetCommentsForPullRequest	プルリクエストについてのコメントを取得する許可を付与。	Read	repository*		
GetCommit	この API を使用して、コミットメッセージやコミット情報など、コミットに関する情報を返す (ただし Git のログアクションは管理しない) アクセス許可を付与	Read	repository*		
GetCommitHistory [許可のみ]	リポジトリでのコミットの履歴に関する情報を取得する許可を付与。	Read	repository*		
GetCommitsFromMergeBase [許可のみ]	潜在的なマージのコンテキストにおけるコミット間の違いに関する情報を取得する許可を付与。	Read	repository*		
GetDifferences	有効なコミット指定子 (ブランチ、タグ、HEAD、コミット ID、または他の完全修飾参照) 間の違いに関する情報を表示する許可を付与。	Read	repository*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetFile	指定されたファイルとそのメタデータの base-64 エンコードコンテンツを返すアクセス許可を付与	Read	repository*		
GetFolder	リポジトリ内の指定されたフォルダの内容を返すアクセス許可を付与	Read	repository*		
GetMergeCommit	マージコミットを作成するプルリクエストのいずれかのマージオプションによって作成されたマージコミットに関する情報を取得する許可を付与。すべてのマージオプションがマージコミットを作成するわけではありません。このアクセス許可では、Git マージアクションを管理できません。	Read	repository*		
				codecommit:References	
GetMergeConflicts	リポジトリ内のプルリクエストについて、前後のコミット ID 間のマージ競合に関する情報を返すアクセス許可を付与	Read	repository*		
GetMergeOptions	2 つのコミットをマージするために使用できるプルリクエストのマージオプションに関する情報を取得する (ただし Git マージアクションは管理しない) アクセス許可を付与	Read	repository*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetObjectIdentifier [許可のみ]	BLOB、ツリー、コミットをそれらの識別子に解決する許可を付与。	Read	repository*		
GetPullRequest	指定されたリポジトリ内のプルリクエストに関する情報を取得する許可を付与。	Read	repository*		
GetPullRequestApprovalStates	入力されたプルリクエストに対する現在の承認を取得する許可を付与	Read	repository*		
GetPullRequestOverrideState	指定されたプルリクエストの現在のオーバーライド状態を取得する許可を付与	Read	repository*		
GetReferences [許可のみ]	AWS CodeCommit リポジトリ内のリファレンスに関する詳細を取得するアクセス許可を付与します。Git リファレンスアクションは制御しません。	読み取り	repository*		
GetRepository	AWS CodeCommit リポジトリに関する情報を取得するアクセス許可を付与します	読み取り	repository*		
GetRepositoryTriggers	リポジトリのために設定されたトリガーに関する情報を取得する許可を付与。	Read	repository*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetTree [許可のみ]	AWS CodeCommit コンソールから、CodeCommit AWS CodeCommit リポジトリ内の指定されたツリーの内容を表示するアクセス許可を付与します	読み取り	repository*		
GetUploadArchiveStatus [許可のみ]	AWS CodePipeline のパイプラインへのアーカイブアップロードに関するステータス情報を取得する許可を付与	読み取り	repository*		
GitPull [許可のみ]	AWS CodeCommit リポジトリからローカルリポジトリに情報をプルするアクセス許可を付与します	読み取り	repository*		
GitPush [許可のみ]	ローカルリポジトリから AWS CodeCommit リポジトリに情報をプッシュするアクセス許可を付与します	書き込み	repository*		
				codecommit:References	
ListApprovalRuleTemplates	AWS リージョン の 内のすべての承認ルールテンプレートを一覧表示するアクセス許可を付与します AWS アカウント	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListAssociatedApprovalRuleTemplatesForRepository	リポジトリに関連付けられた承認規則テンプレートを一覧表示する許可を付与	リスト	repository*		
ListBranches	この API を使用して AWS CodeCommit リポジトリのブランチを一覧表示するアクセス許可を付与します。Git ブランチアクションは制御しません。	リスト	repository*		
ListFileCommitHistory	指定されたファイルへのコミットと変更を一覧表示するアクセス許可を付与します	リスト	repository*		
ListPullRequests	指定されたリポジトリのプルリクエストを一覧表示する許可を付与。	リスト	repository*		
ListRepositories	の現在のリージョンの AWS CodeCommit リポジトリに関する情報を一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListRepositoriesForApprovalRuleTemplate	承認ルールテンプレートに関連付けられているリポジトリを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTagsForResource	CodeCommit リソースの ARN にアタッチされているリソースを一覧表示する許可を付与。	リスト	repository		
MergeBranchesByFastForward	早送りマージオプションを使用して 2 つのコミットを指定された送信先ブランチにマージする許可を付与。	Write	repository*		
				codecommit:References	
MergeBranchesBySquash	スカッシュマージオプションを使用して 2 つのコミットを指定された送信先ブランチにマージする許可を付与。	Write	repository*		
				codecommit:References	
MergeBranchesByThreeWay	3 方向マージオプションを使用して 2 つのコミットを指定された送信先ブランチにマージする許可を付与。	Write	repository*		
				codecommit:References	
MergePullRequestByFastForward	プルリクエストを閉じ、早送りマージオプションを使用して、指定されたコミットでそのプルリクエスト用に指定された送信先ブランチにマージするよう試みるアクセス許可を付与	Write	repository*		
				codecommit:References	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
MergePullRequestBySquash	プルリクエストを閉じ、スカッシュマージオプションを使用して、指定されたコミットでそのプルリクエスト用に指定された送信先ブランチにマージするよう試みるアクセス許可を付与	Write	repository*		
				codecommit:References	
MergePullRequestByThreeWay	プルリクエストを閉じ、3 方向マージオプションを使用して、指定されたコミットでそのプルリクエスト用に指定された送信先ブランチにマージするよう試みるアクセス許可を付与	Write	repository*		
				codecommit:References	
OverridePullRequestApprovalRules	テンプレートによって作成された承認ルールを含む、プル要求のすべての承認ルールを上書きする許可を付与	Write	repository*		
PostCommentForComparedCommit	2 つのコミットの比較に対するコメントを投稿する許可を付与。	Write	repository*		
PostCommentForPullRequest	プルリクエストについてのコメントを投稿する許可を付与。	Write	repository*		
PostCommentReply	コミット間の比較またはプルリクエストに対するコメントに返答する形でコメントを投稿する許可を付与。	Write	repository*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutCommentReaction	コメントに反応を投稿する許可を付与	書き込み	repository*		
PutFile	AWS CodeCommit リポジトリのブランチでファイルを追加または更新し、指定されたブランチに追加するためのコミットを生成するアクセス許可を付与します	書き込み	repository*		
				codecommit:References	
PutRepositoryTriggers	リポジトリのトリガーを作成、更新、または削除する許可を付与。	Write	repository*		
TagResource	CodeCommit リソースの ARN にリソースタグをアタッチする許可を付与。	Tagging	repository		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
TestRepositoryTriggers	トリガーターゲットに情報を送信することで、リポジトリトリガーの機能をテストする許可を付与。	Write	repository*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	CodeCommit リソースの ARN からリソースタグの関連付けを解除する許可を付与。	Tagging	repository		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateApprovalRuleTemplateContent	承認ルールテンプレートのコンテンツを更新する許可を付与。プル要求用に特別に作成された承認ルールのコンテンツを更新するアクセス許可は付与しません	Write			
UpdateApprovalRuleTemplateDescription	承認ルールテンプレートの説明を更新する許可を付与	Write			
UpdateApprovalRuleTemplateName	承認ルールテンプレートの名前を更新する許可を付与	Write			
UpdateComment	ID がコメントの作成に使用された ID と一致する場合にコメントの内容を更新する許可を付与。	書き込み	repository*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateDefaultBranch	AWS CodeCommit リポジトリのデフォルトブランチを変更するアクセス許可を付与します	書き込み	repository*		
UpdatePullRequestApprovalRuleContent	特定のプルリクエストに対して作成された承認ルールのコンテンツを更新する許可を付与。承認ルールテンプレートを使用して作成されたルールの承認ルールコンテンツを更新するアクセス許可は付与しません	Write	repository*		
UpdatePullRequestApprovalState	プルリクエストの承認状態を更新する許可を付与	Write	repository*		
UpdatePullRequestDescription	プルリクエストの説明を更新する許可を付与。	Write	repository*		
UpdatePullRequestStatus	プルリクエストのステータスを更新する許可を付与。	Write	repository*		
UpdatePullRequestTitle	プルリクエストのタイトルを更新する許可を付与。	書き込み	repository*		
UpdateRepositoryDescription	AWS CodeCommit リポジトリの説明を変更するアクセス許可を付与します	書き込み	repository*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateRepositoryEncryptionKey	AWS CodeCommit リポジトリの暗号化と復号に使用される AWS KMS 暗号化キーを変更するアクセス許可を付与します	書き込み	repository*		
UpdateRepositoryName	AWS CodeCommit リポジトリの名前を変更するアクセス許可を付与します	書き込み	repository*		
UploadArchive [アクセス許可のみ]	AWS CodePipeline のサービスロールに、リポジトリの変更をパイプラインにアップロードするアクセス許可を付与します	書き込み	repository*		

AWS CodeCommit で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
repository	arn:${Partition}:codecommit:${Region}:${Account}:${RepositoryName}	aws:ResourceTag/${TagKey}

AWS CodeCommit の条件キー

AWS CodeCommit では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString
codecommit:References	指定された AWS CodeCommit アクションへのアクセスを Git リファレンスでフィルタリングします	String

AWS CodeConnections のアクション、リソース、および条件キー

AWS CodeConnections (サービスプレフィックス: codeconnections) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS CodeConnections で定義されるアクション
- AWS CodeConnections によって定義されるリソースタイプ
- AWS CodeConnections の条件キー

AWS CodeConnections で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateConnection	接続リソースを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys codeconnections:ProviderType	
CreateHost	ホストリソースを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys codeconnections:ProviderType codeconnections:VpcId	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateRepositoryLink	リポジトリリンクを作成するためのアクセス許可を付与	書き込み	Connection*		codeconnections:PassConnection codeconnections:UseConnection
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSyncConfiguration	テンプレート同期設定を作成する許可を付与。	書き込み	RepositoryLink*		codeconnections:PassRepository iam:PassRole
				codeconnections:Branch	
DeleteConnection	接続リソースを削除する許可を付与	書き込み	Connection*		
DeleteHost	ホストリソースを削除する許可を付与	書き込み	Host*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteRepositoryLink	リポジトリリンクを削除するためのアクセス許可を付与	書き込み	RepositoryLink*		
DeleteSyncConfiguration	同期設定を削除するためのアクセス許可を付与	書き込み			
GetConnection	接続リソースに関する詳細を取得する許可を付与	読み取り	Connection*		
GetConnectionToken [許可のみ]	接続トークンを取得してプロバイダーのアクションを呼び出す許可を付与する	読み取り	Connection*		
GetHost	ホストリソースに関する詳細を取得する許可を付与	読み込み	Host*		
GetIndividualAccessToken [許可のみ]	Bitbucket アプリのインストールなど、サードパーティーを接続に関連付けるアクセス許可を付与	読み込み		codeconnections:ProviderType	codeconnections:StartOAuthHandshake
GetInstallationUrl [許可のみ]	Bitbucket アプリのインストールなど、サードパーティーを接続に関連付けるアクセス許可を付与	読み取り		codeconnections:ProviderType	
GetRepositoryLink	リポジトリリンクを記述するためのアクセス許可を付与	読み取り	RepositoryLink*		
GetRepositorySyncStatus	リポジトリの最新の同期ステータスを取得する許可を付与。	読み取り	RepositoryLink*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				codeconnections:Branch	
GetResourceSyncStatus	リソース (cfn スタックまたはその他のリソース) の最新の同期ステータスを取得するためのアクセス許可を付与	読み取り			
GetSyncBlockerSummary	リソース (cfn スタックまたはその他のリソース) のサービス同期ブロッカーを説明するためのアクセス許可を付与	読み取り			
GetSyncConfiguration	同期設定を記述するためのアクセス許可を付与	読み取り			
ListConnections	接続リソースを一覧表示する許可を付与	リスト	Connection*		
				codeconnections:ProviderTypeFilter	
ListHosts	ホストリソースを一覧表示する許可を付与	リスト		codeconnections:ProviderTypeFilter	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListInstallationTargets [許可のみ]	Bitbucket アプリのインストールなど、サードパーティーを接続に関連付けるアクセス許可を付与	リスト			codeconnections:GetIndividualAccessToken codeconnections:StartOAuthHandshake
ListRepositoryLinks	リポジトリリンクを一覧表示するためのアクセス許可を付与	リスト			
ListRepositorySyncDefinitions	リポジトリ同期定義を一覧表示する許可を付与。	リスト			
ListSyncConfigurations	リポジトリリンクの同期設定を一覧表示するためのアクセス許可を付与	リスト			
ListTagsForResource	リソースの管理に使用されるキーと値のペアのセットへの許可を付与	リスト	Connection		
			Host		
			RepositoryLink		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PassConnection [許可のみ]	codepipeline:CreatePipeline などの接続 ARN を入力として受け入れる AWS サービスに接続リソースを渡すアクセス許可を付与します	読み取り	Connection*		
				codeconnections:PassedToService	
PassRepository [許可のみ]	codeconnections:CreateSyncConfiguration などの RepositoryLinkId を入力として受け入れる AWS サービスにリポジトリリンクリソースを渡すアクセス許可を付与します	読み取り	RepositoryLink*		
				codeconnections:PassedToService	
RegisterAppCode [許可のみ]	GitHub Enterprise Server インスタンスなどのサードパーティーサーバーをホストに関連付けるアクセス許可を付与	読み込み		codeconnections:HostArn	
StartAppRegistrationHandshake [許可のみ]	GitHub Enterprise Server インスタンスなどのサードパーティーサーバーをホストに関連付けるアクセス許可を付与	読み込み		codeconnections:HostArn	
StartOAuthHandshake [許可のみ]	Bitbucket アプリのインストールなど、サードパーティーを接続に関連付けるアクセス許可を付与	読み取り		codeconnections:ProviderType	
TagResource	指定されたリソースのタグに追加または変更する許可を付与	Tagging	Connection		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			Host		
			RepositoryLink		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	AWS リソースからタグを削除するアクセス許可を付与します	Tagging	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateConnectionInstallation	CodeStar Connections アプリをインストールした接続リソースを更新する許可を付与	書き込み	Connection*		codeconnections:GetIndividualAccessToken codeconnections:GetInstallationUrl codeconnections:ListInstallationTargets codeconnections:StartOAuthHandshake
				codeconnections:InstallationId	
UpdateHost	ホストリソースを更新するアクセス許可を付与	書き込み	Host*		
				codeconnections:VpcId	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateRepositoryLink	リポジトリリンクを更新するためのアクセス許可を付与	書き込み	RepositoryLink*		
UpdateSyncBlocker	リソース (cfn スタックまたはその他のリソース) の同期ブロッカーを更新するためのアクセス許可を付与	書き込み			
UpdateSyncConfiguration	同期設定を更新するためのアクセス許可を付与	書き込み		codeconnections:Branch	
UseConnection [アクセス許可のみ]	接続リソースを使用してプロバイダーのアクションを呼び出すアクセス許可を付与	読み取り	Connection*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				codeconnections:BranchName codeconnections:FullRepositoryId codeconnections:OwnerId codeconnections:ProviderAction codeconnections:ProviderPermissionsRequired codeconnections:RepositoryName	

AWS CodeConnections によって定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Connection	arn:${Partition}:codeconnections:${Region}:${Account}:connection/${ConnectionId}	aws:ResourceTag/${TagKey}
Host	arn:${Partition}:codeconnections:${Region}:${Account}:host/${HostId}	aws:ResourceTag/${TagKey}
RepositoryLink	arn:${Partition}:codeconnections:${Region}:${Account}:repository-link/${RepositoryLinkId}	aws:ResourceTag/${TagKey}

AWS CodeConnections の条件キー

AWS CodeConnections では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

条件キー	説明	タイプ
codeconnections:Branch	リクエストで渡されたブランチ名でアクセスをフィルタリングします	String
codeconnections:BranchName	リクエストで渡されたブランチ名でアクセスをフィルタリングします 特定のリポジトリブランチへのアクセスに関する UseConnection リクエストにのみ適用します	文字列
codeconnections:FullRepositoryId	リクエストで渡されたリポジトリによるアクセスをフィルタリングします。特定のリポジトリにアクセスするための UseConnection リクエストにのみ適用します	文字列
codeconnections:HostArn	リクエストで使用された接続に関連付けられたホストリソースによってアクセスをフィルタリングします	ARN
codeconnections:InstallationId	Connection の更新に使用されるサードパーティー ID (CodeConnections 用の Bitbucket アプリのインストール ID など) でアクセスをフィルタリングします。Connection を作成するために使用できるサードパーティー製アプリのインストールを制限できます。	文字列
codeconnections:OwnerId	サードパーティーのリポジトリの所有者によるアクセスをフィルタリングします。特定のユーザーが所有するリポジトリへのアクセスに関する UseConnection リクエストにのみ適用	String
codeconnections:PassedToService	プリンシパルが接続または RepositoryLink を渡すことを許可されているサービスでアクセスをフィルタリングします	String
codeconnections:ProviderAction	ListRepositories など、UseConnection リクエストのプロバイダーアクションによってアクセスをフィルタリングします。すべての有効な値については、ドキュメントを参照してください。	文字列

条件キー	説明	タイプ
codeconnections:ProviderPermissionsRequired	UseConnection リクエストのプロバイダーアクションの書き込みアクセス許可でアクセスをフィルタリングします。有効なタイプには、読み取り専用と読み取り書き込みがあります。	文字列
codeconnections:ProviderType	リクエストで渡されたサードパーティープロバイダーのタイプによってアクセスをフィルタリングします。	文字列
codeconnections:ProviderTypeFilter	結果をフィルタリングするために使用されるサードパーティープロバイダーのタイプによってアクセスをフィルタリングします。	文字列
codeconnections:RepositoryName	リクエストで渡されたリポジトリ名でアクセスをフィルタリングします。特定のユーザーが所有するリポジトリへのアクセスに関する UseConnection リクエストにのみ適用	String
codeconnections:VpcId	リクエストで渡された VpcId でアクセスをフィルタリングします	String

AWS CodeDeploy のアクション、リソース、および条件キー

AWS CodeDeploy (サービスプレフィックス: codedeploy) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS CodeDeploy で定義されるアクション
- AWS CodeDeploy で定義されるリソースタイプ
- AWS CodeDeploy の条件キー

AWS CodeDeploy で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddTagsToOnPremisesInstances	1 つ以上のオンプレミスインスタンスにタグを追加するアクセス許可を付与	Tagging	instance*		
BatchGetApplicationRevisions	1 つ以上のアプリケーションのリビジョンに関する情報を取得するアクセス許可を付与	読み込み	application*		
BatchGetApplications	IAM ユーザーに関連付けられた複数のアプリケーションに関する情報を取得するアクセス許可を付与	読み込み	application*		
BatchGetDeploymentGroups	1 つ以上のデプロイグループに関する情報を取得するアクセス許可を付与	読み込み	deploymentgroup*		
BatchGetDeploymentInstances	デプロイグループの一部である 1 つ以上のインスタンスに関する情報を取得するアクセス許可を付与	読み込み	deploymentgroup*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchGetDeploymentTargets	デプロイに関連付けられている 1 つ以上のターゲットの配列を返すアクセス許可を付与 このメソッドはすべてのコンピューティングタイプで動作し、廃止された BatchGetDeploymentInstances の代わりに使用する必要があります。返すことができるターゲットの最大数は 25 です	読み込み			
BatchGetDeployments	IAM ユーザーに関連付けられている複数のデプロイに関する情報を取得するアクセス許可を付与	読み込み	deploymentgroup*		
BatchGetOnPremisesInstances	1 つ以上のオンプレミスインスタンスに関する情報を取得するアクセス許可を付与	読み込み	instance*		
ContinueDeployment	指定された待機時間の経過を待たずに、トラフィックを元の環境のインスタンスから置き換え先環境のインスタンスに再ルーティングするプロセスをスタートするアクセス許可を付与	書き込み			
CreateApplication	IAM ユーザーに関連付けられているアプリケーションを作成するアクセス許可を付与	書き込み	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudFormationDeployment [アクセス許可のみ]	CloudFormation スタック更新のオーケストレーションに貢献する CloudFormation のデプロイを作成するアクセス許可を付与	書き込み			
CreateDeployment	IAM ユーザーに関連付けられているアプリケーションのデプロイを作成するアクセス許可を付与	書き込み	deploymentgroup*		
CreateDeploymentConfig	IAM ユーザーに関連付けられているカスタムデプロイ設定を作成するアクセス許可を付与	書き込み	deploymentconfig*		
CreateDeploymentGroup	IAM ユーザーに関連付けられているアプリケーションのデプロイグループを作成するアクセス許可を付与	書き込み	deploymentgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteApplication	IAM ユーザーに関連付けられているアプリケーションを削除するアクセス許可を付与	書き込み	application*		
DeleteDeploymentConfig	IAM ユーザーに関連付けられているカスタムデプロイ設定を削除するアクセス許可を付与	書き込み	deploymentconfig*		
DeleteDeploymentGroup	IAM ユーザーに関連付けられているアプリケーションのデプロイグループを削除するアクセス許可を付与	書き込み	deploymentgroup*		
DeleteGitHubAccountToken	GitHub アカウント接続を削除するアクセス許可を付与	書き込み			
DeleteResourcesByExternalId	特定の外部 ID に関連付けられているリソースを削除するアクセス許可を付与	書き込み			
DeregisterOnPremisesInstance	オンプレミスインスタンスの登録を解除するアクセス許可を付与	書き込み	instance*		
GetApplication	IAM ユーザーに関連付けられている単一のアプリケーションに関する情報を取得するアクセス許可を付与	リスト	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetApplicationRevision	IAM ユーザーに関連付けられているアプリケーションの、単一のアプリケーションのリビジョンに関する情報を取得するアクセス許可を付与	リスト	application*		
GetDeployment	IAM ユーザーに関連付けられているアプリケーションの、デプロイグループへの単一のデプロイに関する情報を取得するアクセス許可を付与	リスト	deploymentgroup*		
GetDeploymentConfig	IAM ユーザーに関連付けられている単一のデプロイ設定に関する情報を取得するアクセス許可を付与	リスト	deploymentconfig*		
GetDeploymentGroup	IAM ユーザーに関連付けられているアプリケーションの、単一のデプロイグループに関する情報を取得するアクセス許可を付与	リスト	deploymentgroup*		
GetDeploymentInstance	IAM ユーザーに関連付けられているデプロイの、単一のインスタンスに関する情報を取得するアクセス許可を付与	リスト	deploymentgroup*		
GetDeploymentTarget	デプロイターゲットに関する情報を返すアクセス許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetOnPremisesInstance	単一のオンプレミスインスタンスに関する情報を取得するアクセス許可を付与	リスト	instance*		
ListApplicationRevisions	IAM ユーザーに関連付けられているアプリケーションの、すべてのアプリケーションのリビジョンに関する情報を取得するアクセス許可を付与	リスト	application*		
ListApplications	IAM ユーザーに関連付けられているすべてのアプリケーションに関する情報を取得するアクセス許可を付与	リスト			
ListDeploymentConfigs	IAM ユーザーに関連付けられているすべてのデプロイ設定に関する情報を取得するアクセス許可を付与	リスト			
ListDeploymentGroups	IAM ユーザーに関連付けられているアプリケーションの、すべてのデプロイグループに関する情報を取得するアクセス許可を付与	リスト	application*		
ListDeploymentInstances	IAM ユーザーに関連付けられているデプロイの、すべてのインスタンスに関する情報を取得するアクセス許可を付与	リスト	deploymentgroup*		
ListDeploymentTargets	デプロイに関連付けられているターゲット ID の配列を返すアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListDeployments	IAM ユーザーに関連付けられているデプロイグループへのすべてのデプロイに関する情報を取得する、またはIAMユーザーに関連付けられているすべてのデプロイを取得するアクセス許可を付与	リスト	deploymentgroup*		
ListGitHubAccountTokenNames	GitHub アカウントに保存された接続名を一覧表示するアクセス許可を付与	リスト			
ListOnPremisesInstances	1 つ以上のオンプレミスインスタンス名のリストを取得するアクセス許可を付与	リスト			
ListTagsForResource	指定した ARN によって識別されるリソースのタグのリストを返すアクセス許可を付与 タグは、CodeDeploy リソースを整理および分類するために使用されます	リスト	application deploymentgroup		
PutLifecycleEventHookExecutionStatus	IAM ユーザーに関連付けられているデプロイのライフサイクルイベントフックの実行ステータスを通知するアクセス許可を付与	書き込み			
RegisterApplicationRevision	IAM ユーザーに関連付けられているアプリケーションの、アプリケーションのリビジョンに関する情報を登録するアクセス許可を付与	書き込み	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RegisterOnPremisesInstance	オンプレミスインスタンスを登録するアクセス許可を付与	書き込み	instance*		
RemoveTagsFromOnPremisesInstances	1 つ以上のオンプレミスインスタンスからタグを削除するアクセス許可を付与	Tagging	instance*		
SkipWaitTimeForInstanceTermination	指定した待機時間を上書きし、トラフィックのルーティング完了直後にインスタンスの終了をスタートするアクセス許可を付与 このアクションは、blue-green デプロイにのみ適用されます	書き込み			
StopDeployment	デプロイを停止する許可を付与。	書き込み			
TagResource	入力タグパラメータ内のタグのリストを、ResourceArn 入力パラメータにより識別されるリソースに関連付けるアクセス許可を付与	Tagging	application		
			deploymentgroup		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	タグのリストからリソースの関連付けを解除するアクセス許可を付与 リソースは、ResourceArn 入力パラメータによって識別されます。タグは、TagKeys 入力パラメータ内のキーのリストによって識別されます	Tagging	application		
			deploymentgroup		
				aws:TagKeys	
UpdateApplication	アプリケーションを更新する許可を付与	書き込み	application*		
UpdateDeploymentGroup	IAM ユーザーに関連付けられているアプリケーションの、単一のデプロイグループに関する情報を変更するアクセス許可を付与	書き込み	deploymentgroup*		

AWS CodeDeploy で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
application	`arn:${Partition}:codedeploy:${Region}:${Account}:application:${ApplicationName}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
deploymentconfig	arn:${Partition}:codedeploy:${Region}:${Account}:deploymentconfig:${DeploymentConfigurationName}	
deploymentgroup	arn:${Partition}:codedeploy:${Region}:${Account}:deploymentgroup:${ApplicationName}/${DeploymentGroupName}	aws:ResourceTag/${TagKey}
instance	arn:${Partition}:codedeploy:${Region}:${Account}:instance:${InstanceName}	

AWS CodeDeploy の条件キー

AWS CodeDeploy では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアのプレゼンスに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいてアクションをフィルタリングします	ArrayOfString

AWS CodeDeploy セキュアホストコマンドサービスのアクション、リソース、および条件キー

AWS CodeDeploy セキュアホストコマンドサービス (サービスプレフィックス: codedeploy-commands-secure) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS CodeDeploy セキュアホストコマンドサービスで定義されるアクション
- AWS CodeDeploy セキュアホストコマンドサービスで定義されるリソースタイプ
- AWS CodeDeploy セキュアホストコマンドサービスの条件キー

AWS CodeDeploy セキュアホストコマンドサービスで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイ

プが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetDeploymentSpecification	デプロイの仕様を取得する許可を付与	読み取り			
PollHostCommand	ホストエージェントコマンドをリクエストする許可を付与	読み取り			
PutHostCommandAcknowledgement	ホストエージェントコマンドを承認済みとしてマークする許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutHostCommandComplete	ホストエージェントコマンドを完了済みとしてマークする許可を付与	書き込み			

AWS CodeDeploy セキュアホストコマンドサービスで定義されるリソースタイプ

AWS CodeDeploy セキュアホストコマンドサービスは、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS CodeDeploy セキュアホストコマンドサービスへのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS CodeDeploy セキュアホストコマンドサービスの条件キー

CodeDeploy Commands Secure には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon CodeGuru のアクション、リソース、および条件キー

Amazon CodeGuru (サービスプレフィックス: `codeguru`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CodeGuru で定義されるアクション
- Amazon CodeGuru で定義されるリソースタイプ

- Amazon CodeGuru の条件キー

Amazon CodeGuru で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetCodeGuruFreeTrialSummary [アクセス許可のみ]	有効期限日を含む CodeGuru サービスの無料トライアル概要を取得する権限を付与する	読み取り			

Amazon CodeGuru で定義されるリソースタイプ

Amazon CodeGuru では、IAM ポリシーステートメントの `Resource` 要素でのリソース ARN の指定はサポートされていません。Amazon CodeGuru へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

Amazon CodeGuru の条件キー

Amazon CodeGuru には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS「グローバル条件コンテキストキー」を参照してください。

Amazon CodeGuru Profiler のアクション、リソース、および条件キー

Amazon CodeGuru Profiler (サービスプレフィックス: `codeguru-profiler`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CodeGuru Profiler で定義されるアクション
- Amazon CodeGuru Profiler によって定義されるリソースタイプ
- Amazon CodeGuru Profiler の条件キー

Amazon CodeGuru Profiler で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AddNotificationChannels	通知を発行するために、既存の SNS トピックのトピック ARNs を最大 AWS 2 つ追加するアクセス許可を付与します	書き込み	ProfilingGroup*		
BatchGetFrameMetricData	プロファイリンググループのフレームメトリクスデータを取得する許可を付与	リスト	ProfilingGroup*		
ConfigureAgent	オーケストレーションサービスに登録して、エージェントが利用するプロファイリング設定情報を取得する許可を付与	書き込み	ProfilingGroup*		
CreateProfilingGroup	プロファイリンググループを作成する許可を付与。	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteProfilingGroup	プロファイリンググループを削除する許可を付与。	書き込み	ProfilingGroup*		
DescribeProfilingGroup	プロファイリンググループを定義する許可を付与。	読み込み	ProfilingGroup*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetFindingsReportAccountSummary	アカウント内の各プロファイリンググループの最新のレコメンデーションの概要を取得する許可を付与。	読み込み			
GetNotificationConfiguration	通知設定を取得する許可を付与	読み込み	ProfilingGroup*		
GetPolicy	指定されたプロファイリンググループに関連付けられたリソースポリシーを取得するアクセス許可を付与	読み込み	ProfilingGroup*		
GetProfile	特定のプロファイリンググループの集計プロファイルを取得する許可を付与。	読み込み	ProfilingGroup*		
GetRecommendations	レコメンデーションを取得する許可を付与	読み込み	ProfilingGroup*		
ListFindingsReports	特定のプロファイリンググループに利用可能なレコメンデーションレポートを一覧表示する許可を付与	リスト	ProfilingGroup*		
ListProfileTimes	特定のプロファイリンググループに利用可能な集計プロファイルの開始時間を一覧表示する許可を付与	リスト	ProfilingGroup*		
ListProfilingGroups	アカウント内のプロファイリンググループを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTagsForResource	プロファイリンググループのタグを一覧表示する許可を付与	リスト	ProfilingGroup*		
PostAgentProfile	特定のプロファイリンググループに属するエージェントによって収集されたプロファイルを集計用に送信する許可を付与	書き込み	ProfilingGroup*		
PutPermission	指定されたプロファイリンググループに関連付けられたリソースポリシーで、アクショングループに許可されているプリンシパルのリストを更新するアクセス許可を付与	権限の管理	ProfilingGroup*		
RemoveNotificationChannel	通知設定からすでに設定済みの SNSTopic arn を削除する許可を付与	書き込み	ProfilingGroup*		
RemovePermission	指定されたプロファイリンググループに関連付けられたリソースポリシーから、指定されたアクショングループのアクセス許可を削除するアクセス許可を付与	権限の管理	ProfilingGroup*		
SubmitFeedback	有用または有用でない異常に対するユーザーフィードバックを送信する許可を付与	書き込み	ProfilingGroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagResource	プロファイリンググループにタグを追加または上書きする許可を付与	タグ付け	ProfilingGroup*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	プロファイリンググループからタグを削除する許可を付与	タグ付け	ProfilingGroup*		
				aws:TagKeys	
UpdateProfilingGroup	特定のプロファイリンググループを更新する許可を付与	書き込み	ProfilingGroup*		

Amazon CodeGuru Profiler によって定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
ProfilingGroup	`arn:${Partition}:codeguru-profiler:${Region}:${Account}:profilingGroup/${ProfilingGroupName}`	aws:ResourceTag/${TagKey}

Amazon CodeGuru Profiler の条件キー

Amazon CodeGuru Profiler では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

Amazon CodeGuru Reviewer のアクション、リソース、および条件キー

Amazon CodeGuru Reviewer (サービスプレフィックス: codeguru-reviewer) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CodeGuru Reviewer によって定義されるアクション
- Amazon CodeGuru Reviewer によって定義されるリソースタイプ

- Amazon CodeGuru Reviewer の条件キー

Amazon CodeGuru Reviewer によって定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateRepository	リポジトリを Amazon CodeGuru Reviewer に関連付けるアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	codecommit:GetRepository codecommit:ListRepositories codecommit:TagResource codestar-connections:PassConnection events:PutRule events:PutTargets iam:CreateServiceLinkedRole s3:CreateBucket s3:ListBucket

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					s3:PutBucketPolicy s3:PutLifecycleConfiguration
CreateCodeReview	コードレビューを作成する許可を付与。	書き込み	association*		s3:GetObject
				aws:ResourceTag/${TagKey}	
CreateConnectionToken [アクセス許可のみ]	サードパーティープロバイダーのウェブベースの oauth ハンドシェイクを実行する許可を付与。	読み込み			
DescribeCodeReview	コードレビューを記述する許可を付与。	読み込み	association*		
				aws:ResourceTag/${TagKey}	
DescribeRecommendationFeedback	コードレビューのレコメンデーションフィードバックを記述する許可を付与。	読み込み	association*		
				aws:ResourceTag/${TagKey}	
DescribeRepositoryAssociation	リポジトリの関連付けを記述する許可を付与。	読み込み	association*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
DisassociateRepository	リポジトリと Amazon CodeGuru Reviewer の関連付けを解除する許可を付与。	書き込み	association*		codecommit:UntagResource events:DeleteRule events:RemoveTargets
				aws:ResourceTag/${TagKey}	
GetMetricsData [アクセス許可のみ]	コンソールでプルリクエストメトリクスを表示する許可を付与。	読み込み			
ListCodeReviews	コードレビューの概要を一覧表示する許可を付与。	リスト			
ListRecommendationFeedback	コードレビューのレコメンデーションフィードバックの概要を一覧表示する許可を付与。	リスト	association*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListRecommendations	コードレビューのレコメンデーションの概要を一覧表示する許可を付与。	リスト	association*		
				aws:ResourceTag/${TagKey}	
ListRepositoryAssociations	リポジトリの関連付けの概要を一覧表示する許可を付与。	リスト			
ListTagsForResource	関連するリポジトリ ARN に接続されたリソースを一覧表示する許可を付与。	リスト	association*		
				aws:ResourceTag/${TagKey}	
ListThirdPartyRepositories [許可のみ]	コンソールでサードパーティープロバイダーのリポジトリを一覧表示する許可を付与。	読み込み			
PutRecommendationFeedback	コードレビューのレコメンデーションのフィードバックをプットする許可を付与。	書き込み	association*		
				aws:ResourceTag/${TagKey}	
TagResource	関連するリポジトリ ARN にリソースタグを接続する許可を付与。	タグ付け	association*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UnTagResource	関連するリポジトリ ARN からリソースタグの関連付けを解除する許可を付与。	タグ付け	association*		
				aws:TagKeys	

Amazon CodeGuru Reviewer によって定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
association	arn:${Partition}:codeguru-reviewer:${Region}:${Account}:association:${ResourceId}	aws:ResourceTag/${TagKey}
codereview	arn:${Partition}:codeguru-reviewer:${Region}:${Account}:association:${ResourceId}:codereview:${CodeReviewId}	

Amazon CodeGuru Reviewer の条件キー

Amazon CodeGuru Reviewer では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアのプレゼンスに基づいてアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいてアクセスをフィルタリングします	ArrayOfString

Amazon CodeGuru Security のアクション、リソース、および条件キー

Amazon CodeGuru Security (サービスプレフィックス: codeguru-security) では、IAM 許可ポリシーで使用できるように、次のサービス固有のリソース、アクション、および条件キーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CodeGuru Security によって定義されたアクション
- Amazon CodeGuru Security によって定義されたリソースタイプ

- Amazon CodeGuru Security の条件キー

Amazon CodeGuru Security によって定義されたアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchGetFindings	CodeGuru Security によって生成された特定の検出結果をバッチ取得するための許可を付与します	読み取り	ScanName*		
CreateScan	CodeGuru Security スキャンを作成する許可を付与	書き込み	ScanName*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateUploadUrl	コードアーカイブをアップロードするための署名付き URL を生成するための許可を付与します	書き込み	ScanName*		
DeleteScansByCategory [アクセス許可のみ]	特定のカテゴリ別に CodeGuru Security からすべてのスキャンおよび関連する検出結果を削除するための許可を付与します	書き込み			
GetAccountConfiguration	アカウントレベルの設定を取得する許可を付与	読み取り			
GetFindings	CodeGuru Security によって生成されたスキャンの検出結果を取得する許可を付与	リスト	ScanName*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetMetricsSummary	CodeGuru Security AWS によって生成されたアカウントレベルのメトリクスの概要を取得する許可を付与	読み取り			
GetScan	CodeGuru Security スキャンメタデータを取得するための許可を付与します	読み取り	ScanName		
				aws:ResourceTag/${TagKey}	
ListFindings [許可のみ]	CodeGuru Security によって生成された検出結果を取得するための許可を付与します	リスト			
ListFindingsMetrics	アカウントレベルでの検出結果のメトリクスのリストを日付範囲を指定して取得する許可を付与	リスト			
ListScans	CodeGuru Security スキャンメタデータのリストを取得するための許可を付与します	リスト			
ListTagsForResource	スキャンを実行する名前 (ARN) のタグのリストを取得する許可を付与	読み取り	ScanName		
				aws:ResourceTag/${TagKey}	
TagResource	スキャンを実行する名前 (ARN) にタグを追加する許可を付与	Tagging	ScanName		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	スキャンを実行する名前 (ARN) からタグを削除する許可を付与	Tagging	ScanName		
				aws:TagKeys	
UpdateAccountConfiguration	アカウントレベルの設定を更新するための許可を付与します	書き込み			

Amazon CodeGuru Security によって定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
ScanName	`arn:${Partition}:codeguru-security:${Region}:${Account}:scans/${ScanName}`	aws:ResourceTag/${TagKey}

Amazon CodeGuru Security の条件キー

Amazon CodeGuru Security では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS CodePipeline のアクション、リソース、および条件キー

AWS CodePipeline (サービスプレフィックス: codepipeline) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS CodePipeline で定義されるアクション
- AWS CodePipeline で定義されるリソースタイプ

- AWS CodePipeline の条件キー

AWS CodePipeline で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AcknowledgeJob	指定されたジョブに関する情報や、そのジョブがジョブワーカーによって受け取られたかどうかについて表示する許可を付与	書き込み			
AcknowledgeThirdPartyJob	ジョブワーカーが指定されたジョブを受け取ったことを確認する許可を付与 (パートナーアクションのみ)	書き込み			
CreateCustomActionType	に関連付けられたパイプラインで使用できるカスタムアクションを作成するアクセス許可を付与します AWS アカウント	書き込み	actiontype*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePipeline	一意の名前が付けられたパイプラインを作成する許可を付与	書き込み	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCustomActionType	カスタムアクションを削除する許可を付与	書き込み	actiontype*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeletePipeline	指定されたパイプラインを削除する許可を付与	書き込み	pipeline*		
DeleteWebhook	指定されたウェブフックを削除する許可を付与	書き込み	webhook*		
DeregisterWebhookWithThirdParty	設定で指定されたサードパーティーからウェブフックの登録を削除する許可を付与	書き込み	webhook*		
DisableStageTransition	リビジョンがパイプラインの次のステージに移行することを禁止する許可を付与	書き込み	stage*		
EnableStageTransition	リビジョンをパイプラインの次のステージに移行することを許可する許可を付与	書き込み	stage*		
GetActionType	アクションタイプに関する情報を表示する許可を付与	読み込み			
GetJobDetails	ジョブに関する情報を表示する許可を付与 (カスタムアクションのみ)	読み込み			
GetPipeline	パイプライン構造に関する情報を取得する許可を付与	読み込み	pipeline*		
GetPipelineExecution	パイプラインの実行に関する情報 (アーティファクト、パイプラインの実行 ID、パイプラインの名前、バージョン、ステータスなど) を表示する許可を付与	読み込み	pipeline*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetPipelineState	パイプラインのステージとアクションの現在の状態に関する情報を表示する許可を付与	読み込み	pipeline*		
GetThirdPartyJobDetails	サードパーティーアクションのジョブの詳細を表示する許可を付与 (パートナーアクションのみ)	読み込み			
ListActionExecutions	パイプラインで発生したアクション実行を一覧表示する許可を付与	読み込み	pipeline*		
ListActionTypes	アカウントのパイプラインで使用可能なすべてのアクションタイプの概要を一覧表示する許可を付与	読み取り			
ListDeployActionExecutionTargets	パイプラインで発生したデプロイアクション実行のデプロイの詳細を一覧表示するアクセス許可を付与します	読み取り	pipeline*		
ListPipelineExecutions	パイプラインの最新の実行の概要を一覧表示する許可を付与	リスト	pipeline*		
ListPipelines	に関連付けられているすべてのパイプラインの概要を一覧表示するアクセス許可を付与します AWS アカウント	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListRuleExecutions	パイプラインで発生したルール実行を一覧表示する許可を付与する	読み取り	pipeline*		
ListRuleTypes	アカウントのパイプラインで使用可能なすべてのルールタイプの概要を一覧表示する許可を付与する	読み取り			
ListTagsForResource	CodePipeline リソースのタグを一覧表示する許可を付与	読み取り	actiontype		
			pipeline		
			webhook		
ListWebhooks	に関連付けられているすべてのウェブフックを一覧表示するアクセス許可を付与しますAWS アカウント	リスト	webhook*		
OverrideStageCondition	ステージの条件を上書きしてパイプラインの実行を再開する許可を付与する	書き込み	stage*		
PollForJobs	CodePipeline が影響するジョブに関する情報を表示する許可を付与	書き込み	actiontype*		
PollForThirdPartyJobs	ジョブワーカーが処理するサードパーティージョブがあるかどうかを決定する許可を付与 (パートナーアクションのみ)	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutActionRevision	パイプラインのアクションを編集する許可を付与	書き込み	action*		
PutApprovalResult	CodePipeline の手動承認リクエストへのレスポンス (承認済みまたは拒否済み) を提供する許可を付与	書き込み	action*		
PutJobFailureResult	ジョブワーカーによってパイプラインに返されるジョブの失敗を表すアクセス許可を付与します (カスタムアクションのみ)	書き込み			
PutJobSuccessResult	ジョブワーカーによってパイプラインに返されるジョブの成功を表すアクセス許可を付与します (カスタムアクションのみ)	書き込み			
PutThirdPartyJobFailureResult	ジョブワーカーによってパイプラインに返されたサードパーティージョブの失敗を表すアクセス許可を付与します (パートナーアクションのみ)	書き込み			
PutThirdPartyJobSuccessResult	ジョブワーカーによってパイプラインに返されたサードパーティージョブの成功を表すアクセス許可を付与します (パートナーアクションのみ)	書き込み			
PutWebhook	ウェブフックを作成または更新する許可を付与	書き込み	pipeline*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			webhook*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RegisterWebhookWithThirdParty	設定で指定したサードパーティーにウェブフックを登録する許可を付与	書き込み	webhook*		
RetryStageExecution	ステージで最後に失敗したアクションを再試行することでパイプラインの実行を再開する許可を付与	書き込み	stage*		
RollbackStage	ステージを以前の成功した実行にロールバックする許可を付与する	書き込み	stage*		
StartPipelineExecution	パイプラインを通じて最新のリビジョンを実行する許可を付与	書き込み	pipeline*		
StopPipelineExecution	進行中のパイプラインの実行を停止する許可を付与	書き込み	pipeline*		
TagResource	CodePipeline リソースにタグを付けるアクセス許可を付与します	タグ付け	actiontype		
			pipeline		
			webhook		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	CodePipeline リソースからタグを削除する許可を付与	Tagging	actiontype		
			pipeline		
			webhook		
				aws:TagKeys	
UpdateActionType	アクションタイプを更新する許可を付与	書き込み	actiontype*		
UpdatePipeline	パイプラインの構造に対する変更を適用してパイプラインを更新する許可を付与	書き込み	pipeline*		

AWS CodePipeline で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
action	arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}/${StageName}/${ActionName}	aws:ResourceTag/${TagKey}
actiontype	arn:${Partition}:codepipeline:${Region}:${Account}:actiontype:${Owner}/${Category}/${Provider}/${Version}	aws:ResourceTag/${TagKey}
pipeline	arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}	aws:ResourceTag/${TagKey}
stage	arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}/${StageName}	aws:ResourceTag/${TagKey}
webhook	arn:${Partition}:codepipeline:${Region}:${Account}:webhook:${WebhookName}	aws:ResourceTag/${TagKey}

AWS CodePipeline の条件キー

AWS CodePipeline は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアのプレゼンスに基づいてアクションをフィルタリングします	文字列

条件キー	説明	タイプ
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいてアクションをフィルタリングします	ArrayOfString

AWS CodeStar のアクション、リソース、および条件キー

AWS CodeStar (サービスプレフィックス: codestar) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS CodeStar で定義されるアクション
- AWS CodeStar で定義されるリソースタイプ
- AWS CodeStar の条件キー

AWS CodeStar で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateTeamMember	AWS CodeStar プロジェクトのチームにユーザーを追加するアクセス許可を付与します	権限の管理	project*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateProject	最小の構造とカスタマーポリシーを備え、リソースなしでプロジェクトを作成する許可を付与	権限の管理		aws:RequestTag/${TagKey} aws:TagKeys	
CreateUserProfile	ユーザー設定、表示名、E メールを含むユーザー向けプロファイルを作成する許可を付与	書き込み	user*		
DeleteExtendedAccess [アクセス許可のみ]	拡張された削除 API に許可を付与	書き込み	project*		
DeleteProject	プロジェクト (プロジェクトリソースを含む) を削除する許可を付与 プロジェクトに関連付けられているユーザーは削除されませんが、プロジェクトへのアクセスを許可した IAM ロールは削除されます	権限の管理	project*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteUserProfile	表示名や E メールアドレスなど、そのプロファイルに関連付けられたすべての個人設定データを含む、 AWS CodeStar のユーザープロファイルを削除するアクセス許可を付与します。該当ユーザーの履歴 (例: 該当ユーザーが行ったコミットの履歴) は削除されません	書き込み	user*		
DescribeProject	プロジェクトとそのリソースを記述するアクセス許可を付与	読み取り	project*		
DescribeUserProfile	AWS CodeStar のユーザーとすべてのプロジェクトのユーザー属性を記述するアクセス許可を付与します	読み取り			
DisassociateTeamMember	ユーザーをプロジェクトから削除する許可を付与 プロジェクトからユーザーを削除すると、プロジェクトとそのリソースへのアクセスを許可した IAM ポリシーもそのユーザーから削除されます	権限の管理	project*		
GetExtendedAccess [許可のみ]	拡張された読み取り API に許可を付与	読み取り	project*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListProjects	に関連付けられている CodeStar 内のすべてのプロジェクトを一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListResources	CodeStar のプロジェクトに関連付けられているすべてのリソースを一覧表示する許可を付与	リスト	project*		
ListTagsForProject	CodeStar のプロジェクトに関連付けられているタグを一覧表示する許可を付与	リスト	project*		
ListTeamMembers	プロジェクトに関連付けられているすべてのチームメンバーを一覧表示する許可を付与	リスト	project*		
ListUserProfiles	AWS CodeStar でユーザープロファイルを一覧表示する許可を付与	リスト			
PutExtendedAccess [許可のみ]	拡張された書き込み API に許可を付与	書き込み	project*		
TagProject	CodeStar でプロジェクトにタグを追加する許可を付与	Tagging	project*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagProject	CodeStar でプロジェクトからタグを削除する許可を付与	Tagging	project*		
				aws:TagKeys	
UpdateProject	CodeStar でプロジェクトを更新する許可を付与	書き込み	project*		
UpdateTeamMember	CodeStar プロジェクト内のチームメンバーの属性を更新する許可を付与	権限の管理	project*		
UpdateUserProfile	ユーザー設定、表示名、E メールを含むユーザー向けプロファイルを更新する許可を付与	書き込み	user*		
VerifyServiceRole	AWS CodeStar サービスロールがお客様のアカウントに存在するかどうかを確認するアクセス許可を付与します	リスト			

AWS CodeStar で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
project	`arn:${Partition}:codestar:${Region}:${Account}:project/${ProjectId}`	aws:ResourceTag/${TagKey}
user	`arn:${Partition}:iam::${Account}:user/${AwsUserName}`	iam:ResourceTag/${TagKey}

AWS CodeStar の条件キー

AWS CodeStar は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	各タグで許可されている値のセットに基づいてリクエストでアクセスをフィルタリング	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値に基づいて、アクションでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内の必須のタグの存在に基づくリクエストによってアクセスをフィルタリング	ArrayOfString
iam:ResourceTag/${TagKey}	リソースに関連付けられたタグ値に基づいて、アクションでアクセスをフィルタリングします	String

AWS CodeStar Connections のアクション、リソース、および条件キー

AWS CodeStar Connections (サービスプレフィックス: codestar-connections) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS CodeStar Connections で定義されるアクション
- AWS CodeStar Connections で定義されるリソースタイプ
- AWS CodeStar Connections の条件キー

AWS CodeStar Connections で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateConnection	接続リソースを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys codestar-connections:ProviderType	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateHost	ホストリソースを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys codestar-connections:ProviderType codestar-connections:VpcId	
CreateRepositoryLink	リポジトリリンクを作成するためのアクセス許可を付与	書き込み	Connection*		codestar-connections:PassConnection codestar-connections:UseConnection
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSyncConfiguration	テンプレート同期設定を作成する許可を付与。	書き込み	RepositoryLink*		codestar-connections:PassRepository iam:PassRole
				codestar-connections:Branch	
DeleteConnection	接続リソースを削除する許可を付与	書き込み	Connection*		
DeleteHost	ホストリソースを削除する許可を付与	書き込み	Host*		
DeleteRepositoryLink	リポジトリリンクを削除するためのアクセス許可を付与	書き込み	RepositoryLink*		
DeleteSyncConfiguration	同期設定を削除するためのアクセス許可を付与	書き込み			
GetConnection	接続リソースに関する詳細を取得する許可を付与	読み取り	Connection*		
GetConnectionToken [許可のみ]	接続トークンを取得してプロバイダーのアクションを呼び出す許可を付与する	読み取り	Connection*		
GetHost	ホストリソースに関する詳細を取得する許可を付与	読み込み	Host*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetIndividualAccessToken [許可のみ]	Bitbucket アプリのインストールなど、サードパーティーを接続に関連付けるアクセス許可を付与	読み込み		codestar-connections:ProviderType	codestar-connections:StartOAuthHandshake
GetInstallationUrl [許可のみ]	Bitbucket アプリのインストールなど、サードパーティーを接続に関連付けるアクセス許可を付与	読み取り		codestar-connections:ProviderType	
GetRepositoryLink	リポジトリリンクを記述するためのアクセス許可を付与	読み取り	RepositoryLink*		
GetRepositorySyncStatus	リポジトリの最新の同期ステータスを取得する許可を付与。	読み取り	RepositoryLink*		
				codestar-connections:Branch	
GetResourceSyncStatus	リソース (cfn スタックまたはその他のリソース) の最新の同期ステータスを取得するためのアクセス許可を付与	読み取り			
GetSyncBlockerSummary	リソース (cfn スタックまたはその他のリソース) のサービス同期ブロッカーを説明するためのアクセス許可を付与	読み取り			
GetSyncConfiguration	同期設定を記述するためのアクセス許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListConnections	接続リソースを一覧表示する許可を付与	リスト	Connection*		
				codestar-connections:ProviderTypeFilter	
ListHosts	ホストリソースを一覧表示する許可を付与	リスト		codestar-connections:ProviderTypeFilter	
ListInstallationTargets [許可のみ]	Bitbucket アプリのインストールなど、サードパーティーを接続に関連付けるアクセス許可を付与	リスト			codestar-connections:GetIndividualAccessToken codestar-connections:StartOAuthHandshake
ListRepositoryLinks	リポジトリリンクを一覧表示するためのアクセス許可を付与	リスト			
ListRepositorySyncDefinitions	リポジトリ同期定義を一覧表示する許可を付与。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListSyncConfigurations	リポジトリリンクの同期設定を一覧表示するためのアクセス許可を付与	リスト			
ListTagsForResource	リソースの管理に使用されるキーと値のペアのセットへの許可を付与	リスト	Connection		
			Host		
			RepositoryLink		
PassConnection [許可のみ]	codepipeline:CreatePipeline などの接続 ARN を入力として受け入れる AWS サービスに接続リソースを渡すアクセス許可を付与します	読み取り	Connection*		
				codestar-connections:PassedToService	
PassRepository [許可のみ]	codestar-connections:CreateSyncConfiguration などの RepositoryLinkId を入力として受け入れる AWS サービスにリポジトリリンクリソースを渡すアクセス許可を付与します	読み取り	RepositoryLink*		
				codestar-connections:PassedToService	
RegisterAppCode [許可のみ]	GitHub Enterprise Server インスタンスなどのサードパーティーサーバーをホストに関連付けるアクセス許可を付与	読み込み		codestar-connections:HostArn	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartAppRegistrationHandshake [許可のみ]	GitHub Enterprise Server インスタンスなどのサードパーティーサーバーをホストに関連付けるアクセス許可を付与	読み込み		codestar-connections:HostArn	
StartOAuthHandshake [許可のみ]	Bitbucket アプリのインストールなど、サードパーティーを接続に関連付けるアクセス許可を付与	読み取り		codestar-connections:ProviderType	
TagResource	指定されたリソースのタグに追加または変更する許可を付与	Tagging	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	AWS リソースからタグを削除するアクセス許可を付与します	Tagging	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateConnectionInstallation	CodeStar Connections アプリをインストールした接続リソースを更新する許可を付与	書き込み	Connection*		codestar-connections:GetIndividualAccessToken codestar-connections:GetInstallationUrl codestar-connections:ListInstallationTargets codestar-connections:StartOAuthHandshake
				codestar-connections:InstallationId	
UpdateHost	ホストリソースを更新するアクセス許可を付与	書き込み	Host*		
				codestar-connections:VpcId	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateRepositoryLink	リポジトリリンクを更新するためのアクセス許可を付与	書き込み	RepositoryLink*		
UpdateSyncBlocker	リソース (cfn スタックまたはその他のリソース) の同期ブロッカーを更新するためのアクセス許可を付与	書き込み			
UpdateSyncConfiguration	同期設定を更新するためのアクセス許可を付与	書き込み		codestar-connections:Branch	
UseConnection [アクセス許可のみ]	接続リソースを使用してプロバイダーのアクションを呼び出すアクセス許可を付与	読み込み	Connection*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				codestar-connections:BranchName codestar-connections:FullRepositoryId codestar-connections:OwnerId codestar-connections:ProviderAction codestar-connections:ProviderPermissionsRequired codestar-connections:RepositoryName	

AWS CodeStar Connections で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Connection	arn:${Partition}:codestar-connections:${Region}:${Account}:connection/${ConnectionId}	aws:ResourceTag/${TagKey}
Host	arn:${Partition}:codestar-connections:${Region}:${Account}:host/${HostId}	aws:ResourceTag/${TagKey}
RepositoryLink	arn:${Partition}:codestar-connections:${Region}:${Account}:repository-link/${RepositoryLinkId}	aws:ResourceTag/${TagKey}

AWS CodeStar Connections の条件キー

AWS CodeStar Connections では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列

条件キー	説明	タイプ
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
codestar-connections:Branch	リクエストで渡されたブランチ名でアクセスをフィルタリングします	String
codestar-connections:BranchName	リクエストで渡されたブランチ名でアクセスをフィルタリングします 特定のリポジトリブランチへのアクセスに関する UseConnection リクエストにのみ適用します	文字列
codestar-connections:FullRepositoryId	リクエストで渡されたリポジトリによるアクセスをフィルタリングします。特定のリポジトリにアクセスするための UseConnection リクエストにのみ適用します	文字列
codestar-connections:HostArn	リクエストで使用された接続に関連付けられたホストリソースによってアクセスをフィルタリングします	ARN
codestar-connections:InstallationId	Connection の更新に使用されるサードパーティー ID (CodeStar Connections 用の Bitbucket アプリのインストール ID など) でアクセスをフィルタリングします。Connection を作成するために使用できるサードパーティー製アプリのインストールを制限できます。	文字列
codestar-connections:OwnerId	サードパーティーのリポジトリの所有者によるアクセスをフィルタリングします。特定のユーザーが所有するリポジトリへのアクセスに関する UseConnection リクエストにのみ適用	String

条件キー	説明	タイプ
codestar-connections:PassedToService	プリンシパルが接続または RepositoryLink を渡すことを許可されているサービスでアクセスをフィルタリングします	String
codestar-connections:ProviderAction	ListRepositories など、UseConnection リクエストのプロバイダーアクションによってアクセスをフィルタリングします。すべての有効な値については、ドキュメントを参照してください。	文字列
codestar-connections:ProviderPermissionsRequired	UseConnection リクエストのプロバイダーアクションの書き込みアクセス許可でアクセスをフィルタリングします。有効なタイプには、読み取り専用と読み取り書き込みがあります。	文字列
codestar-connections:ProviderType	リクエストで渡されたサードパーティープロバイダーのタイプによってアクセスをフィルタリングします。	文字列
codestar-connections:ProviderTypeFilter	結果をフィルタリングするために使用されるサードパーティープロバイダーのタイプによってアクセスをフィルタリングします。	文字列
codestar-connections:RepositoryName	リクエストで渡されたリポジトリ名でアクセスをフィルタリングします。特定のユーザーが所有するリポジトリへのアクセスに関する UseConnection リクエストにのみ適用	String
codestar-connections:VpcId	リクエストで渡された VpcId でアクセスをフィルタリングします	String

AWS CodeStar Notifications のアクション、リソース、および条件キー

AWS CodeStar Notifications (サービスプレフィックス: codestar-notifications) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS CodeStar Notifications で定義されるアクション
- AWS CodeStar Notifications で定義されるリソースタイプ
- AWS CodeStar Notifications の条件キー

AWS CodeStar Notifications で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateNotificationRule	リソースの通知ルールを作成する許可を付与。	書き込み	notificationrule*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				codestar-notifications:NotificationsForResource	
DeleteNotificationRule	リソースの通知ルールを削除する許可を付与。	書き込み	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
DeleteTarget	通知ルールのターゲットを削除する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeNotificationRule	通知ルールに関する情報を取得する許可を付与。	読み込み	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
ListEventTypes	通知イベントタイプを一覧表示する許可を付与。	リスト			
ListNotificationRules	の通知ルールを一覧表示するアクセス許可を付与しますAWS アカウント	リスト			
ListTagsForResource	通知ルールリソース ARN にアタッチされたタグを一覧表示する許可を付与。	リスト	notificationrule*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
ListTargets	の通知ルールターゲットを一覧表示するアクセス許可を付与します AWS アカウント	リスト		aws:RequestTag/${TagKey} aws:TagKeys	
Subscribe	通知ルールと Amazon SNS トピック間の関連付けを作成する許可を付与。	書き込み	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagResource	通知ルールリソース ARN にリソースタグをアタッチする許可を付与。	タグ付け	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
Unsubscribe	通知ルールと Amazon SNS トピック間の関連付けを削除する許可を付与。	書き込み	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	通知ルールリソース ARN からリソースタグの関連付けを解除する許可を付与。	タグ付け	notificationrule*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateNotificationRule	リソースの通知ルールを変更する許可を付与。	書き込み	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	

AWS CodeStar Notifications で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
notificationrule	arn:${Partition}:codestar-notifications:${Region}:${Account}:notificationrule/${NotificationRuleId}	aws:ResourceTag/${TagKey}

AWS CodeStar Notifications の条件キー

AWS CodeStar Notifications では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアのプレゼンスに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいてアクションをフィルタリングします	ArrayOfString
codestar-notifications:Noti	通知が設定されているリソースの ARN に基づいてアクセスをフィルタリングします。	ARN

条件キー	説明	タイプ
fications ForResource		

Amazon CodeWhisperer のアクション、リソース、および条件キー

Amazon CodeWhisperer (サービスプレフィックス: codewhisperer) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon CodeWhisperer で定義されるアクション
- Amazon CodeWhisperer で定義されるリソースタイプ
- Amazon CodeWhisperer の条件キー

Amazon CodeWhisperer で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AllowVendedLogDeliveryForResource [アクセス許可のみ]	CodeWhisperer カスタマイゼーションリソースの vended log 配信を設定する許可を付与	権限の管理	customization*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateCustomizationPermission [許可のみ]	CodeWhisperer で AssociateCustomizationPermission を呼び出すアクセス許可を付与します	書き込み	customization*		
				aws:ResourceTag/${TagKey}	
CreateCustomization [アクセス許可のみ]	CodeWhisperer で CreateCustomization を呼び出すアクセス許可を付与します	書き込み	customization*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateProfile [アクセス許可のみ]	CodeWhisperer で CreateProfile を呼び出す許可を付与	書き込み	profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteCustomization [アクセス許可のみ]	CodeWhisperer で DeleteCustomization を呼び出すアクセス許可を付与します	書き込み	customization*		
				aws:ResourceTag/${TagKey}	
DeleteProfile [アクセス許可のみ]	CodeWhisperer で DeleteProfile を呼び出すアクセス許可を付与	書き込み	profile*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
DisassociateCustomizationPermission [アクセス許可のみ]	CodeWhisperer で DisassociateCustomizationPermission を呼び出すアクセス許可を付与します	書き込み	customization*		
				aws:ResourceTag/${TagKey}	
GenerateRecommendations [アクセス許可のみ]	CodeWhisperer で GenerateRecommendations を呼び出す許可を付与	読み取り			
GetCustomization [許可のみ]	CodeWhisperer で GetCustomization を呼び出すアクセス許可を付与します	読み取り	customization*		
				aws:ResourceTag/${TagKey}	
ListCustomizationPermissions [許可のみ]	CodeWhisperer で ListCustomizationPermissions を呼び出すアクセス許可を付与します	リスト	customization*		
				aws:ResourceTag/${TagKey}	
ListCustomizationVersions [許可のみ]	CodeWhisperer で ListCustomizationVersions を呼び出すためのアクセス許可を付与	リスト	customization*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
ListCustomizations [許可のみ]	CodeWhisperer で ListCustomizations を呼び出すアクセス許可を付与します	リスト	customization*		
ListProfiles [許可のみ]	CodeWhisperer で ListProfiles を呼び出す許可を付与	リスト			
ListTagsForResource [許可のみ]	CodeWhisperer で istTagsForResource を呼び出すアクセス許可を付与	リスト	customization		
			profile		
				aws:ResourceTag/${TagKey}	
TagResource [許可のみ]	CodeWhisperer で TagResource を呼び出すアクセス許可を付与	Tagging	customization		
			profile		
				aws:ResourceTag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource [アクセス許可のみ]	CodeWhisperer で UntagResource を呼び出すアクセス許可を付与	Tagging	customization		
			profile		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCustomization [アクセス許可のみ]	CodeWhisperer で UpdateCustomization を呼び出すアクセス許可を付与します	書き込み	customization*		
				aws:ResourceTag/${TagKey}	
UpdateProfile [アクセス許可のみ]	CodeWhisperer で UpdateProfile を呼び出す許可を付与	書き込み	profile*		
				aws:ResourceTag/${TagKey}	

Amazon CodeWhisperer で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
profile	arn:${Partition}:codewhisperer:${Region}:${Account}:profile/${Identifier}	aws:ResourceTag/${TagKey}
customization	arn:${Partition}:codewhisperer:${Region}:${Account}:customization/${Identifier}	aws:ResourceTag/${TagKey}

Amazon CodeWhisperer の条件キー

Amazon CodeWhisperer では、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	CodeWhisperer リソースに関連付けられたタグによりアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon Cognito ID のアクション、リソース、および条件キー

Amazon Cognito ID (サービスプレフィックス: cognito-identity) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Cognito ID で定義されるアクション
- Amazon Cognito ID で定義されるリソースタイプ
- Amazon Cognito ID の条件キー

Amazon Cognito ID で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateIdentityPool	新しい ID プールを作成するアクセス権限を付与します	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteIdentities	ID プールから ID を削除するアクセス権限を付与します。削除する 1～60 の ID のリストを指定できます	Write			
DeleteIdentityPool	ユーザープールを削除するアクセス権限を付与します。プールが削除されると、ユーザーはプールで認証できなくなります	Write	identitypool*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeIdentity	ID が作成された日時や関連するリンクされたログインを含む、特定の ID に関連するメタデータを返すアクセス権限を付与します	Read			
DescribeIdentityPool	プール名、ID の説明、作成日、現在のユーザー数など、特定の ID プールに関する詳細を取得するアクセス権限を付与します	Read	identitypool*		
GetCredentialsForIdentity	指定されたアイデンティティ ID の認証情報を返すアクセス権限を付与します	Read			
GetId	Cognito ID を生成 (または取得) するアクセス権限を付与します。複数のログインを提供すると、暗黙的なリンクアカウントが作成されます	書き込み			
GetIdentityPoolAnalytics	すべてのアイデンティティプール ID プロバイダー (IdP) の現在のアイデンティティ合計数に関する分析データを取得する許可を付与	読み取り	identitypool*		
GetIdentityPoolDailyAnalytics	すべてのアイデンティティプール ID プロバイダー (IdP) の新規アイデンティティの数とアイデンティティの合計数に関する分析データを取得する許可を付与	読み取り	identitypool*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetIdentityPoolRoles	ID プールのロールを取得するアクセス権限を付与します	読み取り	identitypool*		
GetIdentityProviderDailyAnalytics	1 つのアイデンティティプール ID プロバイダー (IdP) の新規アイデンティティの数とアイデンティティの合計数に関する分析データを取得する許可を付与	読み取り	identitypool*		
GetOpenIdToken	既知の Cognito ID を使用して OpenID トークンを取得するアクセス権限を付与します	Read			
GetOpenIdTokenForDeveloperIdentity	バックエンド認証プロセスによって認証されたユーザーの Cognito IdentityId と OpenID Connect トークンを登録 (または取得) するアクセス権限を付与します	Read	identitypool*		
GetPrincipalTagAttributeMap	ID プールおよびプロバイダーのプリンシパルタグを取得するアクセス権限を付与します	Read	identitypool*		
ListIdentities	ID プール内の ID を一覧表示するアクセス権限を付与します	リスト	identitypool*		
ListIdentityPools	アカウントに登録されているすべての Cognito ID プールを一覧表示するアクセス権限を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTagsForResource	Amazon Cognito ID プールに割り当てられているタグを一覧表示するアクセス権限を付与します	Read	identitypool		
LookupDeveloperIdentity	既存の ID の IdentityId に関連付けられた DeveloperUserIdentifier または DeveloperUserIdentifiers のリストに関連付けられた IdentityId を取得するアクセス権限を付与します	Read	identitypool*		
MergeDeveloperIdentities	同じ ID プールに存在し、同じデベロッパープロバイダーによって識別される、異なる IdentityId を持つ 2 人のユーザーをマージするアクセス権限を付与します	Write	identitypool*		
SetIdentityPoolRoles	ID プールのロールを設定するアクセス権限を付与します。これらのロールは、GetCredentialsForIdentity アクションを呼び出すときに使用されます	Write			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SetPrincipalTagAttributeMap	ID プールおよびプロバイダーのプリンシパルタグを設定するアクセス権限を付与します。これらのタグは、GetOpenIdToken アクションを呼び出すときに使用されます	Write			
TagResource	Amazon Cognito ID プールに一連のタグを割り当てるアクセス権限を付与します	タグ付け	identitypool		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnlinkDeveloperIdentity	DeveloperUserIdentifier を既存の ID からリンク解除するアクセス権限を付与します	Write	identitypool*		
UnlinkIdentity	フェデレーション ID を既存のアカウントからリンク解除するアクセス権限を付与します	Write			
UntagResource	Amazon Cognito ID プールから指定されたタグを削除するアクセス権限を付与します	タグ付け	identitypool		
				aws:TagKeys	
UpdateIdentityPool	ID プールを更新するアクセス権限を付与します	Write	identitypool*		

Amazon Cognito ID で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
identitypool	arn:${Partition}:cognito-identity:${Region}:${Account}:identitypool/${IdentityPoolId}	aws:ResourceTag/${TagKey}

Amazon Cognito ID の条件キー

Amazon Cognito Identity は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアのプレゼンスに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエストに存在するキーによってアクセスをフィルタリングします	ArrayOfString

Amazon Cognito Sync のアクション、リソース、および条件キー

Amazon Cognito Sync (サービスプレフィックス: cognito-sync) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Cognito Sync で定義されるアクション
- Amazon Cognito Sync で定義されるリソースタイプ
- Amazon Cognito Sync の条件キー

Amazon Cognito Sync で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BulkPublish	設定されたストリームへの ID プールの既存のすべてのデータセットの一括発行を開始するアクセス許可を付与	書き込み	identitypool*		
DeleteDataset	特定のデータセットを削除するアクセス許可を付与	書き込み	dataset*		
DescribeDataset	ID とデータセット名によるデータセットに関するメタデータを取得するアクセス許可を付与	読み込み	dataset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeIdentityPoolUsage	特定の ID プールに関する使用の詳細 (例えば、データストレージ) を取得するアクセス許可を付与	読み込み	identitypool*		
DescribeIdentityUsage	データセットの数やデータ使用量など、ID の使用情報を取得するアクセス許可を付与	読み込み	identity*		
GetBulkPublishDetails	ID プールの最後の BulkPublish オペレーションのステータスを取得するアクセス許可を付与	読み込み	identitypool*		
GetCognitoEvents	ID プールに関連付けられているイベントおよび対応する Lambda 関数を取得するアクセス許可を付与	読み込み	identitypool*		
GetIdentityPoolConfiguration	ID プールの設定を取得するアクセス許可を付与	読み込み	identitypool*		
ListDatasets	ID のデータセットを一覧表示するアクセス許可を付与	リスト	dataset*		
ListIdentityPoolUsage	Cognito に登録されている ID プールのリストを取得するアクセス許可を付与	読み込み	identitypool*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListRecords	データセットと ID の特定の同期カウント後に変更されることがある、ページ分割されたレコードを取得するアクセス許可を付与	読み込み	dataset*		
QueryRecords [許可のみ]	レコードをクエリするアクセス許可を付与	読み込み			
RegisterDevice	プッシュ同期の通知を受信するデバイスを登録するアクセス許可を付与	書き込み	identity*		
SetCognitoEvents	ID プールの特定のイベントタイプに AWS Lambda 関数を設定するアクセス許可を付与します	書き込み	identitypool*		
SetDatasetConfiguration [アクセス許可のみ]	データセットを設定するアクセス許可を付与	書き込み	dataset*		
SetIdentityPoolConfiguration	プッシュ同期に必要な設定を行うためのアクセス許可を付与	書き込み	identitypool*		
SubscribeToDataset	別のデバイスによってデータセットが変更されたときに通知を受け取るようにサブスクライブするアクセス許可を付与	書き込み	dataset*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UnsubscribeFromDataset	別のデバイスによってデータセットが変更されたときに通知を受け取らないようにサブスクライブを停止するアクセス許可を付与	書き込み	dataset*		
UpdateRecords	レコードの更新を告知し、データセットおよびユーザーのレコードを追加および削除するアクセス許可を付与	書き込み	dataset*		

Amazon Cognito Sync で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
dataset	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}/identity/${IdentityId}/dataset/${DatasetName}`	
identity	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}/identity/${IdentityId}`	

リソースタイプ	ARN	条件キー
identitypool	arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}	

Amazon Cognito Sync の条件キー

Cognito Sync には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Cognito ユーザープールのアクション、リソース、および条件キー

Amazon Cognito ユーザープール (サービスプレフィックス: cognito-idp) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Cognito ユーザープールで定義されるアクション
- Amazon Cognito ユーザープールで定義されるリソースタイプ
- Amazon Cognito ユーザープールの条件キー

Amazon Cognito ユーザープールで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AddCustomAttributes	ユーザー属性をユーザープールスキーマに追加するアクセス許可を付与	書き込み	userpool*		
AdminAddUserToGroup	ユーザーをグループに追加するアクセス許可を付与	書き込み	userpool*		
AdminConfirmSignUp	確認コードなしでユーザーの登録を確認するアクセス許可を付与	書き込み	userpool*		
AdminCreateUser	新しいユーザーを作成し、E メールまたは SMS でウェルカムメッセージを送信するアクセス許可を付与	書き込み	userpool*		
AdminDeleteUser	ユーザーを削除するアクセス許可を付与	書き込み	userpool*		
AdminDeleteUserAttributes	ユーザーから属性を削除するアクセス許可を付与	書き込み	userpool*		
AdminDisableProviderForUser	サードパーティーの ID プロバイダー (IdP) ユーザーからユーザープールのユーザーをリンク解除するアクセス許可を付与	書き込み	userpool*		
AdminDisableUser	ユーザーを非アクティブ化するアクセス許可を付与	書き込み	userpool*		
AdminEnableUser	ユーザーをアクティブ化するアクセス許可を付与	書き込み	userpool*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AdminForgetDevice	ユーザーのデバイスの登録を解除するアクセス許可を付与	書き込み	userpool*		
AdminGetDevice	ユーザーのデバイスに関する情報を取得するアクセス許可を付与	読み取り	userpool*		
AdminGetUser	ユーザーをユーザー名で検索するアクセス許可を付与	読み取り	userpool*		
AdminInitiateAuth	ユーザーを認証するアクセス許可を付与	書き込み	userpool*		
AdminLinkProviderForUser	ユーザープールのユーザーをサードパーティーの IdP ユーザーにリンクするアクセス許可を付与	書き込み	userpool*		
AdminListDevices	ユーザーの記憶したデバイスを一覧表示するアクセス許可を付与	リスト	userpool*		
AdminListGroupsForUser	ユーザーが属するグループを一覧表示するアクセス許可を付与	リスト	userpool*		
AdminListUserAuthEvents	ユーザーのサインインイベントを一覧表示するアクセス許可を付与	読み取り	userpool*		
AdminRemoveUserFromGroup	グループからユーザーを削除するアクセス許可を付与	書き込み	userpool*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AdminResetUserPassword	ユーザーのパスワードをリセットするアクセス許可を付与	書き込み	userpool*		
AdminRespondToAuthChallenge	ユーザーの認証中に認証チャレンジに応答するアクセス許可を付与	書き込み	userpool*		
AdminSetUserMFAPreference	ユーザーが優先する MFA メソッドを設定するアクセス許可を付与	書き込み	userpool*		
AdminSetUserPassword	ユーザーのパスワードを設定するアクセス許可を付与	書き込み	userpool*		
AdminSetUserSettings	ユーザーにユーザー設定を設定するアクセス許可を付与	書き込み	userpool*		
AdminUpdateAuthEventFeedback	ユーザーの認証イベントの高度なセキュリティフィードバックを更新するアクセス許可を付与	書き込み	userpool*		
AdminUpdateDeviceStatus	ユーザーの記憶したデバイスのステータスを更新するアクセス許可を付与	書き込み	userpool*		
AdminUpdateUserAttributes	ユーザーの標準属性またはカスタム属性を更新するアクセス許可を付与	書き込み	userpool*		
AdminUserGlobalSignOut	すべてのセッションからユーザーをサインアウトするアクセス許可を付与	書き込み	userpool*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateSoftwareToken	ユーザーの一意に生成された共有シークレットキーコードを返すアクセス許可を付与	書き込み			
AssociateWebACL [アクセス許可のみ]	ユーザープールを AWS WAF ウェブ ACL に関連付けるアクセス許可を付与します	書き込み	userpool*		
			webacl*		
ChangePassword	ユーザープールの指定されたユーザーのパスワードを変更するアクセス許可を付与	書き込み			
ConfirmDevice	デバイスの追跡を確認するアクセス許可を付与 この API コールによって、デバイス追跡が開始します。	書き込み			
ConfirmForgotPassword	忘れたパスワードをリセットする確認コードをユーザーが入力できるようにするアクセス許可を付与	書き込み			
ConfirmSignUp	ユーザーの登録を確認して、以前のユーザーの既存のエイリアスを処理するアクセス許可を付与	書き込み			
CreateGroup	新しいユーザープールグループを作成するアクセス許可を付与	書き込み	userpool*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateIdentityProvider	ID プロバイダーをユーザープールに追加するアクセス許可を付与	書き込み	userpool*		
CreateManagedLoginBranding	マネージドログインのブランド設定を作成し、アプリクライアントに関連付けるアクセス許可を付与します	書き込み	userpool*		
CreateResourceServer	OAuth 2.0 リソースサーバーのスコープを作成および設定するアクセス許可を付与	書き込み	userpool*		
CreateUserImportJob	ユーザー CSV インポートジョブを作成するアクセス許可を付与	書き込み	userpool*		
CreateUserPool	ユーザープールのパスワードポリシーを作成および設定するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateUserPoolClient	ユーザープールアプリケーションクライアントを作成するアクセス許可を付与	書き込み	userpool*		
CreateUserPoolDomain	ユーザープールドメインを追加するアクセス許可を付与	書き込み	userpool*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteGroup	空のユーザープールグループを削除するアクセス許可を付与	書き込み	userpool*		
DeleteIdentityProvider	ユーザープールから ID プロバイダーを削除するアクセス許可を付与	書き込み	userpool*		
DeleteManagedLoginBranding	任意のアプリケーションクライアントのマネージドログインブランドスタイルを削除するアクセス許可を付与します	書き込み	userpool*		
DeleteResourceServer	ユーザープールから OAuth 2.0 リソースサーバーを削除するアクセス許可を付与	書き込み	userpool*		
DeleteUser	ユーザーが自身を削除できるようにするアクセス許可を付与	書き込み			
DeleteUserAttributes	ユーザーの属性を削除するアクセス許可を付与	書き込み			
DeleteUserPool	ユーザープールを削除するアクセス許可を付与	書き込み	userpool*		
DeleteUserPoolClient	ユーザープールアプリケーションクライアントを削除するアクセス許可を付与	書き込み	userpool*		
DeleteUserPoolDomain	ユーザープールドメインを削除するアクセス許可を付与	書き込み	userpool*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeIdentityProvider	ユーザープール ID プロバイダーを記述するアクセス許可を付与	読み取り	userpool*		
DescribeManagedLoginBranding	マネージドログインのブランドスタイルに関する詳細情報を取得する許可を付与	読み取り	userpool*		
DescribeManagedLoginBrandingByClient	アプリケーションに関連付けられたマネージドログインのブランドスタイルに関する詳細情報を取得するアクセス許可を付与します	読み取り	userpool*		
DescribeResourceServer	OAuth 2.0 リソースサーバーを記述するアクセス許可を付与	読み取り	userpool*		
DescribeRiskConfiguration	ユーザープールとアプリケーションクライアントのリスク設定を記述するアクセス許可を付与	読み取り	userpool*		
DescribeUserImportJob	ユーザーインポートジョブを記述するアクセス許可を付与	読み取り	userpool*		
DescribeUserPool	ユーザープールを記述するアクセス許可を付与	読み取り	userpool*		
DescribeUserPoolClient	ユーザープールアプリケーションクライアントを記述するアクセス許可を付与	読み取り	userpool*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeUserPoolDomain	ユーザープールドメインを記述するアクセス許可を付与	読み取り			
DisassociateWebACL [許可のみ]	ユーザープールと AWS WAF ウェブ ACL の関連付けを解除するアクセス許可を付与します	書き込み	userpool*		
ForgetDevice	指定されたデバイスを忘れるアクセス許可を付与	書き込み			
ForgotPassword	ユーザーのパスワードを変更するために必要な確認コードと共にメッセージをエンドユーザーに送信するアクセス許可を付与	書き込み			
GetCSVHeader	ユーザーインポート .csv ファイルのヘッダーを生成するアクセス許可を付与	読み取り	userpool*		
GetDevice	デバイスを取得するアクセス許可を付与	読み取り			
GetGroup	ユーザープールグループを記述するアクセス許可を付与	読み取り	userpool*		
GetIdentityProviderByIdentifier	ユーザープール IdP 識別子を IdP 名に関連付けるアクセス許可を付与	読み取り	userpool*		
GetLogDeliveryConfiguration	ユーザープールの詳細なアクティビティログ設定を取得するアクセス許可を付与	読み取り	userpool*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetSigningCertificate	ユーザープールの署名証明書を検索するアクセス許可を付与	読み取り	userpool*		
GetTokensFromRefreshToken	更新トークンでユーザートークンを更新するアクセス許可を付与します	書き込み			
GetUICustomization	アプリケーションクライアントのホストされている UI の UI カスタマイズ情報を取得するアクセス許可を付与	読み取り	userpool*		
GetUser	ユーザー属性およびユーザーのメタデータを取得するアクセス許可を付与	読み取り			
GetUserAttributeVerificationCode	指定した属性名のユーザー属性検証コードを取得するアクセス許可を付与	読み取り			
GetUserPoolMfaConfig	ユーザープールの MFA 設定を検索するアクセス許可を付与	読み取り	userpool*		
GetWebACLForResource [許可のみ]	Amazon Cognito ユーザープールに関連付けられている AWS WAF ウェブ ACL を取得する許可を付与	読み取り	userpool*		
GlobalSignOut	すべてのデバイスからユーザーをサインアウトするアクセス許可を付与	書き込み			
InitiateAuth	認証フローを開始するアクセス許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListDevices	デバイスを一覧表示するアクセス許可を付与	リスト			
ListGroups	ユーザープール内のすべてのグループを一覧表示するアクセス許可を付与	リスト	userpool*		
ListIdentityProviders	ユーザープール内のすべての ID プロバイダーを一覧表示するアクセス許可を付与	リスト	userpool*		
ListResourceServers	ユーザープール内のすべてのリソースサーバーを一覧表示するアクセス許可を付与	リスト	userpool*		
ListResourcesForWebACL [許可のみ]	AWS WAF ウェブ ACL に関連付けられているユーザープールを一覧表示するアクセス許可を付与します	リスト	webacl*		
ListTagsForResource	Amazon Cognito ユーザープールに割り当てられているタグを一覧表示するアクセス許可を付与	リスト	userpool		
ListUserImportJobs	すべてのユーザーインポートジョブを一覧表示するアクセス許可を付与	リスト	userpool*		
ListUserPoolClients	ユーザープール内のすべてのアプリケーションクライアントを一覧表示するアクセス許可を付与	リスト	userpool*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListUserPools	すべてのユーザープールを一覧表示するアクセス許可を付与	リスト			
ListUsers	すべてのユーザープールのユーザーを一覧表示するアクセス許可を付与	リスト	userpool*		
ListUsersInGroup	グループ内のユーザーを一覧表示するアクセス許可を付与	リスト	userpool*		
ResendConfirmationCode	ユーザープールの特定のユーザーに確認 (登録の確認用) を再送信するアクセス許可を付与	書き込み			
RespondToAuthChallenge	認証チャレンジに応答するアクセス許可を付与	書き込み			
RevokeToken	指定した更新トークンによって生成されたすべてのアクセストークンを取り消すアクセス許可を付与	書き込み			
SetLogDeliveryConfiguration	ユーザープールの詳細なアクティビティログ記録設定をセットアップまたは変更するアクセス許可を付与	書き込み	userpool*		
SetRiskConfiguration	ユーザープールとアプリケーションクライアントのリスク設定をするアクセス許可を付与	書き込み	userpool*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SetUICustomization	アプリケーションクライアントのホストされた UI をカスタマイズするアクセス許可を付与	書き込み	userpool*		
SetUserMFAPreference	ユーザープールのユーザーの MFA 設定を行うアクセス許可を付与	書き込み			
SetUserPoolMfaConfig	ユーザープールの設定をするアクセス許可を付与	書き込み	userpool*		
SetUserSettings	多要素認証 (MFA) などのユーザー設定を行うアクセス許可を付与	書き込み			
SignUp	指定したユーザープールにユーザーを登録し、ユーザー名、パスワード、およびユーザー属性を作成するアクセス許可を付与	書き込み			
StartUserImportJob	ユーザーインポートジョブを開始するアクセス許可を付与	書き込み	userpool*		
StopUserImportJob	ユーザーインポートジョブを停止するアクセス許可を付与	書き込み	userpool*		
TagResource	ユーザープールにタグ付けするアクセス許可を付与	Tagging	userpool		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	ユーザープールからタグを削除するアクセス許可を付与	Tagging	userpool		
				aws:TagKeys	
UpdateAuthEventFeedback	ユーザー認証イベントのフィードバックを更新するアクセス許可を付与	書き込み	userpool*		
UpdateDeviceStatus	デバイスの状態を更新するアクセス許可を付与	書き込み			
UpdateGroup	グループの設定を更新するアクセス許可を付与	書き込み	userpool*		
UpdateIdentityProvider	ユーザープール IdP の設定を更新するアクセス許可を付与	書き込み	userpool*		
UpdateManagedLoginBranding	マネージドログインのブランド設定を更新する許可を付与	書き込み	userpool*		
UpdateResourceServer	OAuth 2.0 リソースサーバーの設定を更新するアクセス許可を付与	書き込み	userpool*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateUserAttributes	特定の属性の更新 (一度に 1 つ) をユーザーに許可するアクセス許可を付与	書き込み			
UpdateUserPool	ユーザープールの設定を更新するアクセス許可を付与	書き込み	userpool*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateUserPoolClient	ユーザープールクライアントを更新するアクセス許可を付与	書き込み	userpool*		
UpdateUserPoolDomain	カスタムドメインの証明書を置き換えるアクセス許可を付与	書き込み	userpool*		
VerifySoftwareToken	ユーザーの入力された TOTP コードを登録し、成功した場合は、ユーザーのソフトウェアトークン MFA ステータスを検証済みとしてマークするアクセス許可を付与	書き込み			
VerifyUserAttribute	1 回限りの検証コードを使用してユーザー属性を検証するアクセス許可を付与	書き込み			

Amazon Cognito ユーザープールで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
userpool	arn:${Partition}:cognito-idp:${Region}:${Account}:userpool/${UserPoolId}	aws:ResourceTag/${TagKey}
webacl	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}	

Amazon Cognito ユーザープールの条件キー

Amazon Cognito ユーザープールは、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエストに存在するキーによってアクセスをフィルタリングします	ArrayOfString

Amazon Comprehend のアクション、リソース、および条件キー

Amazon Comprehend (サービスプレフィックス: comprehend) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Comprehend で定義されるアクション
- Amazon Comprehend で定義されるリソースタイプ
- Amazon Comprehend の条件キー

Amazon Comprehend で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchDetectDominantLanguage	テキストドキュメントのリスト内で言語を検出する許可を付与	読み込み			
BatchDetectEntities	指定されたテキストドキュメントのリスト内で名前付きエンティティ (「人物」、「場所」、「位置」など) を検出する許可を付与	読み込み			
BatchDetectKeyPhrases	テキストドキュメントのリスト内で内容を最もよく表すフレーズを検出する許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchDetectSentiment	ドキュメントのリスト内でテキストの感情 (肯定的、否定的、中立、混在) を検出する許可を付与	読み込み			
BatchDetectSyntax	テキストドキュメントのリスト内で構文情報 (品詞、トークンなど) を検出する許可を付与	読み取り			
BatchDetectTargetedSentiment	指定されたテキストドキュメントのリスト内で特定のエンティティ (ブランドや製品など) に関連付けられた感情を検出するアクセス許可を付与	読み取り			
ClassifyDocument	以前に作成されたトレーニング済みカスタムモデルとエンドポイントを使用して、1 つのドキュメントをリアルタイムで分析するための新しいドキュメント分類リクエストを作成する許可を付与	読み込み	document-classifier-endpoint*		
ContainsPiiEntities	特定の文書内の個人識別可能情報をリアルタイムで分類するアクセス許可を付与	読み取り			
CreateDataset	フライホイール内に新しいデータセットを作成するための許可を付与します	書き込み	flywheel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDocumentClassifier	ドキュメントの分類に使用できる新しいドキュメント分類子を作成するアクセスを付与	書き込み	document-classifier*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
CreateEndpoint	以前にトレーニングされたカスタムモデルの同期推論用にモデル固有のエンドポイントを作成する許可を付与	書き込み	document-classifier*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			document-classifier-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys	
			entity-recognizer*		
			entity-recognizer-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys	
			flywheel		
CreateEntityRecognizer	送信されたファイルを使用してエンティティレコグナイザーを作成する許可を付与	書き込み	entity-recognizer*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateFlywheel	モデルバージョンのトレーニングに使用できる新しいフライホイールを作成するための許可を付与します	書き込み	flywheel*	aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:DataLakeKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			document-classifier		
			entity-recognizer		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteDocumentClassifier	以前に作成したドキュメント分類子を削除する許可を付与	書き込み	document-classifier*		
DeleteEndpoint	以前にトレーニングされたカスタムモデルの固有のエンドポイントを削除する許可を付与。モデルを削除するには、すべてのエンドポイントを削除する必要があります。	書き込み	document-classifier-endpoint*		
			entity-recognizer-endpoint*		
DeleteEntityRecognizer	送信されたエンティティレコグナイザーを削除するアクセスを付与	書き込み	entity-recognizer*		
DeleteFlywheel	フライホイールを削除するための許可を付与します	書き込み	flywheel*		
DeleteResourcePolicy	リソースからポリシーを削除する許可を付与	書き込み	document-classifier*		
			entity-recognizer*		
DescribeDataset	データセットに関連付けられたプロパティを取得するための許可を付与します	読み取り	flywheel-dataset*		
DescribeDocumentClassificationJob	ドキュメント分類ジョブに関連付けられたプロパティを取得する許可を付与	読み込み	document-classification-job*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeDocumentClassifier	ドキュメント分類子に関連付けられたプロパティを取得する許可を付与	読み込み	document-classifier*		
DescribeDominantLanguageDetectionJob	主要言語検出ジョブに関連付けられたプロパティを取得する許可を付与	読み込み	dominant-language-detection-job*		
DescribeEndpoint	特定のエンドポイントに関連付けられたプロパティを取得する許可を付与。このオペレーションを使用して、エンドポイントのステータスを取得します。	読み込み	document-classifier-endpoint*		
			entity-recognizer-endpoint*		
DescribeEntitiesDetectionJob	エンティティ検出ジョブに関連付けられたプロパティを取得する許可を付与	読み込み	entities-detection-job*		
DescribeEntityRecognizer	エンティティレコグナイザーに関する詳細 (ステータス、トレーニングデータを含む S3 バケット、レコグナイザーのメタデータ、メトリクスなど) を提供する許可を付与	読み込み	entity-recognizer*		
DescribeEventsDetectionJob	イベント検出ジョブに関連付けられたプロパティを取得するアクセス許可を付与	読み取り	events-detection-job*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeFlywheel	フライホイールに関連付けられたプロパティを取得するための許可を付与します	読み取り	flywheel*		
DescribeFlywheelIteration	フライホイールのフライホイールイテレーションに関連付けられたプロパティを取得するための許可を付与します	読み取り	flywheel*		
				comprehend:FlywheelIterationId	
DescribeKeyPhrasesDetectionJob	キーフレーズ検出ジョブに関連付けられたプロパティを取得する許可を付与	読み込み	key-phrases-detection-job*		
DescribePiiEntitiesDetectionJob	PII エンティティ検出ジョブに関連付けられたプロパティを取得する許可を付与	読み込み	pii-entities-detection-job*		
DescribeResourcePolicy	リソースに添付されたポリシーの読み取り許可を付与	読み込み	document-classifier*		
			entity-recognizer*		
DescribeSentimentDetectionJob	感情検出ジョブに関連付けられたプロパティを取得する許可を付与	読み込み	sentiment-detection-job*		
DescribeTargetedSentimentDetectionJob	対象の感情検出ジョブに関連付けられたプロパティを取得するアクセス許可を付与	読み込み	targeted-sentiment-detection-job*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeTopicsDetectionJob	トピック検出ジョブに関連付けられたプロパティを取得する許可を付与	読み込み	topics-detection-job*		
DetectDominantLanguage	テキスト内で言語を検出する許可を付与	読み込み			
DetectEntities	指定されたテキストドキュメント内で名前付きエンティティ (「人物」、「場所」、「位置」など) を検出する許可を付与	読み込み	entity-recognizer-endpoint		
DetectKeyPhrases	テキスト内で内容を最もよく表すフレーズを検出する許可を付与	読み込み			
DetectPiiEntities	指定されたテキストドキュメント内で個人を特定できる情報エンティティ (「名前」、「SSN」、「PIN」など) を検出する許可を付与	読み込み			
DetectSentiment	ドキュメント内でテキストの感情 (肯定的、否定的、中立、混在) を検出する許可を付与	読み込み			
DetectSyntax	テキストドキュメント内で構文情報 (品詞、トークンなど) を検出する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DetectTargetedSentiment	ドキュメント内で特定のエンティティ (ブランドや製品など) に関連付けられた感情を検出するアクセス許可を付与	読み取り			
DetectToxicContent	所定のテキストセグメントリスト内にある有害コンテンツを検出する許可を付与	読み取り			
ImportModel	トレーニング済みの Comprehend モデルをインポートするための許可を付与	書き込み	document-classifier*		
			entity-recognizer*		
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:ModelKmsKey	
ListDatasets	フライホイールに関連付けられたデータセットのリストを取得するための許可を付与します	読み取り	flywheel*		
ListDocumentClassificationJobs	送信したドキュメント分類ジョブのリストを取得する許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListDocumentClassifierSummaries	作成したドキュメント分類子の概要のリストを取得する許可を付与	読み込み			
ListDocumentClassifiers	作成したドキュメント分類子のリストを取得する許可を付与	読み込み			
ListDominantLanguageDetectionJobs	送信した主要言語検出ジョブのリストを取得する許可を付与	読み込み			
ListEndpoints	作成した既存のすべてのエンドポイントのリストを取得する許可を付与	読み込み			
ListEntitiesDetectionJobs	送信したエンティティ検出ジョブのリストを取得する許可を付与	読み込み			
ListEntityRecognizerSummaries	作成したドキュメント認識機能の概要のリストを取得する許可を付与	読み込み			
ListEntityRecognizers	作成したすべてのエンティティレコグナイザー (現在トレーニング中のレコグナイザーを含む) のプロパティのリストを取得する許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListEventsDetectionJobs	送信したイベント検出ジョブのリストを取得するアクセス許可を付与	読み取り			
ListFlywheelIterationHistory	フライホイールに関連付けられたイテレーションのリストを取得するための許可を付与します	読み取り	flywheel*		
ListFlywheels	作成したフライホイールのリストを取得するための許可を付与します	読み取り			
ListKeyPhrasesDetectionJobs	ユーザーによって送信されたキーフレーズ検出ジョブのリストを取得する許可を付与	読み込み			
ListPiiEntitiesDetectionJobs	送信した PII エンティティ検出ジョブのリストを取得する許可を付与	読み込み			
ListSentimentDetectionJobs	送信した感情検出ジョブのリストを取得する許可を付与	読み込み			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み込み	document-classification-job		
			document-classifier		
			document-classifier-endpoint		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			dominant-language-detection-job		
			entities-detection-job		
			entity-recognizer		
			entity-recognizer-endpoint		
			events-detection-job		
			flywheel		
			flywheel-dataset		
			key-phrases-detection-job		
			pii-entities-detection-job		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			sentiment-detection-job		
			targeted-sentiment-detection-job		
			topics-detection-job		
ListTargetedSentimentDetectionJobs	送信した対象の感情検出ジョブのリストを取得するアクセス許可を付与	読み込み			
ListTopicsDetectionJobs	送信したトピック検出ジョブのリストを取得する許可を付与	読み込み			
PutResourcePolicy	リソースにポリシーをアタッチする許可を付与	書き込み	document-classifier*		
			entity-recognizer*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartDocumentClassificationJob	非同期ドキュメント分類ジョブを開始する許可を付与	書き込み	document-classification-job*	aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			document-classifier		
			flywheel		
StartDominantLanguageDetectionJob	ドキュメントのコレクションに対して非同期主要言語検出ジョブを開始する許可を付与	書き込み	dominant-language-detection-job*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartEntitiesDetectionJob	ドキュメントのコレクションに対して非同期エンティティ検出ジョブを開始する許可を付与	書き込み	entities-detection-job*	aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			entity-recognizer		
			flywheel		
StartEventsDetectionJob	ドキュメントのコレクションに対して非同期イベント検出ジョブを開始する許可を付与	書き込み	events-detection-job*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:OutputKmsKey	
StartFlywheelIteration	フライホイールのフライホイールイテレーションを開始するための許可を付与します	書き込み	flywheel*		
StartKeyPhrasesDetectionJob	ドキュメントのコレクションに対する非同期キーフレーズ検出ジョブを開始する許可を付与	書き込み	key-phrases-detection-job*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StartPiiEntitiesDetectionJob	ドキュメントのコレクションに対する非同期 PII エンティティ検出ジョブを開始する許可を付与	書き込み	pii-entities-detection-job*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:OutputKmsKey	
StartSentimentDetectionJob	ドキュメントのコレクションに対する非同期感情検出ジョブを開始する許可を付与	書き込み	sentiment-detection-job*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StartTargetedSentimentDetectionJob	ドキュメントのコレクションに対する対象の非同期感情検出ジョブを開始するアクセス許可を付与	書き込み	targeted-sentiment-detection-job*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StartTopicsDetectionJob	非同期ジョブを開始し、ドキュメントのコレクション内で最も一般的なトピックと、各トピックに関連したフレーズを検出する許可を付与	書き込み	topics-detection-job*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StopDominantLanguageDetectionJob	主要言語検出ジョブを停止する許可を付与	書き込み	dominant-language-detection-job*		
StopEntitiesDetectionJob	エンティティ検出ジョブを停止する許可を付与	書き込み	entities-detection-job*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StopEventsDetectionJob	イベント検出ジョブを停止するアクセス許可を付与	書き込み	events-detection-job*		
StopKeyPhrasesDetectionJob	キーフレーズ検出ジョブを停止する許可を付与	書き込み	key-phrases-detection-job*		
StopPiiEntitiesDetectionJob	PII エンティティ検出ジョブを停止する許可を付与	書き込み	pii-entities-detection-job*		
StopSentimentDetectionJob	感情検出ジョブを停止する許可を付与	書き込み	sentiment-detection-job*		
StopTargetedSentimentDetectionJob	対象の感情検出ジョブを停止するアクセス許可を付与	書き込み	targeted-sentiment-detection-job*		
StopTrainingDocumentClassifier	以前に作成したドキュメント分類子トレーニングジョブを停止する許可を付与	書き込み	document-classifier*		
StopTrainingEntityRecognizer	以前に作成されたエンティティレコグナイザーのトレーニングジョブを停止する許可を付与	書き込み	entity-recognizer*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
TagResource	指定されたキーと値のペアでリソースにタグを付けるアクセス許可を付与	タグ付け	document-classification-job		
			document-classifier		
			document-classifier-endpoint		
			dominant-language-detection-job		
			entities-detection-job		
			entity-recognizer		
			entity-recognizer-endpoint		
			events-detection-job		
			flywheel		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			flywheel-dataset		
			key-phrases-detection-job		
			pii-entities-detection-job		
			sentiment-detection-job		
			targeted-sentiment-detection-job		
			topics-detection-job		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	指定されたキーでリソースのタグを削除する許可を付与	タグ付け	document-classification-job		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			document-classifier		
			document-classifier-endpoint		
			dominant-language-detection-job		
			entities-detection-job		
			entity-recognizer		
			entity-recognizer-endpoint		
			events-detection-job		
			flywheel		
			flywheel-dataset		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			key-phrases-detection-job		
			pii-entities-detection-job		
			sentiment-detection-job		
			targeted-sentiment-detection-job		
			topics-detection-job		
				aws:TagKeys	
UpdateEndpoint	指定されたエンドポイントに関する情報を更新する許可を付与	書き込み	document-classifier-endpoint*		
			entity-recognizer-endpoint*		
			flywheel		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateFlywheel	フライホイールの設定を更新するための許可を付与します	書き込み	flywheel*	comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			document-classifier		
			entity-recognizer		

Amazon Comprehend で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
targeted-sentiment-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:targeted-sentiment-detection-job/${JobId}	aws:ResourceTag/${TagKey}
document-classifier	arn:${Partition}:comprehend:${Region}:${Account}:document-classifier/${DocumentClassifierName}	aws:ResourceTag/${TagKey}
document-classifier-endpoint	arn:${Partition}:comprehend:${Region}:${Account}:document-classifier-endpoint/${DocumentClassifierEndpointName}	aws:ResourceTag/${TagKey}
entity-recognizer	arn:${Partition}:comprehend:${Region}:${Account}:entity-recognizer/${EntityRecognizerName}	aws:ResourceTag/${TagKey}
entity-recognizer-endpoint	arn:${Partition}:comprehend:${Region}:${Account}:entity-recognizer-endpoint/${EntityRecognizerEndpointName}	aws:ResourceTag/${TagKey}
dominant-language-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:dominant-language-detection-job/${JobId}	aws:ResourceTag/${TagKey}
entities-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:entities-detection-job/${JobId}	aws:ResourceTag/${TagKey}
pii-entities-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:pii-entities-detection-job/${JobId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
events-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:events-detection-job/${JobId}	aws:ResourceTag/${TagKey}
key-phrases-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:key-phrases-detection-job/${JobId}	aws:ResourceTag/${TagKey}
sentiment-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:sentiment-detection-job/${JobId}	aws:ResourceTag/${TagKey}
topics-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:topics-detection-job/${JobId}	aws:ResourceTag/${TagKey}
document-classification-job	arn:${Partition}:comprehend:${Region}:${Account}:document-classification-job/${JobId}	aws:ResourceTag/${TagKey}
flywheel	arn:${Partition}:comprehend:${Region}:${Account}:flywheel/${FlywheelName}	aws:ResourceTag/${TagKey}
flywheel-dataset	arn:${Partition}:comprehend:${Region}:${Account}:flywheel/${FlywheelName}/dataset/${DatasetName}	aws:ResourceTag/${TagKey}

Amazon Comprehend の条件キー

Amazon Comprehend では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リソース作成リクエストに含まれるタグ値を要求することで、アクセスをフィルタします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値を要求することで、アクセスをフィルタリングします	String
aws:TagKeys	リクエストに必須タグの存在を要求することで、アクセスをフィルタリングします	ArrayOfString
comprehend:DataLakeKmsKey	リクエスト内のフライホイールリソースに関連付けられた DataLake Kms Key によってアクセスをフィルタリングします	ARN
comprehend:FlywheelIterationId	フライホイールの特定の Iteration Id でアクセスをフィルタリングします	String
comprehend:ModelKmsKey	リクエスト内のリソースに関連付けられたモデル KMS キーによってアクセスをフィルタリングします。	ARN
comprehend:OutputKmsKey	リクエスト内のリソースに関連付けられた出力 KMS キーによってアクセスをフィルタリングします。	ARN
comprehend:VolumeKmsKey	リクエスト内のリソースに関連付けられたボリューム KMS キーによってアクセスをフィルタリングします。	ARN
comprehend:VpcSecurityGroupIds	リクエスト内のリソースに関連付けられたすべての VPC セキュリティグループ ID のリストによってアクセスをフィルタリングします	ArrayOfString

条件キー	説明	[Type] (タイプ)
comprehend:VpcSubnets	リクエスト内のリソースに関連付けられたすべての VPC サブネットのリストによってアクセスをフィルタリングします	ArrayOfString

Amazon Comprehend Medical のアクション、リソース、および条件キー

Amazon Comprehend Medical (サービスプレフィックス: comprehendmedical) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Comprehend Medical で定義されるアクション
- Amazon Comprehend Medical で定義されるリソースタイプ
- Amazon Comprehend Medical の条件キー

Amazon Comprehend Medical で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にア

クションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeEntitiesDetectionV2Job	送信した医療エンティティ検出ジョブのプロパティを記述する許可を付与	Read			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeICD10CMInferenceJob	送信した ICD-10-CM リンクジョブのプロパティを記述する許可を付与	Read			
DescribePHIDetectionJob	送信した PHI エンティティ検出ジョブのプロパティを記述する許可を付与	Read			
DescribeRxNormInferenceJob	送信した RxNorm リンクジョブのプロパティを記述する許可を付与	読み取り			
DescribeSNOMEDCTInferenceJob	送信した SNOMED-CT リンクジョブのプロパティを記述する許可を付与	読み取り			
DetectEntitiesV2	指定された医療機関、および特定のテキストドキュメント内のそれらの関係と特性を検出する許可を付与	Read			
DetectPHI	指定されたテキストドキュメント内の保護されるべき医療情報 (PHI) エンティティを検出する許可を付与	Read			
InferICD10CM	指定されたテキストドキュメント内の病状エンティティを検出し、ICD-10-CM コードにリンクする許可を付与	Read			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
InferRxNorm	指定されたテキストドキュメント内の薬剤エンティティを検出し、それを米国国立医学図書館の RxNorm データベースからの RxCUI 概念識別子にリンクする許可を付与	読み取り			
InferSNOMEDCT	指定されたテキストドキュメント内の病状、解剖学、検査、治療、およびプロシージャエンティティを検出し、SNOMED-CT コードにリンクする許可を付与	読み取り			
ListEntitiesDetectionV2Jobs	送信した医療エンティティ検出ジョブを一覧表示する許可を付与	Read			
ListICD10CMInferenceJobs	送信した ICD-10-CM リンクジョブを一覧表示する許可を付与	Read			
ListPHIDetectionJobs	送信した PHI エンティティ検出ジョブを一覧表示する許可を付与	Read			
ListRxNormInferenceJobs	送信した RxNorm リンクジョブを一覧表示する許可を付与	読み取り			
ListSNOMEDCTInferenceJobs	送信した SNOMED-CT リンクジョブを一覧表示する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartEntitiesDetectionV2Job	ドキュメントのコレクションに対して非同期医療エンティティ検出ジョブを開始する許可を付与	Write			
StartICD10CMInferenceJob	ドキュメントのコレクションに対して非同期 ICD-10-CM リンクジョブを開始する許可を付与	Write			
StartPHIDetectionJob	ドキュメントのコレクションに対して非同期 PHI エンティティ検出ジョブを開始する許可を付与	Write			
StartRxNormInferenceJob	ドキュメントのコレクションに対して非同期 RxNorm リンクジョブを開始する許可を付与	書き込み			
StartSNOMEDCTInferenceJob	ドキュメントのコレクションに対して非同期 SNOMED-CT リンクジョブを開始する許可を付与	書き込み			
StopEntitiesDetectionV2Job	エンティティ検出ジョブを停止する許可を付与	Write			
StopICD10CMInferenceJob	ICD-10-CM リンクジョブを停止する許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StopPHIDetectionJob	PHI エンティティ検出ジョブを停止する許可を付与	Write			
StopRxNormInferenceJob	RxNorm リンクジョブを停止する許可を付与	書き込み			
StopSNOMEDCTInferenceJob	SNOMED-CT リンクジョブを停止する許可を付与	書き込み			

Amazon Comprehend Medical で定義されるリソースタイプ

Amazon Comprehend Medical では、IAM ポリシーステートメントの `Resource` 要素でのリソース ARN の指定はサポートされていません。Amazon Comprehend Medical へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

Amazon Comprehend Medical の条件キー

Amazon Comprehend Medical では、IAM ポリシーの `Condition` 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

AWS Compute Optimizer のアクション、リソース、条件キー

AWS Compute Optimizer (サービスプレフィックス: `compute-optimizer`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Compute Optimizer で定義されるアクション
- AWS Compute Optimizer で定義されるリソースタイプ
- AWS Compute Optimizer の条件キー

AWS Compute Optimizer で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteRecommendationPreferences	レコメンデーション優先権を削除するアクセス許可を付与	書き込み		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups ec2:DescribeInstances rds:DescribeDBClusters

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					rds:DescribeDBInstances
DescribeRecommendationExportJobs	推奨事項エクスポートジョブのステータスを表示するアクセス許可を付与	リスト			
ExportAutoScalingGroupRecommendations	指定されたアカウントの autoscaling グループ推奨事項を S3 にエクスポートするアクセス許可を付与	Write			autoscaling:DescribeAutoScalingGroups compute-optimizer:GetAutoScalingGroupRecommendations
ExportEBSVolumeRecommendations	提供されたアカウントについての EBS ボリューム推奨事項を S3 にエクスポートする許可を付与	Write			compute-optimizer:GetEBSVolumeRecommendations ec2:DescribeVolumes

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ExportEC2InstanceRecommendations	提供されたアカウントについての EC2 インスタンス推奨事項を S3 にエクスポートするアクセス許可を付与	書き込み			compute-optimizer:GetEC2InstanceRecommendations ec2:DescribeInstances
ExportECSServiceRecommendations	提供されたアカウントについての EBS サービス推奨事項を S3 にエクスポートするアクセス許可を付与	書き込み			compute-optimizer:GetECSServiceRecommendations ecs:ListClusters ecs:ListServices
ExportIdleRecommendations	提供されたアカウントのアイドル状態のレコメンデーションを S3 にエクスポートするアクセス許可を付与します	書き込み			compute-optimizer:GetIdleRecommendations

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ExportLambdaFunctionRecommendations	提供されたアカウントについての Lambda 関数推奨事項を S3 にエクスポートする許可を付与	書き込み			compute-optimizer:GetLambdaFunctionRecommendations lambda:ListFunctions lambda:ListProvisionedConcurrencyConfigs
ExportLicenseRecommendations	提供されたアカウントについてのライセンス推奨事項を S3 にエクスポートするアクセス許可を付与します	書き込み			compute-optimizer:GetLicenseRecommendations ec2:DescribeInstances

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ExportRDSDatabaseRecommendations	提供されたアカウントについての RDS 推奨事項を S3 にエクスポートする許可を付与する	書き込み			compute-optimizer:GetRDSDatabaseRecommendations rds:DescribeDBClusters rds:DescribeDBInstances
GetAutoScalingGroupRecommendations	提供された autoscaling グループについての推奨事項を取得するアクセス許可を付与	リスト			autoscaling:DescribeAutoScalingGroups
GetEBSVolumeRecommendations	提供された EBS グループについての推奨事項を取得するアクセス許可を付与	リスト			ec2:DescribeVolumes
GetEC2InstanceRecommendations	提供された EC2 インスタンスについての推奨事項を取得するアクセス許可を付与	リスト			ec2:DescribeInstances
GetEC2RecommendationProjectedMetrics	指定したインスタンスについての推奨予測を取得するアクセス許可を付与	リスト			ec2:DescribeInstances

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetECSServiceRecommendationProjectedMetrics	指定した ECS サービスについての推奨予測メトリクスを取得するアクセス許可を付与	リスト			
GetECSServiceRecommendations	提供された EBS サービスについての推奨事項を取得するアクセス許可を付与	リスト			ecs:ListClusters ecs:ListServices

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetEffectiveRecommendationPreferences	有効な推奨設定を取得するアクセス許可を付与	読み取り	compute-optimizer:ResourceType		autoscaling:DescribeAutoScalingGroups autoscaling:DescribeAutoScalingInstances ec2:DescribeInstances rds:DescribeDBClusters rds:DescribeDBInstances
GetEnrollmentStatus	指定したアカウントの登録ステータスを取得するアクセス許可を付与	リスト			
GetEnrollmentStatusesForOrganization	組織のメンバーアカウントの登録ステータスを取得する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetIdleRecommendations	指定されたアカウントのアイドルレコメンデーションを取得するアクセス許可を付与します (複数可)	リスト			
GetLambdaFunctionRecommendations	提供された lambda 関数についての推奨事項を取得するアクセス許可を付与	リスト			lambda:ListFunctions lambda:ListProvisionedConcurrencyConfigs
GetLicenseRecommendations	指定したアカウントについてのライセンス推奨事項を取得するアクセス許可を付与します	リスト			ec2:DescribeInstances
GetRDSDatabaseRecommendationProjectedMetrics	指定したインスタンスについての推奨予測を取得するアクセス許可を付与	リスト			rds:DescribeDBClusters rds:DescribeDBInstances

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetRDSDatabaseRecommendations	指定したアカウントについての RDS 推奨事項を取得する許可を付与する	リスト			rds:DescribeDBClusters rds:DescribeDBInstances
GetRecommendationPreferences	レコメンデーションレポートを取得するアクセス許可を付与	読み取り		compute-optimizer:ResourceType	
GetRecommendationSummaries	指定したアカウントについての推奨概要の概要を取得するアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutRecommendationPreferences	レコメンデーション設定を設定するアクセス許可を付与	書き込み		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups autoscaling:DescribeAutoScalingInstances ec2:DescribeInstances rds:DescribeDBClusters rds:DescribeDBInstances
UpdateEnrollmentStatus	登録ステータスを更新するアクセス許可を付与	Write			

AWS Compute Optimizer で定義されるリソースタイプ

AWS Compute Optimizer は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Compute Optimizer へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Compute Optimizer の条件キー

AWS Compute Optimizer では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
compute-optimizer:ResourceType	リソース所有者の アカウント ID でアクセスをフィルタリングします	String

AWS Config のアクション、リソース、および条件キー

AWS Config (サービスプレフィックス: config) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Config で定義されるアクション
- AWS Config で定義されるリソースタイプ
- AWS Config の条件キー

AWS Config で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateResourceTypes	指定されたすべてのリソースタイプを設定レコーダーの RecordingGroup に追加するアクセス許可を付与し、記録時にそれらのリソースタイプを含めます	書き込み	ConfigurationRecorder*		
BatchGetAggregateResourceConfig	AWS Config アグリゲータに存在するリソースの現在の設定項目を返すアクセス許可を付与します	読み取り	ConfigurationAggregator*		
BatchGetResourceConfig	要求された 1 つまたは複数のリソースの現在の設定を返すアクセス許可を付与します	読み込み			
DeleteAggregationAuthorization	指定されたリージョン内の指定された設定アグリゲータアカウントに付与されているアクセス承認を削除します	書き込み	AggregationAuthorization*		
DeleteConfigRule	指定された Config AWS ルールとそのすべての評価結果を削除するアクセス許可を付与します	書き込み	ConfigRule*		
DeleteConfigurationAggregator	指定された設定アグリゲータとそのアグリゲータに関連付けられている集約データを削除する許可を付与	書き込み	ConfigurationAggregator*		
DeleteConfigurationRecorder	カスタマーマネージド設定レコーダーを削除するアクセス許可を付与します	書き込み	ConfigurationRecorder*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteConformancePack	指定されたコンフォーマンスパックと、そのコンフォーマンスパック内のすべての AWS Config ルールとすべての評価結果を削除するアクセス許可を付与します	書き込み	ConformancePack*		
DeleteDeliveryChannel	配信チャネルを削除する許可を付与	書き込み			
DeleteEvaluationResults	指定された Config ルールの評価結果を削除する許可を付与	書き込み	ConfigRule*		
DeleteOrganizationConfigRule	指定された組織設定ルールと、その組織内のすべてのメンバーアカウントの評価結果を削除する許可を付与	書き込み	OrganizationConfigRule*		
DeleteOrganizationConformancePack	指定された組織コンフォーマンスパックと、その組織内のすべてのメンバーアカウントの評価結果を削除する許可を付与	書き込み	OrganizationConformancePack*		
DeletePendingAggregationRequest	指定されたリージョン内の指定されたアグリゲータアカウントの保留中の権限リクエストを削除する許可を付与	書き込み			
DeleteRemediationConfiguration	修正設定を削除する許可を付与	書き込み	RemediationConfiguration*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteRemediationExceptions	特定の Config ルールの特定のリソースキーの 1 AWS つ以上の修復例外を削除するアクセス許可を付与します	書き込み			
DeleteResourceConfig	削除されたカスタムリソースの設定状態を記録する許可を付与	書き込み			
DeleteRetentionConfiguration	保持存設定を削除する許可を付与	書き込み			
DeleteServiceLinkedConfigurationRecorder	サービスにリンクされた設定レコーダーを削除するアクセス許可を付与します	書き込み	ConfigurationRecorder*		
				config:ConfigurationRecorderServicePrincipal	
DeleteStoredQuery	AWS アカウント 内の の保存されたクエリを削除するアクセス許可を付与します AWS リージョン	書き込み	StoredQuery*		
DeliverConfigSnapshot	指定された配信チャネルの Amazon S3 バケットへの設定スナップショットの配信をスケジュールする許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeAggregateComplianceByConfigRules	準拠および非準拠ルールのリソース数で準拠および非準拠ルールに返すアクセス許可を付与します	読み込み	ConfigurationAggregator*		
DescribeAggregateComplianceByConformancePacks	各コンフォーマンスパック内の準拠ルール数、非準拠ルール、および合計ルール数とともに、準拠および非準拠の準拠パックの一覧を返すアクセス許可を付与します。	読み込み	ConfigurationAggregator*		
DescribeAggregationAuthorizations	さまざまなアグリゲータアカウントおよびリージョンに付与された権限のリストを返すアクセス許可を付与します。	リスト			
DescribeComplianceByConfigRule	指定された Config AWS ルールが準拠しているかどうかを示すアクセス許可を付与します	読み取り			
DescribeComplianceByResource	指定された AWS リソースが準拠しているかどうかを示すアクセス許可を付与します	読み取り			
DescribeConfigRuleEvaluationStatus	各 AWS マネージド Config ルールのステータス情報を返すアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeConfigRules	Config AWS ルールの詳細を返すアクセス許可を付与します	リスト			
DescribeConfigurationAggregatorSourcesStatus	アグリゲータ内のソースのステータス情報を返すアクセス許可を付与します	読み込み	ConfigurationAggregator*		
DescribeConfigurationAggregators	1 つ以上の設定アグリゲータの詳細を返すアクセス許可を付与します。	リスト			
DescribeConfigurationRecorderStatus	指定された設定レコーダーの現在のステータスを返すアクセス許可を付与します。	読み込み	ConfigurationRecorder*		
				config:ConfigurationRecorderServicePrincipal	
DescribeConfigurationRecorders	指定された 1 つまたは複数の設定レコーダーの名前を返すアクセス許可を付与します	読み取り	ConfigurationRecorder*		
				config:ConfigurationRecorderServicePrincipal	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeConformancePackCompliance	そのコンフォーマンスパック内の各ルールのコンプライアンス情報を返すアクセス許可を付与します	読み込み	ConformancePack*		
DescribeConformancePackStatus	1 つまたは複数のコンフォーマンスパックの展開ステータスを提供する許可を付与	読み込み			
DescribeConformancePacks	1 つまたは複数のコンフォーマンスパックのリストを返すアクセス許可を付与します	リスト			
DescribeDeliveryChannelStatus	指定された配信チャネルの現在のステータスを返すアクセス許可を付与します	読み込み			
DescribeDeliveryChannels	指定された配信チャネルの詳細を返すアクセス許可を付与します。	リスト			
DescribeOrganizationConfigRuleStatuses	組織の設定ルールの展開状態を提供する許可を付与	読み込み			
DescribeOrganizationConfigRules	組織設定ルールのリストを返すアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeOrganizationConformancePackStatuses	組織のコンフォーマンスパックの展開ステータスを提供するためのアクセス許可を付与します	読み込み			
DescribeOrganizationConformancePacks	組織のコンフォーマンスパックのリストを返すアクセス許可を付与します	リスト			
DescribePendingAggregationRequests	保留中のすべてのアグリゲーションリクエストのリストを返すアクセス許可を付与します	リスト			
DescribeRemediationConfigurations	1 つまたは複数の修正設定の詳細を返すアクセス許可を付与します	リスト	RemediationConfiguration*		
DescribeRemediationExceptions	1 つまたは複数の修正例外の詳細を返すアクセス許可を付与します	リスト			
DescribeRemediationExecutionStatus	状態、タイムスタンプ、失敗したステップのエラーメッセージなど、一連のリソースに対する修正実行の詳細ビューを提供します	読み込み	RemediationConfiguration*		
DescribeRetentionConfigurations	1つ以上の保持設定の詳細を返すアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DisassociateResourceTypes	設定レコーダーの Recording Group から指定されたすべてのリソースタイプを削除するアクセス許可を付与し、記録時にこれらのリソースタイプを除外します	書き込み	ConfigurationRecorder*		
GetAggregateComplianceDetailsByConfigRule	ルール内の特定のリソースに対して指定された AWS Config ルールの評価結果を返すアクセス許可を付与します	読み取り	ConfigurationAggregator*		
GetAggregateConfigRuleComplianceSummary	アグリゲータ内の 1 つ以上のアカウントとリージョンに対する準拠ルールおよび非準拠ルールの数を返すアクセス許可を付与します	読み込み	ConfigurationAggregator*		
GetAggregateConformancePackComplianceSummary	アグリゲータ内の 1 つ以上のアカウントとリージョンに対する準拠コンフォーマンスパックおよび非準拠コンフォーマンスパックの数を返すアクセス許可を付与します。	読み取り	ConfigurationAggregator*		
GetAggregateDiscoveredResourceCounts	AWS Config アグリゲータに存在するアカウントとリージョン全体のリソース数を返すアクセス許可を付与します	読み取り	ConfigurationAggregator*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetAggregateResourceConfig	特定のソースアカウントとリージョンの特定のリソースに対してアグリゲートされた設定項目を返すアクセス許可を付与します	読み取り	ConfigurationAggregator*		
GetComplianceDetailsByConfigRule	指定された Config AWS ルールの評価結果を返すアクセス許可を付与します	読み取り	ConfigRule*		
GetComplianceDetailsByResource	指定された AWS リソースの評価結果を返すアクセス許可を付与します	読み取り			
GetComplianceSummaryByConfigRule	準拠および非準拠 AWS の Config ルールの数を返すアクセス許可を付与します。各ルールの最大数は 25 です。	読み取り			
GetComplianceSummaryByResourceType	準拠しているリソースの数と準拠していないリソースの数を返すアクセス許可を付与します	読み取り			
GetConformancePackComplianceDetails	コンフォーマンスパックによって監視されるすべての AWS リソースのコンフォーマンスパックのコンプライアンスの詳細を返すアクセス許可を付与します	読み取り	ConformancePack*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetConformancePackComplianceSummary	1 つまたは複数のコンフォーマンスパックに対するコンプライアンス概要を提供する許可を付与	読み取り	ConformancePack*		
GetCustomRulePolicy	AWS Config カスタムポリシールールのロジックを含むポリシー定義を返すアクセス許可を付与します	読み取り	ConfigRule*		
GetDiscoveredResourceCounts	リソースタイプ、各リソースタイプの数、および AWS Config がこのリージョンで について記録しているリソースの総数を返すアクセス許可を付与します AWS アカウント	読み取り			
GetOrganizationConfigRuleDetailedStatus	特定の組織設定ルールについて、組織内の各メンバーアカウントの詳細なステータスを返すアクセス許可を付与します	読み込み	OrganizationConfigRule*		
GetOrganizationConformancePackDetailedStatus	特定の組織コンフォーマンスパックについて、組織内の各メンバーアカウントの詳細なステータスを返すアクセス許可を付与します	読み取り	OrganizationConformancePack*		
GetOrganizationCustomRulePolicy	組織の AWS Config Custom Policy ルールのロジックを含むポリシー定義を返すアクセス許可を付与します	読み取り	OrganizationConfigRule*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetResourceConfigHistory	指定されたリソースの設定項目のリストを返すアクセス許可を付与します	読み取り			
GetResourceEvaluationSummary	特定のリソースの評価 ID のリソース評価の概要を返すアクセス許可を付与	読み取り			
GetStoredQuery	特定の保存されたクエリの詳細を返すアクセス許可を付与します	読み込み	StoredQuery*		
ListAggregateDiscoveredResources	リソースタイプを許容し、アカウントとリージョン全体で特定のリソースタイプについてアグリゲートされたリソース識別子を一覧表示する許可を付与	リスト	ConfigurationAggregator*		
ListConfigurationRecorders	AWS アカウント の の設定レコーダーの概要を一覧表示するアクセス許可を付与します AWS リージョン	リスト			
ListConformancePackComplianceScores	可能なルールとリソースの組み合わせの合計に対する、コンフォーマンスパック内の準拠ルールとリソースの組み合わせの数の割合を返す許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListDiscoveredResources	リソースタイプを受け入れ、そのタイプのリソースのリソース識別子のリストを返すアクセス許可を付与します	リスト			
ListResourceEvaluations	AWS アカウント の のリソース評価の概要を一覧表示するアクセス許可を付与します AWS リージョン	リスト			
ListStoredQueries	AWS アカウント 内の の保存されたクエリを一覧表示するアクセス許可を付与します AWS リージョン	リスト			
ListTagsForResource	Config AWS リソースのタグを一覧表示するアクセス許可を付与します	読み取り	AggregationAuthorization		
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			OrganizationConfigRule		
			OrganizationConformancePack		
			StoredQuery		
PutAggregationAuthorization	アグリゲータアカウントとリージョンに、ソースアカウントとリージョンからデータを収集する許可を付与	書き込み	AggregationAuthorization*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutConfigRule	AWS リソースが目的の設定に準拠しているかどうかを評価するための AWS Config ルールを追加または更新するアクセス許可を付与します	書き込み	ConfigRule*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutConfigurationAggregator	選択したソースアカウントとリージョンを使用して設定アグリゲータを作成および更新する許可を付与	書き込み	ConfigurationAggregator*		iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators
				aws:RequestTag/${TagKey} aws:TagKeys	
PutConfigurationRecorder	カスタマーマネージド設定レコーダーを作成または更新して、選択したリソース設定を記録するアクセス許可を付与します	書き込み	ConfigurationRecorder*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutConformancePack	コンフォーマンスパックを作成または更新する許可を付与	書き込み	ConformancePack*		iam:CreateServiceLinkedRole iam:PassRole s3:GetObject s3:ListBucket ssm:GetDocument
PutDeliveryChannel	Amazon S3 バケットおよび Amazon SNS トピックに設定情報を配信する配信チャネルオブジェクトを作成する許可を付与	書き込み			
PutEvaluations	AWS Lambda 関数が評価結果を Config AWS に配信するために使用するアクセス許可を付与します	書き込み			
PutExternalEvaluation	Config AWS に評価結果を配信するアクセス許可を付与します	書き込み	ConfigRule*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutOrganizationConfigRule	AWS リソースが目的の設定に準拠しているかどうかを評価する、組織全体の組織設定ルールを追加または更新するアクセス許可を付与します	書き込み	OrganizationConfigRule*		iam:CreateServiceLinkedRole iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutOrganizationConformancePack	AWS リソースが目的の設定に準拠しているかどうかを評価する、組織全体の組織コンフォーマンスパックを追加または更新するアクセス許可を付与します	書き込み	OrganizationConformancePack*		iam:CreateServiceLinkedRole iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators s3:GetObject
PutRemediationConfigurations	選択したターゲットまたはアクションを持つ特定の Config AWS ルールで修復設定を追加または更新するアクセス許可を付与します	書き込み	RemediationConfiguration*		iam:PassRole
PutRemediationExceptions	特定の Config AWS ルールの特定のリソースの修正例外を追加または更新するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutResourceConfig	リクエストで提供されたリソースの設定状態を記録する許可を付与	書き込み			
PutRetentionConfiguration	Config が履歴情報を保存する保持期間 (日数) AWS の詳細を使用して保持設定を作成および更新するアクセス許可を付与します	書き込み			
PutServiceLinkedConfigurationRecorder	リンクされたサービスの範囲内のリソース設定を記録する新しいサービスにリンクされた設定レコーダーを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys config:ConfigurationRecorderServicePrincipal	iam:CreateServiceLinkedRole iam:PassRole
PutStoredQuery	新しいクエリを保存する権限を付与するか、既存の保存されたクエリを更新する	書き込み	StoredQuery*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SelectAggregateResourceConfig	構造化クエリ言語 (SQL) SELECT コマンドとアグリゲータを受け入れて、複数のアカウントとリージョンの AWS リソースの設定状態をクエリするアクセス許可を付与し、対応する検索を実行し、プロパティに一致するリソース設定を返します	読み取り	ConfigurationAggregator*		
SelectResourceConfig	構造化クエリ言語 (SQL) の SELECT コマンドを受け入れ、対応する検索を実行し、プロパティに一致するリソース設定を返すアクセス許可を付与します	読み込み			
StartConfigRulesEvaluation	指定した Config ルールに対してリソースを評価する許可を付与	書き込み	ConfigRule*		
StartConfigurationRecorder	で記録するために選択した AWS リソースの設定の記録を開始するアクセス許可をカスタマーマネージド設定レコーダーに付与します AWS アカウント	書き込み	ConfigurationRecorder*		
StartRemediationExecution	最後の既知の修復設定に対して、指定された AWS Config ルールのオンデマンド修復を実行するアクセス許可を付与します	書き込み			iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartResourceEvaluation	アカウントの Config AWS ルールに対してリソースの詳細を評価するアクセス許可を付与します	書き込み			cloudformation:DescribeType
StopConfigurationRecorder	で記録するために選択した AWS リソースの設定の記録を停止するアクセス許可をカスタマーマネージド設定レコーダーに付与します AWS アカウント	書き込み	ConfigurationRecorder*		
TagResource	指定された resourceRN のリソースに指定されたタグを関連付けるアクセス許可を付与します	タグ付け	AggregationAuthorization		
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		
			OrganizationConfigRule		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			OrganizationConformancePack		
			StoredQuery		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	タグ付け	AggregationAuthorization		
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		
			OrganizationConfigRule		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			OrganizationConformancePack		
			StoredQuery		
				aws:TagKeys	

AWS Config で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
AggregationAuthorization	`arn:${Partition}:config:${Region}:${Account}:aggregation-authorization/${AggregatorAccount}/${AggregatorRegion}`	aws:ResourceTag/${TagKey}
ConfigurationAggregator	`arn:${Partition}:config:${Region}:${Account}:config-aggregator/${AggregatorId}`	aws:ResourceTag/${TagKey}
ConfigRule	`arn:${Partition}:config:${Region}:${Account}:config-rule/${ConfigRuleId}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
ConformancePack	arn:${Partition}:config:${Region}:${Account}:conformance-pack/${ConformancePackName}/${ConformancePackId}	aws:ResourceTag/${TagKey}
OrganizationConfigRule	arn:${Partition}:config:${Region}:${Account}:organization-config-rule/${OrganizationConfigRuleId}	aws:ResourceTag/${TagKey}
OrganizationConformancePack	arn:${Partition}:config:${Region}:${Account}:organization-conformance-pack/${OrganizationConformancePackId}	aws:ResourceTag/${TagKey}
RemediationConfiguration	arn:${Partition}:config:${Region}:${Account}:remediation-configuration/${RemediationConfigurationId}	
StoredQuery	arn:${Partition}:config:${Region}:${Account}:stored-query/${StoredQueryName}/${StoredQueryId}	aws:ResourceTag/${TagKey}
ConfigurationRecorder	arn:${Partition}:config:${Region}:${Account}:configuration-recorder/${RecorderName}/${RecorderId}	aws:ResourceTag/${TagKey}

AWS Config の条件キー

AWS Config は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	各タグの許可された値のセットでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値でアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内の必須タグの存在でアクセスをフィルタリングします	ArrayOfString
config:ConfigurationRecorderServicePrincipal	設定レコーダーのサービスプリンシパルでアクセスをフィルタリングします	String

Amazon Connect Cases のアクション、リソース、および条件キー

Amazon Connect Cases (サービスプレフィックス: cases) では、IAM アクセス許可ポリシーで使用できるように、次のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Connect Cases で定義されるアクション
- Amazon Connect Cases で定義されるリソースタイプ
- Amazon Connect Cases の条件キー

Amazon Connect Cases で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchGetCaseRule	ケースドメインのケースルールに関する情報を取得するアクセス許可を付与します	読み取り	CaseRule*		
			Domain*		
BatchGetField	ケースドメイン内のフィールドに関する情報を取得するアクセス許可を付与	読み取り	Domain*		
			Field*		
BatchPutFieldOptions	ケースドメイン内のフィールドオプションを更新するアクセス許可を付与	書き込み	Domain*		
			Field*		
CreateCase	ケースドメイン内にケースを作成するアクセス許可を付与	書き込み	Case*		
			Domain*		
			Field*		
			Template*		
				connect:UserArn	
CreateCaseRule	ケースドメインでケースルールを作成するアクセス許可を付与します	書き込み	CaseRule*		
			Domain*		
CreateDomain	新しいケースドメインを作成するアクセス許可を付与	書き込み			
CreateField	ケースドメイン内にフィールドを作成するアクセス許可を付与	書き込み	Domain*		
			Field*		
CreateLayout		書き込み	Domain*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	ケースドメイン内にレイアウトを作成するアクセス許可を付与		Layout*		
CreateRelatedItem	ケースドメイン内のケースに関連付けられた関連アイテムを作成するアクセス許可を付与	書き込み	Case*		
			Domain*		
			RelatedItem*		
				connect:UserArn	
CreateTemplate	ケースドメイン内にテンプレートを作成するアクセス許可を付与	書き込み	Domain*		
			Layout*		
			Template*		
DeleteCase	ケースドメインでケースを削除するアクセス許可を付与します	書き込み	Case*		
			Domain*		
DeleteCaseRule	ケースドメインのケースルールを削除するアクセス許可を付与します	書き込み	CaseRule*		
			Domain*		
DeleteDomain	ドメインを削除するための許可を付与します	書き込み	Domain*		
DeleteField	ケースドメイン内のフィールドを削除する許可を付与する	書き込み	Domain*		
			Field*		
DeleteLayout	ケースドメイン内のレイアウトを削除する許可を付与する	書き込み	Domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			Layout*		
DeleteRelatedItem	ケースドメインのケースに関連付けられた関連項目を削除するアクセス許可を付与します	書き込み	Case*		
			Domain*		
			RelatedItem*		
DeleteTemplate	ケースドメイン内のテンプレートを削除する許可を付与する	書き込み	Domain*		
			Template*		
GetCase	ケースドメイン内のケースに関する情報を取得するアクセス許可を付与	読み取り	Case*		
			Domain*		
			Field*		
GetCaseAuditEvents	ケースの監査履歴を表示する許可を付与する	読み取り	Case*		
			Domain*		
GetCaseEventConfiguration	ケースドメイン内のケースイベント設定に関する情報を取得するアクセス許可を付与	読み取り	Domain*		
GetDomain	ケースドメインに関する情報を取得するアクセス許可を付与	読み取り	Domain*		
GetLayout	ケースドメイン内のレイアウトに関する情報を取得するアクセス許可を付与	読み取り	Domain*		
			Layout*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetTemplate	ケースドメイン内のテンプレートに関する情報を取得するアクセス許可を付与	読み取り	Domain*		
			Template*		
ListCaseRules	ケースドメインのケースルールを一覧表示するアクセス許可を付与します	リスト	Domain*		
ListCasesForContact	ケースドメイン内の特定の連絡先のケースを一覧表示するアクセス許可を付与	リスト	Domain*		
ListDomains	aws アカウント内にあるすべてのドメインを一覧表示するための許可を付与します	リスト			
ListFieldOptions	ケースドメイン内の単一選択フィールドのフィールドオプションを一覧表示するアクセス許可を付与	リスト	Domain*		
			Field*		
ListFields	ケースドメイン内のフィールドを一覧表示するアクセス許可を付与	リスト	Domain*		
ListLayouts	ケースドメイン内のレイアウトを一覧表示するための許可を付与します	リスト	Domain*		
ListTagsForResource	指定されたリソースのタグを一覧表示するためのアクセス許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTemplates	ケースドメイン内のテンプレートを一覧表示するアクセス許可を付与	リスト	Domain*		
PutCaseEventConfiguration	ケースドメインにケースイベント設定を挿入または更新するアクセス許可を付与	書き込み	Domain*		
SearchCases	ケースドメイン内のケースを検索するアクセス許可を付与	読み取り	Domain*		
SearchRelatedItems	ケースドメイン内のケースに関連付けられている関連アイテムを検索するアクセス許可を付与	読み取り	Case*		
			Domain*		
TagResource	指定されたタグを指定されたリソースに追加するためのアクセス許可を付与	Tagging	Case		
			CaseRule		
			Domain		
			Field		
			Layout		
			RelatedItem		
			Template		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	指定されたリソースから指定されたタグを削除するためのアクセス許可を付与	Tagging	Case		
			CaseRule		
			Domain		
			Field		
			Layout		
			RelatedItem		
			Template		
				aws:TagKeys	
UpdateCase	ケースドメイン内のケースのフィールド値を更新するアクセス許可を付与	書き込み	Case*		
			Domain*		
			Field*		
				connect:UserArn	
UpdateCaseRule		書き込み	CaseRule*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	ケースドメインのケースルールを更新するアクセス許可を付与します		Domain*		
UpdateField	ケースドメイン内のフィールドを更新するアクセスを付与	書き込み	Domain*		
			Field*		
UpdateLayout	ケースドメイン内のレイアウトを更新するアクセス許可を付与	書き込み	Domain*		
			Layout*		
UpdateTemplate	ケースドメイン内のテンプレートを更新するアクセス許可を付与	書き込み	Domain*		
			Template*		

Amazon Connect Cases で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Case	`arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/case/${CaseId}`	aws:ResourceTag/${TagKey}
Domain	`arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
Field	arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/field/${FieldId}	aws:ResourceTag/${TagKey}
Layout	arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/layout/${LayoutId}	aws:ResourceTag/${TagKey}
RelatedItem	arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/case/${CaseId}/related-item/${RelatedItemId}	aws:ResourceTag/${TagKey}
Template	arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/template/${TemplateId}	aws:ResourceTag/${TagKey}
CaseRule	arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/case-rule/${CaseRuleId}	aws:ResourceTag/${TagKey}

Amazon Connect Cases の条件キー

Amazon Connect Cases では、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義しています。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストで渡されたタグによりアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグによりアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーによりアクセスをフィルタリングします	ArrayOfString
connect:UserArn	接続の UserArn でアクセスをフィルタリング	ARN

Amazon Connect Customer Profiles のアクション、リソース、および条件キー

Amazon Connect Customer Profiles (サービスプレフィックス: `profile`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Connect Customer Profiles で定義されるアクション
- Amazon Connect Customer Profiles で定義されるリソースタイプ
- Amazon Connect Customer Profiles の条件キー

Amazon Connect Customer Profiles で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddProfileKey	プロファイルキーを追加する権限を付与します	書き込み	domains*		
BatchGetCalculatedAttributeForProfile	ドメイン内の特定のプロファイル (複数可) の計算された属性を取得する許可を付与する	読み取り	calculated-attributes*		
			domains*		
BatchGetProfile	ドメイン内のプロファイルを取得する許可を付与する	読み取り	domains*		
CreateCalculatedAttributeDefinition	ドメイン内で計算属性の定義を作成する許可を付与	書き込み	calculated-attributes*	aws:RequestTag/${TagKey} aws:TagKeys	
			domains*		
CreateDomain	ドメインを作成する権限を付与します	書き込み	domains*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole
CreateDomainLayout	ドメインにレイアウトを作成するアクセス許可を付与します	書き込み	domains*		
			layouts*	aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
CreateEventStream	ドメイン内にイベントストリームを配置する許可を付与	書き込み	domains*		iam:PutRolePolicy kinesis:DescribeStreamSummary
			event-streams*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventTrigger	ドメインにイベントトリガーを作成するアクセス許可を付与します	書き込み	domains*		
			event-triggers*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateIntegrationWorkflow	ドメイン内で統合ワークフローを作成する許可を付与	書き込み	domains*		
			integrations*	aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateProfile	ドメイン内にプロファイルを作成する権限を付与します	書き込み	domains*		
CreateSegmentDefinition	ドメインでセグメント定義を作成する許可を付与する	書き込み	domains*		
			segment-definitions*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateSegmentEstimate	ドメインでセグメント見積りを作成する許可を付与する	書き込み	domains*		
CreateSegmentSnapshot	ドメインでセグメントスナップショットを作成する許可を付与する	書き込み	domains*		
			segment-definitions*		
CreateSnapshot [アクセス許可のみ]	ドメインでスナップショットを作成する許可を付与する	書き込み	domains*		
CreateUploadJob	ドメインでアップロードジョブを作成するアクセス許可を付与します	書き込み	domains*		
DeleteCalculatedAttributeDefinition	ドメイン内の計算属性の定義を削除する許可を付与	書き込み	calculated-attributes*		
			domains*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteDomain	ドメインを削除する許可を付与	書き込み	domains*		
DeleteDomainLayout	ドメイン内のレイアウトを削除するアクセス許可を付与します	書き込み	domains*		
			layouts*		
DeleteEventStream	ドメイン内のイベントストリームを削除する許可を付与	書き込み	domains*		iam:DeleteRolePolicy
			event-streams*		
DeleteEventTrigger	ドメイン内のイベントトリガーを削除するアクセス許可を付与します	書き込み	domains*		
			event-triggers*		
DeleteIntegration	ドメイン内の統合を削除する権限を付与します	書き込み	domains*		
			integrations*		
DeleteProfile	プロファイルを削除する権限を付与します	書き込み	domains*		
DeleteProfileKey	プロファイルキーを削除する権限を付与します	書き込み	domains*		
DeleteProfileObject	プロファイルオブジェクトを削除する権限を付与します	書き込み	domains*		
			object-types*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteProfileObjectType	ドメイン内の特定のプロファイルオブジェクトタイプを削除する権限を付与します	書き込み	domains*		
			object-types*		
DeleteSegmentDefinition	ドメインのセグメント定義を削除する許可を付与する	書き込み	domains*		
			segment-definitions*		
DeleteWorkflow	ドメイン内で統合ワークフローを削除する許可を付与	書き込み	domains*		
DetectProfileObjectType	オブジェクトタイプを自動検出するためのアクセス許可を付与	読み取り	domains*		
GetAutoMergingPreview	ドメイン内の自動マージのプレビューを取得するアクセス許可を付与します	読み取り	domains*		
GetCalculatedAttributeDefinition	ドメイン内の計算属性の定義を取得する許可を付与	読み取り	calculated-attributes*		
			domains*		
GetCalculatedAttributeForProfile	ドメイン内の特定のプロファイルの計算された属性を取得する許可を付与	読み取り	calculated-attributes*		
			domains*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetDomain	アカウント内の特定のドメインを取得する権限を付与します	読み取り	domains*		
GetDomainLayout	ドメインでレイアウトを取得するアクセス許可を付与します	読み取り	domains*		
			layouts*		
GetEventStream	ドメイン内の特定のイベントストリームを取得する許可を付与	読み取り	domains*		kinesis:DescribeStreamSummary
			event-streams*		
GetEventTrigger	ドメインでイベントトリガーを取得するアクセス許可を付与します	読み取り	domains*		
			event-triggers*		
GetIdentityResolutionJob	ドメイン内の ID 解決ジョブを取得するアクセス許可を付与します	読み込み	domains*		
GetIntegration	ドメイン内にある特定の統合を取得する権限を付与します	読み込み	domains*		
			integrations*		
GetMatches	プロファイル一致を取得する許可を付与	リスト	domains*		
GetProfileObjectType		読み込み	domains*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	ドメイン内の特定のプロファイルオブジェクトタイプを取得する権限を付与します		object-types*		
GetProfileObjectTypeTemplate	特定のオブジェクトタイプテンプレートを取得する権限を付与します	読み取り			
GetSegmentDefinition	ドメインのセグメント定義を取得する許可を付与する	読み取り	domains*		
			segment-definitions*		
GetSegmentEstimate	ドメインでセグメント見積りを取得する許可を付与する	読み取り	domains*		
GetSegmentMembership	特定のプロファイルがドメイン内のセグメントの一部であるかどうかを決定する許可を付与する	読み取り	domains*		
			segment-definitions*		
GetSegmentSnapshot	ドメインでセグメントスナップショットを取得する許可を付与する	読み取り	domains*		
			segment-definitions*		
GetSimilarProfiles	ドメイン内のすべての類似のプロファイルを取得するための許可を付与します	リスト	domains*		
GetSnapshot [許可のみ]	ドメインでスナップショットを取得する許可を付与する	読み取り	domains*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetUploadJob	ドメイン内のアップロードジョブの詳細を取得するアクセス許可を付与します	読み取り	domains*		
GetUploadJobPath	アップロードジョブのファイルをアップロードするための署名付き URL を取得する許可を付与	読み取り	domains*		
GetWorkflow	ドメイン内のワークフロー詳細を取得する許可を付与	読み込み	domains*		
GetWorkflowSteps	ワークフローステップの詳細を取得する許可を付与	読み込み	domains*		
ListAccountIntegrations	アカウント内にあるすべての統合を一覧表示する権限を付与します	リスト			
ListCalculatedAttributeDefinitions	ドメイン内のすべての計算属性の定義を一覧表示する許可を付与	リスト	domains*		
ListCalculatedAttributesForProfile	ドメイン内の特定のプロファイルの計算属性を一覧表示する許可を付与	リスト	domains*		
ListDomainLayouts	ドメイン内のすべてのレイアウトを一覧表示するアクセス許可を付与します	リスト	domains*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListDomains	アカウント内にあるすべてのドメインを一覧表示する権限を付与します	リスト			
ListEventStreams	特定のドメイン内のすべてのイベントストリームを一覧表示する許可を付与	リスト	domains*		
ListEventTriggers	ドメイン内のすべてのイベントトリガーを一覧表示するアクセス許可を付与します	リスト	domains*		
ListIdentityResolutionJobs	ドメイン内の ID 解決ジョブを一覧表示するアクセス許可を付与します	リスト	domains*		
ListIntegrations	特定のドメイン内にあるすべての統合を一覧表示する権限を付与します	リスト	domains*		
ListObjectTypeAttributes	ドメイン内の特定のオブジェクトタイプのすべての属性を一覧表示する許可を付与する	リスト	domains* object-types*		
ListProfileAttributeValues	ドメイン内のプロファイル属性のすべての値を一覧表示する許可を付与する	リスト	domains*		
ListProfileObjectTypeTemplates	アカウント内にあるすべてのプロファイルオブジェクトタイプテンプレートを一覧表示する権限を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListProfileObjectTypes	ドメイン内にあるすべてのプロファイルオブジェクトタイプを一覧表示する権限を付与します	リスト	domains*		
ListProfileObjects	プロファイルのすべてのプロファイルオブジェクトを一覧表示する権限を付与します	リスト	domains*		
			object-types*		
ListRuleBasedMatches	ドメイン内のすべてのルールベースのマッチングの結果を一覧表示するための許可を付与します	リスト	domains*		
ListSegmentDefinitions	ドメインですべてのセグメント定義を一覧表示する許可を付与する	リスト	domains*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	calculated-attributes		
			domains		
			event-streams		
			event-triggers		
			integrations		
			layouts		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			object-types		
			segment-definitions		
ListUploadJobs	ドメイン内のすべてのアップロードジョブを一覧表示するアクセス許可を付与します	リスト	domains*		
ListWorkflows	特定のドメイン内にあるすべてのワークフローを一覧表示する許可を付与	リスト	domains*		
MergeProfiles	プロファイルをマージする許可を付与	書き込み	domains*		
PutIntegration	ドメイン内に統合を配置する権限を付与します	書き込み	domains*		
			integrations*	aws:RequestTag/${TagKey} aws:TagKeys	
PutProfileObject	プロファイルにオブジェクトを配置する権限を付与します	書き込み	domains*		
			object-types*		
PutProfileObjectType	ドメイン内に特定のプロファイルオブジェクトを配置する権限を付与します	書き込み	domains*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			object-types*	aws:RequestTag/${TagKey} aws:TagKeys	
SearchProfiles	ドメイン内のプロファイルを検索する権限を付与します	読み取り	domains*		
StartUploadJob	ドメインでアップロードジョブを開始するアクセス許可を付与します	書き込み	domains*		
StopUploadJob	ドメイン内のアップロードジョブを停止するアクセス許可を付与します	書き込み	domains*		
TagResource	リソースにタグを追加するアクセス許可を付与	タグ付け	calculated-attributes		
			domains		
			event-streams		
			event-triggers		
			integrations		
			layouts		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			object-types		
			segment-definitions		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	Tagging	calculated-attributes		
			domains		
			event-streams		
			event-triggers		
			integrations		
			layouts		
			object-types		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			segment-definitions		
				aws:TagKeys	
UpdateCalculatedAttributeDefinition	ドメイン内の計算属性の定義を更新する許可を付与	書き込み	calculated-attributes*		
			domains*		
UpdateDomain	ドメインを更新する許可を付与	書き込み	domains*		iam:CreateServiceLinkedRole
UpdateDomainLayout	ドメインのレイアウトを更新するアクセス許可を付与します	書き込み	domains*		
			layouts*		
UpdateEventTrigger	ドメインのイベントトリガーを更新するアクセス許可を付与します	書き込み	domains*		
			event-triggers*		
UpdateProfile	ドメイン内のプロファイルを更新する権限を付与します	書き込み	domains*		

Amazon Connect Customer Profiles で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
domains	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}	aws:ResourceTag/${TagKey}
object-types	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/object-types/${ObjectTypeName}	aws:ResourceTag/${TagKey}
integrations	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/integrations/${Uri}	aws:ResourceTag/${TagKey}
event-streams	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/event-streams/${EventStreamName}	aws:ResourceTag/${TagKey}
calculated-attributes	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/calculated-attributes/${CalculatedAttributeName}	aws:ResourceTag/${TagKey}
segment-definitions	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/segment-definitions/${SegmentDefinitionName}	aws:ResourceTag/${TagKey}
event-triggers	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/event-triggers/${EventTriggerName}	aws:ResourceTag/${TagKey}
layouts	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/layouts/${LayoutDefinitionName}	aws:ResourceTag/${TagKey}

Amazon Connect Customer Profiles の条件キー

Amazon Connect Customer Profiles では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	ユーザーが顧客プロファイルサービスに対して行うリクエストに含まれるキーによってアクセスがフィルタリングされます	String
aws:ResourceTag/${TagKey}	タグキーおよび値のペアでアクセスをフィルタリングします。	String
aws:TagKeys	ユーザーが顧客プロファイルサービスに対して行うリクエストに含まれるすべてのタグキー名のリストでアクセスをフィルタリングします	ArrayOfString

Amazon Connect アウトバウンドキャンペーンのアクション、リソース、および条件キー

Amazon Connect アウトバウンドキャンペーン (サービスプレフィックス: connect-campaigns) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Connect アウトバウンドキャンペーンで定義されるアクション
- Amazon Connect アウトバウンドキャンペーンで定義されるリソースタイプ
- Amazon Connect アウトバウンドキャンペーンの条件キー

Amazon Connect アウトバウンドキャンペーンで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateCampaign	キャンペーンを作成する許可を付与	書き込み	campaign*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteCampaign	キャンペーンを削除する許可を付与	書き込み	campaign*		
DeleteCampaignChannelSubtypeConfig	キャンペーンのチャネルサブタイプ設定を削除するアクセス許可を付与します	書き込み	campaign*		
DeleteCampaignCommunicationLimits	キャンペーンの通信制限設定を削除するアクセス許可を付与します	書き込み	campaign*		
DeleteCampaignComm	キャンペーンの通信時間設定を削除するアクセス許可を付与します	書き込み	campaign*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
unication Time					
DeleteConnectInstanceConfig	Amazon Connect インスタンスの設定情報を削除する許可を付与	書き込み			
DeleteConnectInstanceIntegration	Amazon Connect インスタンスの統合情報を削除するアクセス許可を付与します	書き込み			
DeleteInstanceOnboardingJob	Amazon Connect インスタンスのオンボーディングジョブを削除する許可を付与	書き込み			
DescribeCampaign	特定のキャンペーンを記述する許可を付与	読み取り	campaign*		
				aws:RequestTag/${TagKey}	
GetCampaignState	1 つのキャンペーンの状態を取得する許可を付与	読み取り	campaign*		
				aws:RequestTag/${TagKey}	
GetCampaignStateBatch	複数のキャンペーンの状態を取得する許可を付与	読み取り	campaign*		
				aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetConnectInstanceConfig	Amazon Connect インスタンスの設定情報を取得する許可を付与	読み取り			
GetInstanceCommunicationLimits	Amazon Connect インスタンスの通信制限設定を取得する許可を付与	読み取り			
GetInstanceOnboardingJobStatus	Amazon Connect インスタンスのオンボーディングジョブステータスを取得する許可を付与	読み取り			
ListCampaigns	すべてのキャンペーンの概要を提供する許可を付与	リスト		aws:RequestTag/${TagKey}	
ListConnectInstanceIntegrations	Amazon Connect インスタンスとのすべての統合の概要を提供するアクセス許可を付与します	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	campaign		
				aws:ResourceTag/${TagKey}	
PauseCampaign	キャンペーンを一時停止する許可を付与	書き込み	campaign*		
PutConnectInstanceIntegration	Amazon Connect インスタンスとの統合設定を配置するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutDialRequestBatch	指定したキャンペーンのダイヤルリクエストを作成する許可を付与	書き込み	campaign*		
PutInstanceCommunicationLimits	Amazon Connect インスタンスの通信制限設定を配置するアクセス許可を付与します	書き込み			
PutOutboundRequestBatch	指定したキャンペーンのダイヤルリクエストを作成する許可を付与	書き込み	campaign*		
PutProfileOutboundRequestBatch	指定されたキャンペーンのプロファイルアウトバウンドリクエストを作成するアクセス許可を付与します	書き込み	campaign*		
ResumeCampaign	キャンペーンを再開する許可を付与	書き込み	campaign*		
StartCampaign	キャンペーンを開始する許可を付与	書き込み	campaign*		
StartInstanceOnboardingJob	Amazon Connect インスタンスのオンボーディングジョブを開始する許可を付与	書き込み			
StopCampaign	キャンペーンを停止する許可を付与	書き込み	campaign*		
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	campaign*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	リソースのタグを解除する許可を付与	Tagging	campaign*		
				aws:TagKeys	
UpdateCampaignChannelSubtypeConfig	キャンペーンのチャネルサブタイプ設定を更新する許可を付与	書き込み	campaign*		
UpdateCampaignCommunicationLimits	キャンペーンの通信制限設定を更新するアクセス許可を付与します	書き込み	campaign*		
UpdateCampaignCommunicationTime	キャンペーンの通信時間設定を更新する許可を付与	書き込み	campaign*		
UpdateCampaignDialerConfig	キャンペーンのダイヤラー設定を更新する許可を付与	書き込み	campaign*		
UpdateCampaignFlowAssociation	キャンペーンのフロー関連付けを更新するアクセス許可を付与します	書き込み	campaign*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateCampaignName	キャンペーンの名前を更新する許可を付与	書き込み	campaign*		
UpdateCampaignOutboundCallConfig	キャンペーンの発信通話設定を更新する許可を付与	書き込み	campaign*		
UpdateCampaignSchedule	キャンペーンのスケジュールを更新するアクセス許可を付与します	書き込み	campaign*		
UpdateCampaignSource	キャンペーンのソースを更新するアクセス許可を付与します	書き込み	campaign*		

Amazon Connect アウトバウンドキャンペーンで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
campaign	`arn:${Partition}:connect-campaigns:${Region}:${Account}:campaign/${CampaignId}`	aws:ResourceTag/${TagKey}

Amazon Connect アウトバウンドキャンペーンの条件キー

Amazon Connect アウトバウンドキャンペーンでは、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーおよび値のペアのプレゼンスに基づいてアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアに基づいてアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいたアクションでアクセスをフィルタリングします	ArrayOfString

Amazon Connect Voice ID のアクション、リソース、および条件キー

Amazon Connect Voice ID (サービスプレフィックス: voiceid) では、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されており、IAM アクセス許可ポリシーでの使用が可能です。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Connect Voice ID で定義されているアクション

- Amazon Connect Voice ID で定義されるリソースタイプ
- Amazon Connect Voice ID の条件キー

Amazon Connect Voice ID で定義されているアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateFraudster	不正行為者をウォッチリストに関連付けるための許可を付与します	書き込み	domain*		
CreateDomain	ドメインを作成するためのアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWatchlist	ウォッチリストを作成するための許可を付与します	書き込み	domain*		
DeleteDomain	ドメインを削除する許可を付与	書き込み	domain*		
DeleteFraudster	フロードスター (fraudster) を削除するためのアクセス許可を付与	書き込み	domain*		
DeleteSpeaker	スピーカを削除するためのアクセス許可を付与	書き込み	domain*		
DeleteWatchlist	ウォッチリストを削除するための許可を付与します	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeComplianceConsent [アクセス許可のみ]	コンプライアンスの同意を詳細表示するためのアクセス許可を付与	読み取り			
DescribeDomain	ドメインについて詳細表示するためのアクセス許可を付与	読み取り	domain*		
DescribeFraudster	フロードスター (fraudster) について詳細表示するためのアクセス許可を付与	読み取り	domain*		
DescribeFraudsterRegistrationJob	フロードスター (fraudster) 登録ジョブについて詳細表示するためのアクセス許可を付与	読み取り	domain*		
DescribeSpeaker	スピーカについて詳細表示するためのアクセス許可を付与	読み取り	domain*		
DescribeSpeakerEnrollmentJob	スピーカ登録ジョブを記述するためのアクセス許可を付与	読み取り	domain*		
DescribeWatchlist	ウォッチリストを記述するための許可を付与します	読み取り	domain*		
DisassociateFraudster	ウォッチリストから不正行為者の関連付けを解除するための許可を付与します	書き込み	domain*		
EvaluateSession	セッションを評価するためのアクセス許可を付与	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListDomains	アカウント内のドメインを一覧表示するためのアクセス許可を付与	リスト			
ListFraudsterRegistrationJobs	ドメインのフロードスター (fraudster) 登録ジョブを一覧表示するためのアクセス許可を付与	リスト	domain*		
ListFraudsters	ドメインまたはウォッチリストの不正行為者を一覧表示するための許可を付与します	リスト	domain*		
ListSpeakerEnrollmentJobs	ドメインのスピーカ登録ジョブを一覧表示するためのアクセス許可を付与	リスト	domain*		
ListSpeakers	ドメインのスピーカを一覧表示するためのアクセス許可を付与	リスト	domain*		
ListTagsForResource	Voice ID リソースのタグを一覧表示するためのアクセス許可を付与	読み取り	domain		
ListWatchlists	ドメインのウォッチリストを一覧表示するための許可を付与します	リスト	domain*		
OptOutSpeaker	スピーカをオプトアウトするためのアクセス許可を付与	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RegisterComplianceConsent [アクセス許可のみ]	コンプライアンス同意を登録するためのアクセス許可を付与	書き込み			
StartFraudsterRegistrationJob	フロードスター (fraudster) の登録ジョブを開始するためのアクセス許可を付与	書き込み	domain*		
StartSpeakerEnrollmentJob	スピーカの登録ジョブを開始するためのアクセス許可を付与	書き込み	domain*		
TagResource	Voice ID リソースにタグ付けするためのアクセス許可を付与	Tagging	domain		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Voice ID リソースからタグを削除するためのアクセス許可を付与	Tagging	domain		
				aws:TagKeys	
UpdateDomain	ドメインを更新するためのアクセス許可を付与	書き込み	domain*		
UpdateWatchlist	ウォッチリストを更新するための許可を付与します	書き込み	domain*		

Amazon Connect Voice ID で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
domain	arn:${Partition}:voiceid:${Region}:${Account}:domain/${DomainId}	aws:ResourceTag/${TagKey}

Amazon Connect Voice ID の条件キー

Amazon Connect Voice ID では、IAM ポリシーの Condition 要素で使用できる、以下の条件キーを定義しています。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストで渡されたタグによりアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグによりアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーによりアクセスをフィルタリングします	ArrayOfString

AWS Connector Service のアクション、リソース、および条件キー

AWS Connector Service (サービスプレフィックス: awsconnector) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Connector Service で定義されるアクション
- AWS Connector Service で定義されるリソースタイプ
- AWS Connector Service の条件キー

AWS Connector Service で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetConnectorHealth [アクセス許可のみ]	Server Migration Connector から公開済みのすべてのヘルスメトリクスを取得します。	Read			
RegisterConnector [許可のみ]	AWS Connector を AWS Connector Service に登録します。	書き込み			
ValidateConnectorId	AWS Connector Service に登録されたサーバー移行コネクタ ID を検証します。	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
[アクセス許可のみ]					

AWS Connector Service で定義されるリソースタイプ

AWS Connector Service は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Connector Service へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Connector Service の条件キー

Connector Service には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Management Console Mobile App のアクション、リソース、および条件キー

AWS Management Console モバイルアプリ (サービスプレフィックス: `consoleapp`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Management Console Mobile App で定義されるアクション
- AWS Management Console Mobile App で定義されるリソースタイプ

- AWS Management Console Mobile App の条件キー

AWS Management Console Mobile App で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetDeviceIdentity	コンソールモバイルアプリケーションデバイスのデバイス ID を取得するアクセス許可を付与します	読み取り	DeviceIdentity*		
ListDeviceIdentities	デバイス ID のリストを取得するアクセス許可を付与します	リスト			

AWS Management Console Mobile App で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
DeviceIdentity	`arn:${Partition}:consoleapp::${Account}:device/${DeviceId}/identity/${IdentityId}`	

AWS Management Console Mobile App の条件キー

Console Mobile App には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS 一括請求のアクション、リソース、および条件キー

AWS 一括請求 (サービスプレフィックス: consolidatedbilling) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS 一括請求で定義されるアクション
- AWS 一括請求で定義されるリソースタイプ
- AWS 一括請求の条件キー

AWS 一括請求で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetAccountBillingRole [アクセス許可のみ]	アカウントロール (支払人、リンク済み、レギュラー) を取得するアクセス許可を付与	読み取り			
ListLinkedAccounts [許可のみ]	メンバー/連結アカウントのリストを取得するアクセス許可を付与	リスト			

AWS 一括請求で定義されるリソースタイプ

AWS 一括請求では、IAM ポリシーステートメントの Resource要素でのリソース ARN の指定はサポートされていません。 AWS 一括請求へのアクセスを許可するには、ポリシーで "Resource": "*" を指定します。

AWS 一括請求の条件キー

一括請求には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Control Catalog のアクション、リソース、および条件キー

AWS Control Catalog (サービスプレフィックス: controlcatalog) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Control Catalog で定義されるアクション
- AWS Control Catalog で定義されているリソースタイプ
- AWS Control Catalog の条件キー

AWS Control Catalog で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetControl	特定のコントロールの詳細を返す許可を付与する	読み取り	control*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListCommonControls	AWS Control Catalog から一般的なコントロールのページ分割されたリストを返すアクセス許可を付与します	リスト			
ListControlMappings	AWS Control Catalog からコントロールマッピングのページ分割されたリストを返すアクセス許可を付与します	リスト			
ListControls	AWS Control Catalog ライブラリで使用可能なすべてのコントロールのページ分割されたリストを返すアクセス許可を付与します	リスト	control*		
ListDomains	AWS Control Catalog からドメインのページ分割されたリストを返すアクセス許可を付与します	リスト			
ListObjectives	AWS Control Catalog から目標のページ分割されたリストを返すアクセス許可を付与します	リスト			

AWS Control Catalog で定義されているリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
common-control	arn:${Partition}:controlcatalog:::common-control/${CommonControlId}	
control	arn:${Partition}:controlcatalog:::control/${ControlId}	
domain	arn:${Partition}:controlcatalog:::domain/${DomainId}	
objective	arn:${Partition}:controlcatalog:::objective/${ObjectiveId}	

AWS Control Catalog の条件キー

Control Catalog には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Control Tower のアクション、リソース、および条件キー

AWS Control Tower (サービスプレフィックス: controltower) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Control Tower で定義されるアクション
- AWS Control Tower で定義されるリソースタイプ

- AWS Control Tower の条件キー

AWS Control Tower で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateLandingZone	ランディングゾーンを作成するためのアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	controltower:TagResource
CreateManagedAccount [アクセス許可のみ]	AWS Control Tower によって管理されるアカウントを作成するアクセス許可を付与します	書き込み			
DeleteLandingZone	AWS Control Tower ランディングゾーンを削除するアクセス許可を付与します	書き込み	LandingZone*		
DeregisterManagedAccount [アクセス許可のみ]	Account Factory を通じて作成されたアカウントを AWS Control Tower から登録解除する許可を付与	書き込み			
DeregisterOrganizationalUnit [アクセス許可のみ]	AWS Control Tower 管理から組織単位の登録を解除する許可を付与	書き込み			
DescribeAccountFactoryConfig [ア	現在の Account Factory 設定を記述するアクセス許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
クセス許可のみ]					
DescribeCoreService [許可のみ]	AWS Control Tower のコアアカウントによって管理されるリソースを記述するアクセス許可を付与します	読み取り			
DescribeGuardrail [許可のみ]	ガードレールを記述するアクセス許可を付与	読み取り			
DescribeGuardrailForTarget [許可のみ]	組織単位のガードレールを記述するアクセス許可を付与	読み取り			
DescribeLandingZoneConfiguration [許可のみ]	現在のランディングゾーンの設定を記述するための許可を付与します	読み取り			
DescribeManagedAccount [許可のみ]	Account Factory で作成されたアカウントを記述するアクセス許可を付与	読み取り			
DescribeManagedOrganizationalUnit [許可のみ]	AWS Control Tower によって管理される AWS Organizations 組織単位を記述する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeRegisterOrganizationalUnitOperation [許可のみ]	組織単位の登録オペレーションを記述するための許可を付与します	読み取り			
DescribeSingleSignOn [許可のみ]	現在の AWS Control Tower IAM Identity Center 設定を記述するアクセス許可を付与します	読み取り			
DisableBaseline	ターゲットのベースラインを無効にする許可を付与する	書き込み	EnabledBaseline*		
DisableControl	組織単位からコントロールを削除するアクセス許可を付与	書き込み	EnabledControl*		
DisableGuardrail [アクセス許可のみ]	組織単位からガードレールを無効化するアクセス許可を付与	書き込み			
EnableBaseline	ターゲットでベースラインを有効にする許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	controltower:TagResource
EnableControl	組織単位のコントロールをアクティブ化するアクセス許可を付与	書き込み	EnabledControl		controltower:TagResource

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
EnableGuardrail [アクセス許可のみ]	組織単位に対してガードレールを有効化するアクセス許可を付与	書き込み			
GetAccountInfo [アクセス許可のみ]	アカウントの E メールを記述し、それが存在することを検証するための許可を付与します	読み取り			
GetAvailableUpdates [許可のみ]	現在の AWS Control Tower デプロイで利用可能な更新を一覧表示するアクセス許可を付与します	読み取り			
GetBaseline	Baseline の詳細を取得する許可を付与する	読み取り	Baseline*		
GetBaselineOperation	特定の Baseline 操作の現在のステータスを取得するための許可を付与する	読み取り			
GetControlOperation	特定の EnableControl オペレーションまたは DisableControl オペレーションの現在のステータスを取得するアクセス許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetEnabledBaseline	有効な Baseline を取得する許可を付与する	読み取り	EnabledBaseline*		
GetEnabledControl	組織単位から有効化されたコントロールを取得するアクセス許可を付与します	読み取り	EnabledControl*		
GetGuardrailComplianceStatus [許可のみ]	ガードレールの現在のコンプライアンスステータスを取得するアクセス許可を付与	読み取り			
GetHomeRegion [許可のみ]	AWS Control Tower セットアップのホームリージョンを取得する許可を付与	読み取り			
GetLandingZone	ランディングゾーンのセットアップの現在のステータスを取得するアクセス許可を付与	読み取り	LandingZone*		
GetLandingZoneDriftStatus	現在のランディングゾーンのドリフトステータスを取得するための許可を付与します	読み取り			
GetLandingZoneOperation	特定のランディングゾーン操作の現在のステータスを取得するためのアクセス許可を付与	読み取り			
GetLandingZoneStatus [許可のみ]	ランディングゾーンのセットアップの現在のステータスを取得するアクセス許可を付与	読み取り			
ListBaselines	Baselines を一覧表示する許可を付与する	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListControlOperations	すべてのコントロールオペレーションを一覧表示する許可を付与する	リスト			
ListDirectoryGroups [許可のみ]	IAM Identity Center を通じて利用可能な現在のディレクトリグループを一覧表示する許可を付与する	リスト			
ListDriftDetails	AWS Control Tower でドリフトの発生を一覧表示する許可を付与	読み取り			
ListEnabledBaselines	有効なベースラインを一覧表示する許可を付与する	リスト			
ListEnabledControls	指定した組織単位で有効になっているすべてのコントロールを一覧表示するアクセス許可を付与	リスト			
ListEnabledGuardrails [許可のみ]	現在有効なガードレールを一覧表示するアクセス許可を付与	リスト			
ListExtendedGovernancePrecheckDetails [許可のみ]	組織単位の事前チェックの詳細を一覧表示するための許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListExternalConfigRuleCompliance	外部 Config AWS ルールのコンプライアンスを一覧表示するアクセス許可を付与します	読み取り			
ListGuardrailViolations [許可のみ]	既存のガードレール違反を一覧表示するアクセス許可を付与	リスト			
ListGuardrails [許可のみ]	使用可能なすべてのガードレールを一覧表示するアクセス許可を付与	リスト			
ListGuardrailsForTarget [許可のみ]	ガードレールとその現在の状態を組織単位について一覧表示するアクセス許可を付与	リスト			
ListLandingZoneOperations	すべてのランディングゾーン操作を一覧表示する許可を付与する	リスト			
ListLandingZones	すべてのランディングゾーンを一覧表示するためのアクセス許可を付与	リスト			
ListManagedAccounts [許可のみ]	AWS Control Tower を介して管理されるアカウントを一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListManagedAccountsForGuardrail [許可のみ]	指定されたガードレールが適用されたマネージドアカウントを一覧表示するアクセス許可を付与	リスト			
ListManagedAccountsForParent [許可のみ]	組織単位の下のマネージドアカウントを一覧表示するアクセス許可を付与	リスト			
ListManagedOrganizationalUnits [許可のみ]	AWS Control Tower によって管理される組織単位を一覧表示する許可を付与	リスト			
ListManagedOrganizationalUnitsForGuardrail [許可のみ]	指定されたガードレールが適用された管理された組織単位を一覧表示するアクセス許可を付与	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	EnabledBaseline		
			EnabledControl		
			LandingZone		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ManageOrganizationalUnit [許可のみ]	AWS Control Tower によって管理される組織単位を設定するアクセス許可を付与します	書き込み			
PerformPreLaunchChecks [アクセス許可のみ]	アカウントで検証を実行するための許可を付与します	読み取り			
ResetEnabledBaseline	有効なベースラインをリセットする許可を付与する	書き込み	EnabledBaseline*		
ResetEnabledControl	組織単位の有効なコントロールをリセットするアクセス許可を付与します	書き込み	EnabledControl*		
ResetLandingZone	ランディングゾーンをリセットするためのアクセス許可を付与	書き込み	LandingZone*		
SetupLandingZone [アクセス許可のみ]	AWS Control Tower ランディングゾーンを設定または更新するアクセス許可を付与します	書き込み			
TagResource	リソースにタグを追加するアクセス許可を付与します	タグ付け	EnabledBaseline		
			EnabledControl		
			LandingZone		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	Tagging	EnabledBaseline		
			EnabledControl		
			LandingZone		
				aws:TagKeys	
UpdateAccountFactoryConfig [アクセス許可のみ]	Account Factory の設定を更新するアクセス許可を付与	書き込み			
UpdateEnabledBaseline	有効なベースラインを更新する許可を付与する	書き込み	EnabledBaseline*		
UpdateEnabledControl	組織単位で有効になっているコントロールを更新するためのアクセス許可を付与	書き込み	EnabledControl*		
UpdateLandingZone	ランディングゾーンを更新するためのアクセス許可を付与	書き込み	LandingZone*		

AWS Control Tower で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
EnabledControl	arn:${Partition}:controltower:${Region}:${Account}:enabledcontrol/${EnabledControlId}	aws:ResourceTag/${TagKey}
Baseline	arn:${Partition}:controltower:${Region}::baseline/${BaselineId}	
EnabledBaseline	arn:${Partition}:controltower:${Region}:${Account}:enabledbaseline/${EnabledBaselineId}	aws:ResourceTag/${TagKey}
LandingZone	arn:${Partition}:controltower:${Region}:${Account}:landingzone/${LandingZoneId}	aws:ResourceTag/${TagKey}

AWS Control Tower の条件キー

AWS Control Tower は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS のコストと使用状況レポートのアクション、リソース、および条件キー

AWS コストと使用状況レポート (サービスプレフィックス: cur) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS のコストと使用状況レポートで定義されるアクション
- AWS のコストと使用状況レポートで定義されるリソースタイプ
- AWS のコストと使用状況レポートの条件キー

AWS のコストと使用状況レポートで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteReportDefinition	コストと使用状況レポート定義を削除するアクセス許可を付与	書き込み	cur*		
DescribeReportDefinitions	コストと使用状況レポート定義を取得するアクセス許可を付与	読み取り			
GetClassicReport [許可のみ]	請求書 CSV レポートを取得するアクセス許可を付与	読み取り			
GetClassicReportPreferences [許可のみ]	使用状況レポートのクラシックレポート有効化ステータスを取得するアクセス許可を付与	読み取り			
GetUsageReport [許可のみ]	使用状況レポートワークフロー AWS のサービス、使用タイプ、およびオペレーションのリストを取得するアクセス許可を付与します。使用状況レポートのダウンロードも許可または拒否	読み取り			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	cur*		
				aws:ResourceTag/${TagKey}	
ModifyReportDefinition	コストと使用状況レポート定義を変更するアクセス許可を付与	書き込み	cur*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutClassicReportPreferences [アクセス許可のみ]	クラシックレポートを有効にするアクセス許可を付与	書き込み			
PutReportDefinition	コストと使用状況レポート定義を書き込むアクセス許可を付与	書き込み	cur*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	cur*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	リソースのタグを解除する許可を付与	タグ付け	cur*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:TagKeys aws:ResourceTag/${TagKey}	
ValidateReportDestination [アクセス許可のみ]	CUR 配信のための適切なアクセス許可を持つ s3 バケットが存在するかどうかを検証するアクセス許可を付与	読み取り			

AWS のコストと使用状況レポートで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource 工レメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
cur	`arn:${Partition}:cur:${Region}:${Account}:definition/${ReportName}`	

AWS のコストと使用状況レポートの条件キー

AWS コストと使用状況レポートでは、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに

絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Cost Explorer のアクション、リソース、および条件キー

AWS Cost Explorer Service (サービスプレフィックス: ce) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Cost Explorer Service で定義されるアクション
- AWS Cost Explorer Service で定義されるリソースタイプ
- AWS Cost Explorer Service の条件キー

AWS Cost Explorer Service で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateAnomalyMonitor	新しい異常モニターを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnomalySubscription	新しい異常サブスクリプションを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCostCategoryDefinition	要求された名前とルールを使用して新しい Cost Category を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNotificationSubscription [アクセス許可のみ]	予約の有効期限アラートを作成する許可を付与	書き込み			
CreateReport [アクセス許可のみ]	Cost Explorer レポートを作成する許可を付与	書き込み			
DeleteAnomalyMonitor	異常モニターを削除する許可を付与	書き込み	anomalymonitor*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
DeleteAnomalySubscription	異常サブスクリプションを削除する許可を付与	書き込み	anomalysubscription*		
				aws:ResourceTag/${TagKey}	
DeleteCostCategoryDefinition	Cost Category を削除する許可を付与	書き込み	costcategory*		
				aws:ResourceTag/${TagKey}	
DeleteNotificationSubscription [アクセス許可のみ]	予約の有効期限アラートを削除する許可を付与	書き込み			
DeleteReport [アクセス許可のみ]	Cost Explorer レポートを削除する許可を付与	書き込み			
DescribeCostCategoryDefinition	Cost Category の名前、ARN、ルール、定義、発効日などの説明を取得する許可を付与	読み取り	costcategory*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeNotificationSubscription [許可のみ]	予約の有効期限アラートを表示する許可を付与	読み取り			
DescribeReport [許可のみ]	Cost Explorer の [レポート] ページを表示する許可を付与	読み取り			
GetAnomalies	異常を取得する許可を付与	読み取り	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
GetAnomalyMonitors	異常モニターを照会する許可を付与	読み取り	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
GetAnomalySubscriptions	異常サブスクリプションを照会する許可を付与	読み取り	anomalysubscription*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetApproximateUsageRecords	過去 1 か月の使用状況から得た、選択されたリソース、レベル、および時間単位の粒度設定でのおおよその使用レコード数を取得する許可を付与	読み取り			
GetCommitmentPurchaseAnalysis	アカウントのコミットメント購入分析を取得するアクセス許可を付与します	読み取り			
GetConsoleActionSetEnforced [許可のみ]	Billing、Cost Management、および Account コンソールに対する承認を制御するために、既存またはきめ細かい IAM アクションを使用するかどうかを表示するための許可を付与します	読み取り			
GetCostAndUsage	アカウントのコストと利用状況のメトリクスを取得する許可を付与	読み取り	billingview		
				aws:ResourceTag/${TagKey}	
GetCostAndUsageComparisons	アカウントのコストと使用状況の比較を取得するアクセス許可を付与します	読み取り	billingview		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetCostAndUsageWithResources	アカウントのリソースを使用してコストと利用状況のメトリクスを取得する許可を付与	読み取り	billingview		
				aws:ResourceTag/${TagKey}	
GetCostCategories	指定した期間の Cost Catagory の名前と値をクエリする許可を付与	読み取り	billingview		
				aws:ResourceTag/${TagKey}	
GetCostComparisonDrivers	アカウントのコストドライバーを取得するアクセス許可を付与します	読み取り	billingview		
				aws:ResourceTag/${TagKey}	
GetCostForecast	予測期間のコスト予測を取得する許可を付与	読み取り	billingview		
				aws:ResourceTag/${TagKey}	
GetDimensionValues	一定期間にわたってフィルタに使用可能なすべてのフィルタの値を取得する許可を付与	読み取り	billingview		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetPreferences [許可のみ]	Cost Explorer の [設定] ページを表示する許可を付与	読み取り			
GetReservationCoverage	アカウントの予約のカバレッジを取得する許可を付与	読み取り			
GetReservationPurchaseRecommendation	アカウントの予約の推奨事項を取得する許可を付与	読み取り			
GetReservationUtilization	アカウントの予約率を取得する許可を付与	読み取り			
GetRightsizingRecommendation	アカウントの適切なサイズ設定に関する推奨事項を取得する許可を付与	読み取り			
GetSavingsPlanPurchaseRecommendationDetails	アカウントの Savings Plan に関するレコメンデーションの詳細を取得するための許可を付与します	読み取り			
GetSavingsPlansCoverage	アカウントの Savings Plans のカバレッジを取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetSavingsPlansPurchaseRecommendation	アカウントの Savings Plans に関する推奨事項を取得する許可を付与	読み取り			
GetSavingsPlansUtilization	アカウントの Savings Plans 使用率を取得する許可を付与	読み取り			
GetSavingsPlansUtilizationDetails	アカウントの Savings Plans 使用率の詳細を取得する許可を付与	読み取り			
GetTags	指定された期間のタグを照会する許可を付与	読み取り	billingview		
				aws:ResourceTag/${TagKey}	
GetUsageForecast	予測期間の使用状況予測を取得する許可を付与	読み取り	billingview		
				aws:ResourceTag/${TagKey}	
ListCommitmentPurchaseAnalyses	過去のコミットメント購入分析のリストを取得するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListCostAllocationTagBackfillHistory	Cost Allocation Tag のバックフィル履歴を一覧表示する許可を付与する	リスト			
ListCostAllocationTags	コスト割り当てタグを一覧表示する許可を付与	リスト			
ListCostCategoryDefinitions	すべての Cost Categories の名前、ARN、発効日を取得する許可を付与	リスト			
ListSavingsPlansPurchaseRecommendationGeneration	過去のレコメンデーション生成のリストを取得する許可を付与	リスト			
ListTagsForResource	Cost Explorer リソースのタグを一覧表示する許可を付与	読み取り	anomalymonitor		
			anomalysubscription		
			costcategory		
				aws:ResourceTag/${TagKey}	
ProvideAnomalyFeedback	検出された異常に関するフィードバックを提供する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartCommitmentPurchaseAnalysis	コミットメント購入分析をリクエストする許可を付与	書き込み			
StartCostAllocationTagBackfill	コスト配分タグのバックフィルをリクエストする許可を付与する	書き込み			
StartSavingsPlansPurchaseRecommendationGeneration	Savings Plans のレコメンデーション生成をリクエストする許可を付与	書き込み			
TagResource	Cost Explorer リソースにタグ付けする許可を付与	Tagging	anomalymonitor		
			anomalysubscription		
			costcategory		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	Cost Explorer リソースからタグを削除する許可を付与	Tagging	anomalymonitor		
			anomalysubscription		
			costcategory		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAnomalyMonitor	既存の異常モニターを更新する許可を付与	書き込み	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
UpdateAnomalySubscription	既存の異常サブスクリプションを更新する許可を付与	書き込み	anomalysubscription*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateConsoleActionSetEnforced [アクセス許可のみ]	Billing、Cost Management、および Account コンソールに対する承認を制御するために、既存またはきめ細かい IAM アクションを使用するかどうかを変更するための許可を付与します	書き込み			
UpdateCostAllocationTagsStatus	既存のコスト割り当てタグのステータスを更新する許可を付与	書き込み			
UpdateCostCategoryDefinition	既存の Cost Category を更新する許可を付与	書き込み	costcategory*		
				aws:ResourceTag/${TagKey}	
UpdateNotificationSubscription [アクセス許可のみ]	予約の有効期限アラートを更新する許可を付与	書き込み			
UpdatePreferences [アクセス許可のみ]	Cost Explorer の [設定] ページを編集する許可を付与	書き込み			
UpdateReport [アクセス許可のみ]	Cost Explorer レポートを更新する許可を付与	書き込み			

AWS Cost Explorer Service で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
anomalysubscription	`arn:${Partition}:ce::${Account}:anomalysubscription/${Identifier}`	aws:ResourceTag/${TagKey}
anomalymonitor	`arn:${Partition}:ce::${Account}:anomalymonitor/${Identifier}`	aws:ResourceTag/${TagKey}
costcategory	`arn:${Partition}:ce::${Account}:costcategory/${Identifier}`	aws:ResourceTag/${TagKey}
billingview	`arn:${Partition}:billing::${Account}:billingview/${ResourceId}`	aws:ResourceTag/${TagKey}

AWS Cost Explorer Service の条件キー

AWS Cost Explorer Service では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列

条件キー	説明	タイプ
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Cost Optimization Hub のアクション、リソース、および条件キー

AWS Cost Optimization Hub (サービスプレフィックス: `cost-optimization-hub`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Cost Optimization Hub で定義されるアクション
- AWS Cost Optimization Hub で定義されるリソースタイプ
- AWS Cost Optimization Hub の条件キー

AWS Cost Optimization Hub で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetPreferences	設定を取得するためのアクセス許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetRecommendation	レコメンデーション用にリソース設定と見積もりコストの影響を取得するためのアクセス許可を付与	読み取り			
ListEnrollmentStatuses	指定されたアカウントまたは管理アカウントのすべてのメンバーの登録ステータスを一覧表示するためのアクセス許可を付与	リスト			
ListRecommendationSummaries	グループごとにレコメンデーションの概要を一覧表示するためのアクセス許可を付与	リスト			cost-optimization-hub:GetRecommendation
ListRecommendations	レコメンデーションの概要ビューを一覧表示するためのアクセス許可を付与	リスト			cost-optimization-hub:GetRecommendation
UpdateEnrollmentStatus	登録ステータスを更新する権限を付与します	書き込み			
UpdatePreferences	設定を更新するためのアクセス許可を付与	書き込み			

AWS Cost Optimization Hub で定義されるリソースタイプ

AWS Cost Optimization Hub は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Cost Optimization Hub へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Cost Optimization Hub の条件キー

Cost Optimization Hub には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーがありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Customer Verification Service のアクション、リソース、および条件キー

AWS Customer Verification Service (サービスプレフィックス: customer-verification) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Customer Verification Service で定義されるアクション
- AWS Customer Verification Service で定義されるリソースタイプ
- AWS Customer Verification Service の条件キー

AWS Customer Verification Service で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にア

クションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateCustomerVerificationDetails [アクセス許可のみ]	顧客検証データを作成する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateUploadUrls [アクセス許可のみ]	アップロード URL を作成する許可を付与する	書き込み			
GetCustomerVerificationDetails [アクセス許可のみ]	顧客検証データを取得する許可を付与	読み取り			
GetCustomerVerificationEligibility [許可のみ]	顧客検証資格を取得する許可を付与	読み取り			
UpdateCustomerVerificationDetails [許可のみ]	顧客検証データを更新する許可を付与	書き込み			

AWS Customer Verification Service で定義されるリソースタイプ

AWS Customer Verification Service は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Customer Verification Service へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Customer Verification Service の条件キー

Customer Verification Service には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Data Exchange のアクション、リソース、および条件キー

AWS Data Exchange (サービスプレフィックス: dataexchange) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Data Exchange で定義されるアクション
- AWS Data Exchange で定義されるリソースタイプ
- AWS Data Exchange の条件キー

AWS Data Exchange で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptDataGrant	データ許可を受け入れる許可を付与する	書き込み	data-grants*		
CancelJob	ジョブをキャンセルする許可を付与	書き込み	jobs*		
CreateAsset [アクセス許可のみ]	アセットを (ジョブ内などで) 作成するためのアクセス許可を付与	書き込み	revisions*		
CreateDataGrant	データ許可を作成する許可を付与する	書き込み	data-grants*		dataexchange:Publi

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					shToDataGrant
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSet	データセットを作成するためのアクセス許可を付与	書き込み	data-sets*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventAction	イベントアクションを作成するためのアクセス許可を付与	書き込み	event-actions*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJob	アセットをインポートもしくはエクスポートするジョブを作成するためのアクセス許可を付与	書き込み	jobs*		
				dataexchange:JobType	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateRevision	リビジョンを作成するためのアクセス許可を付与	書き込み	data-sets*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAsset	アセットを削除する許可を付与	書き込み	assets*		
DeleteDataGrant	データ許可を削除する許可を付与する	書き込み	data-grants*		
DeleteDataSet	データセットを削除するためのアクセス許可を付与	書き込み	data-sets*		
			entitled-data-sets*		
DeleteEventAction	イベントアクションを削除するためのアクセス許可を付与	書き込み	event-actions*		
DeleteRevision	リビジョンを削除するためのアクセス許可を付与	書き込み	revisions*		
GetAsset	アセットに関する情報を (ジョブ内などで) 取得しエクスポートするためのアクセス許可を付与	読み取り	assets*		
			entitled-assets*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetDataGrant	データ許可を得るための許可を付与する	読み取り	data-grants*		
GetDataSet	データセットに関する情報を取得するためのアクセス許可を付与	読み込み	data-sets*		
			entitled-data-sets*		
GetEventAction	イベントアクションを取得するためのアクセス許可を付与	読み込み	event-actions*		
GetJob	ジョブに関する情報を取得するためのアクセス許可を付与	読み取り	jobs*		
GetReceivedDataGrant	受信したデータ許可を取得する許可を付与する	読み取り	data-grants*		
GetRevision	リビジョンに関する情報を取得するためのアクセス許可を付与	読み取り	entitled-revisions*		
			revisions*		
ListDataGrants	アカウントのデータ許可を一覧表示するための許可を付与する	リスト			
ListDataSetRevisions	データセットのリビジョンを一覧表示するためのアクセス許可を付与	リスト	data-sets*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			entitled-data-sets *		
ListDataSets	アカウントのデータセットを一覧表示するためのアクセス許可を付与	リスト			
ListEventActions	アカウントのイベントアクションを一覧表示するためのアクセス許可を付与	リスト			
ListJobs	アカウントのジョブを一覧表示するためのアクセス許可を付与	リスト			
ListReceivedDataGrants	アカウントの受信データ許可を一覧表示する許可を付与する	リスト			
ListRevisionAssets	リビジョンのアセットに関するリストを取得するためのアクセス許可を付与	リスト	entitled-revisions *		
			revisions *		
ListTagsForResource	指定したリソースに関連付けたタグを一覧表示する許可を付与	リスト	data-grants		
			data-sets		
			event-actions		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			revisions		
PublishDataSet [許可のみ]	データセットを製品に公開する許可を付与する	書き込み	data-sets*		
PublishToDataGrant [アクセス許可のみ]	データセットをデータ許可に公開する許可を付与する	書き込み	data-sets*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RevokeRevision	リビジョンへの受信者アクセスを取り消すアクセス許可を付与	書き込み	revisions*		
SendApiAsset	API アセットにリクエストを送信するアクセス許可を付与	書き込み	assets*		
			entitled-assets*		
SendDataSetNotification	データセットのサブスクライバーに通知を送信するアクセス許可を付与	書き込み	data-sets*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartJob	ジョブを開始するためのアクセス許可を付与	書き込み	jobs*		dataexchange:CreateAsset dataexchange:DeleteDataSet dataexchange:GetAsset dataexchange:GetDataSet dataexchange:GetRevision dataexchange:PublishDataSet redshift:AuthorizeDataShare
TagResource	指定したリソースに 1 つ以上のタグを追加する許可を付与	タグ付け	data-grants		
			data-sets		
			event-actions		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			revisions		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	指定したリソースから 1 つ以上のタグを削除する許可を付与	Tagging	data-grants		
			data-sets		
			event-actions		
			revisions		
				aws:TagKeys	
UpdateAsset	アセットに関する更新情報を取得するためのアクセス許可を付与	書き込み	assets*		
UpdateDataSet	データセットに関する情報を更新するためのアクセス許可を付与	書き込み	data-sets*		
UpdateEventAction	イベントアクションに関する情報を更新するためのアクセス許可を付与	書き込み	event-actions*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateRevision	リビジョンに関する情報を更新するためのアクセス許可を付与	書き込み	revisions *		dataexchange:PublishDataSet dataexchange:PublishToDataGrant

AWS Data Exchange で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
jobs	arn:${Partition}:dataexchange:${Region}:${Account}:jobs/${JobId}	dataexchange:JobType
data-sets	arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}	aws:ResourceTag/${TagKey}
entitled-data-sets	arn:${Partition}:dataexchange:${Region}::data-sets/${DataSetId}	
revisions	arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}/revisions/${RevisionId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
entitled-revisions	arn:${Partition}:dataexchange:${Region}::data-sets/${DataSetId}/revisions/${RevisionId}	
assets	arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}/revisions/${RevisionId}/assets/${AssetId}	
entitled-assets	arn:${Partition}:dataexchange:${Region}::data-sets/${DataSetId}/revisions/${RevisionId}/assets/${AssetId}	
event-actions	arn:${Partition}:dataexchange:${Region}:${Account}:event-actions/${EventActionId}	aws:ResourceTag/${TagKey}
data-grants	arn:${Partition}:dataexchange:${Region}:${Account}:data-grants/${DataGrantId}	aws:ResourceTag/${TagKey}

AWS Data Exchange の条件キー

AWS Data Exchange では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	作成リクエスト内で必須の各タグにより許可された値セットに基き、アクセスをフィルタリングする	String

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値に基づいて、アクセスをフィルタリングする	String
aws:TagKeys	作成リクエスト内の必須タグの存在に基づきアクセスをフィルタリングする	ArrayOfString
dataexchange:JobType	指定されたジョブタイプ でアクセスをフィルタリングする。	String

Amazon Data Lifecycle Manager のアクション、リソース、および条件キー

Amazon Data Lifecycle Manager (サービスプレフィックス: dlm) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Data Lifecycle Manager で定義されるアクション
- Amazon Data Lifecycle Manager で定義されるリソースタイプ
- Amazon Data Lifecycle Manager の条件キー

Amazon Data Lifecycle Manager で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーショ

ンへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateLifecyclePolicy	Amazon EBS スナップショットのスケジュールされた作成と保持を管理するためにデータのライフサイクルポリシーを作成するアクセス許可を付与します。最大 100 個のポリシーを保持できます	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteLifecyclePolicy	既存のデータライフサイクルポリシーを削除するアクセス許可を付与します。さらに、このアクションにより、ポリシーで指定されたスナップショットの作成と削除が停止されます。既存のスナップショットは影響を受けません	書き込み	policy*		
GetLifecyclePolicies	データのライフサイクルポリシーの概要説明のリストを返すアクセス許可を付与します	リスト			
GetLifecyclePolicy	単一のデータのライフサイクルポリシーの詳細な説明を返すアクセス許可を付与します	読み込み	policy*		
ListTagsForResource	リソースに関連付けられているタグを一覧表示する許可を付与	読み込み	policy*		
TagResource	リソースのタグを追加または更新する許可を付与	Tagging	policy*		
				aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
UntagResource	リソースに関連付けられているタグを削除する許可を付与	Tagging	policy*		
				aws:TagKeys	
UpdateLifecyclePolicy	既存のデータライフサイクルポリシーを更新するアクセス許可を付与します	書き込み	policy*		

Amazon Data Lifecycle Manager で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
policy	arn:${Partition}:dlm:${Region}:${Account}:policy/${ResourceName}	aws:ResourceTag/${TagKey}

Amazon Data Lifecycle Manager の条件キー

Amazon Data Lifecycle Manager は、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Data Pipeline のアクション、リソース、および条件キー

AWS Data Pipeline (サービスプレフィックス: `datapipeline`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Data Pipeline で定義されるアクション
- AWS Data Pipeline で定義されるリソースタイプ
- AWS Data Pipeline の条件キー

AWS Data Pipeline で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ActivatePipeline	指定されたパイプラインを検証するアクセス許可を付与し、パイプラインタスクの処理を開始します。パイプラインが検証にパスしなかった場合、アクティベーションは失敗します	書き込み	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	
AddTags	指定されたパイプラインのタグを追加または変更するアクセス許可を付与します	Tagging	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreatePipeline	新しい空のパイプラインを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys datapipeline:Tag/${TagKey}	datapipeline:AddTags
DeactivatePipeline	指定された実行中のパイプラインを非アクティブ化するアクセス許可を付与します	書き込み	pipeline*	datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeletePipeline	パイプライン、およびそのパイプライン定義と実行履歴を削除するアクセス許可を付与します	書き込み	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
DescribeObjects	パイプラインに関連付けられた一連のオブジェクトのオブジェクト定義を取得するアクセス許可を付与します	読み込み	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
DescribePipelines	1 つまたは複数のパイプラインに関するメタデータを取得するアクセス許可を付与します	読み取り	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
EvaluateExpression	EvaluateExpression を呼び出し、指定されたオブジェクトのコンテキストの文字列を評価するアクセス許可をタスクランナーに付与します	読み取り	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
GetAccountLimits [許可のみ]	GetAccountLimits を呼び出すアクセス許可を付与します	リスト			
GetPipelineDefinition	指定されたパイプラインの定義を取得するアクセス許可を付与します	読み込み	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	
ListPipelines	ユーザーがアクセス許可を持つすべてのアクティブパイプラインのパイプライン識別子を一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PollForTask	PollForTask を呼び出し、AWS Data Pipeline から実行するタスクを受信するアクセス許可をタスクランナーに付与します	書き込み		datapipeline:workerGroup	
PutAccountLimits [アクセス許可のみ]	PutAccountLimits を呼び出すアクセス許可を付与します	書き込み			
PutPipelineDefinition	指定されたパイプラインにタスク、スケジュール、および前提条件を追加するアクセス許可を付与します	書き込み	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
QueryObjects	指定された一連の条件に一致するオブジェクトの名前を、指定されたパイプラインでクエリするアクセス許可を付与します	読み込み	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
RemoveTags	指定されたパイプラインから既存のタグを削除するアクセス許可を付与します	Tagging	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	
ReportTaskProgress	タスクが割り当てられていることを確認するために、タスクが割り当てられると、ReportTaskProgress を呼び出すアクセス許可をタスクランナーに付与します	書き込み	pipeline*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ReportTaskRunnerHeartbeat	動作することを示すために、15 分ごとに ReportTaskRunnerHeartbeat を呼び出すアクセス許可をタスクランナーに付与します	書き込み			
SetStatus	指定された物理パイプラインオブジェクト、または論理パイプラインオブジェクトのステータスが、指定されたパイプラインで更新されるようにリクエストするアクセス許可を付与します	書き込み	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
SetTaskStatus	SetTaskStatus を呼び出して、タスクが完了したことを AWS Data Pipeline に通知し、最終ステータスに関する情報を提供するアクセス許可をタスクランナーに付与します	書き込み	pipeline*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ValidatePipelineDefinition	パイプライン定義が正しい形式であり、エラーなく実行できることを確認するために、指定されたパイプライン定義を検証するアクセス許可を付与します	読み込み	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	

AWS Data Pipeline で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
pipeline	arn:${Partition}:datapipeline:${Region}:${Account}:pipeline/${PipelineId}	aws:ResourceTag/${TagKey}

AWS Data Pipeline の条件キー

AWS Data Pipeline では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString
datapipeline:PipelineCreator	パイプラインを作成した IAM ユーザーでアクセスをフィルタリングします	ArrayOfString
datapipeline:Tag/${TagKey}	リソースにアタッチすることができる、顧客が指定したキーと値のペアによってアクセスをフィルタリングします	String
datapipeline:workerGroup	タスクランナーが作業を取得する対象のワーカーグループの名前によってアクセスをフィルタリングします	ArrayOfString

AWS Database Migration Service のアクション、リソース、および条件キー

AWS Database Migration Service (サービスプレフィックス: dms) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Database Migration Service で定義されるアクション
- AWS Database Migration Service で定義されるリソースタイプ
- AWS Database Migration Service の条件キー

AWS Database Migration Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddTagsToResource	レプリケーションインスタンス、エンドポイント、セキュリティグループ、移行タスクなど、DMS リソースにメタデータタグを追加する許可を付与	タグ付け	Certificate		
			DataMigration		
			DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			MigrationProject		
			ReplicationConfig		
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		
			ReplicationTaskAssessmentRun		
			ReplicationTaskIndividualAssessment		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
ApplyPendingMaintenanceAction	保留中のメンテナンスアクションをリソース (例えば、レプリケーションインスタンス) に適用する許可を付与	書き込み	ReplicationInstance*		
AssociateExtensionPack	拡張機能を関連付ける許可を付与	書き込み	MigrationProject*		
BatchStartRecommendations	ソースデータベースごとにターゲットエンジンを推奨するために、最大 20 のソースデータベースの分析を開始するための許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CancelReplicationTaskAssessmentRun	1 回のプレマイグレーション評価の実行をキャンセルする許可を付与	書き込み	ReplicationTaskAssessmentRun*		
CreateDataMigration	指定された設定を使用してデータベース移行を作成する許可を付与	書き込み	MigrationProject*		iam:PassRole
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateDataProvider	提供された設定を使用してデータプロバイダーを作成する許可を付与	書き込み		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole
CreateEndpoint	提供された設定を使用してエンドポイントを作成する許可を付与	書き込み		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateEventSubscription	DMS AWS イベント通知サブスクリプションを作成するアクセス許可を付与します	書き込み		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateFleetAdvisorCollector	指定されたパラメータを使用して Fleet Advisor コレクタを作成するアクセス許可を付与	書き込み			iam:PassRole
CreateInstanceProfile	提供された設定を使用してインスタンスプロファイルを作成する許可を付与	書き込み		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateMigrationProject	提供された設定を使用して移行プロジェクトを作成する許可を付与	書き込み	DataProvider*		iam:PassRole
			InstanceProfile*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateReplicationConfig	指定された設定を使用してレプリケーション設定を作成する許可を付与	書き込み	Endpoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateReplicationInstance	指定されたパラメータを使用してレプリケーションインスタンスを作成する許可を付与	書き込み		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateReplicationSubnetGroup	VPC 内のサブネット ID のリストを指定して、レプリケーションサブネットグループを作成する許可を付与	書き込み		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateReplicationTask	指定されたパラメータを使用してレプリケーションタスクを作成する許可を付与	書き込み	Endpoint* ReplicationInstance*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
DeleteCertificate	指定された証明書を削除する許可を付与	書き込み	Certificate*		
DeleteConnection	レプリケーションインスタンスとエンドポイント間の指定された接続を削除するためのアクセス許可を付与	書き込み	Endpoint*		
			ReplicationInstance*		
DeleteDataMigration	指定されたデータベース移行を削除する許可を付与	書き込み	DataMigration*		
DeleteDataProvider	指定されたデータプロバイダーを削除する許可を付与	書き込み	DataProvider*		
DeleteEndpoint	指定されたエンドポイントを削除する許可を付与	書き込み	Endpoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteEventSubscription	DMS AWS イベントサブスクリプションを削除するアクセス許可を付与します	書き込み	EventSubscription*		
DeleteFleetAdvisorCollector	指定した Fleet Advisor コレクタを削除する許可を付与	書き込み			
DeleteFleetAdvisorDatabases	指定した Fleet Advisor データベースを削除する許可を付与	書き込み			
DeleteInstanceProfile	指定されたインスタンスプロファイルを削除する許可を付与	書き込み	InstanceProfile*		
DeleteMigrationProject	指定された移行プロジェクトを削除する許可を付与	書き込み	MigrationProject*		
DeleteReplicationConfig	指定されたレプリケーション設定を削除する許可を付与	書き込み	ReplicationConfig*		
DeleteReplicationInstance	指定されたレプリケーションインスタンスを削除する許可を付与	書き込み	ReplicationInstance*		
DeleteReplicationSubnetGroup	サブネットグループを削除する許可を付与	書き込み	ReplicationSubnetGroup*		
DeleteReplicationTask	指定されたレプリケーションタスクを削除する許可を付与	書き込み	ReplicationTask*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteReplicationTaskAssessmentRun	1 回のプレマイグレーション評価の実行の記録を削除する許可を付与	書き込み	ReplicationTaskAssessmentRun*		
DescribeAccountAttributes	顧客アカウントのすべての AWS DMS 属性を一覧表示するアクセス許可を付与します	読み取り			
DescribeApplicableIndividualAssessments	新しいプレマイグレーション評価の実行で指定できる個々の評価を一覧表示する許可を付与	読み込み	ReplicationInstance		
			ReplicationTask		
DescribeCertificates	証明書の説明を提供する許可を付与	読み込み			
DescribeConnections	レプリケーションインスタンスとエンドポイント間の接続のステータスを説明する許可を付与	読み取り			
DescribeConversionConfiguration	DMS スキーマ変換プロジェクト構成に関する情報を返すアクセス許可を付与します	読み取り	MigrationProject*		
DescribeDataMigrations	指定されたリージョンでのアカウントのデータベース移行に関する情報を返す許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeEndpointSettings	特定のデータベースエンジンのエンドポイントを作成するときに利用可能なエンドポイント設定を返す許可を付与	読み込み			
DescribeEndpointTypes	利用可能なエンドポイントのタイプについての情報を返すアクセス許可を付与	読み込み			
DescribeEndpoints	現在のリージョンのアカウントのエンドポイントについての情報を返すアクセス許可を付与	読み取り			
DescribeEngineVersions	DMS レプリケーションインスタンスの利用可能なバージョンについての情報を返すアクセス許可を付与します	読み取り			
DescribeEventCategories	すべてのイベントソースタイプか、指定されている場合は、指定されたソースタイプのカテゴリを一覧表示する許可を付与	読み込み			
DescribeEventSubscriptions	お客様アカウントのサブスクリプションの説明をすべて一覧表示する許可を付与	読み込み			
DescribeEvents	指定されたソース識別子とソースタイプのイベントを一覧表示する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeFleetAdvisorCollectors	フィルター設定に基づいて、アカウント内の Fleet Advisor コレクタのページ分割されたリストを返すアクセス許可を付与	読み取り			
DescribeFleetAdvisorDatabases	フィルター設定に基づいて、アカウント内の Fleet Advisor データベースのページ分割されたリストを返すアクセス許可を付与	読み取り			
DescribeFleetAdvisorLsaAnalysis	Fleet Advisor コレクタが作成した大規模評価 (LSA) 分析の説明のページ分割されたリストを返すアクセス許可を付与	読み取り			
DescribeFleetAdvisorSchemaObjectSummary	フィルター設定に基づいて、Fleet Advisor コレクタによって検出されたスキーマの説明のページ分割されたリストを返すアクセス許可を付与	読み取り			
DescribeFleetAdvisorSchemas	フィルター設定に基づいて、Fleet Advisor コレクタによって検出されたスキーマのページ分割されたリストを返すアクセス許可を付与	読み取り			
DescribeMetadataModelImports	移行プロジェクトのメタデータモデルのインポート操作の開始に関する情報を返す許可を付与します	読み取り	MigrationProject*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeOrderableReplicationInstances	指定されたリージョンに作成できるレプリケーションインスタンスタイプについての情報を返すアクセス許可を付与	読み取り			
DescribePendingMaintenanceActions	保留中のメンテナンスアクションに関する情報を返すアクセス許可を付与	読み取り			
DescribeRecommendationLimitations	ターゲット AWS エンジンのレコメンデーションの制限の説明のページ分割されたリストを返すアクセス許可を付与します	読み取り			
DescribeRecommendations	ソースデータベースのターゲットエンジンのレコメンデーションの説明のページ分割されたリストを返すための許可を付与します	読み取り			
DescribeRefreshSchemasStatus	RefreshSchemas 操作のステータスを返すアクセス許可を付与	読み取り	Endpoint*		
DescribeReplicationConfigs	レプリケーション設定を記述する許可を付与	読み取り			
DescribeReplicationInstanceTaskLogs	指定されたタスクのタスクログについて情報を返すアクセス許可を付与	読み込み	ReplicationInstance*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeReplicationInstances	現在のリージョンのアカウントのレプリケーションインスタンスについての情報を返すアクセス許可を付与	読み込み			
DescribeReplicationSubnetGroups	レプリケーションサブネットグループについての情報を返すアクセス許可を付与	読み取り			
DescribeReplicationTableStatistics	レプリケーションテーブル統計を記述する許可を付与	読み取り	ReplicationConfig*		
DescribeReplicationTaskAssessmentResults	Amazon S3 から最新のタスク評価結果を返す許可を付与	読み込み	ReplicationTask		
DescribeReplicationTaskAssessmentRuns	フィルター設定に基づいて、プレマイグレーション評価の実行のページ分割されたリストを返すアクセス許可を付与	読み込み	ReplicationInstance		
			ReplicationTask		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			ReplicationTaskAssessmentRun		
DescribeReplicationTaskIndividualAssessments	フィルタ設定に基づいて個々の評価のページ分割されたリストを返す許可を付与	読み込み	ReplicationTask		
			ReplicationTaskAssessmentRun		
DescribeReplicationTasks	現在のリージョンのアカウントのレプリケーションタスクについての情報を返すアクセス許可を付与	読み取り			
DescribeReplications	レプリケーションを記述する許可を付与	読み取り			
DescribeSchemas	指定されたエンドポイントのスキーマについての情報を返すアクセス許可を付与	読み込み	Endpoint*		
DescribeTableStatistics	テーブル名、挿入行、更新行、削除行などデータベース移行タスクのテーブル統計を返すアクセス許可を付与	読み取り	ReplicationTask*		
ExportMetadataModelAssessment	指定されたメタデータモデル評価をエクスポートする許可を付与	書き込み	MigrationProject		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ImportCertificate	指定された証明書をアップロードする許可を付与	書き込み		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
ListDataProviders	データプロバイダーの AWS DMS 属性を一覧表示する許可を付与	読み取り			
ListExtensionPacks	拡張パックの AWS DMS 属性を一覧表示するアクセス許可を付与します	読み取り	MigrationProject		
ListInstanceProfiles	インスタンスプロファイルの AWS DMS 属性を一覧表示するアクセス許可を付与します	読み取り	InstanceProfile		
ListMetadataModelAssessmentActionItems [許可のみ]	メタデータモデル評価アクション項目の AWS DMS 属性を一覧表示するアクセス許可を付与します。注意。このアクションには StartMetadataModelImport が必要ですが、後者は現在、説明されているスキーマ変換オペレーションを認可していません	読み取り	MigrationProject		dms:StartMetadataModelImport

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListMetadataModelAssessments	メタデータモデル評価の AWS DMS 属性を一覧表示する許可を付与	読み取り	MigrationProject		
ListMetadataModelConversions	メタデータモデル変換の AWS DMS 属性を一覧表示するアクセス許可を付与します	読み取り	MigrationProject		
ListMetadataModelExports	メタデータモデルエクスポートの AWS DMS 属性を一覧表示する許可を付与	読み取り	MigrationProject		
ListMigrationProjects	移行プロジェクトの AWS DMS 属性を一覧表示するアクセス許可を付与します。注意。このアクションには DescribeMigrationProjects と DescribeConversionConfiguration が必要ですが、両方の必要なアクションは現在、説明されているスキーマ変換オペレーションを認可していません。	読み取り	DataProvider		dms:DescribeConversionConfiguration
			InstanceProfile		
			MigrationProject		
ListTagsForResource	DMS AWS リソースのすべてのタグを一覧表示するアクセス許可を付与します	読み取り	Certificate		
			DataMigration		
			DataProvider		
			Endpoint		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			EventSubscription		
			InstanceProfile		
			MigrationProject		
			ReplicationConfig		
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		
			ReplicationTaskAssessmentRun		
			ReplicationTaskIndividualAssessment		
ModifyDataMigration	指定されたデータベース移行を変更する許可を付与	書き込み	DataMigration*		iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ModifyEndpoint	指定されたエンドポイントを変更する許可を付与	書き込み	Endpoint*		iam:PassRole
			Certificate		
ModifyEventSubscription	既存の DMS AWS イベント通知サブスクリプションを変更するアクセス許可を付与します	書き込み			
ModifyFleetAdvisorCollector [アクセス許可のみ]	指定した Fleet Advisor コレクタの名前と説明を変更するアクセス許可を付与	書き込み			
ModifyFleetAdvisorCollectorStatuses [アクセス許可のみ]	指定した Fleet Advisor コレクタのステータスを変更するアクセス許可を付与	書き込み			
ModifyReplicationConfig	指定されたレプリケーション設定を変更する許可を付与	書き込み	ReplicationConfig*		
ModifyReplicationInstance	レプリケーションインスタンスを変更して新しい設定を適用するためのアクセス許可を付与	書き込み	ReplicationInstance*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ModifyReplicationSubnetGroup	指定されたレプリケーションサブネットグループの設定を変更する許可を付与	書き込み			
ModifyReplicationTask	指定されたレプリケーションタスクを変更する許可を付与	書き込み	ReplicationTask*		
MoveReplicationTask	指定されたレプリケーションタスクを別のレプリケーションインスタンスに移動するためのアクセス許可を付与	書き込み	ReplicationInstance*		
			ReplicationTask*		
RebootReplicationInstance	レプリケーションインスタンスを再起動する許可を付与 再起動すると、レプリケーションインスタンスが再度使用可能になるまで、一時的に機能停止になります	書き込み	ReplicationInstance*		
RefreshSchemas	指定されたエンドポイントのスキーマを投入する許可を付与	書き込み	Endpoint*		
			ReplicationInstance*		
ReloadReplicationTables	レプリケーションのソースを使用してターゲットデータベーステーブルをリロードする許可を付与	書き込み	ReplicationConfig*		
ReloadTables	ターゲットデータベース表をソースデータでリロードする許可を付与	書き込み	ReplicationTask*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RemoveTagsFromResource	DMS リソースからメタデータタグを削除する許可を付与	Tagging	Certificate		
			DataMigration		
			DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		
			MigrationProject		
			ReplicationConfig		
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			ReplicationTaskAssessmentRun		
			ReplicationTaskIndividualAssessment		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
RunFleetAdvisorLsaAnalysis	アカウント内のすべての Fleet Advisor コレクタに対して大規模評価 (LSA) 分析を実行するアクセス許可を付与	書き込み			
StartDataMigration	データベース移行を開始する許可を付与	書き込み	DataMigration*		
StartMetadataModelAssessment	メタデータモデルの新しい評価を開始する許可を付与	書き込み	MigrationProject*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartMetadataModelConversion	メタデータモデルの新しい変換を開始する許可を付与	書き込み	MigrationProject*		
StartMetadataModelExportAsScripts	スクリプトとしてのメタデータモデルの新しいエクスポートを開始する許可を付与	書き込み	MigrationProject*		
StartMetadataModelExportToTarget	ターゲットとしてのメタデータモデルの新しいエクスポートを開始する許可を付与	書き込み	MigrationProject*		
StartMetadataModelImport	メタデータモデルの新しいインポートを開始する許可を付与	書き込み	MigrationProject*		
StartRecommendations	ソースデータベースの分析を開始して、ターゲットエンジンのレコメンデーションを提供するための許可を付与します	書き込み			
StartReplication	レプリケーションを開始する許可を付与	書き込み	ReplicationConfig*		
StartReplicationTask	レプリケーションタスクを開始する許可を付与	書き込み	ReplicationTask*		
StartReplicationTaskAssessment	ソースデータベース内のサポートされていないデータ型のレプリケーションタスク評価を開始する許可を付与	書き込み	ReplicationTask*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartReplicationTaskAssessmentRun	移行タスクの 1 つまたは複数の個別の評価に対して、新しいプレマイグレーション評価の実行を開始する許可を付与	書き込み	ReplicationTask*		iam:PassRole
StopDataMigration	データベース移行を停止する許可を付与	書き込み	DataMigration*		
StopReplication	レプリケーションを停止する許可を付与	書き込み	ReplicationConfig*		
StopReplicationTask	レプリケーションタスクを停止する許可を付与	書き込み	ReplicationTask*		
TestConnection	レプリケーションインスタンスとエンドポイント間の接続をテストする許可を付与	読み取り	Endpoint* ReplicationInstance*		
UpdateConversionConfiguration	変換設定を更新する許可を付与	書き込み	MigrationProject*		
UpdateDataProvider	指定されたデータプロバイダーを更新する許可を付与	書き込み	DataProvider*		
UpdateInstanceProfile	指定されたインスタンスプロファイルを更新する許可を付与	書き込み	InstanceProfile*		
UpdateMigrationProject	指定された移行プロジェクトを更新する許可を付与	書き込み	MigrationProject*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateSubscriptionsToEventBridge	DMS サブスクリプションを Eventbridge に移行するアクセス許可を付与	書き込み			
UploadFileMetadataList [アクセス許可のみ]	Amazon S3 バケットにファイルをアップロードするアクセス許可を付与	書き込み			

AWS Database Migration Service で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Certificate	arn:${Partition}:dms:${Region}:${Account}:cert:*	aws:ResourceTag/${TagKey} dms:cert-tag/${TagKey}
DataProvider	arn:${Partition}:dms:${Region}:${Account}:data-provider:*	aws:ResourceTag/${TagKey} dms:data-provider-tag/${TagKey}

リソースタイプ	ARN	条件キー
DataMigration	arn:${Partition}:dms:${Region}:${Account}:data-migration:*	aws:ResourceTag/${TagKey} dms:data-migration-tag/${TagKey}
Endpoint	arn:${Partition}:dms:${Region}:${Account}:endpoint:*	aws:ResourceTag/${TagKey} dms:endpoint-tag/${TagKey}
EventSubscription	arn:${Partition}:dms:${Region}:${Account}:es:*	aws:ResourceTag/${TagKey} dms:es-tag/${TagKey}
InstanceProfile	arn:${Partition}:dms:${Region}:${Account}:instance-profile:*	aws:ResourceTag/${TagKey} dms:instance-profile-tag/${TagKey}
MigrationProject	arn:${Partition}:dms:${Region}:${Account}:migration-project:*	aws:ResourceTag/${TagKey} dms:migration-project-tag/${TagKey}
ReplicationConfig	arn:${Partition}:dms:${Region}:${Account}:replication-config:*	aws:ResourceTag/${TagKey} dms:replication-config-tag/${TagKey}

リソースタイプ	ARN	条件キー
ReplicationInstance	arn:${Partition}:dms:${Region}:${Account}:rep:*	aws:ResourceTag/${TagKey} dms:rep-tag/${TagKey}
ReplicationSubnetGroup	arn:${Partition}:dms:${Region}:${Account}:subgrp:*	aws:ResourceTag/${TagKey} dms:subgrp-tag/${TagKey}
ReplicationTask	arn:${Partition}:dms:${Region}:${Account}:task:*	aws:ResourceTag/${TagKey} dms:task-tag/${TagKey}
ReplicationTaskAssessmentRun	arn:${Partition}:dms:${Region}:${Account}:assessment-run:*	aws:ResourceTag/${TagKey} dms:assessment-run-tag/${TagKey}
ReplicationTaskIndividualAssessment	arn:${Partition}:dms:${Region}:${Account}:individual-assessment:*	aws:ResourceTag/${TagKey} dms:individual-assessment-tag/${TagKey}

AWS Database Migration Service の条件キー

AWS Database Migration Service では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに

絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアによってアクセスをフィルタリングする	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString
dms:assessment-run-tag/${TagKey}	AssessmentRun に対するリクエスト内のタグキーと値のペアが存在するかどうかでアクセスをフィルタリングする	String
dms:cert-tag/${TagKey}	証明書のリクエスト内にタグキーと値のペアが存在するかどうかでアクセスをフィルタリング	String
dms:data-migration-tag/${TagKey}	DataMigration のリクエスト内にタグキーと値のペアが存在するかどうかでアクセスをフィルタリング	String
dms:data-provider-tag/${TagKey}	DataProvider のリクエスト内にあるタグキーと値のペアの存在有無でアクセスをフィルタリング	String
dms:endpoint-tag/${TagKey}	エンドポイントのリクエスト内にタグキーと値のペアが存在するかどうかでアクセスをフィルタリング	String
dms:es-tag/${TagKey}	EventSubscription のリクエスト内にタグキーと値のペアが存在するかどうかでアクセスをフィルタリング	String

条件キー	説明	[Type] (タイプ)
dms:individual-assessment-tag/${TagKey}	IndividualAssessment のリクエスト内のタグキーと値のペアが存在するかどうかでアクセスをフィルタリングする	String
dms:instance-profile-tag/${TagKey}	InstanceProfile のリクエスト内にあるタグキーと値のペアの存在有無でアクセスをフィルタリング	String
dms:migration-project-tag/${TagKey}	MigrationProject のリクエスト内にあるタグキーと値のペアの存在有無でアクセスをフィルタリング	String
dms:rep-tag/${TagKey}	ReplicationInstance のリクエスト内にタグキーと値のペアが存在するかどうかでアクセスをフィルタリング	String
dms:replication-config-tag/${TagKey}	ReplicationConfig のリクエスト内にタグキーと値のペアが存在するかどうかでアクセスをフィルタリング	String
dms:req-tag/${TagKey}	指定されたリクエスト内にタグキーと値のペアが存在するかどうかでアクセスをフィルタリング	String
dms:subgrp-tag/${TagKey}	ReplicationSubnetGroup のリクエスト内にタグキーと値のペアが存在するかどうかでアクセスをフィルタリング	String
dms:task-tag/${TagKey}	ReplicationTask のリクエスト内にタグキーと値のペアが存在するかどうかでアクセスをフィルタリング	String

Database Query Metadata Service のアクション、リソース、および条件キー

Database Query Metadata Service (サービスプレフィックス: dbqms) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Database Query Metadata Service で定義されるアクション
- Database Query Metadata Service で定義されるリソースタイプ
- Database Query Metadata Service の条件キー

Database Query Metadata Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateFavoriteQuery	新しいお気に入りクエリを作成する許可を付与。	Write			
CreateQueryHistory	クエリを履歴に追加する許可を付与。	Write			
CreateTab	新しいクエリタブを作成する許可を付与。	Write			
DeleteFavoriteQueries	保存されたクエリを削除する許可を付与。	Write			
DeleteQueryHistory	履歴クエリを削除する許可を付与。	Write			
DeleteTab	クエリタブを削除する許可を付与。	Write			
DescribeFavoriteQueries	保存されたクエリおよび関連するメタデータを一覧表示する許可を付与。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeQueryHistory	実行されたクエリの履歴を一覧表示する許可を付与。	リスト			
DescribeTabs	クエリタブおよび関連するメタデータを一覧表示する許可を付与。	リスト			
GetQueryString	お気に入りまたは履歴クエリ文字列を ID で検索する許可を付与。	Read			
UpdateFavoriteQuery	保存されたクエリと説明を更新する許可を付与。	Write			
UpdateQueryHistory	クエリ履歴を更新する許可を付与。	Write			
UpdateTab	クエリタブを更新する許可を付与。	Write			

Database Query Metadata Service で定義されるリソースタイプ

Database Query Metadata Service では、IAM ポリシーステートメントの `Resource` 要素でのリソース ARN の指定はサポートされていません。Database Query Metadata Service へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

Database Query Metadata Service の条件キー

DBQMS には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS「グローバル条件コンテキストキー」を参照してください。

AWS DataSync のアクション、リソース、および条件キー

AWS DataSync (サービスプレフィックス: datasync) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS DataSync で定義されるアクション
- AWS DataSync で定義されるリソースタイプ
- AWS DataSync の条件キー

AWS DataSync で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddStorageSystem	ストレージシステムを作成する許可を付与	書き込み	agent*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelTaskExecution	同期タスクの実行をキャンセルする許可を付与	書き込み	taskexecution*		
				aws:ResourceTag/${TagKey}	
CreateAgent	ホストにデプロイしたエージェントをアクティブ化する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationAzureBlob	Microsoft Azure Blob ストレージコンテナのエンドポイントを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationEfs	Amazon EFS ファイルシステムのエンドポイントを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxLustre	Amazon FSx Lustre エンドポイントを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateLocationFsxOntap	Amazon FSx for ONTAP エンドポイントを作成する許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxOpenZfs	Amazon FSx for OpenZFS エンドポイントを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxWindows	Amazon FSx Windows ファイルサーバーファイルシステムのエンドポイントを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationHdfs	Amazon Hdfs エンドポイントを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationNfs	NFS ファイルシステム用のエンドポイントを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateLocationObjectStorage	セルフマネージドオブジェクトストレージバケットのエンドポイントを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationS3	Amazon S3 バケットのエンドポイントを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationSmb	SMB ファイルシステムのエンドポイントを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTask	同期タスクを作成する許可を付与	書き込み	location* agent	aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAgent	エージェントを削除する許可を付与	書き込み	agent*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteLocation	AWS DataSync が使用する場所を削除するアクセス許可を付与します	書き込み	location*		
DeleteTask	同期タスクを削除する許可を付与	書き込み	task*		
DescribeAgent	同期エージェントに関する、名前、ネットワークインターフェイス、ステータス (エージェントが実行されているかどうか) などのメタデータを表示するためのアクセス許可を付与します	読み取り	agent*		
DescribeDiscoveryJob	検出ジョブに関するメタデータを記述する許可を付与	読み取り	discoveryjob*		
DescribeLocationAzureBlob	Azure Blob ストレージ同期場所に関するパス情報などのメタデータを表示する許可を付与	読み取り	location*		
DescribeLocationEfs	Amazon EFS 同期場所に関するパス情報など、メタデータを表示する許可を付与	読み込み	location*		
DescribeLocationFsxLustre	Amazon FSx Lustre 同期場所に関するパス情報などのメタデータを表示する許可を付与	読み取り	location*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeLocationFsxOntap	Amazon FSx for ONTAP 同期場所に関するパス情報などのメタデータを表示する許可を付与	読み取り	location*		
DescribeLocationFsxOpenZfs	Amazon FSx OpenZFS 同期場所に関するパス情報などのメタデータを表示するアクセス許可を付与します	読み込み	location*		
DescribeLocationFsxWindows	Amazon FSx Windows の同期場所に関するパス情報などのメタデータを表示する許可を付与	読み込み	location*		
DescribeLocationHdfs	Amazon HDFS 同期場所に関するパス情報などのメタデータを表示する許可を付与	読み込み	location*		
DescribeLocationNfs	NFS 同期場所に関するパス情報などのメタデータを表示する許可を付与	読み込み	location*		
DescribeLocationObjectStorage	セルフマネージドオブジェクトストレージサーバーの場所に関するメタデータを表示する許可を付与	読み込み	location*		
DescribeLocationS3	Amazon S3 バケットの同期場所に関する、バケット名などのメタデータを表示する許可を付与	読み込み	location*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeLocationSmb	SMB 同期場所に関するパス情報などのメタデータを表示する許可を付与	読み取り	location*		
DescribeStorageSystem	ストレージシステムに関するメタデータを表示する許可を付与	読み取り	storagesystem*		
DescribeStorageSystemResourceMetrics	検出ジョブによって収集されたリソースメトリクスを記述する許可を付与	リスト	discoveryjob*		
DescribeStorageSystemResources	検出ジョブによって識別されたリソースを記述する許可を付与	リスト	discoveryjob*		
DescribeTask	同期タスクに関するメタデータを表示する許可を付与	読み込み	task*		
DescribeTaskExecution	実行中の同期タスクに関するメタデータを表示する許可を付与	読み取り	taskexecution*		
				aws:ResourceTag/${TagKey}	
GenerateRecommendations	検出ジョブによって識別されたリソースのレコメンデーションを生成する許可を付与	書き込み	discoveryjob*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListAgents	リクエストで指定されたリージョン AWS アカウント で が所有するエージェントを一覧表示するアクセス許可を付与します	リスト			
ListDiscoveryJobs	検出ジョブを一覧表示する許可を付与	リスト			
ListLocations	同期元と同期先の場所を一覧表示する許可を付与	リスト			
ListStorageSystems	ストレージシステムを一覧表示する許可を付与	リスト			
ListTagsForResource	指定されたリソースに追加されたタグを一覧表示するためのアクセス許可を付与します	読み込み	agent		
			discoveryjob		
			location		
			storagesystem		
			task		
			taskexecution		
ListTaskExecutions	実行された同期タスクを一覧表示する許可を付与	リスト		aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTasks	すべての同期タスクを一覧表示する許可を付与	リスト			
RemoveStorageSystem	ストレージシステムを削除する許可を付与	書き込み	storagesystem*		
StartDiscoveryJob	ストレージシステムの検出ジョブを開始する許可を付与	書き込み	storagesystem*		
StartTaskExecution	同期タスクの特定の呼び出しを開始する許可を付与	書き込み	task*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
StopDiscoveryJob	検出ジョブを停止する許可を付与	書き込み	discoveryjob*		
TagResource	AWS リソースにキーと値のペアを適用するアクセス許可を付与します	Tagging	agent		
			discoveryjob		
			location		
			storagesystem		
			task		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			taskexecution		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	指定されたリソースから 1 つ以上のタグを削除する権限を付与します	Tagging	agent		
			discoveryjob		
			location		
			storagesystem		
			task		
			taskexecution		
				aws:TagKeys	
UpdateAgent	エージェントの名前を更新する許可を付与	書き込み	agent*		
UpdateDiscoveryJob	検出ジョブを更新する許可を付与	書き込み	discoveryjob*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateLocationAzureBlob	Azure Blob ストレージ同期場所を更新する許可を付与	書き込み	location*		
UpdateLocationEfs	EFS 同期の場所を更新するアクセス許可を付与します	書き込み	location*		
UpdateLocationFsxLustre	FSx Lustre 同期場所を更新するアクセス許可を付与します	書き込み	location*		
UpdateLocationFsxOntap	FSx ONTAP 同期場所を更新する許可を付与	書き込み	location*		
UpdateLocationFsxOpenZfs	FSx OpenZFS 同期場所を更新する許可を付与	書き込み	location*		
UpdateLocationFsxWindows	FSx Windows 同期の場所を更新する許可を付与	書き込み	location*		
UpdateLocationHdfs	HDFS 同期場所を更新する許可を付与	書き込み	location*		
UpdateLocationNfs	NFS 同期場所を更新する許可を付与	書き込み	location*		
UpdateLocationObjectStorage	セルフマネージドオブジェクトストレージサーバーの場所を更新する許可を付与	書き込み	location*		
UpdateLocationS3	S3 同期ロケーションを更新するアクセス許可を付与します	書き込み	location*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateLocationSmb	SMB 同期場所を更新するアクセス許可を付与	書き込み	location*		
UpdateStorageSystem	ストレージシステムを更新する許可を付与	書き込み	storagesystem*		
UpdateTask	同期タスクに関連付けられたメタデータを更新する許可を付与	書き込み	task*		
UpdateTaskExecution	同期タスクの実行を更新する許可を付与	書き込み	taskexecution*		
				aws:ResourceTag/${TagKey}	

AWS DataSync で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
agent	arn:${Partition}:datasync:${Region}:${AccountId}:agent/${AgentId}	aws:ResourceTag/${TagKey}
location	arn:${Partition}:datasync:${Region}:${AccountId}:location/${LocationId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
task	arn:${Partition}:datasync:${Region}:${AccountId}:task/${TaskId}	aws:ResourceTag/${TagKey}
taskexecution	arn:${Partition}:datasync:${Region}:${AccountId}:task/${TaskId}/execution/${ExecutionId}	aws:ResourceTag/${TagKey}
storagesystem	arn:${Partition}:datasync:${Region}:${AccountId}:system/${StorageSystemId}	aws:ResourceTag/${TagKey}
discoveryjob	arn:${Partition}:datasync:${Region}:${AccountId}:system/${StorageSystemId}/job/${DiscoveryJobId}	aws:ResourceTag/${TagKey}

AWS DataSync の条件キー

AWS DataSync は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアによるアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグキーと値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon DataZone のアクション、リソース、および条件キー

Amazon DataZone (サービスプレフィックス: datazone) では、IAM 許可ポリシーで使用できるように、次のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon DataZone によって定義されたアクション
- Amazon DataZone によって定義されたリソースタイプ
- Amazon DataZone の条件キー

Amazon DataZone によって定義されたアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptPredictions	予測を受け入れる許可を付与	書き込み			
AcceptSubscriptionRequest	データアセットのサブスクリプションリクエストを承認する許可を付与	書き込み			
AddEntityOwner	ドメインユニットなどのエンティティに所有者を追加する許可を付与する	書き込み			
AddPolicyGrant	ポリシー付与を追加する許可を付与する	権限の管理			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateEnvironmentRole	デフォルトのサービスブループリント環境でロールを関連付ける許可を付与する	書き込み			
AssociateGovernedTerms	管理対象用語をアセットに関連付けるアクセス許可を付与します	書き込み			
BatchDeleteLinkedTypes [アクセス許可のみ]	Amazon DataZone ドメインからリンク型項目を削除するアクセス許可を付与します	書き込み	domain*		
BatchPutLinkedTypes [アクセス許可のみ]	リンク型項目を Amazon DataZone ドメインに配置するアクセス許可を付与します	書き込み	domain*		
CancelMetadataGenerationRun	メタデータ生成実行をキャンセルする許可を付与する	書き込み			
CancelSubscription	データアセットへの承認されたサブスクリプションの取り消しや解除を行う許可を付与	書き込み			
CreateAccountPool	アカウントプールを作成するアクセス許可を付与します	書き込み			
CreateAsset	アセットを作成する許可を付与する	書き込み			
CreateAssetFilter	アセットフィルターを作成する許可を付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateAssetRevision	アセットの新しいリビジョンを作成する許可を付与	書き込み			
CreateAssetType	アセットタイプを作成する許可を付与	書き込み			
CreateConnection	接続を作成するアクセス許可を付与します	書き込み			
CreateDataProduct	データ製品を作成する許可を付与する	書き込み			
CreateDataProductRevision	データ製品のリビジョンを作成する許可を付与する	書き込み			
CreateDataSource	新しいデータソースを作成する許可を付与	書き込み			
CreateDomain	他の Amazon DataZone リソースを含む上位レベルのエンティティであるドメインをプロビジョニングする許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDomainUnit	ドメインユニットを作成するための許可を付与する	書き込み			
CreateEnvironment	データの公開とサブスクリプションに使用される設定済みリソースのコレクションを作成する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateEnvironmentAction	デフォルトのサービスブループリント環境で環境アクションを作成する許可を付与する	書き込み			
CreateEnvironmentBlueprint [アクセス許可のみ]	ユーザーがプロジェクトに環境を追加できるカスタム環境ブループリントを作成する許可を付与	書き込み			
CreateEnvironmentProfile	環境を作成するために使用できるブループリントからテンプレートを作成する許可を付与	書き込み			
CreateFormType	フォームタイプまたはその新しいリビジョンを作成する許可を付与	書き込み			
CreateGlossary	ビジネス用語集を作成する許可を付与	書き込み			
CreateGlossaryTerm	用語集の用語を作成する許可を付与	書き込み			
CreateGroupProfile	IAM アイデンティティセンターグループの DataZone グループプロファイルを作成する許可を付与	書き込み			
CreateListingChangeSet	リスティングの変更セットを作成する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateProject	チームによるデータの公開とサブスクリプションを可能にするプロジェクトを作成する許可を付与	書き込み			
CreateProjectMembership	ユーザーをプロジェクトに追加する許可を付与	書き込み			
CreateProjectProfile	プロジェクトプロファイルを作成する許可を付与する	書き込み			
CreateRule	ルールを作成するアクセス許可を付与します	書き込み			
CreateSubscriptionGrant	サブスクリプションターゲットで承認済みサブスクリプションへの許可を作成する許可を付与	書き込み			
CreateSubscriptionRequest	データアセットのサブスクリプションリクエストを作成する許可を付与	書き込み			
CreateSubscriptionTarget	プロジェクトの環境のサブスクリプションターゲットを作成する許可を付与	書き込み			
CreateUserProfile	カスタマー IAM アイデンティティセンターの既存のユーザーのユーザープロファイルを作成する許可を付与	書き込み			
DeleteAccountPool	アカウントプールを削除するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteAsset	アセットを削除する許可を付与	書き込み			
DeleteAssetFilter	アセットフィルターを削除する許可を付与する	書き込み			
DeleteAssetType	アセットタイプを削除する許可を付与	書き込み			
DeleteConnection	接続を削除するアクセス許可を付与します	書き込み			
DeleteDataProduct	データ製品を削除する許可を付与する	書き込み			
DeleteDataSource	既存のデータソースを更新する許可を付与	書き込み			
DeleteDomain	プロビジョニングされたドメインを削除する許可を付与	書き込み	domain*		
DeleteDomainSharingPolicy [アクセス許可のみ]	DataZone ドメインのリソースポリシーを削除する許可を付与	権限の管理			
DeleteDomainUnit	既存のドメインユニットを削除する許可を付与する	書き込み			
DeleteEnvironment	環境を削除する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteEnvironmentAction	デフォルトのサービスブループリント環境で環境アクションを削除する許可を付与する	書き込み			
DeleteEnvironmentBlueprint [アクセス許可のみ]	環境ブループリントを削除する許可を付与	書き込み			
DeleteEnvironmentBlueprintConfiguration	環境ブループリントの設定を削除する許可を付与	書き込み			
DeleteEnvironmentProfile	環境プロファイルを削除する許可を付与	書き込み			
DeleteFormType	フォームタイプを削除する許可を付与	書き込み			
DeleteGlossary	ビジネス用語集を削除する許可を付与	書き込み			
DeleteGlossaryTerm	用語集の用語を削除する許可を付与	書き込み			
DeleteListing	リスティングを削除する許可を付与	書き込み			
DeleteProject	チームによるデータの公開とサブスクリプションを可能にするプロジェクトを削除する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteProjectMembership	ユーザーをプロジェクトから削除する許可を付与	書き込み			
DeleteProjectProfile	プロジェクトプロファイルを削除する許可を付与する	書き込み			
DeleteRule	ルールを削除するアクセス許可を付与します	書き込み			
DeleteSubscriptionGrant	サブスクリプションターゲットからサブスクリプション許可を削除する許可を付与	書き込み			
DeleteSubscriptionRequest	データアセットの保留中のサブスクリプションリクエストを削除する許可を付与	書き込み			
DeleteSubscriptionTarget	プロジェクト内の環境からサブスクリプションターゲットを削除する許可を付与	書き込み			
DeleteTimeSeriesDataPoints	既存の TimeSeriesDataPoints を削除する許可を付与する	書き込み			
DisassociateEnvironmentRole	デフォルトのサービスブループリント環境でロールの関連付けを解除する許可を付与する	書き込み			
DisassociateGovernedTerms	管理対象用語とアセットの関連付けを解除するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetAccountPool	アカウントプールの詳細を取得するアクセス許可を付与します	読み取り			
GetAsset	アセットを取得する許可を付与	読み取り			
GetAssetFilter	アセットフィルターを取得する許可を付与する	読み取り			
GetAssetType	アセットタイプを取得する許可を付与	読み取り			
GetConnection	接続を取得するアクセス許可を付与します	読み取り			
GetDataProduct	データ製品を取得する許可を付与する	読み取り			
GetDataSource	識別子を使用して Amazon DataZone 内の既存のデータソースを取得する許可を付与	読み取り			
GetDataSourceRun	識別子を使用して Amazon DataZone 内のデータソースのジョブ実行を取得する許可を付与	読み取り			
GetDomain	ドメインに関する情報を取得するための許可を付与	読み取り	domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetDomainExecutionRoleCredentials [許可のみ]	ドメイン実行ロールの認証情報へのアクセスを必要とする機能を使用する許可を付与	読み取り			
GetDomainSharingPolicy [許可のみ]	DataZone ドメインのリソースポリシーを取得する許可を付与	読み取り			
GetDomainUnit	既存のドメインユニットを取得する許可を付与する	読み取り			
GetEnvironment	環境の詳細を取得する許可を付与	読み取り			
GetEnvironmentAction	デフォルトのサービスブループリント環境で環境アクションを取得する許可を付与する	読み取り			
GetEnvironmentActionLink [許可のみ]	環境アクションリンクを取得する許可を付与	読み取り			
GetEnvironmentBlueprint	環境ブループリントの詳細を取得する許可を付与	読み取り			
GetEnvironmentBlueprintConfiguration	環境ブループリントの設定を取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetEnvironmentCredentials	環境ユーザーロールを引き受ける短期認証情報を取得する許可を付与	読み取り			
GetEnvironmentProfile	環境プロファイルの詳細を取得する許可を付与	読み取り			
GetFormType	フォームタイプを取得する許可を付与	読み取り			
GetGlossary	ビジネス用語集を取得する許可を付与	読み取り			
GetGlossaryTerm	用語集の用語を取得する許可を付与	読み取り			
GetGroupProfile	既存の DataZone グループプロファイルを取得する許可を付与	読み取り			
GetIamPortalLoginUrl	IAM プリンシパルに対して DataZone ポータルにログインする許可を付与	権限の管理			
GetJobRun	ジョブ実行を取得するアクセス許可を付与します	読み取り			
GetLineageEvent	系統イベントを取得する許可を付与	読み取り			
GetLineageNode	系統ノードを取得する許可を付与する	読み取り			
GetListing	リストティングを取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetMetadataGenerationRun	メタデータ生成実行を取得するためのアクセス許可を付与	読み取り			
GetProject	プロジェクトの詳細を取得する許可を付与	読み取り			
GetProjectProfile	プロジェクトプロファイルの詳細を取得する許可を付与する	読み取り			
GetRule	ルールを取得するアクセス許可を付与します	読み取り			
GetSubscription	サブスクリプションを取得する許可を付与	読み取り			
GetSubscriptionEligibility [許可のみ]	サブスクリプションの適格性を取得するための許可を付与	読み取り			
GetSubscriptionGrant	サブスクリプション許可を取得する許可を付与	読み取り			
GetSubscriptionRequestDetails	データアセットのサブスクリプションリクエストを拒否する許可を付与	読み取り			
GetSubscriptionTarget	サブスクリプションターゲットの詳細を取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetTimeSeriesDataPoint	Amazon DataZone 内の既存の TimeSeriesDataPoints をその識別子を使用して取得する許可を付与する	読み取り			
GetUpdateEligibility	プロジェクトコンストラクトの更新適格性ステータスを取得する許可を付与	読み取り			
GetUserProfile	DataZone ドメイン内の既存ユーザーのユーザープロファイルを取得する許可を付与	読み取り			
ListAccountEnvironments	AWS アカウント内のすべてのドメインの環境を一覧表示するアクセス許可を付与します	リスト			
ListAccountPools	アカウントプールを一覧表示するアクセス許可を付与します	リスト			
ListAccountsInAccountPool	アカウントプール内のアカウントを一覧表示するアクセス許可を付与します	リスト			
ListAssetFilters	アセットフィルターを一覧表示する許可を付与する	リスト			
ListAssetRevisions	アセットのリビジョンを一覧表示する許可を付与	リスト			
ListConnections	接続を一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListDataProductRevisions	データ製品のリビジョンを一覧表示する許可を付与する	リスト			
ListDataSourceRunActivities	アセット上のデータソースのジョブ実行アクティビティを一覧表示する許可を付与	リスト			
ListDataSourceRuns	データソースのジョブ実行を一覧表示する許可を付与	リスト			
ListDataSources	既存のデータソースを一覧表示する許可を付与	リスト			
ListDomainUnitsForParent	特定の親ドメインユニットの子ドメインユニットを一覧表示する許可を付与する	リスト			
ListDomains	すべてのドメインを取得するための許可を付与	リスト			
ListEntityOwners	ドメインユニットなどのエンティティの所有者を一覧表示する許可を付与する	リスト			
ListEnvironmentActions	デフォルトのサービスブループリント環境の環境アクションを一覧表示する許可を付与する	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListEnvironmentBlueprintConfigurationSummaries [許可のみ]	環境ブループリントの設定の概要を一覧表示する許可を付与する	リスト			
ListEnvironmentBlueprintConfigurations	環境ブループリントの設定を一覧表示する許可を付与	リスト			
ListEnvironmentBlueprints	環境ブループリントのドメインを一覧表示する許可を付与	リスト			
ListEnvironmentProfiles	環境プロファイルのドメインを一覧表示する許可を付与	リスト			
ListEnvironments	ドメイン内の環境を表示する許可を付与	リスト			
ListGroupsForUser	DataZone ユーザープロファイルがメンバーとなっているすべての DataZone グループプロファイルを一覧表示する許可を付与	リスト			
ListJobRuns	ジョブ実行を一覧表示するアクセス許可を付与します	リスト			
ListLineageEvents	系統イベントを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListLineageNodeHistory	系統ノードの履歴バージョンを一覧表示する許可を付与する	リスト			
ListLinkedTypes [許可のみ]	Amazon DataZone ドメインにリンクされたリンクされたタイプ項目を一覧表示するアクセス許可を付与します	リスト	domain*		
ListMetadataGenerationRuns	メタデータ生成実行を一覧表示するためのアクセス許可を付与	リスト			
ListNotifications	DataZone ユーザーへの通知とイベントを一覧表示する許可を付与	リスト			
ListPolicyGrants	ポリシー許可を一覧表示する許可を付与する	リスト			
ListProjectMemberships	プロジェクトメンバーを一覧表示する許可を付与	リスト			
ListProjectProfiles	プロジェクトプロファイルを一覧表示する許可を付与する	リスト			
ListProjects	プロジェクトを一覧表示する許可を付与	リスト			
ListRules	ルールを一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListSubscriptionGrants	サブスクライブ済みプリンシパルのサブスクリプション許可を一覧表示する許可を付与	リスト			
ListSubscriptionRequests	サブスクリプションリクエストを一覧表示する許可を付与	リスト			
ListSubscriptionTargets	サブスクリプションターゲットを一覧表示する許可を付与	リスト			
ListSubscriptions	サブスクリプションを一覧表示する許可を付与	リスト			
ListTagsForResource	リソースに関連付けられているすべてのタグを取得する許可を付与。	読み取り	domain		
ListTimeSeriesDataPoints	既存の TimeSeriesDataPoints を一覧表示する許可を付与する	リスト			
ListWarehouseMetadata [許可のみ]	利用可能な Manager Secrets を一覧表示する許可を付与	リスト			
PostLineageEvent	系統イベントを投稿する許可を付与する	書き込み			
PostTimeSeriesDataPoints	新しい TimeSeriesDataPoints を投稿する許可を付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ProvisionDomain [アクセス許可のみ]	デフォルトのプロジェクト設定でドメインをプロビジョニングする許可を付与	書き込み			
PutDomainSharingPolicy [アクセス許可のみ]	DataZone ドメインのリソースポリシーを追加する許可を付与	権限の管理			
PutEnvironmentBlueprintConfiguration	環境ブループリントの設定を提供する許可を付与	書き込み			
RefreshToken [アクセス許可のみ]	トークンを更新する許可を付与	書き込み			
RejectPredictions	予測を拒否する許可を付与	書き込み			
RejectSubscriptionRequest	データアセットのサブスクリプションリクエストを拒否する許可を付与	書き込み			
RemoveEntityOwner	ドメインユニットなどのエンティティの既存の所有者を削除する許可を付与する	書き込み			
RemovePolicyGrant	ポリシー権限を削除する許可を付与する	権限の管理			
RevokeSubscription	サブスクリプションの取り消しをする許可を付与	権限の管理			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
Search	DataZone エンティティを検索する許可を付与	リスト			
SearchGroupProfiles	DataZone グループプロファイルと IAM アイデンティティセンターグループを検索する許可を付与	リスト			
SearchListings	リスティングを検索する許可を付与	リスト			
SearchRules [許可のみ]	ルールを検索するアクセス許可を付与します	リスト			
SearchTypes	ドメイン内でアセットタイプやフォームタイプなどのタイプを検索する許可を付与	リスト			
SearchUserProfiles	DataZone ユーザープロファイル、IAM アイデンティティセンターユーザー、および DataZone IAM プリンシパルプロファイルを検索する許可を付与	リスト			
SsoLogin [許可のみ]	SSO を使用してログインする許可を付与	書き込み			
SsoLogout [アクセス許可のみ]	SSO ユーザーとしてログアウトする許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartAccountBootstrapAction [アクセス許可のみ]	ドメインのアカウントブートストラップアクションを開始するアクセス許可を付与します	書き込み			
StartDataSourceRun	データソースのジョブ実行を開始する許可を付与	書き込み			
StartMetadataGenerationRun	メタデータ生成実行を開始するためのアクセス許可を付与	書き込み			
StopMetadataGenerationRun	メタデータ生成実行を停止するためのアクセス許可を付与	書き込み			
TagResource	タグをリソースに追加または更新するための許可を付与します	Tagging	domain*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースに関連付けられているタグを削除する許可を付与	Tagging	domain*		
				aws:TagKeys	
UpdateAccountPool	アカウントプールを更新するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateAssetFilter	アセットフィルターを更新する許可を付与する	書き込み			
UpdateConnection	接続を更新するアクセス許可を付与します	書き込み			
UpdateDataSource	既存のデータソースを更新する許可を付与	書き込み			
UpdateDataSourceRunActivities [アクセス許可のみ]	データソース実行アクティビティを更新する許可を付与する	書き込み			
UpdateDomain	ドメインの情報を更新する許可を付与	書き込み	domain*		
UpdateDomainUnit	既存のドメインユニットを更新する許可を付与する	書き込み			
UpdateEnvironment	環境設定を更新する許可を付与	書き込み			
UpdateEnvironmentAction	デフォルトのサービスブループリント環境で環境アクションを更新する許可を付与する	書き込み			
UpdateEnvironmentBlueprint [アクセス許可のみ]	環境ブループリントの設定を更新する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateEnvironmentConfiguration [アクセス許可のみ]	環境設定を更新する許可を付与	書き込み			
UpdateEnvironmentDeploymentStatus [アクセス許可のみ]	環境デプロイメントのステータスを更新する許可を付与	書き込み			
UpdateEnvironmentProfile	環境プロファイル設定を更新する許可を付与	書き込み			
UpdateGlossary	ビジネス用語集を更新する許可を付与	書き込み			
UpdateGlossaryTerm	用語集の用語を更新する許可を付与	書き込み			
UpdateGroupProfile	DataZone グループプロファイルを更新する許可を付与	書き込み			
UpdateProject	チームによるデータの公開とサブスクリプションを可能にするプロジェクトを更新する許可を付与	書き込み			
UpdateProjectProfile	プロジェクトプロファイルを更新する許可を付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateRule	ルールを更新するアクセス許可を付与します	書き込み			
UpdateSubscriptionGrantStatus	カスタム許可へのサブスクリプション許可の状態を更新する許可を付与	書き込み			
UpdateSubscriptionRequest	データアセットのサブスクリプションリクエストに対するビジネス上の理由を更新する許可を付与	書き込み			
UpdateSubscriptionTarget	サブスクリプションターゲットを更新する許可を付与	書き込み			
UpdateUserProfile	DataZone ユーザープロファイルを更新する許可を付与	書き込み			
ValidatePassRole [アクセス許可のみ]	パスロールを検証する許可を付与	書き込み			

Amazon DataZone によって定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
domain	arn:${Partition}:datazone:${Region}:${Account}:domain/${DomainId}	aws:ResourceTag/${TagKey}

Amazon DataZone の条件キー

Amazon DataZone は、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
datazone:domainId	リクエストで渡されたドメイン ID でアクセスをフィルタリングします	String
datazone:projectId	リクエストで渡されたプロジェクト ID でアクセスをフィルタリングします	String
datazone:userId	リクエストで渡されたユーザー ID でアクセスをフィルタリングします	String

AWS Deadline Cloud のアクション、リソース、および条件キー

AWS Deadline Cloud (サービスプレフィックス: deadline) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Deadline Cloud で定義されるアクション
- AWS Deadline Cloud で定義されるリソースタイプ
- AWS Deadline Cloud の条件キー

AWS Deadline Cloud で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateMemberToFarm	メンバーをファームに関連付ける許可を付与する	権限の管理	farm*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	
AssociateMemberToFleet	メンバーをフリートに関連付ける許可を付与する	権限の管理	fleet*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateMemberToJob	メンバーをジョブに関連付ける許可を付与する	権限の管理	job*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateMemberToQueue	メンバーをキューに関連付ける許可を付与する	権限の管理	queue*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	
AssumeFleetRoleForRead	読み取り専用アクセスのフリートロールを引き受ける許可を付与する	書き込み	fleet*		identitystore:ListGroupMembershipsForMember
AssumeFleetRoleForWorker	ワーカーのフリートロールを引き受ける許可を付与する	書き込み	worker*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssumeQueueRoleForRead	読み取り専用アクセスのキューロールを引き受ける許可を付与する	書き込み	queue*		identitystore:ListGroupMembershipsForMember
AssumeQueueRoleForUser	ユーザーのキューロールを引き受ける許可を付与する	書き込み	queue*		identitystore:ListGroupMembershipsForMember
AssumeQueueRoleForWorker	ワーカーのキューロールを引き受ける許可を付与する	書き込み	queue*		
			worker*		
BatchGetJobEntity	ワーカーのジョブエンティティを取得する許可を付与する	読み取り	worker*		
CopyJobTemplate	ジョブテンプレートを Amazon S3 バケットにコピーする許可を付与する	書き込み	job*		identitystore:ListGroupMembershipsForMember s3:PutObject
CreateBudget	予算を作成する許可を付与する	書き込み	budget*		identitystore:ListGroupMembershipsForMember

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateFarm	ファームを作成する許可を付与する	書き込み	farm*		deadline:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateFleet	フリートを作成する許可を付与	書き込み	fleet*		deadline:TagResource ec2:CreateVpcEndpoint iam:PassRole identitystore:ListGroupMembershipsForMember logs:CreateLogGroup vpc-lattice:GetResourceConfiguration vpc-lattice:GetResourceGateway

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJob	ジョブを作成する許可を付与。	書き込み	job*		deadline:GetJobTemplate identitystore:ListGroupMembershipsForMember
CreateLicenseEndpoint	ライセンスされたソフトウェアまたは製品のライセンスエンドポイントを作成する許可を付与する	書き込み	license-endpoint*		deadline:TagResource ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeVpcEndpoints

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLimit	ファームの制限を作成するアクセス許可を付与します	書き込み	farm*		identitystore:ListGroupMembershipsForMember

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateMonitor	モニターを作成するための許可を付与します	書き込み	monitor*		deadline:TagResource iam:PassRole sso:CreateApplication sso:DeleteApplication sso:PutApplicationAssignmentConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateQueue	キューを作成する許可を付与する	書き込み	queue*		deadline:TagResource iam:PassRole identitystore:ListGroupMembershipsForMember logs:CreateLogGroup s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateQueueEnvironment	キュー環境を作成する許可を付与する	書き込み	queue*		identitystore:ListGroupMembershipsForMember
CreateQueueFleetAssociation	キューフリートの関連付けを作成する許可を付与する	書き込み	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
CreateQueueLimitAssociation	キュー制限の関連付けを作成するアクセス許可を付与します	書き込み	farm*		identitystore:ListGroupMembershipsForMember
			queue*		
CreateStorageProfile	ファームのストレージプロファイルを作成する許可を付与する	書き込み	farm*		identitystore:ListGroupMembershipsForMember

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateWorker	ワーカーを作成するアクセス許可を付与します。	書き込み	worker*		deadline:ListTagsForResource deadline:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBudget	予算を削除する許可を付与する	書き込み	budget*		identitystore:ListGroupMembershipsForMember
DeleteFarm	ファームを削除する許可を付与する	書き込み	farm*		identitystore:ListGroupMembershipsForMember
DeleteFleet	フリートを削除するアクセス許可を付与	書き込み	fleet*		identitystore:ListGroupMembershipsForMember

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteLicenseEndpoint	ライセンスエンドポイントを削除する許可を付与する	書き込み	license-endpoint*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints
DeleteLimit	制限を削除するアクセス許可を付与します	書き込み	farm*		identitystore:ListGroupMembershipsForMember
DeleteMeteredProduct	従量制製品を削除する許可を付与する	書き込み	metered-product*		
DeleteMonitor	モニターを削除するための許可を付与します	書き込み	monitor*		sso:DeleteApplication
DeleteQueue	キューを削除する許可を付与する	書き込み	queue*		identitystore:ListGroupMembershipsForMember
DeleteQueueEnvironment	キュー環境を削除する許可を付与する	書き込み	queue*		identitystore:ListGroupMembershipsForMember

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteQueueFleetAssociation	キューとフリートの関連付けを削除する許可を付与する	書き込み	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
DeleteQueueLimitAssociation	キューと制限の関連付けを削除するアクセス許可を付与します	書き込み	farm*		identitystore:ListGroupMembershipsForMember
			queue*		
DeleteStorageProfile	ストレージプロファイルを削除する許可を付与する	書き込み	farm*		identitystore:ListGroupMembershipsForMember
DeleteWorker	ワーカーを削除するアクセス許可を付与します。	書き込み	worker*		
DisassociateMemberFromFarm	ファームからメンバーの関連付けを解除する許可を付与する	権限の管理	farm*		identitystore:ListGroupMembershipsForMember

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				deadline:AssociatedMembershipLevel	
DisassociateMemberFromFleet	フリートからメンバーの関連付けを解除する許可を付与する	権限の管理	fleet*		identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel	
DisassociateMemberFromJob	ジョブからメンバーの関連付けを解除する許可を付与する	権限の管理	job*		identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel	
DisassociateMemberFromQueue	キューから根場–の関連付けを解除する許可を付与する	権限の管理	queue*		identitystore:ListGroupMembershipsForMember

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				deadline:AssociatedMembershipLevel	
GetApplicationVersion	アプリケーションの最新のバージョンを取得する許可を付与する	読み取り	monitor*		
GetBudget	予算を取得する許可を付与する	読み取り	budget*		identitystore:ListGroupMembershipsForMember
GetFarm	ファームを取得する許可を付与する	読み取り	farm*		identitystore:ListGroupMembershipsForMember
GetFleet	フリートを取得する許可を付与する	読み取り	fleet*		identitystore:ListGroupMembershipsForMember
GetJob	ジョブを取得する許可を付与する	読み取り	job*		identitystore:ListGroupMembershipsForMember

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetJobTemplate [許可のみ]	ジョブテンプレートを読み込む許可を付与する	読み取り	job*		
GetLicenseEndpoint	ライセンスエンドポイントを取得する許可を付与する	読み取り	license-endpoint*		
GetLimit	制限を取得するアクセス許可を付与します	読み取り	farm*		identitystore:ListGroupMembershipsForMember
GetMonitor	モニタを取得する許可を付与する	読み取り	monitor*		
GetQueue	キューを取得する許可を付与する	読み取り	queue*		identitystore:ListGroupMembershipsForMember
GetQueueEnvironment	キュー環境を取得する許可を付与する	読み取り	queue*		identitystore:ListGroupMembershipsForMember
GetQueueFleetAssociation	キューフリートの関連付けを取得する許可を付与する	読み取り	fleet*		identitystore:ListGroupMembershipsForMember

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			queue*		
GetQueueLimitAssociation	キュー制限の関連付けを取得するアクセス許可を付与します	読み取り	farm*		identitystore:ListGroupMembershipsForMember
			queue*		
GetSession	ジョブのセッションを取得する許可を付与する	読み取り	job*		identitystore:ListGroupMembershipsForMember
GetSessionAction	ジョブのセッションアクションを取得する許可を付与する	読み取り	job*		identitystore:ListGroupMembershipsForMember
GetSessionsStatisticsAggregation	セッションに対して収集されたすべての統計を取得する許可を付与する	読み取り	farm		identitystore:ListGroupMembershipsForMember
			fleet		
			queue		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetStep	ジョブのステップを取得する許可を付与する	読み取り	job*		identitystore:ListGroupMembershipsForMember
GetStorageProfile	ストレージプロファイルを取得する許可を付与する	読み取り	farm*		identitystore:ListGroupMembershipsForMember
GetStorageProfileForQueue	キューのストレージプロファイルを取得する許可を付与する	読み取り	queue*		identitystore:ListGroupMembershipsForMember
GetTask	ジョブタスクを取得する許可を付与する	読み取り	job*		identitystore:ListGroupMembershipsForMember
GetWorker	ワーカーを取得する許可を付与します。	読み取り	worker*		identitystore:ListGroupMembershipsForMember
ListAvailableMeteredProducts	ライセンスエンドポイント内で使用可能なすべての従量制製品を一覧表示する許可を付与する	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListBudgets	ファームのすべての予算を一覧表示する許可を付与する	リスト	budget*		identitystore:ListGroupMembershipsForMember
ListFarmMembers	ファームのメンバー全員を一覧表示する許可を付与する	リスト	farm*		identitystore:ListGroupMembershipsForMember
ListFarms	すべてのファームを一覧表示する許可を付与する	リスト	farm*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:PrincipalId deadline:RequesterPrincipalId	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListFleetMembers	フリートのメンバー全員を一覧表示する許可を付与する	リスト	fleet*		identitystore:ListGroupMembershipsForMember
ListFleets	すべてのフリートを一覧表示するアクセス許可を付与	リスト	fleet*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListJobMembers	ジョブのメンバー全員を一覧表示する許可を付与する	リスト	job*		identitystore:ListGroupMembershipsForMember

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListJobParameterDefinitions	ジョブテンプレートでジョブのパラメータ定義を取得する許可を付与する	リスト	job*		identitystore:ListGroupMembershipsForMember
ListJobs	キューのすべてのジョブを一覧表示する許可を付与する	リスト	job*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListLicenseEndpoints	すべてのライセンスエンドポイントを一覧表示する許可を付与する	リスト	license-endpoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListLimits	ファーム内のすべての制限を一覧表示するアクセス許可を付与します	リスト	farm*		identitystore:ListGroupMembershipsForMember
ListMeteredProducts	ライセンスエンドポイント内のすべての従量制製品を一覧表示する許可を付与する	リスト	metered-product*		
ListMonitors	すべてのモニタを一覧表示する許可を付与する	リスト	monitor*		
ListQueueEnvironments	キューが関連付けられているすべてのキュー環境を一覧表示する許可を付与する	リスト	queue*		identitystore:ListGroupMembershipsForMember
ListQueueFleetAssociations	すべてのキューフリートの関連付けを一覧表示する許可を付与する	リスト	farm*		identitystore:ListGroupMembershipsForMember
			fleet*		
			queue*		
ListQueueLimitAssociations	すべてのキューと制限の関連付けを一覧表示するアクセス許可を付与します	リスト	farm*		identitystore:ListGroupMembershipsForMember

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			queue*		
ListQueueMembers	キューのすべてのメンバーを一覧表示する許可を付与する	リスト	queue*		identitystore:ListGroupMembershipsForMember
ListQueues	ファーム上のすべてのキューを一覧表示する許可を付与する	リスト	queue*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:PrincipalId deadline:RequesterPrincipalId	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListSessionActions	ジョブのすべてのセッションアクションを一覧表示する許可を付与する	リスト	job*		identitystore:ListGroupMembershipsForMember
ListSessions	ジョブのすべてのセッションを一覧表示する許可を付与する	リスト	job*		identitystore:ListGroupMembershipsForMember
ListSessionsForWorker	ワーカーのすべてのセッションを一覧表示する許可を付与する	リスト	worker*		identitystore:ListGroupMembershipsForMember
ListStepConsumers	ジョブステップのステップコンシューマーを一覧表示する許可を付与する	リスト	job*		identitystore:ListGroupMembershipsForMember
ListStepDependencies	ジョブステップの依存関係を一覧表示する許可を付与する	リスト	job*		identitystore:ListGroupMembershipsForMember

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListSteps	ジョブのすべてのステップを一覧表示する許可を付与する	リスト	job*		identitystore:ListGroupMembershipsForMember
ListStorageProfiles	ファーム内のすべてのストレージプロファイルを一覧表示する許可を付与する	リスト	farm*		identitystore:ListGroupMembershipsForMember
ListStorageProfilesForQueue	キュー内のすべてのストレージプロファイルを一覧表示する許可を付与する	リスト	queue*		identitystore:ListGroupMembershipsForMember
ListTagsForResource	指定された Deadline Cloud リソースのすべてのタグを一覧表示する許可を付与する	リスト	farm		
			fleet		
			license-endpoint		
			monitor		
			queue		
			worker		
				deadline:CalledAction	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTasks	ジョブのすべてのタスクを一覧表示する許可を付与する	リスト	job*		identitystore:ListGroupMembershipsForMember
ListWorkers	フリート内のすべてのワーカーを一覧表示する許可を付与する	リスト	worker*		identitystore:ListGroupMembershipsForMember
PutMeteredProduct	ライセンスエンドポイントに従量制製品を追加する許可を付与する	書き込み	metered-product*		
SearchJobs	複数のキュー内のジョブを検索する許可を付与する	リスト	queue*		identitystore:ListGroupMembershipsForMember
SearchSteps	1 つのジョブ内のステップを検索するか、複数のキューのステップを検索する許可を付与する	リスト	job		identitystore:ListGroupMembershipsForMember
			queue		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SearchTasks	1 つのジョブ内のタスクを検索するか、複数のキューのタスクを検索する許可を付与する	リスト	job		identitystore:ListGroupMembershipsForMember
			queue		
SearchWorkers	複数のフリートのワーカーを検索する許可を付与する	リスト	fleet*		identitystore:ListGroupMembershipsForMember
StartSessionsStatisticsAggregation	セッションに対して収集されたすべての統計を取得する許可を付与する	読み取り	fleet		identitystore:ListGroupMembershipsForMember
			queue		
TagResource	指定した Deadline Cloud リソースの 1 つ以上のタグを追加または上書きするアクセス許可を付与する	Tagging	farm		
			fleet		
			license-endpoint		
			monitor		
			queue		
			worker		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys deadline:CalledAction	
UntagResource	指定された Deadline Cloud リソースから 1 つ以上のタグの関連付けを解除する許可を付与する	Tagging	farm		
			fleet		
			license-endpoint		
			monitor		
			queue		
			worker		
				aws:TagKeys	
UpdateBudget	予算を更新する許可を付与する	書き込み	budget*		identitystore:ListGroupMembershipsForMember

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateFarm	ファームを更新する許可を付与する	書き込み	farm*		identitystore:ListGroupMembershipsForMember
UpdateFleet	フリートを更新する許可を付与する	書き込み	fleet*		ec2:CreateVpcEndpoint iam:PassRole identitystore:ListGroupMembershipsForMember vpc-lattice:GetResourceConfiguration vpc-lattice:GetResourceGateway
UpdateJob	ジョブを更新する許可を付与。	書き込み	job*		identitystore:ListGroupMembershipsForMember

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateLimit	ファームの制限を更新するアクセス許可を付与します	書き込み	farm*		identitystore:ListGroupMembershipsForMember
UpdateMonitor	モニターを更新するための許可を付与します	書き込み	monitor*		iam:PassRole sso:PutApplicationGrant sso:UpdateApplication
UpdateQueue	キューを更新する許可を付与する	書き込み	queue*		iam:PassRole identitystore:ListGroupMembershipsForMember
UpdateQueueEnvironment	キュー環境を更新する許可を付与する	書き込み	queue*		identitystore:ListGroupMembershipsForMember

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateQueueFleetAssociation	キューとフリートの関連付けを更新する許可を付与する	書き込み	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
UpdateQueueLimitAssociation	キューと制限の関連付けを更新するアクセス許可を付与します	書き込み	farm*		identitystore:ListGroupMembershipsForMember
			queue*		
UpdateSession	ジョブのセッションを更新する許可を付与する	書き込み	job*		identitystore:ListGroupMembershipsForMember
UpdateStep	ジョブのステップを更新する許可を付与する	書き込み	job*		identitystore:ListGroupMembershipsForMember
UpdateStorageProfile	ファームのストレージプロファイルを更新する許可を付与する	書き込み	farm*		identitystore:ListGroupMembershipsForMember

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateTask	タスクを更新するアクセス許可を付与します。	書き込み	job*		identitystore:ListGroupMembershipsForMember
UpdateWorker	ワーカーを更新する許可を付与します。	書き込み	worker*		logs:CreateLogStream
UpdateWorkerSchedule	ワーカーのスケジュールを更新する許可を付与する	書き込み	worker*		logs:CreateLogStream

AWS Deadline Cloud で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
budget	`arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/budget/${BudgetId}`	deadline:FarmMembershipLevels
farm	`arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
		deadline:FarmMembershipLevels
fleet	arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/fleet/${FleetId}	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels deadline:FleetMembershipLevels
job	arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/queue/${QueueId}/job/${JobId}	deadline:FarmMembershipLevels deadline:JobMembershipLevels deadline:QueueMembershipLevels
license-endpoint	arn:${Partition}:deadline:${Region}:${Account}:license-endpoint/${LicenseEndpointId}	aws:ResourceTag/${TagKey}
metered-product	arn:${Partition}:deadline:${Region}:${Account}:license-endpoint/${LicenseEndpointId}/metered-product/${ProductId}	
monitor	arn:${Partition}:deadline:${Region}:${Account}:monitor/${MonitorId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
queue	arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/queue/${QueueId}	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels deadline:QueueMembershipLevels
worker	arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/fleet/${FleetId}/worker/${WorkerId}	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels deadline:FleetMembershipLevels

AWS Deadline Cloud の条件キー

AWS Deadline Cloud は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列

条件キー	説明	タイプ
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
deadline:AssociatedMembershipLevel	リクエストで指定されたプリンシパルの関連付けられたメンバーシップレベルによってアクセスをフィルタリングする	String
deadline:CalledAction	リクエストで許可されたアクションでアクセスをフィルタリングします	String
deadline:FarmMembershipLevels	ファームのメンバーシップレベルでアクセスをフィルタリングする	ArrayOfString
deadline:FleetMembershipLevels	フリートのメンバーシップレベルでアクセスをフィルタリングする	ArrayOfString
deadline:JobMembershipLevels	ジョブのメンバーシップレベルでアクセスをフィルタリングする	ArrayOfString
deadline:MembershipLevel	リクエストで渡されたメンバーシップレベル別にアクセスをフィルタリングする	String
deadline:PrincipalId	リクエストで指定されたプリンシパル ID でアクセスをフィルタリングする	String
deadline:QueueMembershipLevels	キューのメンバーシップレベルでアクセスをフィルタリングする	ArrayOfString
deadline:RequesterPrincipalId	Deadline Cloud API を呼び出すユーザーによってアクセスをフィルタリングする	String

AWS DeepComposer のアクション、リソース、および条件キー

AWS DeepComposer (サービスプレフィックス: deepcomposer) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS DeepComposer で定義されるアクション
- AWS DeepComposer で定義されるリソースタイプ
- AWS DeepComposer の条件キー

AWS DeepComposer で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateCoupon [アクセス許可のみ]	リクエストの送信者に関連付けられたアカウントに DeepComposer クーポン (または DSN) を関連付けるためのアクセス許可を付与	Write			
CreateAudio [アクセス許可のみ]	MIDI コンポジションを wav または mp3 ファイルに変換して、オーディオファイルを作成するためのアクセス許可を付与	Write	audio*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateComposition [アクセス許可のみ]	マルチトラックの MIDI コンポジションを作成するためのアクセス許可を付与	Write	composition*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModel [アクセス許可のみ]	ユーザー提供のピアノメロディーに対する推論を実行し、マルチトラックの MIDI コンポジションを作成できるジェネレーティブモデルの作成/トレーニングを開始するためのアクセス許可を付与	Write	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComposition [アクセス許可のみ]	コンポジションを削除するためのアクセス許可を付与	Write	composition*		
DeleteModel	モデルを削除するためのアクセス許可を付与	Write	model*		
GetComposition [アクセス許可のみ]	コンポジションに関する情報を取得するためのアクセス許可を付与	Read	composition*		
				aws:ResourceTag/${TagKey}	
GetModel [許可のみ]	モデルに関する情報を取得するためのアクセス許可を付与	Read	model*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
GetSampleModel [許可のみ]	サンプル/事前トレーニング済みの DeepComposer モデルに関する情報を取得するためのアクセス許可を付与	Read	model*		
ListCompositions [許可のみ]	リクエストの送信者が所有するすべてのコンポジションを一覧表示するためのアクセス許可を付与	リスト	composition*		
ListModels [許可のみ]	リクエストの送信者が所有するすべてのモデルを一覧表示するためのアクセス許可を付与	リスト	model*		
ListSampleModels [許可のみ]	DeepComposer サービスによって提供されるサンプル/事前トレーニング済みのすべてのモデルを一覧表示するためのアクセス許可を付与	リスト	model*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与。	リスト	composition		
			model		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTrainingTopics [許可のみ]	モデルの作成/トレーニングに関するすべてのトレーニングオプションまたはトピックを一覧表示するためのアクセス許可を付与	リスト	model*		
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	composition		
			model		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	リソースのタグを解除する許可を付与	タグ付け	composition		
			model		
				aws:TagKeys aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateComposition [アクセス許可のみ]	コンポジションに関連付けられた変更可能なプロパティを変更するためのアクセス許可を付与	Write	composition*		
UpdateModel [アクセス許可のみ]	モデルに関連付けられた変更可能なプロパティを変更するためのアクセス許可を付与	Write	model*		

AWS DeepComposer で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
model	arn:${Partition}:deepcomposer:${Region}:${Account}:model/${ModelId}	aws:ResourceTag/${TagKey}
composition	arn:${Partition}:deepcomposer:${Region}:${Account}:composition/${CompositionId}	aws:ResourceTag/${TagKey}
audio	arn:${Partition}:deepcomposer:${Region}:${Account}:audio/${AudioId}	

AWS DeepComposer の条件キー

AWS DeepComposer では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーおよび値のペアのプレゼンスに基づいてアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアに基づいてアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいたアクションでアクセスをフィルタリングします	ArrayOfString

AWS DeepRacer のアクション、リソース、および条件キー

AWS DeepRacer (サービスプレフィックス: deepracer) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS DeepRacer で定義されるアクション
- AWS DeepRacer で定義されるリソースタイプ

- AWS DeepRacer の条件キー

AWS DeepRacer で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AddLeaderboardAccessPermission [アクセス許可のみ]	プライベートリーダーボードへのアクセスを追加する許可を付与	書き込み	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
AdminDescribeAccountKey [アクセス許可のみ]	ユーザーが現在自分のアカウントに割り当てた KMS キーの情報を取得するアクセス許可を付与します	読み取り		deepracer:UserToken deepracer:MultiUser	
AdminGetAccountConfig [許可のみ]	このアカウントの現在の管理者マルチユーザー設定を取得する許可を付与	読み込み			
AdminListAssociatedResources [許可のみ]	このアカウントで作成されたすべての DeepRacer ユーザーとその関連リソースを一覧表示する許可を付与	読み込み			
AdminListAssociatedUsers [許可のみ]	このアカウントに関連付けられているすべてのユーザーのユーザーデータを一覧表示する許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AdminManageUser [許可のみ]	このアカウントに関連付けられているユーザーを管理する許可を付与	書き込み			
AdminSetAccountConfig [アクセス許可のみ]	このアカウントの設定オプションを設定する許可を付与	書き込み			
AdminUpdateAccountKey [アクセス許可のみ]	ユーザーのアカウントに割り当てられた KMS キーを更新するアクセス許可を付与します	書き込み		deepracer:UserToken deepracer:MultiUser	
CloneReinforcementLearningModel [アクセス許可のみ]	既存の DeepRacer モデルのクローンを作成する許可を付与	書き込み	reinforcement_learning_model* track*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	
CreateCar [アクセス許可のみ]	ガレージで DeepRacer カーを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateLeaderboard [アクセス許可のみ]	リーダーボードを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	
CreateLeaderboardAccessToken [アクセス許可のみ]	プライベートリーダーボードのアクセストークンを作成する許可を付与	書き込み	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
CreateLeaderboardSubmission [アクセス許可のみ]	リーダーボードで評価する DeepRacer モデルを送信する許可を付与	書き込み	leaderboard*		
			reinforcement_learning_model*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	
CreateReinforcementLearningModel [アクセス許可のみ]	DeepRacer の強化学習モデルを作成する許可を付与	書き込み	track*		
				aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteLeaderboard [アクセス許可のみ]	リーダーボードを削除する許可を付与	書き込み	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
DeleteModel [アクセス許可のみ]	DeepRacer モデルを削除する許可を付与	書き込み	reinforcement_learning_model*		
				deepracer:UserToken deepracer:MultiUser	
EditLeaderboard [アクセス許可のみ]	リーダーボードを編集する許可を付与	書き込み	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetAccountConfig [アクセス許可のみ]	このアカウントの現在のマルチユーザー設定を取得する許可を付与	読み込み		deepracer:UserToken deepracer:MultiUser	
GetAlias [許可のみ]	リーダーボードに DeepRacer モデルを送信するためのユーザーのエイリアスを取得する許可を付与	読み込み		deepracer:UserToken deepracer:MultiUser	
GetAssetUrl [許可のみ]	既存のDeepRacer モデルの Artifact をダウンロードする許可を付与	読み込み	reinforcement_learning_model*		
				deepracer:UserToken deepracer:MultiUser	
GetCar [許可のみ]	ガレージから特定の DeepRacer カーを回収する許可を付与	読み込み	car*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				deepracer:UserToken deepracer:MultiUser	
GetCars [許可のみ]	ガレージ内のすべての DeepRacer カーを表示する許可を付与	読み込み		deepracer:UserToken deepracer:MultiUser	
GetEvaluation [許可のみ]	既存の DeepRacer モデルの評価ジョブに関する情報を取得する許可を付与	読み込み	evaluation_job*		
				deepracer:UserToken deepracer:MultiUser	
GetLatestUserSubmission [許可のみ]	リーダーボードで最後に送信されたユーザーの DeepRacer モデルがどのようなパフォーマンスを発揮したかに関する情報を取得する許可を付与。	読み込み	leaderboard*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				deepracer:UserToken deepracer:MultiUser	
GetLeaderboard [許可のみ]	リーダーボードに関する情報を取得する許可を付与。	読み込み	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
GetModel [許可のみ]	既存の DeepRacer モデルに関する情報を取得する許可を付与	読み込み	reinforcement_learning_model*		
				deepracer:UserToken deepracer:MultiUser	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetPrivateLeaderboard [許可のみ]	リーダーボードに関する情報を取得する許可を付与	読み込み	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
GetRankedUserSubmission [許可のみ]	リーダーボードに掲示されたユーザーの DeepRacer モデルのパフォーマンスに関する情報を取得する許可を付与。	読み込み	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
GetTrack [許可のみ]	DeepRacer トラックに関する情報を取得する許可を付与。	読み込み	track*		
GetTrainingJob [許可のみ]	既存の DeepRacer モデルのトレーニングジョブに関する情報を取得する許可を付与	読み込み	training_job*		
				deepracer:UserToken deepracer:MultiUser	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ImportModel [許可のみ]	DeepRacer の強化学習モデルをインポートする許可を付与	書き込み		deepracer:UserToken deepracer:MultiUser	
ListEvaluations [アクセス許可のみ]	DeepRacer モデルの評価ジョブを一覧表示する許可を付与	読み込み	reinforcement_learning_model*		
				deepracer:UserToken deepracer:MultiUser	
ListLeaderboardEvaluations [許可のみ]	リーダーボードに対するユーザーのリーダーボード評価ジョブをすべて一覧表示するアクセス許可を付与	読み取り	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListLeaderboardSubmissions [許可のみ]	リーダーボードにユーザーの DeepRacer モデルのすべての送信を一覧表示する許可を付与	読み込み	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
ListLeaderboards [許可のみ]	使用可能なすべてのリーダーボードをリストする許可を付与。	読み込み		deepracer:UserToken deepracer:MultiUser	
ListModels [許可のみ]	既存のすべての DeepRacer モデルをリストする許可を付与。	読み込み		deepracer:UserToken deepracer:MultiUser	
ListPrivateLeaderboardParticipants [許可のみ]	プライベートリーダーボードに関する参加者情報を取得する許可を付与	読み込み	leaderboard*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				deepracer:UserToken deepracer:MultiUser	
ListPrivateLeaderboards [許可のみ]	使用可能なすべてのプライベートリーダーボードを一覧表示する許可を付与	読み込み		deepracer:UserToken deepracer:MultiUser	
ListSubscribedPrivateLeaderboards [許可のみ]	サブスクライブしているすべてのプライベートリーダーボードを一覧表示する許可を付与	読み込み		deepracer:UserToken deepracer:MultiUser	
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み込み	car		
			evaluation_job		
			leaderboard		
			leaderboard_evaluation_job		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			reinforcement_learning_model		
			training_job		
				aws:ResourceTag/${TagKey} deepracer:UserToken deepracer:MultiUser	
ListTracks [許可のみ]	すべての DeepRacer トラックをリストする許可を付与。	読み込み			
ListTrainingJobs [許可のみ]	DeepRacer モデルのトレーニングジョブを一覧表示する許可を付与	読み込み	reinforcement_learning_model*		
				deepracer:UserToken deepracer:MultiUser	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
MigrateModels [許可のみ]	DeepRacer の以前の強化学習モデルを移行する許可を付与	書き込み			
PerformLeaderboardOperation [アクセス許可のみ]	オペレーション属性で指定されたリーダーボードオペレーションを実行する許可を付与	書き込み	leaderboard		
				deepracer:UserToken deepracer:MultiUser	
RemoveLeaderboardAccessPermission [アクセス許可のみ]	プライベートリーダーボードへのアクセスを削除する許可を付与	書き込み	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
SetAlias [アクセス許可のみ]	リーダーボードに DeepRacer モデルを送信するためのユーザーのエイリアスを設定する許可を付与	書き込み		deepracer:UserToken deepracer:MultiUser	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartEvaluation [アクセス許可のみ]	シミュレートされた環境で DeepRacer モデルを評価する許可を付与	書き込み	reinforcement_learning_model*		
			track*		
				aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	
StopEvaluation [アクセス許可のみ]	DeepRacer モデルの評価を停止する許可を付与。	書き込み	evaluation_job*		
				deepracer:UserToken deepracer:MultiUser	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StopTrainingReinforcementLearningModel [アクセス許可のみ]	DeepRacer モデルのトレーニングを停止する許可を付与	書き込み	reinforcement_learning_model*		
				deepracer:UserToken deepracer:MultiUser	
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	car		
			evaluation_job		
			leaderboard		
			leaderboard_evaluation_job		
			reinforcement_learning_model		
			training_job		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} deepracer:UserToken deepracer:MultiUser	
TestRewardFunction [アクセス許可のみ]	報酬関数の正確性をテストする許可を付与。	書き込み			
UntagResource	リソースのタグを解除する許可を付与	タグ付け	car		
			evaluation_job		
			leaderboard		
			leaderboard_evaluation_job		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			reinforcement_learning_model		
			training_job		
				aws:TagKeys deepracer:UserToken deepracer:MultiUser	
UpdateCar [アクセス許可のみ]	ガレージ内の DeepRacer カーを更新する許可を付与	書き込み	car*		
				deepracer:UserToken deepracer:MultiUser	

AWS DeepRacer で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
car	arn:${Partition}:deepracer:${Region}:${Account}:car/${ResourceId}	aws:ResourceTag/${TagKey}
evaluation_job	arn:${Partition}:deepracer:${Region}:${Account}:evaluation_job/${ResourceId}	aws:ResourceTag/${TagKey}
leaderboard	arn:${Partition}:deepracer:${Region}::leaderboard/${ResourceId}	aws:ResourceTag/${TagKey}
leaderboard_evaluation_job	arn:${Partition}:deepracer:${Region}:${Account}:leaderboard_evaluation_job/${ResourceId}	aws:ResourceTag/${TagKey}
reinforcement_learning_model	arn:${Partition}:deepracer:${Region}:${Account}:model/reinforcement_learning/${ResourceId}	aws:ResourceTag/${TagKey}
track	arn:${Partition}:deepracer:${Region}::track/${ResourceId}	
training_job	arn:${Partition}:deepracer:${Region}:${Account}:training_job/${ResourceId}	aws:ResourceTag/${TagKey}

AWS DeepRacer の条件キー

AWS DeepRacer では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString
deepracer:MultiUser	マルチユーザーフラグでアクセスをフィルタリングします	Bool
deepracer:UserToken	リクエスト内のユーザートークンでアクセスをフィルタリングします	String

Amazon Detective のアクション、リソース、および条件キー

Amazon Detective (サービスプレフィックス: `detective`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Detective で定義されるアクション
- Amazon Detective で定義されるリソースタイプ
- Amazon Detective の条件キー

Amazon Detective で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptInvitation	動作グラフのメンバーになるための招待を受け入れるアクセス許可を付与	書き込み	Graph*		
BatchGetGraphMemberDatasources	このアカウントによって管理される動作グラフで、指定されたメンバーアカウントのデータソースパッケージ履歴を取得する許可を付与	読み取り	Graph*		
BatchGetMembershipDatasources	指定されたグラフの呼び出し元アカウントのデータソースパッケージ履歴を取得する許可を付与	読み取り			
CreateGraph	動作グラフを作成してセキュリティ情報の集約を開始する許可を付与。	Write		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	detective:TagResource
CreateMembers	このアカウントによって管理される動作グラフで 1 つ以上のアカウントのメンバーシップをリクエストする許可を付与。	Write	Graph*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteGraph	動作グラフを削除してセキュリティ情報の集約を停止する許可を付与。	Write	Graph*		
DeleteMembers	このアカウントによって管理される動作グラフからメンバーアカウントを削除する許可を付与。	書き込み	Graph*		
DescribeOrganizationConfiguration	Amazon Detective と AWS Organizations の統合に関連する現在の設定を表示するアクセス許可を付与します	読み取り	Graph*		organizations:DescribeOrganization
DisableOrganizationAdminAccount	組織の Amazon Detective 委任管理者アカウントを削除する許可を付与	書き込み			organizations:DescribeOrganization
DisassociateMembership	このアカウントと動作グラフとの関連付けを削除する許可を付与。	書き込み	Graph*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
EnableOrganizationAdminAccount	組織の Amazon Detective 委任管理者アカウントを指定する許可を付与	書き込み			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:RegisterDelegatedAdministrator
GetFreeTrialEligibility [アクセス許可のみ]	無料トライアル期間における動作グラフの資格を取得する許可を付与。	Read	Graph*		
GetGraphIngestState [許可のみ]	動作グラフのデータ取り込み状態を取得する許可を付与。	読み取り	Graph*		
GetInvestigation	調査のステータスとメタデータを取得するためのアクセス許可を付与	読み取り	Graph*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetMembers	動作グラフの指定されたメンバーの詳細を取得する許可を付与。	Read	Graph*		
GetPricingInformation [許可のみ]	Amazon Detective の料金に関する情報を取得する許可を付与。	Read			
GetUsageInformation [許可のみ]	動作グラフの使用状況の情報を一覧表示する許可を付与。	読み取り	Graph*		
InvokeAssistant [許可のみ]	Detective の支援を呼び出すためのアクセス許可を付与	読み取り	Graph*		
ListDatasourcePackages	このアカウントによって管理される動作グラフで、グラフのデータソースパッケージの取り込み状態および最新の状態変更のタイムスタンプを一覧表示する許可を付与	リスト	Graph*		
ListGraphs	このアカウントによって管理される動作グラフを一覧表示する許可を付与。	リスト			
ListHighDegreeEntities [許可のみ]	Detective によるリレーションシップの保存ができない大量のエンティティを取得する許可を付与	リスト	Graph*		
ListIndicators	調査の指標を一覧表示するためのアクセス許可を付与	リスト	Graph*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListInvestigations	動作グラフの調査を一覧表示するためのアクセス許可を付与	リスト	Graph*		
ListInvitations	このアカウントへ参加を招待した動作グラフの詳細を取得する許可を付与。	リスト			
ListMembers	動作グラフのすべてのメンバーの詳細を取得する許可を付与。	リスト	Graph*		
ListOrganizationAdminAccount	組織の現在の Amazon Detective 委任管理者アカウントを表示する許可を付与	リスト			organizations:DescribeOrganization
ListTagsForResource	動作グラフに割り当てられたタグ値を一覧表示する許可を付与。	リスト	Graph*		
				aws:ResourceTag/${TagKey}	
RejectInvitation	動作グラフのメンバーになるための招待を拒否する許可を付与。	Write	Graph*		
SearchGraph [アクセス許可のみ]	動作グラフに保存されたデータを検索する許可を付与。	読み取り	Graph*		
StartInvestigation	調査を開始するためのアクセス許可を付与	書き込み	Graph*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartMonitoringMember	ACCEPTED_BUT_DISABLED ステータスを持つメンバーアカウントのデータ取り込みを開始する許可を付与	書き込み	Graph*		
TagResource	動作グラフにタグ値を割り当てるアクセス許可を付与	タグ付け	Graph*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	動作グラフからタグ値を削除する許可を付与。	Tagging	Graph*		
				aws:TagKeys	
UpdateDatasourcePackages	このアカウントによって管理される動作グラフで、データソースパッケージを有効または無効にする許可を付与	書き込み	Graph*		
UpdateInvestigationState	調査の状態とメタデータを更新するためのアクセス許可を付与	書き込み	Graph*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateOrganizationConfiguration	Amazon Detective と AWS Organizations の統合に関連する現在の設定を更新する許可を付与	書き込み	Graph*		organizations:DescribeOrganization

Amazon Detective で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource 工レメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Graph	arn:${Partition}:detective:${Region}:${Account}:graph:${ResourceId}	aws:ResourceTag/${TagKey}

Amazon Detective の条件キー

Amazon Detective では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストで渡されたタグを指定してアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグを指定してアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーを指定してアクセスをフィルタリングします	ArrayOfString

AWS Device Farm のアクション、リソース、および条件キー

AWS Device Farm (サービスプレフィックス: `devicefarm`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Device Farm で定義されるアクション
- AWS Device Farm で定義されるリソースタイプ
- AWS Device Farm の条件キー

AWS Device Farm で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateDevicePool	プロジェクト内でデバイスプールを作成する許可を付与。	書き込み	project*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateInstanceProfile	デバイスインスタンスプロファイルを作成する許可を付与	書き込み			
CreateNetworkProfile	プロジェクト内でネットワークプロファイルを作成する許可を付与。	書き込み	project*		
CreateProject	モバイルテスト用のプロジェクトを作成する許可を付与。	書き込み			ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
CreateRemoteAccessSession	デバイスインスタンスへのリモートアクセスセッションを開始する許可を付与。	書き込み	device*		
			project*		
			deviceinstance		
			upload		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateTestGridProject	デスクトップテスト用のプロジェクトを作成する許可を付与。	書き込み			ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
CreateTestGridUrl	テストグリッドサービスにアクセスするために使用される新しい署名付き URL を生成する許可を付与	書き込み	testgrid-project*		
CreateUpload	プロジェクト内で新しいファイルまたはアプリケーションをアップロードする許可を付与。	書き込み	project*		
CreateVPCEConfiguration	Amazon Virtual Private Cloud (VPC) エンドポイント設定を作成する許可を付与。	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteDevicePool	ユーザーが生成したデバイスプールを削除する許可を付与。	書き込み	devicepool*		
DeleteInstanceProfile	ユーザーが生成したインスタンスプロファイルを削除する許可を付与。	書き込み	instanceprofile*		
DeleteNetworkProfile	ユーザーが生成したネットワークプロファイルを削除する許可を付与。	書き込み	networkprofile*		
DeleteProject	モバイルテストプロジェクトを削除する許可を付与。	書き込み	project*		
DeleteRemoteAccessSession	完了したリモートアクセスセッションとその結果を削除する許可を付与。	書き込み	session*		
DeleteRun	実行を削除する許可を付与。	書き込み	run*		
DeleteTestGridProject	デスクトップテストプロジェクトを削除する許可を付与。	書き込み	testgrid-project*		
DeleteUpload	ユーザーがアップロードしたファイルを削除する許可を付与。	書き込み	upload*		
DeleteVPCEConfiguration	Amazon Virtual Private Cloud (VPC) エンドポイント設定を削除する許可を付与。	書き込み	vpceconfiguration*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetAccountSettings	アカウントで購入された、計測されていない iOS デバイスや計測されていない Android デバイスの数を取得する許可を付与。	読み込み			
GetDevice	一意のデバイスタイプの情報を取得する許可を付与。	読み込み	device*		
GetDeviceInstance	デバイスインスタンスの情報を取得する許可を付与。	読み込み	deviceinstance*		
GetDevicePool	デバイスプールの情報を取得する許可を付与。	読み込み	devicepool*		
GetDevicePoolCompatibility	テストやアプリケーションとデバイスプールとの互換性に関する情報を取得する許可を付与。	読み込み	devicepool* upload		
GetInstanceProfile	インスタンスプロファイルの情報を取得する許可を付与。	読み込み	instanceprofile*		
GetJob	ジョブの情報を取得する許可を付与。	読み込み	job*		
GetNetworkProfile	ネットワークプロファイルの情報を取得する許可を付与。	読み取り	networkprofile*		
GetOfferingStatus	で購入したすべてのサービスの現在のステータスと将来のステータスを取得するアクセス許可を付与します AWS アカウント	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetProject	モバイルテストプロジェクトに関する情報を取得する許可を付与。	読み込み	project*		
GetRemoteAccessSession	現在実行中のリモートアクセスセッションへのリンクを取得する許可を付与。	読み込み	session*		
GetRun	実行の情報を取得する許可を付与。	読み込み	run*		
GetSuite	テストスイートの情報を取得する許可を付与。	読み込み	suite*		
GetTest	テストケースの情報を取得する許可を付与。	読み込み	test*		
GetTestGridProject	デスクトップテストプロジェクトに関する情報を取得する許可を付与。	読み込み	testgrid-project*		
GetTestGridSession	テストグリッドセッションの情報を取得する許可を付与。	読み込み	testgrid-project		
			testgrid-session		
GetUpload	アップロードされたファイルの情報を取得する許可を付与。	読み込み	upload*		
GetVPCEConfiguration	Amazon Virtual Private Cloud (VPC) エンドポイント設定の情報を取得する許可を付与。	読み込み	vpceconfiguration*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
InstallToRemoteAccessSession	リモートアクセスセッションでデバイスにアプリケーションをインストールする許可を付与。	書き込み	session*		
			upload*		
ListArtifacts	プロジェクトのアーティファクトを一覧表示する許可を付与。	リスト	job		
			run		
			suite		
			test		
ListDeviceInstances	デバイスインスタンスの情報を一覧表示する許可を付与。	リスト			
ListDevicePools	デバイスプールの情報を一覧表示する許可を付与。	リスト	project*		
ListDevices	一意のデバイスタイプの情報を一覧表示する許可を付与。	リスト			
ListInstanceProfiles	デバイスインスタンスプロファイルの情報を一覧表示する許可を付与。	リスト			
ListJobs	実行内のジョブの情報を一覧表示する許可を付与。	リスト	run*		
ListNetworkProfiles	プロジェクト内のネットワークプロファイルの情報を一覧表示する許可を付与。	リスト	project*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListOfferingPromotions	提供しているプロモーションを一覧表示する許可を付与。	リスト			
ListOfferingTransactions	の過去の購入、更新、およびシステム更新トランザクションをすべて一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListOfferings	ユーザーが API を使用して管理できる製品またはサービスを一覧表示する許可を付与。	リスト			
ListProjects	のモバイルテストプロジェクトの情報を一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListRemoteAccessSessions	現在実行中のリモートアクセスセッションの情報を一覧表示する許可を付与。	リスト	project*		
ListRuns	プロジェクト内の実行の情報を一覧表示する許可を付与。	リスト	project*		
ListSamples	プロジェクト内のサンプルの情報を一覧表示する許可を付与。	リスト	job*		
ListSuites	ジョブ内のテストスイートの情報を一覧表示する許可を付与。	リスト	job*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTagsForResource	リソースのタグを一覧表示する許可を付与。	リスト	device		
			deviceinstance		
			devicepool		
			instanceprofile		
			networkprofile		
			project		
			run		
			session		
			testgrid-project		
			testgrid-session		
			vpceconfiguration		
ListTestGridProjects	のデスクトップテストプロジェクトの情報を一覧表示するアクセス許可を付与しますAWS アカウント	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTestGridSessionActions	テストグリッドセッション中に実行されたセッションアクションをリストする許可を付与。	リスト	testgrid-session*		
ListTestGridSessionArtifacts	テストグリッドセッションによって生成されたアーティファクトをリストする許可を付与。	リスト	testgrid-session*		
ListTestGridSessions	テストグリッドプロジェクト内のセッションを一覧表示する許可を付与。	リスト	testgrid-project*		
ListTests	テストスイート内のテストの情報を一覧表示する許可を付与。	リスト	suite*		
ListUniqueProblems	実行内の一意の問題の情報を一覧表示する許可を付与。	リスト	run*		
ListUploads	プロジェクト内のアップロードの情報を一覧表示する許可を付与。	リスト	project*		
ListVPCEConfigurations	Amazon Virtual Private Cloud (VPC) エンドポイント設定の情報を一覧表示する許可を付与。	リスト			
PurchaseOffering	のサービスを購入するアクセス許可を付与します AWS アカウント	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RenewOffering	サービスで更新するデバイスの数を設定する許可を付与。	書き込み			
ScheduleRun	実行をスケジュールする許可を付与。	書き込み	project*		
			devicepool		
			upload		
	シナリオ: Device Pool as filter		devicepool* project* upload		
	シナリオ: Device Selection Configuration as filter		project* upload		
StopJob	実行中のジョブを終了する許可を付与。	書き込み	job*		
StopRemoteAccessSession	実行中のリモートアクセスセッションを終了する許可を付与。	書き込み	session*		
StopRun	実行中のテストランを終了する許可を付与。	書き込み	run*		
TagResource	リソースにタグを追加するアクセス許可を付与します	タグ付け	device		
			deviceinstance		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			devicepool		
			instanceprofile		
			networkprofile		
			project		
			run		
			session		
			testgrid-project		
			testgrid-session		
			vpceconfiguration		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	タグ付け	device		
			deviceinstance		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			devicepool		
			instanceprofile		
			networkprofile		
			project		
			run		
			session		
			testgrid-project		
			testgrid-session		
			vpceconfiguration		
				aws:TagKeys	
UpdateDeviceInstance	既存のデバイスインスタンスを変更する許可を付与。	書き込み	deviceinstance*		
			instanceprofile		
UpdateDevicePool	既存のデバイスプールを変更する許可を付与。	書き込み	devicepool*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateInstanceProfile	既存のインスタンスプロファイルを変更する許可を付与。	書き込み	instanceprofile*		
UpdateNetworkProfile	既存のネットワークプロファイルを変更する許可を付与。	書き込み	networkprofile*		
UpdateProject	既存のモバイルテストプロジェクトを変更する許可を付与。	書き込み	project*		ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateTestGridProject	既存のデスクトップテストプロジェクトを変更する許可を付与。	書き込み	testgrid-project*		ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
UpdateUpload	既存のアップロードを変更する許可を付与。	書き込み	upload*		
UpdateVPCEConfiguration	既存の Amazon Virtual Private Cloud (VPC) エンドポイント設定を変更する許可を付与。	書き込み	vpceconfiguration*		

AWS Device Farm で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
project	arn:${Partition}:devicefarm:${Region}:${Account}:project:${ResourceId}	aws:ResourceTag/${TagKey}
run	arn:${Partition}:devicefarm:${Region}:${Account}:run:${ResourceId}	aws:ResourceTag/${TagKey}
job	arn:${Partition}:devicefarm:${Region}:${Account}:job:${ResourceId}	
suite	arn:${Partition}:devicefarm:${Region}:${Account}:suite:${ResourceId}	
test	arn:${Partition}:devicefarm:${Region}:${Account}:test:${ResourceId}	
upload	arn:${Partition}:devicefarm:${Region}:${Account}:upload:${ResourceId}	
artifact	arn:${Partition}:devicefarm:${Region}:${Account}:artifact:${ResourceId}	
sample	arn:${Partition}:devicefarm:${Region}:${Account}:sample:${ResourceId}	
networkprofile	arn:${Partition}:devicefarm:${Region}:${Account}:networkprofile:${ResourceId}	aws:ResourceTag/${TagKey}
deviceinstance	arn:${Partition}:devicefarm:${Region}::deviceinstance:${ResourceId}	aws:ResourceTag/${TagKey}
session	arn:${Partition}:devicefarm:${Region}:${Account}:session:${ResourceId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
devicepool	arn:${Partition}:devicefarm:${Region}:${Account}:devicepool:${ResourceId}	aws:ResourceTag/${TagKey}
device	arn:${Partition}:devicefarm:${Region}::device:${ResourceId}	aws:ResourceTag/${TagKey}
instanceprofile	arn:${Partition}:devicefarm:${Region}:${Account}:instanceprofile:${ResourceId}	aws:ResourceTag/${TagKey}
vpceconfiguration	arn:${Partition}:devicefarm:${Region}:${Account}:vpceconfiguration:${ResourceId}	aws:ResourceTag/${TagKey}
testgrid-project	arn:${Partition}:devicefarm:${Region}:${Account}:testgrid-project:${ResourceId}	aws:ResourceTag/${TagKey}
testgrid-session	arn:${Partition}:devicefarm:${Region}:${Account}:testgrid-session:${ResourceId}	aws:ResourceTag/${TagKey}

AWS Device Farm の条件キー

AWS Device Farm は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	各タグで許可されている値のセットに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられている tag-value に基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエスト内の必須タグのプレゼンスに基づいてアクションをフィルタリングします	ArrayOfString

Amazon DevOps Guru のアクション、リソース、および条件キー

Amazon DevOps Guru (サービスプレフィックス: devops-guru) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon DevOps Guru で定義されるアクション
- Amazon DevOps Guru で定義されるリソースタイプ
- Amazon DevOps Guru の条件キー

Amazon DevOps Guru で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AddNotificationChannel	DevOps Guru に通知チャネルを追加する権限を付与します	書き込み	topic*		sns:GetTopicAttributes sns:SetTopicAttributes
DeleteInsight	アカウント内の指定されたインサイトを削除するアクセス許可を付与します	書き込み			
DescribeAccountHealth	のオペレーションの正常性を表示するアクセス許可を付与します AWS アカウント	読み取り			
DescribeAccountOverview	の時間範囲内のオペレーションの正常性を表示するアクセス許可を付与します AWS アカウント	読み取り			
DescribeAnomaly	指定された異常の詳細を一覧表示する権限を付与します	読み込み			
DescribeEventSourcesConfig	DevOps Guru のイベントソースの詳細を取得するアクセス許可を付与します	読み込み			
DescribeFeedback	指定されたインサイトのフィードバックの詳細を表示する許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeInsight	指定されたインサイトの詳細を一覧表示する権限を付与します	読み込み			
DescribeOrganizationHealth	組織内のオペレーションの健全性を表示する許可を付与します。	読み込み			
DescribeOrganizationOverview	組織内における時間範囲内のオペレーションの健全性を表示する許可を付与します。	読み取り			
DescribeOrganizationResourceCollectionHealth	組織内の DevOps Guru で指定された各 AWS CloudFormation スタック、 AWS サービス、またはアカウントのオペレーションの正常性を表示するアクセス許可を付与します	読み取り			
DescribeResourceCollectionHealth	DevOps Guru で指定された各 AWS CloudFormation スタックのオペレーションの正常性を表示するアクセス許可を付与します	読み取り			
DescribeServiceIntegration	DevOps Guru と統合できるサービスの統合ステータスを表示する権限を付与します	読み込み			
GetCostEstimation	サービスリソースコストの見積りを一覧表示する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetResourceCollection	DevOps Guru が使用するように設定された AWS CloudFormation スタックを一覧表示するアクセス許可を付与します	読み取り			
ListAnomaliesForInsight	アカウント内にある所与のインサイトの異常を一覧表示する権限を付与します	リスト		devops-guru:ServiceNames	
ListAnomalousLogGroups	アカウントの特定インサイトのログ異常を一覧表示する権限の付与	リスト			
ListEvents	DevOps Guru で評価されるリソースイベントを一覧表示する権限を付与します	リスト			
ListInsights	アカウント内のインサイトを一覧表示する権限を付与します	リスト			
ListMonitoredResources	アカウントのDevOps Guru がモニタリングしているリソースを一覧表示する許可の付与	リスト			
ListNotificationChannels	DevOps Guru 用に設定された通知チャネルをアカウントに表示する権限を付与します。	リスト			
ListOrganizationInsights	組織内のインサイトを一覧表示する権限を付与します。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListRecommendations	指定されたインサイトの推奨事項を一覧表示する権限を付与します	リスト			
PutFeedback	DevOps Guru にフィードバックを送信する権限を付与します	書き込み			
RemoveNotificationChannel	DevOps Guru から通知チャネルを削除する許可を付与します	書き込み	topic*		sns:GetTopicAttributes sns:SetTopicAttributes
SearchInsights	アカウント内のインサイトを検索する権限を付与します	リスト		devops-guru:ServiceNames	
SearchOrganizationInsights	組織内のインサイトを検索する権限を付与します。	リスト			
StartCostEstimation	月額コストの見積もり作成を開始する許可を付与	読み込み			
UpdateEventSourcesConfig	DevOps Guru のイベントソースを更新するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateResourceCollection	DevOps Guru によって分析されるアカウント内の AWS リソースを指定するために使用する AWS CloudFormation スタックのリストを更新するアクセス許可を付与します	書き込み			
UpdateServiceIntegration	DevOps Guru と統合するサービスを有効または無効にする権限を付与します。	書き込み			

Amazon DevOps Guru で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
topic	`arn:${Partition}:sns:${Region}:${Account}:${TopicName}`	

Amazon DevOps Guru の条件キー

Amazon DevOps Guru は、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
devops-guru:ServiceNames	API でアクセスをフィルタリングして、指定された AWS サービス名へのアクセスを制限します	ArrayOfString

AWS 診断ツールのアクション、リソース、条件キー

AWS 診断ツール (サービスプレフィックス: `ts`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS 診断ツールで定義されるアクション
- AWS 診断ツールで定義されるリソースタイプ
- AWS 診断ツールの条件キー

AWS 診断ツールで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetExecution	AWS 診断ツール内の特定の実行に関する詳細を取得するアクセス許可を付与します	読み取り	execution*		
GetExecutionOutput	AWS 診断ツール内の特定の実行出力に関する詳細を取得する許可を付与	読み取り	execution*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetTool	AWS 診断ツール内の特定のツールに関する詳細を取得する許可を付与	読み取り	tool*		
ListExecutions	AWS 診断ツール内で使用可能なすべての実行を一覧表示するアクセス許可を付与します	リスト			
ListTagsForResource	AWS 診断ツールリソースのタグを一覧表示するアクセス許可を付与します	読み取り	execution*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListTools	AWS 診断ツール内で使用可能なすべてのツールを一覧表示するアクセス許可を付与します	リスト			
StartExecution	AWS 診断ツール内で特定のツールの実行ワークフローを開始するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
TagResource	AWS 診断ツールリソースにタグを付けるアクセス許可を付与します	Tagging	execution*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	AWS 診断ツールリソースのタグを解除する許可を付与	Tagging	execution *		
				aws:TagKeys	

AWS 診断ツールで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
execution	arn:${Partition}:ts::${Account}:execution/${UserId}/${ToolId}/${ExecutionId}	aws:ResourceTag/${TagKey}
tool	arn:${Partition}:ts::aws:tool/${ToolId}	

AWS 診断ツールの条件キー

AWS 診断ツールは、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	各タグの許可された値のセットでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値でアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内の必須タグの存在でアクセスをフィルタリングします	ArrayOfString

AWS Direct Connect のアクション、リソース、および条件キー

AWS Direct Connect (サービスプレフィックス: directconnect) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Direct Connect で定義されるアクション
- AWS Direct Connect で定義されるリソースタイプ

- AWS Direct Connect の条件キー

AWS Direct Connect で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AcceptDirectConnectGatewayAssociationProposal	仮想プライベートゲートウェイを Direct Connect ゲートウェイにアタッチするための提案リクエストを受け入れる許可を付与	書き込み	dx-gateway*		
AllocateConnectionOnInterconnect	相互接続上にホスト接続を作成するアクセス許可を付与	書き込み	dxcon*		
AllocateHostedConnection	AWS Direct Connect パートナーのネットワークと特定の AWS Direct Connect ロケーションの間に新しいホスト接続を作成するアクセス許可を付与します	書き込み	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AllocatePrivateVirtualInterface	別の顧客が所有できるようにプライベート仮想インターフェイスをプロビジョニングする許可を付与	書き込み	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AllocatePublicVirtualInterface	別の顧客が所有できるようにパブリック仮想インターフェイスをプロビジョニングする許可を付与	書き込み	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AllocateTransitVirtualInterface	別の顧客が所有できるようにトランジット仮想インターフェイスをプロビジョニングする許可を付与	書き込み	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateConnectionWithLag	コネクションをLink Aggregation Group（LAG）に関連付ける許可を付与	書き込み	dxcon*		
			dxlag*		
AssociateHostedConnection	ホスト接続およびその仮想インターフェイスを Link Aggregation Group (LAG) または相互接続に関連付ける許可を付与	書き込み	dxcon*		
			dxcon		
			dxlag		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateMacSecKey	MAC Security (MACsec) Connection Key Name (CKN)/ Connectivity Association Key (CAK) ペアを AWS Direct Connect 専用接続に関連付けるアクセス許可を付与します	書き込み	dxcon		
			dxlag		
AssociateVirtualInterface	仮想インターフェイスを、指定された Link Aggregation Group (LAG) もしくは接続と関連付ける許可を付与	書き込み	dxvif*		
			dxcon		
			dxlag		
ConfirmConnection	相互接続上にホスト接続が作成されていることを確認する許可を付与	書き込み	dxcon*		
ConfirmCustomerAgreement	接続もしくは Link Aggregation Group (LAG) を作成するときに、契約条件を確認するアクセス許可を付与	書き込み			
ConfirmPrivateVirtualInterface	別の顧客が作成したプライベート仮想インターフェイスの所有権を受け入れる許可を付与	書き込み	dxvif*		
ConfirmPublicVirtualInterface	別の顧客が作成したパブリック仮想インターフェイスの所有権を受け入れる許可を付与	書き込み	dxvif*		
ConfirmTransitVirtualInterface	別の顧客が作成したトランジット仮想インターフェイスの所有権を受け入れる許可を付与	書き込み	dxvif*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateBGPPeer	指定された仮想インターフェイスで BGP ピアを作成する許可を付与	書き込み	dxvif*		
CreateConnection	カスタマーネットワークと特定の AWS Direct Connect ロケーションの間に新しい接続を作成するアクセス許可を付与します	書き込み	dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDirectConnectGateway	Direct Connect ゲートウェイを作成する許可を付与これは、一連の仮想インターフェイスおよび仮想プライベートゲートウェイを接続できるようにする中間オブジェクトです。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDirectConnectGatewayAssociation	Direct Connect ゲートウェイおよび仮想プライベートゲートウェイ間の関連付けを作成する許可を付与	書き込み	dx-gateway*		
CreateDirectConnectGatewayAssociationProposal	指定された仮想プライベートゲートウェイを、指定された Direct Connect ゲートウェイに関連付けるための提案を作成する許可を付与	書き込み	dx-gateway*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateInterconnect	AWS Direct Connect パートナーのネットワークと特定の AWS Direct Connect ロケーションの間に新しい相互接続を作成するアクセス許可を付与します	書き込み	dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLag	カスタマーネットワークと特定の AWS Direct Connect ロケーションとの間で、指定された数のバンドルされた物理接続を持つリンク集約グループ (LAG) を作成するアクセス許可を付与します	書き込み	dxcon		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePrivateVirtualInterface	新しい仮想プライベートゲートウェイを作成する許可を付与	書き込み	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePublicVirtualInterface	新しいパブリック仮想インターフェイスを作成するアクセス許可を付与」	書き込み	dxcon		
			dxlag		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTransitVirtualInterface	新しい中継仮想インターフェイスを作成するアクセス許可を付与	書き込み	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBGPPeer	指定されたカスタマーアドレスおよび ASN を持つ、指定された仮想インターフェイス上の指定された BGP ピアを削除しまする許可を付与	書き込み	dxvif*		
DeleteConnection	接続を削除する許可を付与	書き込み	dxcon*		
DeleteDirectConnectGateway	指定された Direct Connect gatewayの記録設定を削除する許可を付与	書き込み	dx-gateway*		
DeleteDirectConnectGatewayAssociation	指定されたDirect Connect ゲートウェイおよび仮想プライベートゲートウェイ間の関連付けを削除する許可を付与	書き込み	dx-gateway*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteDirectConnectGatewayAssociationProposal	指定されたDirect Connectゲートウェイおよび仮想プライベートゲートウェイ間の関連付け提案リクエストを削除する許可を付与	書き込み			
DeleteInterconnect	指定されたインターコネクトを削除するアクセス許可を付与	書き込み	dxcon*		
DeleteLag	指定された Link Aggregation Group (LAG)を削除するアクセス許可を付与	書き込み	dxlag*		
DeleteVirtualInterface	仮想インターフェースを削除するアクセス許可を付与	書き込み	dxvif*		
DescribeConnectionLoa	接続の LOA-CFA を記述するアクセス許可を付与	読み取り	dxcon*		
DescribeConnections	このリージョンで設定されたすべての接続を記述するアクセス許可を付与	読み取り	dxcon		
DescribeConnectionsOnInterconnect	指定された相互接続でプロビジョニングされている接続のリストを記述をする許可を付与	読み取り	dxcon*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeCustomerMetadata	顧客契約のリスト、署名済みステータス、およびお客様がNniPartner、NniPartnerv2、または非パートナーのいずれであるかを表示するアクセス許可を付与	読み取り			
DescribeDirectConnectGatewayAssociationProposals	仮想プライベートゲートウェイおよび Direct Connect ゲートウェイ間の接続に関する 1 つ以上の関連付け提案の記述する許可を付与	読み取り	dx-gateway		
DescribeDirectConnectGatewayAssociations	Direct Connect ゲートウェイおよび仮想プライベートゲートウェイの間の関連付けを記述する許可を付与	読み取り	dx-gateway		
DescribeDirectConnectGatewayAttachments	Direct Connect ゲートウェイおよび仮想インターフェイス間のアタッチメントを記述する許可を付与	読み取り	dx-gateway		
DescribeDirectConnectGateways	すべての Direct Connect ゲートウェイ、もしくは指定された Direct Connect ゲートウェイのみを記述する許可を付与	読み取り	dx-gateway		
DescribeHostedConnections	指定された相互接続もしくは Link Aggregation Group (LAG) でプロビジョニングされているホスト接続を記述する許可を付与	読み取り	dxcon		
			dxlag		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeInterconnectLoa	相互接続の LOA-CFA を記述するアクセス許可を付与	読み取り	dxcon*		
DescribeInterconnects	が所有する相互接続のリストを記述するアクセス許可を付与します AWS アカウント	読み取り	dxcon		
DescribeLags	すべての Link Aggregation Group (LAG) もしくは指定された LAG を記述するアクセス許可を付与	読み取り	dxlag		
DescribeLoa	接続、相互接続、もしくは Link Aggregation Group (LAG) の LOA-CFA を記述するアクセス許可を付与	読み取り	dxcon		
			dxlag		
DescribeLocations	現在の AWS リージョンの AWS Direct Connect ロケーションのリストを記述するアクセス許可を付与します	読み取り			
DescribeRouterConfiguration	仮想インターフェイスのルータの詳細を説明するアクセス許可を付与	読み取り	dxvif*		
DescribeTags	指定された AWS Direct Connect リソースに関連付けられたタグを記述するアクセス許可を付与します	読み取り	dx-gateway		
			dxcon		
			dxlag		
			dxvif		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeVirtualGateways	が所有する仮想プライベートゲートウェイのリストを記述するアクセス許可を付与します AWS アカウント	読み取り			
DescribeVirtualInterfaces	のすべての仮想インターフェイスを記述するアクセス許可を付与します AWS アカウント	読み取り	dxcon		
			dxlag		
			dxvif		
DisassociateConnectionFromLag	Link Aggation Group (LAG) からの接続の関連付けを解除するアクセス許可を付与	書き込み	dxcon*		
			dxlag*		
DisassociateMacSecKey	MAC セキュリティ (MACsec) セキュリティキーと AWS Direct Connect 専用接続間の関連付けを削除するアクセス許可を付与します	書き込み	dxcon		
			dxlag		
ListVirtualInterfaceTestHistory	仮想インターフェイスのフェイルオーバーテスト履歴を一覧表示する許可を付与	リスト	dxvif*		
StartBgpFailoverTest	BGP ピアリングセッションを DOWN 状態にして、設定が回復性要件を満たしていることを確認する仮想インターフェイスのフェイルオーバーテストを開始する許可を付与 トラフィックを送信して、サービス停止が起こらないことを確認できます。	書き込み	dxvif*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StopBgpFailoverTest	仮想インターフェイスのフェイルオーバーテストを停止するアクセス許可を付与	書き込み	dxvif*		
TagResource	指定された AWS Direct Connect リソースに指定されたタグを追加するアクセス許可を付与します。各リソースには、最大 50 個のタグを設定できます。	Tagging	dx-gateway		
			dxcon		
			dxlag		
			dxvif		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	指定された AWS Direct Connect リソースから 1 つ以上のタグを削除するアクセス許可を付与します	Tagging	dx-gateway		
			dxcon		
			dxlag		
			dxvif		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateConnection	AWS Direct Connect 専用接続設定を更新するアクセス許可を付与します。接続について、次のパラメータを更新できます。接続名または接続の MAC セキュリティ (MACsec) 暗号化モード	書き込み	dxcon*		
UpdateDirectConnectGateway	Direct Connect ゲートウェイの名前を更新するアクセス許可を付与	書き込み	dx-gateway*		
UpdateDirectConnectGatewayAssociation	Direct Connect ゲートウェイの関連付けの指定された属性を更新する許可を付与	書き込み			
UpdateLag	指定された Link Aggregation Group (LAG) の属性を更新する許可を付与	書き込み	dxlag*		
UpdateVirtualInterfaceAttributes	指定された仮想プライベートインターフェースの指定された属性を更新する許可を付与	書き込み	dxvif*		

AWS Direct Connect で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
dxcon	arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}	aws:ResourceTag/${TagKey}
dxlag	arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}	aws:ResourceTag/${TagKey}
dxvif	arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}	aws:ResourceTag/${TagKey}
dx-gateway	arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}	aws:ResourceTag/${TagKey}

AWS Direct Connect の条件キー

AWS Direct Connect では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーおよび値のペアのプレゼンスに基づいてアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアに基づいてアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいたアクションでアクセスをフィルタリングします	ArrayOfString

AWS Directory Service のアクション、リソース、および条件キー

AWS Directory Service (サービスプレフィックス: ds) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Directory Service で定義されるアクション
- AWS Directory Service で定義されるリソースタイプ
- AWS Directory Service の条件キー

AWS Directory Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptSharedDirectory	ディレクトリ所有者アカウントから送信されたディレクトリ共有リクエストを受け入れる許可を付与	書き込み	directory*		
AccessDSData [アクセス許可のみ]	Directory Service Data API を使用してディレクトリデータ	権限の管理	directory*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	にアクセスする許可を付与する				
AddIpRoutes	トラフィックを Amazon Web Services の Microsoft AD との間で正しくルーティングできるように CIDR アドレスブロックを追加する許可を付与	書き込み	directory*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:DescribeSecurityGroups

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AddRegion	指定されたディレクトリの指定されたリージョンに 2 つのドメインコントローラーを追加する許可を付与	書き込み	directory*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddTagsToResource	指定された Amazon Directory Services ディレクトリの 1 つまたは複数のタグを追加または上書きする許可を付与	Tagging	directory*		ec2:CreateTags
				aws:RequestTag/${TagKey} aws:TagKeys	
AuthorizeApplication [アクセス許可のみ]	AWS ディレクトリのアプリケーションを承認するアクセス許可を付与します	書き込み	directory*		
CancelSchemaExtension	進行中の Microsoft AD ディレクトリへのスキーマ拡張をキャンセルする許可を付与	書き込み	directory*		
CheckAlias [アクセス許可のみ]	エイリアスが使用可能であることを確認する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ConnectDirectory	オンプレミスディレクトリに接続するための AD Connector を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateAlias	ディレクトリのエイリアスを作成し、ディレクトリにエイリアスを割り当てる許可を付与	書き込み	directory*		
CreateComputer	指定されたディレクトリにコンピュータアカウントを作成し、コンピュータをディレクトリに結合する許可を付与	書き込み	directory*		
CreateConditionalForwarder	AWS ディレクトリに関連付けられた条件付きフォワーダーを作成するアクセス許可を付与します	書き込み	directory*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateDirectory	Simple AD ディレクトリを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateHybridAD	Hybrid Managed AD ディレクトリを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DescribeVpcs iam:CreateServiceLinkedRole iam:GetRole secretsmanager:DescribeSecret secretsmanager:GetSecretValue ssm:GetCommandInvocation ssm:GetConnectionStatus ssm:ListCommands ssm:SendCommand

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateIdentityPoolDirectory [アクセス許可のみ]	AWS クラウドに IdentityPool ディレクトリを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLogSubscription	Directory Service ドメインコントローラーのセキュリティログを の指定された CloudWatch ロググループに転送するサブスクリプションを作成するアクセス許可を付与します AWS アカウント	書き込み	directory*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateMicrosoftAD	AWS クラウドで Microsoft AD を作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateSnapshot	AWS クラウド内の Simple AD または Microsoft AD ディレクトリのスナップショットを作成するアクセス許可を付与します	書き込み	directory*		
CreateTrust	AWS クラウド内の Microsoft AD と外部ドメイン間の信頼関係の AWS 側の作成を開始するアクセス許可を付与します	書き込み	directory*		
DeleteADAssessment	ディレクトリ評価を削除するアクセス許可を付与します	書き込み			
DeleteConditionalForwarder	AWS ディレクトリに設定された条件付きフォワーダーを削除するアクセス許可を付与します	書き込み	directory*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteDirectory	AWS Directory Service ディレクトリを削除するアクセス許可を付与します	書き込み	directory*		ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup ec2:DescribeNetworkInterfaces ec2:RevokeSecurityGroupEgress ec2:RevokeSecurityGroupIngress
DeleteLogSubscription	指定されたログサブスクリプションを削除する許可を付与	書き込み	directory*		
DeleteSnapshot	ディレクトリスナップショットを削除する許可を付与	書き込み	directory*		
DeleteTrust	AWS クラウド内の Microsoft AD と外部ドメイン間の既存の信頼関係を削除するアクセス許可を付与します	書き込み	directory*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeregisterCertificate	セキュリティで保護された LDAP 接続用に登録された証明書をシステムから削除する許可を付与	書き込み	directory*		
DeregisterEventTopic	指定された SNS トピックへの発行者として指定されたディレクトリを削除する許可を付与	書き込み	directory*		
DescribeADAssessment	ディレクトリ評価を記述するアクセス許可を付与します	読み取り			
DescribeCertificate	セキュリティで保護された LDAP 接続に登録された証明書に関する情報を表示する許可を付与	読み取り	directory*		
DescribeClientAuthenticationSettings	タイプが指定されている場合、指定したディレクトリのクライアント認証のタイプに関する情報を取得する許可を付与 タイプを指定しないと、指定したディレクトリでサポートされているすべてのクライアント認証タイプに関する情報が取得されます。現在は、SmartCard のみがサポートされています。	読み取り	directory*		
DescribeConditionalForwarders	このアカウントの条件付きフォワーダーに関する情報を取得する許可を付与	読み取り	directory*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeDirectories	このアカウントに属するディレクトリに関する情報を取得する許可を付与	リスト			
DescribeDirectoryDataAccess	指定されたディレクトリの Directory Service Data API ステータスを記述する許可を付与する	読み取り	directory*		
DescribeDomainControllers	ディレクトリ内のドメインコントローラに関する情報を提供する許可を付与	読み取り	directory*		
DescribeEventTopics	指定されたディレクトリからステータスメッセージを受信する SNS トピックに関する情報を取得する許可を付与	読み取り	directory*		
DescribeHybridADUpdate	指定されたハイブリッドディレクトリの更新を記述するアクセス許可を付与します	読み取り	directory*		
DescribeLDAPSSettings	指定されたディレクトリの LDAP セキュリティのステータスを説明する許可を付与	読み取り	directory*		
DescribeRegions	マルチリージョンレプリケーション用に設定されているリージョンに関する情報を提供する許可を付与	読み取り	directory*		
DescribeSettings	指定されたディレクトリの設定可能なセッティングに関する情報を取得する許可の付与	読み取り	directory*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeSharedDirectories	アカウント内の共有ディレクトリを返す許可を付与	読み取り	directory*		
DescribeSnapshots	このアカウントに属するディレクトリスナップショットに関する情報を取得する許可を付与	読み取り			
DescribeTrusts	このアカウントの信頼関係に関する情報を取得する許可を付与	読み取り			
DescribeUpdateDirectory	特定の更新タイプのディレクトリの更新を記述する権限を付与する	読み取り	directory*		
DisableClientAuthentication	指定されたディレクトリの代替クライアント認証方法を無効化する許可を付与	書き込み	directory*		
DisableDirectoryDataAccess	指定されたディレクトリの Directory Service Data API を無効にする許可を付与する	書き込み	directory*		
DisableLDAPS	指定されたディレクトリの LDAP セキュアコールを非アクティブ化する許可を付与	書き込み	directory*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisableRadius	AD Connector ディレクトリに対し、Remote Authentication Dial In User Service (RADIUS) サーバーを使った多要素認証 (MFA) を無効にする許可を付与	書き込み	directory*		
DisableRoleAccess [アクセス許可のみ]	AWS ディレクトリ内の ID の AWS Management Console アクセスを無効にするアクセス許可を付与します	書き込み	directory*		
DisableSso	Single Sign-On で使用するディレクトリの関連付けを解除する許可を付与	書き込み	directory*		
EnableClientAuthentication	指定されたディレクトリの代替クライアント認証方式を有効化する許可を付与	書き込み	directory*		
EnableDirectoryDataAccess	指定されたディレクトリの Directory Service Data API を有効にする許可を付与する	書き込み	directory*		
EnableLDAPS	特定のディレクトリのスイッチをアクティブ化して、常に LDAP セキュアコールを使用する許可を付与	書き込み	directory*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
EnableRadius	AD Connector ディレクトリに対し、Remote Authentication Dial In User Service (RADIUS) サーバーを使った多要素認証 (MFA) を有効にする許可を付与	書き込み	directory*		
EnableRoleAccess [アクセス許可のみ]	AWS ディレクトリ内の ID の AWS Management Console アクセスを有効にするアクセス許可を付与します	書き込み	directory*		iam:PassRole
EnableSso	ディレクトリに対してシングルサインオンを有効にする許可を付与	書き込み	directory*		
GetAuthorizedApplicationDetails [アクセス許可のみ]	ディレクトリ上で許可されたアプリケーションの詳細を取得する許可を付与	読み取り	directory*		
GetDirectoryLimits	現在のリージョンのディレクトリ制限情報を取得する許可を付与	読み取り			
GetSnapshotLimits	ディレクトリの手動スナップショットの制限を取得する許可を付与	読み取り	directory*		
ListADAssessments	ディレクトリ評価を一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListAuthorizedApplications [許可のみ]	ディレクトリに対して承認された AWS アプリケーションを取得するアクセス許可を付与します	読み取り	directory*		
ListCertificates	指定されたディレクトリについて、セキュリティで保護された LDAP 接続用に登録されたすべての証明書を一覧表示する許可を付与	リスト	directory*		
ListIpRoutes	ディレクトリに追加されたアドレスブロックを一覧表示する許可を付与	読み取り	directory*		
ListLogSubscriptions	のアクティブなログサブスクリプションを一覧表示するアクセス許可を付与します AWS アカウント	読み取り			
ListSchemaExtensions	Microsoft AD ディレクトリに適用されているすべてのスキーマ拡張を一覧表示する許可を付与	リスト	directory*		
ListTagsForResource	Amazon Directory Services ディレクトリのすべてのタグを一覧表示する許可を付与	読み取り	directory*		
RegisterCertificate	セキュリティで保護された LDAP 接続の証明書を登録する許可を付与	書き込み	directory*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RegisterEventTopic	ディレクトリを SNS トピックに関連付ける許可を付与	書き込み	directory*		sns:GetTopicAttributes
RejectSharedDirectory	ディレクトリ所有者アカウントから送信されたディレクトリ共有リクエストを拒否する許可を付与	書き込み	directory*		
RemoveIpRoutes	ディレクトリから IP アドレスブロックを削除する許可を付与	書き込み	directory*		
RemoveRegion	すべてのレプリケーションを停止し、指定されたリージョンからドメインコントローラーを削除する許可を付与 このオペレーションでは、プライマリリージョンを削除できません。	書き込み	directory*		
RemoveTagsFromResource	Amazon Directory Services ディレクトリからタグを削除する許可を付与	Tagging	directory*		ec2:DeleteTags
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ResetUserPassword	AWS Managed Microsoft AD または Simple AD ディレクトリ内の任意のユーザーのパスワードをリセットするアクセス許可を付与します	書き込み	directory*		
RestoreFromSnapshot	既存のディレクトリスナップショットを使用してディレクトリを復元する許可を付与	書き込み	directory*		
ShareDirectory	(ディレクトリ AWS アカウント 所有者) 内の指定されたディレクトリを別の AWS アカウント (ディレクトリコンシューマー) と共有するためのアクセス許可を付与します。このオペレーションでは、 内の任意の Amazon VPC AWS アカウント から ディレクトリを使用できます。 AWS リージョン	書き込み	directory*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartADAssessment	ディレクトリ評価を開始するアクセス許可を付与します	書き込み			ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup ec2:DescribeNetworkInterfaces

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DescribeSubnets ec2:DescribeVpcs ssm:GetCommandInvocation ssm:GetConnectionStatus ssm:ListCommands ssm:SendCommand
StartSchemaExtension	Microsoft AD ディレクトリにスキーマ拡張を適用する許可を付与	書き込み	directory*		
UnauthorizeApplication [アクセス許可のみ]	AWS ディレクトリからアプリケーションを認可解除するアクセス許可を付与します	書き込み	directory*		
UnshareDirectory	ディレクトリ所有者とコンシューマーアカウントの間のディレクトリ共有を停止する許可を付与	書き込み	directory*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateAuthorizedApplication [アクセス許可のみ]	AWS ディレクトリの承認されたアプリケーションを更新するアクセス許可を付与します	書き込み	directory*		
UpdateConditionalForwarder	AWS ディレクトリに設定された条件付きフォワーダーを更新するアクセス許可を付与します	書き込み	directory*		
UpdateDirectory [アクセス許可のみ]	指定したディレクトリのサービスアカウント認証情報や DNS サーバー IP アドレスなどの設定を更新するアクセス許可を付与します	書き込み	directory*		
UpdateDirectorySetup	特定の更新タイプのディレクトリを更新する権限を付与する	書き込み	directory*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateHybridAD	指定されたハイブリッドディレクトリの設定を更新するアクセス許可を付与します	書き込み	directory*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DescribeVpcs secretsmanager:DescribeSecret secretsmanager:GetSecretValue ssm:GetCommandInvocation ssm:GetConnectionStatus ssm:ListCommands ssm:SendCommand

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateNumberOfDomainControllers	ディレクトリとの間でドメインコントローラを追加または削除する許可を付与 現在の値と新しい値 (この API コールで提供される) の差に基づいて、ドメインコントローラが追加または削除されます。リクエストされた数のドメインコントローラが更新されたら、新しいドメインコントローラが完全にアクティブになるまでに最大 45 分かかる場合があります。この間、別の更新をリクエストすることはできません。	書き込み	directory*		
UpdateRadius	AD Connector ディレクトリの Remote Authentication Dial In User Service (RADIUS) サーバー情報を更新する許可を付与	書き込み	directory*		
UpdateSettings	指定したディレクトリの設定可能なセッティングを更新する許可の付与	書き込み	directory*		
UpdateTrust	AWS Managed Microsoft AD ディレクトリとオンプレミス Active Directory の間で設定された信頼を更新するアクセス許可を付与します	書き込み	directory*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
VerifyTrust	AWS クラウド内の Microsoft AD と外部ドメイン間の信頼関係を検証するアクセス許可を付与します	読み取り	directory*		

AWS Directory Service で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
directory	`arn:${Partition}:ds:${Region}:${Account}:directory/${DirectoryId}`	aws:ResourceTag/${TagKey}

AWS Directory Service の条件キー

AWS Directory Service では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	DS AWS へのリクエストの値でアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	処理対象の DS AWS リソースによってアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Directory Service Data のアクション、リソース、および条件キー

AWS Directory Service Data (サービスプレフィックス: ds-data) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Directory Service Data で定義されるアクション
- AWS Directory Service Data で定義されるリソースタイプ
- AWS Directory Service Data の条件キー

AWS Directory Service Data で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddGroupMember	ディレクトリのグループにメンバーを追加する許可を付与する	書き込み	directory*		ds:AccessDSData

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ds-data:SAMAccountName ds-data:MemberNam ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
CreateGroup	ディレクトリでグループを作成する許可を付与する	書き込み	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
CreateUser	ディレクトリでユーザーを作成する許可を付与する	書き込み	directory*		ds:AccessDSData

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DeleteGroup	ディレクトリでグループを削除する許可を付与する	書き込み	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DeleteUser	ディレクトリのユーザーを削除する許可を付与する	書き込み	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeGroup	ディレクトリのグループを記述する許可を付与する	読み取り	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DescribeUser	ディレクトリでユーザーを記述する許可を付与する	読み取り	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DisableUser	ディレクトリのユーザーを無効にする許可を付与する	書き込み	directory*		ds:AccessDSData

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
ListGroupMembers	ディレクトリのグループのメンバーを一覧表示する許可を付与する	リスト	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
ListGroups	ディレクトリのグループを一覧表示する許可を付与する	リスト	directory*		ds:AccessDSData
				ds-data:Realm	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListGroupsForMember	メンバーがディレクトリにあるグループを一覧表示する許可を付与する	リスト	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
ListUsers	ディレクトリのユーザーを一覧表示する許可を付与する	リスト	directory*		ds:AccessDSData
				ds-data:Realm	
RemoveGroupMember	ディレクトリでグループからメンバーを削除する許可を付与する	書き込み	directory*		ds:AccessDSData

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ds-data:SAMAccountName ds-data:MemberName ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
SearchGroups	ディレクトリでグループを検索する許可を付与する	読み取り	directory*		ds-data:DescribeGroup ds:AccessDSData
				ds-data:Realm	
SearchUsers	ディレクトリでユーザーを検索する許可を付与する	読み取り	directory*		ds-data:DescribeUser ds:AccessDSData

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ds-data:Realm	
UpdateGroup	ディレクトリでグループを更新する許可を付与する	書き込み	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
UpdateUser	ディレクトリ上のユーザーを更新する許可を付与する	書き込み	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	

AWS Directory Service Data で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
directory	`arn:${Partition}:ds:${Region}:${Account}:directory/${DirectoryId}`	aws:ResourceTag/${TagKey}

AWS Directory Service Data の条件キー

AWS Directory Service Data では、IAM ポリシーの `Condition`要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	処理対象の DS AWS リソースによってアクセスをフィルタリングします	String
ds-data:Identifier	リクエストで指定された識別子のタイプ (SAM アカウントネーム) によってアクセスをフィルタリングする	String
ds-data:MemberName	リクエストの MemberName 入力に含まれるディレクトリ SAM アカウント名でアクセスをフィルタリングする	String
ds-data:MemberRealm	リクエストの MemberRealm 入力に含まれるディレクトリレルム名でアクセスをフィルタリングする	String
ds-data:Realm	リクエストのディレクトリレルム名でアクセスをフィルタリングする	String

条件キー	説明	[Type] (タイプ)
ds-data:SAMAccountName	リクエストの SAMAccountName 入力に含まれるディレクトリ SAM アカウント名でアクセスをフィルタリングする	String

Amazon DocumentDB Elastic Clusters のアクション、リソース、および条件キー

Amazon DocumentDB Elastic Clusters (サービスプレフィックス: `docdb-elastic`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon DocumentDB Elastic Clusters で定義されるアクション
- Amazon DocumentDB Elastic Clusters で定義されるリソースタイプ
- Amazon DocumentDB Elastic Clusters の条件キー

Amazon DocumentDB Elastic Clusters で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ApplyPendingMaintenanceAction	Amazon DocDB-Elastic クラスターに保留中のメンテナンス	書き込み	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	アクションを適用するアクセス許可を付与します			aws:ResourceTag/${TagKey}	
CopyClusterSnapshot	新しい Amazon DocDB-Elastic クラススナップショットをコピーする許可を付与する	書き込み	cluster-snapshot*		docdb-elastic:CreateClusterSnapshot kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateCluster	新しい Amazon DocDB-Elastic クラスターを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:GetSecretValue secretsmanager:Lis

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					tSecretVersionIds secretsmanager:ListSecrets

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateClusterSnapshot	新しい Amazon DocDB-Elastic クラススナップショットを作成する許可を付与	書き込み	cluster*		ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:GetSecretValue secretsmanager:Lis

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					tSecretVersionIds secretsmanager:ListSecrets
			cluster-snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteCluster	クラスターを削除するためのアクセス許可を付与	書き込み	cluster*		ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteClusterSnapshot	クラススナップショットを削除する許可を付与	書き込み	cluster-snapshot*		ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetCluster	クラスターの詳細を表示する許可を付与	読み取り	cluster*		
				aws:ResourceTag/${TagKey}	
GetClusterSnapshot	クラススナップショットの詳細を表示する許可を付与	読み取り	cluster-snapshot*		
				aws:ResourceTag/${TagKey}	
GetPendingMaintenanceAction	Amazon DocDB-Elastic クラスターで保留中のメンテナンスアクションに関する詳細を表示するアクセス許可を付与します	読み取り	cluster*		
				aws:ResourceTag/${TagKey}	
ListClusterSnapshots	アカウント内のクラススナップショットを一覧表示する許可を付与	リスト			
ListClusters	アカウント内のクラスターを一覧表示する許可を付与	リスト			
ListPendingMaintenanceActions	Amazon DocDB-Elastic クラスターで保留中のメンテナンスアクションの詳細を一覧表示するアクセス許可を付与します	リスト		aws:ResourceTag/${TagKey}	
ListTagsForResource	DocumentDB Elastic リソースのタグを一覧表示する許可を付与	リスト	cluster		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			cluster-snapshot		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RestoreClusterFromSnapshot	Amazon DocDB-Elastic クラスタースナップショットからのクラスターを復元する許可を付与	書き込み	cluster*		docdb-elastic:CreateCluster ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DescribeVpcs ec2:ModifyVpcEndpoint iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:Get

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					SecretValue secretsmanager:ListSecretVersionIds secretsmanager:ListSecrets
			cluster-snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
StartCluster	停止した Amazon DocDB-Elastic クラスターを起動する許可を付与する	書き込み	cluster*		
				aws:ResourceTag/${TagKey}	
StopCluster	既存の Amazon DocDB-Elastic クラスターを停止する許可を付与する	書き込み	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
TagResource	DocumentDB Elastic リソースをタグ付けする許可を付与	Tagging	cluster		
			cluster-snapshot		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	DocumentDB Elastic リソースのタグを解除する許可を付与	Tagging	cluster		
			cluster-snapshot		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateCluster	クラスターを変更する許可を付与	書き込み	cluster*		ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:GetSecretValue secretsmanager:ListSecretVersionIds

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					secretsmanager:ListSecrets
				aws:ResourceTag/${TagKey}	

Amazon DocumentDB Elastic Clusters で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
cluster	arn:${Partition}:docdb-elastic:${Region}:${Account}:cluster/${ResourceId}	aws:ResourceTag/${TagKey}
cluster-snapshot	arn:${Partition}:docdb-elastic:${Region}:${Account}:cluster-snapshot/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon DocumentDB Elastic Clusters の条件キー

Amazon DocumentDB Elastic Clusters では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーおよび値のペアによるアクセスをフィルタリングします。	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーおよび値のペアによってアクセスをフィルタリングします。	String
aws:TagKeys	リクエスト内のタグキーのセットでアクセスをフィルタリングします。	ArrayOfString

Amazon DynamoDB のアクション、リソース、および条件キー

Amazon DynamoDB (サービスプレフィックス: dynamodb) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon DynamoDB で定義されるアクション
- Amazon DynamoDB で定義されるリソースタイプ
- Amazon DynamoDB の条件キー

Amazon DynamoDB で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchGetItem	1 つ以上の表から 1 つ以上の項目の属性を返す許可を付与します。	読み込み	table*		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:Select	
BatchWriteItem	1 つ以上の表を配置もしくは削除する許可を付与します。	書き込み	table*		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity	
ConditionCheckItem	ConditionCheckItem オペレーションにより、指定されたプライマリキーを持つ項目で一連の属性が存在するかどうか	読み取り	table*		
				dynamodb:Attributes	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	がチェックする許可を付与します。			dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
CreateBackup	既存の表のバックアップを作成するためのアクセス許可を付与します。	書き込み	table*		
CreateGlobalTable	既存の表からグローバル表を作成するアクセス許可を付与します。	書き込み	global-table*		
			table*		
CreateGlobalTableWitness [アクセス許可のみ]	グローバルテーブルに証人を追加する許可を付与	書き込み	table*		
CreateTable	CreateTable オペレーションで新しい表をアカウントに追加しする許可を付与します。	書き込み	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateTableReplica [アクセス許可のみ]	新しいレプリカ表を追加するアクセス許可を付与します。	書き込み	table*		
DeleteBackup	表の既存のバックアップを削除するアクセス許可を付与します。	書き込み	backup*		
DeleteGlobalTableWitness [アクセス許可のみ]	グローバルテーブルから証人を削除するアクセス許可を付与します	書き込み	table*		
DeleteItem	プライマリキーを使用して表から 1 つの項目を削除する権限を付与します。	書き込み	table*	dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteResourcePolicy	リソースに添付されたリソースベースのポリシーを削除する許可を付与する	権限の管理	stream*		
			table*		
DeleteTable	DeleteTable オペレーションで表およびその項目をすべて削除する許可を付与します。	書き込み	table*		
DeleteTableReplica [アクセス許可のみ]	レプリカ表およびその項目をすべて削除するアクセス許可を付与します。	書き込み	table*		
DescribeBackup	表の既存のバックアップを記述するアクセス許可を付与します。	読み取り	backup*		
DescribeContinuousBackups	指定された表のバックアップの復元設定のステータスを確認する許可を付与します。	読み取り	table*		
DescribeContributorInsights	特定の表およびグローバルセカンダリインデックスの寄稿者インサイトステータスを記述する許可を付与します。	読み取り	table*		
			index		
DescribeEndpoints	リージョンレベルのエンドポイントに関する情報を返すための許可を付与します	読み取り			
DescribeExport	表の既存のエクスポートを記述するアクセス許可を付与します。	読み取り	export*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeGlobalTable	指定したグローバル表に関する情報を返すアクセス許可を付与します。	読み取り	global-table*		
DescribeGlobalTableSettings	指定されたグローバル表に関する設定情報を返すアクセス許可を付与します。	読み取り	global-table*		
DescribeImport	既存のインポートを記述する許可を付与	読み取り	import*		
DescribeKinesisStreamingDestination	所与の表の Kinesis ストリーミングのステータスおよび関連する詳細を記述する権限を付与します。	読み取り	table*		
DescribeLimits	リージョン全体とそこで作成した任意の DynamoDB テーブルの両方について、リージョン AWS アカウント 内の の現在のプロビジョニングされた容量制限を返すアクセス許可を付与します	読み取り			
DescribeReservedCapacity [許可のみ]	1 つ以上の購入されたリザーブドキャパシティーを記述する許可を付与します。	読み取り			
DescribeReservedCapacityOfferings [許可のみ]	購入可能なリザーブドキャパシティーの提供内容を記述する許可を付与します。	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeStream	ストリームに関する情報 (例: ストリームの最新ステータス、Amazon リソースネーム (ARN)、シャードの構成、対応する DynamoDB テーブル) を返す許可を付与します。	読み取り	stream*		
DescribeTable	表に関する情報を返すアクセス許可を付与します。	読み取り	table*		
DescribeTableReplicaAutoScaling	グローバル表のすべてのレプリカにおける Auto Scaling 設定を記述する許可を付与します。	読み取り	table*		
DescribeTimeToLive	指定された表の 有効期限 (TTL) ステータスの説明をする許可を付与します。	読み取り	table*		
DisableKinesisStreamingDestination	DynamoDB テーブルから Kinesis データストリームへのレプリケーションを停止する権限を付与します。	書き込み	table*		
EnableKinesisStreamingDestination	イネーブルワークフローで選択されたタイムスタンプに従い、指定された Kinesis データストリームへの表データレプリケーションを開始する権限を付与します。	書き込み	table*		
ExportTableToPointInTime	DynamoDB 表の S3 へのエクスポートを開始するアクセス許可を付与します。	書き込み	table*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetAbacStatus [アクセス許可のみ]	アカウントの属性ベースのアクセスコントロールのステータスを表示するアクセス許可を付与します	読み取り			
GetItem	指定されたプライマリキーを持つ項目の属性のセットを返しますGetlemオペレーションへのアクセス許可を付与します。	読み取り	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:Select	
GetRecords	特定のシャード内からストリームレコードを取得する許可を付与します。	読み取り	stream*		
GetResourcePolicy	リソースのリソースベースのポリシーを表示する許可を付与する	読み取り	stream*		
			table*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetShardIterator	シャードイテレータを返すアクセス許可を付与します。	読み取り	stream*		
ImportTable	S3 から DynamoDB 表へのインポートを開始する許可を付与	書き込み	table*		
ListBackups	アカウントおよびエンドポイントに関連付けられているバックアップを一覧表示するアクセス許可を付与します。	リスト			
ListContributorInsights	現在のアカウントとエンドポイントに関連付けられているすべての表およびグローバルセカンダリインデックスの ContributorInsightsSummary を一覧表示する許可を付与します。	リスト			
ListExports	アカウントおよびエンドポイントに関連付けられているエクスポートを一覧表示するアクセス許可を付与します。	リスト			
ListGlobalTables	指定されたリージョンにレプリカを持つすべてのグローバル表を一覧表示する許可を付与します。	リスト			
ListImports	アカウントおよびエンドポイントに関連付けられているインポートを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListStreams	現在のアカウントおよびエンドポイントに関連付けられたストリーム ARN の配列を返す許可を付与します。	読み取り			
ListTables	現在のアカウントおよびエンドポイントに関連付けられた表の名前の配列を返す許可を付与します。	リスト			
ListTagsOfResource	Amazon DynamoDB リソースのすべてのタグを一覧表示する許可を付与します。	読み取り	table*		
PartiQLDelete	プライマリキーを使用してテーブルから 1 つの項目を削除する権限を付与します。	Write	table*	dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnValues	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PartiQLInsert	同じプライマリキーを持つ項目がテーブルに存在しない場合に新しい項目を作成する権限を付与します。	Write	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys	
PartiQLSelect	テーブルまたはインデックスから項目の属性セットを読み取る権限を付与します	Read	table*		
			index		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:FullTableScan dynamodb:LeadingKeys dynamodb:Select	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PartiQLUpdate	既存の項目の属性を編集する権限を付与します。	書き込み	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnValues	
PurchaseReservedCapacityOfferings [アクセス許可のみ]	アカウントで使用するリザーブドキャパシティーを購入する許可を付与します。	書き込み			
PutItem	新しい項目を作成するか、古い項目を新しい項目に置き換える許可を付与します。	書き込み	table*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
PutResourcePolicy	リソースにリソースベースのポリシーをアタッチする許可を付与する	権限の管理	stream* table*		
Query	表のプライマリキーもしくはセカンダリインデックスを使用してその表もしくはインデックスの項目に直接アクセスする許可を付与します。	読み取り	table* index		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues dynamodb:Select	
RestoreTableFromAwsBackup [許可のみ]	AWS Backup の復旧ポイントから新しいテーブルを作成するアクセス許可を付与します	書き込み	table*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RestoreTableFromBackup	既存のバックアップから新しい 表を作成するアクセス権限を付与します。	書き込み	backup*		dynamodb:BatchWriteItem dynamodb:DeleteItem dynamodb:GetItem dynamodb:PutItem dynamodb:Query dynamodb:Scan dynamodb:UpdateItem
			table*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RestoreTableToPointInTime	表を任意の時点に復元する許可を付与します。	書き込み	table*		dynamodb:BatchWriteItem dynamodb:DeleteItem dynamodb:GetItem dynamodb:PutItem dynamodb:Query dynamodb:Scan dynamodb:UpdateItem
Scan	表もしくはセカンダリインデックスの各項目にアクセスして、1 つ以上の項目または項目属性を返す許可を付与します。	読み取り	table*		
			index		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				dynamodb:Attributes dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues dynamodb:Select	
StartAwsBackupJob [許可のみ]	高度な機能を有効にした AWS バックアップでバックアップを作成するアクセス許可を付与します	書き込み	table*		
TagResource	タグのセットを Amazon DynamoDB リソースに関連付ける許可を付与します。	Tagging	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Amazon DynamoDB リソースからタグの関連付けを削除する許可を付与します。	Tagging	table*		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateAbacStatus [アクセス許可のみ]	アカウントの属性ベースのアクセスコントロールのステータスを更新するアクセス許可を付与します	権限の管理			
UpdateContinuousBackups	連続バックアップを有効または無効にするアクセス許可を付与します。	書き込み	table*		
UpdateContributorInsights	特定のテーブルもしくはグローバルセカンダリインデックスの寄稿者インサイトのステータスを更新します。	書き込み	table*		
			index		
UpdateGlobalTable	指定したグローバル表にユーザーがレプリカを追加または削除するアクセス許可を付与します。	書き込み	global-table*		
			table*		
UpdateGlobalTableSettings	指定されたグローバル表内の設定を更新する権限を付与します。	書き込み	global-table*		
			table*		
UpdateGlobalTableVersion [アクセス許可のみ]	指定されたグローバルテーブル内のバージョンを更新するための許可を付与します	書き込み	global-table*		
			table		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateItem	既存項目の属性を編集、もしくは存在しない場合は新しい項目を表に追加する許可を付与します。	書き込み	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
UpdateKinesisStreamingDestination	指定された Kinesis データストリームのデータレプリケーション設定を更新する許可を付与する	書き込み	table*		
UpdateTable	特定の表のプロビジョンドスループット設定、グローバルセカンダリインデックス、もしくは DynamoDB Streams 設定を変更する許可を付与します。	書き込み	table*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateTableReplicaAutoScaling	レプリカ表の Auto Scaling 設定を更新する許可を付与します。	書き込み	table*		
UpdateTimeToLive	指定された表の TTL を有効または無効にするアクセス許可を付与します	書き込み	table*		

Amazon DynamoDB で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
index	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/index/${IndexName}`	aws:ResourceTag/${TagKey}
stream	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/stream/${StreamLabel}`	
table	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}`	aws:ResourceTag/${TagKey}
backup	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/backup/${BackupName}`	

リソースタイプ	ARN	条件キー
export	arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/export/${ExportName}	
global-table	arn:${Partition}:dynamodb::${Account}:global-table/${GlobalTableName}	
import	arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/import/${ImportName}	

Amazon DynamoDB の条件キー

Amazon DynamoDB では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

> **Note**
>
> IAM ポリシーを使用してコンテキストキーで DynamoDB アクセスを制限する方法については、Amazon DynamoDB 開発者ガイドの「詳細に設定されたアクセスコントロールのための IAM ポリシー条件の使用」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列

条件キー	説明	タイプ
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
dynamodb:Attributes	テーブルの属性 (フィールドまたは列) の名前でフィルタリングします	ArrayOfString
dynamodb:EnclosingOperation	トランザクション API の呼び出しをブロックしてアクセスをフィルタリングし、非トランザクション API の呼び出しを許可します。その逆も可能です	String
dynamodb:FullTableScan	テーブルのフルスキャンをブロックしてアクセスをフィルタリングします	Bool
dynamodb:LeadingKeys	テーブルのパーティションキーでアクセスをフィルタリングします	ArrayOfString
dynamodb:ReturnConsumedCapacity	リクエストの ReturnConsumedCapacity パラメータでアクセスをフィルタリングします。「TOTAL」もしくは「NONE」を含みます。	String
dynamodb:ReturnValues	リクエストの ReturnValues パラメータでアクセスをフィルタリングします。次のいずれかを含みます: 「ALL_OLD」、「UPDATED_OLD」、「ALL_NEW」、「UPDATED_NEW」もしくは「NONE」	String
dynamodb:Select	クエリまたはスキャンリクエストの Select パラメータでアクセスをフィルタリングします	String

Amazon DynamoDB Accelerator (DAX) のアクション、リソース、および条件キー

Amazon DynamoDB Accelerator (DAX) (サービスプレフィックス: dax) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon DynamoDB Accelerator (DAX) で定義されるアクション
- Amazon DynamoDB Accelerator (DAX) で定義されるリソースタイプ
- Amazon DynamoDB Accelerator (DAX) の条件キー

Amazon DynamoDB Accelerator (DAX) で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイ

プが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchGetItem	1 つ以上の表から 1 つ以上の項目の属性を返す許可を付与します。	読み込み	application*		
BatchWriteItem	1 つ以上の表を配置もしくは削除する許可を付与します。	書き込み	application*		
ConditionCheckItem	ConditionCheckItem オペレーションにより、指定されたプライマリキーを持つ項目で一連の属性が存在するかどうか	読み込み	application*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	がチェックするアクセス許可を付与します				

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateCluster	DAX クラスターを作成するアクセス許可を付与します	書き込み	application*		dax:CreateParameterGroup dax:CreateSubnetGroup ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:GetRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					iam:PassRole
CreateParameterGroup	パラメータグループを作成する許可を付与。	書き込み			
CreateSubnetGroup	サブネットグループを作成するアクセス許可を付与します	書き込み			
DecreaseReplicationFactor	DAX クラスターから 1 つまたは複数のノードを削除するアクセス許可を付与します	書き込み	application*		
DeleteCluster	以前にプロビジョニングされた DAX クラスターを削除するアクセス許可を付与します	書き込み	application*		
DeleteItem	プライマリキーを使用してテーブルから 1 つの項目を削除する権限を付与します。	書き込み	application*		
				dax:EnclosingOperation	
DeleteParameterGroup	指定されたパラメータグループを削除するアクセス許可を付与します	書き込み			
DeleteSubnetGroup	サブネットグループを削除するアクセス許可を付与します	書き込み			
DescribeClusters	プロビジョニングされた DAX クラスターに関する情報を返すアクセス許可を付与します	リスト	application		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeDefaultParameters	DAX のデフォルトのシステムパラメータ情報を返すアクセス許可を付与します	リスト			
DescribeEvents	DAX クラスターとパラメータグループに関連するイベントを返すアクセス許可を付与します	リスト			
DescribeParameterGroups	パラメータグループの説明のリストを返すアクセス許可を付与します	リスト			
DescribeParameters	特定のパラメータグループの詳細なパラメータリストを返すアクセス許可を付与します	読み込み			
DescribeSubnetGroups	サブネットグループの説明のリストを返すアクセス許可を付与します	リスト			
GetItem	指定されたプライマリキーを持つ項目の属性のセットを返しますGetIemオペレーションへのアクセス許可を付与します。	読み込み	application*		
				dax:EnclosingOperation	
IncreaseReplicationFactor	DAX クラスターに 1 つまたは複数のノードを追加するアクセス許可を付与します	書き込み	application*		
ListTags	DAX クラスターのすべてのタグのリストを返すアクセス許可を付与します	読み込み	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutItem	新しい項目を作成するか、古い項目を新しい項目に置き換える許可を付与します。	書き込み	application*		
				dax:EnclosingOperation	
Query	表のプライマリキーもしくはセカンダリインデックスを使用してその表もしくはインデックスの項目に直接アクセスする許可を付与します。	読み込み	application*		
RebootNode	DAX クラスターの単一ノードを再起動するアクセス許可を付与します	書き込み	application*		
Scan	表もしくはセカンダリインデックスの各項目にアクセスして、1 つ以上の項目または項目属性を返す許可を付与します。	読み込み	application*		
TagResource	一連のタグを DAX リソースに関連付けるアクセス許可を付与します	Tagging	application*		
UntagResource	DAX リソースからタグの関連付けを削除するアクセス許可を付与します	Tagging	application*		
UpdateCluster	DAX クラスターで使用する設定を変更するアクセス許可を付与します	書き込み	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateItem	既存項目の属性を編集、もしくは存在しない場合は新しい項目を表に追加する許可を付与します。	書き込み	application*		
				dax:EnclosingOperation	
UpdateParameterGroup	パラメータグループのパラメータを変更する許可を付与	書き込み			
UpdateSubnetGroup	既存のサブネットグループを変更するアクセス許可を付与します	書き込み			

Amazon DynamoDB Accelerator (DAX) で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
application	`arn:${Partition}:dax:${Region}:${Account}:cache/${ClusterName}`	

Amazon DynamoDB Accelerator (DAX) の条件キー

Amazon DynamoDB Accelerator (DAX) では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさら

に絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
dax:EnclosingOperation	トランザクション API コールのブロックと非トランザクション API コールの許可に使用します。その逆も可能です。	String

Amazon EC2 Auto Scaling のアクション、リソース、および条件キー

Amazon EC2 Auto Scaling (サービスプレフィックス: `autoscaling`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon EC2 Auto Scaling で定義されるアクション
- Amazon EC2 Auto Scaling で定義されるリソースタイプ
- Amazon EC2 Auto Scaling の条件キー

Amazon EC2 Auto Scaling で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AttachInstances	1 つ以上の EC2 インスタンスを、指定された Auto Scaling グループにアタッチする許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
AttachLoadBalancerTargetGroups	1 つ以上のターゲットグループを、指定された Auto Scaling グループにアタッチする許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TargetGroupARNs	
AttachLoadBalancers	1 つ以上のロードバランサーを、指定された Auto Scaling グループにアタッチする許可を付与	書き込み	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				autoscaling:LoadBalancerNames	
AttachTrafficSources	Auto Scaling グループに 1 つ以上のトラフィックソースをアタッチするための許可を付与します	書き込み	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TrafficSourceIdentifiers	
BatchDeleteScheduledAction	指定されたスケジュールされたアクションを削除する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchPutScheduledUpdateGroupAction	Auto Scaling グループの複数のスケジュールされたスケーリングアクションを作成または更新する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CancelInstanceRefresh	実行中のインスタンスの更新オペレーションをキャンセルする許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CompleteLifecycleAction	指定された結果の指定されたトークンまたはインスタンスのライフサイクルアクションを完了する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateAutoScalingGroup	指定された名前と属性で、Auto Scaling グループを作成する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:CreateServiceLinkedRole iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				autoscaling:CapacityReservationIds autoscaling:CapacityReservationResourceGroupArns autoscaling:InstanceTypes autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSpecified autoscaling:LoadBalancerNames	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				autoscaling:MaxSize autoscaling:MinSize autoscaling:TargetGroupARNs autoscaling:TrafficSourceIdentifiers autoscaling:VPCZoneIdentifiers aws:RequestTag/${TagKey} aws:TagKeys	
CreateLaunchConfiguration	起動設定を作成する許可を付与	Write	launchConfiguration*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				autoscaling:ImageId autoscaling:InstanceType autoscaling:SpotPrice autoscaling:MetadataHttpTokens autoscaling:MetadataHttpPutResponseHopLimit autoscaling:MetadataHttpEndpoint	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateOrUpdateTags	指定された Auto Scaling グループのタグを作成または更新する許可を付与	タグ付け	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAutoScalingGroup	指定された Auto Scaling グループを削除する許可を付与。	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteLaunchConfiguration	指定された起動設定を削除する許可を付与	Write	launchConfiguration*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteLifecycleHook	指定したライフサイクルフックを削除する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteNotificationConfiguration	指定された通知を削除する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeletePolicy	指定された Auto Scaling ポリシーを削除する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteScheduledAction	指定されたスケジュールされたアクションを削除する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteTags	指定されたタグを削除する許可を付与	タグ付け	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteWarmPool	Auto Scaling グループに関連付けられたウォームプールを削除するためのアクセス許可を付与	書き込み	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DescribeAccountLimits	の現在の Auto Scaling リソース制限を記述するアクセス許可を付与します AWS アカウント	リスト			
DescribeAdjustmentTypes	PutScalingPolicy で使用するポリシー調整を記述する許可を付与	リスト			
DescribeAutoScalingGroups	1 つ以上の Auto Scaling グループを記述する許可を付与 名前のリストを指定しない場合は、そのコールによって、すべての Auto Scaling グループの説明が記述されます	リスト			
DescribeAutoScalingInstances	1 つ以上の Auto Scaling インスタンスを記述する許可を付与 リストを指定しない場合は、そのコールによって、すべてのインスタンスが記述されます	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeAutoScalingNotificationTypes	Auto Scaling でサポートされている通知タイプの説明を記述する許可を付与	リスト			
DescribeInstanceRefreshes	Auto Scaling グループの 1 つ以上のインスタンスの更新を記述する許可を付与	リスト			
DescribeLaunchConfigurations	1 つ以上の軌道設定を記述する許可を付与。名前のリストを省略した場合は、そのコールによって、すべての起動設定が記述されます	リスト			
DescribeLifecycleHookTypes	使用可能なライフサイクルフックのタイプを記述する許可を付与	リスト			
DescribeLifecycleHooks	指定された Auto Scaling グループのライフサイクルフックを記述する許可を付与	リスト			
DescribeLoadBalancerTargetGroups	指定された Auto Scaling グループのターゲットグループを記述する許可を付与	リスト			
DescribeLoadBalancers	指定された Auto Scaling グループのロードバランサーを記述する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeMetricCollectionTypes	Auto Scaling の利用可能な CloudWatch メトリクスを記述する許可を付与	リスト			
DescribeNotificationConfigurations	指定された Auto Scaling グループに関連付けられている通知アクションを記述する許可を付与	リスト			
DescribePolicies	指定された Auto Scaling グループのポリシーを記述する許可を付与	リスト			
DescribeScalingActivities	指定された Auto Scaling グループの 1 つ以上のスケーリングアクティビティを記述する許可を付与	リスト			
DescribeScalingProcessTypes	ResumeProcesses および SuspendProcesses で使用するスケーリングプロセスの種類を記述する許可を付与	リスト			
DescribeScheduledActions	実行されていない Auto Scaling グループでスケジュールされているアクションを記述する許可を付与	リスト			
DescribeTags	指定されたタグを記述する許可を付与	Read			
DescribeTerminationPolicyTypes	Auto Scaling でサポートされている終了ポリシーを記述する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeTrafficSources	指定された Auto Scaling グループのターゲットグループを記述する許可を付与	リスト			
DescribeWarmPool	Auto Scaling グループに関連付けられたウォームプールを記述するためのアクセス許可を付与	リスト			
DetachInstances	指定された Auto Scaling グループから 1 つ以上のインスタンスを削除する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DetachLoadBalancerTargetGroups	指定された Auto Scaling グループから 1 つ以上のターゲットグループをデタッチする許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TargetGroupARNs	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DetachLoadBalancers	指定された Auto Scaling グループから 1 つ以上のロードバランサーを削除する許可を付与	書き込み	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:LoadBalancerNames	
DetachTrafficSources	Auto Scaling グループから 1 つ以上のトラフィックソースをデタッチするための許可を付与します	書き込み	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TrafficSourceIdentifiers	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisableMetricsCollection	指定された Auto Scaling グループに対する指定されたメトリクスのモニタリングを無効にする許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
EnableMetricsCollection	指定された Auto Scaling グループに対する指定されたメトリクスのモニタリングを有効にする許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
EnterStandby	指定されたインスタンスをスタンバイモードから解除する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ExecutePolicy	指定されたポリシーを実行する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
ExitStandby	指定されたインスタンスをスタンバイモードから解除する許可を付与	書き込み	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
GetPredictiveScalingForecast	予測スケーリングポリシーの予測データを取得する許可を付与	リスト			
PutLifecycleHook	指定された Auto Scaling グループのライフサイクルフックを作成または更新する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutNotificationConfiguration	特定のイベントが発生したときに Auto Scaling グループが通知を送信するように設定する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutScalingPolicy	Auto Scaling グループのポリシーを作成または更新する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutScheduledUpdateGroupAction	指定された Auto Scaling グループのスケジュールされたスケーリングアクションを作成または更新する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				autoscaling:MaxSize autoscaling:MinSize	
PutWarmPool	指定された Auto Scaling グループに関連付けられたウォームプールを作成または更新するためのアクセス許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
RecordLifecycleActionHeartbeat	指定されたトークンまたはインスタンスに関連付けられたライフサイクルアクションのハートビートを記録する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ResumeProcesses	指定された Auto Scaling グループに対して、停止した指定の Auto Scaling プロセス、またはすべての中断プロセスを再開する許可を付与	書き込み	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
RollbackInstanceRefresh	進行中のインスタンス更新オペレーションをロールバックするための許可を付与します	書き込み	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
SetDesiredCapacity	指定された Auto Scaling グループのサイズを設定する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SetInstanceHealth	指定されたインスタンスのヘルスステータスを設定する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
SetInstanceProtection	指定されたインスタンスのインスタンス保護設定を更新する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
StartInstanceRefresh	新しいインスタンスの更新オペレーションを開始する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SuspendProcesses	指定された Auto Scaling グループに対して、指定された Auto Scaling プロセス、またはすべてのプロセスを中断する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
TerminateInstanceInAutoScalingGroup	指定されたインスタンスを終了し、必要に応じてグループサイズを調整する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
UpdateAutoScalingGroup	指定された Auto Scaling グループの設定を更新する許可を付与	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				autoscaling:CapacityReservationIds autoscaling:CapacityReservationResourceGroupArns autoscaling:InstanceTypes autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSpecified autoscaling:MaxSize autoscaling:MinSize	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				autoscaling:VPCZoneIdentifiers	

Amazon EC2 Auto Scaling で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
autoScalingGroup	arn:${Partition}:autoscaling:${Region}:${Account}:autoScalingGroup:${GroupId}:autoScalingGroupName/${GroupFriendlyName}	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}
launchConfiguration	arn:${Partition}:autoscaling:${Region}:${Account}:launchConfiguration:${Id}:launchConfigurationName/${LaunchConfigurationName}	

Amazon EC2 Auto Scaling の条件キー

Amazon EC2 Auto Scaling では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
autoscaling:CapacityReservationIds	キャパシティ予約 IDs	ArrayOfString
autoscaling:CapacityReservationResourceGroupArns	キャパシティ予約リソースグループの ARN に基づいてアクセスをフィルタリングします	ArrayOfString
autoscaling:ImageId	起動設定の AMI ID に基づいて、アクセスをフィルタリングする	String
autoscaling:InstanceType	起動設定の インスタンス に基づいて、アクセスをフィルタリングする	String
autoscaling:InstanceTypes	混合インスタンスポリシーの起動テンプレートへの上書きとして存在するインスタンスタイプに基づいてアクセスをフィルタリングする これを使用して、ポリシーで明示的に定義できるインスタンス タイプを限定する	String
autoscaling:LaunchConfigurationName	起動設定の名前に基づいて、アクセスをフィルタリングします	文字列
autoscaling:LaunchTemplateVersionSpecified	ユーザーが起動テンプレートの任意のバージョンを指定できるか、最新バージョンまたはデフォルトバージョンのみを指定できるかによって、アクセスをフィルタリングします	Bool

条件キー	説明	[Type] (タイプ)
autoscaling:LoadBalancerNames	ロードバランサーの名前に基づいて、アクセスをフィルタリングします	ArrayOfString
autoscaling:MaxSize	要求される最大スケーリングサイズに基づいて、アクセスをフィルタリングする	数値
autoscaling:MetadataHttpEndpoint	HTTP エンドポイントがインスタンスメタデータサービスに対して有効になっているかどうかに基づいて、アクセスをフィルタリングします	文字列
autoscaling:MetadataHttpPutResponseHopLimit	インスタンスメタデータサービスを呼び出すときに、許可されたホップ数に基づいて、アクセスをフィルタリングします	数値
autoscaling:MetadataHttpTokens	インスタンスメタデータサービスを呼び出すときに、トークンが必要かどうかに基づいて、アクセスをフィルタリングします (オプションまたは必須)	String
autoscaling:MinSize	要求される最小スケーリングサイズに基づいて、アクセスをフィルタリングする	数値
autoscaling:ResourceTag/${TagKey}	リソースに関連付けられているタグに基づいてアクションをフィルタリングします	String
autoscaling:SpotPrice	起動設定のスポットインスタンスの料金に基づいて、アクセスをフィルタリングする	数値
autoscaling:TargetGroupARNs	ターゲットグループの ARN に基づいて、アクセスをフィルタリングします	ArrayOfARN

条件キー	説明	[Type] (タイプ)
autoscaling:TrafficSourceIdentifiers	トラフィックソースの識別子に基づいてアクセスをフィルタリング	ArrayOfString
autoscaling:VPCZoneIdentifiers	VPC ゾーンの識別子に基づいて、アクセスをフィルタリングします	ArrayOfString
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられているタグに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーに基づいてアクションをフィルタリングします	ArrayOfString

Amazon EC2 Image Builder のアクション、リソース、および条件キー

Amazon EC2 Image Builder (サービスプレフィックス: `imagebuilder`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon EC2 Image Builder で定義されるアクション
- Amazon EC2 Image Builder で定義されるリソースタイプ

- Amazon EC2 Image Builder の条件キー

Amazon EC2 Image Builder で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelImageCreation	イメージの作成をキャンセルする許可を付与	書き込み	image*		
CancelLifecycleExecution	ライフサイクル実行をキャンセルするためのアクセス許可を付与	書き込み	lifecycleExecution*		
CreateComponent	新しいコンポーネントを作成する許可を付与	書き込み	component*		imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateContainerRecipe	新しいコンテナ recipe を作成する許可を付与	書き込み	containerRecipe*		ec2:DescribeImages ecr:DescribeImages ecr:DescribeRepositories imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					s3:GetObject s3:ListBucket ssm:GetParameter
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateDistributionConfiguration	新しいディストリビューション設定を作成する許可を付与	書き込み	distributionConfiguration*		ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplates ec2:ModifyLaunchTemplate imagebuilder:TagResource s3:ListBucket ssm:GetParameter
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateImage	新しいイメージを作成する許可を付与	書き込み	image*		ecr:BatchGetRepositoryScanningConfiguration ecr:DescribeRepositories iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetInfrastruct

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ureConfiguration imagebuilder:GetWorkflow imagebuilder:TagResource inspector2:BatchGetAccountStatus
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateImagePipeline	新しいイメージパイプラインを作成する許可を付与	書き込み	imagePipeline*		ecr:BatchGetRepositoryScanningConfiguration ecr:DescribeRepositories iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetInfrastruct

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ureConfiguration imagebuilder:GetWorkflow imagebuilder:TagResource inspector2:BatchGetAccountStatus
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateImageRecipe	新しいイメージ recipe を作成する許可を付与	書き込み	imageRecipe*		ec2:DescribeImages imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource ssm:GetParameter
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateInfrastructureConfiguration	新しいインフラストラクチャ設定を作成する許可を付与	書き込み	infrastructureConfiguration*		ec2:DescribeAvailabilityZones ec2:DescribeHosts iam:PassRole imagebuilder:TagResource resource-groups:GetGroup sns:Publish

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/${TagKey} imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn	
CreateLifecyclePolicy	新しいライフサイクルポリシーを作成するためのアクセス許可を付与	書き込み	lifecyclePolicy*		iam:PassRole imagebuilder:TagResource

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys imagebuilder:LifecyclePolicyResourceType	
CreateWorkflow	新しいワークフローを作成する許可を付与	書き込み	workflow*		imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext s3:GetObject s3:ListBucket

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComponent	コンポーネントを削除する許可を付与	書き込み	component*		
DeleteContainerRecipe	コンテナ recipe を削除する権限を付与します。	書き込み	containerRecipe*		
DeleteDistributionConfiguration	ディストリビューション設定を削除する許可を付与	書き込み	distributionConfiguration*		
DeleteImage	イメージを削除する許可を付与	書き込み	image*		
DeleteImagePipeline	イメージパイプラインを削除する許可を付与	書き込み	imagePipeline*		
DeleteImageRecipe	イメージ recipe を削除する許可を付与。	書き込み	imageRecipe*		
DeleteInfrastructureConfiguration	インフラストラクチャ設定を削除する許可を付与	書き込み	infrastructureConfiguration*		
DeleteLifecyclePolicy	ライフサイクルポリシーを削除するアクセス許可を付与	書き込み	lifecyclePolicy*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteWorkflow	ワークフローを削除するアクセス許可を与えます。	書き込み	workflow*		
GetComponent	コンポーネントの詳細を表示する許可を付与	読み込み	component*		kms:Decrypt
GetComponentPolicy	コンポーネントに関連付けられているリソースポリシーを表示する許可を付与	読み込み	component*		
GetContainerRecipe	コンテナ recipe の詳細を表示する許可を付与	読み込み	containerRecipe*		
GetContainerRecipePolicy	コンテナ recipe に関連付けられているリソースポリシーを表示する許可を付与	読み込み	containerRecipe*		
GetDistributionConfiguration	ディストリビューション設定の詳細を表示する許可を付与	読み込み	distributionConfiguration*		
GetImage	イメージの詳細を表示する許可を付与	読み込み	image*		
GetImagePipeline	イメージパイプラインの詳細を表示する許可を付与	読み込み	imagePipeline*		
GetImagePolicy	イメージに関連付けられているリソースポリシーを表示する許可を付与	読み込み	image*		
GetImageRecipe	イメージ recipe の詳細を表示する許可を付与	読み込み	imageRecipe*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetImageRecipePolicy	イメージ recipe に関連付けられているリソースポリシーを表示する許可を付与	読み込み	imageRecipe*		
GetInfrastructureConfiguration	インフラストラクチャ設定の詳細を表示する許可を付与	読み取り	infrastructureConfiguration*		
GetLifecycleExecution	ライフサイクル実行に関する詳細を表示するためのアクセス許可を付与	読み取り	lifecycleExecution*		
GetLifecyclePolicy	ライフサイクルポリシーに関する詳細を表示するためのアクセス許可を付与	読み取り	lifecyclePolicy*		
GetMarketplaceResource	Marketplace が提供するリソースを取得する許可を付与	読み取り	component*		
GetWorkflow	ワークフローの詳細を表示するアクセス許可を付与	読み取り	workflow*		kms:Decrypt
GetWorkflowExecution	ワークフロー実行の詳細を表示するアクセス許可を付与	読み取り	workflowExecution*		
GetWorkflowStepExecution	ワークフローステップ実行の詳細を表示するアクセス許可を付与	読み取り	workflowStepExecution*		kms:Decrypt

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ImportComponent	新しいコンポーネントをインポートする許可を付与	書き込み	component *		imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ImportDiskImage	ディスクイメージをインポートするアクセス許可を付与します	書き込み	imageVersion*		iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow imagebuilder:TagResource s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ImportVmImage	画像をインポートする許可を付与します	書き込み	imageVersion*		ec2:DescribeImages ec2:DescribeImportImageTasks iam:CreateServiceLinkedRole imagebuilder:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
ListComponentBuildVersions	アカウントのコンポーネントビルドバージョンを一覧表示する許可を付与	リスト	allComponentBuildVersions*		
ListComponents	アカウントが所有する、またはアカウントと共有するコンポーネントバージョンを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListContainerRecipes	アカウントが所有するかアカウントと共有するコンテナ recipe を一覧表示する許可を付与	リスト			
ListDistributionConfigurations	アカウントのディストリビューション設定を一覧表示する許可を付与	リスト			
ListImageBuildVersions	アカウントのイメージビルドバージョンを一覧表示する許可を付与	リスト	allImageBuildVersions*		
ListImagePackages	指定したイメージにインストールされているパッケージのリストを返すアクセス許可を付与	リスト	image*		
ListImagePipelineImages	指定したパイプラインによって作成されたイメージのリストを返すアクセス許可を付与	リスト	imagePipeline*		
ListImagePipelines	アカウントのイメージパイプラインを一覧表示する許可を付与	リスト			
ListImageRecipes	アカウントが所有する、またはアカウントと共有するイメージ recipe を一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListImageScanFindingAggregations	アカウントのイメージスキャンによる結果の集計を一覧表示するアクセス許可を付与	リスト	image		
			imagePipeline		
ListImageScanFindings	アカウント内のイメージに対するイメージスキャンの結果を一覧表示するアクセス許可を付与	リスト	image		inspector2:ListFindings
			imagePipeline		
ListImages	アカウントが所有する、またはアカウントと共有するイメージバージョンを一覧表示する許可を付与	リスト			
ListInfrastructureConfigurations	アカウントのインフラストラクチャ設定を一覧表示する許可を付与	リスト			
ListLifecycleExecutionResources	指定されたライフサイクル実行用のリソースを一覧表示するためのアクセス許可を付与	リスト	lifecycleExecution*		
ListLifecycleExecutions	指定されたリソースのライフサイクル実行を一覧表示するためのアクセス許可を付与	リスト	image		
			lifecyclePolicy		
ListLifecyclePolicies	アカウントのライフサイクルポリシーを一覧表示するためのアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTagsForResource	Image Builder リソースのタグを一覧表示する許可を付与	読み取り	component		
			containerRecipe		
			distributionConfiguration		
			image		
			imagePipeline		
			imageRecipe		
			infrastructureConfiguration		
			lifecyclePolicy		
			workflow		
ListWaitingWorkflowSteps	発信者アカウントに待機中のワークフローステップを一覧表示する許可を付与	リスト			
ListWorkflowBuildVersions	アカウントのワークフロービルドバージョンを一覧表示する許可を付与	リスト	allWorkflowBuildVersions*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListWorkflowExecutions	指定したイメージでのワークフロー実行を一覧表示する許可を付与	リスト	image*		
ListWorkflowStepExecutions	指定したワークフローのワークフローステップ実行を一覧表示するアクセス許可を付与	リスト	workflowExecution*		kms:Decrypt
ListWorkflows	アカウントが所有する、またはアカウントと共有するワークフローバージョンを一覧表示する許可を付与	リスト			
PutComponentPolicy	コンポーネントに関連付けられているリソースポリシーを設定する許可を付与	Permissions management	component*		
PutContainerRecipePolicy	コンテナ recipe に関連付けられているリソースポリシーを設定する許可を付与	Permissions management	containerRecipe*		
PutImagePolicy	イメージに関連付けられたリソースポリシーを設定する許可を付与	Permissions management	image*		
PutImageRecipePolicy	イメージ recipe に関連付けられているリソースポリシーを設定する許可を付与	権限の管理	imageRecipe*		
SendWorkflowStepAction	ワークフローステップにアクションを送信するための許可を付与	書き込み	image*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			workflowStepExecution*		
StartImagePipelineExecution	パイプラインから新しいイメージを作成する許可を付与	書き込み	imagePipeline*		iam:CreateServiceLinkedRole imagebuilder:GetImagePipeline
StartResourceStateUpdate	指定されたリソースの状態の更新を開始するためのアクセス許可を付与	書き込み	image*		
TagResource	Image Builder リソースにタグを付けるアクセス許可を付与します	タグ付け	component		
			containerRecipe		
			distributionConfiguration		
			image		
			imagePipeline		
			imageRecipe		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			infrastructureConfiguration		
			lifecyclePolicy		
			workflow		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Image Builder リソースのタグを解除する許可を付与	タグ付け	component		
			containerRecipe		
			distributionConfiguration		
			image		
			imagePipeline		
			imageRecipe		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			infrastructureConfiguration		
			lifecyclePolicy		
			workflow		
				aws:TagKeys	
UpdateDistributionConfiguration	既存のディストリビューション設定を更新する許可を付与	書き込み	distributionConfiguration*		ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplates ec2:ModifyLaunchTemplate s3:ListBucket ssm:GetParameter

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateImagePipeline	既存のイメージパイプラインを更新する許可を付与	書き込み	imagePipeline*		ecr:BatchGetRepositoryScanningConfiguration ecr:DescribeRepositories iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetInfrastruct

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ureConfiguration imagebuilder:GetWorkflow inspector2:BatchGetAccountStatus
UpdateInfrastructureConfiguration	既存のインフラストラクチャ設定を更新する許可を付与	書き込み	infrastructureConfiguration*		ec2:DescribeAvailabilityZones ec2:DescribeHosts iam:PassRole resource-groups:GetGroup sns:Publish

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/${TagKey} imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn	
UpdateLifecyclePolicy	既存のライフサイクルポリシーを更新するためのアクセス許可を付与	書き込み	lifecyclePolicy*		iam:PassRole
				imagebuilder:LifecyclePolicyResourceType	

Amazon EC2 Image Builder で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアク

ションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
component	arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}/${ComponentBuildVersion}	aws:ResourceTag/${TagKey}
distributionConfiguration	arn:${Partition}:imagebuilder:${Region}:${Account}:distribution-configuration/${DistributionConfigurationName}	aws:ResourceTag/${TagKey}
image	arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}/${ImageBuildVersion}	aws:ResourceTag/${TagKey}
imageVersion	arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}	aws:ResourceTag/${TagKey}
imageRecipe	arn:${Partition}:imagebuilder:${Region}:${Account}:image-recipe/${ImageRecipeName}/${ImageRecipeVersion}	aws:ResourceTag/${TagKey}
containerRecipe	arn:${Partition}:imagebuilder:${Region}:${Account}:container-recipe/${ContainerRecipeName}/${ContainerRecipeVersion}	aws:ResourceTag/${TagKey}
imagePipeline	arn:${Partition}:imagebuilder:${Region}:${Account}:image-pipeline/${ImagePipelineName}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
infrastructureConfiguration	arn:${Partition}:imagebuilder:${Region}:${Account}:infrastructure-configuration/${ResourceId}	aws:ResourceTag/${TagKey}
lifecycleExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:lifecycle-execution/${LifecycleExecutionId}	
lifecyclePolicy	arn:${Partition}:imagebuilder:${Region}:${Account}:lifecycle-policy/${LifecyclePolicyName}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow/${WorkflowType}/${WorkflowName}/${WorkflowVersion}/${WorkflowBuildVersion}	aws:ResourceTag/${TagKey}
workflowExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow-execution/${WorkflowExecutionId}	
workflowStepExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow-step-execution/${WorkflowStepExecutionId}	
allComponentBuildVersions	arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}/*	
allImageBuildVersions	arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}/*	

リソースタイプ	ARN	条件キー
allWorkflowBuildVersions	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow/${WorkflowType}/${WorkflowName}/${WorkflowVersion}/*	

Amazon EC2 Image Builder の条件キー

Amazon EC2 Image Builder では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString
imagebuilder:CreatedResourceTag/${TagKey}	Image Builder によって作成されたリソースにアタッチされたタグキーと値のペアによってアクセスをフィルタリングします	文字列
imagebuilder:CreatedResourceTagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

条件キー	説明	[Type] (タイプ)
imagebuilder:Ec2MetadataHttpTokens	リクエストで指定された EC2 インスタンスメタデータの HTTP トークンの要件により、アクセスをフィルタリングします	String
imagebuilder:LifecyclePolicyResourceType	リクエストで指定されたライフサイクルポリシーのリソースタイプでアクセスをフィルタリングします	String
imagebuilder:StatusTopicArn	ターミナル状態通知が発行されるリクエスト内の SNS トピック Arn により、アクセスをフィルタリングします	ARN

Amazon EC2 Instance Connect のアクション、リソース、および条件キー

Amazon EC2 Instance Connect (サービスプレフィックス: `ec2-instance-connect`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon EC2 Instance Connect で定義されるアクション
- Amazon EC2 Instance Connect で定義されるリソースタイプ
- Amazon EC2 Instance Connect の条件キー

Amazon EC2 Instance Connect で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
OpenTunnel	EC2 Instance Connect Endpoint を使用して、EC2 インスタンスへの SSH 接続を確立する許可を付与	書き込み	instance-connect-endpoint*		
			instance-connect-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2-instance-connect:remotePort ec2-instance-connect:privateIpAddress ec2-instance-connect:MaxTunnelDuration	
SendSSHPublicKey	標準 SSH に使用するための指定された EC2 インスタンスに	書き込み	instance*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	SSH 公開キーをプッシュするアクセス許可を付与します			ec2:osuser	
SendSerialConsoleSSHPublicKey	シリアルコンソールの SSH で使用するための指定された EC2 インスタンスに SSH 公開キーをプッシュするアクセス許可を付与します	書き込み	instance*		

Amazon EC2 Instance Connect で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
instance	arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}
instance-connect-endpoint	arn:${Partition}:ec2:${Region}:${Account}:instance-connect-endpoint/${InstanceConnectEndpointId}	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}

Amazon EC2 Instance Connect の条件キー

Amazon EC2 Instance Connect Service は、IAM ポリシーの `Condition` 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグによりアクセスをフィルタリングします	String
ec2-instance-connect:maxTunnelDuration	インスタンスに関連付けられた最大セッション時間でアクセスをフィルタリング	数値
ec2-instance-connect:privateIpAddress	インスタンスに関連付けられたプライベート IP アドレスでアクセスをフィルタリング	IPAddress
ec2-instance-connect:remotePort	インスタンスに関連付けられたポート番号でアクセスをフィルタリング	数値
ec2:ResourceTag/${TagKey}	リソースに関連付けられたタグによりアクセスをフィルタリングします	String
ec2:osuser	インスタンスの起動に使用した AMI のデフォルトユーザー名を指定して、アクセスをフィルタリングします。	String

Amazon EKS Auth のアクション、リソース、および条件キー

Amazon EKS Auth (サービスプレフィックス: eks-auth) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon EKS Auth で定義されるアクション
- Amazon EKS Auth で定義されるリソースタイプ
- Amazon EKS Auth の条件キー

Amazon EKS Auth で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssumeRoleForPodIdentity	Kubernetes サービスアカウントトークンを一時的な AWS 認証情報と交換するアクセス許可を付与します	読み取り	cluster*		

Amazon EKS Auth で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
cluster	arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}	aws:ResourceTag/${TagKey}

Amazon EKS Auth の条件キー

Amazon EKS Auth は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	タグキーおよび値のペアでアクセスをフィルタリングします。	String

AWS Elastic Beanstalk のアクション、リソース、および条件キー

AWS Elastic Beanstalk (サービスプレフィックス: elasticbeanstalk) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Elastic Beanstalk で定義されるアクション

- AWS Elastic Beanstalk で定義されるリソースタイプ
- AWS Elastic Beanstalk の条件キー

AWS Elastic Beanstalk で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AbortEnvironmentUpdate	進行中の環境設定の更新またはアプリケーションバージョンのデプロイをキャンセルする許可を付与	書き込み	environment*	elasticbeanstalk:InApplication	
AddTags	Elastic Beanstalk リソースにタグを追加する許可とタグ値を更新する許可を付与	Tagging	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ApplyEnvironmentManagedAction	スケジュールされたマネージドアクションを即時に適用する許可を付与	書き込み	environment*	elasticbeanstalk:InApplication	
AssociateEnvironmentOperationsRole	オペレーションロールを環境に関連付けるアクセス許可を付与	書き込み	environment*		
CheckDNSAvailability	CNAME の可用性を確認する許可を付与	読み込み			
ComposeEnvironments	それぞれが 1 つのアプリケーションの別々のコンポーネントを実行する環境のグループを作成または更新する許可を付与	書き込み	application*		
			applicationversion*	elasticbeanstalk:InApplication	
CreateApplication	新しいアプリケーションを作成する許可を付与	書き込み	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApplicationVersion	アプリケーションのアプリケーションバージョンを作成する許可を付与	書き込み	application*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			applicationversion*	elasticbeanstalk:InApplication aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationTemplate	設定テンプレートを作成する許可を付与	書き込み	configurationtemplate*	elasticbeanstalk:InApplication	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				elasticbeanstalk:FromApplication elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromEnvironment elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironment	アプリケーションの環境を起動する許可を付与	書き込み	environment*	elasticbeanstalk:InApplication	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform aws:RequestTag/${TagKey} aws:TagKeys	
CreatePlatformVersion	カスタムプラットフォームの新しいバージョンを作成する許可を付与	書き込み	platform*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorageLocation	このアカウント用に Amazon S3 ストレージの場所を作成する許可を付与	書き込み			
DeleteApplication	関連付けられているすべてのバージョンと設定とともにアプリケーションを削除する許可を付与	書き込み	application*		
DeleteApplicationVersion	アプリケーションからアプリケーションバージョンを削除する許可を付与	書き込み	applicationversion*	elasticbeanstalk:InApplication	
DeleteConfigurationTemplate	設定テンプレートを削除する許可を付与	書き込み	configurationtemplate*	elasticbeanstalk:InApplication	
DeleteEnvironmentConfiguration	実行中の環境に関連付けられているドラフト設定を削除する許可を付与	書き込み	environment*	elasticbeanstalk:InApplication	
DeletePlatformVersion	カスタムプラットフォームのバージョンを削除する許可を付与	書き込み	platform*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeAccountAttributes	アカウント属性 (リソースクォータなど) のリストを取得する許可を付与	読み取り			
DescribeApplicationVersions	AWS Elastic Beanstalk ストレージバケットに保存されているアプリケーションバージョンのリストを取得するアクセス許可を付与します	リスト	applicationversion	elasticbeanstalk:InApplication	
DescribeApplications	既存のアプリケーションの説明を取得する許可を付与	リスト	application		
DescribeConfigurationOptions	環境設定オプションの説明を取得する許可を付与	読み込み	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	
			solutionstack		
DescribeConfigurationSettings	設定セットの設定の説明を取得する許可を付与	読み込み	configurationtemplate	elasticbeanstalk:InApplication	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			environment	elasticbeanstalk:InApplication	
DescribeEnvironmentHealth	環境の全体的な状態に関する情報を取得する許可を付与	読み込み	environment		
DescribeEnvironmentManagedActionHistory	環境の完了済みおよび失敗したマネージドアクションのリストを取得する許可を付与	読み込み	environment	elasticbeanstalk:InApplication	
DescribeEnvironmentManagedActions	環境の今後および進行中のマネージドアクションのリストを取得する許可を付与	読み取り	environment	elasticbeanstalk:InApplication	
DescribeEnvironmentResources	環境の AWS リソースのリストを取得するアクセス許可を付与します	読み取り	environment	elasticbeanstalk:InApplication	
DescribeEnvironments	既存の環境の説明を取得する許可を付与	リスト	environment	elasticbeanstalk:InApplication	
DescribeEvents	一連の条件に一致するイベントの説明のリストを取得する許可を付与	読み込み	application		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			applicationversion	elasticbeanstalk:InApplication	
			configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	
DescribeInstancesHealth	環境インスタンスのヘルスに関する詳細情報を取得する許可を付与	読み取り	environment		
DescribePlatformVersion	マネージドプラットフォームバージョンの説明を取得するアクセス許可を付与します	読み取り	platform		
DisassociateEnvironmentOperationsRole	オペレーションロールと環境との関連付けを解除する許可を付与	書き込み	environment*		
ListAvailableSolutionStacks	使用できるソリューションスタック名のリストを取得する許可を付与	リスト	solutionstack		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListPlatformBranches	使用できるプラットフォームブランチのリストを取得する許可を付与	リスト			
ListPlatformVersions	使用できるプラットフォームのリストを取得する許可を付与	リスト	platform		
ListTagsForResource	Elastic Beanstalk リソースのタグのリストを取得する許可を付与	読み込み	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
PutInstanceStatistics	拡張ヘルスに関するインスタンス統計を送信する許可を付与	書き込み	application*		
			environment*		
RebuildEnvironment	環境のすべての AWS リソースを削除および再作成し、強制的に再起動するアクセス許可を付与します	書き込み	environment*	elasticbeanstalk:InApplication	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RemoveTags	Elastic Beanstalk リソースからタグを削除する許可を付与	Tagging	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
				aws:TagKeys	
RequestEnvironmentInfo	デプロイ済み環境の情報をコンパイルするリクエストを開始する許可を付与	読み込み	environment*	elasticbeanstalk:InApplication	
RestartAppServer	各 Amazon EC2 インスタンスで実行されているアプリケーションコンテナサーバーを再起動するように環境にリクエストする許可を付与	書き込み	environment*	elasticbeanstalk:InApplication	
RetrieveEnvironmentInfo	RequestEnvironmentInfo リクエストからコンパイル済み情報を取得する許可を付与	読み込み	environment*	elasticbeanstalk:InApplication	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SwapEnvironmentCNAMEs	2 つの環境の CNAME をスワップする許可を付与	書き込み	environment*	elasticbeanstalk:InApplication	
				elasticbeanstalk:FromEnvironment	
TerminateEnvironment	環境を終了する許可を付与	書き込み	environment*	elasticbeanstalk:InApplication	
UpdateApplication	指定されたプロパティでアプリケーションを更新する許可を付与	書き込み	application*		
UpdateApplicationResourceLifecycle	アプリケーションに関連付けられているアプリケーションバージョンライフサイクルポリシーを更新する許可を付与	書き込み	application*		
UpdateApplicationVersion	指定されたプロパティでアプリケーションバージョンを更新する許可を付与	書き込み	applicationversion*	elasticbeanstalk:InApplication	
UpdateConfigurationTemplate	設定テンプレートを指定されたプロパティまたは設定オプション値で更新する許可を付与	書き込み	configurationtemplate*	elasticbeanstalk:InApplication	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				elasticbeanstalk:FromApplication elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromEnvironment elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateEnvironment	環境を更新する許可を付与	書き込み	environment*	elasticbeanstalk:InApplication	
				elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateTagsForResource	タグを更新する許可を付与しません。Elastic Beanstalk リソースにタグを追加し、タグを削除し、タグ値を更新する許可を付与するには、Elasticbeanstalk:AddTags と elasticbeanstalk:RemoveTags を指定します	Tagging	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
				aws:RequestTag/${TagKey} aws:TagKeys	
ValidateConfigurationSettings	設定テンプレートまたは環境の一連の構成設定の有効性を確認する許可を付与	読み込み	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	

AWS Elastic Beanstalk で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
application	arn:${Partition}:elasticbeanstalk:${Region}:${Account}:application/${ApplicationName}	aws:ResourceTag/${TagKey}
applicationversion	arn:${Partition}:elasticbeanstalk:${Region}:${Account}:applicationversion/${ApplicationName}/${VersionLabel}	aws:ResourceTag/${TagKey} elasticbeanstalk:InApplication
configurationtemplate	arn:${Partition}:elasticbeanstalk:${Region}:${Account}:configurationtemplate/${ApplicationName}/${TemplateName}	aws:ResourceTag/${TagKey} elasticbeanstalk:InApplication
environment	arn:${Partition}:elasticbeanstalk:${Region}:${Account}:environment/${ApplicationName}/${EnvironmentName}	aws:ResourceTag/${TagKey} elasticbeanstalk:InApplication
solutionstack	arn:${Partition}:elasticbeanstalk:${Region}::solutionstack/${SolutionStackName}	

リソースタイプ	ARN	条件キー
platform	arn:${Partition}:elasticbeanstalk:${Region}::platform/${PlatformNameWithVersion}	

AWS Elastic Beanstalk の条件キー

AWS Elastic Beanstalk では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアのプレゼンスに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいてアクションをフィルタリングします	ArrayOfString
elasticbeanstalk:FromApplication	入力パラメータで依存関係または制約として指定されたアプリケーションでアクセスをフィルター	ARN
elasticbeanstalk:FromApplicationVersion	入力パラメータで依存関係または制約として指定されたアプリケーションバージョンでアクセスをフィルター	ARN

条件キー	説明	タイプ
elasticbeanstalk:FromConfigurationTemplate	入力パラメータで依存関係または制約として指定された設定テンプレートでアクセスをフィルター	ARN
elasticbeanstalk:FromEnvironment	入力パラメータで依存関係または制約として指定された環境でアクセスをフィルター	ARN
elasticbeanstalk:FromPlatform	入力パラメータで依存関係または制約として指定されたプラットフォームでアクセスをフィルター	ARN
elasticbeanstalk:FromSolutionStack	入力パラメータで依存関係または制約として指定されたソリューションスタックでアクセスをフィルター	ARN
elasticbeanstalk:InApplication	アクションの実行対象のリソースが含まれるアプリケーションでアクセスをフィルター	ARN

Amazon Elastic Block Store のアクション、リソース、および条件キー

Amazon Elastic Block Store (サービスプレフィックス: ebs) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Elastic Block Store で定義されるアクション
- Amazon Elastic Block Store で定義されるリソースタイプ
- Amazon Elastic Block Store の条件キー

Amazon Elastic Block Store で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CompleteSnapshot	必要なデータのブロックがすべて書き込まれた後に、スナップショットを封印、完了するためのアクセス許可を付与する	書き込み	snapshot*		
				aws:ResourceTag/${TagKey}	
GetSnapshotBlock	Amazon Elastic Block Store (EBS) スナップショット内のブロックのデータを返すアクセス許可を付与します。	Read	snapshot*		
				aws:ResourceTag/${TagKey}	
ListChangedBlocks	同じボリューム/スナップショット系列の 2 つの Amazon Elastic Block Store (EBS) スナップショット間で異なるブロックを一覧表示する許可を付与。	読み取り	snapshot*		
				aws:ResourceTag/${TagKey}	
ListSnapshotBlocks	Amazon Elastic Block Store (EBS) スナップショット内のブロックを一覧表示するためのアクセス許可を付与する	読み取り	snapshot*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutSnapshotBlock	StartSnapshot オペレーションによって作成されたスナップショットにデータのブロックを書き込むためのアクセス許可を付与する	書き込み	snapshot*		
				aws:ResourceTag/${TagKey}	
StartSnapshot	新しい EBS スナップショットを作成するためのアクセス許可を付与する	書き込み	snapshot		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ebs:Description ebs:ParentSnapshot ebs:VolumeSize	

Amazon Elastic Block Store で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
snapshot	arn:${Partition}:ec2:${Region}::snapshot/${SnapshotId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ebs:Description ebs:ParentSnapshot ebs:VolumeSize

Amazon Elastic Block Store の条件キー

Amazon Elastic Block Store では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	文字列

条件キー	説明	タイプ
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString
ebs:Description	作成中のスナップショットの内容に基づきアクセスをフィルタリングする	String
ebs:ParentSnapshot	親スナップショットの ARN によってアクセスをフィルタリングします	ARN
ebs:VolumeSize	作成中のスナップショットのボリュームのサイズ (GiB 単位) でアクセスをフィルタリングする	数値

Amazon Elastic Container Registry のアクション、リソース、および条件キー

Amazon Elastic Container Registry (サービスプレフィックス: `ecr`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Elastic Container Registry で定義されるアクション
- Amazon Elastic Container Registry で定義されるリソースタイプ
- Amazon Elastic Container Registry の条件キー

Amazon Elastic Container Registry で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchCheckLayerAvailability	指定されたレジストリとリポジトリの複数のイメージレイヤーの可用性を確認する許可を付与。	読み込み	repository*		
BatchDeleteImage	指定したリポジトリ内の指定したイメージのリストを削除する許可を付与。	書き込み	repository*		
BatchGetImage	指定したリポジトリ内の指定したイメージの詳細情報を取得する許可を付与。	読み込み	repository*		
BatchGetRepositoryScanningConfiguration	リポジトリのリストのリポジトリスキャン設定を取得するアクセス許可を付与	読み取り	repository*		
BatchImportUpstreamImage [許可のみ]	アップストリームレジストリからイメージを取得し、プライベートレジストリにインポートするアクセス許可を付与	書き込み	repository*		
CompleteLayerUpload	指定されたレジストリ、リポジトリ名、およびアップロード ID のイメージレイヤーアップロードが完了したことを Amazon ECR に通知する許可を付与。	書き込み	repository*		
CreatePullThroughCacheRule	新しいプルスルーキャッシュルールを作成するアクセス許可を付与	書き込み			iam:CreateServiceLinkedRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateRepository	イメージレポジトリを作成する許可を付与。	書き込み	repository*		ecr:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRepositoryCreationTemplate	リポジトリ作成テンプレートを作成するためのアクセス許可を付与	書き込み			ecr:CreateRepository ecr:PutLifecyclePolicy ecr:SetRepositoryPolicy iam:CreateServiceLinkedRole iam:PassRole
DeleteLifecyclePolicy	指定したライフサイクルポリシーを削除する許可を付与。	書き込み	repository*		
DeletePullThroughCacheRule	プルスルーキャッシュルールを削除するアクセス許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteRegistryPolicy	レジストリポリシーを削除するアクセス許可を付与	権限の管理			
DeleteRepository	既存のイメージリポジトリを削除する許可を付与。	書き込み	repository*		
DeleteRepositoryCreationTemplate	リポジトリ作成テンプレートを削除するためのアクセス許可を付与	書き込み			
DeleteRepositoryPolicy	指定したリポジトリからリポジトリポリシーを削除する許可を付与。	権限の管理	repository*		
DescribeImageReplicationStatus	レジストリ内のイメージに関するレプリケーションステータス (レプリケーションが失敗した場合の失敗の理由を含む) を取得する許可を付与	読み込み	repository*		
DescribeImageScanFindings	指定したイメージのイメージスキャンの結果を記述する許可を付与。	読み込み	repository*		
DescribeImages	リポジトリ内のイメージに関するメタデータ (例: イメージサイズ、イメージタグ、作成日) を取得する許可を付与。	リスト	repository*		
DescribePullThroughCacheRules	プルスルーキャッシュルールを記述するアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeRegistry	レジストリ設定を記述するアクセス許可を付与	読み込み			
DescribeRepositories	レジストリ内のイメージリポジトリを記述する許可を付与。	読み取り	repository*		
DescribeRepositoryCreationTemplates	リポジトリ作成テンプレートを記述するためのアクセス許可を付与	読み取り			
GetAccountSetting	アカウント設定を取得する許可を付与する	読み取り		ecr:AccountSetting	
GetAuthorizationToken	指定したレジストリに対して有効なトークンを 12 時間取得する許可を付与。	読み込み			
GetDownloadUrlForLayer	イメージレイヤーに対応するダウンロード URL を取得する許可を付与。	読み取り	repository*		
GetImageCopyStatus [許可のみ]	イメージコピーに関するステータスを取得するアクセス許可を付与します	読み取り	repository*		
GetLifecyclePolicy	指定されたライフサイクルポリシーを取得する許可を付与。	読み込み	repository*		
GetLifecyclePolicyPreview	指定されたライフサイクルポリシーのプレビューリクエストの結果を取得する許可を付与。	読み込み	repository*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetRegistryPolicy	レジストリポリシーを取得するアクセス許可を付与	読み込み			
GetRegistryScanningConfiguration	レジストリスキャン設定を取得するアクセス許可を付与	読み込み			
GetRepositoryPolicy	指定したリポジトリのリポジトリポリシーを取得する許可を付与。	読み込み	repository*		
InitiateLayerUpload	イメージレイヤーのアップロードを予定していることを Amazon ECR に通知する許可を付与。	書き込み	repository*		
ListImages	特定のリポジトリのすべてのイメージ ID を一覧表示する許可を付与。	リスト	repository*		
ListTagsForResource	Amazon ECR リソースのタグを一覧表示する許可を付与。	読み取り	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutAccountSetting	アカウント設定を更新する許可を付与する	書き込み		ecr:AccountSetting	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutImage	イメージに関連付けられたイメージマニフェストを作成または更新する許可を付与。	書き込み	repository*		
PutImageScanningConfiguration	リポジトリのイメージスキャン設定を更新する許可を付与。	書き込み	repository*		
PutImageTagMutability	リポジトリのイメージタグの変更可能性を更新する許可を付与。	書き込み	repository*		
PutLifecyclePolicy	ライフサイクルポリシーを作成または更新する許可を付与。	書き込み	repository*		
PutRegistryPolicy	レジストリポリシーを更新するアクセス許可を付与	権限の管理			
PutRegistryScanningConfiguration	レジストリスキャン設定を更新するアクセス許可を付与	書き込み			
PutReplicationConfiguration	レジストリのレプリケーション設定を更新する許可を付与	書き込み			iam:CreateServiceLinkedRole
ReplicateImage [アクセス許可のみ]	イメージをレプリケート先レジストリにレプリケートするアクセス許可を付与	書き込み	repository*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SetRepositoryPolicy	指定したリポジトリにリポジトリポリシーを適用してアクセス権限を制御する許可を付与。	Permissions management	repository*		
StartImageScan	イメージスキャンを開始する許可を付与。	書き込み	repository*		
StartLifecyclePolicyPreview	指定したライフサイクルポリシーのプレビューを開始する許可を付与。	書き込み	repository*		
TagResource	Amazon ECR リソースにタグを付けるアクセス許可を付与	タグ付け	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Amazon ECR リソースのタグを解除する許可を付与。	Tagging	repository*		
				aws:TagKeys	
UpdatePullThroughCacheRule	プルスルーキャッシュルールを更新するためのアクセス許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateRepositoryCreationTemplate	リポジトリ作成テンプレートを更新する許可を付与する	書き込み			ecr:CreateRepository ecr:PutLifecyclePolicy ecr:SetRepositoryPolicy iam:CreateServiceLinkedRole iam:PassRole
UploadLayerPart	イメージレイヤー部分を Amazon ECR にアップロードする許可を付与。	書き込み	repository*		
ValidatePullThroughCacheRule	プルスルーキャッシュルールを検証するためのアクセス許可を付与	読み取り			

Amazon Elastic Container Registry で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
repository	arn:${Partition}:ecr:${Region}:${Account}:repository/${RepositoryName}	aws:ResourceTag/${TagKey} ecr:ResourceTag/${TagKey}

Amazon Elastic Container Registry の条件キー

Amazon Elastic Container Service は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	各タグの許可された値のセットでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値でアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内の必須タグの存在でアクセスをフィルタリングします	ArrayOfString
ecr:AccountSetting	ECR アカウント設定名でアクセスをフィルタリングします	String
ecr:ResourceTag/${TagKey}	リソースに関連付けられたタグ値でアクセスをフィルタリングします	String

Amazon Elastic Container Registry Public のアクション、リソース、および条件キー

Amazon Elastic Container Registry Public (サービスプレフィックス: `ecr-public`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Elastic Container Registry Public で定義されるアクション
- Amazon Elastic Container Registry Public で定義されるリソースタイプ
- Amazon Elastic Container Registry Public の条件キー

Amazon Elastic Container Registry Public で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchCheckLayerAvailability	指定されたレジストリとリポジトリの複数のイメージレイヤーの可用性を確認する許可を付与。	読み込み	repository*		
BatchDeleteImage	指定したリポジトリ内の指定したイメージのリストを削除する許可を付与。	書き込み	repository*		
CompleteLayerUpload	指定されたレジストリ、リポジトリ名、およびアップロード ID のイメージレイヤーアッ	書き込み	repository*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	プロードが完了したことを Amazon ECR に通知する許可を付与。				
CreateRepository	イメージレポジトリを作成する許可を付与。	書き込み	repository*		ecr-public:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteRepository	既存のイメージリポジトリを削除する許可を付与。	書き込み	repository*		
DeleteRepositoryPolicy	指定したリポジトリからリポジトリポリシーを削除する許可を付与。	書き込み	repository*		
DescribeImageTags	所与のリポジトリのすべてのイメージ ID を一覧表示する権限を付与します。	リスト	repository*		
DescribeImages	リポジトリ内のイメージに関するメタデータ (例: イメージサイズ、イメージタグ、作成日) を取得する許可を付与。	読み込み	repository*		
DescribeRegistries	レジストリに関連付けられたカタログデータを取得する権限を付与します	リスト	registry*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeRepositories	レジストリ内のイメージリポジトリを記述する許可を付与。	リスト	repository		
GetAuthorizationToken	指定したレジストリに対して有効なトークンを 12 時間取得する許可を付与。	読み込み			
GetRegistryCatalogData	レジストリに関連付けられたカタログデータを取得する権限を付与します	読み込み	registry*		
GetRepositoryCatalogData	リポジトリに関連付けられたカタログデータを取得する権限を付与します	読み込み	repository*		
GetRepositoryPolicy	指定したリポジトリのリポジトリポリシーを取得する許可を付与。	読み込み	repository*		
InitiateLayerUpload	イメージレイヤーのアップロードを予定していることを Amazon ECR に通知する許可を付与。	書き込み	repository*		
ListTagsForResource	Amazon ECR リソースのタグを一覧表示する許可を付与。	読み込み	repository*		
PutImage	イメージに関連付けられたイメージマニフェストを作成または更新する許可を付与。	書き込み	repository*		
PutRegistryCatalogData	レジストリに関連付けられたカタログデータを作成および更新する権限を付与します	書き込み	registry*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutRepositoryCatalogData	リポジトリに関連付けられたカタログデータを更新する権限を付与します	書き込み	repository*		
SetRepositoryPolicy	指定したリポジトリにリポジトリポリシーを適用してアクセス権限を制御する許可を付与。	Permissions management	repository*		
TagResource	Amazon ECR リソースにタグを付けるアクセス許可を付与します。	タグ付け	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Amazon ECR リソースのタグを解除する許可を付与。	タグ付け	repository*		
				aws:TagKeys	
UploadLayerPart	イメージレイヤー部分を Amazon ECR にアップロードする権限を付与します	書き込み	repository*		

Amazon Elastic Container Registry Public で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
repository	`arn:${Partition}:ecr-public::${Account}:repository/${RepositoryName}`	aws:ResourceTag/${TagKey} ecr-public:ResourceTag/${TagKey}
registry	`arn:${Partition}:ecr-public::${Account}:registry/${RegistryId}`	

Amazon Elastic Container Registry Public の条件キー

Amazon Elastic Container Registry Public では、IAM ポリシーの `Condition` 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	各タグで許可されている値のセットに基づいて作成リクエストをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられている tag-value に基づいてアクションをフィルタリングします。	文字列
aws:TagKeys	リクエスト内の必須のタグの存在に基づいて作成リクエストをフィルタリングします	ArrayOfString

条件キー	説明	タイプ
ecr-public:ResourceTag/${TagKey}	リソースに関連付けられている tag-value に基づいてアクションをフィルタリングします。	文字列

Amazon Elastic Container Service のアクション、リソース、および条件キー

Amazon Elastic Container Service (サービスプレフィックス: ecs) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Elastic Container Service で定義されるアクション
- Amazon Elastic Container Service で定義されるリソースタイプ
- Amazon Elastic Container Service の条件キー

Amazon Elastic Container Service で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateCapacityProvider	新しいキャパシティプロバイダーを作成するためのアクセス許可を付与 キャパシティー	Write		aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	プロバイダーは Amazon ECS クラスターに関連付けられ、クラスターの自動スケーリングを容易にするキャパシティープロバイダー戦略で使用されます			aws:TagKeys	
CreateCluster	新しい Amazon ECS クラスターを作成するためのアクセス許可を付与	Write	cluster*	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys ecs:capacity-provider ecs:fargate-ephemeral-storage-kms-key	
CreateService	サービスの作成を通じて、指定されたタスク定義から必要な数のタスクを実行および管理するためのアクセス許可を付与	Write	service*	ecs:cluster aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys ecs:capacity-provider ecs:task-definition ecs:enable-ebs-volumes ecs:enable-execute-command ecs:enable-service-connect ecs:namespace ecs:enable-vpc-lattice	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				ecs:enable-ecs-managed-tags ecs:propagate-tags ecs:auto-assign-public-ip ecs:subnet ecs:task-cpu ecs:task-memory	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateTaskSet	新しい Amazon ECS タスクセットを作成するためのアクセス許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys ecs:cluster ecs:capacity-provider ecs:service ecs:task-definition	
DeleteAccountSetting	アカウントの指定された IAM ユーザー、IAM ロール、またはルートユーザーについて、リソースの ARN およびリソース ID 形式を変更するためのアクセス許可を付与 作成される新しいリソースに対して新しい ARN およびリソース ID 形式を無効にするかどうかを指定できます	Write		ecs:account-setting	
DeleteAttributes	Amazon ECS リソースから 1 つまたは複数のカスタム属性を削除するためのアクセス許可を付与	Write	container-instance*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} ecs:cluster	
DeleteCapacityProvider	指定されたキャパシティプロバイダーを削除するためのアクセス許可を付与	Write	capacity-provider*		
				aws:ResourceTag/${TagKey}	
DeleteCluster	指定されたクラスターを削除するためのアクセス許可を付与	Write	cluster*	aws:ResourceTag/${TagKey}	
DeleteService	クラスター内の指定されたサービスを削除するためのアクセス許可を付与	書き込み	service*		
				aws:ResourceTag/${TagKey} ecs:cluster	
DeleteTaskDefinitions	ファミリーおよびリビジョンによって指定されたタスク定義を削除するための許可を付与します	書き込み	task-definition*		
				aws:ResourceTag/${TagKey}	
DeleteTaskSet		Write	task-set*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	指定したタスクセットを削除するためのアクセス許可を付与			aws:ResourceTag/${TagKey} ecs:cluster ecs:service	
DeregisterContainerInstance	指定されたクラスターから Amazon ECS コンテナインスタンスを登録解除するためのアクセス許可を付与	Write	cluster*	aws:ResourceTag/${TagKey}	
DeregisterTaskDefinition	ファミリーおよびリビジョンによって指定されたタスク定義を登録解除するためのアクセス許可を付与	Write			
DescribeCapacityProviders	1 つ以上の Amazon ECS キャパシティープロバイダーを説明する許可を付与	Read	capacity-provider*		
				aws:ResourceTag/${TagKey}	
DescribeClusters	1 つ以上のクラスターを記述するためのアクセス許可を付与	Read	cluster*	aws:ResourceTag/${TagKey}	
DescribeContainerInstances	Amazon ECS コンテナインスタンスを記述するためのアクセス許可を付与	読み取り	container-instance*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} ecs:cluster	
DescribeServiceDeployments	1 つ以上のサービスデプロイを記述するアクセス許可を付与します	読み取り	service*	ecs:cluster aws:ResourceTag/${TagKey}	
			service-deployment*	ecs:cluster ecs:service aws:ResourceTag/${TagKey}	
DescribeServiceRevisions	1 つ以上のサービスリビジョンを記述するアクセス許可を付与します	読み取り	service*	ecs:cluster aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			service-revision*	ecs:cluster ecs:service aws:ResourceTag/${TagKey}	
DescribeServices	クラスターで実行されている指定されたサービスを記述するためのアクセス許可を付与	Read	service*		
				aws:ResourceTag/${TagKey} ecs:cluster	
DescribeTaskDefinition	タスク定義を記述するためのアクセス許可を付与 ファミリーとリビジョンを指定して、特定のタスク定義に関する情報を検索するか、ファミリーのみを指定して、そのファミリーの最新の ACTIVE リビジョンを検索できます	Read			
DescribeTaskSets	Amazon ECS タスクセットを記述するためのアクセス許可を付与	Read	task-set*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} ecs:cluster ecs:service	
DescribeTasks	指定した 1 つまたは複数のタスクを記述するためのアクセス許可を付与	Read	task*		
				aws:ResourceTag/${TagKey} ecs:cluster	
DiscoverPollEndpoint	Amazon ECS エージェントが更新をポーリングするためのエンドポイントを取得するためのアクセス許可を付与	Write			
ExecuteCommand	Amazon ECS コンテナでリモートでコマンドを実行するためのアクセス許可を付与	書き込み	cluster*		
			task*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} ecs:cluster ecs:container-name ecs:task	
GetTaskProtection	Amazon ECS サービスのタスクの保護ステータスを取得するための許可を付与します	読み取り	task*		
				aws:ResourceTag/${TagKey} ecs:cluster	
ListAccountSettings	指定されたプリンシパルの Amazon ECS リソースのアカウント設定を一覧表示するためのアクセス許可を付与	Read			
ListAttributes	指定されたターゲットタイプおよびクラスター内の Amazon ECS リソースの属性を一覧表示するためのアクセス許可を付与	リスト	cluster*	aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListClusters	既存のクラスターのリストを取得するためのアクセス許可を付与	リスト			
ListContainerInstances	指定されたクラスター内のコンテナインスタンスのリストを取得するためのアクセス許可を付与	リスト	cluster*	aws:ResourceTag/${TagKey}	
ListServiceDeployments	指定されたサービスのサービスデプロイのリストを取得するアクセス許可を付与します	リスト	service*	aws:ResourceTag/${TagKey} ecs:cluster	
ListServices	指定されたクラスターで実行されているサービスのリストを取得するためのアクセス許可を付与	リスト		ecs:cluster	
ListServicesByNamespace	指定された AWS クラウドマップ名前空間で実行されているサービスのリストを取得するアクセス許可を付与します	リスト		ecs:namespace	
ListTagsForResource	指定されたリソースのタグのリストを取得するためのアクセス許可を付与	Read	capacity-provider		
			cluster		
			container-instance		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			service		
			task		
			task-definition		
			task-set		
				aws:ResourceTag/${TagKey}	
ListTaskDefinitionFamilies	アカウントに登録されているタスク定義ファミリーのリストを取得するためのアクセス許可を付与 (ACTIVE タスク定義を持たないタスク定義ファミリーが含まれる場合があります)。	リスト			
ListTaskDefinitions	アカウントに登録されているタスク定義のリストを取得するためのアクセス許可を付与	リスト			
ListTasks	指定したクラスターのタスクの一覧を取得するためのアクセス許可を付与	リスト	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
Poll [許可のみ]	Amazon ECS サービスに接続してステータスを報告し、コマンドを取得するためのアクセス許可をエージェントに付与	Write	container-instance*		
				ecs:cluster	
PutAccountSetting	アカウントの指定された IAM ユーザー、IAM ロール、またはルートユーザーについて、リソースの ARN およびリソース ID 形式を変更するためのアクセス許可を付与 作成される新しいリソースに対して新しい ARN およびリソース ID 形式を有効にするかどうかを指定できます。この設定の有効化は、リソースのタグ付けなどの新しい Amazon ECS 機能を使用するために必要です	Write		ecs:account-setting	
PutAccountSettingDefault	個々のアカウント設定が行われていないアカウントのすべての IAM ユーザーについて、リソースタイプの ARN およびリソース ID 形式を変更するためのアクセス許可を付与 この設定の有効化は、リソースのタグ付けなどの新しい Amazon ECS 機能を使用するために必要です	Write		ecs:account-setting	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutAttributes	Amazon ECS リソースで属性を作成または更新するためのアクセス許可を付与	Write	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
PutClusterCapacityProviders	クラスターの使用可能なキャパシティープロバイダーおよびデフォルトのキャパシティープロバイダー戦略を変更するためのアクセス許可を付与	Write	cluster*	aws:ResourceTag/${TagKey}	
				ecs:capacity-provider	
RegisterContainerInstance	指定されたクラスターに EC2 インスタンスを登録するためのアクセス許可を付与	Write	cluster*	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
RegisterTaskDefinition	指定されたファミリーと containerDefinitions から新しいタスク定義を登録するためのアクセス許可を付与	Write	task-definition*	aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys ecs:compute-compatibility ecs:privileged ecs:task-cpu ecs:task-memory	
RunTask	ランダム配置とデフォルトの Amazon ECS スケジューラを使用してタスクを開始するためのアクセス許可を付与	Write	task-definition*		iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys ecs:cluster ecs:capacity-provider ecs:enable-ebs-volumes ecs:enable-execute-command	
StartTask	指定された 1 つまたは複数のコンテナインスタンスで、指定されたタスク定義から新しいタスクを開始するためのアクセス許可を付与	Write	task-definition*		iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys ecs:cluster ecs:container-instances ecs:enable-ebs-volumes ecs:enable-execute-command	
StartTelemetrySession	テレメトリセッションを開始するためのアクセス許可を付与	書き込み	container-instance* -		
				ecs:cluster	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StopServiceDeployment	進行中のサービスデプロイを停止するアクセス許可を付与します	書き込み	service*	ecs:cluster aws:ResourceTag/${TagKey}	
			service-deployment*	ecs:cluster ecs:service aws:ResourceTag/${TagKey}	
StopTask	実行中のタスクを停止するためのアクセス許可を付与	Write	task*		
				aws:ResourceTag/${TagKey} ecs:cluster	
SubmitAttachmentStateChanges	アタッチメントの状態が変更された旨の確認を送信するためのアクセス許可を付与	Write	cluster*	aws:ResourceTag/${TagKey}	
SubmitContainerStateChange	コンテナの状態が変更された旨の確認を送信するためのアクセス許可を付与	Write	cluster*	aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SubmitTaskStateChange	タスクの状態が変更された旨の確認を送信するためのアクセス許可を付与	Write	cluster*	aws:ResourceTag/${TagKey}	
TagResource	指定されたリソースにタグを付けるアクセス許可を付与	タグ付け	capacity-provider		
			cluster		
			container-instance		
			service		
			task		
			task-definition		
			task-set		
				aws:TagKeys aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} ecs:CreateAction	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	指定されたリソースのタグを解除するアクセス許可を付与	タグ付け	capacity-provider		
			cluster		
			container-instance		
			service		
			task		
			task-definition		
			task-set		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCapacityProvider	指定されたキャパシティープロバイダーを更新するためのアクセス許可を付与	Write	capacity-provider*		
				aws:ResourceTag/${TagKey}	
UpdateCluster	クラスターで使用する構成または設定を変更するためのアクセス許可を付与	Write	cluster*	aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ecs:fargate-ephemeral-storage-kms-key	
UpdateClusterSettings	クラスターで使用する設定を変更するためのアクセス許可を付与	Write	cluster*	aws:ResourceTag/${TagKey}	
UpdateContainerAgent	指定されたコンテナインスタンスの Amazon ECS コンテナエージェントを更新するためのアクセス許可を付与	Write	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
UpdateContainerInstancesState	Amazon ECS コンテナインスタンスのステータスを変更するためのアクセス許可をユーザーに付与	Write	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateService	サービスのパラメータを変更するためのアクセス許可を付与	Write	service*	ecs:cluster aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				ecs:capacity-provider ecs:enable-ebs-volumes ecs:enable-execute-command ecs:enable-service-connect ecs:namespace ecs:task-definition ecs:enable-vpc-lattice ecs:enable-ecs-managed-tags ecs:propagate-tags	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ecs:auto-assign-public-ip ecs:subnet ecs:task-cpu ecs:task-memory	
UpdateServicePrimaryTaskSet	サービスで使用されるプライマリタスクセットを変更するためのアクセス許可を付与	書き込み	service*		
				aws:ResourceTag/${TagKey} ecs:cluster	
UpdateTaskProtection	タスクの保護ステータスを変更するための許可を付与します	書き込み	task*		
				aws:ResourceTag/${TagKey} ecs:cluster	
UpdateTaskSet	指定されたタスクセットを更新するためのアクセス許可を付与	Write	task-set*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} ecs:cluster ecs:service	

Amazon Elastic Container Service で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
cluster	arn:${Partition}:ecs:${Region}:${Account}:cluster/${ClusterName}	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}
container-instance	arn:${Partition}:ecs:${Region}:${Account}:container-instance/${ClusterName}/${ContainerInstanceId}	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
service	arn:${Partition}:ecs:${Region}:${Account}:service/${ClusterName}/${ServiceName}	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}
service-deployment	arn:${Partition}:ecs:${Region}:${Account}:service-deployment/${ClusterName}/${ServiceName}/${ServiceDeploymentId}	aws:ResourceTag/${TagKey} ecs:cluster ecs:service
service-revision	arn:${Partition}:ecs:${Region}:${Account}:service-revision/${ClusterName}/${ServiceName}/${ServiceRevisionId}	aws:ResourceTag/${TagKey} ecs:cluster ecs:service
task	arn:${Partition}:ecs:${Region}:${Account}:task/${ClusterName}/${TaskId}	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}
task-definition	arn:${Partition}:ecs:${Region}:${Account}:task-definition/${TaskDefinitionFamilyName}:${TaskDefinitionRevisionNumber}	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}
capacity-provider	arn:${Partition}:ecs:${Region}:${Account}:capacity-provider/${CapacityProviderName}	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
task-set	arn:${Partition}:ecs:${Region}:${Account}:task-set/${ClusterName}/${ServiceName}/${TaskSetId}	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}

Amazon Elastic Container Service の条件キー

Amazon Elastic Container Service は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
ecs:CreateAction	リソース作成 API アクションの名前によってアクセスをフィルタリングします	String
ecs:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアでアクセスをフィルタリングします	String

条件キー	説明	タイプ
ecs:account-setting	Amazon ECS アカウント設定名でアクセスをフィルタリング	String
ecs:auto-assign-public-ip	awsvpc ネットワークモードを使用する Amazon ECS タスクまたは Amazon ECS サービスのパブリック IP 割り当て設定でアクセスをフィルタリングします	Bool
ecs:capacity-provider	Amazon ECS キャパシティープロバイダーの ARN に基づいて、アクセスをフィルタリングします	ArrayOfARN
ecs:cluster	Amazon ECS クラスターの ARN でアクセスをフィルタリングします	ARN
ecs:compute-compatibility	リクエストで指定された必須の互換性フィールドでアクセスをフィルタリングします	ArrayOfString
ecs:container-instances	Amazon ECS コンテナインスタンスの ARN に基づいて、アクセスをフィルタリングします	ARN
ecs:container-name	ECS タスク定義で定義されている Amazon ECS コンテナの名前に基づいて、アクセスをフィルタリングします	String
ecs:enable-ebs-volumes	ECS タスクまたはサービスの Amazon ECS マネージド Amazon EBS ボリューム機能でアクセスをフィルタリングする	String
ecs:enable-ecs-managed-tags	Amazon ECS タスクまたは Amazon ECS サービスの enableECSManagedTags 設定でアクセスをフィルタリングします	Bool
ecs:enable-execute-command	Amazon ECS タスクまたは Amazon ECS サービスの実行コマンド機能に基づいて、アクセスをフィルタリングします	String
ecs:enable-service-connect	Service Connect 設定の有効フィールド値によりアクセスをフィルタリング	String

条件キー	説明	タイプ
ecs:enable-vpc-lattice	Amazon ECS サービスの VPC 格子機能でアクセスをフィルタリングします	String
ecs:fargate-ephemeral-storage-kms-key	リクエストで指定された AWS KMS キー ID でアクセスをフィルタリングします	String
ecs:namespace	Service Connect 設定で定義されている AWS クラウドマップ名前空間の ARN でアクセスをフィルタリングします	ARN
ecs:privileged	リクエストで指定された特権フィールドでアクセスをフィルタリングします	String
ecs:propagate-tags	Amazon ECS タスクまたは Amazon ECS サービスのタグ伝達設定でアクセスをフィルタリングします	String
ecs:service	Amazon ECS サービスの ARN に基づいて、アクセスをフィルタリングします	ARN
ecs:subnet	awsvpc ネットワークモードを使用する Amazon ECS タスクまたは Amazon ECS サービスのサブネット設定でアクセスをフィルタリングします	ArrayOfString
ecs:task	Amazon ECS タスクの ARN に基づいて、アクセスをフィルタリングします	ARN
ecs:task-cpu	リクエストで指定された 1024 = 1 vCPU の整数として、タスク cpu でアクセスをフィルタリングします	数値
ecs:task-definition	Amazon ECS タスク定義の ARN に基づいて、アクセスをフィルタリングします	ARN
ecs:task-memory	リクエストで指定された MiB を表す整数として、タスクメモリでアクセスをフィルタリングします	数値

AWS Elastic ディザスタリカバリに対するアクション、リソースおよび条件キー

AWS Elastic Disaster Recovery (サービスプレフィックス: drs) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Elastic 災害回復で定義されるアクション
- AWS Elastic 災害回復で定義されるリソースタイプ
- AWS Elastic 災害回復の条件キー

AWS Elastic 災害回復で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateFailbackClientToRecoveryInstanceForDrs [アクセス許可のみ]	リカバリインスタンスに関連付けるフェイルバッククライアントを取得するアクセス許可を付与	書き込み	RecoveryInstanceResource*		
AssociateSourceNetworkStack	CloudFormation スタックをソースネットワークに関連付ける許可を付与	書き込み	SourceNetworkResource*		cloudformation:DescribeStackResource

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					cloudformation:DescribeStacks drs:GetLaunchConfiguration ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					ec2:ModifyLaunchTemplate
				aws:RequestTag/${TagKey} aws:TagKeys	
BatchCreateVolumeSnapshotGroupForDrs [アクセス許可のみ]	ボリュームスナップショットグループを一括で作成する許可を付与	書き込み	RecoveryInstanceResource*		
			SourceServerResource*		
BatchDeleteSnapshotRequestForDrs [アクセス許可のみ]	スナップショットのリクエストを一括で削除する許可を付与。	書き込み			
CreateConvertedSnapshotForDrs [アクセス許可のみ]	スナップショット設定を更新する許可を付与変換されたスナップショットを作成する許可を付与	書き込み	SourceServerResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateExtendedSourceServer	ソースサーバーを拡張する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	drs:DescribeSourceServers drs:GetReplicationConfiguration
CreateLaunchConfigurationTemplate	起動設定テンプレートを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRecoveryInstanceForDrs [アクセス許可のみ]	リカバリインスタンスを作成するためのアクセス許可を付与	書き込み	SourceServerResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateReplicationConfigurationTemplate	レプリケーション構成テンプレートを作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault kms:CreateGrant kms:DescribeKey
CreateSourceNetwork	ソースネットワークを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeInstances ec2:DescribeVpcs

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSourceServerForDrs [アクセス許可のみ]	ソースサーバーを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteJob	ジョブを削除する許可を付与	書き込み	JobResource*		
DeleteLaunchAction	起動アクションを削除するための許可を付与します	書き込み	LaunchConfigurationTemplateResource		
			SourceServerResource		
DeleteLaunchConfigurationTemplate	起動設定テンプレートを削除する許可を付与	書き込み	LaunchConfigurationTemplateResource*		
DeleteRecoveryInstance	回復インスタンスを削除する許可を付与	書き込み	RecoveryInstanceResource*		
DeleteReplicationConfigurationTemplate	レプリケーション構成テンプレートを削除する許可を付与	書き込み	ReplicationConfigurationTemplateResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteSourceNetwork	ソースネットワークを削除する許可を付与	書き込み	SourceNetworkResource*		
DeleteSourceServer	ソースサーバーを削除する許可を付与	書き込み	SourceServerResource*		
DescribeJobLogItems	ジョブログ項目を説明する許可を付与	読み込み	JobResource*		
DescribeJobs	ジョブを記述する許可を付与	読み取り			
DescribeLaunchConfigurationTemplates	起動設定テンプレートを記述する許可を付与	読み取り			
DescribeRecoveryInstances	リカバリインスタンスを記述するアクセス許可を付与	読み込み			drs:DescribeSourceServers ec2:DescribeInstances
DescribeRecoverySnapshots	リカバリスナップショットを記述するアクセス許可を付与	読み込み	SourceServerResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeReplicationConfigurationTemplates	レプリケーション構成テンプレートを記述する許可を付与	読み込み			
DescribeReplicationServerAssociationsForDrs [許可のみ]	レプリケーションサーバーの関連付けを記述する許可を付与	読み込み			
DescribeSnapshotRequestsForDrs [許可のみ]	スナップショットのリクエストを記述する許可を付与	読み取り			
DescribeSourceNetworks	ソースネットワークを記述する許可を付与	読み取り			
DescribeSourceServers	ソースサーバーを記述する許可を付与	読み込み			
DisconnectRecoveryInstance	リカバリインスタンスを切断するアクセス許可を付与	書き込み	RecoveryInstanceResource*		
DisconnectSourceServer	ソースサーバーの接続を切るアクセス許可を付与	書き込み	SourceServerResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ExportSourceNetworkCfnTemplate	ソースネットワークのリソースを含む CloudFormation テンプレートをエクスポートする許可を付与	書き込み	SourceNetworkResource*		s3:GetBucketLocation s3:GetObject s3:PutObject
				aws:RequestTag/${TagKey} aws:TagKeys	
GetAgentCommandForDrs [アクセス許可のみ]	エージェントコマンドを取得する許可を付与	読み込み	RecoveryInstanceResource*		
			SourceServerResource*		
GetAgentConfirmedResumeInfoForDrs [許可のみ]	エージェントに確認済みの再開情報を取得する許可を付与	読み込み	RecoveryInstanceResource*		
			SourceServerResource*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetAgentInstallationAssetsForDrs [許可のみ]	エージェントのインストールアセットを取得する許可を付与	読み込み			
GetAgentReplicationInfoForDrs [許可のみ]	エージェントレプリケーション情報を取得する許可を付与	読み込み	RecoveryInstanceResource*		
			SourceServerResource*		
GetAgentRuntimeConfigurationForDrs [許可のみ]	エージェントのランタイム設定を取得する許可を付与	読み込み	RecoveryInstanceResource*		
			SourceServerResource*		
GetAgentSnapshotCreditsForDrs [許可のみ]	エージェントスナップショットのクレジットを取得する許可を付与	読み込み	RecoveryInstanceResource*		
			SourceServerResource*		
GetChannelCommandsForDrs [許可のみ]	チャネルコマンドを取得する許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetFailbackCommandForDrs [許可のみ]	フェイルバックコマンドを取得する許可を付与	読み込み	RecoveryInstanceResource*		
GetFailbackLaunchRequestedForDrs [許可のみ]	フェイルバック起動を要求するアクセス許可を付与	読み込み	RecoveryInstanceResource*		
GetFailbackReplicationConfiguration	フェイルバックレプリケーション構成を取得する許可を付与	読み込み	RecoveryInstanceResource*		
GetLaunchConfiguration	起動設定を取得する許可を付与。	読み込み	SourceServerResource*		
GetReplicationConfiguration	レプリケーション構成を取得する許可を付与	読み込み	SourceServerResource*		
GetSuggestedFailbackClientDeviceMappingForDrs [許可のみ]	推奨されるフェイルバッククライアントデバイスマッピングを取得するアクセス許可を付与	読み込み	RecoveryInstanceResource*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
InitializeService	サービスを初期化する許可を付与	書き込み			iam:AddRoleToInstanceProfile iam:CreateInstanceProfile iam:CreateServiceLinkedRole iam:GetInstanceProfile
IssueAgentCertificateForDrs [アクセス許可のみ]	エージェント証明書を発行するアクセス許可を付与	書き込み	RecoveryInstanceResource*		
			SourceServerResource*		
ListExtensibleSourceServers	拡張可能なソースサーバーを一覧表示する許可を付与	読み取り			drs:DescribeSourceServers
ListLaunchActions	起動アクションを一覧表示するための許可を付与します	読み取り	LaunchConfigurationTemplateResource		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			SourceServerResource		
ListStagingAccounts	ステージングアカウントを一覧表示する許可を付与	読み取り			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み込み			
NotifyAgentAuthenticationForDrs [許可のみ]	エージェント認証を通知する許可を付与	書き込み	RecoveryInstanceResource*		
			SourceServerResource*		
NotifyAgentConnectedForDrs [アクセス許可のみ]	エージェントが接続されていることを通知する許可を付与	書き込み	RecoveryInstanceResource*		
			SourceServerResource*		
NotifyAgentDisconnectedForDrs [アクセス許可のみ]	エージェントの切断を通知する許可を付与	書き込み	RecoveryInstanceResource*		
			SourceServerResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
NotifyAgentReplicationProgressForDrs [アクセス許可のみ]	エージェントのレプリケーションの進行状況を通知する許可を付与	書き込み	RecoveryInstanceResource*		
			SourceServerResource*		
NotifyConsistencyAttainedForDrs [アクセス許可のみ]	一貫性があることを通知する許可を付与	書き込み	RecoveryInstanceResource*		
NotifyReplicationServerAuthenticationForDrs [アクセス許可のみ]	レプリケーションサーバー認証を通知するアクセス許可を付与	書き込み	RecoveryInstanceResource*		
NotifyVolumeEventForDrs [アクセス許可のみ]	レプリケータ ボリューム イベントを通知する許可の付与	書き込み	SourceServerResource*		
PutLaunchAction	起動アクションを設定するための許可を付与します	書き込み	LaunchConfigurationTemplateResource		ssm:DescribeDocument

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			SourceServerResource		
RetryDataReplication	データレプリケーションを再試行する許可を付与	書き込み	SourceServerResource*		
ReverseReplication	レプリケーションを取り消す許可を付与	書き込み	RecoveryInstanceResource*		drs:DescribeReplicationConfigurationTemplates drs:DescribeSourceServers ec2:DescribeInstances
				aws:RequestTag/${TagKey} aws:TagKeys	
SendAgentLogsForDrs [アクセス許可のみ]	エージェントログを送信する許可を付与。	書き込み	RecoveryInstanceResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			SourceServerResource*		
SendAgentMetricsForDrs [アクセス許可のみ]	エージェントメトリックを送信する許可を付与	書き込み	RecoveryInstanceResource*		
			SourceServerResource*		
SendChannelCommandResultForDrs [アクセス許可のみ]	チャネルコマンドの結果を送信する許可を付与	書き込み			
SendClientLogsForDrs [アクセス許可のみ]	クライアントログを送信する許可を付与	書き込み			
SendClientMetricsForDrs [アクセス許可のみ]	クライアントメトリックを送信する許可を付与	書き込み			
SendVolumeStatsForDrs [アクセス許可のみ]	ボリュームスループット統計を送信する許可の付与	書き込み	SourceServerResource*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartFailbackLaunch	フェイルバック起動を開始するアクセス許可を付与	書き込み	RecoveryInstanceResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartRecovery	リカバリを開始するアクセス許可を付与	書き込み	SourceServerResource*		drs:CreateRecoveryInstanceForDrs drs:ListTagsForResource ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateSnapshot

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:CreateTags ec2:CreateVolume ec2:DeleteLaunchTemplateVersions ec2:DeleteSnapshot ec2:DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstanceAttribute

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DescribeVolumes ec2:DetachVolume ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:RevokeSecurityGroupEgress ec2:RunInstances ec2:StartInstances ec2:StopInstances ec2:TerminateInstances iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
StartReplication	レプリケーションを開始する許可を付与	書き込み	SourceServerResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartSourceNetworkRecovery	ネットワークリカバリを開始する許可を付与	書き込み	SourceNetworkResource*		cloudformation:CreateStack cloudformation:DescribeStackResource cloudformation:DescribeStacks cloudformation:UpdateStack drs:GetLaunchConfiguration ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:ModifyLaunchTemplate s3:GetObject s3:PutObject
				aws:RequestTag/${TagKey} aws:TagKeys	
StartSourceNetworkReplication	ネットワークのレプリケーションを開始する許可を付与	書き込み	SourceNetworkResource*		
StopFailback	フェイルバックを停止するアクセス許可を付与	書き込み	RecoveryInstanceResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StopReplication	レプリケーションを停止する許可を付与	書き込み	SourceServerResource*		
StopSourceNetworkReplication	ネットワークのレプリケーションを停止する許可を付与	書き込み	SourceNetworkResource*		
TagResource	リソースタグを割り当てるアクセス許可を付与	Tagging	JobResource		
			LaunchConfigurationTemplateResource		
			RecoveryInstanceResource		
			ReplicationConfigurationTemplateResource		
			SourceNetworkResource		
			SourceServerResource		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys drs:CreateAction	
TerminateRecoveryInstances	ターゲットインスタンスを終了する許可を付与	書き込み	RecoveryInstanceResource*		drs:DescribeSourceServers ec2:DeleteVolume ec2:DescribeInstances ec2:DescribeVolumes ec2:TerminateInstances
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UntagResource	リソースのタグを解除する許可を付与	タグ付け	JobResource		
			LaunchConfigurationTemplateResource		
			RecoveryInstanceResource		
			ReplicationConfigurationTemplateResource		
			SourceNetworkResource		
			SourceServerResource		
				aws:TagKeys	
UpdateAgentBacklogForDrs [アクセス許可のみ]	エージェントのバックログを更新する許可を付与	書き込み	RecoveryInstanceResource*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			SourceServerResource*		
UpdateAgentConversionInfoForDrs [アクセス許可のみ]	エージェント変換情報を更新する許可を付与	書き込み	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateAgentReplicationInfoForDrs [アクセス許可のみ]	エージェントレプリケーション情報を更新する許可を付与	書き込み	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateAgentReplicationProcessStateForDrs [アクセス許可のみ]	エージェントレプリケーションプロセスの状態を更新する許可を付与	書き込み	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateAgentSourcePropertiesForDrs [アクセス許可のみ]	エージェントのソースプロパティを更新する許可を付与。	書き込み	RecoveryInstanceResource*		
			SourceServerResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateFailbackClientDeviceMappingForDrs [アクセス許可のみ]	フェイルバッククライアントデバイスマッピングを更新するアクセス許可を付与	書き込み	RecoveryInstanceResource*		
UpdateFailbackClientLastSeenForDrs [アクセス許可のみ]	最後に検出されたフェールバッククライアントを更新するアクセス許可を付与	書き込み	RecoveryInstanceResource*		
UpdateFailbackReplicationConfiguration	フェイルバックレプリケーション構成を更新する許可を付与	書き込み	RecoveryInstanceResource*		
UpdateLaunchConfiguration	起動設定を更新する許可を付与	書き込み	SourceServerResource*		ec2:DescribeInstances
UpdateLaunchConfigurationTemplate	起動設定を更新する許可を付与	書き込み	LaunchConfigurationTemplateResource*		
UpdateReplicationCertificateForDrs [アクセス許可のみ]	レプリケーション証明書を更新するためのアクセス許可を付与	書き込み	RecoveryInstanceResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateReplicationConfiguration	レプリケーション構成を更新する許可を付与。	書き込み	SourceServerResource*		ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault kms:CreateGrant kms:DescribeKey

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateReplicationConfigurationTemplate	レプリケーション構成テンプレートを更新する許可を付与	書き込み	ReplicationConfigurationTemplateResource*		ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault kms:CreateGrant kms:DescribeKey

AWS Elastic 災害回復で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
JobResource	arn:${Partition}:drs:${Region}:${Account}:job/${JobID}	aws:ResourceTag/${TagKey}
RecoveryInstanceResource	arn:${Partition}:drs:${Region}:${Account}:recovery-instance/${RecoveryInstanceID}	aws:ResourceTag/${TagKey} drs:EC2InstanceARN
ReplicationConfigurationTemplateResource	arn:${Partition}:drs:${Region}:${Account}:replication-configuration-template/${ReplicationConfigurationTemplateID}	aws:ResourceTag/${TagKey}
LaunchConfigurationTemplateResource	arn:${Partition}:drs:${Region}:${Account}:launch-configuration-template/${LaunchConfigurationTemplateID}	aws:ResourceTag/${TagKey}
SourceServerResource	arn:${Partition}:drs:${Region}:${Account}:source-server/${SourceServerID}	aws:ResourceTag/${TagKey}
SourceNetworkResource	arn:${Partition}:drs:${Region}:${Account}:source-network/${SourceNetworkID}	aws:ResourceTag/${TagKey}

AWS Elastic 災害回復の条件キー

AWS Elastic Disaster Recovery では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString
drs:CreateAction	リソース作成 API アクションの名前によってアクセスをフィルタリングします	String
drs:EC2InstanceARN	リクエストが発生したEC2インスタンス によってアクセスをフィルタリングします。	ARN

Amazon Elastic File System のアクション、リソース、条件キー

Amazon Elastic File System (サービスプレフィックス: `elasticfilesystem`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Elastic File System で定義されるアクション
- Amazon Elastic File System で定義されるリソースタイプ
- Amazon Elastic File System の条件キー

Amazon Elastic File System で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
Backup [アクセス許可のみ]	既存のファイルシステムのバックアップジョブを開始するアクセス許可を付与	書き込み	file-system*		
ClientMount [アクセス許可のみ]	NFS クライアントにファイルシステムの読み取りアクセスを許可するアクセス許可を付与	読み込み	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	
ClientRootAccess [許可のみ]	NFS クライアントにファイルシステムのルートアクセスを許可するアクセス許可を付与	書き込み	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ClientWrite [アクセス許可のみ]	NFS クライアントにファイルシステムの書き込みアクセスを許可するアクセス許可を付与	書き込み	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	
CreateAccessPoint	指定したファイルシステムのアクセスポイントを作成するアクセス許可を付与	書き込み	file-system*		elasticfilesystem:TagResource
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateFileSystem	空のファイルシステムを作成するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys elasticfilesystem:Encrypted	elasticfilesystem:TagResource
CreateMountTarget	ファイルシステムのマウントターゲットを作成するアクセス許可を付与	書き込み	file-system*		
CreateReplicationConfiguration	新しいレプリケーション設定を作成する許可を付与	書き込み	file-system*		
CreateTags	ファイルシステムに関連付けられたタグを作成または上書きするアクセス許可を付与 (非推奨につき、TagResource を参照)	タグ付け	file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessPoint	指定したアクセスポイントを削除するアクセス許可を付与	書き込み	access-point*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteFileSystem	ファイルシステムを削除する (その内容へのアクセスを完全に切断する) アクセス許可を付与	書き込み	file-system*		
DeleteFileSystemPolicy	ファイルシステムのリソースレベルのポリシーを削除するアクセス許可を付与	権限の管理	file-system*		
DeleteMountTarget	指定されたマウントターゲットを削除するアクセス許可を付与	書き込み	file-system*		
DeleteReplicationConfiguration	レプリケーション設定を削除する許可を付与	書き込み	file-system*		
DeleteTags	指定されたタグをファイルシステムから削除するアクセス許可を付与 (非推奨につき、UntagResource を参照)	タグ付け	file-system*		
				aws:TagKeys	
DescribeAccessPoints	Amazon EFS アクセスポイントの説明を表示するアクセス許可を付与	リスト	access-point		
			file-system		
DescribeAccountPreferences	アカウントの有効なアカウント詳細設定を表示するためのアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeBackupPolicy	Amazon EFS ファイルシステムの BackupPolicy オブジェクトを表示するアクセス許可を付与	読み込み	file-system*		
DescribeFileSystemPolicy	Amazon EFS ファイルシステムのリソースレベルのポリシーを表示するアクセス許可を付与	読み取り	file-system		
DescribeFileSystems	ファイルシステム CreationToken または FileSystemId で指定された Amazon EFS ファイルシステムの説明を表示するか、呼び出されるエンドポイントの AWS リージョン AWS アカウント で発信者のが所有するすべてのファイルシステムの説明を表示するアクセス許可を付与します	リスト	file-system		
DescribeLifecycleConfiguration	Amazon EFS ファイルシステムの LifecycleConfiguration オブジェクトを表示するアクセス許可を付与	読み込み	file-system*		
DescribeMountTargetSecurityGroups	マウントターゲットについて現在有効なセキュリティグループを表示するアクセス許可を付与	読み込み	file-system*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeMountTargets	ファイルシステムのすべてのマウントターゲットまたは特定のマウントターゲットの説明を表示するアクセス許可を付与	読み取り	file-system*		
			access-point		
DescribeReplicationConfigurations	FileSystemId で指定された Amazon EFS レプリケーション設定の説明を表示するか、呼び出されるエンドポイントの AWS リージョン AWS アカウント で発信者の が所有するすべてのレプリケーション設定の説明を表示するアクセス許可を付与します	リスト	file-system		
DescribeTags	リソースに関連付けられているタグを表示するアクセス許可を付与	読み込み	file-system*		
ListTagsForResource	指定された Amazon EFS リソースに関連付けられたタグを表示するアクセス許可を付与	読み込み	access-point		
			file-system		
ModifyMountTargetSecurityGroups	マウントターゲットについて現在有効なセキュリティグループのセットを変更するアクセス許可を付与	書き込み	file-system*		
PutAccountPreferences	アカウントのアカウント詳細設定を設定するためのアクセス許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutBackupPolicy	新しい AWS BackupPolicy オブジェクトを作成して Backup で自動バックアップを有効または無効にするアクセス許可を付与します	書き込み	file-system*		
PutFileSystemPolicy	指定されたファイルシステムに所与のアクターから許可または拒否されたアクションを定義するリソースレベルのポリシーを適用するアクセス許可を付与	権限の管理	file-system*		
PutLifecycleConfiguration	新しい LifecycleConfiguration オブジェクトを作成してライフサイクル管理を有効にするアクセス許可を付与	書き込み	file-system*		
ReplicationRead [アクセス許可のみ]	レプリケーション用のファイルシステムデータを読み取るアクセス許可を付与します	読み取り	file-system*		
ReplicationWrite [許可のみ]	ファイルシステムにデータをレプリケートするアクセス許可を付与します	書き込み	file-system*		
Restore [アクセス許可のみ]	ファイルシステムのバックアップの復元ジョブを開始するアクセス許可を付与	書き込み	file-system*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagResource	指定された Amazon EFS リソースに関連付けられたタグを作成または上書きするアクセス許可を付与	タグ付け	access-point		
			file-system		
				aws:RequestTag/${TagKey} aws:TagKeys elasticfilesystem:CreateAction	
UntagResource	指定されたタグを Amazon EFS リソースから削除するアクセス許可を付与	タグ付け	access-point		
			file-system		
				aws:TagKeys	
UpdateFileSystem	スループットモード、または既存のファイルシステムのプロビジョニングされたスループットの量を更新するアクセス許可を付与	書き込み	file-system*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateFileSystemProtection	既存のファイルシステムのファイルシステム保護を更新するためのアクセス許可を付与	書き込み	file-system*		

Amazon Elastic File System で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
file-system	arn:${Partition}:elasticfilesystem:${Region}:${Account}:file-system/${FileSystemId}	aws:ResourceTag/${TagKey}
access-point	arn:${Partition}:elasticfilesystem:${Region}:${Account}:access-point/${AccessPointId}	aws:ResourceTag/${TagKey}

Amazon Elastic File System の条件キー

Amazon Elastic File System では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString
elasticfilesystem:AccessPointArn	ファイルシステムのマウントに使用されるアクセスポイントの ARN でアクセスをフィルタリングします	ARN
elasticfilesystem:AccessedViaMountTarget	ファイルシステムがマウントターゲット経由でアクセスされるかどうかによってアクセスをフィルタリングします	Bool
elasticfilesystem:CreateAction	リソース作成 API アクションの名前によってアクセスをフィルタリングします	String
elasticfilesystem:Encrypted	暗号化されていないファイルシステムをユーザーが作成できるかどうかによってアクセスをフィルタリングします	Bool

Amazon Elastic Kubernetes Service のアクション、リソース、および条件キー

Amazon Elastic Kubernetes Service (サービスプレフィックス: eks) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Elastic Kubernetes Service で定義されるアクション
- Amazon Elastic Kubernetes Service で定義されるリソースタイプ
- Amazon Elastic Kubernetes Service の条件キー

Amazon Elastic Kubernetes Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AccessKubernetesApi [アクセス許可のみ]	AWS EKS コンソールを介して Kubernetes オブジェクトを表示するアクセス許可を付与します	読み取り	cluster*		
AssociateAccessPolicy	Amazon EKS アクセスポリシーを Amazon EKS アクセスエントリに関連付ける許可を付与	書き込み	access-entry*		
				eks:policyArn eks:namespaces eks:accessScope	
AssociateEncryptionConfig	クラスターに暗号化設定を関連付けるアクセス許可を付与	書き込み	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateIdentityProviderConfig	クラスターに ID プロバイダー設定を関連付けるアクセス許可を付与	書き込み	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys eks:clientId eks:issuerUrl	
CreateAccessEntry	Amazon EKS アクセスエントリを作成する許可を付与	書き込み	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys eks:principalArn eks:kubernetesGroups eks:username eks:accessEntryType	
CreateAddon	Amazon EKS アドオンを作成するアクセス許可を付与	書き込み	cluster*		
			podidentityassociation		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateCluster	Amazon EKS クラスターを作成するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys eks:bootstrapClusterCreatorAdminPermissions eks:bootstrapSelfManagedAddons eks:authenticationMode eks:supportType eks:computeConfigEnabled eks:elasticLoadBalancingEnabled	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				eks:blockStorageEnabled	
CreateEksAnywhereSubscription	EKS Anywhere サブスクリプションを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFargateProfile	AWS Fargate プロファイルを作成するアクセス許可を付与します	書き込み	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNodegroup	Amazon EKS ノードグループを作成するアクセス許可を付与	書き込み	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePodIdentityAssociation	EKS Pod Identity の関連付けを作成するためのアクセス許可を付与	書き込み	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessEntry	Amazon EKS アクセスエントリを削除する許可を付与	書き込み	access-entry*		
DeleteAddon	Amazon EKS アドオンを削除するアクセス許可を付与	書き込み	addon*		
			podidentityassociation		
DeleteCluster	Amazon EKS クラスターを削除するアクセス許可を付与	書き込み	cluster*		
DeleteEksAnywhereSubscription	EKS Anywhere サブスクリプションを記述する許可を付与	書き込み	eks-anywhere-subscription*		
DeleteFargateProfile	AWS Fargate プロファイルを削除するアクセス許可を付与します	書き込み	fargateprofile*		
DeleteNodegroup	Amazon EKS ノードグループを削除するアクセス許可を付与	書き込み	nodegroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeletePodIdentityAssociation	EKS Pod Identity の関連付けを削除するためのアクセス許可を付与	書き込み	podidentityassociation*		
DeregisterCluster	外部クラスターの登録を解除する許可を付与	書き込み	cluster*		
DescribeAccessEntry	Amazon EKS アクセスエントリを記述する許可を付与	読み取り	access-entry*		
DescribeAddon	Amazon EKS アドオンに関する説明情報を取得するアクセス許可を付与	読み取り	addon*		
DescribeAddonConfiguration	Amazon EKS アドオンに関する設定オプションを一覧表示するための許可を付与します	読み取り			
DescribeAddonVersions	Amazon EKS アドオンがサポートしているアドオンに関する説明的なバージョン情報を取得するアクセス許可を付与	読み込み			
DescribeCluster	Amazon EKS クラスターに関する説明情報を取得するアクセス許可を付与	読み取り	cluster*		
DescribeClusterVersions	Amazon EKS クラスターがサポートする Kubernetes バージョンに関する説明情報を取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeEksAnywhereSubscription	EKS Anywhere サブスクリプションを記述する許可を付与	読み取り	eks-anywhere-subscription*		
DescribeFargateProfile	クラスターに関連付けられた AWS Fargate プロファイルに関する説明情報を取得する許可を付与	読み取り	fargateprofile*		
DescribeIdentityProviderConfig	クラスターに関連付けられた Idp 設定に関する説明情報を取得するアクセス許可を付与	読み取り	identityproviderconfig*		
DescribeInsight	指定したクラスターで検出されたインサイトの説明情報を取得する許可を付与	読み取り	cluster*		
DescribeNodegroup	Amazon EKS ノードグループに関する説明情報を取得するアクセス許可を付与	読み取り	nodegroup*		
DescribePodIdentityAssociation	EKS Pod Identity の関連付けを記述するためのアクセス許可を付与	読み取り	podidentityassociation*		
DescribeUpdate	(指定されたリージョンまたはデフォルトリージョンにある) 特定の Amazon EKS クラスター/ノードグループ/アドオンの特定の更新を取得するアクセス許可を付与	読み取り	cluster*		
			addon		
			nodegroup		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DisassociateAccessPolicy	Amazon EKS アクセスエントリから Amazon EKS アクセスポリシーを関連付け解除する許可を付与	書き込み	access-entry*		
				eks:policyArn eks:namespaces eks:accessScope	
DisassociateIdentityProviderConfig	関連付けられた Idp 設定を削除するアクセス許可を付与	書き込み	identityproviderconfig*		
ListAccessEntries	すべての Amazon EKS アクセスエントリを一覧表示する許可を付与	リスト	cluster*		
ListAccessPolicies	Amazon EKS アクセスポリシーを一覧表示する許可を付与	リスト			
ListAddons	特定のクラスターの AWS アカウント（指定されたリージョンまたはデフォルトのリージョンの) の Amazon EKS アドオンを一覧表示するアクセス許可を付与します	リスト	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListAssociatedAccessPolicies	Amazon EKS アクセスエントリに関連するアクセスポリシーを一覧表示する許可を付与	リスト	access-entry*		
ListClusters	(指定されたリージョンまたはデフォルトリージョン AWS アカウント の) の Amazon EKS クラスターを一覧表示するアクセス許可を付与します	リスト			
ListDashboardData	ダッシュボードデータを一覧表示するアクセス許可を付与します。Amazon EKS Dashboard は、複数のアカウントとリージョンのクラスターリソースに関する情報を集約します。ダッシュボードには、EC2 インスタンスと EKS クラスターのバージョンに関する情報が含まれています。	読み取り	dashboard*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListDashboardResources	ダッシュボードリソースを一覧表示するアクセス許可を付与します。Amazon EKS Dashboard は、複数のアカウントとリージョンのクラスターリソースに関する情報を集約します。ダッシュボードには、EC2 インスタンスと EKS クラスターのバージョンに関する情報が含まれています。	読み取り	dashboard*		
ListEksAnywhereSubscriptions	EKS Anywhere サブスクリプションを一覧表示する許可を付与	リスト			
ListFargateProfiles	特定のクラスターに関連付けられた AWS アカウント（指定されたリージョンまたはデフォルトのリージョンの) の AWS Fargate プロファイルを一覧表示するアクセス許可を付与します	リスト	cluster*		
ListIdentityProviderConfigs	特定のクラスターに関連付けられた AWS アカウント（指定されたリージョンまたはデフォルトのリージョンの) の Idp 設定を一覧表示するアクセス許可を付与します	リスト	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListInsights	指定したクラスターで検出されたすべてのインサイトのリストを取得する許可を付与	リスト	cluster*		
ListNodegroups	特定のクラスターにアタッチされた AWS アカウント（指定されたリージョンまたはデフォルトのリージョンの) の Amazon EKS ノードグループを一覧表示するアクセス許可を付与します	リスト	cluster*		
ListPodIdentityAssociations	EKS Pod Identity の関連付けを一覧表示するためのアクセス許可を付与	リスト	cluster*		
ListTagsForResource	指定されたリソースのタグを一覧表示する許可を付与	読み込み	addon		
			cluster		
			dashboard		
			eks-anywhere-subscription		
			fargateprofile		
			identityproviderconfig		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			nodegroup		
ListUpdates	(指定されたリージョンまたはデフォルトリージョンにある) 特定の Amazon EKS クラスター/ノードグループの更新を一覧表示するアクセス許可を付与	リスト	cluster*		
			addon		
			nodegroup		
RegisterCluster	外部クラスターを登録する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	指定されたリソースにタグを付けるアクセス許可を付与	タグ付け	access-entry		
			addon		
			cluster		
			dashboard		
			eks-anywhere-subscription		
			fargateprofile		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			identityproviderconfig		
			nodegroup		
			podidentityassociation		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	指定されたリソースのタグを解除するアクセス許可を付与	Tagging	access-entry		
			addon		
			cluster		
			dashboard		
			eks-anywhere-subscription		
			fargateprofile		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			identityproviderconfig		
			nodegroup		
			podidentityassociation		
				aws:TagKeys	
UpdateAccessEntry	Amazon EKS アクセスエントリを更新する許可を付与	書き込み	access-entry*		
UpdateAddon	Amazon EKS アドオン設定 (VPC CNI バージョンなど) を更新するアクセス許可を付与	書き込み	addon*		
			podidentityassociation		
UpdateClusterConfig	Amazon EKS クラスター設定 (API サーバーエンドポイントアクセスなど) を更新するアクセス許可を付与	書き込み	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				eks:authenticationMode eks:supportType eks:computeConfigEnabled eks:elasticLoadBalancingEnabled eks:blockStorageEnabled	
UpdateClusterVersion	Amazon EKS クラスターの Kubernetes バージョンを更新するアクセス許可を付与	書き込み	cluster*		
UpdateEksAnywhereSubscription	EKS Anywhere サブスクリプションを更新する許可を付与	書き込み	eks-anywhere-subscription*		
UpdateNodegroupConfig	Amazon EKS ノードグループ設定を更新するアクセス許可を付与 (例: 最小/最大/希望する容量またはラベル)	書き込み	nodegroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateNodegroupVersion	Amazon EKS ノードグループの Kubernetes バージョンを更新するアクセス許可を付与	書き込み	nodegroup*		
UpdatePodIdentityAssociation	EKS Pod Identity の関連付けを更新するためのアクセス許可を付与	書き込み	podidentityassociation*		

Amazon Elastic Kubernetes Service で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
cluster	arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}	aws:ResourceTag/${TagKey}
nodegroup	arn:${Partition}:eks:${Region}:${Account}:nodegroup/${ClusterName}/${NodegroupName}/${UUID}	aws:ResourceTag/${TagKey}
addon	arn:${Partition}:eks:${Region}:${Account}:addon/${ClusterName}/${AddonName}/${UUID}	aws:ResourceTag/${TagKey}
fargateprofile	arn:${Partition}:eks:${Region}:${Account}:fargateprofile/${ClusterName}/${FargateProfileName}/${UUID}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
identityproviderconfig	arn:${Partition}:eks:${Region}:${Account}:identityproviderconfig/${ClusterName}/${IdentityProviderType}/${IdentityProviderConfigName}/${UUID}	aws:ResourceTag/${TagKey}
eks-anywhere-subscription	arn:${Partition}:eks:${Region}:${Account}:eks-anywhere-subscription/${UUID}	aws:ResourceTag/${TagKey}
podidentityassociation	arn:${Partition}:eks:${Region}:${Account}:podidentityassociation/${ClusterName}/${UUID}	aws:ResourceTag/${TagKey}
access-entry	arn:${Partition}:eks:${Region}:${Account}:access-entry/${ClusterName}/${IamIdentityType}/${IamIdentityAccountID}/${IamIdentityName}/${UUID}	aws:ResourceTag/${TagKey} eks:accessEntryType eks:clusterName eks:kubernetesGroups eks:principalArn eks:username
access-policy	arn:${Partition}:eks::aws:cluster-access-policy/${AccessPolicyName}	
dashboard	arn:${Partition}:eks:${Region}:${Account}:dashboard/${DashboardName}	aws:ResourceTag/${TagKey}

Amazon Elastic Kubernetes Service の条件キー

Amazon Elastic Kubernetes Service では、IAM ポリシーの `Condition` 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	ユーザーが EKS サービスに対して行うリクエストに含まれるキーによってアクセスがフィルタリングされます	文字列
aws:ResourceTag/${TagKey}	タグキーおよび値のペアでアクセスをフィルタリングします。	文字列
aws:TagKeys	ユーザーが EKS サービスに対して行うリクエストに含まれるすべてのタグキー名のリストでアクセスをフィルタリングします	ArrayOfString
eks:accessEntryType	ユーザーが EKS サービスに対して行うアクセスエントリリクエストに含まれるアクセスエントリタイプでアクセスをフィルタリングします	String
eks:accessScope	ユーザーが EKS サービスに対して行う 関連付け/関連付け解除アクセス ポリシーリクエストに存在する accessScope でアクセスをフィルタリングします	String
eks:authenticationMode	クラスターの作成/更新リクエストに存在する authenticationMode でアクセスをフィルタリングする	String
eks:blockStorageEnabled	クラスターの作成/更新リクエストのブロックストレージ対応パラメータでアクセスをフィルタリングします	Bool
eks:bootstrapClusterCreator	クラスター作成リクエストに存在する bootstrapClusterCreatorAdminPermissions でアクセスをフィルタリングします	Bool

条件キー	説明	タイプ
AdminPermissions		
eks:bootstrapSelfManagedAddons	クラスター作成リクエストに存在する bootstrapSelfManagedAddons でアクセスをフィルタリングする	Bool
eks:clientId	ユーザーが EKS サービスに対して行う associate IdentityProviderConfig リクエストに存在する clientId でアクセスをフィルタリングします	String
eks:clusterName	ユーザーが EKS サービスに対して行うアクセスエントリリクエストに存在するクラスター名でアクセスをフィルタリングします	String
eks:computeConfigEnabled	クラスターの作成/更新リクエストのコンピューティング設定が有効なパラメータでアクセスをフィルタリングします	Bool
eks:elasticLoadBalancingEnabled	クラスターの作成/更新リクエストでエラスティックロードバランシングが有効なパラメータでアクセスをフィルタリングします	Bool
eks:issuerUrl	ユーザーが EKS サービスに対して行う associate IdentityProviderConfig リクエストに存在する issuerUrl でアクセスをフィルタリングします	String
eks:kubernetesGroups	ユーザーが EKS サービスに対して行うアクセスエントリリクエストに存在する KubernetesGroups でアクセスをフィルタリングします	ArrayOfString
eks:namespaces	ユーザーが EKS サービスに対して行う関連付け/関連付け解除アクセスポリシーリクエストに存在する名前空間でアクセスをフィルタリングします	ArrayOfString
eks:policyArn	ユーザーが EKS サービスに対して行うリクエストに含まれる policyArn でアクセスをフィルタリングします	ARN

条件キー	説明	タイプ
eks:principalArn	ユーザーが EKS サービスに対して行うアクセスエントリリクエストに存在する principaLarn でアクセスをフィルタリングします	ARN
eks:supportType	クラスターの作成/更新リクエストに存在する supportType でアクセスをフィルタリングする	String
eks:username	ユーザーが EKS サービスに対して行うアクセスエントリリクエストに存在する Kubernetes ユーザー名でアクセスをフィルタリングします	String

AWS Elastic Load Balancing のアクション、リソース、および条件キー

AWS Elastic Load Balancing (サービスプレフィックス: `elasticloadbalancing`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Elastic Load Balancing で定義されるアクション
- AWS Elastic Load Balancing で定義されるリソースタイプ
- AWS Elastic Load Balancing の条件キー

AWS Elastic Load Balancing で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddTags	指定されたタグを指定されたロードバランサーに追加する許可を付与します。ロードバランサーにはそれぞれ、タグを最大 10 個設定できます	Tagging	loadbalancer*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:CreateAction	
ApplySecurityGroupsToLoadBalancer	Virtual Private Cloud (VPC) の 1 つ以上のセキュリティグループをロードバランサーに関連付ける許可を付与	書き込み	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalanci	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ng:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup	
AttachLoadBalancerToSubnets	指定されたロードバランサーの一連の構成済みサブネットに 1 つ以上のサブネットを追加する許可を付与	書き込み	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:Subnet	
ConfigureHealthCheck	バックエンドインスタンスのヘルス状態を評価するときに使用するヘルスチェック設定を指定する許可を付与	書き込み	loadbalancer*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateAppCookieStickinessPolicy	アプリケーションによって生成された Cookie に従うスティッキーセッション存続期間を持つ維持ポリシーを生成する許可を付与	書き込み	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateLBCookieStickinessPolicy	ブラウザ (user-agent) の存続期間または指定された有効期間によって制御されるスティッキーセッション存続期間を持つ維持ポリシーを生成する許可を付与	書き込み	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateLoadBalancer	ロードバランサーを作成する許可を付与	書き込み	loadbalancer		elasticloadbalancing:AddTags

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup elasticloadbalancing:Subnet elasticloadbalancing:Scheme elasticloadbalancing:Listen	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				erProtocol	
CreateLoadBalancerListeners	指定されたロードバランサーに 1 つ以上のリスナーを作成する許可を付与	書き込み	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:ListenerProtocol	
CreateLoadBalancerPolicy	指定されたロードバランサーの指定された属性を持つポリシーを作成する許可を付与	書き込み	loadbalancer*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy	
DeleteLoadBalancer	指定されたロードバランサーを削除する許可を付与	書き込み	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteLoadBalancerListeners	指定されたロードバランサーから指定されたリスナーを削除する許可を付与	書き込み	loadbalancer*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteLoadBalancerPolicy	指定されたロードバランサーから指定されたポリシーを削除する許可を付与 このポリシーでは、リスナーを有効にできません。	書き込み	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeregisterInstancesFromLoadBalancer	指定されたロードバランサーから指定されたインスタンスを登録解除する許可を付与	書き込み	loadbalancer*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DescribeInstanceHealth	指定されたロードバランサーに関して指定されたインスタンスの状態を記述する許可を付与	読み取り			
DescribeLoadBalancerAttributes	指定されたロードバランサーの属性を記述する許可を付与	読み取り			
DescribeLoadBalancerPolicies	指定されたポリシーを記述する許可を付与	読み取り			
DescribeLoadBalancerPolicyTypes	指定されたロードバランサーのポリシータイプを記述する許可を付与	読み取り			
DescribeLoadBalancers	指定されたロードバランサーを記述する許可を付与 ロードバランサーを指定せずに呼び出すと、すべてのロードバランサーの説明が表示されます	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeTags	指定されたロードバランサーに関連付けられているタグを記述する許可を付与	読み取り			
DetachLoadBalancerFromSubnets	指定されたサブネットを、ロードバランサーの一連の構成済みサブネットから削除する許可を付与	書き込み	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DisableAvailabilityZonesForLoadBalancer	指定されたアベイラビリティーゾーンを、指定されたロードバランサーの一連のアベイラビリティーゾーンから削除する許可を付与	書き込み	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
EnableAvailabilityZonesForLoadBalancer	指定されたアベイラビリティーゾーンを、指定されたロードバランサーの一連のアベイラビリティーゾーンに追加する許可を付与	書き込み	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyLoadBalancerAttributes	指定されたロードバランサーの属性を変更する許可を付与	書き込み	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RegisterInstancesWithLoadBalancer	指定されたインスタンスを指定されたロードバランサーに追加するする許可を付与	書き込み	loadbalancer*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTags	指定されたロードバランサーから 1 つ以上のタグを削除する許可を付与	Tagging	loadbalancer*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SetLoadBalancerListenerSSLCertificate	指定されたリスナーの SSL 接続を終了する証明書を設定する許可を付与	書き込み	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetLoadBalancerPoliciesForBackendServer	バックエンドサーバーがリスンしている指定されたポートに関連付けられている一連のポリシーを、新しい一連のポリシーに置き換える許可を付与	書き込み	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetLoadBalancerPoliciesOfListener	指定されたロードバランサーポートの現在の一連のポリシーを、指定された一連のポリシーに置き換える許可を付与	書き込み	loadbalancer*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy	

AWS Elastic Load Balancing で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
loadbalancer	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/${LoadBalancerName}`	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

AWS Elastic Load Balancing の条件キー

AWS Elastic Load Balancing では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString
elasticloadbalancing:CreateAction	リソース作成 API アクションの名前によってアクセスをフィルタリングします	String
elasticloadbalancing:ListenerProtocol	リクエストで許可されているリスナープロトコル (複数) でアクセスをフィルタリング	ArrayOfString
elasticloadbalancing:ResourceTag/	リソースにアタッチされているタグキーと値のペアの先頭文字列によってアクセスをフィルタリングします	String
elasticloadbalancing:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアの先頭文字列によってアクセスをフィルタリングします	String

条件キー	説明	タイプ
elasticloadbalancing:Scheme	リクエストで許可されているロードバランサースキーム (複数) でアクセスをフィルタリング	String
elasticloadbalancing:SecurityGroup	リクエストで許可されているセキュリティグループ ID (複数) でアクセスをフィルタリングします	ArrayOfString
elasticloadbalancing:SecurityPolicy	リクエストで許可されている SSL セキュリティポリシー (複数) でアクセスをフィルタリングします	ArrayOfString
elasticloadbalancing:Subnet	リクエストで許可されているサブネット ID (複数) でアクセスをフィルタリングします	ArrayOfString

AWS Elastic Load Balancing V2 のアクション、リソース、条件キー

AWS Elastic Load Balancing V2 (サービスプレフィックス: `elasticloadbalancing`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Elastic Load Balancing V2 で定義されるアクション
- AWS Elastic Load Balancing V2 で定義されるリソースタイプ
- AWS Elastic Load Balancing V2 の条件キー

AWS Elastic Load Balancing V2 で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AddListenerCertificates	指定された証明書を指定されたセキュアリスナーに追加する許可を付与	書き込み	listener/app*		
			listener/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
AddTags	指定されたタグを指定されたロードバランサーに追加する許可を付与 ロードバランサーにはそれぞれ、タグを最大 10 個設定できます	Tagging	listener-rule/app		
			listener-rule/net		
			listener/app		
			listener/gwy		
			listener/net		
			loadbalancer/app/		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			loadbalancer/gwy/		
			loadbalancer/net/		
			targetgroup		
			truststore		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:CreateAction	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddTrustStoreRevocations	トラストストアに失効を追加する許可を付与	書き込み	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateListener	指定された Application Load Balancer のリスナーを作成する許可を付与		loadbalancer/app/		elasticloadbalancing:AddTags
			loadbalancer/gwy/		
			loadbalancer/net/		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy elasticloadbalancing:ListenerProtocol	
CreateLoadBalancer	ロードバランサーを作成する許可を付与	書き込み	loadbalancer/app/		elasticloadbalancing:AddTags

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			loadbalancer/gwy/		
			loadbalancer/net/		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup elasticloadbalancing:Subnet elasticloadbalancing:Scheme	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateRule	指定されたリスナーのルールを作成する許可を付与	書き込み	listener/app*		elasticloadbalancing:AddTags
			listener/net*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateTargetGroup	ターゲットグループを作成する許可を付与	書き込み	targetgroup*		elasticloadbalancing:AddTags

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateTrustStore	トラストストアを作成する許可を付与	書き込み	truststore		elasticloadbalancing:AddTags

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteListener	指定されたリスナーを削除する許可を付与	書き込み	listener/app*		
			listener/gwy*		
			listener/net*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteLoadBalancer	指定されたロードバランサーを削除する許可を付与	書き込み	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteRule	指定されたルールを削除する許可を付与	書き込み	listener-rule/app*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			listener-rule/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteSharedTrustStoreAssociation	指定された共有トラストストアの関連付けを削除する許可を付与する	書き込み	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteTargetGroup	指定されたターゲットグループを削除する許可を付与	書き込み	targetgroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteTrustStore	指定されたトラストストアを削除する許可を付与	書き込み	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeregisterTargets	指定されたターゲットを指定されたターゲットグループから登録解除する許可を付与	書き込み	targetgroup*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DescribeAccountLimits	の Elastic Load Balancing リソース制限を記述するアクセス許可を付与します AWS アカウント	読み取り			
DescribeCapacityReservation	ロードバランサーのキャパシティ予約を記述するアクセス許可を付与します	読み取り			
DescribeListenerAttributes	指定されたリスナーの属性を記述する許可を付与する	読み取り			
DescribeListenerCertificates	指定されたセキュアリスナーの証明書を記述する許可を付与	読み取り			
DescribeListeners	指定されたリスナー、または指定された Application Load Balancer のリスナーを記述する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeLoadBalancerAttributes	指定されたロードバランサーの属性を記述する許可を付与	読み取り			
DescribeLoadBalancers	指定されたロードバランサーを記述する許可を付与 ロードバランサーを指定せずに呼び出すと、すべてのロードバランサーの説明が表示されます	読み取り			
DescribeRules	指定されたルール、または指定されたリスナーのルールを記述する許可を付与	読み取り			
DescribeSSLPolicies	指定されたポリシー、または SSL ネゴシエーションに使用されるすべてのポリシーを記述する許可を付与	読み取り			
DescribeTags	指定されたリソースに関連付けられているタグを記述する許可を付与	読み取り			
DescribeTargetGroupAttributes	指定されたターゲットグループの属性を記述する許可を付与	読み取り			
DescribeTargetGroups	指定されたターゲットグループまたはすべてのターゲットグループを記述する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeTargetHealth	指定されたターゲットまたはすべてのターゲットの状態を記述する許可を付与	読み取り			
DescribeTrustStoreAssociations	トラストストアとの関連付けを説明する許可を付与	読み取り			
DescribeTrustStoreRevocations	指定したトラストストア、失効、またはトラストストアに関連するすべての失効を記述する許可を付与	読み取り			
DescribeTrustStores	指定されたトラストストアまたはすべてのトラストストアを説明する許可を付与	読み取り			
GetResourcePolicy	リソースに関連付けられたリソースポリシーを取得する許可を付与する	読み取り	truststore		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetTrustStoreCaCertificatesBundle	トラストストア CA 証明書バンドルを取得する許可を付与	読み取り	truststore*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetTrustStoreRevocationContent	トラストストアの失効内容を取得する許可を付与	読み取り	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyCapacityReservation	ロードバランサーのキャパシティ予約を変更するアクセス許可を付与します	書き込み	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyIpPools	ロードバランサーの ip プールを変更するアクセス許可を付与します	書き込み	loadbalancer/app/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyListener	指定されたリスナーの指定されたプロパティを変更する許可を付与	書き込み	listener/app*		
			listener/gwy*		
			listener/net*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy elasticloadbalancing:ListenerProtocol	
ModifyListenerAttributes	指定されたリスナーの属性を変更する許可を付与する	書き込み	listener/app*		
			listener/gwy*		
			listener/net*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyLoadBalancerAttributes	指定されたロードバランサーの属性を変更する許可を付与	書き込み	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyRule	指定されたルールを変更する許可を付与	書き込み	listener-rule/app*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			listener-rule/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTargetGroup	指定されたターゲットグループのターゲットの状態を評価する際に使用するヘルスチェックを変更する許可を付与	書き込み	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTargetGroupAttributes	指定されたターゲットグループの指定された属性を変更する許可を付与	書き込み	targetgroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTrustStore	指定されたトラストストアを変更する許可を付与	書き込み	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RegisterTargets	指定されたターゲットを指定されたターゲットグループに登録する許可を付与	書き込み	targetgroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveListenerCertificates	指定されたセキュアリスナーの指定された証明書を削除する許可を付与	書き込み	listener/app*		
			listener/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTags	指定されたロードバランサーから 1 つ以上のタグを削除する許可を付与	Tagging	listener-rule/app		
			listener-rule/net		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			listener/app		
			listener/gwy		
			listener/net		
			loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
			targetgroup		
			truststore		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTrustStoreRevocations	トラストストアから失効を削除する許可を付与	書き込み	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SetIpAddressType	指定されたロードバランサーのサブネットで使用される IP アドレスのタイプを設定する許可を付与	書き込み	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetRulePriorities	指定されたルールの優先順位を設定する許可を付与	書き込み	listener-rule/app*		
			listener-rule/net*		
SetSecurityGroups	指定されたセキュリティグループを指定されたロードバランサーに関連付ける許可を付与	書き込み	loadbalancer/app/		
			loadbalancer/net/		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup	
SetSubnets	指定されたロードバランサーの指定されたサブネットのアベイラビリティーゾーンを有効にする許可を付与	書き込み	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:Subnet	
SetWebAcl [アクセス許可のみ]	WAF に WebAcl アクセス許可を付与アクセス許可を付与	書き込み			

AWS Elastic Load Balancing V2 で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
listener/gwy	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/gwy/`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
	${LoadBalancerName}/${LoadBalancerId}/${ListenerId}	elasticloadbalancing:ResourceTag/${TagKey}
listener/app	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/app/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener-rule/app	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener-rule/app/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}/${ListenerRuleId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener/net	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/net/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener-rule/net	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener-rule/net/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}/${ListenerRuleId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
loadbalancer/gwy/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/gwy/${LoadBalancerName}/${LoadBalancerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
loadbalancer/app/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
loadbalancer/net/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/net/${LoadBalancerName}/${LoadBalancerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
targetgroup	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:targetgroup/${TargetGroupName}/${TargetGroupId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
truststore	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:truststore/${TrustStoreName}/${TrustStoreId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

AWS Elastic Load Balancing V2 の条件キー

AWS Elastic Load Balancing V2 では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString
elasticloadbalancing:CreateAction	リソース作成 API アクションの名前によってアクセスをフィルタリングします	String
elasticloadbalancing:ListenerProtocol	リクエストで許可されているリスナープロトコルでアクセスをフィルタリングします	String
elasticloadbalancing:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアの先頭文字列によってアクセスをフィルタリングします	String
elasticloadbalancing:Scheme	リクエストで許可されているロードバランサースキームでアクセスをフィルタリングします	String

条件キー	説明	タイプ
elasticloadbalancing:SecurityGroup	リクエストで許可されているセキュリティグループ ID (複数) でアクセスをフィルタリングします	ArrayOfString
elasticloadbalancing:SecurityPolicy	リクエストで許可されている SSL セキュリティポリシー (複数) でアクセスをフィルタリングします	ArrayOfString
elasticloadbalancing:Subnet	リクエストで許可されているサブネット ID (複数) でアクセスをフィルタリングします	ArrayOfString

Amazon Elastic MapReduce のアクション、リソース、および条件キー

Amazon Elastic MapReduce (サービスプレフィックス: `elasticmapreduce`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Elastic MapReduce で定義されるアクション
- Amazon Elastic MapReduce で定義されるリソースタイプ
- Amazon Elastic MapReduce の条件キー

Amazon Elastic MapReduce で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

> **Note**
>
> DescribeJobFlows API は廃止され、最終的には削除されます。代わりに、ListClusters, DescribeCluster, ListSteps, ListInstanceGroups、および ListBootstrapActions の使用をお勧めします。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AccessAllEventLogs	永続アプリケーション履歴サーバー内のすべてのイベントログを表示するアクセス許可を付与します	書き込み	cluster*		
AddInstanceFleet	実行中のクラスターにインスタンスフリートを追加するためのアクセス許可を付与	書き込み	cluster*		
AddInstanceGroups	実行中のクラスターにインスタンスグループを追加するためのアクセス許可を付与	書き込み	cluster*		
AddJobFlowSteps	実行中のクラスターに新しいステップを追加するためのアクセス許可を付与	書き込み	cluster*		
				elasticmapreduce:ExecutionRoleArn	
AddTags	Amazon EMR リソースにタグを追加するためのアクセス許可を付与	Tagging	cluster		
			editor		
			notebook-execution		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			studio		
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
AttachEditor [アクセス許可のみ]	コンピューティングエンジンに EMR Notebooks をアタッチするためのアクセス許可を付与	書き込み	editor*		
CancelSteps	実行中のクラスターで保留中の (1 つないしは複数の) ステップをキャンセルするためのアクセス許可を付与	書き込み	cluster*		
CreateEditor [アクセス許可のみ]	EMR Notebooks を作成するためのアクセス許可を付与	書き込み	cluster		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
CreatePersistentAppUI	永続的なアプリケーション履歴サーバーを作成するためのアクセス許可を付与	書き込み	cluster*		
CreateRepository [アクセス許可のみ]	EMR Notebooks のリポジトリを作成するためのアクセス許可を付与	書き込み			
CreateSecurityConfiguration	セキュリティ設定を作成する許可を付与。	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateStudio	EMR Studio を作成するためのアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
CreateStudioPresignedUrl	IAM 認証モードを使用して EMR Studio を起動するためのアクセス許可を付与	書き込み	studio*		
CreateStudioSessionMapping	EMR Studio のセッションマッピングを作成するためのアクセス許可を付与	書き込み	studio*		
DeleteEditor [アクセス許可のみ]	EMR Notebooks を削除するためのアクセス許可を付与	書き込み	editor*		
DeleteRepository [アクセス許可のみ]	EMR Notebooks のリポジトリを削除するためのアクセス許可を付与	書き込み			
DeleteSecurityConfiguration	セキュリティ設定を削除する許可を付与。	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteStudio	EMR Studio を削除するためのアクセス許可を付与	書き込み	studio*		
DeleteStudioSessionMapping	EMR Studio のセッションマッピングを削除するためのアクセス許可を付与	書き込み	studio*		
DeleteWorkspaceAccess [アクセス許可のみ]	アイデンティティがコラボレーション用ワークスペースを開くことをブロックするアクセス許可を付与	権限の管理	editor*		
DescribeCluster	ステータス、ハードウェアとソフトウェアの設定、VPC 設定およびその他の、クラスターに関する詳細を取得するためのアクセス許可を付与	読み込み	cluster*		
DescribeEditor [アクセス許可のみ]	ステータス、ユーザー、ロール、タグ、場所など、ノートブックに関する情報を表示するためのアクセス許可を付与	読み込み	editor*		
DescribeJobFlows	クラスター (ジョブフロー) について詳細表示するためのアクセス許可を付与 この API は廃止され、最終的には削除されます。代わりに、ListClusters, DescribeCluster, ListSteps, ListInstanceGroups、および ListBootstrapActions の使用をお勧めします。	読み込み	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeNotebookExecution	ノートブックの実行に関する情報を表示するためのアクセス許可を付与	読み込み	notebook-execution*		
DescribePersistentAppUI	永続的なアプリケーション履歴サーバーについて詳細表示するためのアクセス許可を付与	読み込み	cluster*		
DescribeReleaseLabel	サポートされているアプリケーションなど、EMR リリースに関する情報を表示するためのアクセス許可を付与	読み込み			
DescribeRepository [アクセス許可のみ]	EMR Notebooks のリポジトリについて詳細表示するためのアクセス許可を付与	読み込み			
DescribeSecurityConfiguration	セキュリティ設定の詳細を取得するためのアクセス許可を付与	読み込み			
DescribeStep	クラスターステップに関する詳細を取得するためのアクセス許可を付与	読み込み	cluster*		
DescribeStudio	EMR Studio に関する情報を表示するためのアクセス許可を付与	読み込み	studio*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DetachEditor [アクセス許可のみ]	コンピューティングエンジンから EMR Notebooks をデタッチするためのアクセス許可を付与	書き込み	editor*		
GetAutoTerminationPolicy	クラスターに関連付けられた自動終了ポリシーを取得するためのアクセス許可を付与	読み取り	cluster*		
GetBlockPublicAccessConfiguration	リージョンの の EMR ブロックパブリックアクセス設定を取得するアクセス許可を付与 AWS アカウント します	読み取り			
GetClusterSessionCredentials	きめ細かなアクセス制御が可能な EMR クラスターの、特定の実行 IAM ロールに関連する HTTP 基本認証情報を取得するアクセス許可を付与	書き込み	cluster*		
				elasticmapreduce:ExecutionRoleArn	
GetManagedScalingPolicy	クラスターに関連付けられたマネージドスケーリングポリシーを取得するためのアクセス許可を付与	読み込み	cluster*		
GetOnClusterAppUIPresignedURL	クラスターで実行されているアプリケーション履歴サーバーの、署名付き URL を取得するためのアクセス許可を付与	書き込み	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetPersistentAppUIPresignedURL	永続的なアプリケーション履歴サーバーの、署名付き URL を取得するためのアクセス許可を付与	書き込み	cluster*		
				elasticmapreduce:ExecutionRoleArn	
GetStudioSessionMapping	EMR Studio のセッションマッピングに関する情報を表示するためのアクセス許可を付与	読み込み	studio*		
LinkRepository [アクセス許可のみ]	EMR Notebooks のリポジトリを EMR Notebooks にリンクするためのアクセス許可を付与	書き込み			
ListBootstrapActions	クラスターに関連付けられたブートストラップアクションの詳細を取得するためのアクセス許可を付与	読み込み	cluster*		
ListClusters	アクセス可能なクラスターのステータスを取得するためのアクセス許可を付与	リスト			
ListEditors [アクセス許可のみ]	アクセス可能な EMR Notebooks の概要情報をリストするためのアクセス許可を付与	リスト			
ListInstanceFleets	クラスター内のインスタンスフリートの詳細を取得するためのアクセス許可を付与	読み込み	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListInstanceGroups	クラスター内のインスタンスグループの詳細を取得するためのアクセス許可を付与	読み込み	cluster*		
ListInstances	クラスター内の Amazon EC2 インスタンスに関する詳細を取得するためのアクセス許可を付与	読み込み	cluster*		
ListNotebookExecutions	ノートブック実行についての概要情報をリストするためのアクセス許可を付与	リスト			
ListReleaseLabels	現在のリージョンで使用可能な EMR リリースを、リストしてフィルタリングするためのアクセス許可を付与	リスト			
ListRepositories [アクセス許可のみ]	既存の EMR Notebooksリポジトリをリストするためのアクセス許可を付与	リスト			
ListSecurityConfigurations	このアカウントで利用可能なセキュリティ設定を、名前ならびに作成の日付および時刻によりリストするためのアクセス許可を付与	リスト			
ListSteps	クラスターに関連付けられているステップをリストするためのアクセス許可を付与	読み込み	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListStudioSessionMappings	EMR Studio のセッションマッピングに関する概要情報をリストするためのアクセス許可を付与	リスト			
ListStudios	EMR Studios に関する概要情報をリストするためのアクセス許可を付与	リスト			
ListSupportedInstanceTypes	Amazon EMR リリースがサポートする Amazon EC2 インスタンスタイプを一覧表示するアクセス許可を付与します	リスト			
ListWorkspaceAccessIdentities [アクセス許可のみ]	ワークスペースへのアクセス許可を付与アイデンティティを一覧表示するアクセス許可を付与	リスト	editor*		
ModifyCluster	クラスターで同時に実行できるステップ数など、クラスターの設定を変更するためのアクセス許可を付与	書き込み	cluster*		
ModifyInstanceFleet	インスタンスフリートのオンデマンドおよびスポットのターゲットキャパシティーを変更するためのアクセス許可を付与	書き込み	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ModifyInstanceGroups	インスタンスグループにおける EC2 インスタンスの数と設定を変更するためのアクセス許可を付与	書き込み	cluster		
OpenEditorInConsole [アクセス許可のみ]	EMR ノートブックのための Jupyter Notebook エディタを、コンソール内から起動するためのアクセス許可を付与	書き込み	editor* cluster		
PutAutoScalingPolicy	コアインスタンスグループまたはタスクインスタンスグループのための、オートスケーリングポリシーを作成または更新するためのアクセス許可を付与	書き込み	cluster*		
PutAutoTerminationPolicy	クラスターに関連付けられた自動終了ポリシーを作成または更新するためのアクセス許可を付与	書き込み	cluster*		
PutBlockPublicAccessConfiguration	リージョンの の EMR ブロックパブリックアクセス設定を作成または更新するアクセス許可を付与 AWS アカウントします	権限の管理			
PutManagedScalingPolicy	クラスターに関連付けられたマネージドスケーリングポリシーを、作成または更新するためのアクセス許可を付与	書き込み	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutWorkspaceAccess [アクセス許可のみ]	アイデンティティがコラボレーション用ワークスペースを開くことを許可するアクセス許可を付与	権限の管理	editor*		
RemoveAutoScalingPolicy	インスタンスグループからオートスケーリングポリシーを削除するためのアクセス許可を付与	書き込み	cluster*		
RemoveAutoTerminationPolicy	クラスターに関連付けられた自動終了ポリシーを削除するためのアクセス許可を付与	書き込み	cluster*		
RemoveManagedScalingPolicy	クラスターに関連付けられたマネージドスケーリングポリシーを削除するためのアクセス許可を付与	書き込み	cluster*		
RemoveTags	Amazon EMR リソースからタグを削除するためのアクセス許可を付与	Tagging	cluster		
			editor		
			notebook-execution		
			studio		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RunJobFlow	クラスター (ジョブフロー) を作成して起動するためのアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	iam:PassRole
SetKeepJobFlowAliveWhenNoSteps	クラスターのステップ実行後に自動終了を追加および削除する許可を付与する	書き込み	cluster*		
SetTerminationProtection	クラスターの終了保護を追加および削除するためのアクセス許可を付与	書き込み	cluster*		
SetUnhealthyNodeReplacement	クラスターの異常なノード置換を有効または無効にする許可を付与する	書き込み	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SetVisibleToAllUsers	内のすべての AWS Identity and Access Management (IAM) ユーザーがクラスターを表示 AWS アカウント できるかどうかを設定するアクセス許可を付与します。この API は非推奨となり、クラスターはアカウント内のすべてのユーザーに表示される可能性があります。IAM ポリシーを使用してクラスターアクセスを制限するには、「Amazon EMR の AWS Identity and Access Management (https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-access-iam.html)」を参照してください。	書き込み	cluster*		
StartEditor [アクセス許可のみ]	EMR Notebooks を開始するためのアクセス許可を付与	書き込み	editor*		
			cluster		
StartNotebookExecution	EMR Notebooks の実行を開始するためのアクセス許可を付与	書き込み	cluster*		
			editor*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
StopEditor [アクセス許可のみ]	EMR Notebooks をシャットダウンするための許可を付与	書き込み	editor*		
StopNotebookExecution	ノートブックの実行を停止するための許可を付与	書き込み	notebook-execution*		
TerminateJobFlows	クラスター (ジョブフロー) を終了するためのアクセス許可を付与	書き込み	cluster*		
UnlinkRepository [アクセス許可のみ]	EMR Notebooks から EMR ノートブックリポジトリへのリンクを解除するためのアクセス許可を付与	書き込み			
UpdateEditor [アクセス許可のみ]	EMR Notebooks を更新するアクセス許可を付与	書き込み	editor*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateRepository [アクセス許可のみ]	EMR Notebooks のリポジトリを更新するためのアクセス許可を付与	書き込み			
UpdateStudio	EMR Studio に関する情報を更新するためのアクセス許可を付与	書き込み	studio*		
UpdateStudioSessionMapping	EMR Studio のセッションマッピングを更新するためのアクセス許可を付与	書き込み	studio*		
ViewEventsFromAllClustersInConsole [アクセス許可のみ]	EMR コンソールを使用して、すべてのクラスターのイベントを表示するためのアクセス許可を付与	リスト			

Amazon Elastic MapReduce で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
cluster	arn:${Partition}:elasticmapreduce:${Region}:${Account}:cluster/${ClusterId}	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}
editor	arn:${Partition}:elasticmapreduce:${Region}:${Account}:editor/${EditorId}	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}
notebook-execution	arn:${Partition}:elasticmapreduce:${Region}:${Account}:notebook-execution/${NotebookExecutionId}	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}
studio	arn:${Partition}:elasticmapreduce:${Region}:${Account}:studio/${StudioId}	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}

Amazon Elastic MapReduce の条件キー

Amazon Elastic MapReduce では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	アクションでタグと値のペアが指定されているかどうかに基づいてアクセスをフィルタリングする	String
aws:ResourceTag/${TagKey}	Amazon EMR リソースに関連付けられているタグと値のペアによりアクセスをフィルタリングする	String
aws:TagKeys	タグ値に関係なく、アクションでタグキーが指定されているかどうかによりアクセスをフィルタリングする	ArrayOfString
elasticmapreduce:ExecutionRoleArn	実行ロール ARN がアクションで指定されているかどうかによってアクセスをフィルタリング	ARN
elasticmapreduce:RequestTag/${TagKey}	アクションでタグと値のペアが指定されているかどうかに基づいてアクセスをフィルタリングする	String
elasticmapreduce:ResourceTag/${TagKey}	Amazon EMR リソースに関連付けられているタグと値のペアによりアクセスをフィルタリングする	String

Amazon Elastic Transcoder のアクション、リソース、および条件キー

Amazon Elastic Transcoder (サービスプレフィックス: `elastictranscoder`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Elastic Transcoder で定義されるアクション
- Amazon Elastic Transcoder で定義されるリソースタイプ
- Amazon Elastic Transcoder の条件キー

Amazon Elastic Transcoder で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelJob	Elastic Transcoder による処理がまだ開始されていないジョブをキャンセルします。	書き込み	job*		
CreateJob	ジョブの作成	書き込み	pipeline*		
			preset*		
CreatePipeline	パイプラインを作成します。	書き込み			
CreatePreset	プリセットの作成	書き込み			
DeletePipeline	パイプラインを削除します。	Write	pipeline*		
DeletePreset	プリセットを削除します。	Write	preset*		
ListJobsByPipeline	パイプラインに割り当てたジョブのリストを取得します。	リスト	pipeline*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListJobsByStatus	ステータスが AWS アカウント 指定された現在の に関連付けられているすべてのジョブに関する情報を取得する	リスト			
ListPipelines	現在の に関連付けられているパイプラインのリストを取得する AWS アカウント	リスト			
ListPresets	現在の に関連付けられているすべてのプリセットのリストを取得する AWS アカウント	リスト			
ReadJob	ジョブに関する詳細情報を取得します。	Read	job*		
ReadPipeline	パイプラインに関する詳細情報を取得します。	読み取り	pipeline*		
ReadPreset	プリセットに関する詳細情報の取得	読み取り	preset*		
TestRole	パイプラインの設定をテストし、Elastic Transcoder がジョブを作成・処理できることを確実にします。	Write			
UpdatePipeline	パイプラインの設定を更新します。	Write	pipeline*		
UpdatePipelineNotifications	パイプラインに対する Amazon Simple Notification Service (Amazon SNS) 通知のみを更新します。	書き込み	pipeline*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdatePipelineStatus	パイプラインを一時停止または再開することにより、パイプラインがジョブ処理を停止または再開して、パイプラインのステータスを更新	書き込み	pipeline*		

Amazon Elastic Transcoder で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
job	`arn:${Partition}:elastictranscoder:${Region}:${Account}:job/${JobId}`	
pipeline	`arn:${Partition}:elastictranscoder:${Region}:${Account}:pipeline/${PipelineId}`	
preset	`arn:${Partition}:elastictranscoder:${Region}:${Account}:preset/${PresetId}`	

Amazon Elastic Transcoder の条件キー

Elastic Transcoder には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Elastic VMware Service のアクション、リソース、および条件キー

Amazon Elastic VMware Service (サービスプレフィックス: evs) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Elastic VMware Service で定義されるアクション
- Amazon Elastic VMware Service で定義されるリソースタイプ
- Amazon Elastic VMware Service の条件キー

Amazon Elastic VMware Service で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateEnvironment	Amazon EVS 環境を作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateEnvironmentHost	Amazon EVS 環境にホストを追加するアクセス許可を付与します	書き込み	environment*		
DeleteEnvironment	Amazon EVS 環境を削除するアクセス許可を付与します	書き込み	environment*		
DeleteEnvironmentHost	Amazon EVS 環境からホストを削除するアクセス許可を付与します	書き込み	environment*		
GetEnvironment	Amazon EVS 環境を取得する許可を付与	読み取り	environment*		
ListEnvironmentHosts	Amazon EVS 環境に関連付けられたホストのリストを取得するアクセス許可を付与します	リスト	environment*		
ListEnvironmentVlans	Amazon EVS 環境 VLANs	リスト	environment*		
ListEnvironments	アカウント内の Amazon EVS 環境のリストを取得するアクセス許可を付与します	リスト			
ListTagsForResource	指定したリソース ARN のタグを一覧表示する許可を付与	読み取り	environment		
TagResource	指定されたリソース ARN にタグを付ける許可を付与	Tagging	environment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	指定されたリソース ARN からタグを削除する許可を付与	Tagging	environment*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Amazon Elastic VMware Service で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
environment	arn:${Partition}:evs:${Region}:${Account}:environment/${EnvironmentIdentifier}	aws:ResourceTag/${TagKey}

Amazon Elastic VMware Service の条件キー

Amazon Elastic VMware Service では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString

Amazon ElastiCache のアクション、リソース、および条件キー

Amazon ElastiCache (サービスプレフィックス: elasticache) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon ElastiCache で定義されるアクション
- Amazon ElastiCache で定義されるリソースタイプ
- Amazon ElastiCache の条件キー

Amazon ElastiCache で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

> **Note**
>
> IAM で ElastiCache ポリシーを作成する場合、リソースブロックでワイルドカード「*」を使用する必要があります。IAM ポリシーで以下の ElastiCache の API アクションを使用する方法については、Amazon ElastiCache ユーザーガイドの「ElastiCache のアクションと IAM」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddTagsToResource	ElastiCache リソースにタグを追加する許可を付与。	タグ付け	cluster		
			parametergroup		
			replicationgroup		
			reserved-instance		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			securitygroup		
			serverlesscache		
			serverlesscachesnapshot		
			snapshot		
			subnetgroup		
			user		
			usergroup		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
AuthorizeCacheSecurityGroupIngress	ElastiCache セキュリティグループで EC2 セキュリティグループを承認する許可を付与。	Write	securitygroup*		ec2:AuthorizeSecurityGroupIngress

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
BatchApplyUpdateAction	クラスターとレプリケーショングループのセットに ElastiCache サービス更新を適用する許可を付与。	Write	cluster		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs s3:GetObject
			replicationgroup		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchStopUpdateAction	クラスターセットで ElastiCache サービス更新の実行を停止する許可を付与。	Write	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
CompleteMigration	Amazon EC2 でホストされている Redis から ElastiCache へのデータのオンライン移行を完了する許可を付与。	書き込み	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
Connect	指定された ElastiCache ユーザーとして ElastiCache レプリケーショングループまたは ElastiCache サーバーレスキャッシュに接続するためのアクセス許可を付与	書き込み	user*		
			replicationgroup		
			serverlesscache		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CopyServerlessCacheSnapshot	既存のサーバーレスキャッシュスナップショットのコピーを作成するためのアクセス許可を付与	書き込み	serverlessscachesnapshot*	aws:ResourceTag/${TagKey} elasticache:KmsKeyId	elasticache:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CopySnapshot	既存のスナップショットのコピーを作成する許可を付与。	Write	snapshot*		elasticache:AddTagsToResource s3:DeleteObject s3:GetBucketAcl s3:PutObject

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:KmsKeyId	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateCacheCluster	キャッシュクラスターを作成する許可を付与。	Write	parametergroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs elasticache:AddTagsToResource s3:GetObject

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			cluster	aws:RequestTag/${TagKey} aws:TagKeys elasticache:CacheNodeType elasticache:EngineVersion elasticache:EngineType elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheP	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				arameterGroupName	
			replicationgroup	elasticache:CacheNodeType elasticache:EngineVersion elasticache:EngineType elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			securitygroup		
			snapshot		
			subnetgroup		
				aws:ResourceTag/${TagKey}	
CreateCacheParameterGroup	パラメータグループを作成する許可を付与。	Write	parametergroup*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:CacheParameterGroupName	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateCacheSecurityGroup	キャッシュセキュリティグループを作成する許可を付与。	Write	securitygroup*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateCacheSubnetGroup	キャッシュサブネットグループを作成する許可を付与。	Write	subnetgroup*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateGlobalReplicationGroup	グローバルレプリケーショングループを作成する許可を付与。	Write	globalreplicationgroup*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			replicationgroup*		
				aws:ResourceTag/${TagKey}	
CreateReplicationGroup	レプリケーショングループを作成する許可を付与。	書き込み	parametergroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs elasticache:AddTagsToResource s3:GetObject

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			cluster		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			globalreplicationgroup	elasticache:NumNodeGroups elasticache:CacheNodeType elasticache:ReplicasPerNodeGroup elasticache:EngineVersion elasticache:EngineType elasticache:AtRestEncryptionEnabled elasticache:TransitEncryptionEnabled elasticache:AutomaticFailoverEnabled	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				elasticache:MultiAZEnabled elasticache:ClusterModeEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:KmsKeyId elasticache:CacheParameterGroupName	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			replicationgroup	aws:RequestTag/${TagKey} aws:TagKeys elasticache:NumNodeGroups elasticache:CacheNodeType elasticache:ReplicasPerNodeGroup elasticache:EngineVersion elasticache:EngineType elasticache:AtRestEncryptionEnabled elasticache:Transi	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				tEncryptionEnabled elasticache:AutomaticFailoverEnabled elasticache:MultiAZEnabled elasticache:ClusterModeEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:KmsKeyId elasticache:CacheParameterGroupName	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			securitygroup		
			snapshot		
			subnetgroup		
			usergroup		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateServerlessCache	サーバーレスキャッシュを作成するためのアクセス許可を付与	書き込み	serverlesscache*	aws:ResourceTag/${TagKey} elasticache:EngineType elasticache:EngineVersion elasticache:SnapshotRetentionLimit elasticache:KmsKeyId elasticache:MinimumDataStorage elasticache:MaximumDataStorage elasticache:DataStorageUnit	ec2:CreateTags ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeTags ec2:DescribeVpcEndpoints ec2:DescribeVpcs elasticache:AddTagsToResource

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				elasticache:MinimumECPUPerSecond elasticache:MaximumECPUPerSecond	s3:GetObject
			serverlesscachesnapshot	aws:ResourceTag/${TagKey}	
			snapshot	aws:ResourceTag/${TagKey}	
			usergroup	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateServerlessCacheSnapshot	特定の時点でサーバーレスキャッシュのコピーを作成するためのアクセス許可を付与	書き込み	serverlesscache*	aws:ResourceTag/${TagKey}	elasticache:AddTagsToResource

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			serverlessscachesnapshot*	aws:ResourceTag/${TagKey} elasticache:KmsKeyId	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	特定の時点で Redis クラスター全体のコピーを作成する許可を付与。	書き込み	snapshot*	aws:RequestTag/${TagKey} aws:TagKeys elasticache:KmsKeyId	elasticache:AddTagsToResource s3:DeleteObject s3:GetBucketAcl s3:PutObject
			cluster		
			replicationgroup		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
CreateUser	Redis のユーザーを作成する許可を付与します。ユーザーは Redis 6.0 以降でサポートされています	書き込み	user*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:UserAuthenticationMode	
CreateUserGroup	Redis のユーザーグループを作成する許可を付与します。グループは Redis 6.0 以降でサポートされています	書き込み	user*		elasticache:AddTagsToResource

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			usergroup*	aws:RequestTag/${TagKey} aws:TagKeys	
				aws:ResourceTag/${TagKey}	
DecreaseNodeGroupsInGlobalReplicationGroup	グローバルレプリケーショングループ内のノードグループの数を減らすアクセス許可を付与します。	Write	globalreplicationgroup*		
				elasticache:NumNodeGroups	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DecreaseReplicaCount	Redis (クラスターモード無効化) レプリケーショングループのレプリカ数、または Redis (クラスターモード有効化) レプリケーショングループの 1 つ以上のノードグループ (シャード) のレプリカノードの数を減らすアクセス許可を付与します。	Write	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} elasticache:ReplicasPerNodeGroup	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteCacheCluster	以前にプロビジョニングされたクラスターを削除する許可を付与	Write	cluster*	aws:ResourceTag/${TagKey}	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			snapshot		
DeleteCacheParameterGroup	指定されたキャッシュパラメータグループを削除する許可を付与。	Write	parametergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteCacheSecurityGroup	キャッシュセキュリティグループを削除する許可を付与。	Write	securitygroup*		
				aws:ResourceTag/${TagKey}	
DeleteCacheSubnetGroup	キャッシュサブネットグループを削除する許可を付与。	Write	subnetgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
DeleteGlobalReplicationGroup	既存のグローバルレプリケーショングループを削除する許可を付与。	Write	globalreplicationgroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteReplicationGroup	既存のレプリケーショングループを削除する許可を付与。	書き込み	replicationgroup*	aws:ResourceTag/${TagKey}	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			snapshot		
DeleteServerlessCache	サーバーレスキャッシュを削除するためのアクセス許可を付与	書き込み	serverlesscache*	aws:ResourceTag/${TagKey}	ec2:DescribeTags
			serverlesscachesnapshot		
DeleteServerlessCacheSnapshot	サーバーレスキャッシュスナップショットを削除するためのアクセス許可を付与	書き込み	serverlesscachesnapshot*	aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteSnapshot	既存のスナップショットを削除する許可を付与。	Write	snapshot*		
				aws:ResourceTag/${TagKey}	
DeleteUser	既存のユーザーを削除して、そのユーザーを割り当てられたすべてのユーザーグループとレプリケーショングループから削除する許可を付与。	Write	user*		
				aws:ResourceTag/${TagKey}	
DeleteUserGroup	既存のユーザーグループを削除する許可を付与。	Write	usergroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheClusters	プロビジョンドキャッシュクラスターに関する情報を一覧表示する許可を付与。	リスト	cluster*		
				aws:ResourceTag/${TagKey}	
DescribeCacheEngineVersions	利用可能なキャッシュエンジンとそのバージョンをリストするためのアクセス許可を付与する	リスト			
DescribeCacheParameterGroups	キャッシュパラメータグループの説明を一覧表示する許可を付与。	リスト	parametergroup*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
DescribeCacheParameters	特定のキャッシュパラメータグループの詳細なパラメータリストを取得する許可を付与。	リスト	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheSecurityGroups	キャッシュセキュリティグループの説明を一覧表示する許可を付与。	リスト	securitygroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheSubnetGroups	キャッシュサブネットグループの説明を一覧表示する許可を付与。	リスト	subnetgroup*		
				aws:ResourceTag/${TagKey}	
DescribeEngineDefaultParameters	指定されたキャッシュエンジンのデフォルトのエンジンおよびシステムパラメータ情報を取得する許可を付与。	リスト			
DescribeEvents	クラスター、キャッシュセキュリティグループ、キャッシュパラメータグループに関連するイベントを一覧表示する許可を付与。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeGlobalReplicationGroups	グローバルレプリケーショングループに関する情報を一覧表示する許可を付与。	リスト	globalreplicationgroup*		
DescribeReplicationGroups	プロビジョンドレプリケーショングループに関する情報を一覧表示する許可を付与。	リスト	replicationgroup*		
				aws:ResourceTag/${TagKey}	
DescribeReservedCacheNodes	購入したリザーブドキャッシュノードに関する情報を一覧表示する許可を付与。	リスト	reserved-instance*		
				aws:ResourceTag/${TagKey}	
DescribeReservedCacheNodesOfferings	利用可能なリザーブドキャッシュノードを一覧表示する許可を付与。	リスト			
DescribeServerlessCacheSnapshots	サーバーレスキャッシュスナップショットに関する情報を一覧表示するためのアクセス許可を付与	リスト	serverlesscachesnapshot*	aws:ResourceTag/${TagKey}	
			serverlesscache	aws:ResourceTag/${TagKey}	
DescribeServerlessCaches	サーバーレスキャッシュを一覧表示するためのアクセス許可を付与	リスト	serverlesscache*	aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeServiceUpdates	サービス更新の詳細を一覧表示する許可を付与。	リスト			
DescribeSnapshots	クラスターまたはレプリケーショングループのスナップショットに関する情報を一覧表示する許可を付与。	リスト	snapshot*		
				aws:ResourceTag/${TagKey}	
DescribeUpdateActions	クラスターまたはレプリケーショングループのセットの更新アクションの詳細を一覧表示する許可を付与。	リスト	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
DescribeUserGroups	Redis ユーザーグループに関する情報を一覧表示する許可を付与。	リスト	usergroup*		
				aws:ResourceTag/${TagKey}	
DescribeUsers	Redis ユーザーに関する情報を一覧表示する許可を付与。	リスト	user*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisassociateGlobalReplicationGroup	グローバルレプリケーショングループからセカンダリレプリケーショングループを削除する許可を付与。	書き込み	globalreplicationgroup*		
ExportServerlessCacheSnapshot	特定の時点でのサーバーレスキャッシュのコピーを S3 バケットにエクスポートするためのアクセス許可を付与	書き込み	serverlesscachesnapshot*	aws:ResourceTag/${TagKey}	s3:DeleteObject s3:ListAllMyBuckets s3:PutObject
FailoverGlobalReplicationGroup	グローバルレプリケーショングループで選択したセカンダリリージョンにプライマリリージョンをフェイルオーバーする許可を付与。	Write	globalreplicationgroup*		
IncreaseNodeGroupsInGlobalReplicationGroup	グローバルレプリケーショングループのノードグループ数を増やすアクセス許可を付与します。	Write	globalreplicationgroup*		
				elasticache:NumNodeGroups	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
IncreaseReplicaCount	Redis (クラスターモード無効化) レプリケーショングループのレプリカ数、または Redis (クラスターモード有効化) レプリケーショングループの 1 つ以上のノードグループ (シャード) のレプリカノードの数を増やすアクセス許可を付与します。	書き込み	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} elasticache:ReplicasPerNodeGroup	
InterruptClusterAzPower [アクセス許可のみ]	ElastiCache リソースの AZ 間電源遮断をテストするためのアクセス許可を付与	書き込み	replicationgroup*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListAllowedNodeTypeModifications	特定の Redis クラスターまたはレプリケーショングループのスケーリングに使用できるノードタイプを一覧表示する許可を付与。	リスト	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	ElastiCache リソースのタグを一覧表示する許可を付与。	Read	cluster		
			parametergroup		
			replicationgroup		
			reserved-instance		
			securitygroup		
			serverlesscache		
			serverlesscachesnapshot		
			snapshot		
			subnetgroup		
			user		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			usergroup		
				aws:ResourceTag/${TagKey}	
ModifyCacheCluster	クラスターの設定を変更する許可を付与。	Write	cluster*	elasticache:CacheNodeType elasticache:EngineVersion elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName	
			parametergroup		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			securitygroup		
				aws:ResourceTag/${TagKey}	
ModifyCacheParameterGroup	キャッシュパラメータグループのパラメータを変更する許可を付与。	Write	parametergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	
ModifyCacheSubnetGroup	既存のキャッシュサブネットグループを変更する許可を付与。	Write	subnetgroup*		
				aws:ResourceTag/${TagKey}	
ModifyGlobalReplicationGroup	グローバルレプリケーショングループの設定を変更する許可を付与。	Write	globalreplicationgroup*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				elasticache:CacheNodeType elasticache:EngineVersion elasticache:AutomaticFailoverEnabled	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ModifyReplicationGroup	レプリケーショングループの設定を変更する許可を付与。	Write	replicationgroup*	elasticache:CacheNodeType elasticache:EngineVersion elasticache:AutomaticFailoverEnabled elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName elasticache:TransitEncrypti	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				onEnabled elasticache:ClusterModeEnabled	
			parametergroup		
			securitygroup		
			usergroup		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ModifyReplicationGroupShardConfiguration	レプリケーショングループの既存のシャード間でシャードの追加、シャードの削除、またはキースペースの再調整を行うアクセス許可を付与します。	書き込み	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} elasticache:NumNodeGroups	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ModifyServerlessCache	サーバーレスキャッシュのパラメータを変更するためのアクセス許可を付与	書き込み	serverlesscache*	aws:ResourceTag/${TagKey} elasticache:EngineVersion elasticache:SnapshotRetentionLimit elasticache:MinimumDataStorage elasticache:MaximumDataStorage elasticache:DataStorageUnit elasticache:MinimumECPUPerSecond elasticache:Maximu	ec2:DescribeSecurityGroups ec2:DescribeTags

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				mECPUPerSecond	
			usergroup	aws:ResourceTag/${TagKey}	
ModifyUser	Redis ユーザーのパスワードまたはアクセス文字列を変更する許可を付与。	Write	user*		
				aws:ResourceTag/${TagKey} elasticache:UserAuthenticationMode	
ModifyUserGroup	ユーザーグループに属するユーザーのリストを変更する許可を付与。	Write	user*		
			usergroup*		
				aws:ResourceTag/${TagKey}	
PurchaseReservedCacheNodesOffering	リザーブドキャッシュノードの提供を購入する許可を付与。	Write	reserved-instance*		elasticache:AddTagsToResource

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
RebalanceSlotsInGlobalReplicationGroup	スロットを再配布し、グローバルレプリケーショングループ内の既存のシャード間で統一されたキーを配布することを保証するために、キースペースリバランス操作を実行する許可を付与。	Write	globalreplicationgroup*		
RebootCacheCluster	プロビジョンドキャッシュクラスターまたはレプリケーショングループ内のキャッシュノードの一部またはすべてを再起動する許可を付与 (クラスターモードは無効化)。	Write	cluster*		
				aws:ResourceTag/${TagKey}	
RemoveTagsFromResource	ElastiCache リソースからタグを削除する許可を付与。	タグ付け	cluster		
			parametergroup		
			replicationgroup		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			reserved-instance		
			securitygroup		
			serverlesscache		
			serverlesscachesnapshot		
			snapshot		
			subnetgroup		
			user		
			usergroup		
				aws:TagKeys aws:ResourceTag/${TagKey}	
ResetCacheParameterGroup	キャッシュパラメータグループのパラメータをデフォルト値に戻すためのアクセス許可を付与します。	Write	parametergroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	
RevokeCacheSecurityGroupIngress	ElastiCache セキュリティグループから EC2 セキュリティグループの進入を削除する許可を付与。	Write	securitygroup*		
				aws:ResourceTag/${TagKey}	
StartMigration	Amazon EC2 でホストされている Redis から ElastiCache for Redis へのデータの移行を開始する許可を付与。	Write	replicationgroup*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
TestFailover	レプリケーショングループ内の指定されたノードグループで自動フェイルオーバーをテストする許可を付与。	書き込み	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
TestMigration	Amazon EC2 でホストされている Redis から ElastiCache for Redis へのデータの移行をテストする許可を付与	書き込み	replicationgroup*		
				aws:ResourceTag/${TagKey}	

Amazon ElastiCache で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
parameter group	arn:${Partition}:elasticache:${Region}:${Account}:parametergroup:${CacheParameterGroupName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:CacheParameterGroupName
securitygroup	arn:${Partition}:elasticache:${Region}:${Account}:securitygroup:${CacheSecurityGroupName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
subnetgroup	arn:${Partition}:elasticache:${Region}:${Account}:subnetgroup:${CacheSubnetGroupName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

リソースタイプ	ARN	条件キー
replicationgroup	arn:${Partition}:elasticache:${Region}:${Account}:replicationgroup:${ReplicationGroupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:AtRestEncryptionEnabled elasticache:AuthTokenEnabled elasticache:AutomaticFailoverEnabled elasticache:CacheNodeType elasticache:CacheParameterGroupName elasticache:ClusterModeEnabled elasticache:EngineType elasticache:EngineVersion elasticache:KmsKeyId elasticache:MultiAZEnabled

リソースタイプ	ARN	条件キー
		elasticache:NumNodeGroups elasticache:ReplicasPerNodeGroup elasticache:SnapshotRetentionLimit elasticache:TransitEncryptionEnabled

リソースタイプ	ARN	条件キー
cluster	arn:${Partition}:elasticache:${Region}:${Account}:cluster:${CacheClusterId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:AuthTokenEnabled elasticache:CacheNodeType elasticache:CacheParameterGroupName elasticache:EngineType elasticache:EngineVersion elasticache:MultiAZEnabled elasticache:SnapshotRetentionLimit
reserved-instance	arn:${Partition}:elasticache:${Region}:${Account}:reserved-instance:${ReservedCacheNodeId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

リソースタイプ	ARN	条件キー
snapshot	arn:${Partition}:elasticache:${Region}:${Account}:snapshot:${SnapshotName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:KmsKeyId

リソースタイプ	ARN	条件キー
globalreplicationgroup	arn:${Partition}:elasticache::${Account}:globalreplicationgroup:${GlobalReplicationGroupId}	elasticache:AtRestEncryptionEnabled elasticache:AuthTokenEnabled elasticache:AutomaticFailoverEnabled elasticache:CacheNodeType elasticache:CacheParameterGroupName elasticache:ClusterModeEnabled elasticache:EngineType elasticache:EngineVersion elasticache:KmsKeyId elasticache:MultiAZEnabled elasticache:NumNodeGroups elasticache:ReplicasPerNodeGroup elasticache:SnapshotRetentionLimit

リソースタイプ	ARN	条件キー
		elasticache:TransitEncryptionEnabled
user	arn:${Partition}:elasticache:${Region}:${Account}:user:${UserId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:UserAuthenticationMode
usergroup	arn:${Partition}:elasticache:${Region}:${Account}:usergroup:${UserGroupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

リソースタイプ	ARN	条件キー
serverlesscache	arn:${Partition}:elasticache:${Region}:${Account}:serverlesscache:${ServerlessCacheName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:DataStorageUnit elasticache:EngineType elasticache:EngineVersion elasticache:KmsKeyId elasticache:MaximumDataStorage elasticache:MaximumECPUPerSecond elasticache:MinimumDataStorage elasticache:MinimumECPUPerSecond elasticache:SnapshotRetentionLimit

リソースタイプ	ARN	条件キー
serverlesscachesnapshot	arn:${Partition}:elasticache:${Region}:${Account}:serverlesscachesnapshot:${ServerlessCacheSnapshotName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:KmsKeyId

Amazon ElastiCache の条件キー

Amazon ElastiCache では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

> **Note**
>
> 文字列型の条件キーを使用して条件要素を構築するには、大文字と小文字を区別しない条件演算子 StringEqualsIgnoreCase または StringNotEqualsIgnoreCase を使用して、キーを文字列値と比較します。
> IAM ポリシーの条件で ElastiCache へのアクセスを制御する方法については、Amazon ElastiCache ユーザーガイドの「ElastiCache キー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします。	文字列

条件キー	説明	タイプ
aws:ResourceTag/${TagKey}	リソースに関連付けられているタグに基づいてアクションをフィルタリングします。	文字列
aws:TagKeys	リクエストで渡されたタグキーに基づいてアクションをフィルタリングします。	ArrayOfString
elasticache:AtRestEncryptionEnabled	リクエストに存在する AtRestEncryptionEnabled パラメータ、またはパラメータが存在しない場合はデフォルト false 値によって、アクセスをフィルタリングします。	Bool
elasticache:AuthTokenEnabled	リクエスト内の空でない AuthToken パラメータが存在することでアクセスをフィルタリングします。	Bool
elasticache:AutomaticFailoverEnabled	リクエスト内の AutomaticFailoverEnabled パラメータでアクセスをフィルタリングします。	Bool
elasticache:CacheNodeType	リクエストに存在する cacheNodeType パラメータでアクセスをフィルタリングします。このキーを使用して、クラスターの作成またはスケーリング操作に使用できるキャッシュノードタイプを制限できます。	String
elasticache:CacheParameterGroupName	リクエスト内の CacheParameterGroupName パラメータでアクセスをフィルタリングします	String
elasticache:ClusterModeEnabled	リクエストに存在するクラスターモードのパラメータでアクセスをフィルタリングします。単一ノードグループ (シャード) 作成のデフォルト値は false です。	Bool

条件キー	説明	タイプ
elasticache:DataStorageUnit	CreateServerlessCache および ModifyServerlessCache リクエスト内の CacheUsageLimits.DataStorage.Unit パラメータでアクセスをフィルタリングします	String
elasticache:EngineType	作成リクエストに存在するエンジンタイプでアクセスをフィルタリングします。レプリケーショングループの作成には、パラメータが存在しない場合、デフォルトのエンジン「redis」がキーとして使用されます	String
elasticache:EngineVersion	作成リクエストまたはクラスター変更リクエストに存在する engineVersion パラメータでアクセスをフィルタリングします。	String
elasticache:KmsKeyId	KMS キーのキー ID でアクセスをフィルタリングします	String
elasticache:MaximumDataStorage	CreateServerlessCache および ModifyServerlessCache リクエスト内の CacheUsageLimits.DataStorage.Maximum パラメータでアクセスをフィルタリングします	数値
elasticache:MaximumECPUPerSecond	CreateServerlessCache および ModifyServerlessCache リクエスト内の CacheUsageLimits.ECPUPerSecond.Maximum パラメータでアクセスをフィルタリングします	数値
elasticache:MinimumDataStorage	CreateServerlessCache および ModifyServerlessCache ModifyServerlessCache リクエストの CacheUsageLimits.DataStorage.Minimum パラメータでアクセスをフィルタリングします	数値
elasticache:MinimumECPUPerSecond	CreateServerlessCache および ModifyServerlessCache リクエストの CacheUsageLimits.ECPUPerSecond.Minimum パラメータでアクセスをフィルタリングします ModifyServerlessCache	数値

条件キー	説明	タイプ
elasticache:MultiAZEnabled	AzMode パラメータ、MultiAZEnabled パラメータ、またはクラスターやレプリケーショングループを配置できるアベイラビリティーゾーンの数でアクセスをフィルタリングします。	Bool
elasticache:NumNodeGroups	リクエストで指定された NumNodeGroups または NodeGroupCount パラメータでアクセスをフィルタリングします。このキーを使用して、作成またはスケーリング操作後にクラスターが持つことができるノードグループ (シャード) の数を制限できます。	数値
elasticache:ReplicasPerNodeGroup	作成またはスケーリングリクエストで指定されたノードグループ (シャード) ごとのレプリカの数でアクセスをフィルタリングします。	数値
elasticache:SnapshotRetentionLimit	リクエスト内の SnapshotRetentionLimit パラメータでアクセスをフィルタリングします。	数値
elasticache:TransitEncryptionEnabled	リクエストに存在する TransitEncryptionEnabled パラメータでアクセスをフィルタリングします。レプリケーショングループの作成には、パラメータが存在しない場合、デフォルト値「false」がキーとして使用されます	Bool
elasticache:UserAuthenticationMode	リクエスト内の UserAuthenticationMode パラメータでアクセスをフィルタリングします	String

AWS Elemental アプライアンスとソフトウェアのアクション、リソース、および条件キー

AWS Elemental Appliances and Software (サービスプレフィックス: `elemental-appliances-software`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Elemental Appliances and Software で定義されるアクション
- AWS Elemental Appliances and Software で定義されるリソースタイプ
- AWS Elemental Appliances and Software の条件キー

AWS Elemental Appliances and Software で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CompleteUpload [アクセス許可のみ]	見積もりまたは注文の添付ファイルのアップロードを完了する許可を付与	書き込み			
CreateOrderV1 [アクセス許可のみ]	順序を作成する許可を付与します。	書き込み			
CreateQuote [アクセス許可のみ]	見積りを作成するアクセス許可を付与	書き込み	quote*		
GetAvsCorrectAddress [アクセス許可のみ]	住所を認証する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetBillingAddresses [許可のみ]	AWS アカウントの請求先住所を一覧表示するアクセス許可を付与します	読み取り			
GetDeliveryAddressesV2 [許可のみ]	AWS アカウントの配信アドレスを一覧表示するアクセス許可を付与します	読み取り			
GetOrder [許可のみ]	注文を記述する許可を付与	読み取り			
GetOrdersV2 [許可のみ]	AWS アカウント内の注文を一覧表示するアクセス許可を付与します	読み取り			
GetQuote [許可のみ]	見積りを記述するアクセス許可を付与	読み込み	quote*		
GetTaxes [許可のみ]	注文にかかる税金を計算する許可を付与	読み取り			
ListQuotes [許可のみ]	AWS アカウントの引用符を一覧表示するアクセス許可を付与します	リスト			
StartUpload [許可のみ]	見積もりまたは注文の添付ファイルのアップロードを開始する許可を付与	書き込み			
SubmitOrderV1 [アクセス許可のみ]	注文を送信する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateQuote [アクセス許可のみ]	見積りを変更するアクセス許可を付与	書き込み	quote*		

AWS Elemental Appliances and Software で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
quote	arn:${Partition}:elemental-appliances-software:${Region}:${Account}:quote/${ResourceId}	

AWS Elemental Appliances and Software の条件キー

Elemental Appliances and Software には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Elemental Appliances and Software Activation Service のアクション、リソース、および条件キー

AWS Elemental Appliances and Software Activation Service (サービスプレフィックス: elemental-activations) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Elemental Appliances and Software Activation Service で定義されるアクション
- AWS Elemental Appliances and Software Activation Service で定義されるリソースタイプ
- AWS Elemental Appliances and Software Activation Service の条件キー

AWS Elemental Appliances and Software Activation Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CompleteAccountRegistration [アクセス許可のみ]	Elemental Appliances and Software Purchases AWS のユーザーアカウントを登録するプロセスを完了するアクセス許可を付与します	書き込み			
CompleteFileUpload [アクセス許可のみ]	Elemental Appliances and Software Purchases AWS のソフトウェアファイルをアップロードするプロセスを完了する許可を付与	書き込み			
ConfirmAccount [アクセス許可のみ]	アセットの所有権を確認する許可を付与する	書き込み			
DownloadKickstart [アク	AWS Elemental Appliances and Software 購入のキックス	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
セス許可のみ]	タートファイルをダウンロードする許可を付与				
DownloadSoftware [許可のみ]	Elemental Appliances and Software Purchases AWS のソフトウェアファイルをダウンロードする許可を付与	読み取り			
GenerateLicense [許可のみ]	AWS Elemental Appliances and Software 購入用のソフトウェアライセンスを生成するアクセス許可を付与します	書き込み			
GenerateLicenses [アクセス許可のみ]	Elemental Appliances and Software Purchases AWS のソフトウェアライセンスを生成するアクセス許可を付与します	書き込み			
GetArtifactGroupSoftwareVersions [アクセス許可のみ]	アーティファクトグループのソフトウェアバージョンを記述する許可を付与する	読み取り			
GetAsset [許可のみ]	アセットを記述する許可を付与	読み取り			
GetAssets [許可のみ]	リクエスト元のアカウントに関連付けられたアセットを記述する許可を付与する	読み取り			
GetProductAdvisories [許可のみ]	すべての製品アドバイザーを取得する許可を付与する	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetSoftwareVersions [許可のみ]	利用可能なソフトウェアバージョンを記述する許可を付与する	読み取り			
StartFileUpload [許可のみ]	Elemental Appliances and Software Purchases AWS のソフトウェアファイルのアップロードプロセスを開始するアクセス許可を付与します	書き込み			

AWS Elemental Appliances and Software Activation Service で定義されるリソースタイプ

AWS Elemental Appliances and Software Activation Service は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Elemental Appliances and Software Activation Service へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Elemental Appliances and Software Activation Service の条件キー

Elemental Activations には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Elemental MediaConnect のアクション、リソース、および条件キー

AWS Elemental MediaConnect (サービスプレフィックス: `mediaconnect`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Elemental MediaConnect で定義されるアクション
- AWS Elemental MediaConnect で定義されるリソースタイプ
- AWS Elemental MediaConnect の条件キー

AWS Elemental MediaConnect で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddBridgeOutputs	出力を既存のブリッジに追加するアクセス許可を付与します	書き込み	Bridge*		
AddBridgeSources	ソースを既存のブリッジに追加するアクセス許可を付与します	書き込み	Bridge*		
AddFlowMediaStreams	メディアストリームをフローに追加する許可を付与	Write			
AddFlowOutputs	出力をフローに追加する許可を付与	Write			
AddFlowSources	ソースをフローに追加する許可を付与	Write			
AddFlowVpcInterfaces	VPC インターフェイスをフローに追加する許可を付与	書き込み			
CreateBridge	ブリッジを作成するアクセス許可を付与します	書き込み			
CreateFlow	フローを作成する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateGateway	ゲートウェイを作成するアクセス許可を付与します	書き込み			
DeleteBridge	ブリッジを削除するアクセス許可を付与します	書き込み	Bridge*		
DeleteFlow	トピックを削除する許可を付与	書き込み			
DeleteGateway	ゲートウェイを削除するアクセス許可を付与します	書き込み	Gateway*		
DeregisterGatewayInstance	ゲートウェイインスタンスを登録解除するアクセス許可を付与します	書き込み	GatewayInstance*		
DescribeBridge	ブリッジの詳細を表示するアクセス許可を付与します	読み取り	Bridge*		
DescribeFlow	フローの ARN、名前、アベイラビリティーゾーンなどのフローの詳細、およびソース、出力、資格についての詳細を表示する許可を付与	読み取り			
DescribeFlowSourceMetadata	フローのソーストランスポートストリームとプログラムに関する情報を表示する許可を付与する	読み取り			
DescribeFlowSourceThumbnail	フローのソースサムネイルを表示する許可を付与する	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeGateway	ゲートウェイの ARN、名前、CIDR ブロックなどのゲートウェイの詳細、およびネットワークについての詳細を表示するアクセス許可を付与します	読み取り	Gateway*		
DescribeGatewayInstance	ゲートウェイインスタンスの詳細を表示するアクセス許可を付与します	読み取り	GatewayInstance*		
DescribeOffering	サービスの詳細を表示する許可を付与	Read			
DescribeReservation	予約の詳細を表示する許可を付与	読み取り			
DiscoverGatewayPollEndpoint	ゲートウェイポーリングエンドポイントを検出するアクセス許可を付与します	書き込み			
GrantFlowEntitlements	フローで資格を与えるアクセス許可を付与	書き込み			
ListBridges	このアカウントとオプションで指定された Arn に関連付けられているブリッジのリストを表示するアクセス許可を付与します	リスト	Bridge*		
ListEntitlements	アカウントに与えられたすべての資格のリストを表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListFlows	このアカウントに関連付けられているフローのリストを表示する許可を付与	リスト			
ListGatewayInstances	このゲートウェイに関連付けられているインスタンスのリストを表示するアクセス許可を付与します	リスト	GatewayInstance*		
ListGateways	このアカウントに関連付けられているゲートウェイのリストを表示するアクセス許可を付与します	リスト			
ListOfferings	現在の のアカウントで利用可能なすべてのサービスのリストを表示するアクセス許可を付与します AWS リージョン	リスト			
ListReservations	現在の のアカウントによって購入されたすべての予約のリストを表示するアクセス許可を付与します AWS リージョン	リスト			
ListTagsForResource	リソースに関連付けられたすべてのタグのリストを表示する許可を付与	読み取り			
PollGateway	ゲートウェイをポーリングするアクセス許可を付与します	書き込み			
PurchaseOffering	サービスを購入する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RemoveBridgeOutput	既存のブリッジの出力を削除するアクセス許可を付与します	書き込み	Bridge*		
RemoveBridgeSource	既存のブリッジのソースを削除するアクセス許可を付与します	書き込み	Bridge*		
RemoveFlowMediaStream	フローからソースを削除する許可を付与	Write			
RemoveFlowOutput	フローから出力を削除する許可を付与	Write			
RemoveFlowSource	フローからソースを削除する許可を付与	Write			
RemoveFlowVpcInterface	フローから VPC インターフェイスを削除する許可を付与	Write			
RevokeFlowEntitlement	フローで資格を取り消すアクセス許可を付与	Write			
StartFlow	フローを開始する許可を付与	Write			
StopFlow	フローを停止する許可を付与	書き込み			
SubmitGatewayStateChange	ゲートウェイの状態変更を送信するアクセス許可を付与します	書き込み			
TagResource	タグをリソースに関連付けるアクセス許可を付与	タグ付け			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UntagResource	リソースからタグを削除する許可を付与	Tagging			
UpdateBridge	ブリッジを更新するアクセス許可を付与します	書き込み	Bridge*		
UpdateBridgeOutput	既存のブリッジの出力を更新するアクセス許可を付与します	書き込み	Bridge*		
UpdateBridgeSource	既存のブリッジのソースを更新するアクセス許可を付与します	書き込み	Bridge*		
UpdateBridgeState	既存のブリッジの状態を更新するアクセス許可を付与します	書き込み	Bridge*		
UpdateFlow	フローを更新する許可を付与	Write			
UpdateFlowEntitlement	フローに関する資格を更新する許可を付与	Writ			
UpdateFlowMediaStream	フローに関する資格を更新する許可を付与	Write			
UpdateFlowOutput	フローで出力を更新する許可を付与	Write			
UpdateFlowSource	フローでソースを更新する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateGatewayInstance	既存のゲートウェイインスタンスの設定を更新するアクセス許可を付与	書き込み	GatewayInstance*		

AWS Elemental MediaConnect で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Entitlement	arn:${Partition}:mediaconnect:${Region}:${Account}:entitlement:${FlowId}:${EntitlementName}	
Flow	arn:${Partition}:mediaconnect:${Region}:${Account}:flow:${FlowId}:${FlowName}	
Output	arn:${Partition}:mediaconnect:${Region}:${Account}:output:${OutputId}:${OutputName}	
Source	arn:${Partition}:mediaconnect:${Region}:${Account}:source:${SourceId}:${SourceName}	

リソースタイプ	ARN	条件キー
Gateway	arn:${Partition}:mediaconnect:${Region}:${Account}:gateway:${GatewayId}:${GatewayName}	
Bridge	arn:${Partition}:mediaconnect:${Region}:${Account}:bridge:${FlowId}:${FlowName}	
GatewayInstance	arn:${Partition}:mediaconnect:${Region}:${Account}:gateway:${GatewayId}:${GatewayName}:instance:${InstanceId}	

AWS Elemental MediaConnect の条件キー

MediaConnect には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Elemental MediaConvert のアクション、リソース、および条件キー

AWS Elemental MediaConvert (サービスプレフィックス: mediaconvert) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Elemental MediaConvert で定義されるアクション

- AWS Elemental MediaConvert で定義されるリソースタイプ
- AWS Elemental MediaConvert の条件キー

AWS Elemental MediaConvert で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
Associate Certificate	AWS Certificate Manager (ACM) Amazon リソースネーム (ARN) を AWS Elemental MediaConvert に関連付けるアクセス許可を付与します	書き込み			
CancelJob	キューで待機している AWS Elemental MediaConvert ジョブをキャンセルするアクセス許可を付与します	書き込み	Job*		
CreateJob	Elemental MediaConvert AWS ジョブを作成して送信するアクセス許可を付与します	書き込み	JobTemplate		
			Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys mediaconvert:HttpInputsAllowed	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				mediaconvert:HttpsInputsAllowed mediaconvert:S3InputsAllowed	
CreateJobTemplate	Elemental MediaConvert AWS カスタムジョブテンプレートを作成するアクセス許可を付与します	書き込み	Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePreset	Elemental MediaConvert AWS カスタム出力プリセットを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateQueue	Elemental MediaConvert AWS ジョブキューを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteJobTemplate	Elemental MediaConvert AWS カスタムジョブテンプレートを削除するアクセス許可を付与します	書き込み	JobTemplate*		
DeletePolicy	Elemental MediaConvert AWS ポリシーを削除するアクセス許可を付与します	書き込み			
DeletePreset	Elemental MediaConvert AWS カスタム出力プリセットを削除する許可を付与	書き込み	Preset*		
DeleteQueue	Elemental MediaConvert AWS ジョブキューを削除するアクセス許可を付与します	書き込み	Queue*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeEndpoints	アカウント固有のエンドポイントのリクエストを送信して、Elemental MediaConvert AWS サービスをサブスクライブするアクセス許可を付与します。すべてのトランスコーディングリクエストは、サービスが返すエンドポイントに送信される必要があります。	リスト			
DisassociateCertificate	AWS Certificate Manager (ACM) 証明書の Amazon リソースネーム (ARN) と AWS Elemental MediaConvert リソース間の関連付けを削除するアクセス許可を付与します	書き込み			
GetJob	Elemental MediaConvert AWS ジョブを取得する許可を付与	読み取り	Job*		
GetJobTemplate	Elemental MediaConvert AWS ジョブテンプレートを取得する許可を付与	読み取り	JobTemplate*		
GetPolicy	Elemental MediaConvert AWS ポリシーを取得する許可を付与	読み取り			
GetPreset	Elemental MediaConvert AWS 出力プリセットを取得する許可を付与	読み取り	Preset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetQueue	Elemental MediaConvert AWS ジョブキューを取得する許可を付与	読み取り	Queue*		
ListJobTemplates	Elemental MediaConvert AWS ジョブテンプレートを一覧表示する許可を付与	リスト			
ListJobs	Elemental MediaConvert AWS ジョブを一覧表示する許可を付与	リスト	Queue		
ListPresets	Elemental MediaConvert AWS 出力プリセットを一覧表示する許可を付与	リスト			
ListQueues	Elemental MediaConvert AWS ジョブキューを一覧表示する許可を付与	リスト			
ListTagsForResource	MediaConvert キュー、プリセット、またはジョブテンプレートのタグを取得する許可を付与。	読み取り	Job		
			JobTemplate		
			Preset		
			Queue		
ListVersions	Elemental MediaConvert AWS ジョブエンジンのバージョンを一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
Probe	ファイルを調査するアクセス許可を付与します	読み取り			
PutPolicy	Elemental MediaConvert AWS ポリシーを配置するアクセス許可を付与します	書き込み			
SearchJobs	Elemental MediaConvert AWS ジョブを検索する許可を付与	リスト	Queue		
TagResource	MediaConvert キュー、プリセット、またはジョブテンプレートにタグを追加する許可を付与。	タグ付け	Job		
			JobTemplate		
			Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	MediaConvert キュー、プリセット、またはジョブテンプレートからタグを削除する許可を付与。	Tagging	Job		
			JobTemplate		
			Preset		
			Queue		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
UpdateJobTemplate	Elemental MediaConvert AWS カスタムジョブテンプレートを更新する許可を付与	書き込み	JobTemplate*		
			Preset		
			Queue		
UpdatePreset	Elemental MediaConvert AWS カスタム出力プリセットを更新する許可を付与	書き込み	Preset*		
UpdateQueue	Elemental MediaConvert AWS ジョブキューを更新する許可を付与	書き込み	Queue*		

AWS Elemental MediaConvert で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Job	arn:${Partition}:mediaconvert:${Region}:${Account}:jobs/${JobId}	aws:ResourceTag/${TagKey}
Queue	arn:${Partition}:mediaconvert:${Region}:${Account}:queues/${QueueName}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
Preset	arn:${Partition}:mediaconvert:${Region}:${Account}:presets/${PresetName}	aws:ResourceTag/${TagKey}
JobTemplate	arn:${Partition}:mediaconvert:${Region}:${Account}:jobTemplates/${JobTemplateName}	aws:ResourceTag/${TagKey}
CertificateAssociation	arn:${Partition}:mediaconvert:${Region}:${Account}:certificates/${CertificateArn}	

AWS Elemental MediaConvert の条件キー

AWS Elemental MediaConvert では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString
mediaconvert:HttpInputsAllowed	アカウントに存在する HTTP 入力ポリシーでアクセスをフィルタリングします	Bool

条件キー	説明	タイプ
mediaconvert:HttpsInputsAllowed	アカウントに存在する HTTPS 入力ポリシーでアクセスをフィルタリングします	Bool
mediaconvert:S3InputsAllowed	アカウントに存在する S3 入力ポリシーでアクセスをフィルタリングします	Bool

AWS Elemental MediaLive のアクション、リソース、および条件キー

AWS Elemental MediaLive (サービスプレフィックス: `medialive`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Elemental MediaLive で定義されるアクション
- AWS Elemental MediaLive で定義されるリソースタイプ
- AWS Elemental MediaLive の条件キー

AWS Elemental MediaLive で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptInputDeviceTransfer	入力デバイス転送を受け入れるアクセス許可を付与	書き込み	input-device*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchDelete	チャネル、入力、入力セキュリティグループ、およびマルチプレックスを削除する許可を付与	書き込み			
BatchStart	チャンネルとマルチプレックスを開始する許可を付与	書き込み			
BatchStop	チャンネルとマルチプレックスを停止する許可を付与	書き込み			
BatchUpdateSchedule	チャネルのスケジュールにアクションを追加および削除する許可を付与	書き込み	channel*		
CancelInputDeviceTransfer	入力デバイス転送をキャンセルする許可を付与	書き込み	input-device*		
ClaimDevice	入力デバイスを請求する許可を付与	書き込み	input-device*		
CreateChannel	チャネルを作成する許可を付与	書き込み	channel*		
			input*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateChannelPlacementGroup	クラスターを作成する許可を付与	書き込み	channel-placement-group*		
			cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudWatchAlarmTemplate	Cloudwatch アラームテンプレートを作成する許可を付与する	書き込み	cloudwatch-alarm-template*		
			cloudwatch-alarm-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudWatchAlarmTemplateGroup	Cloudwatch アラームテンプレートグループを作成する許可を付与する	書き込み	cloudwatch-alarm-template-group*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCluster	クラスターを作成する許可を付与	書き込み	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventBridgeRuleTemplate	Eventbridge ルールテンプレートを作成する許可を付与する	書き込み	eventbridge-rule-template*		
			eventbridge-rule-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateEventBridgeRuleTemplateGroup	Eventbridge ルールテンプレートグループを作成する許可を付与する	書き込み	eventbridge-rule-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInput	入力を作成する許可を付与	書き込み	input*		
			input-security-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInputSecurityGroup	入力セキュリティグループを作成する許可を付与	書き込み	input-security-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateMultiplex	マルチプレックスを作成する許可を付与	書き込み	multiplex*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMultiplexProgram	マルチプレックスプログラムを作成する許可を付与	書き込み	multiplex*		
CreateNetwork	ネットワークを作成するアクセス許可を付与	書き込み	network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNode	ノードを作成する許可を付与する	書き込み	cluster*		
			node*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNodeRegistrationScript	ノード登録スクリプトを作成する許可を付与する	書き込み	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreatePartnerInput	パートナーリソースを作成する許可を付与	書き込み	input*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSdiSource	SDI ソースを作成するアクセス許可を付与します	書き込み	sdi-source*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSignalMap	シグナルマップを作成する許可を付与する	書き込み	signal-map*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateTags	チャネル、入力、入力セキュリティグループ、マルチプレックス、予約、ノード、ネットワーク、クラスター、チャネルプレイスメントグループ、シグナルマップ、SDI ソース、テンプレートグループ、テンプレートのタグを作成するアクセス許可を付与します	Tagging	channel		
			channel-placement-group		
			cloudwatch-alarm-template		
			cloudwatch-alarm-template-group		
			cluster		
			eventbridge-rule-template		
			eventbridge-rule-template-group		
			input		
			input-security-group		
			multiplex		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			network		
			node		
			reservation		
			sdi-source		
			signal-map		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChannel	チャネルを削除する許可を付与	書き込み	channel*		
DeleteChannelPlacementGroup	クラスターを削除するためのアクセス許可を付与	書き込み	channel-placement-group*		
DeleteCloudWatchAlarmTemplate	CloudWatch アラームテンプレートを削除する許可を付与する	書き込み	cloudwatch-alarm-template*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteCloudWatchAlarmTemplateGroup	Cloudwatch アラームテンプレートグループを削除する許可を付与する	書き込み	cloudwatch-alarm-template-group*		
DeleteCluster	クラスターを削除するためのアクセス許可を付与	書き込み	cluster*		
DeleteEventBridgeRuleTemplate	Eventbridge ルールテンプレートを削除する許可を付与する	書き込み	eventbridge-rule-template*		
DeleteEventBridgeRuleTemplateGroup	Eventbridge ルールテンプレートグループを削除する許可を付与する	書き込み	eventbridge-rule-template-group*		
DeleteInput	入力を削除する許可を付与	書き込み	input*		
DeleteInputSecurityGroup	入力セキュリティグループを削除する許可を付与	書き込み	input-security-group*		
DeleteMultiplex	マルチプレックスを削除する許可を付与	書き込み	multiplex*		
DeleteMultiplexProgram	マルチプレックスプログラムを削除する許可を付与	書き込み	multiplex*		
DeleteNetwork	ネットワークを削除するアクセス許可を付与	書き込み	network*		
DeleteNode	ノードを削除する許可を付与する	書き込み	node*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteReservation	期限切れの予約を削除する許可を付与	書き込み	reservation*		
DeleteSchedule	チャンネルのすべてのスケジュールアクションを削除する許可を付与	書き込み	channel*		
DeleteSdiSource	SDI ソースを削除するアクセス許可を付与します	書き込み	sdi-source*		
DeleteSignalMap	シグナルマップを削除する許可を付与する	書き込み	signal-map*		
DeleteTags	チャネル、入力、入力セキュリティグループ、マルチプレックス、予約、ノード、クラスター、ネットワーク、チャネルプレイスメントグループ、SDI ソース、シグナルマップ、テンプレートグループ、テンプレートからタグを削除するアクセス許可を付与します	Tagging	channel		
			channel-placement-group		
			cloudwatch-alarm-template		
			cloudwatch-alarm-template-group		
			cluster		
			eventbridge-rule-template		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			eventbridge-rule-template-group		
			input		
			input-security-group		
			multiplex		
			network		
			node		
			reservation		
			sdi-source		
			signal-map		
				aws:TagKeys	
DescribeAccountConfiguration	顧客のアカウント設定を表示する許可を付与	読み取り			
DescribeChannel	チャネルに関する詳細を取得する許可を付与	読み取り	channel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeChannelPlacementGroup	チャネル配置グループを記述する許可を付与する	読み取り	channel-placement-group*		
DescribeCluster	クラスターを詳細表示するためのアクセス許可を付与	読み取り	cluster*		
DescribeInput	入力を記述する許可を付与	読み込み	input*		
DescribeInputDevice	入力デバイスを記述する許可を付与	読み込み	input-device*		
DescribeInputDeviceThumbnail	入力デバイスのサムネイルを記述する許可を付与	読み込み	input-device*		
DescribeInputSecurityGroup	入力セキュリティグループを記述する許可を付与	読み込み	input-security-group*		
DescribeMultiplex	マルチプレックスを記述する許可を付与	読み込み	multiplex*		
DescribeMultiplexProgram	マルチプレックスプログラムを記述する許可を付与	読み取り	multiplex*		
DescribeNetwork	ネットワークを記述する許可を付与する	読み取り	network*		
DescribeNode	ノードを記述する許可を付与する	読み取り	node*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeOffering	予約サービスに関する詳細を取得する許可を付与	読み込み	offering*		
DescribeReservation	予約に関する詳細を取得する許可を付与	読み込み	reservation*		
DescribeSchedule	チャネルでスケジュールされているアクションのリストを表示する許可を付与	読み取り	channel*		
DescribeSdiSource	SDI ソースを記述するアクセス許可を付与します	読み取り	sdi-source*		
DescribeThumbnails	チャンネルのサムネイルを表示する許可を付与	読み取り	channel*		
GetCloudWatchAlarmTemplate	Cloudwatch アラームテンプレートを取得する許可を付与する	読み取り	cloudwatch-alarm-template*		
GetCloudWatchAlarmTemplateGroup	Cloudwatch アラームテンプレートグループを取得する許可を付与する	読み取り	cloudwatch-alarm-template-group*		
GetEventBridgeRuleTemplate	Eventbridge ルールテンプレートを取得する許可を付与する	読み取り	eventbridge-rule-template*		
GetEventBridgeRuleTemplateGroup	Eventbridge ルールテンプレートグループを取得する許可を付与する	読み取り	eventbridge-rule-template-group*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetSignalMap	シグナルマップを取得する許可を付与する	読み取り	signal-map*		
ListChannelPlacementGroups	チャネルプレイスメントグループを一覧表示する許可を付与する	リスト			
ListChannels	チャネルを一覧表示する許可を付与。	リスト			
ListCloudWatchAlarmTemplateGroups	Cloudwatch アラームテンプレートグループを一覧表示する許可を付与する	リスト			
ListCloudWatchAlarmTemplates	Cloudwatch アラームテンプレートを一覧表示する許可を付与する	リスト			
ListClusters	クラスターを一覧表示するためのアクセス許可を付与	リスト			
ListEventBridgeRuleTemplateGroups	Eventbridge ルールテンプレートグループを一覧表示する許可を付与する	リスト			
ListEventBridgeRuleTemplates	Eventbridge ルールテンプレートを一覧表示する許可を付与する	リスト			
ListInputDeviceTransfers	入力デバイスを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListInputDevices	入力デバイスを一覧表示する許可を付与。	リスト			
ListInputSecurityGroups	入力セキュリティグループを一覧表示する許可を付与。	リスト			
ListInputs	入力を一覧表示する許可を付与	リスト			
ListMultiplexPrograms	マルチプレックスプログラムを一覧表示する許可を付与	リスト			
ListMultiplexes	マルチプレックスを一覧表示する許可を付与	リスト			
ListNetworks	ネットワークを一覧表示するアクセス許可を付与	リスト			
ListNodes	ノードを一覧表示する許可を付与する	リスト			
ListOfferings	予約サービスを一覧表示する許可を付与	リスト			
ListReservations	予約を一覧表示する許可を付与。	リスト			
ListSdiSources	SDI ソースを一覧表示する許可を付与	リスト			
ListSignalMaps	シグナルマップを一覧表示する許可を付与する	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTagsForResource	チャネル、入力、入力セキュリティグループ、マルチプレックス、予約、ノード、クラスター、ネットワーク、チャネルプレイスメントグループ、SDI ソース、シグナルマップ、テンプレートグループ、テンプレートのタグを一覧表示するアクセス許可を付与します	リスト	channel		
			channel-placement-group		
			cloudwatch-alarm-template		
			cloudwatch-alarm-template-group		
			cluster		
			eventbridge-rule-template		
			eventbridge-rule-template-group		
			input		
			input-security-group		
			multiplex		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			network		
			node		
			reservation		
			sdi-source		
			signal-map		
ListVersions	MediaLive の利用可能なバージョンを一覧表示するアクセス許可を付与します	リスト			
PollAnywhere	クラスターをポーリングする許可をノードに付与する	書き込み			
PurchaseOffering	予約サービスを購入する許可を付与	書き込み	offering*		
			reservation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RebootInputDevice	入力デバイスを再起動する許可を付与	書き込み	input-device*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RejectInputDeviceTransfer	入力デバイス転送を拒否する許可を付与	書き込み	input-device*		
RestartChannelPipelines	実行中のチャンネルでパイプラインを再起動する許可を付与する	書き込み	channel*		
StartChannel	チャネルを開始する許可を付与	書き込み	channel*		
StartDeleteMonitorDeployment	シグナルマップのモニタの削除を開始する許可を付与する	書き込み	signal-map*		
StartInputDevice	MediaConnect フローに接続された入力デバイスを開始するアクセス許可を付与します	書き込み	input-device*		
StartInputDeviceMaintenanceWindow	入力デバイスのメンテナンスウィンドウを開始する許可を付与	書き込み	input-device*		
StartMonitorDeployment	シグナルマップモニタのデプロイを開始する許可を付与する	書き込み	signal-map*		
StartMultiplex	マルチプレックスを開始する許可を付与	書き込み	multiplex*		
StartUpdateSignalMap	シグナルマップの更新を開始する許可を付与する	書き込み	signal-map*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StopChannel	チャネルを停止する許可を付与	書き込み	channel*		
StopInputDevice	MediaConnect フローに接続された入力デバイスを停止するアクセス許可を付与します	書き込み	input-device*		
StopMultiplex	マルチプレックスを停止する許可を付与	書き込み	multiplex*		
SubmitAnywhereStateChange	クラスターに状態変更を送信する許可をノードに付与する	書き込み			
TransferInputDevice	入力デバイスを転送する許可を付与	書き込み	input-device*		
UpdateAccountConfiguration	顧客のアカウント設定を更新する許可を付与	書き込み			
UpdateChannel	チャネルを更新する許可を付与	書き込み	channel*		
UpdateChannelClass	チャネルのクラスを更新する許可を付与	書き込み	channel*		
UpdateChannelPlacementGroup	ノードを更新する許可を付与する	書き込み	channel-placement-group*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateCloudWatchAlarmTemplate	CloudWatch アラームテンプレートを更新する許可を付与する	書き込み	cloudwatch-alarm-template*		
			cloudwatch-alarm-template-group*		
UpdateCloudWatchAlarmTemplateGroup	CloudWatch アラームテンプレートグループを更新する許可を付与する	書き込み	cloudwatch-alarm-template-group*		
UpdateCluster	クラスターを更新するためのアクセス許可を付与	書き込み	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateEventBridgeRuleTemplate	Eventbridge ルールテンプレートを更新する許可を付与する	書き込み	eventbridge-rule-template*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			eventbridge-rule-template-group*		
UpdateEventBridgeRuleTemplateGroup	Eventbridge ルールテンプレートグループを更新する許可を付与する	書き込み	eventbridge-rule-template-group*		
UpdateInput	入力を更新する許可を付与	書き込み	input*		
UpdateInputDevice	入力デバイスを更新する許可を付与。	書き込み	input-device*		
UpdateInputSecurityGroup	入力セキュリティグループを更新する許可を付与	書き込み	input-security-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateMultiplex	マルチプレックスを更新する許可を付与	書き込み	multiplex*		
UpdateMultiplexProgram	マルチプレックスプログラムを更新する許可を付与	書き込み	multiplex*		
UpdateNetwork	ノードの状態を更新する許可を付与する	書き込み	network*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateNode	ノードを更新する許可を付与する	書き込み	node*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateNodeState	ノードの状態を更新する許可を付与する	書き込み	node*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateReservation	予約を更新する許可を付与	書き込み	reservation*		
UpdateSdiSource	sdi ソースの状態を更新するアクセス許可を付与します	書き込み	sdi-source*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	

AWS Elemental MediaLive で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
channel	arn:${Partition}:medialive:${Region}:${Account}:channel:${ChannelId}	aws:ResourceTag/${TagKey}
input	arn:${Partition}:medialive:${Region}:${Account}:input:${InputId}	aws:ResourceTag/${TagKey}
input-device	arn:${Partition}:medialive:${Region}:${Account}:inputDevice:${DeviceId}	
input-security-group	arn:${Partition}:medialive:${Region}:${Account}:inputSecurityGroup:${InputSecurityGroupId}	aws:ResourceTag/${TagKey}
multiplex	arn:${Partition}:medialive:${Region}:${Account}:multiplex:${MultiplexId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
reservation	arn:${Partition}:medialive:${Region}:${Account}:reservation:${ReservationId}	aws:ResourceTag/${TagKey}
offering	arn:${Partition}:medialive:${Region}:${Account}:offering:${OfferingId}	
signal-map	arn:${Partition}:medialive:${Region}:${Account}:signal-map:${SignalMapId}	aws:ResourceTag/${TagKey}
cloudwatch-alarm-template-group	arn:${Partition}:medialive:${Region}:${Account}:cloudwatch-alarm-template-group:${CloudWatchAlarmTemplateGroupId}	aws:ResourceTag/${TagKey}
cloudwatch-alarm-template	arn:${Partition}:medialive:${Region}:${Account}:cloudwatch-alarm-template:${CloudWatchAlarmTemplateId}	aws:ResourceTag/${TagKey}
eventbridge-rule-template-group	arn:${Partition}:medialive:${Region}:${Account}:eventbridge-rule-template-group:${EventBridgeRuleTemplateGroupId}	aws:ResourceTag/${TagKey}
eventbridge-rule-template	arn:${Partition}:medialive:${Region}:${Account}:eventbridge-rule-template:${EventBridgeRuleTemplateId}	aws:ResourceTag/${TagKey}
cluster	arn:${Partition}:medialive:${Region}:${Account}:cluster:${ClusterId}	aws:ResourceTag/${TagKey}
node	arn:${Partition}:medialive:${Region}:${Account}:node:${ClusterId}/${NodeId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
network	arn:${Partition}:medialive:${Region}:${Account}:network:${NetworkId}	aws:ResourceTag/${TagKey}
channel-placement-group	arn:${Partition}:medialive:${Region}:${Account}:channelPlacementGroup:${ClusterId}/${ChannelPlacementGroupId}	aws:ResourceTag/${TagKey}
sdi-source	arn:${Partition}:medialive:${Region}:${Account}:sdiSource:${SdiSourceId}	aws:ResourceTag/${TagKey}

AWS Elemental MediaLive の条件キー

AWS Elemental MediaLive では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Elemental MediaPackage のアクション、リソース、および条件キー

AWS Elemental MediaPackage (サービスプレフィックス: mediapackage) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Elemental MediaPackage で定義されるアクション
- AWS Elemental MediaPackage で定義されるリソースタイプ
- AWS Elemental MediaPackage の条件キー

AWS Elemental MediaPackage で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ConfigureLogs	チャネルのアクセスログを設定する許可を付与	書き込み	channels*		iam:CreateServiceLinkedRole
CreateChannel	Elemental MediaPackage AWS でチャネルを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateHarvestJob	Elemental MediaPackage AWS で収集ジョブを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
CreateOriginEndpoint	Elemental MediaPackage AWS でエンドポイントを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Elemental MediaPackage AWS でチャネルを削除するアクセス許可を付与します	書き込み	channels*		
DeleteOriginEndpoint	Elemental MediaPackage AWS でエンドポイントを削除するアクセス許可を付与します	書き込み	origin_endpoints*		
DescribeChannel	Elemental MediaPackage AWS でチャネルの詳細を表示するアクセス許可を付与します	読み取り	channels*		
DescribeHarvestJob	Elemental MediaPackage AWS で収集ジョブの詳細を表示するアクセス許可を付与します	読み取り	harvest_jobs*		
DescribeOriginEndpoint	Elemental MediaPackage AWS でエンドポイントの詳細を表示するアクセス許可を付与します	読み取り	origin_endpoints*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListChannels	Elemental MediaPackage AWS でチャネルのリストを表示するアクセス許可を付与します	読み取り			
ListHarvestJobs	Elemental MediaPackage AWS で収集ジョブのリストを表示するアクセス許可を付与します	読み取り			
ListOriginEndpoints	Elemental MediaPackage AWS でエンドポイントのリストを表示するアクセス許可を付与します	読み取り			
ListTagsForResource	チャネルまたは OriginEndpoint に割り当てられたタグを一覧表示する許可を付与	読み取り	channels		
			harvest_jobs		
			origin_endpoints		
RotateChannelCredentials	AWS Elemental MediaPackage のチャネルの最初の IngestEndpoint の認証情報を更新する許可を付与	書き込み	channels*		
RotateIngestEndpointCredentials	AWS Elemental MediaPackage でチャネルの IngestEndpoint 認証情報を更新する許可を付与	書き込み	channels*		
TagResource	MediaPackage リソースをタグ付けする許可を付与	Tagging	channels		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			harvest_jobs		
			origin_endpoints		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	チャネルまたは OriginEndpoint に対するタグを削除する許可を付与	Tagging	channels		
			harvest_jobs		
			origin_endpoints		
				aws:TagKeys	
UpdateChannel	Elemental MediaPackage AWS でチャネルを変更するアクセス許可を付与します	書き込み	channels*		
UpdateOriginEndpoint	Elemental MediaPackage AWS でエンドポイントを変更するアクセス許可を付与します	書き込み	origin_endpoints*		

AWS Elemental MediaPackage で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
channels	arn:${Partition}:mediapackage:${Region}:${Account}:channels/${ChannelIdentifier}	aws:ResourceTag/${TagKey}
origin_endpoints	arn:${Partition}:mediapackage:${Region}:${Account}:origin_endpoints/${OriginEndpointIdentifier}	aws:ResourceTag/${TagKey}
harvest_jobs	arn:${Partition}:mediapackage:${Region}:${Account}:harvest_jobs/${HarvestJobIdentifier}	aws:ResourceTag/${TagKey}

AWS Elemental MediaPackage の条件キー

AWS Elemental MediaPackage では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	MediaPackage リクエストのタグでアクセスをフィルタリングします。	String

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	MediaPackage リソースのタグでアクセスをフィルタリングします。	String
aws:TagKeys	MediaPackage リソースまたはリクエストのタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Elemental MediaPackage V2 のアクション、リソース、および条件キー

AWS Elemental MediaPackage V2 (サービスプレフィックス: `mediapackagev2`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Elemental MediaPackage V2 で定義されるアクション
- AWS Elemental MediaPackage V2 で定義されるリソースタイプ
- AWS Elemental MediaPackage V2 の条件キー

AWS Elemental MediaPackage V2 で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーショ

ンへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CancelHarvestJob	収集ジョブをキャンセルするアクセス許可を付与します	書き込み	Channel*		
			ChannelGroup*		
			HarvestJob*		
			OriginEndpoint*		
CreateChannel	チャネルグループにチャネルを作成する許可を付与	書き込み	Channel*		
			ChannelGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateChannelGroup	チャネルグループを作成する許可を付与	書き込み	ChannelGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHarvestJob	収集ジョブを作成するアクセス許可を付与します	書き込み	Channel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			ChannelGroup*		
			HarvestJob*		
			OriginEndpoint*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOriginEndpoint	チャネルのオリジンエンドポイントを作成する許可を付与	書き込み	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	チャネルグループ内のチャネルを削除する許可を付与	書き込み	Channel*		
			ChannelGroup*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteChannelGroup	チャネルグループを削除する許可を付与	書き込み	ChannelGroup*		
DeleteChannelPolicy	チャネルからリソースポリシーを削除する許可を付与	書き込み	Channel*		
			ChannelGroup*		
			ChannelPolicy*		
DeleteOriginEndpoint	チャネルのオリジンエンドポイントを削除する許可を付与	書き込み	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
DeleteOriginEndpointPolicy	オリジンエンドポイントからリソースポリシーを削除する許可を付与	書き込み	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
			OriginEndpointPolicy*		
GetChannel	チャネルグループ内のチャネルの詳細を取得する許可を付与	読み取り	Channel*		
			ChannelGroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetChannelGroup	チャネルグループの詳細を取得する許可を付与	読み取り	ChannelGroup*		
GetChannelPolicy	チャネルのリソースポリシーを取得する許可を付与	読み取り	Channel*		
			ChannelGroup*		
			ChannelPolicy*		
GetHarvestJob	収集ジョブの詳細を取得するアクセス許可を付与します	読み取り	Channel*		
			ChannelGroup*		
			HarvestJob*		
			OriginEndpoint*		
GetHeadObject	MediaPackage に GetHeadObject リクエストを実行する許可を付与	読み取り	OriginEndpoint*		
GetObject	MediaPackage に GetObject リクエストを実行する許可を付与	読み取り	OriginEndpoint*		
GetOriginEndpoint	オリジンエンドポイントの詳細を取得する許可を付与	読み取り	Channel*		
			ChannelGroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			OriginEndpoint*		
GetOriginEndpointPolicy	オリジンエンドポイントのリソースポリシーの詳細を取得する許可を付与	読み取り	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
			OriginEndpointPolicy*		
HarvestObject	MediaPackage に HarvestObject リクエストを行う許可を付与	読み取り	OriginEndpoint*		
ListChannelGroups	AWS アカウントのすべてのチャネルグループを一覧表示する許可を付与	リスト			
ListChannels	チャネルグループ内のすべてのチャネルを一覧表示する許可を付与	リスト	ChannelGroup*		
ListHarvestJobs	チャネルグループ、チャネル、オリジンエンドポイント内のすべての収集ジョブを一覧表示するアクセス許可を付与します	リスト	ChannelGroup*		
ListOriginEndpoints		リスト	Channel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	チャネルのすべてのオリジンエンドポイントを一覧表示する許可を付与		ChannelGroup*		
ListTagsForResource	指定されたリソースのタグを一覧表示する許可を付与	読み取り	Channel		
			ChannelGroup		
			HarvestJob		
			OriginEndpoint		
PutChannelPolicy	チャネルのリソースポリシーをアタッチする許可を付与	書き込み	Channel*		
			ChannelGroup*		
			ChannelPolicy*		
PutObject	MediaPackage に PutObject リクエストを実行する許可を付与	書き込み	Channel*		
PutOriginEndpointPolicy	リソースポリシーを元のエンドポイントにアタッチする許可を付与	書き込み	Channel*		
			ChannelGroup*		
			OriginEndpoint*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			OriginEndpointPolicy*		
ResetChannelState	チャネルをリセットするアクセス許可を付与します	書き込み	Channel*		
			ChannelGroup*		
ResetOriginEndpointState	オリジンエンドポイントをリセットするアクセス許可を付与します	書き込み	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
TagResource	指定されたタグを指定されたリソースに追加する許可を付与	Tagging	Channel		
			ChannelGroup		
			HarvestJob		
			OriginEndpoint		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	指定されたリソースから指定されたタグを削除するためのアクセス許可を付与	Tagging	Channel		
			ChannelGroup		
			HarvestJob		
			OriginEndpoint		
				aws:TagKeys	
UpdateChannel	チャネルグループ内のチャネルを更新する許可を付与	書き込み	Channel*		
			ChannelGroup*		
UpdateChannelGroup	チャネルグループを更新する許可を付与	書き込み	ChannelGroup*		
UpdateOriginEndpoint	チャネルのオリジンエンドポイントを更新する許可を付与	書き込み	Channel*		
			ChannelGroup*		
			OriginEndpoint*		

AWS Elemental MediaPackage V2 で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
ChannelGroup	arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}	aws:ResourceTag/${TagKey}
ChannelPolicy	arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}	
Channel	arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}	aws:ResourceTag/${TagKey}
OriginEndpointPolicy	arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}/originEndpoint/${OriginEndpointName}	
OriginEndpoint	arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}/originEndpoint/${OriginEndpointName}	aws:ResourceTag/${TagKey}
HarvestJob	arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}/originEndpoint/${OriginEndpointName}/harvestJob/${HarvestJobName}	aws:ResourceTag/${TagKey}

AWS Elemental MediaPackage V2 の条件キー

AWS Elemental MediaPackage V2 では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストで渡されたタグによりアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグによりアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーによりアクセスをフィルタリングします	ArrayOfString

AWS Elemental MediaPackage VOD のアクション、リソース、および条件キー

AWS Elemental MediaPackage VOD (サービスプレフィックス: mediapackage-vod) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Elemental MediaPackage VOD で定義されるアクション
- AWS Elemental MediaPackage VOD で定義されるリソースタイプ
- AWS Elemental MediaPackage VOD の条件キー

AWS Elemental MediaPackage VOD で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ConfigureLogs	PackagingGroup の送信アクセスログを設定する許可を付与	書き込み	packaging-groups*		iam:CreateServiceLinkedRole
CreateAsset	Elemental MediaPackage AWS でアセットを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePackagingConfiguration	Elemental MediaPackage AWS でパッケージ設定を作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePackagingGroup	Elemental MediaPackage AWS でパッケージンググループを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAsset	Elemental MediaPackage AWS でアセットを削除するアクセス許可を付与します	書き込み	assets*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeletePackagingConfiguration	Elemental MediaPackage AWS でパッケージ設定を削除するアクセス許可を付与します	書き込み	packaging-configurations*		
DeletePackagingGroup	Elemental MediaPackage AWS でパッケージンググループを削除する許可を付与	書き込み	packaging-groups*		
DescribeAsset	Elemental MediaPackage AWS でアセットの詳細を表示するアクセス許可を付与します	読み取り	assets*		
DescribePackagingConfiguration	Elemental MediaPackage AWS でパッケージ設定の詳細を表示するアクセス許可を付与します	読み取り	packaging-configurations*		
DescribePackagingGroup	Elemental MediaPackage AWS でパッケージンググループの詳細を表示するアクセス許可を付与します	読み取り	packaging-groups*		
ListAssets	Elemental MediaPackage AWS でアセットのリストを表示するアクセス許可を付与します	リスト			
ListPackagingConfigurations	Elemental MediaPackage AWS でパッケージ設定のリストを表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListPackagingGroups	Elemental MediaPackage AWS でパッケージンググループのリストを表示するアクセス許可を付与します	リスト			
ListTagsForResource	PackagingGroup、PackagingConfiguration、または Asset に割り当てられているタグを一覧表示するアクセス許可を付与します	読み込み	assets		
			packaging-configurations		
			packaging-groups		
TagResource	PackagingGroup、PackagingConfiguration、または Asset にタグを割り当てるアクセス許可を付与します	Tagging	assets		
			packaging-configurations		
			packaging-groups		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	PackagingGroup、PackagingConfiguration、または Asset からタグを削除するアクセス許可を付与します	Tagging	assets		
			packaging-configurations		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			packaging-groups		
				aws:TagKeys	
UpdatePackagingGroup	Elemental MediaPackage AWS でパッケージンググループを更新する許可を付与	書き込み	packaging-groups*		

AWS Elemental MediaPackage VOD で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
assets	`arn:${Partition}:mediapackage-vod:${Region}:${Account}:assets/${AssetIdentifier}`	aws:ResourceTag/${TagKey}
packaging-configurations	`arn:${Partition}:mediapackage-vod:${Region}:${Account}:packaging-configurations/${PackagingConfigurationIdentifier}`	aws:ResourceTag/${TagKey}
packaging-groups	`arn:${Partition}:mediapackage-vod:${Region}:${Account}:packaging-groups/${PackagingGroupIdentifier}`	aws:ResourceTag/${TagKey}

AWS Elemental MediaPackage VOD の条件キー

AWS Elemental MediaPackage VOD では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアのプレゼンスに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいてアクションをフィルタリングします	ArrayOfString

AWS Elemental MediaStore のアクション、リソース、および条件キー

AWS Elemental MediaStore (サービスプレフィックス: mediastore) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Elemental MediaStore で定義されるアクション

- AWS Elemental MediaStore で定義されるリソースタイプ
- AWS Elemental MediaStore の条件キー

AWS Elemental MediaStore で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateContainer	コンテナを作成する許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteContainer	コンテナを削除する許可を付与	書き込み	container*		
DeleteContainerPolicy	コンテナのアクセスポリシーを削除する許可を付与	権限の管理	container*		
DeleteCorsPolicy	コンテナから CORS ポリシーを削除する許可を付与	書き込み	container*		
DeleteLifecyclePolicy	コンテナからライフサイクルポリシーを削除する許可を付与	書き込み	container*		
DeleteMetricPolicy	コンテナからメトリクスポリシーを削除する許可を付与	書き込み	container*		
DeleteObject	オブジェクトを削除する許可を付与	書き込み	object*		
DescribeContainer	コンテナの詳細を取得する許可を付与	リスト	container*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeObject	オブジェクトのメタデータを取得する許可を付与	リスト	object*		
GetContainerPolicy	コンテナのアクセスポリシーを取得する許可を付与	読み取り	container*		
GetCorsPolicy	コンテナの CORS ポリシーを取得する許可を付与	読み取り	container*		
GetLifecyclePolicy	コンテナに割り当てられているライフサイクルポリシーを取得する許可を付与	読み取り	container*		
GetMetricPolicy	コンテナに割り当てられているメトリクスポリシーを取得する許可を付与	読み取り	container*		
GetObject	オブジェクトを取得する許可を付与	読み取り	object*		
ListContainers	現在のアカウントのコンテナのリストを取得する許可を付与	リスト			
ListItems	フォルダに保存されているオブジェクトとサブフォルダのリストを取得する許可を付与	リスト	folder		
ListTagsForResource	コンテナのタグを一覧表示する許可を付与	読み取り	container		
PutContainerPolicy	コンテナのアクセスポリシーを作成または置換する許可を付与	権限の管理	container*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutCorsPolicy	コンテナの CORS ポリシーを追加または変更する許可を付与	書き込み	container*		
PutLifecyclePolicy	コンテナに割り当てられているライフサイクルポリシーを追加または変更する許可を付与	書き込み	container*		
PutMetricPolicy	コンテナに割り当てられているメトリクスポリシーを追加または変更する許可を付与	書き込み	container*		
PutObject	オブジェクトをアップロードする許可を付与	書き込み	object*		
StartAccessLogging	コンテナのアクセスログを開始する許可を付与	書き込み	container*		iam:PassRole
StopAccessLogging	コンテナのアクセスログを停止する許可を付与	書き込み	container*		
TagResource	コンテナにタグを追加する許可を付与	Tagging	container		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	コンテナからタグを削除する許可を付与	Tagging	container		
				aws:TagKeys	

AWS Elemental MediaStore で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
container	`arn:${Partition}:mediastore:${Region}:${Account}:container/${ContainerName}`	aws:ResourceTag/${TagKey}
object	`arn:${Partition}:mediastore:${Region}:${Account}:container/${ContainerName}/${ObjectPath}`	
folder	`arn:${Partition}:mediastore:${Region}:${Account}:container/${ContainerName}/${FolderPath}`	

AWS Elemental MediaStore の条件キー

AWS Elemental MediaStore では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列

条件キー	説明	タイプ
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Elemental MediaTailor のアクション、リソース、および条件キー

AWS Elemental MediaTailor (サービスプレフィックス: `mediatailor`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Elemental MediaTailor で定義されるアクション
- AWS Elemental MediaTailor で定義されるリソースタイプ
- AWS Elemental MediaTailor の条件キー

AWS Elemental MediaTailor で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ConfigureLogsForChannel	指定されたチャネル名を持つチャネルでログを設定するための許可を付与します	書き込み	channel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ConfigureLogsForPlaybackConfiguration	再生設定のログを設定する許可を付与	書き込み	playbackConfiguration*		iam:CreateServiceLinkedRole
CreateChannel	チャネルモデレーターを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLiveSource	指定されたソースの場所の名前を使用して、ソースロケーションに新しいライブソースを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePrefetchSchedule	指定された再生設定名で再生設定にプリフェッチスケジュールを作成する許可を付与	書き込み	playbackConfiguration*		
CreateProgram	指定されたチャネル名で新しいプログラムを作成する許可を付与	書き込み			
CreateSourceLocation	新しいソースの場所を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateVodSource	指定されたソースの場所の名前を使用して、ソースロケーションに新しい VOD ソースを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	指定されたチャネル名を削除する許可を付与	書き込み	channel*		
DeleteChannelPolicy	指定されたチャネル名を持つチャネルの IAM ポリシーを削除する許可を付与	権限の管理	channel*		
DeleteLiveSource	指定されたソースの場所の名前を持つソースの場所で、指定されたライブソース名を持つライブソースを削除する許可を付与する	書き込み	liveSource*		
DeletePlaybackConfiguration	指定された再生設定を削除する許可を付与	書き込み	playbackConfiguration*		
DeletePrefetchSchedule	指定されたプリフェッチスケジュール名で再生設定のプリフェッチスケジュールを削除する許可を付与	書き込み	playbackConfiguration*		
			prefetchSchedule*		
DeleteProgram	指定されたチャネル名を持つチャネルで、指定されたプログラム名を持つプログラムを削除する許可を付与	書き込み	program*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteSourceLocation	指定されたソースの場所の名前を持つソースロケーションを削除する許可を付与	書き込み	sourceLocation*		
DeleteVodSource	指定されたソースの場所の名前を持つソースの場所で、指定された VOD ソース名を持つ VOD ソースを削除する許可を付与	書き込み	vodSource*		
DescribeChannel	指定されたチャネル名を持つチャネルを取得する許可を付与	読み取り	channel*		
DescribeLiveSource	指定されたソースの場所の名前を持つソースの場所で、指定されたライブソース名を持つライブソースを取得する許可を付与する	読み取り	liveSource*		
DescribeProgram	指定されたチャネル名を持つチャネルで、指定されたプログラム名を持つプログラムを取得する許可を付与	読み込み	program*		
DescribeSourceLocation	指定されたソースの場所の名前を持つソースの場所を取得する許可を付与	読み込み	sourceLocation*		
DescribeVodSource	指定されたソースの場所の名前を持つソースの場所で、指定された VOD ソース名を持つ VOD ソースを取得する許可を付与	読み込み	vodSource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetChannelPolicy	指定されたチャネル名を持つチャネルで IAM ポリシーを読み取る許可を付与	読み込み	channel*		
GetChannelSchedule	指定されたチャネル名を持つチャネルでプログラムのスケジュールを取得する許可を付与	読み込み	channel*		
GetPlaybackConfiguration	指定された名前の設定を取得する許可を付与。	読み込み	playbackConfiguration*		
GetPrefetchSchedule	指定されたプリフェッチスケジュール名で再生設定のプリフェッチスケジュールを取得する許可を付与	読み込み	playbackConfiguration*		
			prefetchSchedule*		
ListAlerts	リソースでアラートのリストを取得する許可を付与	読み込み			
ListChannels	既存のチャネルのリストを取得する許可を付与	読み取り			
ListLiveSources	指定されたソースの場所の名前を持つソースの場所で、既存のライブソースのリストを取得する許可を付与する	読み取り			
ListPlaybackConfigurations	利用可能な設定のリストを取得する許可を付与。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListPrefetchSchedules	指定されたプリフェッチスケジュール名のリストを取得する許可を付与	リスト	playbackConfiguration*		
ListSourceLocations	既存のソースの場所のリストを取得する許可を付与	読み込み			
ListTagsForResource	指定した再生設定リソースに割り当てられたタグを一覧表示する許可を付与	読み込み	channel		
			liveSource		
			playbackConfiguration		
			sourceLocation		
			vodSource		
ListVodSources	指定されたソースの場所の名前を持つソースの場所で、既存の VOD ソースのリストを取得する許可を付与	読み込み			
PutChannelPolicy	指定されたチャネル名を持つチャネルで IAM ポリシーを設定する許可を付与	権限の管理	channel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutPlaybackConfiguration	新しい設定を追加する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
StartChannel	指定されたチャネル名を持つチャネルを開始する許可を付与	書き込み	channel*		
StopChannel	指定されたチャネル名を持つチャネルを停止する許可を付与	書き込み	channel*		
TagResource	タグを指定された再生設定リソースに追加する許可を付与	Tagging	channel		
			liveSource		
			playbackConfiguration		
			sourceLocation		
			vodSource		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	指定された再生設定リソースからタグを削除する許可を付与	Tagging	channel		
			liveSource		
			playbackConfiguration		
			sourceLocation		
			vodSource		
				aws:TagKeys	
UpdateChannel	指定されたチャネル名を持つチャネルを更新する許可を付与	書き込み	channel*		
UpdateLiveSource	指定されたソースの場所の名前を持つソースの場所で、指定されたライブソース名を持つライブソースを更新する許可を付与する	書き込み	liveSource*		
UpdateProgram	指定されたチャネル名を持つチャネルで、指定されたプログラム名を持つプログラムを更新するための許可を付与します	書き込み	program*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateSourceLocation	指定されたソースの場所の名前を持つソースの場所を更新する許可を付与	書き込み	sourceLocation*		
UpdateVodSource	指定されたソースの場所の名前を持つソースの場所で、指定された VOD ソース名を持つ VOD ソースを更新する許可を付与	書き込み	vodSource*		

AWS Elemental MediaTailor で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
playbackConfiguration	arn:${Partition}:mediatailor:${Region}:${Account}:playbackConfiguration/${ResourceId}	aws:ResourceTag/${TagKey}
prefetchSchedule	arn:${Partition}:mediatailor:${Region}:${Account}:prefetchSchedule/${ResourceId}	
channel	arn:${Partition}:mediatailor:${Region}:${Account}:channel/${ChannelName}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
program	arn:${Partition}:mediatailor:${Region}:${Account}:program/${ChannelName}/${ProgramName}	
sourceLocation	arn:${Partition}:mediatailor:${Region}:${Account}:sourceLocation/${SourceLocationName}	aws:ResourceTag/${TagKey}
vodSource	arn:${Partition}:mediatailor:${Region}:${Account}:vodSource/${SourceLocationName}/${VodSourceName}	aws:ResourceTag/${TagKey}
liveSource	arn:${Partition}:mediatailor:${Region}:${Account}:liveSource/${SourceLocationName}/${LiveSourceName}	aws:ResourceTag/${TagKey}

AWS Elemental MediaTailor の条件キー

AWS Elemental MediaTailor は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

AWS Elemental Support Cases のアクション、リソース、条件キー

AWS Elemental Support Cases (サービスプレフィックス: `elemental-support-cases`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Elemental Support Cases で定義されたアクション
- AWS Elemental Support Cases で定義されたリソースタイプ
- AWS Elemental Support Cases の条件キー

AWS Elemental Support Cases で定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddCaseComment [アクセス許可のみ]	サポートケースにコメントを追加する許可を付与	書き込み	case*		
CheckCasePermission	発信者がサポートケース操作を実行するための許可を持っ	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
[アクセス許可のみ]	ているかどうかを確認する許可を付与				
CompleteMultipartUpload [アクセス許可のみ]	サポートケースへのマルチパートファイルのアップロードを完了する許可を付与	書き込み	case*		
CreateCase [アクセス許可のみ]	サポートケースを作成する許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateS3CLIUploadCommand [アクセス許可のみ]	サポートケースへのファイルのアップロードを許可する cli コマンドを作成するアクセス許可を付与します	書き込み	case*		
CreateS3DownloadUrl [アクセス許可のみ]	サポートケースからファイルをダウンロードする許可を付与	書き込み	case*		
GetCase [アクセス許可のみ]	アカウントでサポートケースを記述する許可を付与	読み取り	case*		
GetCasePermission [許可のみ]	発信者がサポートケース操作を実行するための許可を持っているかどうかを確認する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetCases [許可のみ]	アカウントでサポートケースを一覧表示する許可を付与	読み取り			
GetUICache [許可のみ]	コンソールで使用するキャッシュされたケースユーザーデータを取得する許可を付与	読み取り			
ListTagsForCase [許可のみ]	サポートケースのタグを一覧表示するアクセス許可を付与します	読み取り	case*		
StartMultipartUpload [許可のみ]	サポートケースへのマルチパートファイルのアップロードを開始する許可を付与	書き込み	case*		
TagCase [アクセス許可のみ]	サポートケースにタグを追加する許可を付与	Tagging	case*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagCase [アクセス許可のみ]	サポートケースのタグを削除するアクセス許可を付与します	Tagging	case*		
				aws:TagKeys	
UpdateCase [アクセス許可のみ]	サポートケースを更新する許可を付与	書き込み	case*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateCaseStatus [アクセス許可のみ]	サポートケースのステータスを更新するアクセス許可を付与します	書き込み	case*		
UpdateMultipartUpload [アクセス許可のみ]	サポートケースへのマルチパートファイルアップロードを更新する許可を付与	書き込み	case*		

AWS Elemental Support Cases で定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
case	`arn:${Partition}:elemental-support-cases::${Account}:case/${ResourceId}`	aws:ResourceTag/${TagKey}

AWS Elemental Support Cases の条件キー

AWS Elemental Support Cases では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストで渡されたタグによりアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグによりアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーによりアクセスをフィルタリングします	ArrayOfString

AWS Elemental Support Content のアクション、リソース、条件キー

AWS Elemental Support Content (サービスプレフィックス: `elemental-support-content`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Elemental Support Content で定義されたアクション
- AWS Elemental Support Content で定義されたリソースタイプ
- AWS Elemental Support Content の条件キー

AWS Elemental Support Content で定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
Query [アクセス許可のみ]	サポートコンテンツを検索する許可を付与	読み取り			

AWS Elemental Support Content で定義されたリソースタイプ

AWS Elemental Support Content は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Elemental Support Content へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Elemental Support Content の条件キー

Elemental Support Content には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon EMR on EKS (EMR コンテナ) のアクション、リソース、および条件キー

Amazon EMR on EKS (EMR コンテナ) (サービスプレフィックス: `emr-containers`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件キーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon EMR on EKS (EMR コンテナ) で定義されるアクション

- Amazon EMR on EKS (EMR コンテナ) で定義されるリソースタイプ
- Amazon EMR on EKS (EMR コンテナ) の条件キー

Amazon EMR on EKS (EMR コンテナ) で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelJobRun	ジョブ実行をキャンセルする権限を付与します	書き込み	jobRun*		
CreateCertificate	CreateCertificate メソッドを呼び出して CertificateSigningRequest を受け入れ、署名付き証明書を返すアクセス許可を付与します	書き込み			
CreateJobTemplate	ジョブテンプレートを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateManagedEndpoint	マネージドエンドポイントを作成するためのアクセス許可を付与します	書き込み	virtualCluster*		
				aws:RequestTag/${TagKey} aws:TagKeys emr-containers:Exe	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				cutionRoleArn	
CreateSecurityConfiguration	セキュリティ設定を作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateVirtualCluster	仮想クラスターを作成する権限を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteJobTemplate	ジョブテンプレートを削除する許可を付与	書き込み	jobTemplate*		
DeleteManagedEndpoint	マネージドエンドポイントを削除するためのアクセス許可を付与します	Write	managedEndpoint*		
DeleteVirtualCluster	仮想クラスターを削除する権限を付与します	Write	virtualCluster*		
DescribeJobRun	ジョブ実行を記述する権限を付与します	読み取り	jobRun*		
DescribeJobTemplate	ジョブテンプレートを記述する許可を付与	読み取り	jobTemplate*		
DescribeManagedEndpoint	マネージドエンドポイントを記述するためのアクセス許可を付与します	読み取り	managedEndpoint*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeSecurityConfiguration	セキュリティ設定を記述する許可を付与する	読み取り	securityConfiguration*		
DescribeVirtualCluster	仮想クラスターを記述する権限を付与します	読み取り	virtualCluster*		
GetManagedEndpointSessionCredentials	マネージドエンドポイントへの接続に使用されるセッショントークンを生成する許可を付与します	書き込み	managedEndpoint*		
ListJobRuns	仮想クラスターに関連付けられているジョブ実行を一覧表示する権限を付与します	リスト	virtualCluster*		
ListJobTemplates	ジョブテンプレートを一覧表示する許可を付与	リスト			
ListManagedEndpoints	仮想クラスターに関連付けられたマネージドエンドポイントを一覧表示するためのアクセス許可を付与します	リスト	virtualCluster*		
ListSecurityConfigurations	セキュリティ設定を一覧表示する許可を付与	リスト			
ListTagsForResource	指定されたリソースのタグを一覧表示する許可を付与	リスト	jobRun		
			jobTemplate		
			managedEndpoint		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			securityConfiguration		
			virtualCluster		
ListVirtualClusters	仮想クラスターを一覧表示する権限を付与します	リスト			
StartJobRun	ジョブ実行を開始する権限を付与します	Write	virtualCluster*		
				aws:RequestTag/${TagKey} aws:TagKeys emr-containers:ExecutionRoleArn emr-containers:JobTemplateArn	
TagResource	指定されたリソースにタグを付けるアクセス許可を付与	タグ付け	jobRun		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			jobTemplate		
			managedEndpoint		
			securityConfiguration		
			virtualCluster		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	指定されたリソースのタグを解除するアクセス許可を付与	タグ付け	jobRun		
			jobTemplate		
			managedEndpoint		
			securityConfiguration		
			virtualCluster		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:TagKeys	

Amazon EMR on EKS (EMR コンテナ) で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
virtualCluster	arn:${Partition}:emr-containers:${Region}:${Account}:/virtualclusters/${VirtualClusterId}	aws:ResourceTag/${TagKey}
jobRun	arn:${Partition}:emr-containers:${Region}:${Account}:/virtualclusters/${VirtualClusterId}/jobruns/${JobRunId}	aws:ResourceTag/${TagKey}
jobTemplate	arn:${Partition}:emr-containers:${Region}:${Account}:/jobtemplates/${JobTemplateId}	aws:ResourceTag/${TagKey}
managedEndpoint	arn:${Partition}:emr-containers:${Region}:${Account}:/virtualclusters/${VirtualClusterId}/endpoints/${EndpointId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
securityConfiguration	`arn:${Partition}:emr-containers:${Region}:${Account}:/securityconfigurations/${SecurityConfigurationId}`	aws:ResourceTag/${TagKey}

Amazon EMR on EKS (EMR コンテナ) の条件キー

Amazon EMR on EKS (EMR コンテナ) は、Condition ポリシーの IAM 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内にあるタグキーと値のペアによりアクセスをフィルタリング	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内にあるタグキーによりアクセスをフィルタリング	ArrayOfString
emr-containers:ExecutionRoleArn	リクエスト内にある実行ロール ARN によりアクセスをフィルタリング	ARN
emr-containers:JobTemplateArn	リクエスト内にあるジョブテンプレート ARN によりアクセスをフィルタリング	ARN

Amazon EMR Serverless のアクション、リソース、および条件キー

Amazon EMR Serverless (サービスプレフィックス: `emr-serverless`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon EMR Serverless で定義されるアクション
- Amazon EMR Serverless で定義されるリソースタイプ
- Amazon EMR Serverless の条件キー

Amazon EMR Serverless で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AccessInteractiveEndpoints [アクセス許可のみ]	アプリケーション上でインタラクティブなワークロードを実行するアクセス許可を付与します	書き込み	application*		iam:PassRole
AccessLivyEndpoints [アクセス許可のみ]	EMR Serverless Application で有効になっている Livy エンドポイントでインタラクティブワークロードを実行する許可を付与する	書き込み	application*		iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AccessSystemProfileLogs [アクセス許可のみ]	システムプロファイルログにアクセスする許可を付与	書き込み	jobRun*		
CancelJobRun	ジョブ実行をキャンセルする権限を付与します	書き込み	jobRun*		
CreateApplication	アプリケーションを作成する許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	アプリケーションを削除する許可を付与	書き込み	application*		
GetApplication	アプリケーションを取得する許可を付与します	読み取り	application*		
GetDashboardForJobRun	ジョブ実行ダッシュボードを取得するための許可を付与します	読み取り	jobRun*		
GetJobRun	ジョブ実行を取得する許可を付与します	読み取り	jobRun*		
ListApplications	アプリケーションを一覧表示する許可を付与	リスト			
ListJobRunAttempts	ジョブ実行に関連付けられたジョブ実行の試行を一覧表示する許可を付与する	リスト	jobRun*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListJobRuns	アプリケーションに関連付けられたジョブ実行を一覧表示する許可を付与します	リスト	application*		
ListTagsForResource	指定されたリソースのタグを一覧表示する許可を付与	読み取り	application		
			jobRun		
StartApplication	アプリケーションを開始する許可を付与します	書き込み	application*		
StartJobRun	ジョブ実行を開始する許可を付与します	書き込み	application*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
StopApplication	アプリケーションを停止する許可を付与します	書き込み	application*		
TagResource	指定されたリソースにタグを付けるアクセス許可を付与	タグ付け	application		
			jobRun		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	指定されたリソースのタグを解除するアクセス許可を付与	Tagging	application		
			jobRun		
				aws:TagKeys	
UpdateApplication	アプリケーションを更新する許可を付与します	書き込み	application*		

Amazon EMR Serverless で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
application	`arn:${Partition}:emr-serverless:${Region}:${Account}:/applications/${ApplicationId}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
jobRun	arn:${Partition}:emr-serverless:${Region}:${Account}:/applications/${ApplicationId}/jobruns/${JobRunId}	aws:ResourceTag/${TagKey}

Amazon EMR Serverless の条件キー

Amazon EMR Serverless では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

AWS エンドユーザーメッセージング SMS および音声 V2 のアクション、リソース、および条件キー

AWS エンドユーザーメッセージング SMS および音声 V2 (サービスプレフィックス: sms-voice) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS エンドユーザーメッセージング SMS および音声 V2 で定義されるアクション
- AWS エンドユーザーメッセージング SMS および音声 V2 で定義されるリソースタイプ
- AWS エンドユーザーメッセージング SMS および音声 V2 の条件キー

AWS エンドユーザーメッセージング SMS および音声 V2 で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシーの概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateOriginationIdentity	発信元の電話番号または送信者 ID をプールに関連付けるアクセス許可を付与します	書き込み	Pool*		
			PhoneNumber		
			SenderId		
AssociateProtectConfiguration	保護設定を設定セットに関連付ける許可を付与する	書き込み	ConfigurationSet*		
			ProtectConfiguration*		
CreateConfigurationSet	設定セットを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateEventDestination	設定セット内のイベントの宛先を作成するアクセス許可を付与します	書き込み	ConfigurationSet*		iam:PassRole
CreateOptOutList	オプトアウトリストを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreatePool	プールを作成するアクセス許可を付与します	書き込み	PhoneNumber		sms-voice:TagResource
			SenderId		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProtectConfiguration	保護設定を作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateRegistration	登録を作成するためのアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateRegistrationAssociation	登録を電話番号または別の登録と関連付けるためのアクセス許可を付与	書き込み	Registration* PhoneNumber		
CreateRegistrationAttachment	登録アタッチメントを作成するためのアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateRegistrationVersion	登録バージョンを作成するためのアクセス許可を付与	書き込み	Registration*		
CreateVerifiedDestinationNumber	検証済み送信先番号を作成するためのアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
DeleteAccountDefaultProtectConfiguration	アカウントのデフォルト保護設定を削除する許可を付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteConfigurationSet	設定セットを削除するアクセス許可を付与します	書き込み	ConfigurationSet*		
DeleteDefaultMessageType	設定セットのデフォルトのメッセージタイプを削除するアクセス許可を付与します	書き込み	ConfigurationSet*		
DeleteDefaultSenderId	設定セットのデフォルトの送信者 ID を削除するアクセス許可を付与します	書き込み	ConfigurationSet*		
DeleteEventDestination	設定セット内のイベントの宛先を削除するアクセス許可を付与します	書き込み	ConfigurationSet*		
DeleteKeyword	プールまたは発信元の電話番号のキーワードを削除するアクセス許可を付与します	書き込み	PhoneNumber Pool		
DeleteMediaMessageSpendLimitOverride	アカウントのメディアメッセージの月額使用制限の上書きを削除する許可を付与する	書き込み			
DeleteOptOutList	オプトアウトリストを削除するアクセス許可を付与します	書き込み	OptOutList*		
DeleteOptedOutNumber	オプトアウトリストから送信先電話番号を削除するアクセス許可を付与します	書き込み	OptOutList*		
DeletePool	プールを削除するアクセス許可を付与します	書き込み	Pool*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteProtectConfiguration	保護設定を削除する許可を付与する	書き込み	ProtectConfiguration*		
DeleteProtectConfigurationRuleSetNumberOverride	保護設定の電話番号オーバーライドを削除するアクセス許可を付与します	書き込み	ProtectConfiguration*		
DeleteRegistration	登録を削除するためのアクセス許可を付与	書き込み	Registration*		
DeleteRegistrationAttachment	登録アタッチメントを削除するためのアクセス許可を付与	書き込み	RegistrationAttachment*		
DeleteRegistrationFieldValue	オプションの登録フィールド値を削除するためのアクセス許可を付与	書き込み	Registration*		
DeleteResourcePolicy	リソースポリシーを削除する許可を付与。	権限の管理	OptOutList		
			PhoneNumber		
			Pool		
			SenderId		
DeleteTextMessageSpendLimitOverride	アカウントのテキストメッセージの月額使用制限の上書きを削除するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteVerifiedDestinationNumber	検証済み送信先番号を削除するためのアクセス許可を付与	書き込み	VerifiedDestinationNumber*		
DeleteVoiceMessageSpendLimitOverride	アカウントのボイスメッセージの月額使用制限の上書きを削除するアクセス許可を付与します	書き込み			
DescribeAccountAttributes	アカウントの属性を記述するアクセス許可を付与します	読み込み			
DescribeAccountLimits	アカウントのサービスクォータを記述するアクセス許可を付与します	読み込み			
DescribeConfigurationSets	アカウントの設定セットを記述するアクセス許可を付与します	読み込み	ConfigurationSet		
DescribeKeywords	プールまたは発信元の電話番号のキーワードを記述するアクセス許可を付与します	読み込み	PhoneNumber		
			Pool		
DescribeOptOutLists	アカウント内のオプトアウトリストを記述するアクセス許可を付与します	読み込み	OptOutList		
DescribeOptedOutNumbers	オプトアウトリスト内の宛先の電話番号を記述するアクセス許可を付与します	読み込み	OptOutList*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribePhoneNumbers	アカウント内の発信元の電話番号を記述するアクセス許可を付与します	読み込み	PhoneNumber		
DescribePools	アカウント内のプールを記述するアクセス許可を付与します	読み取り	Pool		
DescribeProtectConfigurations	アカウントの保護設定を記述する許可を付与する	読み取り	ProtectConfiguration		
DescribeRegistrationAttachments	アカウント内の登録アタッチメントを記述するためのアクセス許可を付与	読み取り	RegistrationAttachment		
DescribeRegistrationFieldDefinitions	特定の登録タイプのフィールド定義を記述するためのアクセス許可を付与	読み取り			
DescribeRegistrationFieldValues	特定の登録のフィールド値を記述するためのアクセス許可を付与	読み取り	Registration*		
DescribeRegistrationSectionDefinitions	特定の登録タイプのセクション定義を記述するためのアクセス許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeRegistrationTypeDefinitions	サービスでサポートされている登録タイプを記述するためのアクセス許可を付与	読み取り			
DescribeRegistrationVersions	特定の登録のバージョンを記述するためのアクセス許可を付与	読み取り	Registration*		
DescribeRegistrations	アカウント内の登録を記述するためのアクセス許可を付与	読み取り	Registration		
DescribeSenderIds	アカウントの送信者 ID を記述するアクセス許可を付与します	読み込み	SenderId		
DescribeSpendLimits	アカウントの月額使用制限を記述するアクセス許可を付与します	読み取り			
DescribeVerifiedDestinationNumbers	アカウント内の検証済み送信先番号を記述するためのアクセス許可を付与	読み取り	VerifiedDestinationNumber		
DisassociateOriginationIdentity	プールから発信元の電話番号または送信者 ID の関連付けを解除するアクセス許可を付与します	書き込み	Pool*		
			PhoneNumber		
			SenderId		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DisassociateProtectConfiguration	設定セットから保護設定の関連付けを解除する許可を付与する	書き込み	ConfigurationSet*		
			ProtectConfiguration*		
DiscardRegistrationVersion	特定の登録の最新バージョンを破棄するためのアクセス許可を付与	書き込み	Registration*		
GetProtectConfigurationCountryRuleSet	保護設定の国ルールセットを取得する許可を付与する	読み取り	ProtectConfiguration*		
GetResourcePolicy	リソースポリシーを取得する許可の付与	読み取り	OptOutList		
			PhoneNumber		
			Pool		
			SenderId		
ListPoolOriginationIdentities	プールに関連付けられている発信元の電話番号と送信者 ID を一覧表示するアクセス許可を付与します	読み取り	Pool*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListProtectConfigurationRuleSetNumberOverrides	保護設定のすべての電話番号オーバーライドを一覧表示するアクセス許可を付与します	読み取り	ProtectConfiguration*		
ListRegistrationAssociations	登録に関連付けられているすべてのリソースを一覧表示するためのアクセス許可を付与	読み取り	Registration*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み込み	ConfigurationSet		
			OptOutList		
			PhoneNumber		
			Pool		
			ProtectConfiguration		
			Registration		
			RegistrationAttachment		
			SenderId		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			VerifiedDestinationNumber		
PutKeyword	プールまたは発信元の電話番号のキーワードを作成または更新するアクセス許可を付与します	書き込み	PhoneNumber		
			Pool		
PutMessageFeedback	テキスト、音声、またはメディアメッセージのフィードバックを配置するアクセス許可を付与します	書き込み	Message*		
PutOptedOutNumber	送信先の電話番号をオプトアウトリストに入れるアクセス許可を付与します	書き込み	OptOutList*		
PutProtectConfigurationRuleSetNumberOverride	保護設定の電話番号オーバーライドを配置するアクセス許可を付与します	書き込み	ProtectConfiguration*		
PutRegistrationFieldValue	登録フィールド値を入力するためのアクセス許可を付与	書き込み	Registration*		
PutResourcePolicy	リソースポリシーを配置する許可を付与	権限の管理	OptOutList		
			PhoneNumber		
			Pool		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			SenderId		
ReleasePhoneNumber	発信元の電話番号をリリースするアクセス許可を付与します	書き込み	PhoneNumber*		
ReleaseSenderId	送信者 ID をリリースするためのアクセス許可を付与	書き込み	SenderId*		
RequestPhoneNumber	発信元の電話番号をリクエストするアクセス許可を付与します	書き込み	Pool		sms-voice:AssociateOriginationIdentity sms-voice:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
RequestSenderId	未登録の送信者 ID をリクエストするためのアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SendDestinationNumberVerificationCode	送信先の電話番号に検証コードを含むテキストまたはボイスメッセージを送信するためのアクセス許可を付与	書き込み	PhoneNumber		sms-voice:SendTextMessage sms-voice:SendVoiceMessage
			Pool		
			SenderId		
SendMediaMessage	宛先電話番号にメディアメッセージを送信する許可を付与する	書き込み	PhoneNumber		
			Pool		
SendTextMessage	送信先の電話番号にテキストメッセージを送信するアクセス許可を付与します	書き込み	PhoneNumber		
			Pool		
			SenderId		
SendVoiceMessage	宛先電話番号にボイスメッセージを送信するアクセス許可を付与します	書き込み	PhoneNumber		
			Pool		
SetAccountDefaultProtectConfiguration	アカウントのデフォルトの保護設定を設定する許可を付与する	書き込み	ProtectConfiguration*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SetDefaultMessageFeedbackEnabled	設定セットのデフォルトのメッセージフィードバックを設定するアクセス許可を付与します	書き込み	ConfigurationSet*		
SetDefaultMessageType	設定セットのデフォルトのメッセージタイプを設定するアクセス許可を付与します	書き込み	ConfigurationSet*		
SetDefaultSenderId	設定セットのデフォルトの送信者 ID を設定するアクセス許可を付与します	書き込み	ConfigurationSet*		
SetMediaMessageSpendLimitOverride	アカウントのメディアメッセージの月額使用制限の上書きを設定する許可を付与する	書き込み			
SetTextMessageSpendLimitOverride	アカウントのテキストメッセージの月額使用制限の上書きを設定するアクセス許可を付与します	書き込み			
SetVoiceMessageSpendLimitOverride	アカウントのボイスメッセージの月間使用制限の上書きを設定するアクセス許可を付与します	書き込み			
SubmitRegistrationVersion	特定の登録の最新バージョンを送信するためのアクセス許可を付与	書き込み	Registration*		
TagResource	リソースにタグを追加するアクセス許可を付与します	タグ付け	ConfigurationSet		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			OptOutList		
			PhoneNumber		
			Pool		
			ProtectConfiguration		
			Registration		
			RegistrationAttachment		
			SenderId		
			VerifiedDestinationNumber		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	Tagging	ConfigurationSet		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			OptOutList		
			PhoneNumber		
			Pool		
			ProtectConfiguration		
			Registration		
			RegistrationAttachment		
			SenderId		
			VerifiedDestinationNumber		
				aws:TagKeys	
UpdateEventDestination	設定セット内のイベント送信先を更新するアクセス許可を付与します	書き込み	ConfigurationSet*		iam:PassRole
UpdatePhoneNumber	発信元の電話番号の設定を更新するアクセス許可を付与します	書き込み	PhoneNumber*		iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdatePool	プールの設定を更新するアクセス許可を付与します	書き込み	Pool*		iam:PassRole
UpdateProtectConfiguration	保護設定を更新する許可を付与する	書き込み	ProtectConfiguration*		
UpdateProtectConfigurationCountryRuleSet	保護設定の国ルールセットを更新する許可を付与する	書き込み	ProtectConfiguration*		
UpdateSenderId	送信者 ID の設定を更新するためのアクセス許可を付与	書き込み	SenderId*		
VerifyDestinationNumber	送信先の電話番号を検証するためのアクセス許可を付与	書き込み	VerifiedDestinationNumber*		

AWS エンドユーザーメッセージング SMS および音声 V2 で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
ConfigurationSet	arn:${Partition}:sms-voice:${Region}:${Account}:configuration-set/${ConfigurationSetName}	aws:ResourceTag/${TagKey}
OptOutList	arn:${Partition}:sms-voice:${Region}:${Account}:opt-out-list/${OptOutListName}	aws:ResourceTag/${TagKey}
PhoneNumber	arn:${Partition}:sms-voice:${Region}:${Account}:phone-number/${PhoneNumberId}	aws:ResourceTag/${TagKey}
Pool	arn:${Partition}:sms-voice:${Region}:${Account}:pool/${PoolId}	aws:ResourceTag/${TagKey}
ProtectConfiguration	arn:${Partition}:sms-voice:${Region}:${Account}:protect-configuration/${ProtectConfigurationId}	aws:ResourceTag/${TagKey}
SenderId	arn:${Partition}:sms-voice:${Region}:${Account}:sender-id/${SenderId}/${IsoCountryCode}	aws:ResourceTag/${TagKey}
Registration	arn:${Partition}:sms-voice:${Region}:${Account}:registration/${RegistrationId}	aws:ResourceTag/${TagKey}
RegistrationAttachment	arn:${Partition}:sms-voice:${Region}:${Account}:registration-attachment/${RegistrationAttachmentId}	aws:ResourceTag/${TagKey}
VerifiedDestinationNumber	arn:${Partition}:sms-voice:${Region}:${Account}:verified-destination-number/${VerifiedDestinationNumberId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
Message	arn:${Partition}:sms-voice:${Region}:${Account}:message/${MessageId}	

AWS エンドユーザーメッセージング SMS および音声 V2 の条件キー

AWS エンドユーザーメッセージング SMS および音声 V2 では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS End User Messaging Social のアクション、リソース、および条件キー

AWS End User Messaging Social (サービスプレフィックス: social-messaging) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS エンドユーザーメッセージングソーシャルで定義されるアクション
- AWS End User Messaging Social で定義されるリソースタイプ
- AWS End User Messaging Social の条件キー

AWS エンドユーザーメッセージングソーシャルで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateWhatsAppBusinessAccount	WhatsApp ビジネスアカウントを に関連付けるアクセス許可を付与します AWS アカウント	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateWhatsAppMessageTemplate	WhatsApp メッセージテンプレートを作成するアクセス許可を付与します	書き込み			
CreateWhatsAppMessageTemplateFromLibrary	Meta のテンプレートライブラリから WhatsApp メッセージテンプレートを作成するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateWhatsAppMessageTemplateMedia	WhatsApp メッセージテンプレートのメディアを作成するアクセス許可を付与します	書き込み			
DeleteWhatsAppMessageMedia	WhatsApp からメディアオブジェクトを削除する許可を付与する	書き込み	phone-number-id*		
DeleteWhatsAppMessageTemplate	WhatsApp メッセージテンプレートを削除するアクセス許可を付与します	書き込み			
DisassociateWhatsAppBusinessAccount	から WhatsApp ビジネスアカウントの関連付けを解除するアクセス許可を付与します AWS アカウント	書き込み	waba*		
GetLinkedWhatsAppBusinessAccount	WhatsApp ビジネスアカウントの詳細を表示する許可を付与する	読み取り	waba*		
GetLinkedWhatsAppBusinessAccountPhoneNumber	電話番号の詳細を表示する許可を付与する	読み取り	phone-number-id*		
GetWhatsAppMessageMedia	WhatsApp からメディアオブジェクトを取得する許可を付与する	書き込み	phone-number-id*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetWhatsAppMessageTemplate	WhatsApp メッセージテンプレートの詳細を取得するアクセス許可を付与します	読み取り			
ListLinkedWhatsAppBusinessAccounts	すべての WhatsApp ビジネスアカウントを表示する許可を付与する	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	phone-number-id		
			waba		
ListWhatsAppMessageTemplates	WhatsApp メッセージテンプレートを一覧表示する許可を付与	リスト			
ListWhatsAppTemplateLibrary	Meta のテンプレートライブラリから使用可能なテンプレートを一覧表示する許可を付与	リスト			
PostWhatsAppMessageMedia	WhatsApp にメディアオブジェクトをアップロードする許可を付与する	書き込み	phone-number-id*		
PutWhatsAppBusinessAccountEventDestinations	WhatsApp ビジネスアカウントのイベント送信先を更新する許可を付与する	書き込み	waba*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SendWhatsAppMessage	WhatsApp 経由でメッセージを送信する許可を付与する	書き込み	phone-number-id*		
TagResource	リソースにタグを追加する許可を付与	タグ付け	phone-number-id		
			waba		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	Tagging	phone-number-id		
			waba		
				aws:ResourceTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateWhatsAppMessageTemplate	WhatsApp メッセージテンプレートを更新する許可を付与	書き込み			

AWS End User Messaging Social で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
phone-number-id	`arn:${Partition}:social-messaging:${Region}:${Account}:phone-number-id/${OriginationPhoneNumberId}`	aws:ResourceTag/${TagKey}
waba	`arn:${Partition}:social-messaging:${Region}:${Account}:waba/${WabaId}`	aws:ResourceTag/${TagKey}

AWS End User Messaging Social の条件キー

AWS End User Messaging Social では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Entity Resolution のアクション、リソース、および条件キー

AWS Entity Resolution (サービスプレフィックス: `entityresolution`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Entity Resolution によって定義されたアクション
- AWS Entity Resolution によって定義されたリソースタイプ
- AWS Entity Resolution の条件キー

AWS Entity Resolution によって定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AddPolicyStatement	AWS エンティティ解決リソースを使用するアクセス許可を AWS サービスまたは別のアカウントに付与するアクセス許可を付与します	権限の管理			
BatchDeleteUniqueId	一意の ID を一括削除する許可を付与する	書き込み	MatchingWorkflow*		
CreateIdMappingWorkflow	idmapping ワークフローを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIdNamespace	IdNamespace を作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMatchingWorkflow	マッチングワークフローを作成するための許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchemaMapping	スキーママッピングを作成するための許可を付与します	書き込み		aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
DeleteIdMappingWorkflow	idmapping ワークフローを削除するアクセス許可を付与します	書き込み	IdMappingWorkflow*		
DeleteIdNamespace	IdNamespace を削除する許可を付与する	書き込み	IdNamespace*		
DeleteMatchingWorkflow	マッチングワークフローを削除するための許可を付与します	書き込み	MatchingWorkflow*		
DeletePolicyStatement	AWS エンティティ解決リソースを使用するアクセス許可を AWS サービスまたは別のアカウントに付与されたアクセス許可を削除するアクセス許可を付与します	権限の管理			
DeleteSchemaMapping	スキーママッピングを削除するための許可を付与します	書き込み	SchemaMapping*		
GenerateMatchId	一致 ID を生成するアクセス許可を付与します	書き込み	MatchingWorkflow*		
GetIdMappingJob	idmapping ジョブを取得するアクセス許可を付与します	読み取り	IdMappingWorkflow*		
GetIdMappingWorkflow	idmapping ワークフローを取得するアクセス許可を付与します	読み取り	IdMappingWorkflow*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetIdNamespace	IdNamespace を取得する許可を付与する	読み取り	IdNamespace*		
GetMatchId	一致 ID を取得するための許可を付与します	読み取り	MatchingWorkflow*		
GetMatchingJob	マッチングジョブを取得するための許可を付与します	読み取り	MatchingWorkflow*		
GetMatchingWorkflow	マッチングワークフローを取得するための許可を付与します	読み取り	MatchingWorkflow*		
GetPolicy	AWS エンティティ解決リソースのリソースポリシーを取得するアクセス許可を付与します	読み取り			
GetProviderService	プロバイダサービスを取得するアクセス許可を付与します	読み取り	ProviderService*		
GetSchemaMapping	スキーママッピングを取得するための許可を付与します	読み取り	SchemaMapping*		
ListIdMappingJobs	idmapping ジョブを一覧表示するアクセス許可を付与します	リスト	IdMappingWorkflow*		
ListIdMappingWorkflows	idmapping ワークフローを一覧表示するためのアクセス許可を付与します	リスト			
ListIdNamespaces	IdNamespaces を一覧表示する許可を付与する	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListMatchingJobs	マッチングジョブを一覧表示するための許可を付与します	リスト	MatchingWorkflow*		
ListMatchingWorkflows	マッチングワークフローを一覧表示するための許可を付与します	リスト			
ListProviderServices	プロバイダサービスを一覧表示するアクセス許可を付与します	リスト			
ListSchemaMappings	スキーママッピングを一覧表示するための許可を付与します	リスト			
ListTagsForResource	リソースのタグを一覧表示するための許可を付与します	読み取り			
PutPolicy	AWS エンティティ解決リソースのリソースポリシーを配置するアクセス許可を付与します	権限の管理			
StartIdMappingJob	idmapping ジョブを開始するアクセス許可を付与します	書き込み	IdMappingWorkflow*		
StartMatchingJob	マッチングジョブを開始するための許可を付与します	書き込み	MatchingWorkflow*		
TagResource	リソースにタグを追加するアクセス許可を付与	Tagging	IdMappingWorkflow		
			IdNamespace		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			MatchingWorkflow		
			ProviderService		
			SchemaMapping		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースのタグを解除する許可を付与	Tagging	IdMappingWorkflow		
			IdNamespace		
			MatchingWorkflow		
			ProviderService		
			SchemaMapping		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateIdMappingWorkflow	idmapping ワークフローを更新するアクセス許可を付与します	書き込み	IdMappingWorkflow*		
UpdateIdNamespace	IdNamespace を更新する許可を付与する	書き込み	IdNamespace*		
UpdateMatchingWorkflow	マッチングワークフローを更新するための許可を付与します	書き込み	MatchingWorkflow*		
UpdateSchemaMapping	スキーママッピングを更新するための許可を付与します	書き込み	SchemaMaping*		
UseIdNamespace	ワークフロー内で IdNamespace を使用するアクセス許可を AWS サービスまたは別のアカウントに付与するアクセス許可を付与します	権限の管理			
UseWorkflow	IdNamespace 内のワークフローを使用するアクセス許可を AWS サービスまたは別のアカウントに付与するアクセス許可を付与します	権限の管理			

AWS Entity Resolution によって定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
MatchingWorkflow	arn:${Partition}:entityresolution:${Region}:${Account}:matchingworkflow/${WorkflowName}	aws:ResourceTag/${TagKey}
SchemaMapping	arn:${Partition}:entityresolution:${Region}:${Account}:schemamapping/${SchemaName}	aws:ResourceTag/${TagKey}
IdMappingWorkflow	arn:${Partition}:entityresolution:${Region}:${Account}:idmappingworkflow/${WorkflowName}	aws:ResourceTag/${TagKey}
ProviderService	arn:${Partition}:entityresolution:${Region}:${Account}:providerservice/${ProviderName}/${ProviderServiceName}	aws:ResourceTag/${TagKey}
IdNamespace	arn:${Partition}:entityresolution:${Region}:${Account}:idnamespace/${IdNamespaceName}	aws:ResourceTag/${TagKey}

AWS Entity Resolution の条件キー

AWS Entity Resolution では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	ユーザーがエンティティ解決サービスに対して実行するリクエストに含まれるキーでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	タグキーおよび値のペアでアクセスをフィルタリングします。	String
aws:TagKeys	ユーザーがエンティティ解決サービスに対して実行するリクエストに含まれるすべてのタグキー名のリストでアクセスをフィルタリングします	ArrayOfString

Amazon EventBridge のアクション、リソース、および条件キー

Amazon EventBridge (サービスプレフィックス: `events`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon EventBridge で定義されるアクション
- Amazon EventBridge で定義されるリソースタイプ
- Amazon EventBridge の条件キー

Amazon EventBridge で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ActivateEventSource	パートナーイベントソースをアクティブ化するアクセス許可を付与	書き込み	event-source*		
AllowVendedLogDeliveryForResource [アクセス許可のみ]	EventBridge 用に提供されたログ配信を設定するアクセス許可を付与します	書き込み	event-bus*		
CancelReplay	再生をキャンセルするアクセス許可を付与	書き込み	replay*		
CreateApiDestination	新しい API の送信先を作成するアクセス許可を付与	書き込み	api-destination*		
			connection*		
CreateArchive	新しいアーカイブを作成するアクセス許可を付与	書き込み	archive*		
			event-bus*		
			alias		
			key		
CreateConnection	新しい接続を作成する許可を付与	書き込み	connection*		
CreateEndpoint	エンドポイントを作成するアクセス許可を付与	書き込み	endpoint*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				events:EventBusArn	
CreateEventBus	イベントバスを作成するアクセス許可を付与	書き込み	event-bus*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePartnerEventSource	パートナーイベントソースを作成するアクセス許可を付与	書き込み	event-source*		
DeactivateEventSource	イベントソースを被アクティブにするアクセス許可を付与	書き込み	event-source*		
DeauthorizeConnection	接続の認可を解除するアクセス許可を付与し、保存されている認可シークレットを削除します	書き込み	connection*		
DeleteApiDestination	API 送信先を削除するアクセス許可を付与	書き込み	api-destination*		
DeleteArchive	アーカイブを削除するアクセス許可を付与	書き込み	archive*		
DeleteConnection	接続を削除する許可を付与。	書き込み	connection*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteEndpoint	エンドポイントを削除する許可を付与	書き込み	endpoint*		
DeleteEventBus	イベントバスを削除するアクセス許可を付与	書き込み	event-bus*		
DeletePartnerEventSource	パートナーイベントソースを削除するアクセス許可を付与	書き込み	event-source*		
DeleteRule	ルールを削除するアクセス許可を付与	書き込み	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	
DescribeApiDestination	API 送信先の詳細を取得するアクセス許可を付与	読み込み	api-destination*		
			connection*		
DescribeArchive	アーカイブの詳細を削除するアクセス許可を付与	読み込み	archive*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeConnection	接続の詳細を取得するアクセス許可を付与	読み込み	connection*		
DescribeEndpoint	エンドポイントの詳細を取得するアクセス許可を付与	読み込み	endpoint*		
DescribeEventBus	イベントバスの詳細を取得するアクセス許可を付与	読み込み	event-bus		
DescribeEventSource	イベントソースの詳細を取得するアクセス許可を付与	読み込み	event-source*		
DescribePartnerEventSource	パートナーイベントソースの詳細を取得するアクセス許可を付与	読み込み	event-source*		
DescribeReplay	再生の詳細を取得するアクセス許可を付与	読み込み	replay*		
DescribeRule	ルールの詳細を取得するアクセス許可を付与	読み込み	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisableRule	ルールを無効にするアクセス許可を付与	書き込み	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	
EnableRule	ルールを有効にするアクセス許可を付与	書き込み	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
InvokeApiDestination [アクセス許可のみ]	API 送信先を呼び出すアクセス許可を付与	書き込み	api-destination*		
ListApiDestinations	API 送信先のリストを取得するアクセス許可を付与	リスト			
ListArchives	アーカイブのリストを取得するアクセス許可を付与	リスト			
ListConnections	接続のリストを取得する許可を付与。	リスト			
ListEndpoints	エンドポイントのリストを取得するアクセス許可を付与	リスト			
ListEventBuses	アカウント内のイベントバスのリストを取得するアクセス許可を付与	リスト			
ListEventSources	このアカウントで共有されているイベントソースのリストを取得するアクセス許可を付与	リスト			
ListPartnerEventSourceAccounts	イベントソースに関連付けられた AWS アカウント IDs のリストを取得するアクセス許可を付与します	リスト	event-source*		
ListPartnerEventSources	パートナーイベントソースのリストを取得するアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListReplays	再生のリストを取得するアクセス許可を付与	リスト			
ListRuleNamesByTarget	ターゲットに関連付けられたルール名のリストを取得するアクセス許可を付与	リスト			
ListRules	アカウント内の Amazon EventBridge ルールのリストを取得するアクセス許可を付与	リスト			
ListTagsForResource	Amazon EventBridge リソースに関連付けられたタグのリストを取得するアクセス許可を付与	リスト	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount	
ListTargetsByRule	ルールについて定義されたターゲットのリストを取得するアクセス許可を付与	リスト	rule-on-custom-event-bus		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			rule-on-default-event-bus		
				events:creatorAccount	
PutEvents	カスタムイベントを Amazon EventBridge に送信するアクセス許可を付与	書き込み	event-bus*		
				events:detail-type events:source events:eventBusInvocation	
PutPartnerEvents	カスタムイベントを Amazon EventBridge に送信するアクセス許可を付与	書き込み			
PutPermission	PutPermission アクションを使用して、デフォルトのイベントバスにイベントを配置 AWS アカウント するアクセス許可を別の に付与するアクセス許可を付与します	権限の管理			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutRule	ルールを作成または更新するアクセス許可を付与	書き込み	rule-on-custom-event-bus		
			rule-on-default-event-bus		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				events:detail.userIdentity.principalId events:detail-type events:source events:detail.service events:detail.eventTypeCode aws:RequestTag/${TagKey} aws:TagKeys events:creatorAccount events:ManagedBy	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutTargets	ルールにターゲットを追加するアクセス許可を付与	書き込み	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:TargetArn events:creatorAccount events:ManagedBy	
RemovePermission	デフォルトのイベントバスにイベントを配置 AWS アカウント する別の のアクセス許可を取り消すアクセス許可を付与します	権限の管理			
RemoveTargets	ルールからターゲットを削除するアクセス許可を付与	書き込み	rule-on-custom-event-bus		
			rule-on-default-event-bus		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				events:creatorAccount events:ManagedBy	
RetrieveConnectionCredentials [アクセス許可のみ]	接続から認証情報を取得するためのアクセス許可を付与	書き込み	connection*		
StartReplay	アーカイブの再生を開始するアクセス許可を付与	書き込み	archive*		
			event-bus*		
			replay*		
TagResource	Amazon EventBridge リソースにタグを追加するアクセス許可を付与	Tagging	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey} events:creatorAccount	
TestEventPattern	イベントパターンが指定のイベントと一致するかどうかをテストするアクセス許可を付与	読み込み			
UntagResource	Amazon EventBridge リソースからタグを削除するアクセス許可を付与	タグ付け	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		
				aws:TagKeys events:creatorAccount	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateApiDestination	API 送信先を更新するアクセス許可を付与	書き込み	api-destination*		
UpdateArchive	アーカイブを更新するアクセス許可を付与	書き込み	archive*		
			alias		
			key		
UpdateConnection	接続を更新する許可を付与。	書き込み	connection*		
UpdateEndpoint	エンドポイントを更新するアクセス許可を付与	書き込み	endpoint*		
				events:EventBusArn	
UpdateEventBus	イベントバスを更新する許可を付与する	書き込み	event-bus*		

Amazon EventBridge で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
event-source	`arn:${Partition}:events:${Region}::event-source/${EventSourceName}`	

リソースタイプ	ARN	条件キー
event-bus	arn:${Partition}:events:${Region}:${Account}:event-bus/${EventBusName}	aws:ResourceTag/${TagKey}
rule-on-default-event-bus	arn:${Partition}:events:${Region}:${Account}:rule/${RuleName}	aws:ResourceTag/${TagKey}
rule-on-custom-event-bus	arn:${Partition}:events:${Region}:${Account}:rule/${EventBusName}/${RuleName}	aws:ResourceTag/${TagKey}
archive	arn:${Partition}:events:${Region}:${Account}:archive/${ArchiveName}	
replay	arn:${Partition}:events:${Region}:${Account}:replay/${ReplayName}	
connection	arn:${Partition}:events:${Region}:${Account}:connection/${ConnectionName}	
api-destination	arn:${Partition}:events:${Region}:${Account}:api-destination/${ApiDestinationName}	
endpoint	arn:${Partition}:events:${Region}:${Account}:endpoint/${EndpointName}	
create-snapshot	arn:${Partition}:events:${Region}:${Account}:target/create-snapshot	
reboot-instance	arn:${Partition}:events:${Region}:${Account}:target/reboot-instance	
stop-instance	arn:${Partition}:events:${Region}:${Account}:target/stop-instance	

リソースタイプ	ARN	条件キー
terminate-instance	arn:${Partition}:events:${Region}:${Account}:target/terminate-instance	
alias	arn:${Partition}:kms:${Region}:${Account}:alias/${Alias}	
key	arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}	

Amazon EventBridge の条件キー

Amazon EventBridge では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	各タグの許可された値のセットに基づいて、イベントバスおよびルールアクションへのアクセスをフィルタリングします。	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値に基づいて、イベントバスおよびルールアクションへのアクセスをフィルタリングします。	String
aws:TagKeys	リクエスト内の必須タグの存在に基づいて、イベントバスおよびルールアクションへのアクセスをフィルタリングします。	ArrayOfString
events:EventBusArn	CreateEndpoint アクションおよび UpdateEndpoint アクションへのエンドポイントに関連付けることができるイベントバスの ARN でアクセスをフィルタリングします	ArrayOfARN

条件キー	説明	[Type] (タイプ)
events:ManagedBy	AWS サービスでアクセスをフィルタリングします。ユーザーに代わって AWS サービスによってルールが作成された場合、値はルールを作成したサービスのプリンシパル名です。	String
events:TargetArn	ルールに設定できるターゲットの ARN に基づいて、PutTargets アクションへのアクセスをフィルタリングします。TargetARN には DeadLetterConfigArn は含まれていません	ArrayOfARN
events:creatorAccount	ルールが作成されたアカウントに基づいて、ルールのアクションへのアクセスをフィルタリングします	String
events:detail-type	イベントの詳細タイプのリテラル文字列に基づいて、PutEvents および PutRule アクションへのアクセスをフィルタリングします	String
events:detail.eventTypeCode	イベントの detail.eventTypeCode フィールドのリテラル文字列に基づいて、PutRule アクションへのアクセスをフィルタリングします	String
events:detail.service	イベントの detail.service フィールドのリテラル文字列に基づいて、PutRule アクションへのアクセスをフィルタリングします	String
events:detail.userIdentity.principalId	イベントの detail.useridentity.principalid フィールドのリテラル文字列に基づいて、PutRule アクションへのアクセスをフィルタリングします	String
events:eventBusInvocation	イベントが API またはクロスアカウントバスの呼び出しのいずれによって生成されたかに基づいて、PutEvents アクションへのアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
events:source	PutEvents および PutRule アクションに対してイベントを生成した AWS サービスまたは AWS パートナーイベントソースによってアクセスをフィルタリングします。イベントのソースフィールドのリテラル文字列をマッチングします	ArrayOfString

Amazon EventBridge Pipes のアクション、リソース、および条件キー

Amazon EventBridge Pipes (サービスプレフィックス: `pipes`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon EventBridge Pipes で定義されるアクション
- Amazon EventBridge Pipes で定義されるリソースタイプ
- Amazon EventBridge Pipes の条件キー

Amazon EventBridge Pipes で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreatePipe	パイプを作成する許可を付与	書き込み	pipe*		iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeletePipe	パイプを削除する許可を付与	書き込み	pipe*		
				aws:ResourceTag/${TagKey}	
DescribePipe	パイプを記述する許可を付与	読み取り	pipe*		
				aws:ResourceTag/${TagKey}	
ListPipes	アカウント内のすべてのパイプを一覧表示する許可を付与	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	pipe*		
				aws:ResourceTag/${TagKey}	
StartPipe	パイプを開始する許可を付与	書き込み	pipe*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
StopPipe	パイプを停止する許可を付与	書き込み	pipe*		
				aws:ResourceTag/${TagKey}	
TagResource	リソースにタグを追加するアクセス許可を付与します	タグ付け	pipe*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	Tagging	pipe*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdatePipe	パイプを更新する許可を付与	書き込み	pipe*		iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	

Amazon EventBridge Pipes で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
pipe	arn:${Partition}:pipes:${Region}:${Account}:pipe/${Name}	aws:ResourceTag/${TagKey}

Amazon EventBridge Pipes の条件キー

Amazon EventBridge Pipes では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	各タグの許可された値のセットでアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値でアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内の必須タグの存在でアクセスをフィルタリングします	ArrayOfString

Amazon EventBridge Scheduler のアクション、リソース、および条件キー

Amazon EventBridge Scheduler (サービスプレフィックス: `scheduler`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon EventBridge Scheduler で定義されるアクション
- Amazon EventBridge Scheduler で定義されるリソースタイプ
- Amazon EventBridge Scheduler の条件キー

Amazon EventBridge Scheduler で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSchedule	Amazon EventBridge Scheduler スケジュールを作成する許可を付与	書き込み	schedule*		iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
CreateScheduleGroup	Amazon EventBridge Scheduler スケジュールグループを作成する許可を付与	書き込み	schedule-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSchedule	Amazon EventBridge Scheduler スケジュールを削除する許可を付与	書き込み	schedule*		
				aws:ResourceTag/${TagKey}	
DeleteScheduleGroup	Amazon EventBridge Scheduler スケジュールグループを削除する許可を付与	書き込み	schedule-group*		scheduler:DeleteSchedule
				aws:ResourceTag/${TagKey}	
GetSchedule	Amazon EventBridge Scheduler スケジュールの詳細を表示する許可を付与	読み取り	schedule*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetScheduleGroup	Amazon EventBridge Scheduler スケジュールグループの詳細を表示する許可を付与	読み取り	schedule-group*		
				aws:ResourceTag/${TagKey}	
ListScheduleGroups	アカウント内の Amazon EventBridge Scheduler スケジュールグループを一覧表示する許可を付与	リスト			
ListSchedules	アカウント内の Amazon EventBridge Scheduler スケジュールを一覧表示する許可を付与	リスト			
ListTagsForResource	Amazon EventBridge Scheduler のタグを一覧表示する許可を付与	読み取り	schedule-group		
				aws:ResourceTag/${TagKey}	
TagResource	Amazon EventBridge Scheduler リソースにタグ付けする許可を付与	Tagging	schedule-group*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Amazon EventBridge Scheduler リソースのタグを解除する許可を付与	Tagging	schedule-group*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateSchedule	Amazon EventBridge Scheduler スケジュールを変更する許可を付与	書き込み	schedule*		iam:PassRole
				aws:ResourceTag/${TagKey}	

Amazon EventBridge Scheduler で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
schedule-group	arn:${Partition}:scheduler:${Region}:${Account}:schedule-group/${GroupName}	aws:ResourceTag/${TagKey}
schedule	arn:${Partition}:scheduler:${Region}:${Account}:schedule/${GroupName}/${ScheduleName}	

Amazon EventBridge Scheduler の条件キー

Amazon EventBridge Scheduler では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon EventBridge スキーマのアクション、リソース、および条件キー

Amazon EventBridge スキーマ (サービスプレフィックス: schemas) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon EventBridge スキーマで定義されるアクション
- Amazon EventBridge スキーマで定義されるリソースタイプ
- Amazon EventBridge スキーマの条件キー

Amazon EventBridge スキーマで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateDiscoverer	イベントスキーマ Discoverer を作成するアクセス許可を付与します。作成後、イベントは自動的に対応するスキーマドキュメントにマッピングされます。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegistry	アカウントに新しいスキーマレジストリを作成するアクセス許可を付与します	書き込み	registry*	aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
CreateSchema	アカウントに新しいスキーマを作成するアクセス許可を付与します	書き込み	schema*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDiscoverer	アカウント内の Discoverer を削除するアクセス許可を付与します	書き込み	discoverer*		
DeleteRegistry	アカウント内の既存のレジストリを削除するアクセス許可を付与します	書き込み	registry*		
DeleteResourcePolicy	特定のレジストリにアタッチされているリソースベースのポリシーを削除するアクセス許可を付与します	書き込み	registry*		
DeleteSchema	アカウント内の既存のスキーマを削除するアクセス許可を付与します	書き込み	schema*		
DeleteSchemaVersion	アカウント内の特定のバージョンのスキーマを削除するアクセス許可を付与します	書き込み	schema*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeCodeBinding	アカウント内の特定のスキーマに生成されたコードのメタデータを取得するアクセス許可を付与します	読み込み	schema*		
DescribeDiscoverer	アカウント内の Discoverer メタデータを取得するアクセス許可を付与します	読み込み	discoverer*		
DescribeRegistry	アカウント内の既存のレジストリメタデータを記述するアクセス許可を付与します	読み込み	registry*		
DescribeSchema	アカウント内の既存のスキーマを取得するアクセス許可を付与します	読み取り	schema*		
ExportSchema	OpenAPI 3 形式で AWS レジストリまたは検出されたスキーマを JSONSchema 形式にエクスポートする許可を付与	読み取り	registry*		
			schema*		
GetCodeBindingSource	アカウント内の特定のスキーマに生成されたコードのメタデータを取得するアクセス許可を付与します	読み込み	schema*		
GetDiscoveredSchema	提供されたサンプルイベントのリストのスキーマを取得するアクセス許可を付与します	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetResourcePolicy	指定されたレジストリにアタッチされているリソースベースのポリシーを取得するアクセス許可を付与します	読み込み	registry*		
ListDiscoverers	アカウント内のすべての Discoverer を一覧表示するアクセス許可を付与します	リスト	discoverer*		
ListRegistries	アカウント内のすべてのレジストリを一覧表示するアクセス許可を付与します	リスト	registry*		
ListSchemaVersions	スキーマのすべてのバージョンを一覧表示するアクセス許可を付与します	リスト	schema*		
ListSchemas	すべてのスキーマを一覧表示するアクセス許可を付与します	リスト	schema*		
ListTagsForResource	リソースのタグを一覧表示するアクセス許可を付与します	読み込み	discoverer		
			registry		
			schema		
PutCodeBinding	アカウント内の特定のスキーマに対してコードを生成するアクセス許可を付与します	書き込み	schema*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutResourcePolicy	リソースベースのポリシーを特定のレジストリにアタッチするアクセス許可を付与します	書き込み	registry*		
SearchSchemas	アカウント内の指定したキーワードに基づいてスキーマを検索するアクセス許可を付与します	リスト	schema*		
StartDiscoverer	指定された Discoverer を開始するアクセス許可を付与します。開始すると、Discoverer は発行されたイベントのスキーマをアカウントで設定されたソースに自動的に登録します。	書き込み	discoverer*		
StopDiscoverer	指定した Discoverer を停止するアクセス許可を付与します。停止すると、Discoverer は発行されたイベントのスキーマをアカウントで設定されたソースに自動的に登録しなくなります	書き込み	discoverer*		
TagResource	リソースにタグを付けるアクセス許可を付与	Tagging	discoverer		
			registry		
			schema		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	リソースからタグを削除する許可を付与	Tagging	discoverer		
			registry		
			schema		
				aws:TagKeys	
UpdateDiscoverer	アカウント内の既存の Discoverer を更新するアクセス許可を付与します	書き込み	discoverer*		
UpdateRegistry	アカウント内の既存のレジストリメタデータを更新するアクセス許可を付与します	書き込み	registry*		
UpdateSchema	アカウント内の既存のスキーマを更新するアクセス許可を付与します	書き込み	schema*		

Amazon EventBridge スキーマで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
discoverer	arn:${Partition}:schemas:${Region}:${Account}:discoverer/${DiscovererId}	aws:ResourceTag/${TagKey}
registry	arn:${Partition}:schemas:${Region}:${Account}:registry/${RegistryName}	aws:ResourceTag/${TagKey}
schema	arn:${Partition}:schemas:${Region}:${Account}:schema/${RegistryName}/${SchemaName}	aws:ResourceTag/${TagKey}

Amazon EventBridge スキーマの条件キー

Amazon EventBridge スキーマでは、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	各タグの許可された値のセットでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値でアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内の必須タグの存在でアクセスをフィルタリングします	ArrayOfString

AWS Fault Injection Service のアクション、リソース、および条件キー

AWS Fault Injection Service (サービスプレフィックス: fis) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Fault Injection Service によって定義されたアクション
- AWS Fault Injection Service で定義されるリソースタイプ
- AWS Fault Injection Service の条件キー

AWS Fault Injection Service によって定義されたアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateExperimentTemplate	FIS AWS 実験テンプレートを作成するアクセス許可を付与します	書き込み	action*		
			experiment-template*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateTargetAccountConfiguration	FIS AWS ターゲットアカウント設定を作成するアクセス許可を付与します	書き込み	experiment-template*		
DeleteExperimentTemplate	FIS AWS 実験テンプレートを削除するアクセス許可を付与します	書き込み	experiment-template*		
DeleteTargetAccountConfiguration	FIS AWS ターゲットアカウント設定を削除するアクセス許可を付与します	書き込み	experiment-template*		
GetAction	FIS AWS アクションを取得するアクセス許可を付与します	読み取り	action*		
				aws:ResourceTag/${TagKey}	
GetExperiment	FIS AWS 実験を取得する許可を付与	読み取り	experiment*		
				aws:ResourceTag/${TagKey}	
GetExperimentTargetAccountConfiguration	FIS AWS 実験の FIS AWS ターゲットアカウント設定を取得するアクセス許可を付与します	読み取り	experiment*		
GetExperimentTemplate	FIS AWS 実験テンプレートを取得するアクセス許可を付与します	読み取り	experiment-template*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
GetSafetyLever	安全レバーに関する情報を取得する許可を付与する	読み取り	safety-lever*		
GetTargetAccountConfiguration	FIS AWS 実験テンプレートの FIS AWS ターゲットアカウント設定を取得するアクセス許可を付与します	読み取り	experiment-template*		
GetTargetResourceType	指定されたリソースタイプに関する情報を取得する許可を付与	読み取り			
InjectApiInternalError [許可のみ]	FIS Experiment から提供された AWS サービスに API 内部エラーを挿入するアクセス許可を付与します	書き込み	experiment*		
				fis:Service fis:Operations fis:Percentage fis:Targets	
InjectApiThrottleError [アクセス許可のみ]	FIS Experiment から提供された AWS サービスに API スロットルエラーを挿入するアクセス許可を付与します	書き込み	experiment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				fis:Service fis:Operations fis:Percentage fis:Targets	
InjectApiUnavailableError [アクセス許可のみ]	FIS 実験から提供された AWS サービスに API 使用不可エラーを挿入するアクセス許可を付与します	書き込み	experiment*		
				fis:Service fis:Operations fis:Percentage fis:Targets	
ListActions	使用可能なすべての FIS AWS アクションを一覧表示するアクセス許可を付与します	リスト			
ListExperimentResolvedTargets	FIS AWS 実験の解決済みターゲットを一覧表示するアクセス許可を付与します	リスト	experiment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListExperimentTargetAccountConfigurations	FIS AWS 実験のターゲットアカウント設定を一覧表示するアクセス許可を付与します	リスト	experiment*		
ListExperimentTemplates	使用可能なすべての FIS AWS 実験テンプレートを一覧表示するアクセス許可を付与します	リスト			
ListExperiments	使用可能なすべての FIS AWS 実験を一覧表示するアクセス許可を付与します	リスト			
ListTagsForResource	FIS AWS リソースのタグを一覧表示するアクセス許可を付与します	読み取り	action		
			experiment		
			experiment-template		
ListTargetAccountConfigurations	FIS AWS 実験テンプレートのターゲットアカウント設定を一覧表示する許可を付与	リスト	experiment-template*		
ListTargetResourceTypes	リソースタイプのタグを一覧表示する許可を付与	リスト			
StartExperiment	FIS AWS 実験を実行するアクセス許可を付与します	書き込み	experiment*		iam:CreateServiceLinkedRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			experiment-template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StopExperiment	FIS AWS 実験を停止するアクセス許可を付与します	書き込み	experiment*		
TagResource	FIS AWS リソースにタグを付けるアクセス許可を付与します	Tagging	action		
			experiment		
			experiment-template		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	FIS AWS リソースのタグを解除するアクセス許可を付与します	Tagging	action		
			experiment		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			experiment-template		
				aws:TagKeys	
UpdateExperimentTemplate	指定された FIS AWS 実験テンプレートを更新する許可を付与	書き込み	experiment-template*		
			action		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateSafetyLeverState	安全レバーの状態を更新する許可を付与する	書き込み	safety-lever*		
UpdateTargetAccountConfiguration	FIS AWS ターゲットアカウント設定を更新する許可を付与	書き込み	experiment-template*		

AWS Fault Injection Service で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
action	arn:${Partition}:fis:${Region}:${Account}:action/${Id}	aws:ResourceTag/${TagKey}
experiment	arn:${Partition}:fis:${Region}:${Account}:experiment/${Id}	aws:ResourceTag/${TagKey}
experiment-template	arn:${Partition}:fis:${Region}:${Account}:experiment-template/${Id}	aws:ResourceTag/${TagKey}
safety-lever	arn:${Partition}:fis:${Region}:${Account}:safety-lever/${Id}	

AWS Fault Injection Service の条件キー

AWS Fault Injection Service は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString

条件キー	説明	タイプ
fis:Operations	FIS AWS アクションの影響を受ける AWS サービスのオペレーションのリストでアクセスをフィルタリングします	ArrayOfString
fis:Percentage	FIS AWS アクションの影響を受けるコールの割合でアクセスをフィルタリングします	数値
fis:Service	FIS AWS アクションの影響を受ける AWS サービスによってアクセスをフィルタリングします	String
fis:Targets	FIS アクションの対象となるリソース ARNs AWS のリストでアクセスをフィルタリングします	ArrayOfString

Amazon FinSpace のアクション、リソース、および条件キー

Amazon FinSpace (サービスプレフィックス: `finspace`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon FinSpace で定義されるアクション
- Amazon FinSpace で定義されるリソースタイプ
- Amazon FinSpace の条件キー

Amazon FinSpace で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ConnectKxCluster [アクセス許可のみ]	KDB クラスターに接続する許可を付与	書き込み	kxCluster*		
CreateEnvironment	FinSpace 環境を作成する許可を付与	書き込み	environment*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxChangeset	KDB データベース用の変更セットを作成する許可を付与	書き込み	kxDatabase*		
CreateKxCluster	マネージド型の KDB 環境でクラスターを作成する許可を付与	書き込み	kxCluster*		ec2:DescribeSubnets finspace:MountKxDatabase
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateKxDatabase	マネージド型の KDB 環境で KDB データベースを作成する許可を付与	書き込み	kxDatabase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxDataview	マネージド型の KDB 環境でデータビューを作成する許可を付与	書き込み	kxDataview*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxEnvironment	マネージド型の KDB 環境を作成する許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxScalingGroup	マネージド型の KDB 環境でスケールしたグループを作成する許可を付与	書き込み	kxScalingGroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxUser	マネージド型の KDB 環境でユーザーを作成する許可を付与	書き込み	kxEnvironment*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxVolume	マネージド型の KDB 環境でボリュームを作成する許可を付与	書き込み	kxVolume*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateUser	FinSpace ユーザーを作成する許可を付与	書き込み	environment*		
			user*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteEnvironment	FinSpace 環境を削除する許可を付与	書き込み	environment*		
DeleteKxCluster	KDB クラスターを削除する許可を付与	書き込み	kxCluster*		
DeleteKxClusterNode	KDB クラスターからノードを削除する許可を付与する	書き込み	kxCluster*		
DeleteKxDatabase	KDB データベースを削除する許可を付与	書き込み	kxDatabase*		
DeleteKxDataview	マネージド型の KDB 環境でデータビューを削除する許可を付与	書き込み	kxDataview*		
DeleteKxEnvironment	マネージド型の KDB 環境を削除する許可を付与	書き込み	kxEnvironment*		
DeleteKxScalingGroup	マネージド型の KDB 環境でスケールしたグループを削除する許可を付与	書き込み	kxScalingGroup*		
DeleteKxUser	KDB ユーザーを削除する許可を付与	書き込み	kxUser*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteKxVolume	マネージド型の KDB 環境でボリュームを削除する許可を付与	書き込み	kxVolume*		
GetEnvironment	FinSpace 環境の詳細を取得する許可を付与	読み取り	environment*		
GetKxChangeset	KDB データベースの変更セットを記述する許可を付与	読み取り	kxDatabase*		
GetKxCluster	マネージド型の KDB 環境でクラスターを記述する許可を付与	読み取り	kxCluster*		
GetKxConnectionString	KDB クラスターの接続文字列を取得する許可を付与	読み取り	kxCluster*		finspace:ConnectKxCluster
GetKxDatabase	KDB データベースを記述する許可を付与	読み取り	kxDatabase*		
GetKxDataview	マネージド型の KDB 環境でデータビューを記述する許可を付与	読み取り	kxDataview*		
GetKxEnvironment	マネージド型の KDB 環境を記述する許可を付与	読み取り	kxEnvironment*		
GetKxScalingGroup	マネージド型の KDB 環境でスケールしたグループを記述する許可を付与	読み取り	kxScalingGroup*		
GetKxUser	KDB ユーザーを記述する許可を付与	読み取り	kxUser*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetKxVolume	マネージド型の KDB 環境でボリュームを記述する許可を付与	読み取り	kxVolume*		
GetLoadSampleDataSetGroupIntoEnvironmentStatus	サンプルデータバンドルのロードのステータスをリクエストする許可を付与	読み取り	environment*		
GetUser	FinSpace ユーザーの詳細を取得する許可を付与	読み取り	environment*		
			user*		
ListEnvironments	で FinSpace 環境を一覧表示するアクセス許可を付与します AWS アカウント	リスト	environment*		
ListKxChangesets	KDB データベース用の変更セットを一覧表示する許可を付与	リスト	kxDatabase*		
ListKxClusterNodes	マネージド型の KDB 環境でクラスターノードを一覧表示する許可を付与	リスト	kxCluster*		
ListKxClusters	マネージド型の KDB 環境でクラスターを一覧表示する許可を付与	リスト	kxEnvironment*		
ListKxDatabases	マネージド型の KDB 環境で KDB データベースを一覧表示する許可を付与	リスト	kxEnvironment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListKxDataviews	データベース内のデータビューを一覧表示する許可を付与	リスト	kxDatabase*		
ListKxEnvironments	マネージド型の KDB 環境を一覧表示する許可を付与	リスト			
ListKxScalingGroups	マネージド型の KDB 環境でスケールしたグループを一覧表示する許可を付与	リスト	kxEnvironment*		
ListKxUsers	マネージド型の KDB 環境でユーザーを一覧表示する許可を付与	リスト	kxEnvironment*		
ListKxVolumes	マネージド型の KDB 環境でボリュームを一覧表示する許可を付与	リスト	kxEnvironment*		
ListTagsForResource	リソースのタグのリストを返す許可を付与	リスト	environment*		
			kxCluster*		
			kxDatabase*		
			kxDataview*		
			kxEnvironment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			kxScalingGroup*		
			kxUser*		
			kxVolume*		
ListUsers	環境内の FinSpace ユーザーを一覧表示する許可を付与	リスト	environment*		
			user*		
LoadSampleDataSetGroupIntoEnvironment	FinSpace 環境にサンプルデータバンドルをロードする許可を付与	書き込み	environment*		
MountKxDatabase [アクセス許可のみ]	データベースを KDB クラスターにマウントする許可を付与	書き込み	kxDatabase*		
ResetUserPassword	FinSpace ユーザーのパスワードをリセットする許可を付与	書き込み	environment*		
			user*		
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	environment		
			kxCluster		
			kxDatabase		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			kxDataview		
			kxEnvironment		
			kxScalingGroup		
			kxUser		
			kxVolume		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	リソースのタグを解除する許可を付与	Tagging	environment		
			kxCluster		
			kxDatabase		
			kxDataview		
			kxEnvironment		
			kxScalingGroup		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			kxUser		
			kxVolume		
				aws:TagKeys	
UpdateEnvironment	FinSpace 環境を更新する許可を付与	書き込み	environment*		
UpdateKxClusterCodeConfiguration	マネージド KDB 環境でクラスターのコード設定を更新する許可を付与	書き込み	kxCluster*		
UpdateKxClusterDatabases	マネージド型の KDB 環境でクラスターのデータベースを更新する許可を付与	書き込み	kxCluster*		
UpdateKxDatabase	KDB データベースを更新する許可を付与	書き込み	kxDatabase*		
UpdateKxDataview	マネージド型の KDB 環境でデータビューを更新する許可を付与	書き込み	kxDataview*		
UpdateKxEnvironment	マネージド型の KDB 環境を更新する許可を付与	書き込み	kxEnvironment*		
UpdateKxEnvironmentNetwork	マネージド型の KDB 環境のネットワークを更新する許可を付与	書き込み	kxEnvironment*		
UpdateKxUser	KDB ユーザーを更新する許可を付与	書き込み	kxUser*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateKxVolume	マネージド型の KDB 環境でボリュームを更新する許可を付与	書き込み	kxVolume*		
UpdateUser	FinSpace ユーザーを更新する許可を付与	書き込み	environment*		
			user*		

Amazon FinSpace で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
environment	arn:${Partition}:finspace:${Region}:${Account}:environment/${EnvironmentId}	aws:ResourceTag/${TagKey}
user	arn:${Partition}:finspace:${Region}:${Account}:user/${UserId}	aws:ResourceTag/${TagKey}
kxEnvironment	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
kxUser	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxUser/${UserName}	aws:ResourceTag/${TagKey}
kxCluster	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxCluster/${KxCluster}	aws:ResourceTag/${TagKey}
kxDatabase	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxDatabase/${KxDatabase}	aws:ResourceTag/${TagKey}
kxScalingGroup	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxScalingGroup/${KxScalingGroup}	aws:ResourceTag/${TagKey}
kxDataview	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxDatabase/${KxDatabase}/kxDataview/${KxDataview}	aws:ResourceTag/${TagKey}
kxVolume	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxVolume/${KxVolume}	aws:ResourceTag/${TagKey}

Amazon FinSpace の条件キー

Amazon FinSpace は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

Amazon FinSpace API のアクション、リソース、および条件キー

Amazon FinSpace API (サービスプレフィックス: `finspace-api`) は、IAM 許可ポリシーで使用する次のサービス固有のリソース、アクション、および条件コンテキストキーを提供します。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon FinSpace API で定義されるアクション
- Amazon FinSpace API で定義されるリソースタイプ
- Amazon FinSpace API の条件キー

Amazon FinSpace API で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーショ

ンへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetProgrammaticAccessCredentials	FinSpace のプログラムによるアクセス認証情報を取得するための許可を付与します	読み取り	credential*		

Amazon FinSpace API で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
credential	arn:${Partition}:finspace-api:${Region}:${Account}:/credentials/programmatic	

Amazon FinSpace API の条件キー

FinSpace API には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Firewall Manager のアクション、リソース、および条件キー

AWS Firewall Manager (サービスプレフィックス: fms) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Firewall Manager で定義されるアクション
- AWS Firewall Manager で定義されるリソースタイプ
- AWS Firewall Manager の条件キー

AWS Firewall Manager で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateAdminAccount	AWS Firewall Manager 管理者アカウントを設定するアクセス許可を付与し、すべての組織アカウントでサービスを有効にします	書き込み			
AssociateThirdPartyFirewall	Firewall Manager 管理者を、サードパーティーのファイアウォールサービスのテナント管理者として設定するアクセス許可を付与します	書き込み			
BatchAssociateResource	AWS Firewall Manager リソースセットにリソースを関連付ける許可を付与	書き込み	resource-set*		
BatchDisassociateResource	AWS Firewall Manager リソースセットからリソースの関連付けを解除する許可を付与	書き込み	resource-set*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteAppsList	AWS Firewall Manager アプリケーションリストを完全に削除するアクセス許可を付与します	書き込み	applications-list*		
DeleteNotificationChannel	組織全体の主要な FM イベントとエラーを FM 管理者に通知するために使用される IAM ロールと Amazon Simple Notification Service (SNS) トピックとの AWS Firewall Manager の関連付けを削除するアクセス許可を付与します	書き込み			
DeletePolicy	AWS Firewall Manager ポリシーを完全に削除するアクセス許可を付与します	書き込み	policy*		
				aws:ResourceTag/${TagKey}	
DeleteProtocolsList	AWS Firewall Manager プロトコルリストを完全に削除するアクセス許可を付与します	書き込み	protocols-list*		
DeleteResourceSet	AWS Firewall Manager リソースセットを完全に削除するアクセス許可を付与します	書き込み	resource-set*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisassociateAdminAccount	AWS Firewall Manager 管理者アカウントとして設定されたアカウントの関連付けを解除するアクセス許可を付与し、すべての組織アカウントのサービスを無効にします	書き込み			
DisassociateThirdPartyFirewall	Firewall Manager 管理者とサードパーティのファイアウォールテナントとの関連付けを解除するアクセス許可を付与します	書き込み			
GetAdminAccount	Firewall Manager 管理者として AWS Firewall Manager に関連付けられている AWS Organizations AWS アカウントを返す許可を付与	読み取り			
GetAdminScope	指定されたアカウントの管理者の権限適用範囲に関する情報を返す許可を付与します	読み取り			
GetAppsList	指定された AWS Firewall Manager アプリケーションリストに関する情報を返すアクセス許可を付与します	読み取り	applications-list*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetComplianceDetail	指定されたメンバーアカウントについての詳細なコンプライアンス情報を取得する許可を付与。詳細には、指定されたポリシーに準拠しているかどうかにかかわらず、リソースが含まれます	読み取り	policy*		
GetNotificationChannel	AWS Firewall Manager SNS ログの記録に使用される Amazon Simple Notification Service (SNS) トピックに関する情報を取得する許可を付与	読み取り			
GetPolicy	指定された AWS Firewall Manager ポリシーに関する情報を取得するアクセス許可を付与します	読み取り	policy*		
GetProtectionStatus	DDoS 攻撃の可能性が発生した場合に、ポリシーレベルの攻撃概要情報を取得する許可を付与	読み取り	policy*		
GetProtocolsList	指定された AWS Firewall Manager プロトコルリストに関する情報を返すアクセス許可を付与します	読み取り	protocols-list*		
GetResourceSet	指定された AWS Firewall Manager リソースセットに関する情報を取得するアクセス許可を付与します	読み取り	resource-set*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetThirdPartyFirewallAssociationStatus	サードパーティーのファイアウォールベンダーのテナントに Firewall Manager 管理者アカウントのオンボーディングステータスを取得するアクセス許可を付与します	読み取り			
GetViolationDetails	指定された AWS Firewall Manager ポリシーと AWS アカウント	読み取り	policy*		
ListAdminAccountsForOrganization	AssociateAdminAccount によって Firewall Manager にオンボーディングされた組織内の Firewall Manager 管理者を一覧表示する AdminAccounts オブジェクトを返す許可を付与します	リスト			
ListAdminsManagingAccount	指定された AWS Organizations メンバーアカウントを管理しているアカウントを一覧表示するアクセス許可を付与します	リスト			
ListAppsLists	AppsListDataSummary オブジェクトの配列を返すアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListComplianceStatus	レスポンス内の PolicyComplianceStatus オブジェクトの配列を取得する許可を付与。PolicyComplianceStatus を使用して、指定されたポリシーによって保護されているメンバーアカウントの概要を取得します	リスト	policy*		
ListDiscoveredResources	リソースセットに関連付けることのできる組織アカウント内のリソースの配列を取得する許可を付与	リスト			
ListMemberAccounts	発信者が FMS 管理者アカウントの場合、メンバーアカウント ID の配列を取得するためのアクセス許可を付与します	リスト			
ListPolicies	レスポンス内の PolicySummary オブジェクトの配列を取得する許可を付与。	リスト			
ListProtocolsLists	ProtocolsListDataSummary オブジェクトの配列を返すアクセス許可を付与します	リスト			
ListResourceSetResources	リソースセットに現在関連付けられているリソースの配列を取得する許可を付与	リスト	resource-set*		
ListResourceSets	ResourceSetSummary オブジェクトの配列を取得する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み込み	policy*		
ListThirdPartyFirewallFirewallPolicies	サードパーティーのファイアウォール管理者のアカウントに関連付けられているすべてのサードパーティー製ファイアウォールポリシーのリストを取得するアクセス許可を付与します	リスト			
PutAdminAccount	Firewall Manager 管理者アカウントを作成または更新する許可を付与します	書き込み			
PutAppsList	AWS Firewall Manager アプリケーションリストを作成する許可を付与	書き込み	applications-list*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutNotificationChannel	AWS Firewall Manager (FM) が FM 管理者に組織全体の主要な FM イベントとエラーを通知するために使用できる IAM ロールと Amazon Simple Notification Service (SNS) トピックを指定するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutPolicy	AWS Firewall Manager ポリシーを作成するアクセス許可を付与します	書き込み	policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutProtocolsList	AWS Firewall Manager プロトコルリストを作成するアクセス許可を付与します	書き込み	protocols-list*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutResourceSet	AWS Firewall Manager リソースセットを作成するアクセス許可を付与します	書き込み	resource-set*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	リソースにタグを追加する許可を付与	タグ付け	applications-list		
			policy		
			protocols-list		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			resource-set		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	タグ付け	applications-list		
			policy		
			protocols-list		
			resource-set		
				aws:TagKeys	

AWS Firewall Manager で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
policy	arn:${Partition}:fms:${Region}:${Account}:policy/${Id}	aws:ResourceTag/${TagKey}
applications-list	arn:${Partition}:fms:${Region}:${Account}:applications-list/${Id}	aws:ResourceTag/${TagKey}
protocols-list	arn:${Partition}:fms:${Region}:${Account}:protocols-list/${Id}	aws:ResourceTag/${TagKey}
resource-set	arn:${Partition}:fms:${Region}:${Account}:resource-set/${Id}	aws:ResourceTag/${TagKey}

AWS Firewall Manager の条件キー

AWS Firewall Manager は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングする	ArrayOfString

Amazon Forecast のアクション、リソース、および条件キー

Amazon Forecast (サービスプレフィックス: `forecast`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Forecast で定義されるアクション
- Amazon Forecast で定義されるリソースタイプ
- Amazon Forecast の条件キー

Amazon Forecast で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateAutoPredictor	自動予測子を作成するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	データセットを作成する許可を付与	書き込み	dataset*	aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
CreateDatasetGroup	データセットグループを無効にするアクセス許可を付与	書き込み	datasetGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatasetImportJob	データセットインポートジョブを作成するアクセス許可を付与	書き込み	datasetImportJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExplainability	説明可能性を作成するアクセス許可を付与	書き込み	forecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExplainabilityExport	説明可能性のリソースを使用して説明可能性のエクスポートを作成するアクセス許可を付与	書き込み	explainability*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateForecast	予測を作成するアクセス許可を付与	書き込み	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateForecastEndpoint [アクセス許可のみ]	Predictor リソースを使用してエンドポイントを作成するアクセス許可を付与	書き込み	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateForecastExportJob	予測リソースを使用して予測エクスポートジョブを作成するアクセス許可を付与	書き込み	forecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMonitor		書き込み	predictor*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	Predictor リソースを使用してモニターを作成するアクセス許可を付与			aws:RequestTag/${TagKey} aws:TagKeys	
CreatePredictor	予測子を作成するアクセス許可を付与	書き込み	datasetGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePredictorBacktestExportJob	予測子を使用して予測子バックテストエクスポートジョブを作成するアクセス許可を付与	書き込み	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWhatIfAnalysis	What-If 分析を作成するアクセス許可を付与	書き込み	forecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateWhatIfForecast	What-If 予測を作成するアクセス許可を付与	書き込み	whatIfAnalysis*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWhatIfForecastExport	What-If 予測リソースを使用して What-If 予測エクスポートを作成するアクセス許可を付与	書き込み	whatIfForecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDataset	データセットを削除する許可を付与	書き込み	dataset*		
DeleteDatasetGroup	データセットグループを削除するアクセス許可を付与	書き込み	datasetGroup*		
DeleteDatasetImportJob	データセットインポートジョブを削除するアクセス許可を付与	書き込み	datasetImportJob*		
DeleteExplainability	期限切れの予約を削除する許可を付与。	書き込み	explainability*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteExplainabilityExport	既存のエクスポートを削除する許可を付与	書き込み	explainabilityExport*		
DeleteForecast	予測を削除するアクセス許可を付与	書き込み	forecast*		
DeleteForecastEndpoint [アクセス許可のみ]	エンドポイントリソースを削除するアクセス許可を付与	書き込み	endpoint*		
DeleteForecastExportJob	予測エクスポートジョブを削除するアクセス許可を付与	書き込み	forecastExport*		
DeleteMonitor	モニターリソースを削除するアクセス許可を付与	書き込み	monitor*		
DeletePredictor	予測子を削除するアクセス許可を付与	書き込み	predictor*		
DeletePredictorBacktestExportJob	予測子バックテストエクスポートジョブを削除するアクセス許可を付与	書き込み	predictorBacktestExportJob*		
DeleteResourceTree	リソースとその子リソースを削除するためのアクセス許可を付与	書き込み	dataset*		
			datasetGroup*		
			datasetImportJob*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			endpoint*		
			explainability*		
			explainabilityExport*		
			forecast*		
			forecastExport*		
			monitor*		
			predictor*		
			predictorBacktestExportJob*		
			whatIfAnalysis*		
			whatIfForecast*		
			whatIfForecastExport*		
DeleteWhatIfAnalysis	What-If 分析を削除するアクセス許可を付与	書き込み	whatIfAnalysis*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteWhatIfForecast	What-If 予測を削除するアクセス許可を付与	書き込み	whatIfForecast*		
DeleteWhatIfForecastExport	What-If 予測エクスポートを削除するアクセス許可を付与	書き込み	whatIfForecastExport*		
DescribeAutoPredictor	自動予測子を記述するアクセス許可を付与	読み込み	predictor*		
DescribeDataset	データセットを記述するアクセス許可を付与	読み込み	dataset*		
DescribeDatasetGroup	データセットグループを記述するアクセス許可を付与	読み込み	datasetGroup*		
DescribeDatasetImportJob	データセットインポートジョブを記述するアクセス許可を付与	読み込み	datasetImportJob*		
DescribeExplainability	説明可能性を記述するアクセス許可を付与	読み込み	explainability*		
DescribeExplainabilityExport	説明可能性エクスポートを記述するアクセス許可を付与	読み込み	explainabilityExport*		
DescribeForecast	予測を記述するアクセス許可を付与	読み取り	forecast*		
DescribeForecastEndpoint [許可のみ]	エンドポイントリソースを記述するアクセス許可を付与	読み取り	endpoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeForecastExportJob	予測エクスポートジョブを記述するアクセス許可を付与	読み取り	forecastExport*		
DescribeMonitor	モニターリソースを記述するアクセス許可を付与	読み取り	monitor*		
DescribePredictor	予測子を記述するアクセス許可を付与	読み込み	predictor*		
DescribePredictorBacktestExportJob	予測子バックテストエクスポートジョブを記述するアクセス許可を付与	読み取り	predictorBacktestExportJob*		
DescribeWhatIfAnalysis	What-If 分析を記述するアクセス許可を付与	読み取り	whatIfAnalysis*		
DescribeWhatIfForecast	What-If 予測を記述するアクセス許可を付与	読み取り	whatIfForecast*		
DescribeWhatIfForecastExport	What-If 予測エクスポートを記述するアクセス許可を付与	読み取り	whatIfForecastExport*		
GetAccuracyMetrics	予測子の精度メトリクスを取得するアクセス許可を付与	読み取り	predictor*		
GetRecentForecastContext [許可のみ]	エンドポイントの時系列の予測コンテキストを取得するアクセス許可を付与	読み取り	endpoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
InvokeForecastEndpoint [許可のみ]	エンドポイントを呼び出して時系列の予測を取得するアクセス許可を付与	読み取り	endpoint*		
ListDatasetGroups	すべてのデータセットグループを一覧表示するアクセス許可を付与	読み込み			
ListDatasetImportJobs	すべてのデータセットインポートジョブを一覧表示するアクセス許可を付与	読み込み			
ListDatasets	すべてのデータセットを一覧表示するアクセス許可を付与	読み込み			
ListExplainabilities	すべての説明可能性を一覧表示するアクセス許可を付与	読み込み			
ListExplainabilityExports	すべての説明可能性を一覧表示するアクセス許可を付与	読み込み			
ListForecastExportJobs	すべての予測エクスポートジョブを一覧表示するアクセス許可を付与	読み込み			
ListForecasts	すべての予測を一覧表示するアクセス許可を付与	読み取り			
ListMonitorEvaluations	モニターのすべてのモニター評価結果を一覧表示するアクセス許可を付与	読み取り	monitor*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListMonitors	すべてのモニターリソースを一覧表示するアクセス許可を付与	読み取り			
ListPredictorBacktestExportJobs	すべての予測子バックテストエクスポートジョブを一覧表示するアクセス許可を付与	読み込み			
ListPredictors	すべての予測子を一覧表示するアクセス許可を付与	読み込み			
ListTagsForResource	Amazon Forecast リソースのタグを一覧表示するアクセス許可を付与	読み取り	dataset		
			datasetGroup		
			datasetImportJob		
			endpoint		
			explainability		
			explainabilityExport		
			forecast		
			forecastExport		
			monitor		
			predictor		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			predictorBacktestExportJob		
			whatIfAnalysis		
			whatIfForecast		
			whatIfForecastExport		
ListWhatIfAnalyses	すべての What-If 分析を一覧表示するアクセス許可を付与	読み取り			
ListWhatIfForecastExports	すべての What-If 予測エクスポートを一覧表示するアクセス許可を付与	読み取り			
ListWhatIfForecasts	すべての What-If 予測を一覧表示するアクセス許可を付与	読み取り			
QueryForecast	単一項目に関する予測を取得するアクセス許可を付与	読み取り	forecast*		
QueryWhatIfForecast	単一項目に関する What-If 予測を取得するアクセス許可を付与	読み取り	whatIfForecast*		
ResumeResource	Amazon Forecast リソースジョブを再開するアクセス許可を付与	書き込み	monitor*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
StopResource	Amazon Forecast リソースジョブを停止するアクセス許可を付与	書き込み	datasetImportJob*		
			endpoint*		
			explainability*		
			explainabilityExport*		
			forecast*		
			forecastExport*		
			monitor*		
			predictor*		
			predictorBacktestExportJob*		
			whatIfAnalysis*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			whatIfForecast*		
			whatIfForecastExport*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	指定されたタグをリソースに関連付けるアクセス許可を付与	タグ付け	dataset		
			datasetGroup		
			datasetImportJob		
			endpoint		
			explainability		
			explainabilityExport		
			forecast		
			forecastExport		
			monitor		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			predictor		
			predictorBacktestExportJob		
			whatIfAnalysis		
			whatIfForecast		
			whatIfForecastExport		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースについて指定されたタグを削除するアクセス許可を付与	タグ付け	dataset		
			datasetGroup		
			datasetImportJob		
			endpoint		
			explainability		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			explainabilityExport		
			forecast		
			forecastExport		
			monitor		
			predictor		
			predictorBacktestExportJob		
			whatIfAnalysis		
			whatIfForecast		
			whatIfForecastExport		
				aws:TagKeys	
UpdateDatasetGroup	データセットを更新するアクセス許可を付与	書き込み	dataset*		
			datasetGroup*		

Amazon Forecast で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
dataset	arn:${Partition}:forecast:${Region}:${Account}:dataset/${ResourceId}	aws:ResourceTag/${TagKey}
datasetGroup	arn:${Partition}:forecast:${Region}:${Account}:dataset-group/${ResourceId}	aws:ResourceTag/${TagKey}
datasetImportJob	arn:${Partition}:forecast:${Region}:${Account}:dataset-import-job/${ResourceId}	aws:ResourceTag/${TagKey}
algorithm	arn:${Partition}:forecast:::algorithm/${ResourceId}	
predictor	arn:${Partition}:forecast:${Region}:${Account}:predictor/${ResourceId}	aws:ResourceTag/${TagKey}
predictorBacktestExportJob	arn:${Partition}:forecast:${Region}:${Account}:predictor-backtest-export-job/${ResourceId}	aws:ResourceTag/${TagKey}
forecast	arn:${Partition}:forecast:${Region}:${Account}:forecast/${ResourceId}	aws:ResourceTag/${TagKey}
forecastExport	arn:${Partition}:forecast:${Region}:${Account}:forecast-export-job/${ResourceId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
explainability	arn:${Partition}:forecast:${Region}:${Account}:explainability/${ResourceId}	aws:ResourceTag/${TagKey}
explainabilityExport	arn:${Partition}:forecast:${Region}:${Account}:explainability-export/${ResourceId}	aws:ResourceTag/${TagKey}
monitor	arn:${Partition}:forecast:${Region}:${Account}:monitor/${ResourceId}	aws:ResourceTag/${TagKey}
whatIfAnalysis	arn:${Partition}:forecast:${Region}:${Account}:what-if-analysis/${ResourceId}	aws:ResourceTag/${TagKey}
whatIfForecast	arn:${Partition}:forecast:${Region}:${Account}:what-if-forecast/${ResourceId}	aws:ResourceTag/${TagKey}
whatIfForecastExport	arn:${Partition}:forecast:${Region}:${Account}:what-if-forecast-export/${ResourceId}	aws:ResourceTag/${TagKey}
endpoint	arn:${Partition}:forecast:${Region}:${Account}:forecast-endpoint/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon Forecast の条件キー

Amazon Forecast では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon Fraud Detector のアクション、リソース、および条件キー

Amazon Fraud Detector (サービスプレフィックス: `frauddetector`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Fraud Detector で定義されるアクション
- Amazon Fraud Detector で定義されるリソースタイプ
- Amazon Fraud Detector の条件キー

Amazon Fraud Detector で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchCreateVariable	変数のバッチを作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
BatchGetVariable	変数のバッチを取得する許可を付与。	リスト	variable*		
CancelBatchImportJob	指定されたバッチインポートジョブをキャンセルするためのアクセス許可を付与する	書き込み	batch-import*		
CancelBatchPredictionJob	指定したバッチ予測ジョブをキャンセルする許可を付与。	書き込み	batch-prediction*		
CreateBatchImportJob	バッチインポートジョブを作成するためのアクセス許可を付与する	書き込み	batch-import*		
			event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBatchPredictionJob	バッチ予測ジョブを作成する許可を付与。	書き込み	batch-prediction*		
			detector*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			detector-version*		
			event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDetectorVersion	ディテクターのバージョンを作成する許可を付与。ディテクターのバージョンは DRAFT ステータスで開始されます。	書き込み	detector*		
			external-model		
			model-version		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateList	リストを作成するためのアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateModel	指定されたモデルタイプを使用してモデルを作成する許可を付与。	書き込み	event-type*		
			model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelVersion	指定されたモデルタイプとモデル ID を使用してモデルのバージョンを作成する許可を付与。	書き込み	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRule	指定されたディテクターで使用するルールを作成する許可を付与。	書き込み	detector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVariable	変数を作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteBatchImportJob	バッチインポートジョブを削除するためのアクセス許可を付与する	書き込み	batch-import*		
DeleteBatchPredictionJob	バッチ予測ジョブを削除する許可を付与。	書き込み	batch-prediction*		
DeleteDetector	ディテクターを削除する許可を付与。ディテクターを削除する前に、ディテクターに関連付けられたすべてのディテクターバージョンとルールバージョンを削除する必要があります。	書き込み	detector*		
DeleteDetectorVersion	ディテクターのバージョンを削除する許可を付与。ステータスが ACTIVE のディテクターバージョンは削除できません。	書き込み	detector-version*		
DeleteEntityType	エンティティタイプを削除する許可を付与。イベントタイプに含まれているエンティティタイプは削除できません。	書き込み	entity-type*		
DeleteEvent	指定されたイベントを削除する許可を付与。	書き込み	event-type*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteEventType	イベントタイプを削除する許可を付与。ディテクターまたはモデルで使用されているイベントタイプは削除できません。	書き込み	event-type*		
DeleteEventsByEventType	指定されたタイプのイベントを削除するためのアクセス許可を付与する	書き込み	event-type*		
DeleteExternalModel	Amazon Fraud Detector から SageMaker モデルを削除する許可を付与。ディテクターのバージョンに関連付けられていない場合は、Amazon SageMaker モデルを削除できます。	書き込み	external-model*		
DeleteLabel	ラベルを削除する許可を付与。Amazon Fraud Detector のイベントタイプに含まれるラベルは削除できません。イベント ID に割り当てられたラベルは削除できません。まず、関連するイベント ID を削除する必要があります。	書き込み	label*		
DeleteList	リストを削除するための許可を付与します	書き込み	list*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteModel	モデルを削除する許可を付与。ディテクターのバージョンに関連付けられていない場合は、Amazon Fraud Detector でモデルとモデルバージョンを削除できます。	書き込み	model*		
DeleteModelVersion	モデルのバージョンを削除する許可を付与。ディテクターのバージョンに関連付けられていない場合は、Amazon Fraud Detector でモデルとモデルバージョンを削除できます。	書き込み	model-version*		
DeleteOutcome	結果を削除する許可を付与。ルールバージョンで使用されている結果を削除することはできません。	書き込み	outcome*		
DeleteRule	ルールを削除する許可を付与。ACTIVE または INACTIVE のディテクターバージョンで使用されている場合はルールを削除できません。	書き込み	rule*		
DeleteVariable	変数を削除する許可を付与。Amazon Fraud Detector のイベントタイプに含まれる変数は削除できません。	書き込み	variable*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeDetector	指定されたディテクターのすべてのバージョンを取得する許可を付与。	読み込み	detector*		
DescribeModelVersions	指定したモデルタイプ、または指定したモデルタイプとモデル ID のすべてのモデルバージョンを取得する許可を付与。また、指定した単一のモデルバージョンの詳細を取得することもできます。	読み取り	model-version		
GetBatchImportJobValidationReport [許可のみ]	特定のバッチインポートジョブのデータ検証レポートを取得するための許可を付与します	読み取り	batch-import*		
GetBatchImportJobs	すべてのバッチインポートジョブ、またはジョブ ID により指定した特定のジョブを、取得するためのアクセス許可を付与する	リスト	batch-import		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetBatchPredictionJobs	すべてのバッチ予測ジョブ、またはジョブ ID を指定した場合は、指定されたジョブを取得するためのアクセス許可を付与します。これはページ分割された API です。null の maxResults を指定した場合、このアクションでは、1 ページあたり最大 50 個のレコードを取得します。maxResults を指定する場合、値は 1～50 の間である必要があります。次のページの結果を取得するには、リクエストの一部として GetBatchPredictionJobsResponse からページ分割トークンを指定します。null のページ分割トークンは、最初からレコードを取得します。	リスト	batch-prediction		
GetDeleteEventsByEventTypeStatus	特定のイベントタイプでの DeleteEventsByEventType API の実行ステータスを、取得するためのアクセス許可を付与する	読み込み	event-type*		
GetDetectorVersion	特定のディテクターバージョンを取得する許可を付与。	読み込み	detector-version*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetDetectors	DetectorId が指定されている場合は、すべてのディテクター、または 1 つのディテクターを取得する許可を付与。これはページ分割された API です。null の maxResults を指定した場合、このアクションでは、1 ページあたり最大 10 個のレコードを取得します。maxResults を指定する場合、値は 5 ~ 10 の間である必要があります。次のページの結果を取得するには、リクエストの一部として GetDetectorsResponse からページ分割トークンを指定します。null のページ分割トークンは、最初からレコードを取得します。	リスト	detector		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetEntityTypes	すべてのエンティティタイプ、または名前が指定されている場合は、指定されたエンティティタイプを取得するためのアクセス許可を付与します。これはページ分割された API です。null の maxResults を指定した場合、このアクションでは、1 ページあたり最大 10 個のレコードを取得します。maxResults を指定する場合、値は 5~10 の間である必要があります。次のページの結果を取得するには、リクエストの一部として GetEntityTypesResponse からページ分割トークンを指定します。null のページ分割トークンは、最初からレコードを取得します。	リスト	entity-type		
GetEvent	指定されたイベントの詳細を取得するためのアクセス許可を付与する	読み込み	event-type*		
GetEventPrediction	ディテクターのバージョンに対してイベントを評価する許可を付与。バージョン ID が指定されていない場合は、ディテクターの (ACTIVE) バージョンが使用されます	読み取り	detector*		
			detector-version*		
			event-type*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetEventPrediction Metadata	特定の予測の詳細を取得する許可を付与	読み込み	detector*		
			detector-version*		
			event-type*		
GetEventTypes	すべてのイベントタイプ、または名前が指定されている場合は、指定されたイベントタイプを取得するためのアクセス許可を付与します。これはページ分割された API です。null の maxResults を指定した場合、このアクションでは、1 ページあたり最大 10 個のレコードを取得します。maxResults を指定する場合、値は 5～10 の間である必要があります。次のページの結果を取得するには、リクエストの一部として GetEventTypesResponse からページ分割トークンを指定します。null のページ分割トークンは、最初からレコードを取得します。	リスト	event-type		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetExternalModels	サービスにインポートされた 1 つ以上の Amazon SageMaker モデルの詳細を取得する許可を付与。これはページ分割された API です。null の maxResults を指定した場合、このアクションでは、1 ページあたり最大 10 個のレコードを取得します。maxResults を指定する場合、値は 5 ~ 10 の間である必要があります。次のページの結果を取得するには、リクエストの一部として GetExternalModelsResult からページ分割トークンを指定します。null のページ分割トークンは、最初からレコードを取得します。	リスト	external-model		
GetKMSEncryptionKey	Amazon Fraud Detector のコンテンツの暗号化に使用される Key Management Service (KMS) カスタマーマスターキー (CMK) が指定されている場合は、暗号化キーを取得する許可を付与。	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetLabels	名前が指定されている場合は、すべてのラベルまたは指定されたラベルを取得するためのアクセス許可を付与します。これはページ分割された API です。null の maxResults を指定した場合、このアクションでは、1 ページあたり最大 50 個のレコードを取得します。maxResults を指定する場合、値は 10～50 の間である必要があります。次のページの結果を取得するには、リクエストの一部として GetGetLabelsResponse からページ分割トークンを指定します。null のページ分割トークンは、最初からレコードを取得します。	リスト	label		
GetListElements	リストの要素を取得するための許可を付与します	読み取り	list*		
				aws:ResourceTag/${TagKey}	
GetListsMetadata	リストに関するメタデータを取得するための許可を付与します	リスト	list		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetModelVersion	指定されたモデルバージョンの詳細を取得する許可を付与。	読み込み	model-version*		
GetModels	1 つまたは複数のモデルを取得する許可を付与。モデルタイプがなく、モデル ID が指定されていない場合 AWS アカウント は、 のすべてのモデルを取得します。モデルタイプが指定されていてもモデル ID が指定されていない場合、AWS アカウント および モデルタイプのすべてのモデルを取得します。(モデルタイプ、モデル ID) タプルが指定されている場合は、指定されたモデルを取得します。	リスト	model		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetOutcomes	1 つ以上の結果を取得する許可を付与。これはページ分割された API です。null の maxResults を指定した場合、このアクションでは、1 ページあたり最大 100 個のレコードを取得します。maxResults を指定する場合、値は 50 ~ 100 の間である必要があります。次のページの結果を取得するには、リクエストの一部として GetOutcomesResult からページ分割トークンを指定します。null のページ分割トークンは、最初からレコードを取得します。	リスト	outcome		
GetRules	ruleID と ruleVersion が指定されていない場合は、ディテクターのすべてのルールを取得する許可を付与 (ページ分割)。ディテクタのすべてのルールと存在する場合は ruleID (ページ分割) を取得します。ruleId と ruleVersion の両方が指定されている場合は、指定されたルールを取得します。	リスト	rule		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetVariables	すべての変数または指定された変数を取得する許可を付与します。これはページ分割された API です。null の maxSizePerPage を指定すると、1 ページあたり最大 100 個のレコードを取得します。maxSizePerPage を指定する場合、値は 50 ~ 100 の間である必要があります。次のページの結果を取得するには、リクエストの一部として GetVariablesResult からページ分割トークンを指定します。null のページ分割トークンは、最初からレコードを取得します。	リスト	variable		
ListEvent Predictions	過去の予測のリストを取得する許可を付与	リスト	detector		
			detector-version		
			event-type		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTagsForResource	リソースに関連付けられたすべてのタグを一覧表示する許可を付与。これはページ分割された API です。次のページの結果を取得するには、リクエストの一部としてレスポンスからページ分割トークンを指定します。null のページ分割トークンは、最初からレコードを取得します。	読み込み	batch-import		
			batch-prediction		
			detector		
			detector-version		
			entity-type		
			event-type		
			external-model		
			label		
			list		
			model		
			model-version		
			outcome		
			rule		
			variable		
PutDetector	ディテクターを作成または更新する許可を付与	書き込み	detector*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutEntityType	エンティティタイプを作成または更新する許可を付与。エンティティは、イベントを実行しているユーザーを表します。不正予測の一部として、イベントを実行した特定のエンティティを示すエンティティ ID を渡します。エンティティタイプは、エンティティを分類します。分類の例には、お客様、マーチャント、アカウントなどがあります。	書き込み	entity-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutEventType	イベントタイプを作成または更新する許可を付与。イベントとは、不正リスクについて評価される事業活動です。Amazon Fraud Detector では、イベントの不正予測を生成します。イベントタイプは、Amazon Fraud Detector に送信されるイベントの構造を定義します。これには、イベントの一部として送信される変数、イベントを実行するエンティティ (お客様など)、イベントを分類するラベルが含まれます。イベントタイプには、オンライン支払いトランザクション、アカウント登録、認証などがあります。	書き込み	event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutExternalModel	Amazon SageMaker モデルエンドポイントを作成または更新する許可を付与。また、このアクションを使用して、IAM ロールやマッピングされた変数など、モデルのエンドポイントの設定を更新することもできます。	書き込み	event-type*		
			external-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutKMSEncryptionKey	Amazon Fraud Detector のコンテンツの暗号化に使用する Key Management Service (KMS) カスタマーマスターキー (CMK) を指定する許可を付与。	書き込み			
PutLabel	ラベルを作成または更新する許可を付与。ラベルは、イベントを不正または正当として分類します。ラベルはイベントタイプに関連付けられ、Amazon Fraud Detector で教師あり機械学習モデルをトレーニングするために使用されます。	書き込み	label*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutOutcome	結果を作成または更新する許可を付与。	書き込み	outcome*		
				aws:RequestTag/${TagKey} aws:TagKeys	
SendEvent	イベントを送信するためのアクセス許可を付与する	書き込み	event-type*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	リソースにタグを割り当てるアクセス許可を付与します。	タグ付け	batch-import		
			batch-prediction		
			detector		
			detector-version		
			entity-type		
			event-type		
			external-model		
			label		
			list		
			model		
			model-version		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			outcome		
			rule		
			variable		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	リソースからタグを削除する許可を付与	タグ付け	batch-import		
			batch-prediction		
			detector		
			detector-version		
			entity-type		
			event-type		
			external-model		
			label		
			list		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			model		
			model-version		
			outcome		
			rule		
			variable		
				aws:TagKeys	
UpdateDetectorVersion	ディテクターのバージョンを更新する許可を付与。更新できる探知器バージョン属性には、モデル、外部モデルのエンドポイント、ルール、ルール実行モードおよび説明が含まれます。DRAFT のディテクターバージョンのみを更新できます。	書き込み	detector*		
			external-model		
			model-version		
UpdateDetectorVersionMetadata	ディテクターのバージョン説明を更新する許可を付与。任意のディテクターバージョン (DRAFT、ACTIVE、または INACTIVE) のメタデータを更新できます。	書き込み	detector-version*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateDetectorVersionStatus	ディテクターのバージョンのステータスを更新する許可を付与します。UpdateDetectorVersionStatus を使用して、昇格または降格 (DRAFT から ACTIVE へ、ACTIVE から INACTIVE へ、INACTIVE から ACTIVE へ) を実行できます。	書き込み	detector-version*		
UpdateEventLabel	既存のイベントについてレコードのラベル値を更新するためのアクセス許可を付与する	書き込み	event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateList	リストを更新するためのアクセス許可を付与します	書き込み	list*		
				aws:ResourceTag/${TagKey}	
UpdateModel	モデルを更新する許可を付与。このアクションを使用して、説明属性を更新できます。	書き込み	model*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateModelVersion	モデルバージョンを更新する許可を付与。モデルバージョンを更新すると、更新されたトレーニングデータを使用して既存のモデルバージョンが再トレーニングされ、モデルの新しいマイナーバージョンが作成されます。このアクションを使用して、トレーニングデータセットの場所とデータアクセスロールの属性を更新できます。このアクションにより、モデルの新しいマイナーバージョン (バージョン 1.01、1.02、1.03 など) が作成され、トレーニングされます。	書き込み	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateModelVersionStatus	モデルバージョンのステータスを更新する許可を付与。	書き込み	model-version*		
UpdateRuleMetadata	ルールのメタデータを更新する許可を付与。説明属性は更新できます。	書き込み	rule*		
UpdateRuleVersion	ルールバージョンを更新して新しいルールバージョンを作成する許可を付与。新しいルールバージョンになるルールバージョンを更新します (バージョン 1、2、3...)。	書き込み	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateVariable	変数を更新する許可を付与。	書き込み	variable*		

Amazon Fraud Detector で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
batch-prediction	arn:${Partition}:frauddetector:${Region}:${Account}:batch-prediction/${ResourcePath}	aws:ResourceTag/${TagKey}
detector	arn:${Partition}:frauddetector:${Region}:${Account}:detector/${ResourcePath}	aws:ResourceTag/${TagKey}
detector-version	arn:${Partition}:frauddetector:${Region}:${Account}:detector-version/${ResourcePath}	aws:ResourceTag/${TagKey}
entity-type	arn:${Partition}:frauddetector:${Region}:${Account}:entity-type/${ResourcePath}	aws:ResourceTag/${TagKey}
external-model	arn:${Partition}:frauddetector:${Region}:${Account}:external-model/${ResourcePath}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
event-type	arn:${Partition}:frauddetector:${Region}:${Account}:event-type/${ResourcePath}	aws:ResourceTag/${TagKey}
label	arn:${Partition}:frauddetector:${Region}:${Account}:label/${ResourcePath}	aws:ResourceTag/${TagKey}
model	arn:${Partition}:frauddetector:${Region}:${Account}:model/${ResourcePath}	aws:ResourceTag/${TagKey}
model-version	arn:${Partition}:frauddetector:${Region}:${Account}:model-version/${ResourcePath}	aws:ResourceTag/${TagKey}
outcome	arn:${Partition}:frauddetector:${Region}:${Account}:outcome/${ResourcePath}	aws:ResourceTag/${TagKey}
rule	arn:${Partition}:frauddetector:${Region}:${Account}:rule/${ResourcePath}	aws:ResourceTag/${TagKey}
variable	arn:${Partition}:frauddetector:${Region}:${Account}:variable/${ResourcePath}	aws:ResourceTag/${TagKey}
batch-import	arn:${Partition}:frauddetector:${Region}:${Account}:batch-import/${ResourcePath}	aws:ResourceTag/${TagKey}
list	arn:${Partition}:frauddetector:${Region}:${Account}:list/${ResourcePath}	aws:ResourceTag/${TagKey}

Amazon Fraud Detector の条件キー

Amazon Fraud Detector では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします。	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられているタグに基づいてアクションをフィルタリングします。	文字列
aws:TagKeys	リクエストで渡されたタグキーに基づいてアクションをフィルタリングします。	ArrayOfString

AWS 無料利用枠のアクション、リソース、および条件キー

AWS 無料利用枠 (サービスプレフィックス: freetier) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS 無料利用枠で定義されるアクション
- AWS 無料利用枠で定義されるリソースタイプ

- AWS 無料利用枠の条件キー

AWS 無料利用枠で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetAccountActivity	特定のアクティビティレコードを取得する許可を付与	読み取り			
GetAccountPlanState	無料利用枠に関連するアカウントプランの状態に関連するすべての情報を取得する許可を付与	読み取り			
GetFreeTierAlertPreference [許可のみ]	無料利用枠のアラート設定 (E メールアドレス) を取得するアクセス許可を付与	読み取り			
GetFreeTierUsage	無料利用枠の使用制限と MTD の使用状況を取得するアクセス許可を付与	読み取り			
ListAccountActivities	使用可能なアクティビティを一覧表示するアクセス許可を付与します	リスト			
PutFreeTierAlertPreference [許可のみ]	無料利用枠のアラート設定 (E メールアドレス) を設定するアクセス許可を付与	書き込み			
UpgradeAccountPlan	アカウントプランのアップグレードをトリガーするアクセス許可を付与します	書き込み			

AWS 無料利用枠で定義されるリソースタイプ

AWS 無料利用枠では、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定はサポートされていません。 AWS 無料利用枠へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS 無料利用枠の条件キー

無料利用枠には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon FreeRTOS のアクション、リソース、および条件キー

Amazon FreeRTOS (サービスプレフィックス: `freertos`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon FreeRTOS で定義されるアクション
- Amazon FreeRTOS で定義されるリソースタイプ
- Amazon FreeRTOS の条件キー

Amazon FreeRTOS で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSoftwareConfiguration	ソフトウェア設定を作成する許可を付与	書き込み	configuration*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscription	FreeRTOS 拡張メンテナンスプラン (EMP) のサブスクリプションを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSoftwareConfiguration	ソフトウェア設定を削除する許可を付与	書き込み	configuration*		
DescribeHardwarePlatform	ハードウェアプラットフォームを記述する許可を付与	読み取り			
DescribeSoftwareConfiguration	ソフトウェア設定を記述する許可を付与	読み取り	configuration*		
DescribeSubscription	FreeRTOS 延長メンテナンスプラン (EMP) のサブスクリプションを記述する許可を付与	読み取り	subscription*		
GetEmpPatchUrl	FreeRTOS 拡張メンテナンスプラン (EMP) のソフトウェアパッチリリース、パッチ差分、リリースノートへの URL を取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetSoftwareURL	Amazon FreeRTOS ソフトウェアのダウンロード用の URL を取得する許可を付与	読み取り			
GetSoftwareURLForConfiguration	設定に基づいて、Amazon FreeRTOS ソフトウェアのダウンロード用の URL を取得する許可を付与	読み取り			
GetSubscriptionBillingAmount	FreeRTOS 延長メンテナンスプラン (EMP) のサブスクリプションに対する請求金額を取得する許可を付与	読み取り			
ListFreeRTOSVersions	Amazon FreeRTOS のバージョンを一覧表示する許可を付与	リスト			
ListHardwarePlatforms	ハードウェアプラットフォームを一覧表示する許可を付与	リスト			
ListHardwareVendors	ハードウェアベンダーを一覧表示する許可を付与	リスト			
ListSoftwareConfigurations	ソフトウェア設定を一覧表示する許可を付与	リスト			
ListSoftwarePatches	FreeRTOS 延長メンテナンスプラン (EMP) サブスクリプションのソフトウェアパッチを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListSubscriptionEmails	FreeRTOS 延長メンテナンスプラン (EMP) のサブスクリプションに関する E メールを一覧表示する許可を付与	リスト			
ListSubscriptions	FreeRTOS 拡張メンテナンスプラン (EMP) のサブスクリプションを一覧表示する許可を付与	リスト			
UpdateEmailRecipients	FreeRTOS 延長メンテナンスプラン (EMP) のサブスクリプション用 E メールアドレスの一覧を更新する許可を付与	書き込み			
UpdateSoftwareConfiguration	ソフトウェア設定を更新する許可を付与	書き込み	configuration*		
VerifyEmail	FreeRTOS 延長メンテナンスプラン (EMP) 用の E メールを確認する許可を付与	書き込み			

Amazon FreeRTOS で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
configuration	arn:${Partition}:freertos:${Region}:${Account}:configuration/${ConfigurationName}	aws:ResourceTag/${TagKey}
subscription	arn:${Partition}:freertos:${Region}:${Account}:subscription/${SubscriptionID}	aws:ResourceTag/${TagKey}

Amazon FreeRTOS の条件キー

Amazon FreeRTOS は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	ユーザーが Amazon FreeRTOS に対して行うリクエストに含まれるタグキーによってアクセスをフィルタリングする	String
aws:ResourceTag/${TagKey}	Amazon FreeRTOS リソースに添付されたタグキーコンポーネントによってアクセスをフィルタリングする	String
aws:TagKeys	リクエスト内のリソースに関連付けられているすべてのタグキー名のリストによりアクセスををフィルタリングします	ArrayOfString

Amazon FSx のアクション、リソース、および条件キー

Amazon FSx (サービスプレフィックス: fsx) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon FSx で定義されるアクション
- Amazon FSx で定義されるリソースタイプ
- Amazon FSx の条件キー

Amazon FSx で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリス

ク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateFileGateway [アクセス許可のみ]	ファイルゲートウェイインスタンスを Amazon FSx for Windows File Server 用のファイルシステムに関連付けるアクセス許可を付与します。	書き込み	file-system*		
AssociateFileSystemAliases	Amazon FSx for Windows File Server ファイルシステムに DNS エイリアスを関連付けるアクセス権限を付与します	書き込み	file-system*		
BypassSnaplockEnterpriseRet	アクティブな保持期間が設定されている WORM (Write Once Read Many) ファイ	権限の管理	volume*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ention [アクセス許可のみ]	ルを含む FSx for ONTAP SnapLock Enterprise ボリュームの削除を許可するための許可を付与します				
CancelDataRepositoryTask	データリポジトリタスクをキャンセルするアクセス権限を付与します	書き込み	task*		
CopyBackup	バックアップをコピーする許可を付与。	書き込み	backup*		fsx:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CopySnapshotAndUpdateVolume	別の Amazon FSx for OpenZFS ファイルシステムのスナップショットを使用して既存のボリュームを更新するためのアクセス許可を付与	書き込み	snapshot*		
			volume*		
CreateAndAttachS3AccessPoint	S3 アクセスポイントを作成して FSx ファイルシステムにアタッチするアクセス許可を付与します	書き込み	volume		s3:CreateAccessPoint s3:GetAccessPoint s3:PutAccessPointPolicy

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateBackup	Amazon FSx ファイルシステムまたは Amazon FSx ボリュームの新しいバックアップを作成する許可を付与	書き込み	backup*		fsx:TagResource
			file-system		
			volume		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataRepositoryAssociation	Amazon FSx for Lustre ファイルシステム用の新しいデータリポジトリタスクを作成するアクセス権限を付与します。	書き込み	association*		fsx:TagResource
			file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataRepositoryTask	Amazon FSx for Lustre ファイルシステム用の新しいデータリポジトリタスクを作成するアクセス権限を付与します	書き込み	file-system*		fsx:TagResource
			task*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateFileCache	新しい空の Amazon ファイルキャッシュを作成するための許可を付与します	書き込み	file-cache*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:GetSecurityGroupsForVpc fsx:CreateDataRepositoryAssociation fsx:TagResource logs:CreateLogGroup logs:CreateLogStream logs:PutLogEvents

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					s3:ListBucket
			association	fsx:NfsDataRepositoryEncryptionInTransitEnabled fsx:NfsDataRepositoryAuthenticationEnabled	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFileSystem	新しい空の Amazon FSx ファイルシステムを作成するアクセス権限を付与します	書き込み	file-system*		ec2:GetSecurityGroupsForVpc fsx:TagResource

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFileSystemFromBackup	既存のバックアップから新しい Amazon FSx ファイルシステムを作成するアクセス権限を付与します	書き込み	backup*		ec2:GetSecurityGroupsForVpc fsx:TagResource
			file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	大量の新しい スナップショットを作成する許可を付与します。	書き込み	snapshot*		fsx:TagResource
			volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateStorageVirtualMachine	Amazon FSx for Ontap ファイルシステム内に新しいストレージ仮想マシンを作成する許可を付与	書き込み	file-system*		fsx:TagResource
			storage-virtual-machine*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVolume	新しいボリュームを作成する許可を付与	書き込み	volume*		fsx:TagResource
			snapshot		
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId fsx:ParentVolumeId	
CreateVolumeFromBackup	バックアップから新しいボリュームを作成する許可を付与	書き込み	backup*		fsx:TagResource

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			storage-virtual-machine*		
			volume*		
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId	
DeleteBackup	バックアップを削除するアクセス権限を付与し、その内容を削除します。削除後、バックアップは存在しなくなり、そのデータは使用できなくなります。	書き込み	backup*		
DeleteDataRepositoryAssociation	リポジトリの関連付けを記述する許可を付与します。	書き込み	association*		
DeleteFileCache	ファイルキャッシュを削除するための許可を付与し、その内容を削除します	書き込み	file-cache*		fsx:DeleteDataRepositoryAssociation
			association		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFileSystem	ファイルシステムを削除するアクセス権限を付与し、そのコンテンツおよびファイルシステムの既存の自動バックアップを削除します	書き込み	file-system*		fsx:CreateBackup fsx:TagResource
			backup		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteResourcePolicy [アクセス許可のみ]	AWS Resource Access Manager (RAM) を使用して FSx ボリュームのクロスアカウント共有を管理するために必要です。PutResourcePolicy と GetResourcePolicy も必要です	権限の管理	volume*		
DeleteSnapshot	大量のスナップショットを削除する許可を付与します。	書き込み	snapshot*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteStorageVirtualMachine	ストレージ仮想マシンを削除して、その内容を削除する許可を付与します。	書き込み	storage-virtual-machine*		
DeleteVolume	ボリュームを削除して、その内容およびボリュームの既存の自動バックアップを削除する許可を付与します。	書き込み	volume*		fsx:TagResource
			backup		
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId fsx:ParentVolumeId	
DescribeAssociatedFileGateways [アクセス許可のみ]	Amazon FSx for Windows File Server ファイルシステムに関連付けられたファイルゲートウェイインスタンスを記述する許可を付与。	読み取り	file-system*		
DescribeBackups	呼び出しているエンドポイントの AWS アカウント で が所有するすべてのバックアップの説明 AWS リージョン を返すアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeDataRepositoryAssociations	呼び出しているエンドポイントの AWS アカウント で が所有するすべてのデータリポジトリ AWS リージョン の関連付けの説明を返すアクセス許可を付与します	読み取り			
DescribeDataRepositoryTasks	呼び出しているエンドポイントの AWS アカウント で が所有するすべてのデータリポジトリタスクの説明 AWS リージョン を返すアクセス許可を付与します	読み取り			
DescribeFileCaches	呼び出しているエンドポイントの AWS アカウント で が所有するすべてのファイルキャッシュの説明 AWS リージョン を返すアクセス許可を付与します	読み取り			
DescribeFileSystemAliases	Amazon FSx for Windows File Server ファイルシステムが所有しているすべての DNS エイリアスの説明を返すアクセス権限を付与します	読み取り	file-system*		
DescribeFileSystems	呼び出しているエンドポイント AWS リージョン の AWS アカウント で が所有するすべてのファイルシステムの説明を返すアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeS3AccessPointAttachments	S3 アクセスポイントアタッチメントの説明を返すアクセス許可を付与します	読み取り			
DescribeSharedVpcConfiguration	参加者アカウントからの FSx ルートテーブルの更新が自分のアカウントで許可されているかどうかの説明を返すためのアクセス許可を付与	読み取り			
DescribeSnapshots	呼び出しているエンドポイントの AWS アカウント でが所有するすべてのスナップショットの説明 AWS リージョン を返すアクセス許可を付与します	読み取り			
DescribeStorageVirtualMachines	呼び出しているエンドポイントの AWS アカウント で が所有するすべてのストレージ仮想マシンの説明 AWS リージョン を返すアクセス許可を付与します	読み取り			
DescribeVolumes	呼び出しているエンドポイント AWS リージョン の AWS アカウント で が所有するすべてのボリュームの説明を返すアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DetachAndDeleteS3AccessPoint	Amazon FSx ファイルシステムから S3 アクセスポイントをデタッチし、S3 アクセスポイントを削除するアクセス許可を付与します	書き込み	volume		s3:DeleteAccessPoint
DisassociateFileGateway [アクセス許可のみ]	Amazon FSx for Windows File Server ファイルシステムからファイルゲートウェイインスタンスの関連付けを解除する許可を付与。	書き込み	file-system*		
DisassociateFileSystemAliases	ファイルシステムエイリアスと Amazon FSx for Windows File Server ファイルシステムの関連付けを解除するアクセス権限を付与します	書き込み	file-system*		
GetResourcePolicy [アクセス許可のみ]	AWS Resource Access Manager (RAM) を使用して FSx ボリュームのクロスアカウント共有を管理するために必要です。PutResourcePolicy と DeleteResourcePolicy も必要です	権限の管理	volume*		
ListTagsForResource	Amazon FSx リソースのタグを一覧表示するアクセス権限を付与します	読み取り	association		
			backup		
			file-cache		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		
ManageBackupPrincipalAssociations [許可のみ]	AWS Backup を使用してバックアッププリンシパルの関連付けを管理するアクセス許可を付与します	権限の管理	backup*		
PutResourcePolicy [許可のみ]	AWS Resource Access Manager (RAM) を使用して FSx ボリュームのクロスアカウント共有を管理するために必要です。DeleteResourcePolicy と GetResourcePolicy も必要です	権限の管理	volume*		
ReleaseFileSystemNfsV3Locks	ファイルシステムの NFS V3 のロックをリリースする許可を付与します	書き込み	file-system*		
RestoreVolumeFromSnapshot	スナップショットからボリューム状態を復元するアクセス許可を付与します。	書き込み	snapshot*		
			volume*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartMisconfiguredStateRecovery	誤って設定された状態のリカバリを開始するアクセス許可を付与します	書き込み	file-system*		
TagResource	Amazon FSx リソースにタグを付けるアクセス権限を付与します	タグ付け	association		
			backup		
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Amazon FSx リソースからタグを削除するアクセス権限を付与します	Tagging	association		
			backup		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		
				aws:TagKeys	
UpdateDataRepositoryAssociation	データリポジトリ関連付け設定を更新するアクセス許可を付与します。	書き込み	association*		
UpdateFileCache	ファイルキャッシュ設定を更新するための許可を付与します	書き込み	file-cache*		
UpdateFileSystem	ファイルシステム設定を更新するアクセス権限を付与します	書き込み	file-system*		
UpdateSharedVpcConfiguration	参加者アカウントからの FSx ルートテーブルの更新を自分のアカウントで有効または無効にするためのアクセス許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateSnapshot	スナップショット設定を更新する許可を付与します。	書き込み	snapshot*		
UpdateStorageVirtualMachine	ストレージ仮想マシンの設定を更新する許可を付与	書き込み	storage-virtual-machine*		
UpdateVolume	ボリュームの設定を更新する許可を付与	書き込み	volume*		
				fsx:StorageVirtualMachineId fsx:ParentVolumeId	

Amazon FSx で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

> **Note**
>
> Amazon FSx for Windows File Server、Lustre、および Ontap は、それぞれ同じ ARN 形式で、いくつかの同じリソースタイプを共有します。

リソースタイプ	ARN	条件キー
file-system	arn:${Partition}:fsx:${Region}:${Account}:file-system/${FileSystemId}	aws:ResourceTag/${TagKey}
file-cache	arn:${Partition}:fsx:${Region}:${Account}:file-cache/${FileCacheId}	aws:ResourceTag/${TagKey}
backup	arn:${Partition}:fsx:${Region}:${Account}:backup/${BackupId}	aws:ResourceTag/${TagKey}
storage-virtual-machine	arn:${Partition}:fsx:${Region}:${Account}:storage-virtual-machine/${FileSystemId}/${StorageVirtualMachineId}	aws:ResourceTag/${TagKey}
task	arn:${Partition}:fsx:${Region}:${Account}:task/${TaskId}	aws:ResourceTag/${TagKey}
association	arn:${Partition}:fsx:${Region}:${Account}:association/${FileSystemIdOrFileCacheId}/${DataRepositoryAssociationId}	aws:ResourceTag/${TagKey}
volume	arn:${Partition}:fsx:${Region}:${Account}:volume/${FileSystemId}/${VolumeId}	aws:ResourceTag/${TagKey}
snapshot	arn:${Partition}:fsx:${Region}:${Account}:snapshot/${VolumeId}/${SnapshotId}	aws:ResourceTag/${TagKey}

Amazon FSx の条件キー

Amazon FSx では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
fsx:IsBackupCopyDestination	バックアップが CopyBackup オペレーションの送信先バックアップであるかどうかによって、アクセスをフィルターします。	Bool
fsx:IsBackupCopySource	バックアップが CopyBackup 操作のソースバックアップであるかどうかによってアクセスをフィルタリングします。	Bool
fsx:NfsDataRepositoryAuthenticationEnabled	認証をサポートする NFS データリポジトリによるアクセスをフィルタリングします	Bool
fsx:NfsDataRepositoryEncryptionInTransitEnabled	転送中の暗号化をサポートする NFS データリポジトリによるアクセスをフィルタリングします	Bool
fsx:ParentVolumeId	ボリュームオペレーションを変更するために、ペアレントボリュームを含むことでアクセスをフィルタリングします。	String

条件キー	説明	タイプ
fsx:StorageVirtualMachineId	ボリュームオペレーションを変更するために、ボリュームについて包含するストレージ仮想マシンでアクセスをフィルタリングします	String

Amazon GameLift サーバーのアクション、リソース、および条件キー

Amazon GameLift Servers (サービスプレフィックス: gamelift) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon GameLift サーバーで定義されるアクション
- Amazon GameLift サーバーで定義されるリソースタイプ
- Amazon GameLift サーバーの条件キー

Amazon GameLift サーバーで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にア

クションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptMatch	プレイヤーの、提案された FlexMatch マッチの受け入れまたは拒否を登録する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ClaimGameServer	新しいゲームセッションをホストするゲームサーバーを検索して予約する許可を付与	書き込み	gameServerGroup*		
CreateAlias	フリートの新しいエイリアスを定義する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateBuild	Amazon S3 バケットに格納されたファイルを使用して新しいゲームビルドを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource iam:PassRole s3:GetObject

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateContainerFleet	ゲームサーバーを実行するためのコンピューティングリソースの新しいコンテナフリートを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeAvailabilityZones ec2:DescribeRegions gamelift:TagResource iam:PassRole
CreateContainerGroupDefinition	Amazon ECR リポジトリに保存されているイメージを使用して新しいコンテナグループ定義を作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	ecr:BatchGetImage ecr:DescribeImages ecr:GetAuthorizationToken ecr:GetDownloadUrlForLayer gamelift:TagResource

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateFleet	ゲームサーバーを稼働するための新しいコンピューティングリソース群を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeAvailabilityZones ec2:DescribeRegions gamelift:TagResource iam:PassRole
CreateFleetLocations	フリートに追加の口ケーションを指定する許可を付与	書き込み	containerFleet		ec2:DescribeAvailabilityZones ec2:DescribeRegions
			fleet		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateGameServerGroup	新しいゲームサーバーグループを作成し、対応する Auto Scaling グループを設定し、インスタンスを起動してゲームサーバーをホストする許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	autoscaling:CreateAutoScalingGroup autoscaling:DescribeAutoScalingGroups autoscaling:PutLifecycleHook autoscaling:PutScalingPolicy ec2:DescribeAvailabilityZones ec2:DescribeSubnets events:PutRule events:PutTargets

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					gamelift:TagResource iam:PassRole
CreateGameSession	指定されたフリートで新しいゲームセッションを開始する許可を付与	書き込み			
CreateGameSessionQueue	ゲームセッションプレイスメントリクエストを処理するための新しいキューを設定する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateLocation	フリートの新しいロケーションを定義する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateMatchmakingConfiguration	新しい FlexMatch マッチメイカーを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateMatchmakingRuleSet	FlexMatch の新しいマッチメイキングルールセットを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreatePlayerSession	プレイヤーに利用可能なゲームセッションスロットを予約する許可を付与	書き込み			
CreatePlayerSessions	複数のプレイヤーに利用可能なゲームセッションスロットを予約する許可を付与	書き込み			
CreateScript	新しいリアルタイムサーバースクリプトを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource iam:PassRole s3:GetObject

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateVpcPeeringAuthorization	GameLift フリート VPC と別の VPC 間のピア接続を作成または削除することを GameLift に許可するアクセス許可を付与します AWS アカウント	書き込み			ec2:AcceptVpcPeeringConnection ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateRoute ec2:DeleteRoute ec2:DescribeRouteTables ec2:DescribeSecurityGroups ec2:RevokeSecurityGroupEgress

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					ec2:RevokeSecurityGroupIngress
CreateVpcPeeringConnection	GameLift フリート VPC と別のアカウントの VPC の間にピア接続を確立する許可を付与	書き込み			
DeleteAlias	エイリアスを削除する許可を付与	書き込み	alias*		
DeleteBuild	ゲームビルドを削除する許可を付与	書き込み	build*		
DeleteContainerFleet	コンテナフリートを削除するアクセス許可を付与します	書き込み	containerFleet*		
DeleteContainerGroupDefinition	コンテナグループ定義を削除するアクセス許可を付与します	書き込み	containerGroupDefinition*		
DeleteFleet	空のフリートを削除する許可を付与	書き込み	fleet*		
DeleteFleetLocations	フリートのロケーションを削除する許可を付与	書き込み	containerFleet		
			fleet		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteGameServerGroup	ゲームサーバーグループを完全に削除し、対応する Auto Scaling グループの FleetIQ アクティビティを終了する許可を付与	書き込み	gameServerGroup*		autoscaling:DeleteAutoScalingGroup autoscaling:DescribeAutoScalingGroups autoscaling:ExitStandby autoscaling:ResumeProcesses autoscaling:SetInstanceProtection autoscaling:UpdateAutoScalingGroup
DeleteGameSessionQueue	既存のゲームセッションキューを削除する許可を付与	書き込み	gameSessionQueue*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteLocation	ロケーションを削除する許可を付与	書き込み	location*		
DeleteMatchmakingConfiguration	既存の FlexMatch マッチメイカーを削除する許可を付与	書き込み	matchmakingConfiguration*		
DeleteMatchmakingRuleSet	既存の FlexMatch マッチメイキングルールセットを削除する許可を付与	書き込み	matchmakingRuleSet*		
DeleteScalingPolicy	自動スケーリングルールのセットを削除する許可を付与	書き込み	containerFleet		
			fleet		
DeleteScript	リアルタイムサーバースクリプトを削除する許可を付与	書き込み	script*		
DeleteVpcPeeringAuthorization	VPC ピア認可をキャンセルする許可を付与	書き込み			
DeleteVpcPeeringConnection	VPC 間のピア接続を削除する許可を付与	書き込み			
DeregisterCompute	フリートに対するコンピューティングの登録を解除する許可を付与	書き込み	fleet*		
DeregisterGameServer	ゲームサーバーグループからゲームサーバーを削除する許可を付与	書き込み	gameServerGroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeAlias	エイリアスのプロパティを取得するためのアクセス許可を付与します	読み込み	alias*		
DescribeBuild	ゲームビルドのプロパティを取得するためのアクセス許可を付与します	読み取り	build*		
DescribeCompute	フリート内のコンピューティングの情報を取得するアクセス許可を付与します	読み取り	containerFleet		
			fleet		
DescribeContainerFleet	既存のコンテナフリートのプロパティを取得するアクセス許可を付与します	読み取り	containerFleet*		
DescribeContainerGroupDefinition	既存のコンテナグループ定義のプロパティを取得するアクセス許可を付与します	読み取り	containerGroupDefinition*		
DescribeEC2InstanceLimits	EC2 インスタンスタイプの最大使用量および現在の使用量を取得するためのアクセス許可を付与します	読み込み			
DescribeFleetAttributes	フリートの一般プロパティ (ステータスを含む) を取得するためのアクセス許可を付与します	読み取り			
DescribeFleetCapacity	マネージドフリートの現在の容量設定を取得するアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeFleetDeployment	既存のフリートデプロイのプロパティを取得するアクセス許可を付与します	読み取り	containerFleet*		
DescribeFleetEvents	フリートのイベントログからエントリを取得するためのアクセス許可を付与します	読み込み	containerFleet		
			fleet		
DescribeFleetLocationAttributes	フリートのロケーションに関する一般的なプロパティ (ステータスを含む) を取得するためのアクセス許可を付与します	読み込み	containerFleet		
			fleet		
DescribeFleetLocationCapacity	フリートのロケーションの現在の容量設定を取得するためのアクセス許可を付与します	読み込み	containerFleet		
			fleet		
DescribeFleetLocationUtilization	フリートのロケーションの使用状況統計情報を取得するためのアクセス許可を付与します	読み込み	fleet*		
DescribeFleetPortSettings	フリートのインバウンド接続の権限を取得するためのアクセス許可を付与します	読み込み	fleet*		
DescribeFleetUtilization	フリートの使用率統計情報を取得するためのアクセス許可を付与します	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeGameServer	ゲームサーバーのプロパティを取得するためのアクセス許可を付与します	読み込み	gameServerGroup*		
DescribeGameServerGroup	ゲームサーバーグループのプロパティを取得するためのアクセス許可を付与します	読み込み	gameServerGroup*		
DescribeGameServerInstances	ゲームサーバーグループのEC2 インスタンスのステータスを取得するためのアクセス許可を付与します	読み込み	gameServerGroup*		
DescribeGameSessionDetails	保護ポリシーを含む、フリート内のゲームセッションのプロパティを取得するためのアクセス許可を付与します	読み込み			
DescribeGameSessionPlacement	ゲームセッションプレイスメントリクエストの詳細を取得するためのアクセス許可を付与します	読み込み			
DescribeGameSessionQueues	ゲームセッションキューのプロパティを取得するためのアクセス許可を付与します	読み込み			
DescribeGameSessions	フリート内のゲームセッションのプロパティを取得するためのアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeInstances	マネージドフリート内のインスタンスに関する情報を取得するアクセス許可を付与します	読み取り	containerFleet		
			fleet		
DescribeMatchmaking	マッチメイキングチケットの詳細を取得するためのアクセス許可を付与します	読み込み			
DescribeMatchmakingConfigurations	FlexMatch マッチメイカーのプロパティを取得するためのアクセス許可を付与します	読み込み			
DescribeMatchmakingRuleSets	FlexMatch マッチメイキングルールセットのプロパティを取得するためのアクセス許可を付与します	読み込み			
DescribePlayerSessions	ゲームセッションでプレイヤーセッションのプロパティを取得するためのアクセス許可を付与します	読み込み			
DescribeRuntimeConfiguration	フリートの現在のランタイム設定を取得するためのアクセス許可を付与します	読み込み	fleet*		
DescribeScalingPolicies	フリートに適用されるすべてのスケーリングポリシーを取得するためのアクセス許可を付与します	読み込み	containerFleet		
			fleet		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeScript	リアルタイムサーバースクリプトのプロパティを取得するためのアクセス許可を付与します	読み込み	script*		
DescribeVpcPeeringAuthorizations	有効な VPC ピア認証を取得するためのアクセス許可を付与します	読み込み			
DescribeVpcPeeringConnections	アクティブまたは保留中の VPC ピア接続の詳細を取得するためのアクセス許可を付与します	読み取り			
GetComputeAccess	マネージドフリート内のコンピューティングにリモートアクセスするための認証情報を取得するアクセス許可を付与します	読み取り	containerFleet		
			fleet		
GetComputeAuthToken	コンピューティング上のプロセスが Amazon GameLift サービスにリクエストを送信できるようにする認証トークンを取得するアクセス許可を付与します	読み取り	containerFleet		
			fleet		
GetGameSessionLogUrl	ゲームセッションで保存されたログの場所を取得するためのアクセス許可を付与します	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetInstanceAccess	指定されたフリートインスタンスへのリモートアクセスをリクエストする許可を付与	読み込み	fleet*		
ListAliases	現在のリージョンで定義されているすべてのエイリアスを取得する許可を付与	リスト			
ListBuilds	現在のリージョン内のすべてのゲームビルドを取得する許可を付与	リスト			
ListCompute	現在のリージョン内のすべてのコンピューティングリソースを取得する許可を付与	リスト	containerFleet		
			fleet		
ListContainerFleets	現在のリージョン内のすべての既存のコンテナフリートのプロパティを取得するアクセス許可を付与します	リスト			
ListContainerGroupDefinitionVersions	既存のコンテナグループ定義のすべてのバージョンのプロパティを取得するアクセス許可を付与します	リスト	containerGroupDefinition*		
ListContainerGroupDefinitions	現在のリージョン内のすべての既存のコンテナグループ定義のプロパティを取得するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListFleetDeployments	現在のリージョン内のすべての既存のフリートデプロイのプロパティを取得するアクセス許可を付与します	リスト			
ListFleets	現在のリージョンにおけるすべてのフリートのフリート IDリストを取得する許可を付与	リスト			
ListGameServerGroups	現在のリージョンで定義されているすべてのゲームサーバーグループを取得する許可を付与	リスト			
ListGameServers	ゲームサーバーグループで現在実行中のすべてのゲームサーバーを取得するためのアクセス許可を付与します	リスト	gameServerGroup*		
ListLocations	このアカウントのすべてのロケーションを取得する許可を付与	リスト			
ListScripts	現在のリージョンのすべての Realtime Server スクリプトのプロパティを取得するためのアクセス許可を付与します	リスト			
ListTagsForResource	GameLift リソースのタグを取得するためのアクセス許可を付与します	読み込み	alias		
			build		
			containerFleet		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			containerGroupDefinition		
			fleet		
			gameServerGroup		
			gameSessionQueue		
			location		
			matchmakingConfiguration		
			matchmakingRuleSet		
			script		
PutScalingPolicy	フリートの自動スケーリングポリシーを作成または更新する許可を付与	書き込み	containerFleet		
			fleet		
RegisterCompute	フリートに対するコンピューティングを登録する許可を付与	書き込み	fleet*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RegisterGameServer	新しいゲームサーバーがゲームプレイをホストする準備ができたときに GameLift FleetIQ に通知する許可を付与	書き込み	gameServerGroup*		
RequestUploadCredentials	新しいゲームビルドをアップロードするときに使用する新しいアップロード認証情報を取得するためのアクセス許可を付与します	読み込み	build*		
ResolveAlias	エイリアスに関連付けられたフリート ID を取得するためのアクセス許可を付与します	読み込み	alias*		
ResumeGameServerGroup	ゲームサーバーグループの一時停止された FleetIQ アクティビティを復元する許可を付与	書き込み	gameServerGroup*		
SearchGameSessions	一連の検索条件に一致するゲームセッションを取得するためのアクセス許可を付与します	読み込み			
StartFleetActions	StopFleetActions() で中断されたフリートで自動スケーリングアクティビティを再開する許可を付与	書き込み	containerFleet		
			fleet		
StartGameSessionPlacement	ゲームセッションプレイスメントリクエストをゲームセッションキューに送信する許可を付与	書き込み	gameSessionQueue*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartMatchBackfill	FlexMatch マッチメーキングをリクエストして、既存のゲームセッションで使用可能なプレイヤースロットを埋めるアクセス許可を付与します	書き込み			
StartMatchmaking	1 人のプレイヤーまたはプレイヤーグループに FlexMatch マッチメイキングをリクエストし、ゲームセッションプレイスメントを開始する許可を付与	書き込み			
StopFleetActions	フリートで自動スケーリングアクティビティを一時停止する許可を付与	書き込み	containerFleet		
			fleet		
StopGameSessionPlacement	進行中のゲームセッションプレイスメントリクエストをキャンセルする許可を付与	書き込み			
StopMatchmaking	マッチメイキングをキャンセルするか、処理中のバックフィルリクエストを照合する許可を付与	書き込み			
SuspendGameServerGroup	ゲームサーバーグループの FleetIQ アクティビティを一時的に停止する許可を付与	書き込み	gameServerGroup*		
TagResource	GameLift リソースにタグを付けるアクセス許可を付与します	Tagging	alias		
			build		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			containerFleet		
			containerGroupDefinition		
			fleet		
			gameServerGroup		
			gameSessionQueue		
			location		
			matchmakingConfiguration		
			matchmakingRuleSet		
			script		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
TerminateGameSession	既存のゲームセッションをシャットダウンするアクセス許可を付与します	書き込み			
UntagResource	GameLift リソースのタグ付けを解除する許可を付与	タグ付け	alias		
			build		
			containerFleet		
			containerGroupDefinition		
			fleet		
			gameServerGroup		
			gameSessionQueue		
			location		
			matchmakingConfiguration		
			matchmakingRuleSet		
			script		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateAlias	既存のエイリアスのプロパティを更新する許可を付与	書き込み	alias*		
UpdateBuild	既存のビルドのメタデータを更新する許可を付与	書き込み	build*		
UpdateContainerFleet	既存のコンテナフリートを更新する許可を付与	書き込み	containerFleet*		
UpdateContainerGroupDefinition	既存のコンテナグループ定義のプロパティを更新する許可を付与	書き込み	containerGroupDefinition*		ecr:BatchGetImage ecr:DescribeImages ecr:GetAuthorizationToken ecr:GetDownloadUrlForLayer
UpdateFleetAttributes	既存のフリートの一般プロパティを更新する許可を付与	書き込み	fleet*		
UpdateFleetCapacity	マネージドフリートの容量設定を調整するアクセス許可を付与します	書き込み	containerFleet fleet		
UpdateFleetPortSettings	フリートのポート設定を調整する許可を付与	書き込み	fleet*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateGameServer	ゲームサーバーのプロパティ、ヘルスステータス、または使用状況ステータスを変更する許可を付与	書き込み	gameServerGroup*		
UpdateGameServerGroup	許可されたインスタンスタイプを含む、ゲームサーバーグループのプロパティを更新する許可を付与	書き込み	gameServerGroup*		iam:PassRole
UpdateGameSession	既存のゲームセッションのプロパティを更新する許可を付与	書き込み			
UpdateGameSessionQueue	既存のゲームセッションキューのプロパティを更新する許可を付与	書き込み	gameSessionQueue*		
UpdateMatchmakingConfiguration	既存の FlexMatch マッチメイキング設定のプロパティを更新する許可を付与	書き込み	matchmakingConfiguration*		
UpdateRuntimeConfiguration	既存のフリートのインスタンスでサーバープロセスの設定方法を更新する許可を付与	書き込み	fleet*		
UpdateScript	既存の Realtime Server スクリプトのメタデータとコンテンツを更新する許可を付与	書き込み	script*		iam:PassRole s3:GetObject
ValidateMatchmakingRuleSet	FlexMatch マッチメイキングルールセットの構文を検証する許可を付与	読み取り			

Amazon GameLift サーバーで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
alias	arn:${Partition}:gamelift:${Region}::alias/${AliasId}	aws:ResourceTag/${TagKey}
build	arn:${Partition}:gamelift:${Region}:${Account}:build/${BuildId}	aws:ResourceTag/${TagKey}
containerGroupDefinition	arn:${Partition}:gamelift:${Region}:${Account}:containergroupdefinition/${Name}	aws:ResourceTag/${TagKey}
containerFleet	arn:${Partition}:gamelift:${Region}:${Account}:containerfleet/${FleetId}	aws:ResourceTag/${TagKey}
fleet	arn:${Partition}:gamelift:${Region}:${Account}:fleet/${FleetId}	aws:ResourceTag/${TagKey}
gameServerGroup	arn:${Partition}:gamelift:${Region}:${Account}:gameservergroup/${GameServerGroupName}	aws:ResourceTag/${TagKey}
gameSessionQueue	arn:${Partition}:gamelift:${Region}:${Account}:gamesessionqueue/${GameSessionQueueName}	aws:ResourceTag/${TagKey}
location	arn:${Partition}:gamelift:${Region}:${Account}:location/${LocationId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
matchmakingConfiguration	arn:${Partition}:gamelift:${Region}:${Account}:matchmakingconfiguration/${MatchmakingConfigurationName}	aws:ResourceTag/${TagKey}
matchmakingRuleSet	arn:${Partition}:gamelift:${Region}:${Account}:matchmakingruleset/${MatchmakingRuleSetName}	aws:ResourceTag/${TagKey}
script	arn:${Partition}:gamelift:${Region}:${Account}:script/${ScriptId}	aws:ResourceTag/${TagKey}

Amazon GameLift サーバーの条件キー

Amazon GameLift Servers では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon GameLift Streams のアクション、リソース、および条件キー

Amazon GameLift Streams (サービスプレフィックス: gameliftstreams) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon GameLift Streams で定義されるアクション
- Amazon GameLift Streams で定義されるリソースタイプ
- Amazon GameLift Streams の条件キー

Amazon GameLift Streams で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddStreamGroupLocations	StreamGroup リモートロケーションをアタッチする許可を付与	書き込み	streamgroup*		ec2:DescribeRegions
AssociateApplications	アプリケーションを StreamGroup に関連付けるアクセス許可を付与します	書き込み	application*		
			streamgroup*		
CreateApplication	アプリケーションを作成する許可を付与します。	書き込み		aws:RequestTag/${TagKey}	gameliftstreams:TagResource

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	s3:GetObject s3:ListBucket
CreateStreamGroup	StreamGroup を作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	gamelifstreams:TagResource
CreateStreamSessionConnection	ストリームセッション接続を作成するアクセス許可を付与します	書き込み	streamgroup*		
DeleteApplication	アプリケーションを削除する許可を付与	書き込み	application*		
DeleteStreamGroup	StreamGroup を削除するアクセス許可を付与します	書き込み	streamgroup*		
DisassociateApplications	StreamGroup からアプリケーションの関連付けを解除するアクセス許可を付与します	書き込み	application*		
			streamgroup*		
ExportStreamSessionFiles	アプリケーションが生成するストリームセッションファイルをエクスポートするアクセス許可を付与します	書き込み	streamgroup*		s3:PutObject
GetApplication	アプリケーションを取得する許可を付与	読み取り	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetStreamGroup	StreamGroup を取得するための「アクセス許可」を付与します	読み取り	streamgroup*		
GetStreamSession	ストリームセッションを取得するアクセス許可を付与します	読み取り	streamgroup*		
ListApplications	アプリケーションを一覧表示する許可を付与	リスト			
ListStreamGroups	StreamGroups を一覧表示するアクセス許可を付与します	リスト			
ListStreamSessions	ストリームセッションを一覧表示する許可を付与	読み取り	streamgroup*		
ListStreamSessionsByAccount	ストリームセッションを一覧表示する許可を付与	読み取り			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	application		
			streamgroup		
RemoveStreamGroupLocations	StreamGroup リモートロケーションをデタッチするアクセス許可を付与します	書き込み	streamgroup*		
StartStreamSession	ストリームセッションを作成するアクセス許可を付与します	書き込み	streamgroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagResource	リソースにタグを付けるアクセス許可を付与	Tagging	application		
			streamgroup		
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateStreamSession	ストリームセッションを終了するアクセス許可を付与します	書き込み	streamgroup*		
UntagResource	リソースのタグを解除する許可を付与	タグ付け	application		
			streamgroup		
				aws:TagKeys	
UpdateApplication	アプリケーションを更新する許可を付与	書き込み	application*		
UpdateStreamGroup	StreamGroup を更新するアクセス許可を付与します	書き込み	streamgroup*		

Amazon GameLift Streams で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
application	`arn:${Partition}:gameliftstreams:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}
stream group	`arn:${Partition}:gameliftstreams:${Region}:${Account}:streamgroup/${StreamGroupId}`	aws:ResourceTag/${TagKey}

Amazon GameLift Streams の条件キー

Amazon GameLift Streams では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストで渡されたタグによりアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString

AWS Global Accelerator のアクション、リソース、および条件キー

AWS Global Accelerator (サービスプレフィックス: `globalaccelerator`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Global Accelerator で定義されるアクション
- AWS Global Accelerator で定義されるリソースタイプ
- AWS Global Accelerator の条件キー

AWS Global Accelerator で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddCustomRoutingEndpoints	仮想プライベートクラウド (VPC) サブネットエンドポイントをカスタムルーティングアクセラレータエンドポイントグループに追加するアクセス許可を付与します	書き込み	endpointgroup*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AddEndpoints	標準アクセラレーターエンドポイントグループにエンドポイントを追加する許可を付与します	書き込み	endpointgroup*		globalaccelerator:UpdateEndpointGroup
AdvertiseByoipCidr	自分の IP アドレスを使用 (BYOIP) して、アクセラレータを使用するためにプロビジョニングされている IPv4 アドレス範囲をアドバタイズするアクセス許可を付与します	書き込み			
AllowCustomRoutingTraffic	特定の VPC サブネット内のプライベート宛先 IP:PORT へのユーザトラフィックのカスタムルーティングを可能にするアクセス許可を付与します	書き込み	endpointgroup*		
CreateAccelerator	標準アクセラレータを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCrossAccountAttachment	CrossAccountAttachment を作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateCustomRoutingAccelerator	カスタムルーティングアクセラレータを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomRoutingEndpointGroup	カスタムルーティングアクセラレータの指定されたリスナーのエンドポイントグループを作成するアクセス許可を付与します	書き込み	listener*		
CreateCustomRoutingListener	クライアントからカスタムルーティングアクセラレータへの着信接続を処理するリスナーを作成するアクセス許可を付与します	書き込み	accelerator*		
CreateEndpointGroup	標準アクセラレータリスナーにエンドポイントグループを追加するアクセス許可を付与します	書き込み	listener*		
CreateListener	標準アクセラレータにリスナーを追加するアクセス許可を付与します	書き込み	accelerator*		
DeleteAccelerator	標準アクセラレータを削除するアクセス許可を付与します	書き込み	accelerator*		
DeleteCrossAccountAttachment	CrossAccountAttachment を削除するアクセス許可を付与します	書き込み	attachment*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteCustomRoutingAccelerator	カスタムルーティングアクセラレータを削除するアクセス許可を付与します	書き込み	accelerator*		
DeleteCustomRoutingEndpointGroup	カスタムルーティングアクセラレータのリスナーからエンドポイントグループを削除するアクセス許可を付与します	書き込み	endpointgroup*		
DeleteCustomRoutingListener	カスタムルーティングアクセラレータのリスナーを削除するアクセス許可を付与します	書き込み	listener*		
DeleteEndpointGroup	標準アクセラレータリスナーに関連付けられたエンドポイントグループを削除するアクセス許可を付与します	書き込み	endpointgroup*		
DeleteListener	標準アクセラレータからリスナーを削除するアクセス許可を付与します	書き込み	listener*		
DenyCustomRoutingTraffic	特定の VPC サブネット内のプライベート宛先 IP:PORT へのユーザトラフィックのカスタムルーティングを禁止するアクセス許可を付与します	書き込み	endpointgroup*		
DeprovisionByoipCidr	自分の IP アドレスを使用 (BYOIP) して、アクセラレータで使用するためにプロビジョニングした、指定されたアドレス範囲を解放するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeAccelerator	標準アクセラレータを記述するアクセス許可を付与します	読み込み	accelerator*		
DescribeAcceleratorAttributes	標準アクセラレータ属性を記述するアクセス許可を付与します	読み取り	accelerator*		
DescribeCrossAccountAttachment	CrossAccountAttachment を説明するアクセス許可を付与します	読み取り	attachment*		
DescribeCustomRoutingAccelerator	カスタムルーティングアクセラレータを記述するアクセス許可を付与します	読み込み	accelerator*		
DescribeCustomRoutingAcceleratorAttributes	カスタムルーティングアクセラレータの属性を記述するアクセス許可を付与します	読み込み	accelerator*		
DescribeCustomRoutingEndpointGroup	カスタムルーティングアクセラレータのエンドポイントグループを記述するアクセス許可を付与します	読み込み	endpointgroup*		
DescribeCustomRoutingListener	カスタムルーティングアクセラレータのリスナーを記述するアクセス許可を付与します	読み込み	listener*		
DescribeEndpointGroup	標準アクセラレータエンドポイントグループを記述するアクセス許可を付与します	読み込み	endpointgroup*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeListener	標準アクセラレータリスナーを記述するアクセス許可を付与します	読み込み	listener*		
ListAccelerators	すべての標準アクセラレータを一覧表示するアクセス許可を付与します	リスト			
ListByoipCidrs	BYOIP CIDR を一覧表示するアクセス許可を付与します	リスト			
ListCrossAccountAttachments	すべての CrossAccountAttachments を一覧表示するアクセス許可を付与します	リスト			
ListCrossAccountResourceAccounts	発信者をプリンシパルとしてリストする CrossAccountAttachments を持つアカウントを一覧表示するアクセス許可を付与します	リスト			
ListCrossAccountResources	発信者が使用できるすべての CrossAccountAttachment リソースを一覧表示するアクセス許可を付与します	リスト			
ListCustomRoutingAccelerators	のカスタムルーティングアクセラレーターを一覧表示するアクセス許可を付与します AWS アカウント	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListCustomRoutingEndpointGroups	カスタムルーティングアクセラレータのリスナーに関連付けられたエンドポイントグループを一覧表示するアクセス許可を付与します	リスト	listener*		
ListCustomRoutingListeners	カスタムルーティングアクセラレータのリスナーを一覧表示するアクセス許可を付与します	リスト	accelerator*		
ListCustomRoutingPortMappings	カスタムルーティングアクセラレータのポートマッピングを一覧表示するアクセス許可を付与します	リスト	accelerator*		
ListCustomRoutingPortMappingsByDestination	サブネット内の特定のエンドポイント IP アドレス (宛先アドレス) のポートマッピングを一覧表示する許可を付与	リスト			
ListEndpointGroups	標準アクセラレータリスナーに関連付けられたすべてのエンドポイントグループを一覧表示するアクセス許可を付与します	リスト	listener*		
ListListeners	標準アクセラレータに関連付けられたすべてのリスナーを一覧表示するアクセス許可を付与します	リスト	accelerator*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTagsForResource	グローバルアクセラレータリソースのタグを一覧表示するアクセス許可を付与します	読み込み	accelerator		
			attachment		
ProvisionByoipCidr	自分の IP アドレスを使用 (BYOIP) して、アクセラレータで使用するアドレス範囲をプロビジョニングするアクセス許可を付与します	書き込み			
RemoveCustomRoutingEndpoints	カスタムルーティングアクセラレータエンドポイントグループから仮想プライベートクラウド (VPC) サブネットエンドポイントを削除するアクセス許可を付与します	書き込み	endpointgroup*		
RemoveEndpoints	標準アクセラレーターエンドポイントグループからエンドポイントを削除する許可を付与します	書き込み	endpointgroup*		globalaccelerator:UpdateEndpointGroup
TagResource	グローバルアクセラレータリソースにタグを追加するアクセス許可を付与します	Tagging	accelerator		
			attachment		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	グローバルアクセラレータリソースからタグを削除するアクセス許可を付与します	Tagging	accelerator		
			attachment		
				aws:TagKeys	
UpdateAccelerator	標準アクセラレータを更新するアクセス許可を付与します	書き込み	accelerator*		
UpdateAcceleratorAttributes	標準アクセラレータ属性を更新するアクセス許可を付与します	書き込み	accelerator*		
UpdateCrossAccountAttachment	CrossAccountAttachment を更新するアクセス許可を付与します	書き込み	attachment*		
UpdateCustomRoutingAccelerator	カスタムルーティングアクセラレータを更新するアクセス許可を付与します	書き込み	accelerator*		
UpdateCustomRoutingAcceleratorAttributes	カスタムルーティングアクセラレータの属性を更新するアクセス許可を付与します	書き込み	accelerator*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateCustomRoutingListener	カスタムルーティングアクセラレータのリスナーを更新するアクセス許可を付与します	書き込み	listener*		
UpdateEndpointGroup	標準アクセラレータリスナーのエンドポイントグループを更新するアクセス許可を付与します	書き込み	endpointgroup*		
UpdateListener	標準アクセラレータのリスナーを更新するアクセス許可を付与します	書き込み	listener*		
WithdrawByoipCidr	BYOIP IPv4 アドレスのアドバタイズを停止するアクセス許可を付与します	書き込み			

AWS Global Accelerator で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
accelerator	`arn:${Partition}:globalaccelerator::${Account}:accelerator/${ResourceId}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
listener	arn:${Partition}:globalaccelerator::${Account}:accelerator/${ResourceId}/listener/${ListenerId}	aws:ResourceTag/${TagKey}
endpointgroup	arn:${Partition}:globalaccelerator::${Account}:accelerator/${ResourceId}/listener/${ListenerId}/endpoint-group/${EndpointGroupId}	aws:ResourceTag/${TagKey}
attachment	arn:${Partition}:globalaccelerator::${Account}:attachment/${ResourceId}	aws:ResourceTag/${TagKey}

AWS Global Accelerator の条件キー

AWS Global Accelerator は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

AWS Glue のアクション、リソース、および条件キー

AWS Glue (サービスプレフィックス: glue) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Glue で定義されるアクション
- AWS Glue で定義されるリソースタイプ
- AWS Glue の条件キー

AWS Glue で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリス

ク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AuthorizeInboundIntegration [アクセス許可のみ]	ターゲット Arn がソース ARN からレプリケートされたデータを受信できることを継続的に検証するアクセス許可を Glue に付与します	書き込み	integration*		
BatchCreatePartition	1 つ以上のパーティションを作成する許可を付与。	書き込み	database*		
			rootcatalog*		
			table*		
			catalog		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchDeleteConnection	1 つ以上の接続を削除する許可を付与。	書き込み	connection*		
			rootcatalog*		
BatchDeletePartition	1 つ以上のパーティションを削除する許可を付与。	書き込み	database*		
			rootcatalog*		
			table*		
			catalog		
BatchDeleteTable	1 つ以上のテーブルを削除する許可を付与。	書き込み	database*		
			rootcatalog*		
			table*		
			catalog		
BatchDeleteTableVersion	テーブルの 1 つ以上のバージョンを削除する許可を付与。	書き込み	database*		
			rootcatalog*		
			table*		
			catalog		
BatchGetBlueprints	1 つまたは複数のブループリントを取得する許可を付与	読み込み	blueprint*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchGetCrawlers	1 つ以上のクローラを取得する許可を付与。	読み取り	crawler*		
BatchGetCustomEntityTypes	1 つ以上のカスタムエンティティタイプを取得する許可を付与する	読み取り			
BatchGetDevEndpoints	1 つ以上の開発エンドポイントを取得する許可を付与。	読み込み	devendpoint*		
BatchGetJobs	1 つ以上のジョブを取得する許可を付与。	読み込み	job*		
BatchGetPartition	1 つ以上のパーティションを取得する許可を付与。	読み取り	database*		
			rootcatalog*		
			table*		
			catalog		
BatchGetStageFiles	SparkUI のステージファイルをバッチ取得する許可を付与する	権限の管理			
BatchGetTableOptimizer	指定されたテーブルオプティマイザーの設定を返す許可を付与	読み取り	database*		glue:GetTable
			rootcatalog*		
			table*		
BatchGetTriggers	1 つ以上のトリガーを取得する許可を付与。	読み込み	trigger*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchGetWorkflows	1 つ以上のワークフローを取得する許可を付与。	読み込み	workflow*		
BatchStopJobRun	1 つ以上のジョブ実行を停止する許可を付与。	書き込み	job*		
BatchUpdatePartition	1 つまたは複数のパーティションを更新する許可を付与	書き込み	database*		
			rootcatalog*		
			table*		
			catalog		
CancelDataQualityRuleRecommendationRun	推奨データ品質ルールの実行を停止する許可を付与	書き込み	dataQualityRuleset*		
CancelDataQualityRulesetEvaluationRun	進行中のデータ品質ルールセット評価実行を停止する許可を付与	書き込み	dataQualityRuleset*		
CancelMLTaskRun	ML タスクの実行を停止する許可を付与。	書き込み	mlTransform*		
CancelStatement	インタラクティブセッションでステートメントをキャンセルする許可を付与	書き込み	session*		
CheckSchemaVersionValidity	スキーマバージョンの妥当性をチェックする許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateBlueprint	ブループリントを作成する許可を付与	書き込み	blueprint*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCatalog	カタログを作成するアクセス許可を付与します	書き込み	catalog*		
			rootcatalog*		
CreateClassifier	分類子を作成する許可を付与。	書き込み			
CreateColumnStatisticsTaskSettings	列統計タスクの設定を作成するアクセス許可を付与します	書き込み	database*		
			rootcatalog*		
			table*		
CreateConnection	接続を作成する許可を付与。	書き込み	rootcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateCrawler	クローラを作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomEntityType	カスタムエンティティタイプを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataQualityRuleset	Data Quality ルールセットを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatabase	データベースを作成する許可を付与。	書き込み	database* rootcatalog* catalog		
CreateDevEndpoint	開発エンドポイントを作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateGlueIdentityCenterConfiguration	Glue を Identity Center に接続する許可を付与	書き込み			
CreateInboundIntegration [アクセス許可のみ]	ソースからターゲットにレプリケートされるデータのインバウンド統合を作成するアクセス許可をソースプリンシパルに付与します	書き込み			
CreateIntegration	統合を作成するアクセス許可を付与します	書き込み	catalog*		kms:CreateGrant kms:DescribeKey
			connection*		
			database*		
			integration*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateIntegrationResourceProperty	統合リソースプロパティを作成するアクセス許可を付与します	書き込み	catalog*		
			connection*		
			database*		
CreateIntegrationTableProperties	統合テーブルプロパティを作成するアクセス許可を付与します	書き込み	catalog*		
			connection*		
			database*		
CreateJob	ジョブを作成する許可を付与。	書き込み	job*		
				aws:RequestTag/${TagKey} aws:TagKeys glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateMLTransform	ML 変換を作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePartition	パーティションを作成する許可を付与。	書き込み	database*		
			rootcatalog*		
			table*		
			catalog		
CreatePartitionIndex	既存のテーブルに指定したパーティションインデックスを作成する許可を付与	書き込み	database*		
			rootcatalog*		
			table*		
			catalog		
CreateRegistry	新しいスキーマレジストリを作成する許可を付与	書き込み	registry*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchema	新しいスキーマコンテナーを作成する許可を付与	書き込み	registry*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			schema*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScript	スクリプトを作成する許可を付与。	書き込み			
CreateSecurityConfiguration	セキュリティ設定を作成する許可を付与。	書き込み			
CreateSession	インタラクティブセッションを作成する許可を付与	書き込み	session*		
				aws:RequestTag/${TagKey} aws:TagKeys glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateTable	テーブルを作成する許可を付与。	書き込み	database*		
			rootcatalog*		
			table*		
			catalog		
CreateTableOptimizer	特定の関数の新しいテーブルオプティマイザーを作成する許可を付与します。現在サポートされているオプティマイザータイプはコンパクションだけです。	書き込み	database*		glue:GetTable
			rootcatalog*		
			table*		
CreateTrigger	トリガーを作成する許可を付与。	書き込み	trigger*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUsageProfile	使用プロファイルを作成する許可を付与する	書き込み	usageProfile*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateUserDefinedFunction	関数定義を作成する許可を付与。	書き込み	database*		
			rootcatalog*		
			catalog		
CreateWorkflow	ワークフローを作成する許可を付与。	書き込み	workflow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBlueprint	ブループリントを削除する許可を付与	書き込み	blueprint*		
DeleteCatalog	カタログを削除するアクセス許可を付与します	書き込み	rootcatalog*		
			catalog		
DeleteClassifier	分類子を削除する許可を付与。	書き込み			
DeleteColumnStatisticsForPartition	列のパーティション列統計を削除する許可を付与	書き込み	database*		
			rootcatalog*		
			table*		
			catalog		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteColumnStatisticsForTable	列のテーブル統計を削除する許可を付与	書き込み	database*		
			rootcatalog*		
			table*		
			catalog		
DeleteColumnStatisticsTaskSettings	列統計タスクの設定を削除するアクセス許可を付与します	書き込み	database*		
			rootcatalog*		
			table*		
DeleteConnection	接続を削除する許可を付与。	書き込み	connection*		
			rootcatalog*		
DeleteCrawler	クローラを削除する許可を付与。	書き込み	crawler*		
DeleteCustomEntityType	カスタムエンティティタイプを削除する許可を付与する	書き込み			
DeleteDataQualityRuleset	Data Quality ルールセットを削除する許可を付与	書き込み	dataQualityRuleset*		
DeleteDatabase	データベースを削除する許可を付与。	書き込み	database*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			rootcatalog*		
			table*		
			userdefinedfunction*		
			catalog		
DeleteDevEndpoint	開発エンドポイントを削除する許可を付与。	書き込み	devendpoint*		
DeleteGlueIdentityCenterConfiguration	Identity Center で Glue を切断する許可を付与	書き込み			
DeleteIntegration	統合を削除するアクセス許可を付与します	書き込み	integration*		
				aws:ResourceTag/${TagKey}	
DeleteIntegrationTableProperties	統合テーブルのプロパティを削除するアクセス許可を付与します	書き込み	catalog*		
			connection*		
			database*		
DeleteJob	ジョブを削除する許可を付与	書き込み	job*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteMLTransform	ML 変換を削除する許可を付与。	書き込み	mlTransform*		
DeletePartition	パーティションを削除する許可を付与。	書き込み	database*		
			rootcatalog*		
			table*		
			catalog		
DeletePartitionIndex	既存のテーブルから指定したパーティションインデックスを削除する許可を付与	書き込み	database*		
			rootcatalog*		
			table*		
			catalog		
DeleteRegistry	スキーマレジストリを削除する許可を付与	書き込み	registry*		
DeleteResourcePolicy	リソースポリシーを削除する許可を付与。	Permissions management	rootcatalog*		
DeleteSchema	スキーマコンテナを削除する許可を付与	書き込み	registry*		
			schema*		
DeleteSchemaVersions	スキーマバージョンの範囲を削除する許可を付与	書き込み	registry*		
			schema*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteSecurityConfiguration	セキュリティ設定を削除する許可を付与。	書き込み			
DeleteSession	セッションを停止した後にインタラクティブセッションを削除する許可を付与 (まだ停止していない場合)	書き込み	session*		
DeleteTable	テーブルを削除する許可を付与。	書き込み	database*		
			rootcatalog*		
			table*		
			catalog		
DeleteTableOptimizer	オプティマイザーと、テーブルに関連付けられているすべてのメタデータを削除する許可を付与 最適化はテーブルに対して実行されなくなります	書き込み	database*		glue:GetTable
			rootcatalog*		
			table*		
DeleteTableVersion	テーブルのバージョンを削除する許可を付与。	書き込み	database*		
			rootcatalog*		
			table*		
			catalog		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteTrigger	トリガーを削除する許可を付与。	書き込み	trigger*		
DeleteUsageProfile	使用プロファイルを削除する許可を付与する	書き込み	usageProfile*		
DeleteUserDefinedFunction	関数定義を削除する許可を付与。	書き込み	database*		
			rootcatalog*		
			userdefinedfunction*		
			catalog		
DeleteWorkflow	ワークフローを削除するアクセス許可を与えます。	書き込み	workflow*		
DeregisterDataPreview	Glue Studio Notebook セッションを終了する許可を付与	権限の管理			
DescribeConnectionType	Glue Studio で接続タイプを記述する許可を付与する	権限の管理			
DescribeEntity	Glue Studio のエンティティを記述する許可を付与する	権限の管理	connection*		
			rootcatalog*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeInboundIntegrations	インバウンド統合を一覧表示する許可を付与	リスト			
DescribeIntegrations	ゼロ ETL 統合を記述する許可を付与	リスト	integration*		
				aws:ResourceTag/${TagKey}	
GetBlueprint	ブループリントを取得する許可を付与	読み込み	blueprint*		
GetBlueprintRun	ブループリントの実行を取得する許可を付与	読み込み	blueprint*		
GetBlueprintRuns	ブループリントのすべての実行を取得する許可を付与	読み取り	blueprint*		
GetCatalog	カタログを取得するアクセス許可を付与します	読み取り	rootcatalog*		
			catalog		
				glue:EnabledForRedshiftAutoDiscovery	
GetCatalogImportStatus	カタログのインポートステータスを取得する許可を付与。	読み取り	rootcatalog*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetCatalogs	すべてのカタログを取得するアクセス許可を付与します	読み取り	rootcatalog*		
			catalog		
				glue:EnabledForRedshiftAutoDiscovery	
GetClassifier	分類子を取得する許可を付与。	読み込み			
GetClassifiers	すべての分類子を一覧表示する許可を付与。	読み込み			
GetColumnStatisticsForPartition	列のパーティション統計を取得する許可を付与	読み込み	database*		
			rootcatalog*		
			table*		
			catalog		
GetColumnStatisticsForTable	列のテーブル統計を取得する許可を付与	読み取り	database*		
			rootcatalog*		
			table*		
			catalog		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetColumnStatisticsTaskRun	run-id に基づいて、テーブルの列統計実行情報を取得する許可を付与	読み取り			
GetColumnStatisticsTaskRuns	run-id に基づいてテーブルの列統計実行情報を取得する許可を付与	読み取り			
GetColumnStatisticsTaskSettings	列統計タスクの設定を取得するアクセス許可を付与します	読み取り			
GetCompletion	AWS Q から Glue で完了リクエストに対して生成されたレスポンスを取得するアクセス許可を付与します	読み取り	completion*		
GetConnection	接続を取得する許可を付与。	読み込み	connection*		
			rootcatalog*		
GetConnections	接続のリストを取得する許可を付与。	読み込み	connection*		
			rootcatalog*		
GetCrawler	クローラを取得する許可を付与。	読み込み	crawler*		
GetCrawlerMetrics	クローラに関するメトリクスを取得する許可を付与。	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetCrawlers	すべてのクローラを取得する許可を付与。	読み取り			
GetCustomEntityType	カスタムエンティティタイプを読み取る許可を付与する	読み取り			
GetDashboardUrl	spark live UI にアクセスするための署名付き URL を生成するアクセス許可を付与します	読み取り	session*		
GetDataCatalogEncryptionSettings	カタログ暗号化設定を取得する許可を付与。	読み取り	rootcatalog*		
GetDataPreviewStatement	Data Preview Statement を取得するための許可を付与します	権限の管理			
GetDataQualityModel	統計の予測モデルのトレーニングステータスを取得する許可を付与する	読み取り	dataQualityRuleset*		
			job*		
GetDataQualityModelResult	最新のモデルから統計の予測を取得する許可を付与する	読み取り	dataQualityRuleset*		
			job*		
GetDataQualityResult	Data Quality の結果を取得する許可を付与	読み取り	dataQualityRuleset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetDataQualityRuleRecommendationRun	推奨 Data Quality ルールの実行を取得する許可を付与	読み取り	dataQualityRuleset*		
GetDataQualityRuleset	Data Quality のルールセットを取得する許可を付与	読み取り	dataQualityRuleset*		
GetDataQualityRulesetEvaluationRun	推奨 Data Quality ルールの実行を取得する許可を付与	読み取り	dataQualityRuleset*		
GetDatabase	データベースを取得する許可を付与。	読み込み	database*		
			rootcatalog*		
			catalog		
GetDatabases	すべてのデータベースを取得する許可を付与。	読み込み	database*		
			rootcatalog*		
			catalog		
GetDataflowGraph	スクリプトを Directed Acyclic Graph (DAG) に変換する許可を付与。	読み込み			
GetDevEndpoint	開発エンドポイントを取得する許可を付与。	読み込み	devendpoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetDevEndpoints	すべての開発エンドポイントを取得する許可を付与。	読み取り			
GetEntityRecords	Glue のエンティティレコードをプレビューするアクセス許可を付与します	読み取り	catalog*		
			connection		
GetEnvironment	SparkUI の環境の詳細を取得する許可を付与する	権限の管理			
GetExecutors	SparkUI のエグゼキューターを取得する許可を付与する	権限の管理			
GetExecutorsThreads	SparkUI のエグゼキュータースレッドを取得する許可を付与する	権限の管理			
GetGeneratedCode	有向非巡回グラフ (DAG) をコードに変換します	読み取り			
GetGlueIdentityCenterConfiguration	マネージド Idc アプリケーションを取得する許可を付与	読み取り			
GetIntegrationResourceProperty	統合リソースプロパティを取得するアクセス許可を付与します	読み取り	catalog*		
			connection*		
			database*		
GetIntegrationTableProperties	統合テーブルのプロパティを取得する許可を付与	読み取り	catalog*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			connection*		
			database*		
GetJob	ジョブを取得する許可を付与。	読み込み	job*		
GetJobBookmark	ジョブのブックマークを取得する許可を付与。	読み込み			
GetJobRun	ジョブ実行を取得する許可を付与。	読み込み	job*		
GetJobRuns	すべてのジョブ実行を取得する許可を付与。	読み取り	job*		
GetJobUpgradeAnalysis	ジョブのアップグレード分析を取得する許可を付与	読み取り	job*		
GetJobs	現在のすべてのジョブを取得する許可を付与。	読み取り			
GetLogParsingStatus	SparkUI のログ解析ステータスを取得する許可を付与する	権限の管理			
GetMLTaskRun	ML タスクの実行を取得する許可を付与。	読み込み	mlTransform*		
GetMLTaskRuns	すべての ML タスクの実行を取得する許可を付与。	リスト	mlTransform*		
GetMLTransform	ML 変換を取得する許可を付与。	読み込み	mlTransform*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetMLTransforms	すべての ML 変換を取得する許可を付与。	リスト	mlTransform*		
GetMapping	マッピングを作成する許可を付与。	読み取り			
GetNotebookInstanceStatus	Glue Studio Notebooks セッションステータスを取得する許可を付与	権限の管理			
GetPartition	パーティションを取得する許可を付与。	読み込み	database*		
			rootcatalog*		
			table*		
			catalog		
GetPartitionIndexes	テーブルのパーティションインデックスを取得する許可を付与	読み込み	database*		
			rootcatalog*		
			table*		
			catalog		
GetPartitions	テーブルのパーティションを取得する許可を付与。	読み込み	database*		
			rootcatalog*		
			table*		
			catalog		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetPlan	スクリプトのマッピングを取得する許可を付与。	読み取り			
GetQueries	SparkUI のクエリを取得する許可を付与する	権限の管理			
GetQuery	SparkUI の特定のクエリを取得する許可を付与する	権限の管理			
GetRecipeAction	Data Preparation Recipe ステートメントの結果を取得する許可を付与する	権限の管理			
GetRegistry	スキーマレジストリを取得する許可を付与	読み込み	registry*		
GetResourcePolicies	リソースポリシーを取得する許可を付与	読み込み	rootcatalog*		
GetResourcePolicy	リソースポリシーを取得する許可を付与。	読み込み	rootcatalog*		
GetSchema	スキーマコンテナを取得する許可を付与	読み込み	registry*		
			schema*		
GetSchemaByDefinition	スキーマ定義に基づいて、スキーマバージョンを取得する許可を付与	読み込み	registry*		
			schema*		
GetSchemaVersion	スキーマバージョンを取得する許可を付与	読み込み	registry		
			schema		
GetSchemaVersionsDiff		読み込み	registry*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	スキーマレジストリ内の 2 つのスキーマバージョンを比較する許可を付与		schema*		
GetSecurityConfiguration	セキュリティ設定を取得する許可を付与。	読み込み			
GetSecurityConfigurations	1 つ以上のセキュリティ設定を取得する許可を付与。	読み込み			
GetSession	インタラクティブセッションを取得する許可を付与	読み取り	session*		
GetStage	SparkUI のステージを取得する許可を付与する	権限の管理			
GetStageAttempt	SparkUI のステージ試行を取得する許可を付与する	権限の管理			
GetStageAttemptTaskList	SparkUI のステージ試行のタスクリストを取得する許可を付与する	権限の管理			
GetStageAttemptTaskSummary	SparkUI のステージ試行のタスク概要を取得する許可を付与する	権限の管理			
GetStageFiles	SparkUI のステージファイルを取得する許可を付与する	権限の管理			
GetStages	SparkUI のステージを取得する許可を付与する	権限の管理			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetStatement	インタラクティブセッションでステートメントに関する結果と情報を取得する許可を付与	読み取り	session*		
GetStorage	SparkUI のストレージの詳細を取得する許可を付与する	権限の管理			
GetStorageUnit	SparkUI のストレージユニットの詳細を取得する許可を付与する	権限の管理			
GetTable	テーブルを取得する許可を付与。	読み取り	database*		
			rootcatalog*		
			table*		
			catalog		
GetTableOptimizer	指定されたテーブルに関連付けられているすべてのオプティマイザーの設定を返す許可を付与	読み取り	database*		glue:GetTable
			rootcatalog*		
			table*		
GetTableVersion	テーブルのバージョンを取得する許可を付与。	読み込み	database*		
			rootcatalog*		
			table*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			catalog		
GetTableVersions	テーブルのバージョンのリストを取得する許可を付与。	読み込み	database*		
			rootcatalog*		
			table*		
			catalog		
GetTables	データベース内のテーブルを取得する許可を付与。	読み込み	database*		
			rootcatalog*		
			table*		
			catalog		
GetTags	リソースに関連付けられているすべてのタグを取得する許可を付与。	読み込み	blueprint		
			crawler		
			customEntityType		
			devendpoint		
			job		
			trigger		
			usageProfile		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			workflow		
GetTrigger	トリガーを取得する許可を付与。	読み込み	trigger*		
GetTriggers	ジョブに関連付けられているトリガーを取得する許可を付与。	読み取り			
GetUsageProfile	使用プロファイルを取得する許可を付与する	読み取り	usageProfile*		
GetUserDefinedFunction	関数定義を取得する許可を付与	読み込み	database*		
			rootcatalog*		
			userdefinedfunction*		
			catalog		
GetUserDefinedFunctions	複数の関数定義を取得する許可を付与。	読み込み	database*		
			rootcatalog*		
			userdefinedfunction*		
			catalog		
GetWorkflow	ワークフローを取得する許可を付与。	読み込み	workflow*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetWorkflowRun	ワークフロー実行を取得する許可を付与。	読み込み	workflow*		
GetWorkflowRunProperties	ワークフロー実行プロパティを取得する許可を付与。	読み込み	workflow*		
GetWorkflowRuns	すべてのワークフロー実行を取得する許可を付与。	読み取り	workflow*		
GlueNotebookAuthorize	Glue Studio Notebooks にアクセスする許可を付与	権限の管理			
GlueNotebookRefreshCredentials	Glue Studio Notebooks の認証情報を更新する許可を付与	権限の管理			
ImportCatalogToGlue	Athena データカタログを AWS Glue にインポートする許可を付与	書き込み	rootcatalog*		
ListBlueprints	すべてのブループリントを取得する許可を付与	リスト			
ListColumnStatisticsTaskRuns	アカウントに実行されたすべての列統計の run-id を一覧表示する許可を付与	読み取り			
ListConnectionTypes	Glue Studio で接続タイプを一覧表示する許可を付与する	権限の管理			
ListCrawlers	すべてのクローラを取得する許可を付与。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListCrawls	クローラーのクロール実行履歴を取得する権限を付与する。	リスト	crawler*		
ListCustomEntityTypes	すべてのカスタムエンティティタイプを取得する許可を付与する	リスト			
ListDataQualityResults	すべての Data Quality の結果を取得する許可を付与	リスト	dataQualityRuleset*		
ListDataQualityRuleRecommendationRuns	すべての推奨 Data Quality ルールの実行を取得する許可を付与	リスト	dataQualityRuleset*		
ListDataQualityRulesetEvaluationRuns	すべての推奨 Data Quality ルールの実行を取得する許可を付与	リスト	dataQualityRuleset*		
ListDataQualityRulesets	Data Quality のルールセットのリストを取得する許可を付与	リスト	dataQualityRuleset*		
ListDevEndpoints	すべての開発エンドポイントを取得する許可を付与。	リスト			
ListEntities	Glue Studio でエンティティを一覧表示する許可を付与する	権限の管理	connection*		
			rootcatalog*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListJobUpgradeAnalyses	ジョブのアップグレード分析を一覧表示する許可を付与	リスト	job*		
ListJobs	現在のすべてのジョブを取得する許可を付与。	リスト			
ListMLTransforms	すべての ML 変換を取得する許可を付与。	リスト	mlTransform*		
ListRegistries	スキーマレジストリのリストを取得する許可を付与	リスト			
ListSchemaVersions	スキーマバージョンのリストを取得する許可を付与	リスト	registry*		
			schema*		
ListSchemas	スキーマコンテナのリストを取得する許可を付与	リスト	registry		
ListSessions	インタラクティブセッションのリストを取得する許可を付与	リスト			
ListStatements	インタラクティブセッションでステートメントのリストを取得する許可を付与	リスト	session*		
ListTableOptimizerRuns	特定のテーブルについての以前のオプティマイザーの実行の履歴を一覧表示する許可を付与	リスト	database*		glue:GetTable
			rootcatalog*		
			table*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTriggers	すべてのトリガーを取得する許可を付与。	リスト			
ListUsageProfiles	使用プロファイルのリストを取得する許可を付与する	リスト			
ListWorkflows	すべてのワークフローを取得する許可を付与。	リスト			
ModifyIntegration	ゼロ ETL 統合を変更する許可を付与	書き込み	integration*		
				aws:ResourceTag/${TagKey}	
NotifyEvent	イベント駆動型ワークフローにイベントを通知する許可を付与	書き込み	workflow*		
PassConnection [アクセス許可のみ]	Glue 接続名を必要とする API の入力に Glue 接続名を渡す許可を付与	書き込み	connection*		
PublishDataQuality [アクセス許可のみ]	Data Quality の結果を発行する許可を付与	書き込み	dataQualityRuleset*		
PutDataCatalogEncryptionSettings	カタログ暗号化設定を更新する許可を付与。	書き込み	rootcatalog*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutDataQualityProfileAnnotation	プロファイルのすべてのデータポイントに注釈を付ける許可を付与する	書き込み	dataQualityRuleset*		
			job*		
PutDataQualityStatisticAnnotation	特定のデータ品質統計のデータポイントに経時的に注釈を付ける許可を付与する	書き込み	dataQualityRuleset*		
			job*		
PutResourcePolicy	リソースポリシーを更新する許可を付与。	Permissions management	rootcatalog*		
PutSchemaVersionMetadata	スキーマバージョンにメタデータを追加する許可を付与	書き込み	registry		
			schema		
PutWorkflowRunProperties	ワークフロー実行プロパティを更新する許可を付与。	書き込み	workflow*		
QuerySchemaVersionMetadata	スキーマバージョンのメタデータをフェッチする許可を付与	リスト	registry		
			schema		
RefreshOAuth2Tokens	ジョブの実行中、接続のために oauth2 トークンを更新する許可を付与する	権限の管理	connection*		
			rootcatalog*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RegisterSchemaVersion	新しいスキーマバージョンを作成する許可を付与します	書き込み	registry*		
			schema*		
RemoveSchemaVersionMetadata	スキーマバージョンからメタデータを削除する許可を付与	書き込み	registry		
			schema		
RequestLogParsing	SparkUI のログ解析をリクエストする許可を付与する	権限の管理			
ResetJobBookmark	ジョブのブックマークをリセットする権限を付与します。	書き込み			
ResumeWorkflowRun	ワークフローの実行を再開する許可を付与	書き込み	workflow*		
RunDataPreviewStatement	Data Preview Statement を実行するための許可を付与します	権限の管理			
RunStatement	インタラクティブセッションでコードまたはステートメントを実行する許可を付与	書き込み	session*		
SearchTables	カタログ内のテーブルを取得する許可を付与。	読み取り	database*		
			rootcatalog*		
			table*		
			catalog		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SendFeedback	AWS Q でのグルー補完エクスペリエンスに関するフィードバックを提供するアクセス許可を付与します	書き込み			
SendRecipeAction	データプレビューで Data Preparation Recipe ステートメントを実行する許可を付与する	権限の管理			
StartBlueprintRun	ブループリントの実行を開始する許可を付与	書き込み	blueprint*		
StartColumnStatisticsTaskRun	テーブルの列統計の生成を開始する許可を付与	書き込み	database*		glue:GetSecurityConfiguration glue:GetTable
			rootcatalog*		
			table*		
StartColumnStatisticsTaskRunSchedule	列統計タスク実行スケジュールを開始するアクセス許可を付与します	書き込み	database*		
			rootcatalog*		
			table*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartCompletion	Glue for AWS Q experience で完了リクエストを作成するアクセス許可を付与します	書き込み			
StartCrawler	クローラを開始する許可を付与。	書き込み	crawler*		
StartCrawlerSchedule	クローラのスケジュール状態を SCHEDULED に変更する許可を付与。	書き込み			
StartDataQualityRuleRecommendationRun	推奨 Data Quality ルールの実行を開始する許可を付与	書き込み	dataQualityRuleset*		
StartDataQualityRulesetEvaluationRun	推奨 Data Quality ルールの実行を開始する許可を付与	書き込み	dataQualityRuleset*		
StartExportLabelsTaskRun	エクスポートラベル ML タスクの実行を開始する許可を付与。	書き込み	mlTransform*		
StartImportLabelsTaskRun	インポートラベル ML タスクの実行を開始する許可を付与。	書き込み	mlTransform*		
StartJobRun	ジョブの実行を開始する許可を付与	書き込み	job*		
StartJobUpgradeAnalysis	ジョブのアップグレード分析の実行を開始するアクセス許可を付与します	書き込み	job*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartMLEvaluationTaskRun	評価 ML タスクの実行を開始する許可を付与。	書き込み	mlTransform*		
StartMLLabelingSetGenerationTaskRun	ラベリングセット生成 ML タスクの実行を開始する許可を付与。	書き込み	mlTransform*		
StartNotebook	Glue Studio Notebooks を開始する許可を付与	権限の管理			
StartTrigger	トリガーを開始する許可を付与。	書き込み	trigger*		
StartWorkflowRun	ワークフローの実行を開始する許可を付与。	書き込み	workflow*		
StopColumnStatisticsTaskRun	列統計の実行を停止する許可を付与	書き込み	database*		
			rootcatalog*		
			table*		
StopColumnStatisticsTaskRunSchedule	列統計タスク実行スケジュールを停止するアクセス許可を付与します	書き込み	database*		
			rootcatalog*		
			table*		
StopCrawler	クローラの実行を停止する許可を付与。	書き込み	crawler*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StopCrawlerSchedule	クローラのスケジュール状態を NOT_SCHEDULED に設定する許可を付与。	書き込み			
StopJobUpgradeAnalysis	ジョブの継続的なアップグレード分析を停止するアクセス許可を付与します	書き込み	job*		
StopSession	インタラクティブセッションを停止する許可を付与	書き込み	session*		
StopTrigger	トリガーを停止する許可を付与。	書き込み	trigger*		
StopWorkflowRun	ワークフローの実行を停止する許可を付与	書き込み	workflow*		
TagResource	リソースにタグを追加するアクセス許可を付与します	Tagging	blueprint		
			connection		
			crawler		
			customEntityType		
			dataQualityRuleset		
			devendpoint		
			integration		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			job		
			mlTransform		
			registry		
			schema		
			session		
			trigger		
			usageProfile		
			workflow		
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateNotebook	Glue Studio Notebooks を終了する許可を付与	権限の管理			
TestConnection	Glue Studio で接続をテストする許可を付与	権限の管理			
UntagResource	リソースに関連付けられているタグを削除する許可を付与	Tagging	blueprint		
			connection		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			crawler		
			customEntityType		
			dataQualityRuleset		
			devendpoint		
			integration		
			job		
			mlTransform		
			registry		
			schema		
			session		
			trigger		
			usageProfile		
			workflow		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateBlueprint	ブループリントを更新する許可を付与	書き込み	blueprint*		
UpdateCatalog	カタログを更新するアクセス許可を付与します	書き込み	rootcatalog*		
			catalog		
UpdateClassifier	分類子を更新する許可を付与。	書き込み			
UpdateColumnStatisticsForPartition	列のパーティション統計を更新する許可を付与	書き込み	database*		
			rootcatalog*		
			table*		
			catalog		
UpdateColumnStatisticsForTable	列のテーブル統計を更新する許可を付与	書き込み	database*		
			rootcatalog*		
			table*		
			catalog		
UpdateColumnStatisticsTaskSettings	列統計タスクの設定を更新する許可を付与	書き込み	database*		
			rootcatalog*		
			table*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateConnection	接続を更新する許可を付与。	書き込み	connection*		
			rootcatalog*		
UpdateCrawler	クローラを更新する許可を付与。	書き込み	crawler*		
UpdateCrawlerSchedule	クローラのスケジュールを更新する許可を付与。	書き込み			
UpdateDataQualityRuleset	Data Quality のルールセットを更新する許可を付与	書き込み	dataQualityRuleset*		
UpdateDatabase	データベースを更新する許可を付与。	書き込み	database*		
			rootcatalog*		
			catalog		
UpdateDevEndpoint	開発エンドポイントを更新する許可を付与。	書き込み	devendpoint*		
UpdateGlueIdentityCenterConfiguration	マネージド Idc アプリケーションを更新する許可を付与	書き込み			
UpdateIntegrationResourceProperty	統合リソースプロパティを更新する許可を付与	書き込み	catalog*		
			connection*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			database*		
UpdateIntegrationTableProperties	統合テーブルのプロパティを更新する許可を付与	書き込み	catalog*		
			connection*		
			database*		
UpdateJob	ジョブを更新する許可を付与。	書き込み	job*		
				glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	
UpdateJobFromSourceControl	ソース管理プロバイダーからジョブを更新するための許可を付与します	書き込み	job*		
UpdateMLTransform	ML 変換を更新する許可を付与。	書き込み	mlTransform*		
UpdatePartition	パーティションを更新する許可を付与。	書き込み	database*		
			rootcatalog*		
			table*		
			catalog		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateRegistry	スキーマレジストリを更新する許可を付与します	書き込み	registry*		
UpdateSchema	スキーマコンテナを更新する許可を付与します	書き込み	registry*		
			schema*		
UpdateSourceControlFromJob	ジョブからソース管理プロバイダーを更新するための許可を付与します	書き込み	job*		
UpdateTable	テーブルを更新する許可を付与。	書き込み	database*		
			rootcatalog*		
			table*		
			catalog		
UpdateTableOptimizer	既存のテーブルオプティマイザーの設定を更新する許可を付与	書き込み	database*		glue:GetTable
			rootcatalog*		
			table*		
UpdateTrigger	トリガーを更新する許可を付与。	書き込み	trigger*		
UpdateUsageProfile	使用プロファイルを更新する許可を付与する	書き込み	usageProfile*		
	関数定義を更新する許可を付与。	書き込み	database*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateUserDefinedFunction			rootcatalog*		
			userdefinedfunction*		
			catalog		
UpdateWorkflow	ワークフローを更新する許可を付与。	書き込み	workflow*		
UpgradeJob	ジョブを最新バージョンにアップグレードするアクセス許可を付与します	書き込み	job*		
UseGlueStudio	Glue Studio の使用とその内部 API へのアクセス権限を付与する	権限の管理			
UseMLTransforms [許可のみ]	Glue ETL スクリプト内から ML 変換を使用する許可を付与。	書き込み	mlTransform*		

AWS Glue で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
rootcatalog	arn:${Partition}:glue:${Region}:${Account}:catalog	
catalog	arn:${Partition}:glue:${Region}:${Account}:catalog/${CatalogName}	
database	arn:${Partition}:glue:${Region}:${Account}:database/${DatabaseName}	
table	arn:${Partition}:glue:${Region}:${Account}:table/${DatabaseName}/${TableName}	
tableversion	arn:${Partition}:glue:${Region}:${Account}:tableVersion/${DatabaseName}/${TableName}/${TableVersionName}	
connection	arn:${Partition}:glue:${Region}:${Account}:connection/${ConnectionName}	aws:ResourceTag/${TagKey}
userdefinedfunction	arn:${Partition}:glue:${Region}:${Account}:userDefinedFunction/${DatabaseName}/${UserDefinedFunctionName}	
devendpoint	arn:${Partition}:glue:${Region}:${Account}:devEndpoint/${DevEndpointName}	aws:ResourceTag/${TagKey}
job	arn:${Partition}:glue:${Region}:${Account}:job/${JobName}	aws:ResourceTag/${TagKey}
trigger	arn:${Partition}:glue:${Region}:${Account}:trigger/${TriggerName}	aws:ResourceTag/${TagKey}
crawler	arn:${Partition}:glue:${Region}:${Account}:crawler/${CrawlerName}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
workflow	arn:${Partition}:glue:${Region}:${Account}:workflow/${WorkflowName}	aws:ResourceTag/${TagKey}
blueprint	arn:${Partition}:glue:${Region}:${Account}:blueprint/${BlueprintName}	aws:ResourceTag/${TagKey}
mlTransform	arn:${Partition}:glue:${Region}:${Account}:mlTransform/${TransformId}	aws:ResourceTag/${TagKey}
registry	arn:${Partition}:glue:${Region}:${Account}:registry/${RegistryName}	aws:ResourceTag/${TagKey}
schema	arn:${Partition}:glue:${Region}:${Account}:schema/${SchemaName}	aws:ResourceTag/${TagKey}
session	arn:${Partition}:glue:${Region}:${Account}:session/${SessionId}	aws:ResourceTag/${TagKey}
usageProfile	arn:${Partition}:glue:${Region}:${Account}:usageProfile/${UsageProfileId}	aws:ResourceTag/${TagKey}
dataQualityRuleset	arn:${Partition}:glue:${Region}:${Account}:dataQualityRuleset/${RulesetName}	aws:ResourceTag/${TagKey}
customEntityType	arn:${Partition}:glue:${Region}:${Account}:customEntityType/${CustomEntityTypeId}	aws:ResourceTag/${TagKey}
completion	arn:${Partition}:glue:${Region}:${Account}:completion/${CompletionId}	
integration	arn:${Partition}:glue:${Region}:${Account}:integration:${IntegrationId}	aws:ResourceTag/${TagKey}

AWS Glue の条件キー

AWS Glue では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString
glue:CredentialIssuingService	リクエストの認証情報が発行されたサービスでアクセスをフィルタリングします	String
glue:EnabledForRedshiftAutoDiscovery	ロールのアイデンティティベースのポリシー用に設定されたキーの存在によってアクセスをフィルタリングします	Bool
glue:RoleAssumedBy	顧客ロールを引き受けることによって、リクエストの資格情報が取得されるサービスでアクセスをフィルタリングします	String
glue:SecurityGroupIds	Glue ジョブで設定されたセキュリティグループの ID でアクセスをフィルタリングします	ArrayOfString
glue:SubnetIds	Glue ジョブで設定されたサブネットの ID でアクセスをフィルタリングします	ArrayOfString

条件キー	説明	[Type] (タイプ)
glue:VpcIds	Glue ジョブで設定された VPC の ID でアクセスをフィルタリングします	ArrayOfString

AWS Glue DataBrew のアクション、リソース、および条件キー

AWS Glue DataBrew (サービスプレフィックス: `databrew`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Glue DataBrew で定義されるアクション
- AWS Glue DataBrew で定義されるリソースタイプ
- AWS Glue DataBrew の条件キー

AWS Glue DataBrew で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchDeleteRecipeVersion	1 つ以上のレシピバージョンを削除する許可を付与	書き込み	Recipe*		
CreateDataset	データセットを作成する許可を付与	書き込み		aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:TagKeys aws:ResourceTag/${TagKey}	
CreateProfileJob	プロファイルジョブを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateProject	プロジェクトを作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateRecipe	recipe を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateRecipeJob	レシピジョブを作成する許可を付与します。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateRuleset	ルールセットを作成する許可を付与します。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSchedule	スケジュールを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteDataset	データセットを削除する許可を付与	書き込み	Dataset*		
DeleteJob	ジョブを削除する許可を付与	書き込み	Job*		
DeleteProject	プロジェクトを削除する許可を付与	書き込み	Project*		
DeleteRecipeVersion	recipe バージョンを削除する許可を付与	書き込み	Recipe*		
DeleteRuleset	ルールセットを削除するアクセス許可を付与します。	書き込み	Ruleset*		
DeleteSchedule	スケジュールを削除する許可を付与	書き込み	Schedule*		
DescribeDataset	データセットの詳細を表示する許可を付与	読み込み	Dataset*		
DescribeJob	ジョブの詳細を表示する許可を付与	読み込み	Job*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeJobRun	指定されたジョブのジョブ実行に関する詳細を表示する許可を付与	読み込み	Job*		
DescribeProject	プロジェクトの詳細を表示する許可を付与。	読み込み	Project*		
DescribeRecipe	recipe の詳細を表示する許可を付与	読み込み	Recipe*		
DescribeRuleset	ルールセットについての詳細を表示する許可を付与します。	読み込み	Ruleset*		
DescribeSchedule	スケジュールの詳細を表示する許可を付与	読み込み	Schedule*		
ListDatasets	アカウント内のデータセットを一覧表示する許可を付与	読み込み			
ListJobRuns	特定のジョブの実行を一覧表示する許可を付与	読み込み	Job*		
ListJobs	アカウントのジョブを一覧表示する許可を付与	読み込み			
ListProjects	アカウントのプロジェクトを一覧表示する許可を付与	読み込み			
ListRecipeVersions	recipe 内のバージョンを一覧表示する許可を付与	読み込み	Recipe*		
ListRecipes	アカウントの recipe を一覧表示する許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListRulesets	アカウント内のルールセットを一覧表示する権限を付与します。	読み込み			
ListSchedules	アカウントのスケジュールを一覧表示する許可を付与	読み込み			
ListTagsForResource	リソースに関連付けられているすべてのタグを取得する許可を付与	読み込み	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		
			Schedule		
PublishRecipe	recipe のメジャーバージョンを発行する許可を付与	書き込み	Recipe*		
SendProjectSessionAction	プロジェクトのインタラクティブなセッションにアクションを送信する許可を付与	書き込み	Project*		
StartJobRun	ジョブの実行を開始する許可を付与	書き込み	Job*		
StartProjectSession	プロジェクトのインタラクティブなセッションを開始する許可を付与	書き込み	Project*		
StopJobRun	ジョブのジョブ実行を停止する許可を付与	書き込み	Job*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
TagResource	リソースにタグを追加するアクセス許可を付与します	タグ付け	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		
			Schedule		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースに関連付けられているタグを削除する許可を付与	タグ付け	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		
			Schedule		
				aws:TagKeys	
UpdateDataset	データセットを変更する許可を付与	書き込み	Dataset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateProfileJob	プロファイルジョブを変更する許可を付与	書き込み	Job*		
UpdateProject	プロジェクトを変更する許可を付与	書き込み	Project*		
UpdateRecipe	recipe を変更する許可を付与	書き込み	Recipe*		
UpdateRecipeJob	recipe ジョブを変更する許可を付与	書き込み	Job*		
UpdateRuleset	ルールセットを変更する許可を付与します。	書き込み	Ruleset*		
UpdateSchedule	スケジュールを変更する許可を付与	書き込み	Schedule*		

AWS Glue DataBrew で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Project	arn:${Partition}:databrew:${Region}:${Account}:project/${ResourceId}	aws:ResourceTag/${TagKey}
Dataset	arn:${Partition}:databrew:${Region}:${Account}:dataset/${ResourceId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
Ruleset	arn:${Partition}:databrew:${Region}:${Account}:ruleset/${ResourceId}	aws:ResourceTag/${TagKey}
Recipe	arn:${Partition}:databrew:${Region}:${Account}:recipe/${ResourceId}	aws:ResourceTag/${TagKey}
Job	arn:${Partition}:databrew:${Region}:${Account}:job/${ResourceId}	aws:ResourceTag/${TagKey}
Schedule	arn:${Partition}:databrew:${Region}:${Account}:schedule/${ResourceId}	aws:ResourceTag/${TagKey}

AWS Glue DataBrew の条件キー

AWS Glue DataBrew では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Ground Station のアクション、リソース、および条件キー

AWS Ground Station (サービスプレフィックス: `groundstation`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Ground Station で定義されるアクション
- AWS Ground Station で定義されるリソースタイプ
- AWS Ground Station の条件キー

AWS Ground Station で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelContact	連絡先をキャンセルする許可を付与。	書き込み	Contact*		
CreateConfig	設定を作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataflowEndpointGroup	データフローエンドポイントグループを作成する許可を付与。	書き込み		aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
CreateEphemeris	エフェメリス項目を作成するための許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMissionProfile	ミッションプロファイルを作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfig	設定を削除する許可を付与。	書き込み	Config*		
DeleteDataflowEndpointGroup	データフローエンドポイントグループを削除する許可を付与。	書き込み	DataflowEndpointGroup*		
DeleteEphemeris	エフェメリス項目を削除するための許可を付与します	書き込み	EphemerisItem*		
DeleteMissionProfile	ミッションプロファイルを削除する許可を付与。	書き込み	MissionProfile*		
DescribeContact	連絡先を記述する許可を付与。	読み取り	Contact*		
DescribeEphemeris	エフェメリス項目を記述するための許可を付与します	読み取り	EphemerisItem*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetAgentConfiguration	エージェントの設定を取得するための許可を付与します	読み取り	Agent*		
GetConfig	設定を返すアクセス許可を付与します。	読み込み	Config*		
GetDataflowEndpointGroup	データフローエンドポイントグループを返すアクセス許可を付与します。	読み込み	DataflowEndpointGroup*		
GetMinuteUsage	使用分数を返すアクセス許可を付与します。	読み込み			
GetMissionProfile	ミッションプロファイルを取得する許可を付与。	読み込み	MissionProfile*		
GetSatellite	衛星に関する情報を返すアクセス許可を付与します。	読み込み	Satellite*		
ListConfigs	過去の設定のリストを返すためのアクセス許可を付与します	リスト			
ListContacts	連絡先のリストを返すアクセス許可を付与します。	リスト			
ListDataflowEndpointGroups	データフローエンドポイントグループを一覧表示する許可を付与。	リスト			
ListEphemerides	エフェメリスを一覧表示するための許可を付与します	リスト			
ListGroundStations	地上ステーションを一覧表示する許可を付与。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListMissionProfiles	ミッションプロファイルのリストを返すアクセス許可を付与します。	リスト			
ListSatellites	衛星を一覧表示する許可を付与。	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	Config		
			Contact		
			DataflowEndpointGroup		
			MissionProfile		
RegisterAgent	エージェントを登録するための許可を付与します	書き込み			
ReserveContact	連絡先を予約する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	リソースタグを割り当てるアクセス許可を付与	Tagging	Config		
			Contact		
			DataflowEndpointGroup		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			Ephemeris Item		
			MissionProfile		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	リソースタグの割り当てを解除するアクセス許可を付与します	Tagging	Config		
			Contact		
			DataflowEndpointGroup		
			Ephemeris Item		
			MissionProfile		
				aws:TagKeys	
UpdateAgentStatus	エージェントのステータスを更新するための許可を付与します	書き込み	Agent*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateConfig	設定を更新する許可を付与。	書き込み	Config*		
UpdateEphemeris	エフェメリス項目を更新するための許可を付与します	書き込み	EphemerisItem*		
UpdateMissionProfile	ミッションプロファイルを更新する許可を付与。	書き込み	MissionProfile*		

AWS Ground Station で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Config	`arn:${Partition}:groundstation:${Region}:${Account}:config/${ConfigType}/${ConfigId}`	aws:ResourceTag/${TagKey} groundstation:ConfigId groundstation:ConfigType
Contact	`arn:${Partition}:groundstation:${Region}:${Account}:contact/${ContactId}`	aws:ResourceTag/${TagKey} groundstation:ContactId

リソースタイプ	ARN	条件キー
DataflowEndpointGroup	arn:${Partition}:groundstation:${Region}:${Account}:dataflow-endpoint-group/${DataflowEndpointGroupId}	aws:ResourceTag/${TagKey} groundstation:DataflowEndpointGroupId
EphemerisItem	arn:${Partition}:groundstation:${Region}:${Account}:ephemeris/${EphemerisId}	aws:ResourceTag/${TagKey} groundstation:EphemerisId
GroundStationResource	arn:${Partition}:groundstation:${Region}:${Account}:groundstation:${GroundStationId}	groundstation:GroundStationId
MissionProfile	arn:${Partition}:groundstation:${Region}:${Account}:mission-profile/${MissionProfileId}	aws:ResourceTag/${TagKey} groundstation:MissionProfileId
Satellite	arn:${Partition}:groundstation:${Region}:${Account}:satellite/${SatelliteId}	groundstation:SatelliteId
Agent	arn:${Partition}:groundstation:${Region}:${Account}:agent/${AgentId}	groundstation:AgentId

AWS Ground Station の条件キー

AWS Ground Station では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
groundstation:AgentId	エージェントの ID でアクセスをフィルタリングします	String
groundstation:ConfigId	設定の ID でアクセスをフィルタリングします。	文字列
groundstation:ConfigType	設定のタイプでアクセスをフィルタリングします。	文字列
groundstation:ContactId	連絡先の ID でアクセスをフィルタリングします。	文字列
groundstation:DataflowEndpointGroupId	データフローエンドポイントグループの ID でアクセスをフィルタリングします。	String
groundstation:EphemerisId	エフェメリスの ID でアクセスをフィルタリングします	String
groundstation:GroundStationId	地上ステーションの ID でアクセスをフィルタリングします。	文字列

条件キー	説明	タイプ
groundstation:MissionProfileId	ミッションプロファイルの ID でアクセスをフィルタリングします。	文字列
groundstation:SatelliteId	衛星の ID でアクセスをフィルタリングします。	文字列

Amazon GroundTruth Labeling のアクション、リソース、および条件キー

Amazon GroundTruth Labeling (サービスプレフィックス: `groundtruthlabeling`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon GroundTruth Labeling で定義されるアクション
- Amazon GroundTruth Labeling で定義されるリソースタイプ
- Amazon GroundTruth Labeling の条件キー

Amazon GroundTruth Labeling で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociatePatchToManifestJob [ア	マニフェストファイルを更新するために、パッチファイル	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
クセス許可のみ]	をマニフェストファイルに関連付けるアクセス許可を付与				
CreateBatch [アクセス許可のみ]	GT バッチを作成するアクセス許可を付与します	書き込み			
CreateIntakeForm [アクセス許可のみ]	インテークフォームを作成する許可を付与する	書き込み			
CreateProject [アクセス許可のみ]	GT プロジェクトを作成するアクセス許可を付与します	書き込み			
CreateWorkflowDefinition [アクセス許可のみ]	GT ワークフロー定義を作成するアクセス許可を付与します	書き込み			
DescribeConsoleJob [アクセス許可のみ]	GroundTruthLabeling ジョブのステータスを取得する許可を付与。	Read			
GenerateLIDARPreviewTaskConfigJob [許可のみ]	LiDAR プレビュータスクを生成する許可を付与する	書き込み			
GetBatch [アクセス許可のみ]	GT バッチを取得するアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetIntakeFormStatus [許可のみ]	インテークフォームを取得する許可を付与する	読み取り			
ListBatches [許可のみ]	GT バッチを一覧表示するアクセス許可を付与します	読み取り			
ListDatasetObjects [許可のみ]	マニフェストファイル内のデータセットオブジェクトを一覧表示する許可を付与。	Read			
ListProjects [許可のみ]	GT プロジェクトを一覧表示するアクセス許可を付与します	読み取り			
RunFilterOrSampleDatasetJob [許可のみ]	S3 Select を使用してマニフェストファイルからレコードをフィルタリングする許可を付与。ランダムサンプリングに基づいてサンプルエントリを取得します。	Write			
RunGenerateManifestByCrawlingJob [アクセス許可のみ]	S3 プレフィックスを一覧表示し、その場所にオブジェクトからのマニフェストファイルを作成する許可を付与。	書き込み			
RunGenerateManifestMetricsJob [アクセス許可のみ]	マニフェスト内のオブジェクトからメトリクスを生成する許可を付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateBatch [アクセス許可のみ]	GT バッチを更新するアクセス許可を付与します	書き込み			

Amazon GroundTruth Labeling で定義されるリソースタイプ

Amazon GroundTruth Labeling では、IAM ポリシーステートメントの `Resource` 要素でのリソース ARN の指定はサポートされていません。Amazon GroundTruth Labeling へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

Amazon GroundTruth Labeling の条件キー

GroundTruth Labeling には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon GuardDuty のアクション、リソース、および条件キー

Amazon GuardDuty (サービスプレフィックス: `guardduty`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon GuardDuty で定義されるアクション
- Amazon GuardDuty で定義されるリソースタイプ

- Amazon GuardDuty の条件キー

Amazon GuardDuty で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AcceptAdministratorInvitation	GuardDuty メンバーアカウントになるための招待を受け入れるアクセス許可を付与します	書き込み			
AcceptInvitation	GuardDuty メンバーアカウントになるための招待を受け入れるアクセス許可を付与します	Write			
ArchiveFindings	GuardDuty の結果をアーカイブする許可を付与	Write			
CreateDetector	ディテクターを作成する許可を付与	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateFilter	GuardDuty フィルターを作成する許可を付与。フィルターは、結果のフィルタリングに使用される結果の属性と条件を定義します	Write	filter*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateIPSet	IPSet を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:DeleteRolePolicy iam:PutRolePolicy
CreateMalwareProtectionPlan	新しい Malware Protection プランを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateMembers	GuardDuty メンバーアカウントを作成する許可を付与。メンバーの作成に使用したアカウントが GuardDuty 管理者アカウントになります	Write			
CreatePublishingDestination	発行先を作成する許可を付与	Write			s3:GetObject s3:ListBucket

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateSampleFindings	サンプル結果を作成する許可を付与。	書き込み			
CreateThreatEntitySet	GuardDuty ThreatEntitySets を作成するアクセス許可を付与します。ThreatEntitySet は、GuardDuty が検出結果を生成するために使用される既知の悪意のある IP アドレスやドメインで構成されます。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
CreateThreatIntelSet	GuardDuty ThreatIntelSet を作成する許可を付与。ThreatIntelSet は、GuardDuty が結果を生成するために使用する既知の悪意のある IP アドレスで構成されます	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrustedEntitySet	TrustedEntitySet を作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject
DeclineInvitations	GuardDuty メンバーアカウントになるための招待を拒否する許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteDetector	GuardDuty ディテクターを削除する許可を付与	Write	detector*		
DeleteFilter	GuardDuty フィルターを削除する許可を付与	Write	filter*		
DeleteIPSet	GuardDuty IPSets を削除する許可を付与	Write	ipset*		
DeleteInvitations	GuardDuty メンバーアカウントになるための招待を削除する許可を付与	書き込み			
DeleteMalwareProtectionPlan	Malware Protection プランを削除する許可を付与する	書き込み	malwareprotectionplan*		
DeleteMembers	GuardDuty メンバーアカウントを削除する許可を付与	Write			
DeletePublishingDestination	発行先を削除する許可を付与	書き込み	publishingDestination*		
DeleteThreatEntitySet	GuardDuty ThreatEntitySets を削除するアクセス許可を付与します	書き込み	threatentityset*		
DeleteThreatIntelSet	GuardDuty ThreatIntelSets を削除する許可を付与	書き込み	threatintelset*		
DeleteTrustedEntitySet	GuardDuty TrustedEntitySets を削除するアクセス許可を付与します	書き込み	trustedentityset*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeMalwareScans	マルウェアスキャンの詳細を削除する許可を付与します	読み取り			
DescribeOrganizationConfiguration	GuardDuty ディテクターに関連付けられた委任管理者に関する詳細を取得する許可を付与	Read			
DescribePublishingDestination	発行先の詳細を取得する許可を付与	Read	publishingDestination*		
DisableOrganizationAdminAccount	GuardDuty の組織の委任管理者を無効にする許可を付与	書き込み			
DisassociateFromAdministratorAccount	GuardDuty メンバーアカウントと GuardDuty マスターアカウントの関連付けを解除する許可を付与する	書き込み			
DisassociateFromMasterAccount	GuardDuty メンバーアカウントと GuardDuty マスターアカウントの関連付けを解除する許可を付与する	書き込み			
DisassociateMembers	GuardDuty メンバーアカウントの管理者 GuardDuty アカウントとの関連付けを解除する許可を付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
EnableOrganizationAdminAccount	GuardDuty の組織の委任管理者を有効にする許可を付与	書き込み			
GetAdministratorAccount	メンバーアカウントに関連付けられている GuardDuty 管理者アカウントの詳細を取得する許可を付与する	読み取り			
GetCoverageStatistics	リージョン内で指定した GuardDuty アカウントについて、Amazon GuardDuty のカバレッジ状況の統計を一覧表示するための許可を付与	読み取り	detector*		
GetDetector	GuardDuty ディテクターを取得する許可を付与	Read	detector*		
GetFilter	GuardDuty フィルターを取得する許可を付与	Read	filter*		
GetFindings	GuardDuty の結果を取得する許可を付与	Read			
GetFindingsStatistics	GuardDuty の結果統計のリストを取得する許可を付与	読み取り			
GetIPSet	GuardDuty IPSets を取得する許可を付与	読み取り	ipset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetInvitationsCount	指定されたアカウントに送信されたすべての GuardDuty 招待の件数を取得する許可を付与。このアカウントには、承認された招待は含まれません	読み取り			
GetMalwareProtectionPlan	Malware Protection プランの詳細を取得する許可を付与する	読み取り	malwareprotectionplan*		
GetMalwareScanSettings	マルウェアスキャン設定を取得する許可を付与	読み取り			
GetMasterAccount	メンバーアカウントに関連付けられている GuardDuty 管理者アカウントの詳細を取得する許可を付与する	読み取り			
GetMemberDetectors	メンバーアカウントディテクターで有効になっているデータソースを記述する許可を付与	読み取り			
GetMembers	管理者アカウントに関連付けられたメンバーアカウントを取得する許可を付与する	読み取り			
GetOrganizationStatistics	リージョンのメンバーアカウントの GuardDuty 保護プランの適用範囲統計を取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetRemainingFreeTrialDays	無料試用期間に使用された各データソースの残り日数を提供するアクセス許可を付与	読み取り			
GetThreatEntitySet	GuardDuty ThreatEntitySets を取得するアクセス許可を付与します	読み取り	threatentityset*		
GetThreatIntelSet	GuardDuty ThreatIntelSets を取得する許可を付与	読み取り	threatintelset*		
GetTrustedEntitySet	GuardDuty TrustedEntitySets を取得するアクセス許可を付与します	読み取り	trustedentityset*		
GetUsageStatistics	指定されたディテクター ID について、過去 30 日間の Amazon GuardDuty の使用状況の統計を一覧表示する許可を付与	読み取り			
InviteMembers	GuardDuty を有効にして GuardDuty メンバー AWS アカウントになるように他のアカウントを招待するアクセス許可を付与します	書き込み			
ListCoverage	リソース内の特定のアカウントについて、すべてのリソースの詳細を一覧表示する許可を付与	リスト	detector*		
ListDetectors	GuardDuty ディテクターのリストを取得する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListFilters	GuardDuty フィルターのリストを取得する許可を付与	リスト			
ListFindings	GuardDuty の結果のリストを取得する許可を付与	リスト			
ListIPSets	GuardDuty IPSets のリストを取得する許可を付与	リスト			
ListInvitations	に送信されたすべての GuardDuty メンバーシップ招待のリストを取得するアクセス許可を付与します AWS アカウント	リスト			
ListMalwareProtectionPlans	Malware Protection プランのリストを取得する許可を付与する	リスト			
ListMembers	管理者アカウントに関連付けられている GuardDuty メンバーアカウントのリストを取得する許可を付与する	リスト			
ListOrganizationAdminAccounts	GuardDuty の組織の委任管理者に関する詳細を一覧表示する許可を付与	リスト			
ListPublishingDestinations	発行先のリストを取得する許可を付与	リスト			
ListTagsForResource	GuardDuty リソースに関連付けられたタグのリストを取得する許可を付与	読み取り	detector		
			filter		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			ipset		
			malwareprotectionplan		
			threatentityset		
			threatintelset		
			trustedentityset		
ListThreatEntitySets	GuardDuty ThreatEntitySets のリストを取得するアクセス許可を付与します	リスト			
ListThreatIntelSets	GuardDuty ThreatIntelSets のリストを取得する許可を付与	リスト			
ListTrustedEntitySets	GuardDuty TrustedEntitySets のリストを取得するアクセス許可を付与します	リスト			
SendSecurityTelemetry	リージョン内の特定の GuardDuty アカウントに対するセキュリティテレメトリを送信する許可を付与	書き込み			
StartMalwareScan	新しいマルウェアスキャンを開始する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartMonitoringMembers	GuardDuty 管理者アカウントに GuardDuty メンバーアカウントからの調査結果をモニタリングする許可を付与	Write			
StopMonitoringMembers	メンバーアカウントからの結果のモニタリングを無効にする許可を付与	Write			
TagResource	GuardDuty リソースにタグを追加する許可を付与	タグ付け	detector		
			filter		
			ipset		
			malwareprotectionplan		
			threatentityset		
			threatintelset		
			trustedentityset		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UnarchiveFindings	GuardDuty の結果を解凍する許可を付与	Write			
UntagResource	GuardDuty リソースからタグを削除する許可を付与	タグ付け	detector		
			filter		
			ipset		
			malwareprotectionplan		
			threatentityset		
			threatintelset		
			trustedentityset		
				aws:TagKeys	
UpdateDetector	GuardDuty ディテクターを更新する許可を付与	Write	detector*		
UpdateFilter	GuardDuty フィルターを更新する許可を付与	Write	filter*		
UpdateFindingsFeedback	GuardDuty の結果を有用または無用としてマークするように、結果のフィードバックを更新する許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateIPSet	GuardDuty IPSets を更新する許可を付与	書き込み	ipset*		iam:DeleteRolePolicy iam:PutRolePolicy
UpdateMalwareProtectionPlan	Malware Protection プランを更新する許可を付与する	書き込み	malwareprotectionplan*		
UpdateMalwareScanSettings	マルウェアスキャン設定を更新する許可を付与	書き込み			
UpdateMemberDetectors	メンバーアカウントディテクターで有効になっているデータソースを更新する許可を付与	Write			
UpdateOrganizationConfiguration	GuardDuty ディテクターに関連付けられた委任管理者設定を更新する許可を付与	Write			
UpdatePublishingDestination	発行先を更新する許可を付与	書き込み	publishingDestination*		s3:GetObject s3:ListBucket
UpdateThreatEntitySet	GuardDuty ThreatEntitySets を更新する許可を付与	書き込み	threatentityset*		s3:GetObject

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateThreatIntelSet	GuardDuty ThreatIntelSets を更新する許可を付与	書き込み	threatintelset*		iam:DeleteRolePolicy iam:PutRolePolicy
UpdateTrustedEntitySet	GuardDuty TrustedEntitySets を更新する許可を付与	書き込み	trustedentityset*		s3:GetObject

Amazon GuardDuty で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
detector	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}`	aws:ResourceTag/${TagKey}
filter	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/filter/${FilterName}`	aws:ResourceTag/${TagKey}
ipset	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/ipset/${IPSetId}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
threatintelset	arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/threatintelset/${ThreatIntelSetId}	aws:ResourceTag/${TagKey}
trustedentityset	arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/trustedentityset/${TrustedEntitySetId}	aws:ResourceTag/${TagKey}
threatentityset	arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/threatentityset/${ThreatEntitySetId}	aws:ResourceTag/${TagKey}
publishingDestination	arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/publishingDestination/${PublishingDestinationId}	
malwareprotectionplan	arn:${Partition}:guardduty:${Region}:${Account}:malware-protection-plan/${MalwareProtectionPlanId}	aws:ResourceTag/${TagKey}

Amazon GuardDuty の条件キー

Amazon GuardDuty では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Health APIs and Notifications のアクション、リソース、および条件キー

AWS Health APIsと通知 (サービスプレフィックス: `health`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Health APIs and Notifications で定義されるアクション
- AWS Health APIs and Notifications で定義されるリソースタイプ
- AWS Health APIs and Notifications の条件キー

AWS Health APIs and Notifications で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeAffectedAccountsForOrganization	組織内の指定されたイベントの影響を受けたアカウントのリストを取得する許可を付与	読み取り			organizations:ListAccounts
DescribeAffectedEntities	指定されたイベントの影響を受けたエンティティのリストを取得する許可を付与	読み取り	event*		
				health:eventTypeCode health:service	
DescribeAffectedEntitiesForOrganization	組織内の指定されたイベントおよびアカウントの影響を受けたエンティティのリストを取得する許可を付与	読み取り			organizations:ListAccounts
DescribeEntityAggregates	指定されたそれぞれのイベントによって影響を受けるエンティティの数を取得する許可を付与	読み取り			
DescribeEntityAggregatesForOrganization	組織内の指定された各イベントによって影響を受けるエンティティの数を取得するための許可を付与します	読み取り			organizations:ListAccounts
DescribeEventAggregates	各イベントタイプ (発行、スケジュール変更、およびアカウント通知) のイベント数を取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeEventDetails	1 つ以上の指定されたイベントに関する詳細情報を取得する許可を付与	読み取り	event*		
				health:eventTypeCode health:service	
DescribeEventDetailsForOrganization	組織内の指定されたアカウントに対して指定された 1 つ以上のイベントに関する詳細情報を取得する許可を付与	読み取り			organizations:ListAccounts
DescribeEventTypes	指定されたフィルター条件に一致するイベントタイプを取得する許可を付与	読み取り			
DescribeEvents	指定されたフィルター条件に一致するイベントに関する情報を取得する許可を付与	読み取り			
DescribeEventsForOrganization	組織内の指定されたフィルター条件に一致するイベントに関する情報を取得する許可を付与	読み取り			organizations:ListAccounts
DescribeHealthServiceStatusForOrganization	組織ビュー機能の有効化または無効化のステータスを取得する許可を付与	読み取り			organizations:ListAccounts

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisableHealthServiceAccessForOrganization	組織ビュー機能を無効にする許可を付与	権限の管理			organizations:DisableAWSServiceAccess organizations:ListAccounts
EnableHealthServiceAccessForOrganization	組織ビュー機能を有効にする許可を付与	権限の管理			iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess organizations:ListAccounts

AWS Health APIs and Notifications で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
event	arn:${Partition}:health:*::event/${Service}/${EventTypeCode}/*	

AWS Health APIs and Notifications の条件キー

AWS Health APIsと通知では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
health:eventTypeCode	イベントタイプでアクセスをフィルタリング	String
health:service	影響を受けるサービスでアクセスをフィルタリング	String

AWS HealthImaging のアクション、リソース、および条件キー

AWS HealthImaging (サービスプレフィックス: medical-imaging) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS HealthImaging によって定義されたアクション
- AWS HealthImaging によって定義されたリソースタイプ
- AWS HealthImaging の条件キー

AWS HealthImaging によって定義されたアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CopyImageSet	イメージセットをコピーするための許可を付与します	書き込み	datastore*		
			imageset*		
CreateDatastore	イメージングデータを取り込むためにデータストアを作成するための許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDatastore	データストアを削除するための許可を付与します	書き込み	datastore*		
DeleteImageSet	イメージセットを削除するための許可を付与します	書き込み	datastore*		
			imageset*		
GetDICOMBulkdata	バイナリ形式で dicom bulkdata を取得する許可を付与	読み取り	datastore*		
GetDICOMImportJob	インポートジョブのプロパティを取得するための許可を付与します	読み取り	datastore*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetDICOMInstance	dcm 形式で dicom インスタンスを取得する許可を付与する	読み取り	datastore*		
GetDICOMInstanceFrames	顧客がリクエストした形式で dicom インスタンスフレームを取得する許可を付与する	読み取り	datastore*		
GetDICOMInstanceMetadata	DICOM JSON 形式で dicom インスタンスメタデータを取得する許可を付与する	読み取り	datastore*		
GetDICOMSeriesMetadata	特定の DICOM シリーズに属するすべての DICOM インスタンスのメタデータを DICOM JSON 形式で取得するアクセス許可を付与します	読み取り	datastore*		
GetDatastore	データストアのプロパティを取得するための許可を付与します	読み取り	datastore*		
GetImageFrame	イメージフレームのプロパティを取得するための許可を付与します	読み取り	datastore*		
			imageset*		
GetImageSet	イメージセットのプロパティを取得するための許可を付与します	読み取り	datastore*		
			imageset*		
GetImageSetMetadata	イメージセットのメタデータプロパティを取得するための許可を付与します	読み取り	datastore*		
			imageset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListDICOMImportJobs	データストアのインポートジョブを一覧表示するための許可を付与します	リスト	datastore*		
ListDatastores	データストアを一覧表示するための許可を付与します	リスト			
ListImageSetVersions	イメージセットのバージョンを一覧表示するための許可を付与します	リスト	datastore*		
			imageset*		
ListTagsForResource	医用画像リソースのタグを一覧表示するための許可を付与します	リスト	datastore		
			imageset		
SearchDICOMInstances	DICOM JSON 形式でデータを返す dicom インスタンスを検索する許可を付与	読み取り	datastore*		
SearchDICOMSeries	DICOM JSON 形式でデータを返す dicom シリーズを検索する許可を付与	読み取り	datastore*		
SearchDICOMStudies	DICOM JSON 形式でデータを返す dicom スタディを検索する許可を付与	読み取り	datastore*		
SearchImageSets	イメージセットを検索するための許可を付与します	読み取り	datastore*		
StartDICOMImportJob	DICOM インポートジョブを開始するための許可を付与します	書き込み	datastore*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StoreDICOM	結果を DICOM JSON 形式で返す dicom インスタンスを保存するアクセス許可を付与します	書き込み	datastore*		
StoreDICOMStudy	結果を DICOM JSON 形式で返す DICOM 検査を保存するアクセス許可を付与します	書き込み	datastore*		
TagResource	医用画像リソースにタグを追加するための許可を付与します	Tagging	datastore		
			imageset		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	医用画像リソースからタグを削除するための許可を付与します	Tagging	datastore		
			imageset		
				aws:TagKeys	
UpdateImageSetMetadata	イメージセットのメタデータプロパティを更新するための許可を付与します	書き込み	datastore*		
			imageset*		

AWS HealthImaging によって定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
datastore	`arn:${Partition}:medical-imaging:${Region}:${Account}:datastore/${DatastoreId}`	aws:ResourceTag/${TagKey}
imageset	`arn:${Partition}:medical-imaging:${Region}:${Account}:datastore/${DatastoreId}/imageset/${ImageSetId}`	aws:ResourceTag/${TagKey}

AWS HealthImaging の条件キー

AWS HealthImaging では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	文字列

条件キー	説明	タイプ
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString

AWS HealthLake のアクション、リソース、および条件キー

AWS HealthLake (サービスプレフィックス: healthlake) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS HealthLake によって定義されたアクション
- AWS HealthLake によって定義されたリソースタイプ
- AWS HealthLake の条件キー

AWS HealthLake によって定義されたアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelFHIRExportJobWithDelete	Delete で実行中の FHIR エクスポートジョブをキャンセルする許可を付与する	書き込み	datastore*		
CreateFHIRDatastore	FHIR データの取り込みと エクスポートが可能なデータストアを作成する許可を付与	書き込み		aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
CreateResource	リソースを作成する許可を付与	書き込み	datastore*		
DeleteFHIRDatastore	データストアを削除する許可を付与	書き込み	datastore*		
DeleteResource	リソースを削除する許可を付与	書き込み	datastore*		
DescribeFHIRDatastore	データストア ID、データストア ARN、データストア名、データストアの状態、作成場所、データストアタイプのバージョン、データストアエンドポイントなど、FHIR データストアに関連付けられたプロパティを取得するためのアクセス許可を付与します	読み込み	datastore*		
DescribeFHIRExportJob	データストアの ID、ARN、名前、ステータスなど、FHIR エクスポートジョブのプロパティを表示する許可を付与	読み取り	datastore*		
DescribeFHIRExportJobWithGet	Get でデータストアの ID、ARN、名前、ステータスなど、FHIR エクスポートジョブのプロパティを表示する許可を付与する	読み取り	datastore*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeFHIRImportJob	データストアの ID、ARN、名前、ステータスなど、FHIR インポートジョブのプロパティを表示する許可を付与	読み込み	datastore*		
GetCapabilities	FHIR データストアの機能を取得する許可を付与	読み取り	datastore*		
GetExportedFile	Get で開始された FHIR Export ジョブからエクスポートされたファイルにアクセスする許可を付与	読み取り	datastore*		
GetHistoryByResourceId	リソース履歴を読み取るアクセス許可を付与します	読み取り	datastore*		
ListFHIRDatastores	データストアのステータスに関係なく、ユーザーのアカウントにあるすべての FHIR データストアを一覧表示する許可を付与する	リスト			
ListFHIRExportJobs	指定したデータストアのエクスポートジョブのリストを取得する許可を付与	リスト	datastore*		
ListFHIRImportJobs	指定したデータストアのインポートジョブのリストを取得する許可を付与	リスト	datastore*		
ListTagsForResource	指定されたデータストアのタグのリストを取得する許可を付与	リスト	datastore		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ProcessBundle	複数のリソースオペレーションをバンドルするアクセス許可を付与します	書き込み	datastore*		
ReadResource	リソースを読み取るアクセス許可を付与します	読み取り	datastore*		
SearchEverything	患者に関連するすべてのリソースを検索する許可を付与する	読み取り	datastore*		
SearchWithGet	GET メソッドでリソースを検索する許可を付与	読み込み	datastore*		
SearchWithPost	POST メソッドでリソースを検索する許可を付与	読み込み	datastore*		
StartFHIRExportJob	FHIR エクスポートジョブを開始する許可を付与	書き込み	datastore*		
StartFHIRExportJobWithGet	Get で FHIR エクスポートジョブを開始する許可を付与	書き込み	datastore*		
StartFHIRExportJobWithPost	Post で FHIR エクスポートジョブを開始する許可を付与する	書き込み	datastore*		
StartFHIRImportJob	FHIR インポートジョブを開始する許可を付与	書き込み	datastore*		
TagResource	データストアにタグを追加する許可を付与	タグ付け	datastore		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	データストアに関連付けられているタグを削除する許可を付与	タグ付け	datastore		
				aws:TagKeys	
UpdateResource	リソースを更新する許可を付与	書き込み	datastore*		
VersionReadResource	リソースのバージョンを読み取るアクセス許可を付与します	読み取り	datastore*		

AWS HealthLake によって定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
datastore	arn:${Partition}:healthlake:${Region}:${Account}:datastore/fhir/${DatastoreId}	aws:ResourceTag/${TagKey}

AWS HealthLake の条件キー

AWS HealthLake は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアによってアクセスをフィルタリングする	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

AWS HealthOmics のアクション、リソース、および条件キー

AWS HealthOmics (サービスプレフィックス: omics) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS HealthOmics によって定義されたアクション
- AWS HealthOmics によって定義されたリソースタイプ
- AWS HealthOmics の条件キー

AWS HealthOmics によって定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AbortMultipartReadSetUpload	リードセットのマルチパートアップロードを中止する許可を付与	書き込み	sequenceStore*		
AcceptShare	共有を承諾する許可を付与	書き込み			
BatchDeleteReadSet	特定の Sequence Store 内のリードセットを一括で削除する許可を付与	書き込み	sequenceStore*		
CancelAnnotationImportJob	Annotation Import Job をキャンセルする許可を付与	書き込み			
CancelRun	ワークフロータスクの実行をキャンセルし、すべてのワークフロータスクを停止する許可を付与	書き込み	run*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CancelVariantImportJob	Variant Import Job をキャンセルする許可を付与	書き込み			
CompleteMultipartReadSetUpload	リードセットのマルチパートアップロードを完了する許可を付与	書き込み	sequenceStore*		
CreateAnnotationStore	Annotation Store を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnnotationStoreVersion	Annotation Store のバージョンを作成する許可を付与	書き込み	AnnotationStore*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMultipartReadSetUpload	リードセットのマルチパートアップロードを作成する許可を付与	書き込み	sequenceStore*		
CreateReferenceStore	Reference Store を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateRunCache	新しいワークフロー実行キャッシュを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRunGroup	新しいワークフロー実行グループを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSequenceStore	Sequence Store を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateShare	共有を作成する許可を付与	書き込み			
CreateVariantStore	Variant Store を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateWorkflow	ワークフロー定義とワークフローパラメータのテンプレートを使用して新しいワークフローを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkflowVersion	ワークフロー定義とワークフローパラメータのテンプレートを使用して新しいワークフローバージョンを作成するアクセス許可を付与します	書き込み	workflow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAnnotationStore	Annotation Store を削除する許可を付与	書き込み	AnnotationStore*		
DeleteAnnotationStoreVersions	Annotation Store のバージョンを削除する許可を付与	書き込み	AnnotationStore*		
			AnnotationStoreVersion*		
DeleteReference	指定された Reference Store のリファレンスを削除する許可を付与	書き込み	reference*		
			referenceStore*		
DeleteReferenceStore	Reference Store を削除する許可を付与	書き込み	referenceStore*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteRun	ワークフロー実行を削除する許可を付与	書き込み	run*		
DeleteRunCache	ワークフロー実行キャッシュを削除するアクセス許可を付与します	書き込み	runCache*		
DeleteRunGroup	ワークフロー実行グループを削除する許可を付与	書き込み	runGroup*		
DeleteS3AccessPolicy	特定のストアのアクセスポリシーを削除するアクセス許可を付与します	書き込み	sequenceStore*		
DeleteSequenceStore	Sequence Store を削除する許可を付与	書き込み	sequenceStore*		
DeleteShare	共有を削除する許可を付与	書き込み			
DeleteVariantStore	Variant Store を削除する許可を付与	書き込み	VariantStore*		
DeleteWorkflow	ワークフローを削除するアクセス許可を与えます。	書き込み	workflow*		
DeleteWorkflowVersion	ワークフローバージョンを削除するアクセス許可を付与します	書き込み	WorkflowVersion*		
			workflow*		
GetAnnotationImportJob	Annotation Import Job のステータスを取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetAnnotationStore	Annotation Store に関する詳細情報を取得する許可を付与	読み取り	AnnotationStore*		
GetAnnotationStoreVersion	Annotation Store のバージョンに関する詳細情報を取得する許可を付与	読み取り	AnnotationStoreVersion*		
GetReadSet	特定の Sequence Store のリードセットを取得する許可を付与	読み取り	readSet*		
			sequenceStore*		
GetReadSetActivationJob	特定の Sequence Store 用におけるリードセットのアクティベーションジョブに関する詳細を取得する許可を付与	読み取り	sequenceStore*		
GetReadSetExportJob	特定の Sequence Store におけるリードセットのエクスポートジョブに関する詳細を取得する許可を付与	読み取り	sequenceStore*		
GetReadSetImportJob	特定の Sequence Store のリードセットのインポートジョブに関する詳細を取得する許可を付与	読み取り	sequenceStore*		
GetReadSetMetadata	特定の Sequence Store のリードセットに関する詳細を取得する許可を付与	読み取り	readSet*		
			sequenceStore*		
GetReference	特定の Reference Store のリファレンスを取得する許可を付与	読み取り	reference*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			referenceStore*		
GetReferenceImportJob	特定の Reference Store におけるリファレンスのインポートジョブに関する詳細を取得する許可を付与	読み取り	referenceStore*		
GetReferenceMetadata	特定の Reference Store におけるリファレンスに関する詳細を取得する許可を付与	読み取り	reference*		
			referenceStore*		
GetReferenceStore	Reference Store に関する詳細を取得する許可を付与	読み取り	referenceStore*		
GetRun	ワークフロー実行の詳細を取得する許可を付与	読み取り	run*		
GetRunCache	ワークフロー実行キャッシュの詳細を取得するアクセス許可を付与します	読み取り	runCache*		
GetRunGroup	ワークフロー実行グループの詳細を取得する許可を付与	読み取り	runGroup*		
GetRunTask	ワークフロータスクの詳細を取得する許可を付与	読み取り	TaskResource*		
			run*		
GetS3AccessPolicy	特定のストアのアクセスポリシーに関する詳細を取得するアクセス許可を付与します	読み取り	sequenceStore*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetSequenceStore	Sequence Store に関する詳細を取得する許可を付与	読み取り	sequenceStore*		
GetShare	共有に関する詳細情報を取得する許可を付与	読み取り			
GetVariantImportJob	Variant Import Job のステータスを取得する許可を付与	読み取り			
GetVariantStore	Variant Store に関する詳細情報を取得する許可を付与	読み取り	VariantStore*		
GetWorkflow	ワークフロー詳細を取得する許可を付与	読み取り	workflow*		
GetWorkflowVersion	ワークフローバージョンの詳細を取得するアクセス許可を付与します	読み取り	WorkflowVersion*		
			workflow*		
ListAnnotationImportJobs	Annotation Import Job の一覧表示を取得する許可を付与	リスト			
ListAnnotationStoreVersions	Annotation Store のバージョンに関する情報の一覧を取得する許可を付与	リスト	AnnotationStore*		
ListAnnotationStores	Annotation Store に関する情報の一覧表示を取得する許可を付与	リスト			
ListMultipartReadSetUploads	リードセットのマルチパートアップロードを一覧表示する許可を付与	リスト	sequenceStore*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListReadSetActivationJobs	特定の Sequence Store におけるリードセットのアクティベーションジョブを一覧表示する許可を付与	リスト	sequenceStore*		
ListReadSetExportJobs	特定の Sequence Store におけるリードセットのエクスポートジョブを一覧表示する許可を付与	リスト	sequenceStore*		
ListReadSetImportJobs	特定の Sequence Store におけるリードセットのインポートジョブを一覧表示する許可を付与	リスト	sequenceStore*		
ListReadSetUploadParts	リードセットのアップロードパーツを一覧表示する許可を付与	リスト	sequenceStore*		
ListReadSets	特定の Sequence Store のリードセットを一覧表示する許可を付与	リスト	sequenceStore*		
ListReferenceImportJobs	特定の Reference Store におけるリファレンスのインポートジョブを一覧表示する許可を付与	リスト	referenceStore*		
ListReferenceStores	Reference Store を一覧表示する許可を付与	リスト			
ListReferences	特定の Reference Store のリファレンスを一覧表示する許可を付与	リスト	referenceStore*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListRunCaches	ワークフロー実行キャッシュのリストを取得するアクセス許可を付与します	リスト			
ListRunGroups	ワークフローグループのリストを取得する許可を付与	リスト			
ListRunTasks	ワークフロー実行タスクのリストを取得する許可を付与	リスト	run*		
ListRuns	ワークフロー実行のリストを取得する許可を付与	リスト			
ListSequenceStores	Sequence Store を一覧表示する許可を付与	リスト			
ListShares	共有に関する情報の一覧を取得する許可を付与	リスト			
ListTagsForResource	リソース AWS タグのリストを取得するアクセス許可を付与します	リスト			
ListVariantImportJobs	Variant Import Job のリストを取得する許可を付与	リスト			
ListVariantStores	Variant Store におけるメタデータのリストを取得する許可を付与	リスト			
ListWorkflowVersions	ワークフローで使用可能なバージョンのリストを取得するアクセス許可を付与します	リスト	workflow*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListWorkflows	可能なワークフローのリストを取得する許可を付与	リスト			
PutS3AccessPolicy	特定のストアにアクセスポリシーを配置するアクセス許可を付与します	書き込み	sequenceStore*		
StartAnnotationImportJob	Annotation ファイルのリストを Annotation Store にインポートする許可を付与	書き込み	AnnotationStore*		
			AnnotationStoreVersion*		
StartReadSetActivationJob	特定の Sequence Store におけるリードセットのアクティベーションジョブを開始する許可を付与	書き込み	sequenceStore*		
StartReadSetExportJob	特定の Sequence Store におけるリードセットのエクスポートジョブを開始する許可を付与	書き込み	sequenceStore*		
StartReadSetImportJob	特定の Sequence Store におけるリードセットのインポートジョブを開始する許可を付与	書き込み	sequenceStore*		
StartReferenceImportJob	特定の Reference Store におけるリファレンスのインポートジョブを開始する許可を付与	書き込み	referenceStore*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartRun	ワークフローの実行を開始する許可を付与	書き込み	run*		iam:PassRole
			runCache		
			runGroup		
			workflow		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartVariantImportJob	Variant ファイルのリストを Variant Store にインポートする許可を付与	書き込み	VariantStore*		
TagResource	リソースに AWS タグを追加するアクセス許可を付与します	Tagging	AnnotationStore		
			AnnotationStoreVersion		
			VariantStore		
			WorkflowVersion		
			readSet		
			reference		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			referenceStore		
			run		
			runCache		
			runGroup		
			sequenceStore		
			workflow		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソース AWS タグを削除するアクセス許可を付与します	Tagging	AnnotationStore		
			AnnotationStoreVersion		
			VariantStore		
			WorkflowVersion		
			readSet		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			reference		
			referenceStore		
			run		
			runCache		
			runGroup		
			sequenceStore		
			workflow		
				aws:TagKeys	
UpdateAnnotationStore	Annotation Store に関する情報を更新する許可を付与	書き込み	AnnotationStore*		
UpdateAnnotationStoreVersion	Annotation Store のバージョンに関する情報を更新する許可を付与	書き込み	AnnotationStoreVersion*		
UpdateRunCache	ワークフロー実行キャッシュを更新する許可を付与	書き込み	runCache*		
UpdateRunGroup	ワークフロー実行グループを更新する許可を付与	書き込み	runGroup*		
UpdateSequenceStore	Sequence Store の詳細を更新するアクセス許可を付与します	書き込み	sequenceStore*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateVariantStore	Variant Store に関するメタデータを更新する許可を付与	書き込み	VariantStore*		
UpdateWorkflow	ワークフロー詳細を更新する許可を付与	書き込み	workflow*		
UpdateWorkflowVersion	ワークフローバージョンの詳細を更新する許可を付与	書き込み	WorkflowVersion*		
			workflow*		
UploadReadSetPart	リードセットパーツをアップロードする許可を付与	書き込み	sequenceStore*		

AWS HealthOmics によって定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
AnnotationStore	`arn:${Partition}:omics:${Region}:${Account}:annotationStore/${AnnotationStoreName}`	aws:ResourceTag/${TagKey}
AnnotationStoreVersion	`arn:${Partition}:omics:${Region}:${Account}:annotationStore/${AnnotationStoreName}/version/${AnnotationStoreVersionName}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
readSet	arn:${Partition}:omics:${Region}:${Account}:sequenceStore/${SequenceStoreId}/readSet/${ReadSetId}	aws:ResourceTag/${TagKey}
reference	arn:${Partition}:omics:${Region}:${Account}:referenceStore/${ReferenceStoreId}/reference/${ReferenceId}	aws:ResourceTag/${TagKey}
referenceStore	arn:${Partition}:omics:${Region}:${Account}:referenceStore/${ReferenceStoreId}	aws:ResourceTag/${TagKey}
run	arn:${Partition}:omics:${Region}:${Account}:run/${Id}	aws:ResourceTag/${TagKey}
runCache	arn:${Partition}:omics:${Region}:${Account}:runCache/${Id}	aws:ResourceTag/${TagKey}
runGroup	arn:${Partition}:omics:${Region}:${Account}:runGroup/${Id}	aws:ResourceTag/${TagKey}
sequenceStore	arn:${Partition}:omics:${Region}:${Account}:sequenceStore/${SequenceStoreId}	aws:ResourceTag/${TagKey}
TaggingResource	arn:${Partition}:omics:${Region}:${Account}:tag/${TagKey}	
TaskResource	arn:${Partition}:omics:${Region}:${Account}:task/${Id}	
VariantStore	arn:${Partition}:omics:${Region}:${Account}:variantStore/${VariantStoreName}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
workflow	arn:${Partition}:omics:${Region}:${Account}:workflow/${Id}	aws:ResourceTag/${TagKey}
WorkflowVersion	arn:${Partition}:omics:${Region}:${Account}:workflow/${Id}/version/${VersionName}	aws:ResourceTag/${TagKey}

AWS HealthOmics の条件キー

AWS HealthOmics では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアによってアクセスをフィルタリングする	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

Amazon Honeycode のアクション、リソース、および条件キー

Amazon Honeycode (サービスプレフィックス: honeycode) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Honeycode で定義されるアクション
- Amazon Honeycode で定義されるリソースタイプ
- Amazon Honeycode の条件キー

Amazon Honeycode で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ApproveTeamAssociation [アクセス許可のみ]	AWS アカウントのチーム関連付けリクエストを承認するアクセス許可を付与します	書き込み			
BatchCreateTableRows	テーブルに新しい行を作成するアクセス許可を付与	Write	table*		
BatchDeleteTableRows	テーブルから行を削除するアクセス許可を付与	Write	table*		
BatchUpdateTableRows	テーブル内の行を更新するアクセス許可を付与	Write	table*		
BatchUpsertTableRows	テーブル内の行をマージ (アップサート) するアクセス許可を付与	Write	table*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateTeam [アクセス許可のみ]	AWS アカウントの新しい Amazon Honeycode チームを作成するアクセス許可を付与します	書き込み			
CreateTenant [アクセス許可のみ]	AWS アカウントの Amazon Honeycode 内に新しいテナントを作成するアクセス許可を付与します	書き込み			
DeleteDomains [アクセス許可のみ]	AWS アカウントの Amazon Honeycode ドメインを削除するアクセス許可を付与します	書き込み			
DeregisterGroups [アクセス許可のみ]	AWS アカウントの Amazon Honeycode チームからグループを削除するアクセス許可を付与します	書き込み			
DescribeTableDataImportJob	テーブルデータインポートジョブの詳細を取得するアクセス許可を付与	Read	table*		
DescribeTeam [許可のみ]	AWS アカウントの Amazon Honeycode チームの詳細を取得するアクセス許可を付与します	読み取り			
GetScreenData	画面からデータをロードする許可を付与	Read	screen*		
InvokeScreenAutomation	画面のオートメーションを呼び出すアクセス許可を付与	Write	screen-automation*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListDomains [アクセス許可のみ]	AWS アカウントのすべての Amazon Honeycode ドメインとその検証ステータスを一覧表示するアクセス許可を付与します	リスト			
ListGroups [許可のみ]	AWS アカウントの Amazon Honeycode チーム内のすべてのグループを一覧表示するアクセス許可を付与します	リスト			
ListTableColumns	テーブル内の列を一覧表示するアクセス許可を付与	リスト	table*		
ListTableRows	テーブル内の行を一覧表示するアクセス許可を付与	リスト	table*		
ListTables	ワークブック内のテーブルを一覧表示するアクセス許可を付与	リスト	workbook*		
ListTagsForResource	リソースのすべてのタグを一覧表示する許可を付与	Tagging			
ListTeamAssociations [アクセス許可のみ]	AWS アカウントとの保留中および承認済みのチームの関連付けをすべて一覧表示するアクセス許可を付与します	リスト			
ListTenants [許可のみ]	AWS アカウントの Amazon Honeycode のすべてのテナントを一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
QueryTableRows	フィルタを使用してテーブル行を照会するアクセス許可を付与	Read	table*		
RegisterDomainForVerification [許可のみ]	AWS アカウントの Amazon Honeycode ドメインの検証をリクエストするアクセス許可を付与します	書き込み			
RegisterGroups [アクセス許可のみ]	AWS アカウントの Amazon Honeycode チームにグループを追加するアクセス許可を付与します	書き込み			
RejectTeamAssociation [アクセス許可のみ]	AWS アカウントのチーム関連付けリクエストを拒否するアクセス許可を付与します	書き込み			
RestartDomainVerification [アクセス許可のみ]	AWS アカウントの Amazon Honeycode ドメインの検証を再開するアクセス許可を付与します	書き込み			
StartTableDataImportJob	テーブルデータインポートジョブを開始するアクセス許可を付与	書き込み	table*		
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け			
UntagResource	リソースのタグを解除する許可を付与	タグ付け			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateTeam [アクセス許可のみ]	AWS アカウントの Amazon Honeycode チームを更新する許可を付与	書き込み			

Amazon Honeycode で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
workbook	arn:${Partition}:honeycode:${Region}:${Account}:workbook:workbook/${WorkbookId}	
table	arn:${Partition}:honeycode:${Region}:${Account}:table:workbook/${WorkbookId}/table/${TableId}	
screen	arn:${Partition}:honeycode:${Region}:${Account}:screen:workbook/${WorkbookId}/app/${AppId}/screen/${ScreenId}	
screen-automation	arn:${Partition}:honeycode:${Region}:${Account}:screen-automation:workbook/${WorkbookId}/app/${AppId}/screen/${ScreenId}/automation/${AutomationId}	

Amazon Honeycode の条件キー

Honeycode には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS IAM Access Analyzer のアクション、リソース、および条件キー

AWS IAM Access Analyzer (サービスプレフィックス: access-analyzer) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IAM Access Analyzer で定義されるアクション
- AWS IAM Access Analyzer で定義されるリソースタイプ
- AWS IAM Access Analyzer の条件キー

AWS IAM Access Analyzer で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ApplyArchiveRule	アーカイブルールを適用する許可を付与	書き込み	Analyzer*		
CancelPolicyGeneration	ポリシーの生成をキャンセルする許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CheckAccessNotGranted	指定されたアクセスがポリシーによって許可されていないことを確認する許可を付与	読み取り			
CheckNoNewAccess	既存のポリシーと比較して、新しいアクセスが許可されていないことを確認する許可を付与	読み取り			
CheckNoPublicAccess	リソースポリシーによってパブリックアクセスが許可されていないことを確認する許可を付与する	読み取り			
CreateAccessPreview	指定したアナライザーのアクセスプレビューを作成する許可を付与	書き込み	Analyzer*		
CreateAnalyzer	アナライザーを作成する許可を付与	書き込み	Analyzer*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateArchiveRule	指定したアナライザーのアーカイブルールを作成する許可を付与	書き込み	ArchiveRule*		
DeleteAnalyzer	指定したアナライザーを削除する許可を付与	書き込み	Analyzer*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteArchiveRule	指定したアナライザーのアーカイブルールを削除する許可を付与	書き込み	ArchiveRule*		
GenerateFindingRecommendation	検出結果を解決するための推奨手順を生成する許可を付与する	書き込み	Analyzer*		
GetAccessPreview	アクセスプレビューについての情報を取得する許可を付与	読み込み	Analyzer*		
GetAnalyzedResource	分析されたリソースに関する情報を取得する許可を付与	読み込み	Analyzer*		
GetAnalyzer	アナライザーに関する情報を取得する許可を付与	読み込み	Analyzer*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetArchiveRule	指定したアナライザーのアーカイブルールに関する情報を取得する許可を付与	読み込み	ArchiveRule*		
GetFinding	検出結果を取得する許可を付与	読み取り	Analyzer*		
GetFindingRecommendation	検出結果を解決するためのレコメンデーションステップを取得する許可を付与する	読み取り	Analyzer*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetFindingsStatistics	検出結果の統計を取得する許可を付与	読み取り	Analyzer*		
GetGeneratedPolicy	StartPolicyGeneration を使用して生成されたポリシーを取得する許可を付与	読み込み			
ListAccessPreviewFindings	アクセスプレビューから検出結果のリストを取得する許可を付与	読み込み	Analyzer*		
ListAccessPreviews	アクセスプレビューのリストを取得する許可を付与	リスト	Analyzer*		
ListAnalyzedResources	分析されたリソースのリストを取得する許可を付与	読み込み	Analyzer*		
ListAnalyzers	アナライザーのリストを取得する許可を付与	リスト			
ListArchiveRules	アナライザーからアーカイブルールのリストを取得する許可を付与	リスト	Analyzer*		
ListFindings	アナライザーから検出結果のリストを取得する許可を付与	読み込み	Analyzer*		
ListPolicyGenerations	最近開始されたすべてのポリシー世代を一覧表示する許可を付与	読み込み			
ListTagsForResource	リソースに適用されたタグのリストを取得する許可を付与	読み込み	Analyzer		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartPolicyGeneration	ポリシー生成を開始する許可を付与	書き込み			iam:PassRole
StartResourceScan	リソースに適用されたポリシーのスキャンを開始する許可を付与	書き込み	Analyzer*		
TagResource	リソースにタグを追加する許可を付与	タグ付け	Analyzer		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	Tagging	Analyzer		
				aws:TagKeys	
UpdateAnalyzer	アナライザーの設定を変更するアクセス許可を付与します	書き込み	Analyzer*		
UpdateArchiveRule	アーカイブルールを変更する許可を付与	書き込み	ArchiveRule*		
UpdateFindings	検出結果を変更する許可を付与	書き込み	Analyzer*		
ValidatePolicy	ポリシーを検証する許可を付与	読み込み			

AWS IAM Access Analyzer で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Analyzer	`arn:${Partition}:access-analyzer:${Region}:${Account}:analyzer/${AnalyzerName}`	aws:ResourceTag/${TagKey}
ArchiveRule	`arn:${Partition}:access-analyzer:${Region}:${Account}:analyzer/${AnalyzerName}/archive-rule/${RuleName}`	

AWS IAM Access Analyzer の条件キー

AWS IAM Access Analyzer では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアのプレゼンスに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアに基づいてアクションをフィルタリングします	文字列

条件キー	説明	タイプ
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいてアクションをフィルタリングします	ArrayOfString

AWS IAM Identity Center のアクション、リソース、および条件キー

AWS IAM Identity Center (サービスプレフィックス: sso) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IAM Identity Center で定義されるアクション
- AWS IAM Identity Center で定義されるリソースタイプ
- AWS IAM Identity Center の条件キー

AWS IAM Identity Center で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
Associate Directory	IAM Identity Center AWS が使用するディレクトリを接続するアクセス許可を付与します	書き込み			ds:AuthorizeApplication
Associate Profile	ディレクトリユーザーまたはグループとプロファイルとの間に関連付けを作成する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AttachCustomerManagedPolicyReferenceToPermissionSet	カスタマー管理ポリシーリファレンスを許可セットにアタッチする許可を付与	権限の管理	Instance*		
			PermissionSet*		
AttachManagedPolicyToPermissionSet	AWS 管理ポリシーをアクセス許可セットにアタッチするアクセス許可を付与します	権限の管理	Instance*		
			PermissionSet*		
CreateAccountAssignment	指定されたアクセス許可セット AWS アカウント を使用して、指定された のプリンシパルにアクセスを割り当てるアクセス許可を付与します	書き込み	Account*		
			Instance*		
			PermissionSet*		
CreateApplication	アプリケーションを作成する許可を付与	書き込み	ApplicationProvider*		
			Instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApplicationAssignment	アプリケーション割り当てを作成する許可を付与	書き込み	Application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				sso:ApplicationAccount	
CreateApplicationInstance	IAM Identity Center AWS にアプリケーションインスタンスを追加するアクセス許可を付与します	書き込み			
CreateApplicationInstanceCertificate	アプリケーションインスタンスに新しい証明書を追加する許可を付与	書き込み			
CreateInstance	アイデンティティセンターインスタンスを作成する許可を付与	書き込み	Instance*		iam:CreateServiceLinkedRole organizations:DescribeOrganization
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateInstanceAccessControlAttributeConfiguration	ABAC のインスタンスを有効にし、属性を指定する許可を付与	書き込み	Instance*		iam:AttachRolePolicy iam:CreateRole iam:DeleteRole iam:DeleteRolePolicy iam:DetachRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:ListRolePolicies iam:PutRolePolicy iam:UpdateAssumeRolePolicy

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateManagedApplicationInstance	マネージドアプリケーションインスタンスを IAM Identity Center AWS に追加する許可を付与	書き込み			
CreatePermissionSet	アクセス許可セットを作成する許可を付与	書き込み	Instance*		
			PermissionSet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfile	アプリケーションインスタンスのプロファイルを作成する許可を付与	書き込み			
CreateTrust	ターゲットアカウントにフェデレーションの信頼を作成する許可を付与	書き込み			
CreateTrustedTokenIssuer	インスタンスの信頼できるトークン発行元を作成する許可を付与	書き込み	Instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteAccountAssignment	指定されたアクセス許可セット AWS アカウント を使用して、指定された からプリンシパルのアクセスを削除するアクセス許可を付与します	書き込み	Account*		
			Instance*		
			PermissionSet*		
DeleteApplication	アプリケーションを削除する許可を付与	書き込み	Application*		
				sso:ApplicationAccount	
DeleteApplicationAccessScope	アプリケーションへのアクセス範囲を削除する許可を付与	書き込み	Application*		
				sso:ApplicationAccount	
DeleteApplicationAssignment	アプリケーションの割り当てを削除する許可を付与	書き込み	Application*		
				sso:ApplicationAccount	
DeleteApplicationAuthenticationMethod	認証方法を削除する許可をアプリケーションに付与	書き込み	Application*		
				sso:ApplicationAccount	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteApplicationGrant	アプリケーションから付与を削除する許可を付与	書き込み	Application*		
				sso:ApplicationAccount	
DeleteApplicationInstance	アプリケーションインスタンスを削除する許可を付与	書き込み			
DeleteApplicationInstanceCertificate	非アクティブまたは期限切れの証明書をアプリケーションインスタンスから削除する許可を付与	書き込み			
DeleteInlinePolicyFromPermissionSet	指定されたアクセス許可セットからインラインポリシーを削除するアクセス許可を付与します	書き込み	Instance*		
			PermissionSet*		
DeleteInstance	アイデンティティセンターインスタンスを削除する許可を付与	書き込み	Instance*		
DeleteInstanceAccessControlAttributeConfiguration	ABAC を無効にし、インスタンスの属性リストを削除する許可を付与	書き込み	Instance*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteManagedApplicationInstance	管理対象アプリケーションインスタンスを削除する許可を付与	書き込み			
DeletePermissionSet	アクセス許可セットを削除する許可を付与	書き込み	Instance* PermissionSet*		
DeletePermissionsBoundaryFromPermissionSet	許可セットから許可境界を削除する許可を付与	権限の管理	Instance* PermissionSet*		
DeleteProfile	アプリケーションインスタンスのプロファイルを削除する許可を付与	書き込み			
DeleteTrustedTokenIssuer	インスタンスの信頼されたトークン発行元を削除する許可を付与	書き込み	TrustedTokenIssuer*		
DescribeAccountAssignmentCreationStatus	割り当て作成リクエストのステータスを記述するアクセス許可を付与します	読み込み	Instance*		
DescribeAccountAssignmentDeletionStatus	割り当て削除リクエストのステータスを記述するアクセス許可を付与します	読み取り	Instance*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeApplication	アプリケーションに関する情報を取得する許可を付与	読み取り	Application*		
				sso:ApplicationAccount	
DescribeApplicationAssignment	アプリケーションの割り当てを取得する許可を付与	読み取り	Application*		
				sso:ApplicationAccount	
DescribeApplicationProvider	アプリケーションプロバイダーを記述する許可を付与	読み取り	ApplicationProvider*		
DescribeInstance	アイデンティティセンターインスタンスに関する情報を取得する許可を付与	読み取り	Instance*		
DescribeInstanceAccessControlAttributeConfiguration	ABAC のインスタンスによって使用される属性のリストを取得する許可を付与	読み込み	Instance*		
DescribePermissionSet	アクセス許可セットを説明する許可を付与	読み込み	Instance*		
			PermissionSet*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribePermissionSetProvisioningStatus	指定されたアクセス許可セットのプロビジョニングリクエストのステータスを記述するアクセス許可を付与します	読み取り	Instance*		
DescribeRegisteredRegions	組織が IAM Identity Center AWS を有効にしているリージョンを取得する許可を付与	読み取り			
DescribeTrustedTokenIssuer	インスタンスの信頼されたトークン発行元を説明する許可を付与	読み取り	TrustedTokenIssuer*		
DetachCustomerManagedPolicyReferenceFromPermissionSet	カスタマー管理ポリシーリファレンスを許可セットからデタッチする許可を付与	権限の管理	Instance* PermissionSet*		
DetachManagedPolicyFromPermissionSet	指定されたアクセス許可セットからアタッチされた AWS 管理ポリシーをデタッチするアクセス許可を付与します	権限の管理	Instance* PermissionSet*		
DisassociateDirectory	IAM Identity Center AWS が使用するディレクトリの関連付けを解除するアクセス許可を付与します	書き込み			ds:UnauthorizeApplication
DisassociateProfile	プロファイルからディレクトリユーザーまたはグループの関連付けを解除する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetApplicationAccessScope	アプリケーションへのアクセス範囲を取得する許可を付与	読み取り	Application*		
				sso:ApplicationAccount	
GetApplicationAssignmentConfiguration	アプリケーションの割り当て設定を読み取る許可を付与	読み取り	Application*		
				sso:ApplicationAccount	
GetApplicationAuthenticationMethod	アプリケーションに認証方法を取得する許可を付与	読み取り	Application*		
				sso:ApplicationAccount	
GetApplicationGrant	アプリケーションに属する付与に関する詳細を取得する許可を付与	読み取り	Application*		
				sso:ApplicationAccount	
GetApplicationInstance	アプリケーションインスタンスの詳細を取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetApplicationSessionConfiguration	アプリケーションのセッション設定を取得するアクセス許可を付与します	読み取り	Application*		
				sso:ApplicationAccount	
GetApplicationTemplate	アプリケーションテンプレートの詳細を取得する許可を付与	読み込み			
GetInlinePolicyForPermissionSet	アクセス許可セットに割り当てられたインラインポリシーを取得するアクセス許可を付与します	読み込み	Instance*		
			PermissionSet*		
GetManagedApplicationInstance	アプリケーションインスタンスの詳細を取得する許可を付与	読み込み			
GetMfaDeviceManagementForDirectory	ディレクトリの MFA デバイス管理設定を取得する許可を付与	読み込み			
GetPermissionSet	アクセス許可セットの詳細を取得する許可を付与	読み取り			
GetPermissionsBoundaryForPermissionSet	許可セットの許可境界を取得する許可を付与	読み取り	Instance*		
			PermissionSet*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetProfile	アプリケーションインスタンスのプロファイルを取得する許可を付与	読み取り			
GetSSOStatus	IAM Identity Center AWS が有効になっているかどうかを確認するアクセス許可を付与します	読み取り			
GetSharedSsoConfiguration	現在の SSO インスタンスの共有設定を取得する許可を付与	読み込み			
GetSsoConfiguration	現在の SSO インスタンスの設定を取得する許可を付与	読み込み			
GetTrust	ターゲットアカウントでフェデレーションの信頼を取得する許可を付与	読み込み			
ImportApplicationInstanceServiceProviderMetadata	サービスプロバイダーが提供するアプリケーション SAML メタデータファイルをアップロードして、アプリケーションインスタンスを更新する許可を付与	書き込み			
ListAccountAssignmentCreationStatus	指定された SSO インスタンス AWS アカウント の割り当て作成リクエストのステータスを一覧表示するアクセス許可を付与します	リスト	Instance*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListAccountAssignmentDeletionStatus	指定された SSO インスタンス AWS アカウント の割り当て削除リクエストのステータスを一覧表示するアクセス許可を付与します	リスト	Instance*		
ListAccountAssignments	指定されたアクセス許可セット AWS アカウント を使用して、指定された の担当者を一覧表示するアクセス許可を付与します	リスト	Account*		
			Instance*		
			PermissionSet*		
ListAccountAssignmentsForPrincipal	ユーザーまたはグループに割り当てられたアカウントを一覧表示する許可を付与	リスト	Instance*		
ListAccountsForProvisionedPermissionSet	指定されたアクセス許可セットがプロビジョニングされているすべての AWS アカウントを一覧表示するアクセス許可を付与します	リスト	Instance*		
			PermissionSet*		
ListApplicationAccessScopes	アプリケーションにアクセス範囲を一覧表示する許可を付与	リスト	Application*		
				sso:ApplicationAccount	
ListApplicationAssignments	アプリケーションの割り当てを一覧表示する許可を付与	リスト	Application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				sso:ApplicationAccount	
ListApplicationAssignmentsForPrincipal	ユーザーまたはグループに割り当てられたアプリケーションを一覧表示する許可を付与	リスト	Instance*		
				sso:ApplicationAccount	
ListApplicationAuthenticationMethods	アプリケーションに認証方法を一覧表示する許可を付与	リスト	Application*		
				sso:ApplicationAccount	
ListApplicationGrants	アプリケーションから付与を一覧表示する許可を付与	リスト	Application*		
				sso:ApplicationAccount	
ListApplicationInstanceCertificates	指定されたアプリケーションインスタンスのすべての証明書を取得する許可を付与	読み込み			
ListApplicationInstances	すべてのアプリケーションインスタンスを取得する許可を付与	リスト			sso:GetApplicationInstance

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListApplicationProviders	アプリケーションプロバイダーを一覧表示する許可を付与	リスト	ApplicationProvider*		
ListApplicationTemplates	サポートされているすべてのアプリケーションテンプレートを取得する許可を付与	リスト			sso:GetApplicationTemplate
ListApplications	IAM Identity Center のインスタンスに関連付けられているすべてのアプリケーションを取得する許可を付与	リスト			
ListCustomerManagedPolicyReferencesInPermissionSet	許可セットにアタッチされているカスタマー管理ポリシーリファレンスを一覧表示する許可を付与します	リスト	Instance* PermissionSet*		
ListDirectoryAssociations	IAM Identity Center AWS に接続されたディレクトリに関する詳細を取得するアクセス許可を付与します	読み取り			
ListInstances	呼び出し元がアクセスできる SSO インスタンスを一覧表示するアクセス許可を付与します	リスト			
ListManagedPoliciesInPermissionSet	指定されたアクセス許可セットにアタッチされている AWS 管理ポリシーを一覧表示するアクセス許可を付与します	リスト	Instance* PermissionSet*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListPermissionSetProvisioningStatus	指定した SSO インスタンスに対するアクセス許可セットのプロビジョニングリクエストのステータスを一覧表示するアクセス許可を付与します	リスト	Instance*		
ListPermissionSets	すべてのアクセス許可セットを取得する許可を付与	リスト	Instance*		
ListPermissionSetsProvisionedToAccount	指定された にプロビジョニングされているすべてのアクセス許可セットを一覧表示するアクセス許可を付与しますAWS アカウント	リスト	Account*		
			Instance*		
ListProfileAssociations	プロファイルに関連付けられたディレクトリユーザーまたはグループを取得する許可を付与	読み込み			
ListProfiles	アプリケーションインスタンスのすべてのプロファイルを取得する許可を付与	リスト			sso:GetProfile
ListTagsForResource	指定されたリソースにアタッチされているタグを一覧表示するアクセス許可を付与します	読み取り	Application		
			Instance		
			PermissionSet		
			TrustedTokenIssuer		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTrustedTokenIssuers	インスタンスの信頼されたトークン発行元を一覧表示する許可を付与	リスト	Instance*		
ProvisionPermissionSet	指定されたアクセス許可セットを指定されたターゲットにプロビジョニングするアクセス許可を付与します	書き込み	Account*		
			Instance*		
			PermissionSet*		
PutApplicationAccessScope	アプリケーションへのアクセス範囲を作成または更新する許可を付与	書き込み	Application*		
				sso:ApplicationAccount	
PutApplicationAssignmentConfiguration	アプリケーションに割り当て設定を追加するアクセス許可を付与	書き込み	Application*		
				sso:ApplicationAccount	
PutApplicationAuthenticationMethod	アプリケーションに認証方法を作成または更新する許可を付与	書き込み	Application*		
				sso:ApplicationAccount	
PutApplicationGrant	アプリケーションに付与を作成/更新する許可を付与	書き込み	Application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				sso:ApplicationAccount	
PutApplicationSessionConfiguration	アプリケーションのセッション設定を配置するアクセス許可を付与します	書き込み	Application*		
				sso:ApplicationAccount	
PutInlinePolicyToPermissionSet	IAM インラインポリシーをアクセス許可セットにアタッチするアクセス許可を付与します	書き込み	Instance*		
			PermissionSet*		
PutMfaDeviceManagementForDirectory	ディレクトリの MFA デバイス管理設定を配置する許可を付与	書き込み			
PutPermissionsBoundaryToPermissionSet	許可セットに許可境界を追加する許可を付与	権限の管理	Instance*		
			PermissionSet*		
PutPermissionsPolicy	アクセス許可セットにポリシーを追加する許可を付与	Permissions management			
SearchGroups	関連付けられたディレクトリ内のグループを検索する許可を付与。	読み込み			ds:DescribeDirectories

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SearchUsers	関連付けられたディレクトリ内のユーザーを検索する許可を付与。	読み取り			ds:DescribeDirectories
StartSSO	IAM Identity Center AWS を初期化するアクセス許可を付与します	書き込み			organizations:DescribeOrganization organizations:EnableAWSServiceAccess
TagResource	一連のタグを指定されたリソースに関連付けるアクセス許可を付与します	Tagging	Application		
			Instance		
			PermissionSet		
			TrustedTokenIssuer		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	指定したリソースから一連のタグの関連付けを解除するアクセス許可を付与します	Tagging	Application		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			Instance		
			PermissionSet		
			TrustedTokenIssuer		
				aws:TagKeys	
UpdateApplication	アプリケーションを更新する許可を付与	書き込み	Application*		
				sso:ApplicationAccount	
UpdateApplicationInstanceActiveCertificate	このアプリケーションインスタンスのアクティブな証明書として証明書を設定する許可を付与	書き込み			
UpdateApplicationInstanceDisplayData	アプリケーションインスタンスの表示データを更新する許可を付与	書き込み			
UpdateApplicationInstanceResponseConfiguration	アプリケーションインスタンスのフェデレーションレスポンス設定を更新する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateApplicationInstanceResponseSchemaConfiguration	アプリケーションインスタンスのフェデレーションレスポンススキーマ設定を更新する許可を付与	書き込み			
UpdateApplicationInstanceSecurityConfiguration	アプリケーションインスタンスのセキュリティ詳細を更新する許可を付与	書き込み			
UpdateApplicationInstanceServiceProviderConfiguration	アプリケーションインスタンスのサービスプロバイダーに関する設定を更新する許可を付与	書き込み			
UpdateApplicationInstanceStatus	アプリケーションインスタンスのステータスを更新する許可を付与	書き込み			
UpdateInstance	アイデンティティセンターインスタンスを更新する許可を付与	書き込み	Instance*		
UpdateInstanceAccessControlAttributeConfiguration	ABAC のインスタンスで使用する属性を更新する許可を付与	書き込み	Instance*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateManagedApplicationInstanceStatus	管理対象アプリケーションインスタンスのステータスを更新する許可を付与	書き込み			
UpdatePermissionSet	アクセス許可セットを更新するアクセス許可を付与します	権限の管理	Instance*		
			PermissionSet*		
UpdateProfile	アプリケーションインスタンスのプロファイルを更新する許可を付与	書き込み			
UpdateSSOConfiguration	現在の SSO インスタンスの設定を更新する許可を付与	書き込み			
UpdateTrust	ターゲットアカウントでフェデレーションの信頼を更新する許可を付与	書き込み			
UpdateTrustedTokenIssuer	インスタンスの信頼されたトークン発行元を更新する許可を付与	書き込み	TrustedTokenIssuer*		

AWS IAM Identity Center で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
PermissionSet	arn:${Partition}:sso:::permissionSet/${InstanceId}/${PermissionSetId}	aws:ResourceTag/${TagKey}
Account	arn:${Partition}:sso:::account/${AccountId}	
Instance	arn:${Partition}:sso:::instance/${InstanceId}	aws:ResourceTag/${TagKey}
Application	arn:${Partition}:sso::${AccountId}:application/${InstanceId}/${ApplicationId}	aws:ResourceTag/${TagKey} sso:ApplicationAccount
TrustedTokenIssuer	arn:${Partition}:sso::${AccountId}:trustedTokenIssuer/${InstanceId}/${TrustedTokenIssuerId}	aws:ResourceTag/${TagKey}
ApplicationProvider	arn:${Partition}:sso::aws:applicationProvider/${ApplicationProviderId}	

AWS IAM Identity Center の条件キー

AWS IAM Identity Center では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列

条件キー	説明	タイプ
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
sso:ApplicationAccount	アプリケーションを作成するアカウントでアクセスをフィルタリングします。この条件キーは、カスタマーマネージド SAML アプリケーションではサポートされていません	String

AWS IAM Identity Center ディレクトリのアクション、リソース、および条件キー

AWS IAM Identity Center ディレクトリ (サービスプレフィックス: `sso-directory`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IAM Identity Center ディレクトリで定義されるアクション
- AWS IAM Identity Center ディレクトリで定義されるリソースタイプ
- AWS IAM Identity Center ディレクトリの条件キー

AWS IAM Identity Center ディレクトリで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AddMemberToGroup	IAM Identity Center AWS がデフォルトで提供するディレクトリ内のグループにメンバーを追加するアクセス許可を付与します	書き込み			
CompleteVirtualMfaDeviceRegistration	仮想 MFA デバイスの作成プロセスを完了する許可を付与。	Write			
CompleteWebAuthnDeviceRegistration	WebAuthn デバイスの登録プロセスを完了する許可を付与	書き込み			
CreateAlias	AWS IAM Identity Center がデフォルトで提供するディレクトリのエイリアスを作成するアクセス許可を付与します	書き込み			
CreateBearerToken	特定のプロビジョニングテナントのベアラートークンを作成する許可を付与。	Write			
CreateExternalIdPConfigurationForDirectory	ディレクトリ用の外部 ID プロバイダ設定を作成する許可を付与。	書き込み			
CreateGroup	IAM Identity Center AWS がデフォルトで提供するディレク	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	トリにグループを作成するアクセス許可を付与します				
CreateProvisioningTenant	指定したディレクトリのプロビジョニングテナントを作成する許可を付与。	書き込み			
CreateUser	IAM Identity Center AWS がデフォルトで提供するディレクトリにユーザーを作成するアクセス許可を付与します	書き込み			
DeleteBearerToken	ベアラートークンを削除する許可を付与。	Write			
DeleteExternalIdPCertificate	指定された外部 IdP 証明書を削除する許可を付与。	Write			
DeleteExternalIdPConfigurationForDirectory	ディレクトリに関連付けられた外部 ID プロバイダ設定を削除する許可を付与。	書き込み			
DeleteGroup	IAM Identity Center AWS がデフォルトで提供するディレクトリからグループを削除するアクセス許可を付与します	書き込み			
DeleteMfaDeviceForUser	特定のユーザーのデバイス名によって MFA デバイスを削除する許可を付与。	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteProvisioningTenant	プロビジョニングテナントを削除する許可を付与。	書き込み			
DeleteUser	IAM Identity Center AWS がデフォルトで提供するディレクトリからユーザーを削除するアクセス許可を付与します	書き込み			
DescribeDirectory	IAM Identity Center AWS がデフォルトで提供するディレクトリに関する情報を取得するアクセス許可を付与します	読み取り			
DescribeGroup	ユーザーおよびグループメンバーを含まない、グループデータをクエリする許可を付与	読み取り			
DescribeGroups	IAM Identity Center AWS がデフォルトで提供するディレクトリからグループに関する情報を取得するアクセス許可を付与します	読み取り			
DescribeProvisioningTenant	プロビジョニングテナントを説明する許可を付与	読み取り			
DescribeUser	IAM Identity Center AWS がデフォルトで提供するディレクトリからユーザーに関する情報を取得するアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeUserByUniqueAttribute	ユーザーに対して表される有効な一意の属性を使用してユーザーを説明する許可を付与	読み取り			
DescribeUsers	IAM Identity Center AWS がデフォルトで提供するディレクトリからユーザーに関する情報を取得するアクセス許可を付与します	読み取り			
DisableExternalIdPConfigurationForDirectory	外部 ID プロバイダを使用したエンドユーザーの認証を無効にする許可を付与。	書き込み			
DisableUser	IAM Identity Center AWS がデフォルトで提供するディレクトリ内のユーザーを非アクティブ化するアクセス許可を付与します	書き込み			
EnableExternalIdPConfigurationForDirectory	外部 ID プロバイダを使用したエンドユーザーの認証を有効にする許可を付与。	書き込み			
EnableUser	IAM Identity Center AWS がデフォルトで提供するディレクトリでユーザーをアクティブ化するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetAWSSPConfigurationForDirectory	ディレクトリの AWS IAM Identity Center サービスプロバイダー設定を取得するアクセス許可を付与します	読み取り			
GetGroupId	IAM Identity Center がデフォルトで提供するディレクトリからグループに関する ID AWS 情報を取得するアクセス許可を付与します	読み取り			
GetUserId	IAM Identity Center がデフォルトで提供するディレクトリからユーザーに関する ID AWS 情報を取得するアクセス許可を付与します	読み取り			
GetUserPoolInfo	(非推奨) UserPool 情報を取得する許可を付与	読み取り			
ImportExternalIdPCertificate	外部 IdP レスポンスの検証に使用される IdP 証明書をインポートする許可を付与。	書き込み			
IsMemberInGroup	メンバーが IAM Identity Center AWS がデフォルトで提供するディレクトリ内のグループの一部であるかどうかをチェックするアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
IsMemberInGroups	メンバーが IAM Identity Center AWS がデフォルトで提供するディレクトリ内の複数のグループの一部であるかどうかをチェックするアクセス許可を付与します	読み取り			
ListBearerTokens	特定のプロビジョニングテナントのベアラートークンを一覧表示する許可を付与。	Read			
ListExternalIdPCertificates	指定されたディレクトリと IdP の外部 IdP 証明書を一覧表示する許可を付与。	Read			
ListExternalIdPConfigurationsForDirectory	ディレクトリ用に作成されたすべての外部 ID プロバイダ設定を一覧表示する許可を付与。	読み取り			
ListGroups	IAM Identity Center AWS がデフォルトで提供するディレクトリからグループを一覧表示するアクセス許可を付与します	読み取り			
ListGroupsForMember	ターゲットメンバーのグループを一覧表示する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListGroupsForUser	IAM Identity Center AWS がデフォルトで提供するディレクトリからユーザーのグループを一覧表示するアクセス許可を付与します	読み取り			
ListMembersInGroup	IAM Identity Center AWS がデフォルトで提供するディレクトリ内のグループの一部であるすべてのメンバーを取得するアクセス許可を付与します	読み取り			
ListMfaDevicesForUser	すべてのアクティブな MFA デバイスとそのユーザーの MFA デバイスメタデータを一覧表示する許可を付与。	Read			
ListProvisioningTenants	指定したディレクトリのプロビジョニングテナントを一覧表示する許可を付与。	読み取り			
ListUsers	IAM Identity Center AWS がデフォルトで提供するディレクトリからユーザーを一覧表示するアクセス許可を付与します	読み取り			
RemoveMemberFromGroup	AWS IAM Identity Center がデフォルトで提供するディレクトリ内のグループの一部であるメンバーを削除するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SearchGroups	関連付けられたディレクトリ内のグループを検索する許可を付与。	読み込み			
SearchUsers	関連付けられたディレクトリ内のユーザーを検索する許可を付与。	Read			
StartVirtualMfaDeviceRegistration	仮想 MFA デバイスの作成プロセスを開始する許可を付与。	Write			
StartWebAuthnDeviceRegistration	WebAuthn デバイスの登録プロセスを開始する許可を付与します	Write			
UpdateExternalIdPConfigurationForDirectory	ディレクトリに関連付けられた外部 ID プロバイダ設定を更新する許可を付与。	書き込み			
UpdateGroup	IAM Identity Center AWS がデフォルトで提供するディレクトリ内のグループに関する情報を更新するアクセス許可を付与します	書き込み			
UpdateGroupDisplayName	グループ表示名を更新し、グループ表示名レスポンスを更新する許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateMfaDeviceForUser	MFA デバイス情報を更新する許可を付与	書き込み			
UpdatePassword	E メールでパスワードリセットリンクを送信するか、 AWS IAM Identity Center がデフォルトで提供するディレクトリでユーザーのワンタイムパスワードを生成してパスワードを更新するアクセス許可を付与します	書き込み			
UpdateUser	IAM Identity Center AWS がデフォルトで提供するディレクトリ内のユーザー情報を更新するアクセス許可を付与します	書き込み			
UpdateUserName	ユーザー名を更新し、ユーザー名のレスポンスを更新する許可を付与	Write			
VerifyEmail	ユーザーの E メールアドレスを検証する許可を付与。	書き込み			

AWS IAM Identity Center ディレクトリで定義されるリソースタイプ

AWS IAM Identity Center ディレクトリは、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS IAM Identity Center ディレクトリへのアクセスを許可するには、ポリシー`"Resource": "*"`で を指定します。

AWS IAM Identity Center ディレクトリの条件キー

IAM Identity Center ディレクトリには、ポリシーステートメントの Condition要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS IAM Identity Center OIDC サービスのアクション、リソース、および条件キー

AWS IAM Identity Center OIDC サービス (サービスプレフィックス: sso-oauth) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IAM Identity Center OIDC サービスによって定義されるアクション
- AWS IAM Identity Center OIDC サービスによって定義されるリソースタイプ
- AWS IAM Identity Center OIDC サービスの条件キー

AWS IAM Identity Center OIDC サービスによって定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にア

クションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateTokenWithIAM	IAM Identity Center 統合アプリケーションにアクセスするための OAuth/OIDC トークンを作成する許可を付与	書き込み	Application*		

AWS IAM Identity Center OIDC サービスによって定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource 要素で使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Application	`arn:${Partition}:sso::${AccountId}:application/${InstanceId}/${ApplicationId}`	

AWS IAM Identity Center OIDC サービスの条件キー

OIDC サービスには、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Identity and Access Management (IAM) のアクション、リソース、および条件キー

AWS Identity and Access Management (IAM) (サービスプレフィックス: iam) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Identity And Access Management (IAM) によって定義されるアクション
- AWS Identity And Access Management (IAM) で定義されるリソースタイプ
- AWS Identity And Access Management (IAM) の条件キー

AWS Identity And Access Management (IAM) によって定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AddClientIDToOpenIDConnectProvider	指定された IAM OpenID Connect(OIDC) プロバイダーリソースに登録された ID のリストに新しいクライアント ID (閲覧者) を追加する許可を付与	書き込み	oidc-provider*		
AddRoleToInstanceProfile	指定されたインスタンスプロファイルに IAM ロールを追加する許可を付与	書き込み	instance-profile*		iam:PassRole
AddUserToGroup	指定された IAM グループに IAM ユーザーを追加する許可を付与	書き込み	group*		
AttachGroupPolicy	指定された IAM グループに管理ポリシーをアタッチする許可を付与	Permissions management	group*		
				iam:PolicyARN	
AttachRolePolicy	指定された IAM ロールに管理ポリシーをアタッチする許可を付与	Permissions management	role*		
				iam:PolicyARN iam:PermissionsBoundary	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AttachUserPolicy	指定された IAM ユーザーに管理ポリシーをアタッチする許可を付与	権限の管理	user*		
				iam:PolicyARN iam:PermissionsBoundary	
ChangePassword	IAM ユーザーに自分のパスワードを変更するアクセス許可を付与します。	書き込み	user*		
CreateAccessKey	指定された IAM ユーザーのアクセスキーとシークレットアクセスキーを作成する許可を付与。	書き込み	user*		
CreateAccountAlias	のエイリアスを作成するアクセス許可を付与します AWS アカウント	書き込み			
CreateGroup	新しいグループを作成する許可を付与	書き込み	group*		
CreateInstanceProfile	新しいインスタンスプロファイルを作成する許可を付与	書き込み	instance-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateLoginProfile	指定された IAM ユーザーのパスワードを作成する許可を付与	書き込み	user*		
CreateOpenIDConnectProvider	OpenID Connect (OIDC) をサポートする ID プロバイダー (IdP) について説明する IAM リソースを作成する許可を付与	書き込み	oidc-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePolicy	新しい管理ポリシーを作成する許可を付与	Permissions management	policy*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePolicyVersion	指定された管理ポリシーの新しいバージョンを作成する許可を付与	Permissions management	policy*		
CreateRole	新しいロールを作成する許可を付与	書き込み	role*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				iam:PermissionsBoundary aws:TagKeys aws:RequestTag/${TagKey}	
CreateSAMLProvider	SAML 2.0 をサポートする ID プロバイダー (IdP) について説明する IAM リソースを作成する許可を付与	書き込み	saml-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceLinkedRole	AWS サービスがユーザーに代わってアクションを実行できるようにする IAM ロールを作成するアクセス許可を付与します	書き込み	role*		
				iam:AWSServiceName	
CreateServiceSpecificCredential	IAM ユーザーの新しいサービス固有の認証情報を作成する許可を付与	書き込み	user*		
CreateUser	新しい IAM ユーザーを作成する許可を付与	書き込み	user*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				iam:PermissionsBoundary aws:TagKeys aws:RequestTag/${TagKey}	
CreateVirtualMFADevice	新しい仮想 MFA デバイスを作成する許可を付与	書き込み	mfa*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeactivateMFADevice	指定された MFA デバイスを非アクティブ化し、最初に有効にされた IAM ユーザーとの関連付けを削除する許可を付与	書き込み	user*		
DeleteAccessKey	指定された IAM ユーザーに関連付けられたアクセスキーペアを削除する許可を付与	書き込み	user*		
DeleteAccountAlias	指定された AWS アカウントエイリアスを削除するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteAccountPasswordPolicy	のパスワードポリシーを削除するアクセス許可を付与します AWS アカウント	権限の管理			
DeleteCloudFrontPublicKey	既存の CloudFront 公開鍵を削除するアクセス許可を付与	書き込み			
DeleteGroup	指定した IAM グループを削除するアクセス許可を付与	書き込み	group*		
DeleteGroupPolicy	グループから指定されたインラインポリシーを削除する許可を付与	Permissions management	group*		
DeleteInstanceProfile	指定されたインスタンスプロファイルを削除する許可を付与	書き込み	instance-profile*		
DeleteLoginProfile	指定された IAM ユーザーのパスワードを削除する許可を付与	書き込み	user*		
DeleteOpenIDConnectProvider	IAM で OpenID Connect ID プロバイダー (IdP) リソースオブジェクトを削除する許可を付与	書き込み	oidc-provider*		
DeletePolicy	指定した管理ポリシーを削除し、それがアタッチされている IAM エンティティ (ユーザー、グループ、またはロール) から削除する許可を付与	Permissions management	policy*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeletePolicyVersion	指定された管理ポリシーからバージョンを削除する許可を付与	Permissions management	policy*		
DeleteRole	指定したロールを削除するアクセス許可を付与	書き込み	role*		
DeleteRolePermissionsBoundary	ロールからアクセス許可境界を削除する許可を付与	Permissions management	role*		
				iam:PermissionsBoundary	
DeleteRolePolicy	指定されたロールから指定されたインラインポリシーを削除する許可を付与	Permissions management	role*		
				iam:PermissionsBoundary	
DeleteSAMLProvider	IAM で SAML プロバイダーリソースを削除する許可を付与	書き込み	saml-provider*		
DeleteSSHPublicKey	指定された SSH パブリックキーを削除する許可を付与	書き込み	user*		
DeleteServerCertificate	指定されたサーバー証明書を削除する許可を付与	書き込み	server-certificate*		
DeleteServiceLinkedRole	AWS サービスで使用されなくなった場合に、特定のサービスにリンクされた IAM ロールを削除するアクセス許可を付与します	書き込み	role*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteServiceSpecificCredential	IAM ユーザーの指定されたサービス固有の認証情報を削除する許可を付与	書き込み	user*		
DeleteSigningCertificate	指定された IAM ユーザーに関連付けられている署名証明書を削除する許可を付与	書き込み	user*		
DeleteUser	指定した IAM ユーザーを削除するアクセス許可を付与	書き込み	user*		
DeleteUserPermissionsBoundary	指定された IAM ユーザーからアクセス許可境界を削除する許可を付与	Permissions management	user*		
				iam:PermissionsBoundary	
DeleteUserPolicy	IAM ユーザーから指定されたインラインポリシーを削除する許可を付与	Permissions management	user*		
				iam:PermissionsBoundary	
DeleteVirtualMFADevice	仮想 MFA デバイスを削除する許可を付与	書き込み	mfa		
			sms-mfa		
DetachGroupPolicy	指定された IAM グループから管理ポリシーをデタッチする許可を付与	Permissions management	group*		
				iam:PolicyARN	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DetachRolePolicy	指定されたロールから管理ポリシーをデタッチする許可を付与	Permissions management	role*		
				iam:PolicyARN iam:PermissionsBoundary	
DetachUserPolicy	指定された IAM ユーザーから管理ポリシーをデタッチする許可を付与	権限の管理	user*		
				iam:PolicyARN iam:PermissionsBoundary	
DisableOrganizationsRootCredentialsManagement	現在のアカウントで管理されている組織のメンバーアカウントのルートユーザー認証情報の管理を無効にするアクセス許可を付与します	書き込み			
DisableOrganizationsRootSessions	現在のアカウントで管理されている組織のメンバーアカウントで特権ルートアクションを無効にするアクセス許可を付与します	書き込み			
EnableMFADevice	MFA デバイスを有効にして、指定された IAM ユーザーに関連付けるアクセス許可を付与	書き込み	user*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				iam:RegisterSecurityKey iam:FIDO-FIPS-140-2-certification iam:FIDO-FIPS-140-3-certification iam:FIDO-certification	
EnableOrganizationsRootCredentialsManagement	現在のアカウントで管理されている組織のメンバーアカウントのルートユーザー認証情報の管理を有効にするアクセス許可を付与します	書き込み			
EnableOrganizationsRootSessions	現在のアカウントで管理されている組織のメンバーアカウントで特権ルートアクションを有効にするアクセス許可を付与します	書き込み			
GenerateCredentialReport	の認証情報レポートを生成するアクセス許可を付与しますAWS アカウント	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GenerateOrganizationsAccessReport	AWS Organizations エンティティのアクセスレポートを生成するアクセス許可を付与します	読み取り	access-report*		organizations:DescribePolicy organizations:ListChildren organizations:ListParents organizations:ListPoliciesForTarget organizations:ListRoots organizations:ListTargetsForPolicy
				iam:OrganizationsPolicyId	
GenerateServiceLastAccessedDetails	IAM リソースのサービスの最終アクセス時間データレポートを生成する許可を付与	読み込み	group*		
			policy*		
			role*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			user*		
GetAccessKeyLastUsed	指定されたアクセスキーの最後の使用時の情報を取得する許可を付与	読み取り	user*		
GetAccountAuthorizationDetails	相互の関係など、 内のすべての IAM ユーザー、グループ AWS アカウント、ロール、ポリシーに関する情報を取得するアクセス許可を付与します	読み取り			
GetAccountEmailAddress	アカウントに関連付けられている E メールアドレスを取得するアクセス許可を付与	読み取り			
GetAccountName	アカウントに関連付けられているアカウント名を取得するアクセス許可を付与	読み取り			
GetAccountPasswordPolicy	のパスワードポリシーを取得するアクセス許可を付与します AWS アカウント	読み取り			
GetAccountSummary	の IAM エンティティの使用状況と IAM クォータに関する情報を取得するアクセス許可を付与します AWS アカウント	リスト			
GetCloudFrontPublicKey	指定した CloudFront 公開ビューに関する情報を取得するアクセス許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetContextKeysForCustomPolicy	指定されたポリシーで参照されているコンテキストキーのすべてのリストを取得する許可を付与	読み込み			
GetContextKeysForPrincipalPolicy	指定された IAM アイデンティティ (ユーザー、グループ、ロール) にアタッチされているすべての IAM ポリシーで参照される、すべてのコンテキストキーのリストを取得する許可を付与	読み取り	group		
			role		
			user		
GetCredentialReport	の認証情報レポートを取得するアクセス許可を付与しますAWS アカウント	読み取り			
GetGroup	指定された IAM グループで IAM ユーザーのリストを取得する許可を付与	読み込み	group*		
GetGroupPolicy	指定の IAM グループに埋め込まれたインラインポリシードキュメントを取得する許可を付与	読み込み	group*		
GetInstanceProfile	指定されたインスタンスプロファイルについて、インスタンスプロファイルのパス、GUID、ARN、ロールといった情報を取得するアクセス許可を付与	読み込み	instance-profile*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetLoginProfile	指定された IAM ユーザーのユーザー名とパスワードの作成日を取得する許可を付与	リスト	user*		
GetMFADevice	指定されたユーザーの MFA デバイスに関する情報を取得するアクセス許可を付与します	読み取り	user*		
GetOpenIDConnectProvider	IAM の指定された OpenID Connect (OIDC) プロバイダーリソースに関する情報を取得する許可を付与	読み取り	oidc-provider*		
GetOrganizationsAccessReport	AWS Organizations アクセスレポートを取得する許可を付与	読み取り			
GetPolicy	指定された管理ポリシーについて、そのポリシーのデフォルトバージョン、そのポリシーがアタッチされているアイデンティティの総数といった情報を取得するアクセス許可を付与	読み込み	policy*		
GetPolicyVersion	指定の管理ポリシーのバージョンについて、ポリシードキュメントなどの情報を取得する許可を付与	読み込み	policy*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetRole	指定されたロールについて、そのロールのパス、GUID、ARN、そのロールの信頼ポリシーといった情報を取得するアクセス許可を付与	読み込み	role*		
GetRolePolicy	指定の IAM ロールに埋め込まれたインラインポリシードキュメントを取得する許可を付与	読み込み	role*		
GetSAMLProvider	IAM SAML プロバイダーリソースオブジェクトの作成時または更新時にアップロードされた SAML プロバイダーメタデータドキュメントを取得するアクセス許可を付与	読み込み	saml-provider*		
GetSSHPublicKey	指定された SSH パブリックキーを、そのキーに関するメタデータを含めて取得する許可を付与	読み込み	user*		
GetServerCertificate	IAM に保存されている指定のサーバー証明書に関する情報を取得する許可を付与	読み込み	server-certificate*		
GetServiceLastAccessedDetails	サービスの最終アクセス時間データレポートに関する情報を取得する許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetServiceLastAccessedDetailsWithEntities	サービスの最終アクセス時間データレポートからのエンティティに関する情報を取得する許可を付与	読み込み			
GetServiceLinkedRoleDeletionStatus	IAM サービスにリンクされたロールの削除ステータスを取得する許可を付与	読み込み	role*		
GetUser	この例では、ユーザーの作成日、パス、一意の ID、ARN を含む、指定された IAM ユーザーに関する情報を取得するアクセス許可を付与	読み込み	user*		
GetUserPolicy	指定の IAM ユーザーに埋め込まれたインラインポリシードキュメントを取得する許可を付与	読み込み	user*		
ListAccessKeys	指定の IAM ユーザーに関連付けられたアクセスキー ID に関する情報を一覧表示する許可を付与	リスト	user*		
ListAccountAliases	に関連付けられているアカウントエイリアスを一覧表示するアクセス許可を付与しますAWS アカウント	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListAttachedGroupPolicies	指定された IAM グループにアタッチされている管理ポリシーを一覧表示する許可を付与	リスト	group*		
ListAttachedRolePolicies	指定された IAM ロールにアタッチされている管理ポリシーを一覧表示する許可を付与	リスト	role*		
ListAttachedUserPolicies	指定された IAM ユーザーにアタッチされている管理ポリシーを一覧表示する許可を付与	リスト	user*		
ListCloudFrontPublicKeys	アカウント内にあるすべての最新の CloudFront 公開鍵を一覧表示するアクセス許可を付与	リスト			
ListEntitiesForPolicy	指定した管理ポリシーがアタッチされているすべての IAM アイデンティティをリストする許可を付与	リスト	policy*		
ListGroupPolicies	指定された IAM グループに埋め込まれているインラインポリシーの名前を一覧表示するアクセス許可を付与	リスト	group*		
ListGroups	指定されたパスのプレフィックスを持つ IAM グループを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListGroupsForUser	指定された IAM ユーザーが属する IAM グループを一覧表示する許可を付与	リスト	user*		
ListInstanceProfileTags	指定されたインスタンスプロファイルにアタッチされているタグを一覧表示する許可を付与	リスト	instance-profile*		
ListInstanceProfiles	指定されたパスのプレフィックスを持つインスタンスプロファイルを一覧表示する許可を付与	リスト			
ListInstanceProfilesForRole	指定された IAM ロールが関連付けられているインスタンスプロファイルを一覧表示する許可を付与	リスト	role*		
ListMFADeviceTags	指定された仮想 MFA デバイスにアタッチされているタグを一覧表示する許可を付与	リスト	mfa*		
ListMFADevices	IAM ユーザーの MFA デバイスを一覧表示する許可を付与	リスト	user		
ListOpenIDConnectProviderTags	指定された OpenID Connect プロバイダーにアタッチされているタグを一覧表示する許可を付与	リスト	oidc-provider*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListOpenIDConnectProviders	で定義されている IAM OpenID Connect (OIDC) プロバイダーリソースオブジェクトに関する情報を一覧表示するアクセス許可を付与しますAWS アカウント	リスト			
ListOrganizationsFeatures	組織で有効になっている一元化されたルートアクセス機能を一覧表示するアクセス許可を付与します	リスト			
ListPolicies	すべての管理ポリシーを一覧表示する許可を付与	リスト			
ListPoliciesGrantingServiceAccess	エンティティに特定のサービスへのアクセスを付与ポリシーに関する情報をリストする許可を付与	リスト	group*		
			role*		
			user*		
ListPolicyTags	指定された管理ポリシーにアタッチされているタグを一覧表示する許可を付与	リスト	policy*		
ListPolicyVersions	ポリシーのデフォルトバージョンとして設定されているバージョンを含め、指定された管理ポリシーのバージョンに関する情報を一覧表示するアクセス許可を付与	リスト	policy*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListRolePolicies	指定された IAM ロールに埋め込まれているインラインポリシーの名前を一覧表示するアクセス許可を付与	リスト	role*		
ListRoleTags	指定された IAM ロールにアタッチされているタグを一覧表示する許可を付与	リスト	role*		
ListRoles	指定されたパスのプレフィックスを持つ IAM ロールを一覧表示する許可を付与	リスト			
ListSAMLProviderTags	指定された SAML プロバイダーにアタッチされているタグを一覧表示する許可を付与	リスト	saml-provider*		
ListSAMLProviders	IAM で SAML プロバイダーリソースを一覧表示する許可を付与	リスト			
ListSSHPublicKeys	指定された IAM ユーザーに関連付けられた SSH パブリックキーに関する情報を一覧表示する許可を付与	リスト	user*		
ListSTSRegionalEndpointsStatus	すべてのアクティブな STS リージョンエンドポイントのステータスを一覧表示するアクセス許可を付与	リスト			
ListServerCertificateTags	指定されたサーバー証明書にアタッチされているタグを一覧表示する許可を付与	リスト	server-certificate*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListServerCertificates	指定されたパスのプレフィックスを持つサーバー証明書を一覧表示する許可を付与	リスト			
ListServiceSpecificCredentials	指定された IAM ユーザーに関連付けられたサービス固有の認証情報に関する情報を一覧表示する許可を付与	リスト	user*		
ListSigningCertificates	指定の IAM ユーザーに関連付けられているデジタル署名用証明書に関する情報を一覧表示する許可を付与	リスト	user*		
ListUserPolicies	指定された IAM ユーザーに埋め込まれているインラインポリシーの名前を一覧表示するアクセス許可を付与	リスト	user*		
ListUserTags	指定された IAM ユーザーにアタッチされているタグを一覧表示する許可を付与	リスト	user*		
ListUsers	指定されたパスのプレフィックスを持つ IAM ユーザーを一覧表示する許可を付与	リスト			
ListVirtualMFADevices	割り当てステータスにより仮想 MFA デバイスを一覧表示する許可を付与	リスト			
PassRole [許可のみ]	サービスにロールを渡すアクセス許可を付与	書き込み	role*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				iam:AssociatedResourceArn iam:PassedToService	
PutGroupPolicy	指定の IAM グループに埋め込まれたインラインポリシードキュメントを作成または更新する許可を付与	Permissions management	group*		
PutRolePermissionsBoundary	ロールのアクセス許可境界として管理ポリシーを設定する許可を付与	Permissions management	role*		
				iam:PermissionsBoundary	
PutRolePolicy	指定の IAM ロールに埋め込まれたインラインポリシードキュメントを作成または更新する許可を付与	Permissions management	role*		
				iam:PermissionsBoundary	
PutUserPermissionsBoundary	IAM ユーザーのアクセス許可境界として管理ポリシーを設定する許可を付与	Permissions management	user*		
				iam:PermissionsBoundary	
PutUserPolicy	指定の IAM ユーザーに埋め込まれたインラインポリシードキュメントを作成または更新する許可を付与	Permissions management	user*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				iam:PermissionsBoundary	
RemoveClientIDFromOpenIDConnectProvider	指定された IAM OpenID Connect(OIDC) プロバイダーリソースにあるクライアント ID のリストからクライアント ID (閲覧者) を削除する許可を付与	書き込み	oidc-provider*		
RemoveRoleFromInstanceProfile	指定の EC2 インスタンスプロファイルから指定の IAM ロールを削除する許可を付与	書き込み	instance-profile*		
RemoveUserFromGroup	指定されたグループから IAM ユーザーを削除する許可を付与	書き込み	group*		
ResetServiceSpecificCredential	IAM ユーザー用のサービス固有の認証情報について、パスワードをリセットする許可を付与	書き込み	user*		
ResyncMFADevice	指定された MFA デバイスをその IAM エンティティ (ユーザーまたはロール) に同期させるアクセス許可を付与	書き込み	user*		
SetDefaultPolicyVersion	指定されたポリシーの指定されたバージョンを、ポリシーのデフォルトバージョンとして設定する許可を付与	権限の管理	policy*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SetSTSRegionalEndpointStatus	STS リージョナルエンドポイントをアクティブ化または非アクティブ化するアクセス許可を付与	書き込み			
SetSecurityTokenServicePreferences	STS グローバルエンドポイントのトークンバージョンを設定する許可を付与	書き込み			
SimulateCustomPolicy	アイデンティティベースのポリシーまたはリソースベースのポリシーが、特定の API オペレーションおよびリソースのアクセス許可を提供するかどうかをシミュレートする許可を付与	読み込み			
SimulatePrincipalPolicy	指定された IAM エンティティ (ユーザーまたはロール) にアタッチされているアイデンティティベースのポリシーが、特定の API オペレーションおよびリソースのアクセス許可を提供するかどうかをシミュレートする許可を付与	読み込み	group		
			role		
			user		
TagInstanceProfile	インスタンスプロファイルにタグを追加する許可を付与	タグ付け	instance-profile*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
TagMFADevice	仮想 MFA デバイスにタグを追加する許可を付与	タグ付け	mfa*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagOpenIDConnectProvider	OpenID Connect プロバイダーにタグを追加する許可を付与	タグ付け	oidc-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagPolicy	管理ポリシーにタグを追加する許可を付与	タグ付け	policy*		
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagRole	IAM ロールにタグを追加する許可を付与。	タグ付け	role*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagSAMLProvider	SAML プロバイダーにタグを追加する許可を付与	タグ付け	saml-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagServerCertificate	サーバー証明書にタグを追加する許可を付与	タグ付け	server-certificate*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagUser	IAM ユーザーにタグを追加する許可を付与。	タグ付け	user*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagInstanceProfile	インスタンスプロファイルから指定したタグを削除する許可を付与	タグ付け	instance-profile*		
				aws:TagKeys	
UntagMFADevice	仮想 MFA デバイスから指定したタグを削除する許可を付与	タグ付け	mfa*		
				aws:TagKeys	
UntagOpenIDConnectProvider	指定されたタグを OpenID Connect プロバイダーから削除する許可を付与	タグ付け	oidc-provider*		
				aws:TagKeys	
UntagPolicy	管理ポリシーから指定したタグを削除する許可を付与	タグ付け	policy*		
				aws:TagKeys	
UntagRole	ロールから指定したタグを削除する許可を付与	タグ付け	role*		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagSAMLProvider	SAML プロバイダーから指定したタグを削除する許可を付与	タグ付け	saml-provider*		
				aws:TagKeys	
UntagServerCertificate	サーバー証明書から指定したタグを削除する許可を付与	タグ付け	server-certificate*		
				aws:TagKeys	
UntagUser	ユーザーから指定したタグを削除する許可を付与	タグ付け	user*		
				aws:TagKeys	
UpdateAccessKey	指定されたアクセスキーステータスをアクティブまたは非アクティブとして更新するアクセス許可を付与	書き込み	user*		
UpdateAccountEmailAddress	アカウントに関連付けられている E メールアドレスを更新するアクセス許可を付与	書き込み			
UpdateAccountName	アカウントに関連付けられているアカウント名を更新するアクセス許可を付与	書き込み			
UpdateAccountPasswordPolicy	のパスワードポリシー設定を更新するアクセス許可を付与します AWS アカウント	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateAssumeRolePolicy	IAM エンティティにロールを継承する権限を与えるポリシーを更新する許可を付与	権限の管理	role*		
UpdateCloudFrontPublicKey	既存の CloudFront 公開鍵を更新するアクセス許可を付与	書き込み			
UpdateGroup	指定された IAM グループの名前またはパスを更新する許可を付与	書き込み	group*		
UpdateLoginProfile	指定された IAM ユーザーのパスワードを変更する許可を付与	書き込み	user*		
UpdateOpenIDConnectProviderThumbprint	OpenID Connect(OIDC) プロバイダーリソースに関連付けられているサーバー証明書のサムプリントのリスト全体を更新する許可を付与	書き込み	oidc-provider*		
UpdateRole	ロールの説明または最大セッション継続時間の設定を更新する許可を付与	書き込み	role*		
UpdateRoleDescription	ロールの説明のみを更新する許可を付与	書き込み	role*		
UpdateSAMLProvider	既存の SAML プロバイダーリソースのメタデータドキュメントを更新する許可を付与	書き込み	saml-provider*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateSSHPublicKey	IAM ユーザーの SSH パブリックキーのステータスをアクティブまたは非アクティブに更新する許可を付与	書き込み	user*		
UpdateServerCertificate	IAM に保存されている指定のサーバー証明書の名前やパスを更新する許可を付与	書き込み	server-certificate*		
UpdateServiceSpecificCredential	IAM ユーザーに対し、サービス固有の認証情報のステータスをアクティブまたは非アクティブに更新するアクセス許可を付与	書き込み	user*		
UpdateSigningCertificate	指定されたユーザー署名証明書のステータスを有効または無効に更新する許可を付与	書き込み	user*		
UpdateUser	指定された &IAM; ユーザーの名前またはパスを更新する許可を付与	書き込み	user*		
UploadCloudFrontPublicKey	既存の CloudFront 公開鍵をアップロードするアクセス許可を付与	書き込み			
UploadSSHPublicKey	指定された IAM ユーザーに関連付けられた SSH パブリックキーを更新する許可を付与	書き込み	user*		
UploadServerCertificate	のサーバー証明書エンティティをアップロードするアクセス許可を付与します AWS アカウント	書き込み	server-certificate*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
UploadSigningCertificate	X.509 デジタル署名用証明書をアップロードし、指定の IAM ユーザーに関連付けるアクセス許可を付与	書き込み	user*		

AWS Identity And Access Management (IAM) で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
access-report	arn:${Partition}:iam::${Account}:access-report/${EntityPath}	
assumed-role	arn:${Partition}:iam::${Account}:assumed-role/${RoleName}/${RoleSessionName}	
federated-user	arn:${Partition}:iam::${Account}:federated-user/${UserName}	

リソースタイプ	ARN	条件キー
group	arn:${Partition}:iam::${Account}:group/${GroupNameWithPath}	
instance-profile	arn:${Partition}:iam::${Account}:instance-profile/${InstanceProfileNameWithPath}	aws:ResourceTag/${TagKey}
mfa	arn:${Partition}:iam::${Account}:mfa/${MfaTokenIdWithPath}	aws:ResourceTag/${TagKey}
oidc-provider	arn:${Partition}:iam::${Account}:oidc-provider/${OidcProviderName}	aws:ResourceTag/${TagKey}
policy	arn:${Partition}:iam::${Account}:policy/${PolicyNameWithPath}	aws:ResourceTag/${TagKey}
role	arn:${Partition}:iam::${Account}:role/${RoleNameWithPath}	aws:ResourceTag/${TagKey} iam:ResourceTag/${TagKey}
saml-provider	arn:${Partition}:iam::${Account}:saml-provider/${SamlProviderName}	aws:ResourceTag/${TagKey}
server-certificate	arn:${Partition}:iam::${Account}:server-certificate/${CertificateNameWithPath}	aws:ResourceTag/${TagKey}
sms-mfa	arn:${Partition}:iam::${Account}:sms-mfa/${MfaTokenIdWithPath}	

リソースタイプ	ARN	条件キー
user	arn:${Partition}:iam::${Account}:user/${UserNameWithPath}	aws:ResourceTag/${TagKey} iam:ResourceTag/${TagKey}

AWS Identity And Access Management (IAM) の条件キー

AWS Identity and Access Management (IAM) では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられているタグに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーに基づいてアクションをフィルタリングします	ArrayOfString
iam:AWSServiceName	このロールがアタッチされている AWS サービスによってアクセスをフィルタリングします	String
iam:AssociatedResourceArn	ロールが代わりに使用されるリソースによるアクセスをフィルタリングします	ARN

条件キー	説明	タイプ
iam:FIDO-FIPS-140-2-certification	FIDO セキュリティキーの登録時に MFA デバイス FIPS-140-2 検証証明書レベルによるアクセスをフィルタリングします	String
iam:FIDO-FIPS-140-3-certification	FIDO セキュリティキーの登録時に MFA デバイス FIPS-140-3 検証証明書レベルによるアクセスをフィルタリングします	String
iam:FIDO-certification	FIDO セキュリティキーの登録時に MFA デバイス FIDO 認定レベルによるアクセスをフィルタリングします	String
iam:OrganizationsPolicyId	AWS Organizations ポリシーの ID でアクセスをフィルタリングします	String
iam:PassedToService	このロールが渡される AWS サービスによってアクセスをフィルタリングします	String
iam:PermissionsBoundary	指定されたポリシーが、IAM エンティティ (ユーザーまたはロール) でアクセス許可の境界として設定されているかどうかによりアクセスをフィルタリングします。	ARN
iam:PolicyARN	IAM ポリシーの ARN によるアクセスをフィルタリングします。	ARN
iam:RegisterSecurityKey	MFA デバイス有効化の現在の状態によってアクセスをフィルタリングします	String
iam:ResourceTag/${TagKey}	IAM エンティティ (ユーザーまたはロール) にアタッチされたタグによるアクセスをフィルタリングする	String

AWS Identity and Access Management Roles Anywhere のアクション、リソース、条件キー

AWS Identity and Access Management Roles Anywhere (サービスプレフィックス: `rolesanywhere`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Identity And Access Management Roles Anywhere で定義されるアクション
- AWS Identity And Access Management Roles Anywhere で定義されたリソースタイプ
- AWS Identity and Access Management Roles Anywhere の条件キー

AWS Identity And Access Management Roles Anywhere で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイ

プが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateProfile	プロファイルを作成する許可の付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateTrustAnchor	トラストアンカーを作成する許可の付与	書き込み		aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
DeleteAttributeMapping	プロファイルからマッピングルールを削除する許可を付与する	書き込み	profile*		
DeleteCrl	証明書失効リスト (crl) を削除する許可の付与	書き込み	crl*		
DeleteProfile	プロファイルを削除する権限を付与します	書き込み	profile*		
DeleteTrustAnchor	トラストアンカーを削除する許可の付与	書き込み	trust-anchor*		
DisableCrl	証明書失効リスト (crl) を無効にする許可の付与	書き込み	crl*		
DisableProfile	プロファイルを無効にする許可の付与	書き込み	profile*		
DisableTrustAnchor	トラストアンカーを無効にする許可の付与	書き込み	trust-anchor*		
EnableCrl	証明書失効リスト (crl) を有効にする許可の付与	書き込み	crl*		
EnableProfile	プロファイルを有効にする許可の付与	書き込み	profile*		iam:PassRole
EnableTrustAnchor	トラストアンカーを有効にする許可の付与	書き込み	trust-anchor*		
GetCrl	証明書失効リスト (crl) を取得する許可の付与	読み取り	crl*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetProfile	プロファイルを取得する許可の付与	読み取り	profile*		
GetSubject	件名を取得する許可の付与	読み取り	subject*		
GetTrustAnchor	トラストアンカーを取得する許可の付与	読み取り	trust-anchor*		
ImportCrl	証明書失効リスト (crl) をインポートする許可の付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
ListCrls	証明書失効リスト (crls) を一覧表示する許可の付与	リスト			
ListProfiles	プロファイルを一覧表示する許可の付与	リスト			
ListSubjects	件名を一覧表示する許可の付与	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与。	リスト			
ListTrustAnchors	トラストアンカーを一覧表示する許可の付与	リスト			
PutAttributeMapping	マッピングルールをプロファイルに配置する許可を付与する	書き込み	profile*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutNotificationSettings	通知設定をトラストアンカーにアタッチする許可を付与	書き込み	trust-anchor*		
ResetNotificationSettings	カスタム通知設定を IAM Roles Anywhere で定義されたデフォルト状態にリセットする許可を付与	書き込み	trust-anchor*		
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	crl		
			profile		
			subject		
			trust-anchor		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースのタグを解除する許可を付与	Tagging	crl		
			profile		
			subject		
			trust-anchor		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateCrl	証明書失効リスト (crl) を更新する許可の付与	書き込み	crl*		
UpdateProfile	プロファイルを更新する許可の付与	書き込み	profile*		iam:PassRole
UpdateTrustAnchor	トラストアンカーを更新する許可の付与	書き込み	trust-anchor*		

AWS Identity And Access Management Roles Anywhere で定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
trust-anchor	arn:${Partition}:rolesanywhere:${Region}:${Account}:trust-anchor/${TrustAnchorId}	aws:ResourceTag/${TagKey}
profile	arn:${Partition}:rolesanywhere:${Region}:${Account}:profile/${ProfileId}	aws:ResourceTag/${TagKey}
subject	arn:${Partition}:rolesanywhere:${Region}:${Account}:subject/${SubjectId}	aws:ResourceTag/${TagKey}
crl	arn:${Partition}:rolesanywhere:${Region}:${Account}:crl/${CrlId}	aws:ResourceTag/${TagKey}

AWS Identity and Access Management Roles Anywhere の条件キー

AWS Identity and Access Management Roles Anywhere では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Identity Store のアクション、リソース、および条件キー

AWS Identity Store (サービスプレフィックス: identitystore) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Identity Store で定義されるアクション

- AWS Identity Store で定義されるリソースタイプ
- AWS Identity Store の条件キー

AWS Identity Store で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateGroup	指定された IdentityStore にグループを作成するアクセス許可を付与	書き込み	Identitystore*		
CreateGroupMembership	指定された IdentityStore 内のグループにメンバーを作成するアクセス許可を付与	書き込み	Group*		
			Identitystore*		
			User*		
CreateUser	指定された IdentityStore にユーザーを作成するアクセス許可を付与	書き込み	Identitystore*		
DeleteGroup	指定された IdentityStore 内のグループを削除するアクセス許可を付与	書き込み	Group*		
			Identitystore*		
DeleteGroupMembership	指定された IdentityStore 内のグループに属するメンバーを削除するアクセス許可を付与	書き込み	Group*		
			GroupMembership*		
			Identitystore*		
			User*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteUser	指定された IdentityStore 内のユーザーを削除するアクセス許可を付与	書き込み	Identitystore*		
			User*		
DescribeGroup	指定された IdentityStore 内のグループに関する情報を取得するアクセス許可を付与	読み取り	Group*		
			Identitystore*		
DescribeGroupMembership	指定された IdentityStore 内のグループに属するメンバーに関する情報を取得するアクセス許可を付与	読み取り	Group*		
			GroupMembership*		
			Identitystore*		
			User*		
DescribeUser	指定された IdentityStore 内のユーザーに関する情報を取得するアクセス許可を付与	読み取り	Identitystore*		
			User*		
GetGroupId	指定した IdentityStore 内のグループに関する ID 情報を取得するアクセス許可を付与	読み取り	Group*		
			Identitystore*		
GetGroupMembershipId	指定された IdentityStore 内のグループに属するメンバーの ID 情報を取得するアクセス許可を付与	読み取り	Group*		
			GroupMembership*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			Identitystore*		
			User*		
GetUserId	指定された IdentityStore 内のユーザーに関する ID 情報を取得するアクセス許可を付与	読み取り	Identitystore*		
			User*		
IsMemberInGroups	メンバーが、指定された IdentityStore 内のグループに属するかどうかを確認するアクセス許可を付与	読み取り	AllGroupMemberships*		
			Group*		
			Identitystore*		
			User*		
ListGroupMemberships	指定された IdentityStore 内のグループに属するすべてのメンバーを取得するアクセス許可を付与	リスト	AllGroupMemberships*		
			Group*		
			Identitystore*		
ListGroupMembershipsForMember	指定された IdentityStore 内のターゲットメンバーのグループを一覧表示するアクセス許可を付与	リスト	AllGroupMemberships*		
			Identitystore*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			User*		
ListGroups	指定された IdentityStore 内のグループを検索するアクセス許可を付与	リスト	AllGroups*		
			IdentityStore*		
ListUsers	指定された IdentityStore 内のユーザーを検索するアクセス許可を付与	リスト	AllUsers*		
			IdentityStore*		
UpdateGroup	指定された IdentityStore 内のグループに関する情報を更新するアクセス許可を付与	書き込み	Group*		
			IdentityStore*		
UpdateUser	指定された IdentityStore 内のユーザー情報を更新するアクセス許可を付与	書き込み	IdentityStore*		
			User*		

AWS Identity Store で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Identitystore	arn:${Partition}:identitystore::${Account}:identitystore/${IdentityStoreId}	
User	arn:${Partition}:identitystore:::user/${UserId}	
Group	arn:${Partition}:identitystore:::group/${GroupId}	
GroupMembership	arn:${Partition}:identitystore:::membership/${MembershipId}	
AllUsers	arn:${Partition}:identitystore:::user/*	
AllGroups	arn:${Partition}:identitystore:::group/*	
AllGroupMemberships	arn:${Partition}:identitystore:::membership/*	

AWS Identity Store の条件キー

AWS Identity Store では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
identitystore:UserId	IAM Identity Center ユーザー ID でアクセスをフィルタリングします	String

AWS Identity Store Auth のアクション、リソース、条件キー

AWS Identity Store Auth (サービスプレフィックス: `identitystore-auth`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Identity Store Auth で定義されたアクション
- AWS Identity Store Auth で定義されたリソースタイプ
- AWS Identity Store Auth の条件キー

AWS Identity Store Auth で定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchDeleteSession [アクセス許可のみ]	指定されたセッションのバッチを削除する許可を付与	書き込み			
BatchGetSession [アクセス許可のみ]	指定されたセッションのバッチのセッション属性を返す許可を付与	読み取り			
ListSessions [許可のみ]	指定されたユーザーのアクティブなセッションのリストを取得する許可を付与	リスト			

AWS Identity Store Auth で定義されたリソースタイプ

AWS Identity Store Auth は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Identity Store Auth へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Identity Store Auth の条件キー

Identity Store Auth には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Identity Sync のアクション、リソース、および条件キー

AWS Identity Sync (サービスプレフィックス: `identity-sync`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Identity Sync で定義されるアクション
- AWS Identity Sync で定義されるリソースタイプ
- AWS Identity Sync の条件キー

AWS Identity Sync で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AllowVendedLogDeliveryForRe	Sync Profile の vended log 配信を設定する許可を付与する	権限の管理	SyncProfileResource*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
source [アクセス許可のみ]					
CreateSyncFilter	同期プロファイルで同期フィルターを作成するアクセス許可を付与	書き込み	SyncProfileResource*		
CreateSyncProfile	ID ソースの同期プロファイルを作成する許可を付与	書き込み			ds:AuthorizeApplication
CreateSyncTarget	ID ソースの同期ターゲットを作成する許可を付与	書き込み	SyncProfileResource*		
DeleteSyncFilter	同期プロファイルから同期フィルターを削除する許可を付与	書き込み	SyncProfileResource*		
DeleteSyncProfile	ソースから同期プロファイルを削除する許可を付与	書き込み	SyncProfileResource*		ds:UnauthorizeApplication
DeleteSyncTarget	ソースから同期ターゲットを削除する許可を付与	書き込み	SyncProfileResource*		
			SyncTargetResource*		
GetSyncProfile	同期プロファイル名を使用して同期プロファイルを取得する許可を付与	読み取り	SyncProfileResource*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetSyncTarget	同期プロファイルから同期ターゲットを取得する許可を付与	読み取り	SyncProfileResource*		
			SyncTargetResource*		
ListSyncFilters	同期プロファイルから同期フィルターを一覧表示する許可を付与	リスト	SyncProfileResource*		
StartSync	同期プロセスを開始または以前一時停止した同期プロセスを再開する許可を付与	書き込み	SyncProfileResource*		
StopSync	同期スケジュール内の計画された同期プロセスの開始を停止する許可を付与	書き込み	SyncProfileResource*		
UpdateSyncTarget	同期プロファイルの同期ターゲットを更新するアクセス許可を付与	書き込み	SyncProfileResource*		
			SyncTargetResource*		

AWS Identity Sync で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
SyncProfileResource	`arn:${Partition}:identity-sync:${Region}:${Account}:profile/${SyncProfileName}`	
SyncTargetResource	`arn:${Partition}:identity-sync:${Region}:${Account}:target/${SyncProfileName}/${SyncTargetName}`	

AWS Identity Sync の条件キー

Identity Sync には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Import Export Disk Service のアクション、リソース、および条件キー

AWS Import Export Disk Service (サービスプレフィックス: `importexport`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Import Export Disk Service で定義されるアクション
- AWS Import Export Disk Service で定義されるリソースタイプ

- AWS Import Export Disk Service の条件キー

AWS Import Export Disk Service で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CancelJob	このアクションは指定されたジョブをキャンセルします。ジョブの所有者のみがキャンセルできます。ジョブがすでに開始されている場合や完了している場合は、アクションは失敗します。	Write			
CreateJob	このアクションは、データのアップロードまたはダウンロードをスケジュールするプロセスを開始します。	書き込み			
GetShippingLabel	このアクションは、デバイスを に配送して AWS 処理するために使用する前払い配送ラベルを生成します。	読み取り			
GetStatus	このアクションは、ジョブが一連のプロセスのどの段階にあるか、結果のステータス、ジョブに関連付けられた署名値を含む、ジョブに関する情報を返します。	Read			
ListJobs	このアクションは、リクエスタに関連付けられたジョブを返します。	リスト			
UpdateJob	このアクションを使用して、新しいマニフェストファイルを提供し元のマニフェスト	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	ファイルで指定されているパラメータを変更できます。				

AWS Import Export Disk Service で定義されるリソースタイプ

AWS Import Export Disk Service は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Import Export Disk Service へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Import Export Disk Service の条件キー

Import/Export には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Inspector のアクション、リソース、および条件キー

Amazon Inspector (サービスプレフィックス: `inspector`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Inspector で定義されるアクション
- Amazon Inspector で定義されるリソースタイプ
- Amazon Inspector の条件キー

Amazon Inspector で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AddAttributesToFindings	検出結果の ARN によって指定されている検出結果に属性 (キーと値のペア) を割り当てるためのアクセス許可を付与	Write			
CreateAssessmentTarget	CreateResourceGroup によって生成されているリソースグループの ARN を使用して、新しい評価ターゲットを作成する許可を付与	Write			
CreateAssessmentTemplate	評価ターゲットの ARN によって指定されている評価ターゲットの評価テンプレートを作成する許可を付与	Write			
CreateExclusionsPreview	指定された評価テンプレートの除外プレビューの生成を開始する許可を付与	Write			
CreateResourceGroup	Amazon Inspector の評価ターゲットに含まれる EC2 インスタンスの選択に使用される、指定されたタグセット (キーと値のペア) を使用してリソースグループを作成する許可を付与	Write			
DeleteAssessmentRun	評価の実行の ARN によって指定されている評価の実行を削除する許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteAssessmentTarget	評価ターゲットの ARN によって指定されている評価ターゲットを削除する許可を付与	Write			
DeleteAssessmentTemplate	評価テンプレートの ARN によって指定されている評価テンプレートを削除する許可を付与	Write			
DescribeAssessmentRuns	評価の実行の ARN によって指定されている評価の実行を記述する許可を付与	Read			
DescribeAssessmentTargets	評価ターゲットの ARN によって指定されている評価ターゲットを記述する許可を付与	Read			
DescribeAssessmentTemplates	評価テンプレートの ARN によって指定されている評価テンプレートを記述する許可を付与	読み取り			
DescribeCrossAccountAccessRole	Amazon Inspector が にアクセスできるようにする IAM ロールを記述するアクセス許可を付与します AWS アカウント	読み取り			
DescribeExclusions	除外の ARN によって指定されている除外を記述する許可を付与	Read			
DescribeFindings	検出結果の ARN によって指定されている検出結果を記述する許可を付与	Read			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeResourceGroups	リソースグループの ARN によって指定されているリソースグループを記述する許可を付与	Read			
DescribeRulesPackages	ルールパッケージの ARN によって指定されているルールパッケージを記述する許可を付与	Read			
GetAssessmentReport	指定された評価の実行の詳細かつ包括的な結果を含む評価レポートを作成する許可を付与	Read			
GetExclusionsPreview	プレビュートークンによって指定されている除外プレビュー (ExclusionPreview オブジェクトのリスト) を取得する許可を付与	Read			
GetTelemetryMetadata	指定された評価の実行用に収集されているデータに関する情報を取得する許可を付与	Read			
ListAssessmentRunAgents	評価の実行の ARN によって指定されている評価の実行のエージェントを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListAssessmentRuns	評価テンプレートの ARN によって指定されている評価テンプレートに対応する評価の実行を一覧表示する許可を付与	リスト			
ListAssessmentTargets	この内の評価ターゲットの ARNs を一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListAssessmentTemplates	評価ターゲットの ARN によって指定されている評価ターゲットに対応する評価テンプレートを一覧表示する許可を付与	リスト			
ListEventSubscriptions	評価テンプレートの ARN によって指定されている評価テンプレートのすべてのイベントサブスクリプションを一覧表示する許可を付与	リスト			
ListExclusions	評価の実行によって生成された除外を一覧表示する許可を付与	リスト			
ListFindings	評価の実行の ARN によって指定されている評価の実行によって生成された結果を一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListRulesPackages	利用可能な Amazon Inspector ルールパッケージを一覧表示する許可を付与	リスト			
ListTagsForResource	評価テンプレートに関連付けられたすべてのタグを一覧表示する許可を付与	Read			
PreviewAgents	指定された評価ターゲットの一部である EC2 インスタンスにインストールされているエージェントをプレビューする許可を付与	Read			
RegisterCrossAccountAccessRole	評価の実行の開始時または PreviewAgents アクションを呼び出す際に Amazon Inspector による EC2 インスタンスの一覧表示に使用される IAM ロールを登録する許可を付与	Write			
RemoveAttributesFromFindings	指定されたキーを持つ属性が存在する検索結果の ARN によって指定されている検索結果から属性全体 (キーと値のペア) を削除する許可を付与	Write			
SetTagsForResource	タグ (キーと値のペア) を評価テンプレートの ARN によって指定されている評価テンプレートに設定する許可を付与	タグ付け			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartAssessmentRun	評価テンプレートの ARN によって指定されている評価の実行を開始する許可を付与	Write			
StopAssessmentRun	評価の実行の ARN によって指定されている評価の実行を停止する許可を付与	Write			
SubscribeToEvent	指定されたイベントに関する Amazon Simple Notification Service (SNS) 通知を指定された SNS トピックに送信するプロセスを有効にする許可を付与	Write			
UnsubscribeFromEvent	指定されたイベントに関する Amazon Simple Notification Service (SNS) 通知を指定された SNS トピックに送信するプロセスを無効にする許可を付与	Write			
UpdateAssessmentTarget	評価ターゲットの ARN によって指定されている評価ターゲットを更新する許可を付与	Write			

Amazon Inspector で定義されるリソースタイプ

Amazon Inspector では、IAM ポリシーステートメントの `Resource` 要素でのリソース ARN の指定はサポートされていません。Amazon Inspector へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

Amazon Inspector の条件キー

Inspector には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Inspector2 のアクション、リソース、および条件キー

Amazon Inspector2(サービスプレフィックス: inspector2) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース,アクションおよび条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Inspector2 で定義されるアクション
- Amazon Inspector2によって定義されるリソースタイプ
- Amazon Inspector2 の条件キー

Amazon Inspector2 で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateMember	アカウントを Amazon Inspector 管理者アカウントに関連付けるアクセス許可を付与します。	書き込み			
BatchAssociateCodeSecurityS	複数のコードリポジトリを Amazon Inspector コードセキュリティスキャン設定に関	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
canConfiguration	連付けるアクセス許可を付与します				
BatchDisassociateCodeSecurityScanConfiguration	Amazon Inspector コードセキュリティスキャン設定から複数のコードリポジトリの関連付けを解除するアクセス許可を付与します	書き込み			
BatchGetAccountStatus	アカウントの Amazon Inspectorアカウントに関する情報を取得するアクセス許可を付与します。	読み取り			
BatchGetCodeSnippet	コードの脆弱性に関する 1 つ以上の検出結果に関するコードスニペットの情報を取得するための許可を付与します	読み取り			
BatchGetFindingDetails	検出結果に関する強化された脆弱性インテリジェンスの詳細をお客様が取得できるようにするアクセス許可を付与します	読み取り			
BatchGetFreeTrialInfo	アカウントの Amazon Inspector アカウントに関する無料トライアル期間の資格を取得する権限を付与します。	読み取り			
BatchGetMemberEc2DeepInspectionStatus	委任管理者にメンバーアカウントの ec2 Deep Inspection ステータスを取得するアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchUpdateMemberEc2DeepInspectionStatus	関連するメンバーアカウントの委任管理者による ec2 Deep Inspection ステータスを更新するアクセス許可を付与します	書き込み			
CancelFindingsReport	調査結果レポートの生成をキャンセルするアクセス許可を付与します。	書き込み			
CancelSbomExport	SBOM レポートの生成をキャンセルする許可を付与	書き込み			
CreateCisScanConfiguration	CIS スキャン設定の設定を作成および定義する許可を付与する	書き込み	CIS Scan Configuration*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateCodeSecurityIntegration	ソースコードリポジトリプロバイダーとのコードセキュリティ統合を作成するアクセス許可を付与します	書き込み	Code Security Integration*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCodeSecurityScanConfiguration	コードセキュリティスキャンのスキャン設定を作成するアクセス許可を付与します	書き込み	CodeSecurityScanConfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFilter	結果フィルターの設定を作成および定義する許可を付与	書き込み	Filter*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingsReport	調査結果レポートの生成を要求する権限を付与します。	書き込み			
CreateSbomExport	SBOM レポートの生成をリクエストする許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteCisScanConfiguration	CIS スキャン設定を削除する許可を付与する	書き込み	CIS Scan Configuration*		
				aws:ResourceTag/${TagKey}	
DeleteCodeSecurityIntegration	コードセキュリティ統合を削除するアクセス許可を付与します	書き込み	Code Security Integration*		
DeleteCodeSecurityScanConfiguration	コードセキュリティスキャン設定を削除するアクセス許可を付与します	書き込み	Code Security Scan Configuration*		
DeleteFilter	結果フィルターを削除する許可を付与	書き込み	Filter*		
DescribeOrganizationConfiguration	AWS 組織の Amazon Inspector 設定に関する情報を取得するアクセス許可を付与します	読み取り			
Disable	Amazon Inspector アカウントを無効にするアクセス許可を付与します。	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisableDelegatedAdminAccount	AWS 組織の委任 Amazon Inspector 管理者アカウントとしてアカウントを無効にするアクセス許可を付与します	書き込み			
DisassociateMember	Amazon Inspector 管理者アカウントに Inspector メンバーアカウントとの関連付けを解除する許可を付与します。	書き込み			
Enable	新しい Amazon Inspector アカウントの設定を有効にして指定するためのアクセス許可を付与します。	書き込み			
EnableDelegatedAdminAccount	AWS 組織の委任 Amazon Inspector 管理者アカウントとしてアカウントを有効にするアクセス許可を付与します	書き込み			
GetCisScanReport	完了した CIS スキャンに関する情報を含むレポートを取得する許可を付与する	読み取り			
GetCisScanResultDetails	1 つの CIS スキャンと 1 つのターゲットリソースに関連するすべての詳細に関する情報を取得する許可を付与する	リスト			
GetClustersForImage	継続的にスキャンされる特定の Amazon Ecr イメージのクラスター情報を取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetCodeSecurityIntegration	コードセキュリティ統合に関する情報を取得するアクセス許可を付与します	読み取り			
GetCodeSecurityScan	特定のコードセキュリティスキャンに関する情報を取得するアクセス許可を付与します	読み取り			
GetCodeSecurityScanConfiguration	コードセキュリティスキャン設定に関する情報を取得するアクセス許可を付与します	読み取り			
GetConfiguration	の Amazon Inspector 設定に関する情報を取得するアクセス許可を付与します AWS アカウント	読み取り			
GetDelegatedAdminAccount	Amazon Inspector 管理者アカウントに関する情報を取得するアクセス許可をアカウントに付与します。	読み取り			
GetEc2DeepInspectionConfiguration	スタンドアロンアカウント、委任管理者、およびメンバーアカウントの ec2 Deep Inspection 構成を取得するアクセス許可を付与します	読み取り			
GetEncryptionKey	コードス二ペットの暗号化に使用される KMS キーに関する情報を取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetFindingsReportStatus	リクエストされた結果レポートのステータスを取得するアクセス許可を付与します。	読み取り			
GetMember	Amazon Inspector 管理者アカウントに関連付けられているアカウントに関する情報を取得する許可を付与します。	読み取り			
GetSbomExport	リクエストされた SBOM レポートを取得する許可を付与	読み取り			
ListAccountPermissions	組織内の Amazon Inspector アカウントに関連付けられている機能設定アクセス許可を取得するアクセス許可を付与します	リスト			
ListCisScanConfigurations	すべての CIS スキャン設定に関する情報を取得する許可を付与する	リスト			
ListCisScanResultsAggregatedByChecks	1 つの CIS スキャンに関連するすべてのチェックに関する情報を取得する許可を付与する	リスト			
ListCisScanResultsAggregatedByTargetResource	1 つの CIS スキャンに関連するすべてのリソースに関する情報を取得する許可を付与する	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListCisScans	完了した CIS スキャンに関する情報を取得する許可を付与する	リスト			
ListCodeSecurityIntegrations	アカウント内のすべてのコードセキュリティ統合を一覧表示するアクセス許可を付与します	リスト			
ListCodeSecurityScanConfigurationAssociations	コードリポジトリと Amazon Inspector コードセキュリティスキャン設定間の関連付けを一覧表示するアクセス許可を付与します	リスト			
ListCodeSecurityScanConfigurations	アカウント内のすべてのコードセキュリティスキャン設定を一覧表示するアクセス許可を付与します	リスト			
ListCoverage	Amazon Inspector がリソースインスペクターモニターに対して生成できる統計情報のタイプを取得する権限を付与します。	リスト			
ListCoverageStatistics	Amazon Inspector がモニターするリソースに関する統計データおよびその他の情報を取得する許可を付与します。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListDelegatedAdminAccounts	AWS 組織の委任 Amazon Inspector 管理者アカウントに関する情報を取得する許可を付与	リスト			
ListFilters	すべての結果フィルターに関する情報を取得する許可を付与	リスト			
ListFindingAggregations	Amazon Inspector の調査結果に関する統計データおよびその他の情報を取得するアクセス許可を付与します。	リスト			
ListFindings	1 つ以上の結果に関する情報のサブセットを取得する許可を付与	リスト			
ListMembers	Inspector 管理者アカウントに関連付けられている Amazon Inspector メンバーアカウントに関する情報を取得する許可を付与します。	リスト			
ListTagsForResource	Amazon Inspector リソースのタグを取得する許可を付与します。	読み取り			
ListUsageTotals	アカウントの集計使用状況データを取得する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ResetEncryptionKey	Amazon が所有する KMS キーを使用してコードスニペットを暗号化するため、お客様がリセットできるようにする許可を付与	書き込み			
SearchVulnerabilities	特定の脆弱性に対する Amazon Inspector のカバレッジ詳細を一覧表示する許可を付与します	読み取り			
SendCisSessionHealth	CIS スキャンの CIS ヘルスを送信する許可を付与する	書き込み			
SendCisSessionTelemetry	CIS スキャンの CIS テレメトリを送信する許可を付与する	書き込み			
StartCisSession	CIS スキャンセッションを開始する許可を付与する	書き込み			
StartCodeSecurityScan	指定されたリポジトリでコードセキュリティスキャンを開始するアクセス許可を付与します	書き込み			
StopCisSession	CIS スキャンセッションを停止する許可を付与する	書き込み			
TagResource	Amazon Inspector リソースのタグを追加もしくは更新する許可を付与します。	Tagging	CIS Scan Configuration		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			Code Security Integration		
			Code Security Scan Configuration		
			Filter		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
UntagResource	Amazon Inspectorリソースからタグを削除するためのアクセス許可を付与します。	Tagging	CIS Scan Configuration		
			Code Security Integration		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			Code Security Scan Configuration		
			Filter		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCisScanConfiguration	CIS スキャン設定の設定を更新する許可を付与する	書き込み	CIS Scan Configuration*		
				aws:ResourceTag/${TagKey}	
UpdateCodeSecurityIntegration	既存のコードセキュリティ統合を更新するアクセス許可を付与します	書き込み	Code Security Integration*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateCodeSecurityScanConfiguration	既存のコードセキュリティスキャン設定を更新するアクセス許可を付与します	書き込み	CodeSecurityScanConfiguration*		
				aws:ResourceTag/${TagKey}	
UpdateConfiguration	の Amazon Inspector 設定に関する情報を更新するアクセス許可を付与します AWS アカウント	書き込み			
UpdateEc2DeepInspectionConfiguration	委任管理者、メンバー、およびスタンドアロンアカウントによる ec2 Deep Inspection 構成を更新するアクセス許可を付与します	書き込み			
UpdateEncryptionKey	お客様が KMS キーを使用してコードスニペットを暗号化できるようにする許可を付与	書き込み			
UpdateFilter	結果フィルターの設定を更新する許可を付与	書き込み	Filter*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateOrgEc2DeepInspectionConfiguration	関連するメンバーアカウントの委任管理者による ec2 Deep Inspection 構成を更新するアクセス許可を付与します	書き込み			
UpdateOrganizationConfiguration	AWS 組織の Amazon Inspector 設定を更新する許可を付与	書き込み			

Amazon Inspector2によって定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Filter	arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/filter/${FilterId}	aws:ResourceTag/${TagKey}
Finding	arn:${Partition}:inspector2:${Region}:${Account}:finding/${FindingId}	
CIS Scan Configuration	arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/cis-configuration/${CISScanConfigurationId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
Code Security Scan Configuration	arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/codesecurity-configuration/${CodeSecurityScanConfigurationId}	aws:ResourceTag/${TagKey}
Code Security Integration	arn:${Partition}:inspector2:${Region}:${Account}:codesecurity-integration/${CodeSecurityIntegrationId}	aws:ResourceTag/${TagKey}

Amazon Inspector2 の条件キー

Amazon Inspector2 では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

Amazon InspectorScan のアクション、リソース、および条件キー

Amazon InspectorScan (サービスプレフィックス: `inspector-scan`) では、IAM 許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon InspectorScan で定義されるアクション
- Amazon InspectorScan で定義されるリソースタイプ
- Amazon InspectorScan の条件キー

Amazon InspectorScan で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ScanSbom	お客様提供の SBOM をスキャンし、内部で検出された脆弱性を返すためのアクセス許可を付与	読み取り			

Amazon InspectorScan で定義されるリソースタイプ

Amazon InspectorScan では、IAM ポリシーステートメントの Resource 要素でリソース ARN を指定することはできません。Amazon InspectorScan へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

Amazon InspectorScan の条件キー

InspectorScan には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーがありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Interactive Video Service のアクション、リソース、および条件キー

Amazon Interactive Video Service (サービスプレフィックス: ivs) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Interactive Video Service で定義されるアクション
- Amazon Interactive Video Service で定義されるリソースタイプ
- Amazon Interactive Video Service の条件キー

Amazon Interactive Video Service で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にア

クションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchGetChannel	チャネル ARN によって複数のチャネルを同時に取得する許可を付与。	Read	Channel*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchGetStreamKey	ストリームキー ARN によって複数のストリームキーを同時に取得する許可を付与。	読み取り	Stream-Key*		
BatchStartViewerSessionRevocation	複数のチャネル ARN とビューワー ID のペアに対して StartViewerSessionRevocation を同時に実行するための許可を付与します	書き込み	Channel*		
CreateChannel	新しいチャネルおよび関連付けられているストリームキーを作成する許可を付与。	書き込み	Channel*		
			Stream-Key*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEncoderConfiguration	新しいエンコーダー設定を作成するためのアクセス許可を付与	書き込み	Encoder-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateIngestConfiguration	新しい取り込み設定を作成する許可を付与する	書き込み	Ingest-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateParticipantToken	参加者トークンを作成するための許可を付与します	書き込み	Stage*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePlaybackRestrictionPolicy	再生制限ポリシーを作成する許可を付与する	書き込み	Playback-Restriction-Policy*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRecordingConfiguration	新しい記録設定を作成する許可を付与。	書き込み	Recording-Configuration*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStage	ステージを作成するための許可を付与します	書き込み	Stage*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStorageConfiguration	新しいストレージ設定を作成するためのアクセス許可を付与	書き込み	Storage-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStreamKey	ストリームキーを作成する許可を付与。	Write	Stream-Key*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChannel	チャネルおよびチャネルのストリームキーを削除する許可を付与。	書き込み	Channel*		
			Stream-Key*		
DeleteEncoderConfiguration	指定された ARN のエンコーダー設定を削除するためのアクセス許可を付与	書き込み	Encoder-Configuration*		
DeleteIngestConfiguration	指定された ARN の取り込み設定を削除する許可を付与する	書き込み	Ingest-Configuration*		
DeletePlaybackKeyPair	指定された ARN の再生キーペアを削除する許可を付与。	書き込み	Playback-Key-Pair*		
DeletePlaybackRestrictionPolicy	指定された ARN の再生制限ポリシーを削除する許可を付与する	書き込み	Playback-Restriction-Policy*		
DeletePublicKey	指定された ARN のパブリックキーを削除する許可を付与する	書き込み	Public-Key*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteRecordingConfiguration	指定した ARN の記録設定を削除する許可を付与。	書き込み	Recording-Configuration*		
DeleteStage	指定された ARN のステージを削除するための許可を付与します	書き込み	Stage*		
DeleteStorageConfiguration	指定された ARN のストレージ設定を削除するためのアクセス許可を付与	書き込み	Storage-Configuration*		
DeleteStreamKey	指定された ARN のストリームキーを削除する許可を付与。	書き込み	Stream-Key*		
DisconnectParticipant	指定されたステージ ARN から参加者を切断するための許可を付与します	書き込み	Stage*		
GetChannel	指定されたチャネル ARN のチャネル設定を取得する許可を付与。	読み取り	Channel*		
GetComposition	指定された ARN の構成を取得するためのアクセス許可を付与	読み取り	Composition*		
GetEncoderConfiguration	指定された ARN のエンコーダー設定を取得するためのアクセス許可を付与	読み取り	Encoder-Configuration*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetIngestConfiguration	指定された ARN の取り込み設定を取得する許可を付与する	読み取り	Ingest-Configuration*		
GetParticipant	指定されたステージ ARN、セッション、および参加者の参加者情報を取得するアクセス許可を付与します	読み取り	Stage*		
GetPlaybackKeyPair	指定された ARN の再生キーペア情報を取得する許可を付与。	読み取り	Playback-Key-Pair*		
GetPlaybackRestrictionPolicy	指定された ARN の再生制限ポリシーを取得する許可を付与する	読み取り	Playback-Restriction-Policy*		
GetPublicKey	指定された ARN のパブリックキーを取得する許可を付与する	読み取り	Public-Key*		
GetRecordingConfiguration	指定した ARN の記録設定を取得する許可を付与。	読み取り	Recording-Configuration*		
GetStage	指定された ARN のステージ情報を取得するための許可を付与します	読み取り	Stage*		
GetStageSession	指定されたステージ ARN とセッションのステージセッション情報を取得するアクセス許可を付与します	読み取り	Stage*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetStorageConfiguration	指定された ARN のストレージ設定を取得するためのアクセス許可を付与	読み取り	Storage-Configuration*		
GetStream	指定されたチャネルのアクティブ (ライブ) ストリームに関する情報を取得する許可を付与。	Read	Channel*		
GetStreamKey	指定された ARN のストリームキー情報を取得する許可を付与。	読み取り	Stream-Key*		
GetStreamSession	指定されたチャネルのストリームセッションに関する情報を取得する許可を付与します。	読み取り	Channel*		
ImportPlaybackKeyPair	パブリックキーをインポートする許可を付与。	書き込み	Playback-Key-Pair*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ImportPublicKey	パブリックキーをインポートする許可を付与する	書き込み	Public-Key*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
ListChannels	チャネルの概要情報を取得する許可を付与。	リスト	Channel*		
ListCompositions	構成に関する情報を取得するためのアクセス許可を付与	リスト	Encoder-Configuration		
			Stage		
ListEncoderConfigurations	エンコーダー設定に関する概要情報を取得するためのアクセス許可を付与	リスト			
ListIngestConfigurations	取り込み設定に関する概要情報を取得するための許可を付与する	リスト			
ListParticipantEvents	指定されたステージ ARN、セッション、および参加者の参加者イベントを一覧表示するアクセス許可を付与します	リスト	Stage*		
ListParticipantReplicas	参加者レプリカに関する概要情報を取得する許可を付与	リスト	Stage*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListParticipants	指定されたステージ ARN とセッションの参加者を一覧表示するアクセス許可を付与します	リスト	Stage*		
ListPlaybackKeyPairs	再生キーペアに関する概要情報を取得する許可を付与。	リスト	Playback-Key-Pair*		
ListPlaybackRestrictionPolicies	再生制限ポリシーの概要情報を取得する許可を付与する	リスト			
ListPublicKeys	パブリックキーの概要情報を取得する許可を付与する	リスト			
ListRecordingConfigurations	記録設定に関する概要情報を取得する許可を付与。	リスト	Recording-Configuration*		
ListStageSessions	指定されたステージ ARN のステージセッションを一覧表示するアクセス許可を付与します	リスト	Stage*		
ListStages	ステージの概要情報を取得するための許可を付与します	リスト	Stage*		
ListStorageConfigurations	ストレージ設定に関する概要情報を取得するためのアクセス許可を付与	リスト			
ListStreamKeys	ストリームキーの概要情報を取得する許可を付与。	リスト	Channel*		
			Stream-Key*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListStreamSessions	指定されたチャネルのストリームセッションに関する情報を取得する許可を付与します。	リスト	Channel*		
ListStreams	ライブストリームの概要情報を取得する許可を付与。	リスト	Channel*		
ListTagsForResource	指定された ARN のタグに関する情報を取得する許可を付与。	Read	Channel		
			Composition		
			Encoder-Configuration		
			Ingest-Configuration		
			Playback-Key-Pair		
			Playback-Restriction-Policy		
			Public-Key		
			Recording-Configuration		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			Stage		
			Storage-Configuration		
			Stream-Key		
				aws:TagKeys aws:RequestTag/${TagKey}	
PutMetadata	指定されたチャネルの RTMP ストリームにメタデータを挿入する許可を付与。	書き込み	Channel*		
StartComposition	新しい構成を開始するためのアクセス許可を付与	書き込み	Encoder-Configuration*		
			Stage*		
			Channel		
			Storage-Configuration		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
StartParticipantReplication	新しい参加者のレプリケーションを開始するアクセス許可を付与します	書き込み	Stage*		
				aws:TagKeys aws:RequestTag/${TagKey}	
StartViewerSessionRevocation	指定されたチャネル ARN とビューワー ID に関連付けられたビューワーセッションを取り消すプロセスを開始するための許可を付与します	書き込み	Channel*		
StopComposition	指定された ARN の構成を停止するためのアクセス許可を付与	書き込み	Composition*		
StopParticipantReplication	指定された ARN の参加者のレプリケーションを停止するアクセス許可を付与します	書き込み	Stage*		
StopStream	指定されたチャネルのストリーマを切断する許可を付与。	Write	Channel*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
TagResource	指定された ARN を持つリソースのタグを追加または更新する許可を付与。	タグ付け	Channel		
			Composition		
			Encoder-Configuration		
			Ingest-Configuration		
			Playback-Key-Pair		
			Playback-Restriction-Policy		
			Public-Key		
			Recording-Configuration		
			Stage		
			Storage-Configuration		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			Stream-Key		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	指定された ARN を持つリソースのタグを削除する許可を付与。	タグ付け	Channel		
			Composition		
			Encoder-Configuration		
			Ingest-Configuration		
			Playback-Key-Pair		
			Playback-Restriction-Policy		
			Public-Key		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			Recording-Configuration		
			Stage		
			Storage-Configuration		
			Stream-Key		
				aws:TagKeys	
UpdateChannel	チャネルの設定を更新する許可を付与。	書き込み	Channel*		
UpdateIngestConfiguration	指定された ARN の取り込み設定を更新する許可を付与する	書き込み	Ingest-Configuration*		
UpdatePlaybackRestrictionPolicy	指定された ARN の再生制限ポリシーを更新する許可を付与する	書き込み	Playback-Restriction-Policy*		
UpdateStage	ステージの設定を更新するための許可を付与します	書き込み	Stage*		

Amazon Interactive Video Service で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Channel	arn:${Partition}:ivs:${Region}:${Account}:channel/${ResourceId}	aws:ResourceTag/${TagKey}
Stream-Key	arn:${Partition}:ivs:${Region}:${Account}:stream-key/${ResourceId}	aws:ResourceTag/${TagKey}
Playback-Key-Pair	arn:${Partition}:ivs:${Region}:${Account}:playback-key/${ResourceId}	aws:ResourceTag/${TagKey}
Playback-Restriction-Policy	arn:${Partition}:ivs:${Region}:${Account}:playback-restriction-policy/${ResourceId}	aws:ResourceTag/${TagKey}
Recording-Configuration	arn:${Partition}:ivs:${Region}:${Account}:recording-configuration/${ResourceId}	aws:ResourceTag/${TagKey}
Stage	arn:${Partition}:ivs:${Region}:${Account}:stage/${ResourceId}	aws:ResourceTag/${TagKey}
Composition	arn:${Partition}:ivs:${Region}:${Account}:composition/${ResourceId}	aws:ResourceTag/${TagKey}
Encoder-Configuration	arn:${Partition}:ivs:${Region}:${Account}:encoder-configuration/${ResourceId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
Storage-Configuration	arn:${Partition}:ivs:${Region}:${Account}:storage-configuration/${ResourceId}	aws:ResourceTag/${TagKey}
Public-Key	arn:${Partition}:ivs:${Region}:${Account}:public-key/${ResourceId}	aws:ResourceTag/${TagKey}
Ingest-Configuration	arn:${Partition}:ivs:${Region}:${Account}:ingest-configuration/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon Interactive Video Service の条件キー

Amazon Interactive Video Service は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストに関連付けられたタグでアクセスをフィルタリングします。	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon Interactive Video Service Chat のアクション、リソース、および条件キー

Amazon Interactive Video Service Chat (サービスプレフィックス: `ivschat`) では、IAM 許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Interactive Video Service Chat で定義されるアクション
- Amazon Interactive Video Service Chat で定義されるリソースタイプ
- Amazon Interactive Video Service Chat の条件キー

Amazon Interactive Video Service Chat で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイ

プが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateChatToken	ルームへの個々の WebSocket 接続を確立するために使用される暗号化されたトークンを作成する権限を付与する	書き込み	Room*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLoggingConfiguration	クライアントがルームメッセージを記録することができ	書き込み	Logging-C		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	るログ設定を作成する許可を付与		onfiguration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRoom	クライアントが接続してメッセージを渡すことができるルームを作成する許可を付与する	書き込み	Room*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteLoggingConfiguration	指定したログ設定 ARN のログ設定を削除する許可を付与	書き込み	Logging-Configuration*		
DeleteMessage	特定のルームにイベントを送信する権限を付与し、クライアントに特定のメッセージを削除するように指示します。	書き込み	Room*		
DeleteRoom	指定されたルーム ARN のルームを削除する許可を付与する	書き込み	Room*		
DisconnectUser	ルームから指定されたユーザー ID を使用してすべての接続を切断する権限を付与する	書き込み	Room*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetLoggingConfiguration	指定したログ設定 ARN のログ設定を取得する許可を付与	読み取り	Logging-Configuration*		
GetRoom	指定されたルーム ARN のルーム設定を取得する許可を付与する	読み取り	Room*		
ListLoggingConfigurations	ログ設定に関する概要情報を取得する許可を付与	リスト	Logging-Configuration*		
ListRooms	ルームの概要情報を取得する許可を付与する	リスト	Room*		
ListTagsForResource	指定された ARN のタグに関する情報を取得する許可を付与。	読み取り	Room		
				aws:TagKeys aws:RequestTag/${TagKey}	
SendEvent	ルームにイベントを送信する許可を付与する	書き込み	Room*		
TagResource	指定された ARN を持つリソースのタグを追加または更新する許可を付与。	タグ付け	Logging-Configuration		
			Room		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	指定された ARN を持つリソースのタグを削除する許可を付与。	Tagging	Logging-Configuration		
			Room		
				aws:TagKeys	
UpdateLoggingConfiguration	指定したログ設定 ARN のログ設定を更新する許可を付与	書き込み	Logging-Configuration*		
UpdateRoom	指定したルーム ARN のルーム設定を削除する許可を付与する	書き込み	Room*		

Amazon Interactive Video Service Chat で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Room	arn:${Partition}:ivschat:${Region}:${Account}:room/${ResourceId}	aws:ResourceTag/${TagKey}
Logging-Configuration	arn:${Partition}:ivschat:${Region}:${Account}:logging-configuration/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon Interactive Video Service Chat の条件キー

Amazon Interactive Video Service Chat は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストに関連付けられたタグでアクセスをフィルタリングします。	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS 請求サービスのアクション、リソース、および条件キー

AWS Invoicing Service (サービスプレフィックス: invoicing) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS 請求サービスで定義されるアクション
- AWS 請求サービスで定義されるリソースタイプ
- AWS 請求サービスの条件キー

AWS 請求サービスで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchGetInvoiceProfile	組織内のアカウントの請求書プロファイルの詳細を取得する許可を付与	読み取り			
CreateInvoiceUnit	組織の請求書単位を作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteInvoiceUnit	組織の請求書単位を更新するアクセス許可を付与します	書き込み	invoice-unit*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetInvoiceEmailDeliveryPreferences [アクセス許可のみ]	請求書の E メール配信設定を取得するアクセス許可を付与	読み取り			
GetInvoicePDF [許可のみ]	請求書 PDF を取得するアクセス許可を付与	読み取り			
GetInvoiceUnit	組織の請求書ユニットを取得するアクセス許可を付与します	読み取り	invoice-unit*		
ListInvoiceSummaries	アカウントまたは連結アカウントの請求書概要情報を取得するアクセス許可を付与	読み取り			
ListInvoiceUnits	組織の請求書単位を一覧表示するアクセス許可を付与します	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み込み	invoice-unit*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutInvoiceEmailDeliveryPreferences [許可のみ]	請求書の E メール配信設定を配置するアクセス許可を付与	書き込み			
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	invoice-unit*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	リソースのタグを解除する許可を付与	Tagging	invoice-unit*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateInvoiceUnit	組織の請求書単位を更新するアクセス許可を付与します	書き込み	invoice-unit*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	

AWS 請求サービスで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
invoice-unit	arn:${Partition}:invoicing::${Account}:invoice-unit/${Identifier}	aws:ResourceTag/${TagKey}

AWS 請求サービスの条件キー

AWS Invoicing Service では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	各タグの許可された値のセットでアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値でアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内の必須タグが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

AWS IoT 1-Click のアクション、リソース、および条件キー

AWS IoT 1-Click (サービスプレフィックス: `iot1click`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IoT 1-Click で定義されるアクション
- AWS IoT 1-Click で定義されるリソースタイプ
- AWS IoT 1-Click の条件キー

AWS IoT 1-Click で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateDeviceWithPlacement	デバイスを配置に関連付けるアクセス許可を付与する	書き込み	project*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ClaimDevicesByClaimCode	登録コードを使用してデバイスのバッチを申請する許可を付与	読み込み			
CreatePlacement	プロジェクト内に新しい配置を作成する許可を付与	書き込み	project*		
CreateProject	新しいプロジェクトを作成するアクセス許可を付与	書き込み	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePlacement	プロジェクトから配置を削除する許可を付与	書き込み	project*		
DeleteProject	プロジェクトを削除する許可を付与	書き込み	project*		
DescribeDevice	デバイスを記述する許可を付与	読み込み	device*		
DescribePlacement	配置を説明する許可を付与	読み込み	project*		
DescribeProject	プロジェクトを記述する許可を付与	読み込み	project*		
DisassociateDeviceFromPlacement	デバイスと配置の関連付けを解除する許可を付与	書き込み	project*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
FinalizeDeviceClaim	デバイスの登録を確定する許可を付与	読み込み	device*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetDeviceMethods	デバイスの利用可能なメソッドを取得する許可を付与	読み込み	device*		
GetDevicesInPlacement	配置に関連付けられたデバイスを取得する許可を付与	読み込み	project*		
InitiateDeviceClaim	デバイスの登録を初期化する許可を付与	読み込み	device*		
InvokeDeviceMethod	デバイスメソッドを呼び出すアクセス許可を付与する	書き込み	device*		
ListDeviceEvents	デバイス別に公開された過去のイベントを一覧表示する許可を付与	読み込み	device*		
ListDevices	すべてのデバイスを一覧表示する許可を付与	リスト			
ListPlacements	プロジェクト内の配置を一覧表示する許可を付与	読み込み	project*		
ListProjects	すべてのプロジェクトを一覧表示する権限を付与します	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み込み	device		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			project		
TagResource	リソースのタグを追加または変更する許可を付与	タグ付け	device		
			project		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnclaimDevice	デバイスの登録を取り消すアクセス許可を付与する	読み込み	device*		
UntagResource	指定されたタグ (メタデータ) をリソースから削除する許可を付与	タグ付け	device		
			project		
				aws:TagKeys	
UpdateDeviceState	デバイスの状態を更新する許可を付与	書き込み	device*		
UpdatePlacement	配置を更新する許可を付与	書き込み	project*		
UpdateProject	プロジェクトを更新します。	書き込み	project*		

AWS IoT 1-Click で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
device	arn:${Partition}:iot1click:${Region}:${Account}:devices/${DeviceId}	aws:ResourceTag/${TagKey}
project	arn:${Partition}:iot1click:${Region}:${Account}:projects/${ProjectName}	aws:ResourceTag/${TagKey}

AWS IoT 1-Click の条件キー

AWS IoT 1-Click では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします。	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられているタグに基づいてアクションをフィルタリングします。	文字列
aws:TagKeys	リクエストで渡されたタグキーに基づいてアクションをフィルタリングします。	ArrayOfString

AWS IoT Analytics のアクション、リソース、および条件キー

AWS IoT Analytics (サービスプレフィックス: `iotanalytics`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IoT Analytics で定義されるアクション
- AWS IoT Analytics で定義されるリソースタイプ
- AWS IoT Analytics の条件キー

AWS IoT Analytics で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchPutMessage	メッセージのバッチを指定されたチャネルに書き込みます	書き込み	channel*		
CancelPipelineReprocessing	指定されたパイプラインの再処理をキャンセルします	書き込み	pipeline*		
CreateChannel	チャネルを作成します	書き込み	channel*		
				aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
CreateDataset	データセットを作成します。	書き込み	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatasetContent	指定されたデータセットから (データセットアクションを実行して) コンテンツを生成します	書き込み	dataset*		
CreateDatastore	データストアを作成します	書き込み	datastore*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePipeline	パイプラインを作成します	書き込み	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteChannel	指定されたチャネルを削除します	書き込み	channel*		
DeleteDataset	指定されたデータセットを削除します	書き込み	dataset*		
DeleteDatasetContent	指定されたデータセットのコンテンツを削除します	書き込み	dataset*		
DeleteDatastore	指定されたデータストアを削除します	書き込み	datastore*		
DeletePipeline	指定されたパイプラインを削除します	書き込み	pipeline*		
DescribeChannel	指定されたチャネルの説明を表示します	読み込み	channel*		
DescribeDataset	指定されたデータセットの説明を表示します	読み込み	dataset*		
DescribeDatastore	指定されたデータストアの説明を表示します	読み込み	datastore*		
DescribeLoggingOptions	アカウントのログ記録オプションの説明を表示します	読み込み			
DescribePipeline	指定されたパイプラインの説明を表示します	読み込み	pipeline*		
GetDatasetContent	指定されたデータセットのコンテンツを取得します	読み込み	dataset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListChannels	アカウントのチャネルを一覧表示します	リスト			
ListDatasetContents	作成されたデータセットコンテンツの情報を一覧表示します	リスト	dataset*		
ListDatasets	アカウントのデータセットを一覧表示します	リスト			
ListDatastores	アカウントのデータストアを一覧表示します	リスト			
ListPipelines	アカウントのパイプラインを一覧表示します	リスト			
ListTagsForResource	リソースに割り当てられたタグ (メタデータ) を一覧表示します	読み込み	channel		
			dataset		
			datastore		
			pipeline		
PutLoggingOptions	アカウントのログ記録オプションを設定します	書き込み			
RunPipelineActivity	指定されたパイプラインのアクティビティを実行します	読み込み			
SampleChannelData	指定されたチャネルのデータをサンプリングします	読み込み	channel*		
StartPipelineReprocessing	指定されたパイプラインの再処理を開始します	書き込み	pipeline*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagResource	指定されたリソースのタグを追加または変更します。タグは、リソースを管理するために使用できるメタデータです	Tagging	channel		
			dataset		
			datastore		
			pipeline		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	指定されたタグ (メタデータ) をリソースから削除します	Tagging	channel		
			dataset		
			datastore		
			pipeline		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateChannel	指定されたチャネルを更新します	書き込み	channel*		
UpdateDataset	指定されたデータセットを更新します	書き込み	dataset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateDatastore	指定されたデータストアを更新します	書き込み	datastore*		
UpdatePipeline	指定されたパイプラインを更新します	書き込み	pipeline*		

AWS IoT Analytics で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
channel	`arn:${Partition}:iotanalytics:${Region}:${Account}:channel/${ChannelName}`	aws:RequestTag/${TagKey} aws:TagKeys iotanalytics:ResourceTag/${TagKey}
dataset	`arn:${Partition}:iotanalytics:${Region}:${Account}:dataset/${DatasetName}`	aws:RequestTag/${TagKey} aws:TagKeys iotanalytics:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
datastore	arn:${Partition}:iotanalytics:${Region}:${Account}:datastore/${DatastoreName}	aws:RequestTag/${TagKey} aws:TagKeys iotanalytics:ResourceTag/${TagKey}
pipeline	arn:${Partition}:iotanalytics:${Region}:${Account}:pipeline/${PipelineName}	aws:RequestTag/${TagKey} aws:TagKeys iotanalytics:ResourceTag/${TagKey}

AWS IoT Analytics の条件キー

AWS IoT Analytics では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいてアクセスをフィルタリングします	ArrayOfString
iotanalytics:Resou	リソースにアタッチされているタグのキーと値のペアでアクセスをフィルタリングします	String

条件キー	説明	タイプ
rceTag/${ TagKey}		

AWS IoT Core Device Advisor のアクション、リソース、および条件キー

AWS IoT Core Device Advisor (サービスプレフィックス: `iotdeviceadvisor`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IoT Core Device Advisor で定義されるアクション
- AWS IoT Core Device Advisor で定義されるリソースタイプ
- AWS IoT Core Device Advisor の条件キー

AWS IoT Core Device Advisor で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSuiteDefinition	スイート定義を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteSuiteDefinition	スイート定義を削除する許可を付与	書き込み	Suitedefinition*		
GetEndpoint	Device Advisor エンドポイントを取得するアクセス許可を付与	読み込み			
GetSuiteDefinition	スイートの定義を取得する許可を付与	読み込み	Suitedefinition*		
GetSuiteRun	スイートの実行を取得する許可を付与	読み込み	Suiterun*		
GetSuiteRunReport	スイート実行の資格レポートを取得する許可を付与	読み込み	Suiterun*		
ListSuiteDefinitions	スイート定義を一覧表示する許可を付与	リスト			
ListSuiteRuns	スイート実行を一覧表示する許可を付与	リスト	Suitedefinition*		
ListTagsForResource	リソースに割り当てられたタグ (メタデータ) を一覧表示する許可を付与	読み込み	Suitedefinition		
			Suiterun		
StartSuiteRun	スイート実行を開始する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StopSuiteRun	スイートの実行を停止するためのアクセス許可を付与します	書き込み	Suiterun*		
TagResource	指定されたリソースのタグに追加または変更する許可を付与。タグは、リソースを管理するために使用できるメタデータです	タグ付け	Suitedefinition		
			Suiterun		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	指定されたタグ (メタデータ) をリソースから削除する許可を付与	タグ付け	Suitedefinition		
			Suiterun		
				aws:TagKeys	
UpdateSuiteDefinition	スイート定義を更新する許可を付与	書き込み	Suitedefinition*		

AWS IoT Core Device Advisor で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Suitedefinition	arn:${Partition}:iotdeviceadvisor:${Region}:${Account}:suitedefinition/${SuiteDefinitionId}	aws:ResourceTag/${TagKey}
Suiterun	arn:${Partition}:iotdeviceadvisor:${Region}:${Account}:suiterun/${SuiteDefinitionId}/${SuiteRunId}	aws:ResourceTag/${TagKey}

AWS IoT Core Device Advisor の条件キー

AWS IoT Core Device Advisor では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS IoT Device Tester のアクション、リソース、および条件キー

AWS IoT Device Tester (サービスプレフィックス: iot-device-tester) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IoT Device Tester で定義されるアクション
- AWS IoT Device Tester で定義されるリソースタイプ
- AWS IoT Device Tester の条件キー

AWS IoT Device Tester で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CheckVersion	IoT Device Tester に、特定の製品セット、テストスイート、およびデバイステスターバージョンに互換性があるかどうかを確認する権限を付与する	読み取り			
DownloadTestSuite	互換性のあるテストスイートのバージョンをダウンロードする権限を IoT Device Tester に付与する	読み取り			
LatestIdt	使用可能なデバイステスターの最新バージョンに関する情報を取得する権限を IoT Device Tester に付与する	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SendMetrics	ユーザーに代わって使用状況メトリクスを送信する権限を IoT Device Tester に付与する	書き込み			
Supported Version	サポートされている製品とテストスイートのバージョンのリストを取得する権限を IoT Device Tester に付与する	読み取り			

AWS IoT Device Tester で定義されるリソースタイプ

AWS IoT Device Tester は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS IoT Device Tester へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS IoT Device Tester の条件キー

IoT Device Tester には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS IoT Events のアクション、リソース、および条件キー

AWS IoT Events (サービスプレフィックス: `iotevents`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IoT Events で定義されるアクション
- AWS IoT Events で定義されるリソースタイプ
- AWS IoT Events の条件キー

AWS IoT Events で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchAcknowledgeAlarm	1 つ以上の確認アクションリクエストを AWS IoT Events に送信するアクセス許可を付与します	書き込み	alarmModel*		
BatchDeleteDetector	AWS IoT Events システム内のディテクターインスタンスを削除するアクセス許可を付与します	書き込み	detectorModel*		
BatchDisableAlarm	1 つまたは複数のアラームインスタンスを無効にする許可を付与	Write	alarmModel*		
BatchEnableAlarm	1 つまたは複数のアラームインスタンスを有効にする許可を付与	書き込み	alarmModel*		
BatchPutMessage	AWS IoT Events システムに一連のメッセージを送信するアクセス許可を付与します	書き込み	input*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchResetAlarm	1 つまたは複数のアラームインスタンスをリセットする許可を付与	Write	alarmModel*		
BatchSnoozeAlarm	1 つまたは複数のアラームインスタンスをスヌーズモードに変更する許可を付与	書き込み	alarmModel*		
BatchUpdateDetector	AWS IoT Events システム内のディテクターインスタンスを更新する許可を付与	書き込み	detectorModel*		
CreateAlarmModel	IoT Events 入力属性または AWS IoT AWS IoT SiteWise アセットプロパティをモニタリングするアラームモデルを作成するアクセス許可を付与します	書き込み	alarmModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDetectorModel	AWS IoT Events 入力属性をモニタリングするディテクターモデルを作成する許可を付与	書き込み	detectorModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInput	IotEvents に Input を作成する許可を付与	Write	input*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlarmModel	アラームモデルを削除する許可を付与	Write	alarmModel*		
DeleteDetectorModel	検出器モデルを削除する許可を付与	Write	detectorModel*		
DeleteInput	入力を削除する許可を付与	Write	input*		
DescribeAlarm	アラームインスタンスについての情報を取得する許可を付与	Read	alarmModel*		
DescribeAlarmModel	アラームモデルについての情報を取得する許可を付与	Read	alarmModel*		
DescribeDetector	検出器インスタンスについての情報を取得する許可を付与	Read	detectorModel*		
DescribeDetectorModel	検出器モデルについての情報を取得する許可を付与	読み取り	detectorModel*		
DescribeDetectorModelAnalysis	検出器モデルについての情報を取得する許可を付与	読み取り			
DescribeInput	Input についての情報を取得する許可を付与	読み取り	input*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeLoggingOptions	AWS IoT Events ログ記録オプションの現在の設定を取得する許可を付与	読み取り			
GetDetectorModelAnalysisResults	ディテクターモデル分析結果を取得する許可を付与	読み取り			
ListAlarmModelVersions	アラームモデルのすべてのバージョンを一覧表示する許可を付与	リスト	alarmModel*		
ListAlarmModels	作成したアラームモデルを一覧表示する許可を付与	リスト			
ListAlarms	alarmModel ごとにすべてのアラームインスタンスについての情報を取得する許可を付与。	リスト	alarmModel*		
ListDetectorModelVersions	検出器モデルのすべてのバージョンを一覧表示する許可を付与	リスト	detectorModel*		
ListDetectorModels	作成した検出器モデルを一覧表示する許可を付与	リスト			
ListDetectors	検出器モデルごとにすべての検出器インスタンスについての情報を取得する許可を付与	リスト	detectorModel*		
ListInputRoutings	1 つまたは複数の入力ルーティングを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListInputs	作成した入力を一覧表示する許可を付与	リスト			
ListTagsForResource	リソースに割り当てたタグ (メタデータ) を一覧表示する許可を付与	読み取り	alarmModel		
			detectorModel		
			input		
PutLoggingOptions	AWS IoT Events ログ記録オプションを設定または更新する許可を付与	書き込み			
StartDetectorModelAnalysis	ディテクターモデル分析を開始する許可を付与	書き込み			
TagResource	指定のリソースのタグを追加または変更する許可を付与。タグは、リソースを管理するために使用できるメタデータです	タグ付け	alarmModel		
			detectorModel		
			input		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	指定のタグ (メタデータ) をリソースから削除する許可を付与	タグ付け	alarmModel		
			detectorModel		
			input		
				aws:TagKeys	
UpdateAlarmModel	アラームモデルを更新する許可を付与	Write	alarmModel*		
UpdateDetectorModel	検出器モデルを更新する許可を付与	Write	detectorModel*		
UpdateInput	入力を更新する許可を付与	Write	input*		
UpdateInputRouting	入力ルーティングを更新する許可を付与	Write	input*		

AWS IoT Events で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
detectorModel	arn:${Partition}:iotevents:${Region}:${Account}:detectorModel/${DetectorModelName}	aws:ResourceTag/${TagKey}
alarmModel	arn:${Partition}:iotevents:${Region}:${Account}:alarmModel/${AlarmModelName}	aws:ResourceTag/${TagKey}
input	arn:${Partition}:iotevents:${Region}:${Account}:input/${InputName}	aws:ResourceTag/${TagKey}

AWS IoT Events の条件キー

AWS IoT Events では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアによるアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエスト内のタグキーでアクションをフィルタリングします	ArrayOfString
iotevents:keyValue	メッセージの instanceId (キー値) でアクセスをフィルタリングします	文字列

AWS IoT Fleet Hub for Device Management のアクション、リソース、および条件キー

AWS IoT Fleet Hub for Device Management (サービスプレフィックス: `iotfleethub`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IoT Fleet Hub for Device Management で定義されるアクション
- AWS IoT Fleet Hub for Device Management で定義されるリソースタイプ
- AWS IoT Fleet Hub for Device Management の条件キー

AWS IoT Fleet Hub for Device Management で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateApplication	アプリケーションを作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	sso:CreateManagedApplicationInstance sso:DescribeRegisteredRegions
DeleteApplication	アプリケーションを削除する許可を付与	書き込み	application*		sso:DeleteManagedA

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					pplicatio nInstance
DescribeApplication	アプリケーションを記述する許可を付与	読み込み	application*		
ListApplications	すべてのアプリケーションを一覧表示する許可を付与	リスト			
ListTagsForResource	リソースのすべてのタグを一覧表示する許可を付与	読み込み	application		
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	application		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	リソースのタグを解除する許可を付与	タグ付け	application		
				aws:TagKeys	
UpdateApplication	アプリケーションを更新する許可を付与	書き込み	application*		

AWS IoT Fleet Hub for Device Management で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアク

ションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
application	`arn:${Partition}:iotfleethub:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}

AWS IoT Fleet Hub for Device Management の条件キー

AWS IoT Fleet Hub for Device Management では、IAM ポリシーの `Condition`要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアによるアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエスト内のタグキーでアクションをフィルタリングします	ArrayOfString

AWS IoT FleetWise のアクション、リソース、および条件キー

AWS IoT FleetWise (サービスプレフィックス: `iotfleetwise`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IoT FleetWiseで定義されるアクション
- AWS IoT FleetWiseで定義されるリソースタイプ
- AWS IoT FleetWiseの条件キー

AWS IoT FleetWiseで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateVehicleFleet	指定された車両をフリートに関連付けるアクセス許可を付与	書き込み	fleet*		
			vehicle*		
CreateCampaign	キャンペーンを作成する許可を付与	書き込み	campaign*		
			fleet*		
			signalcatalog*		
			vehicle*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys iotfleetwise:DestinationArn	
CreateDecoderManifest	既存のモデルのデコーダーマニフェストを作成するアクセス許可を付与	書き込み	decodermanifest*		
			modelmanifest*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFleet	フリートを作成する許可を付与	書き込み	fleet*		
			signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateModelManifest	モデルマニフェストの定義を作成する許可を付与	書き込み	modelmanifest*		
			signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSignalCatalog	シグナルカタログを作成する許可を付与	書き込み	signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStateTemplate	状態テンプレートを作成するアクセス許可を付与します	書き込み	signalcatalog*		
			statetemplate*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateVehicle	車両を作成するアクセス許可を付与	書き込み	decodermanifest*		iot:CreateThing iot:DescribeThing
			modelmanifest*		
			vehicle*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCampaign	キャンペーンを削除する許可を付与	書き込み	campaign*		
DeleteDecoderManifest	指定されたデコーダマニフェストを削除するアクセス許可を付与	書き込み	decodermanifest*		
DeleteFleet	フリートを削除するアクセス許可を付与	書き込み	fleet*		
DeleteModelManifest	指定されたモデルマニフェストを削除するアクセス許可を付与	書き込み	modelmanifest*		
DeleteSignalCatalog	特定の信号カタログを削除するアクセス許可を付与	書き込み	signalcatalog*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteStateTemplate	状態テンプレートを削除するアクセス許可を付与します	書き込み	statetemplate*		
DeleteVehicle	車両を削除するアクセス許可を付与	書き込み	vehicle*		
DisassociateVehicleFleet	既存のフリートから車両の関連付けを解除するアクセス許可を付与	書き込み	fleet*		
			vehicle*		
GenerateCommandPayload [アクセス許可のみ]	車両でコマンドを実行するためのペイロードを生成するアクセス許可を付与します	権限の管理	vehicle*		
			statetemplate		
				iotfleetwise:Signals	
GetCampaign	特定のキャンペーンの概要情報を取得するアクセス許可を付与	読み取り	campaign*		
GetDecoderManifest	特定のデコーダマニフェスト定義の概要情報を取得するアクセス許可を付与	読み取り	decodermanifest*		
GetEncryptionConfiguration	の KMS ベースの暗号化ステータスを取得する許可を付与 AWS アカウント	読み取り			
GetFleet	フリートの概要情報を取得する許可を付与	読み取り	fleet*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetLoggingOptions	のログ記録オプションを取得するアクセス許可を付与します AWS アカウント	読み取り			
GetModelManifest	特定のモデルマニフェスト定義の概要情報を取得するアクセス許可を付与	読み取り	modelmanifest*		
GetRegisterAccountStatus	IoT FleetWise でアカウント登録ステータスを取得するためのアクセス許可を付与	読み取り			
GetSignalCatalog	特定のシグナルカタログの概要情報を取得するアクセス許可を付与	読み取り	signalcatalog*		
GetStateTemplate	特定の状態テンプレートの概要情報を取得するアクセス許可を付与します	読み取り	statetemplate*		
GetVehicle	車両の概要情報を取得する許可を付与	読み取り	vehicle*		
GetVehicleStatus	特定の車両で実行されているキャンペーンのステータスを取得する許可を付与	読み取り	vehicle*		
ImportDecoderManifest	既存のデコーダーマニフェストをインポートするためのアクセス許可を付与	書き込み	decodermanifest*		
ImportSignalCatalog	既存の定義をインポートして、シグナルカタログを作成するアクセス許可を付与	書き込み	signalcatalog*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
ListCampaigns	キャンペーンを一覧表示する許可を付与	読み取り			
ListDecoderManifestNetworkInterfaces	既存のデコーダーマニフェストに関連付けられたネットワークインターフェイスを一覧表示するアクセス許可を付与	リスト	decodermanifest*		
ListDecoderManifestSignals	デコーダマニフェストシグナルを一覧表示するアクセス許可を付与	リスト	decodermanifest*		
ListDecoderManifests	モデルマニフェストのオプションのフィルタを使用して、すべてのデコーダーマニフェストを一覧表示するアクセス許可を付与	読み取り			
ListFleets	すべてのフリートを一覧表示するアクセス許可を付与	読み取り			
ListFleetsForVehicle	指定された車両が関連付けられているすべてのフリートを一覧表示する許可を付与	読み取り	vehicle*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListModelManifestNodes	指定されたモデルマニフェストのすべてのノードを一覧表示するアクセス許可を付与	リスト	modelmanifest*		
ListModelManifests	シグナルカタログにオプションのフィルタを使用して、すべてのモデルマニフェストを一覧表示するアクセス許可を付与	読み取り			
ListSignalCatalogNodes	指定されたシグナルカタログのすべてのノードを一覧表示するアクセス許可を付与	読み取り	signalcatalog*		
ListSignalCatalogs	すべてのシグナルカタログを一覧表示するアクセス許可を付与	読み取り			
ListStateTemplates	状態テンプレートを一覧表示するアクセス許可を付与します	読み取り			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	campaign		
			decodermanifest		
			fleet		
			modelmanifest		
			signalcatalog		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			statetemplate		
			vehicle		
ListVehicles	モデルマニフェストのオプションのフィルタを使用して、すべての車両をリストするアクセス許可を付与	読み取り			
ListVehiclesInFleet	指定されたフリート内の車両を一覧表示する許可を付与	読み取り	fleet*		
PutEncryptionConfiguration	の KMS ベースの暗号化を有効または無効にするアクセス許可を付与します AWS アカウント	書き込み			
PutLoggingOptions	のログ記録オプションを配置するアクセス許可を付与します AWS アカウント	書き込み			
RegisterAccount	IoT FleetWise AWS アカウント に を登録するアクセス許可を付与します	書き込み			iam:PassRole
TagResource	リソースにタグを追加するアクセス許可を付与します	タグ付け	campaign		
			decodermanifest		
			fleet		
			modelmanifest		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			signalcatalog		
			statetemplate		
			vehicle		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	Tagging	campaign		
			decodermanifest		
			fleet		
			modelmanifest		
			signalcatalog		
			statetemplate		
			vehicle		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateCampaign	指定されたキャンペーンを更新する許可を付与	書き込み	campaign*		
UpdateDecoderManifest	デコーダマニフェスト定義を更新するアクセス許可を付与	書き込み	decodermanifest*		
UpdateFleet	フリートを更新する許可を付与	書き込み	fleet*		
UpdateModelManifest	指定されたモデルマニフェスト定義を更新するアクセス許可を付与	書き込み	modelmanifest*		
UpdateSignalCatalog	特定のシグナルカタログ定義を更新するアクセス許可を付与	書き込み	signalcatalog*		
UpdateStateTemplate	指定された状態テンプレートを更新するアクセス許可を付与します	書き込み	statetemplate*		
UpdateVehicle	車両を更新する許可を付与	書き込み	vehicle*		
			decodermanifest		
			modelmanifest		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				iotfleetwise:UpdateToModelManifestArn iotfleetwise:UpdateToDecoderManifestArn	

AWS IoT FleetWiseで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
campaign	arn:${Partition}:iotfleetwise:${Region}:${Account}:campaign/${CampaignName}	aws:ResourceTag/${TagKey}
decodermanifest	arn:${Partition}:iotfleetwise:${Region}:${Account}:decoder-manifest/${Name}	aws:ResourceTag/${TagKey}
fleet	arn:${Partition}:iotfleetwise:${Region}:${Account}:fleet/${FleetId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
modelmanifest	arn:${Partition}:iotfleetwise:${Region}:${Account}:model-manifest/${Name}	aws:ResourceTag/${TagKey}
signalcatalog	arn:${Partition}:iotfleetwise:${Region}:${Account}:signal-catalog/${Name}	aws:ResourceTag/${TagKey}
vehicle	arn:${Partition}:iotfleetwise:${Region}:${Account}:vehicle/${VehicleId}	aws:ResourceTag/${TagKey}
statetemplate	arn:${Partition}:iotfleetwise:${Region}:${Account}:state-template/${StateTemplateId}	aws:ResourceTag/${TagKey}

AWS IoT FleetWiseの条件キー

AWS IoT FleetWise では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

条件キー	説明	[Type] (タイプ)
iotfleetwise:DestinationArn	キャンペーンの宛先 ARN でアクセスをフィルタリング (例: S3 バケット ARN または Timestream ARN)	ARN
iotfleetwise:Signals	完全修飾シグナル名でアクセスをフィルタリングします	ArrayOfString
iotfleetwise:UpdateToDecoderManifestArn	IoT FleetWise デコーダマニフェスト ARN のリストによってアクセスをフィルタリングします。	ARN
iotfleetwise:UpdateToModelManifestArn	IoT FleetWise モデルマニフェスト ARN のリストによってアクセスをフィルタリングします。	ARN

AWS IoT Greengrass のアクション、リソース、および条件キー

AWS IoT Greengrass (サービスプレフィックス: `greengrass`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IoT Greengrass で定義されるアクション
- AWS IoT Greengrass で定義されるリソースタイプ
- AWS IoT Greengrass の条件キー

AWS IoT Greengrass で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateRoleToGroup	ロールをグループに関連付けるアクセス許可を付与 ロールのアクセス許可は、Greengrass コア Lambda 関数とコネクタが他の AWS サービスでアクションを実行することを許可する必要があります	書き込み	group*		
AssociateServiceRoleToAccount	ロールをアカウントに関連付けるアクセス許可を付与します。 AWS IoT Greengrass はこのロールを使用して Lambda 関数と AWS IoT リソースにアクセスします	権限の管理			
CreateConnectorDefinition	コネクタ定義を作成する許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectorDefinitionVersion	既存のコネクタ定義のバージョンを作成する許可を付与	Write	connectorDefinition*		
CreateCoreDefinition	コア定義を作成する許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateCoreDefinitionVersion	既存のコア定義のバージョンを作成する許可を付与。Greengrass グループには、それぞれ 1 つの Greengrass コアが含まれている必要があります。	Write	coreDefinition*		
CreateDeployment	デプロイを作成する許可を付与	Write	group*		
CreateDeviceDefinition	デバイス定義を作成する許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceDefinitionVersion	既存のデイバス定義のバージョンを作成する許可を付与	Write	deviceDefinition*		
CreateFunctionDefinition	Lambda 関数とその設定のリストを含むグループで使用される Lambda 関数定義を作成する許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunctionDefinitionVersion	既存の Lambda 関数定義のバージョンを作成する許可を付与	書き込み	functionDefinition*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateGroup	グループを作成するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGroupCertificateAuthority	グループの CA を作成、または既存の CA をローテーションする許可を付与	Write	group*		
CreateGroupVersion	すでに定義されているグループのバージョンを作成する許可を付与	Write	group*		
CreateLoggerDefinition	ロガー定義を作成する許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLoggerDefinitionVersion	既存のロガー定義のバージョンを作成する許可を付与	Write	loggerDefinition*		
CreateResourceDefinition	グループ内で使用されるリソースのリストを含むリソース定義を作成する許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateResourceDefinitionVersion	既存のリソース定義のバージョンを作成する許可を付与	書き込み	resourceDefinition*		
CreateSoftwareUpdateJob	Greengrass コアをトリガーして実行中のソフトウェアを更新する AWS IoT ジョブを作成するアクセス許可を付与します	書き込み			
CreateSubscriptionDefinition	サブスクリプション定義を作成する許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscriptionDefinitionVersion	既存のサブスクリプション定義のバージョンを作成する許可を付与	Write	subscriptionDefinition*		
DeleteConnectorDefinition	コネクタ定義を削除する許可を付与	Write	connectorDefinition*		
DeleteCoreDefinition	コア定義を削除する許可を付与。デプロイで現在使用されている定義を削除すると、今後のデプロイに影響します	Write	coreDefinition*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteDeviceDefinition	デバイス定義を削除する許可を付与。デプロイで現在使用されている定義を削除すると、今後のデプロイに影響します	Write	deviceDefinition*		
DeleteFunctionDefinition	Lambda 関数定義を削除する許可を付与。デプロイで現在使用されている定義を削除すると、今後のデプロイに影響します	Write	functionDefinition*		
DeleteGroup	デプロイで現在使用されていないグループを削除する許可を付与	Write	group*		
DeleteLoggerDefinition	ロガー定義を削除する許可を付与。デプロイで現在使用されている定義を削除すると、今後のデプロイに影響します	Write	loggerDefinition*		
DeleteResourceDefinition	リソース定義を削除する許可を付与	Write	resourceDefinition*		
DeleteSubscriptionDefinition	サブスクリプション定義を削除する許可を付与。デプロイで現在使用されている定義を削除すると、今後のデプロイに影響します	Write	subscriptionDefinition*		
DisassociateRoleFromGroup	ロールのグループへの関連付けを解除する許可を付与	Write	group*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DisassociateServiceRoleFromAccount	アカウントからサービスロールの関連付けを解除する許可を付与。サービスロールがない場合、デプロイは動作しません。	Write			
Discover	Greengrass コアに接続するために必要な情報を取得する許可を付与	Read	thing*		
GetAssociatedRole	グループに関連付けられているロールを取得する許可を付与	Read	group*		
GetBulkDeploymentStatus	一括デプロイのステータスを返すアクセス許可を付与	Read	bulkDeployment*		
GetConnectivityInfo	コアの接続情報を取得する許可を付与	Read	connectivityInfo*		
GetConnectorDefinition	コネクタ定義に関する情報を取得する許可を付与	Read	connectorDefinition*		
GetConnectorDefinitionVersion	コネクタ定義バージョンに関する情報を取得する許可を付与	Read	connectorDefinition*		
			connectorDefinitionVersion*		
GetCoreDefinition	コア定義に関する情報を取得する許可を付与	Read	coreDefinition*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetCoreDefinitionVersion	コア定義バージョンに関する情報を取得する許可を付与	Read	coreDefinition*		
			coreDefinitionVersion*		
GetDeploymentStatus	デプロイのステータスを返すアクセス許可を付与	Read	deployment*		
			group*		
GetDeviceDefinition	デバイス定義に関する情報を取得する許可を付与	Read	deviceDefinition*		
GetDeviceDefinitionVersion	デバイス定義バージョンに関する情報を取得する許可を付与	Read	deviceDefinition*		
			deviceDefinitionVersion*		
GetFunctionDefinition	Lambda 関数定義に関する情報 (作成時刻や最新バージョンなど) を取得する許可を付与	Read	functionDefinition*		
GetFunctionDefinitionVersion	バージョンに含まれる Lambda 関数やその設定など、Lambda 関数定義バージョンに関する情報を取得する許可を付与	Read	functionDefinition*		
			functionDefinitionVersion*		
GetGroup	グループに関する情報を取得する許可を付与	Read	group*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetGroupCertificateAuthority	グループに関連付けられた CA のパブリックキーを返すアクセス許可を付与	Read	certificateAuthority*		
			group*		
GetGroupCertificateConfiguration	グループが使用する CA の設定を取得する許可を付与	Read	group*		
GetGroupVersion	グループのバージョンに関する情報を取得する許可を付与	Read	group*		
			groupVersion*		
GetLoggerDefinition	ロガー定義に関する情報を取得する許可を付与	Read	loggerDefinition*		
GetLoggerDefinitionVersion	ロガー定義バージョンに関する情報を取得する許可を付与	Read	loggerDefinition*		
			loggerDefinitionVersion*		
GetResourceDefinition	リソース定義に関する情報 (作成時刻や最新バージョンなど) を取得する許可を付与	Read	resourceDefinition*		
GetResourceDefinitionVersion	バージョンに含まれるリソースなど、リソース定義バージョンに関する情報を取得する許可を付与	Read	resourceDefinition*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			resourceDefinitionVersion*		
GetServiceRoleForAccount	アカウントにアタッチされているサービスのロールを取得する許可を付与	Read			
GetSubscriptionDefinition	サブスクリプション定義に関する情報を取得する許可を付与	Read	subscriptionDefinition*		
GetSubscriptionDefinitionVersion	サブスクリプション定義バージョンに関する情報を取得する許可を付与	Read	subscriptionDefinition*		
			subscriptionDefinitionVersion*		
GetThingRuntimeConfiguration	モノのランタイム設定を取得する許可を付与	Read	thingRuntimeConfig*		
ListBulkDeploymentDetailedReports	一括デプロイオペレーションで開始されたデプロイとそれらの現在のデプロイステータスのページ分割リストを取得する許可を付与	Read	bulkDeployment*		
ListBulkDeployments	一括デプロイのリストを取得する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListConnectorDefinitionVersions	コネクタ定義のバージョンを一覧表示する許可を付与	リスト	connectorDefinition*		
ListConnectorDefinitions	コネクタ定義のリストを取得する許可を付与	リスト			
ListCoreDefinitionVersions	コア定義のバージョンを一覧表示する許可を付与	リスト	coreDefinition*		
ListCoreDefinitions	コア定義のリストを取得する許可を付与	リスト			
ListDeployments	グループのすべてのデプロイのリストを取得する許可を付与	リスト	group*		
ListDeviceDefinitionVersions	デバイス定義のバージョンを一覧表示する許可を付与	リスト	deviceDefinition*		
ListDeviceDefinitions	デバイス定義のリストを取得する許可を付与	リスト			
ListFunctionDefinitionVersions	Lambda 関数定義のバージョンを一覧表示する許可を付与	リスト	functionDefinition*		
ListFunctionDefinitions	Lambda 関数定義のリストを取得する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListGroupCertificateAuthorities	グループの現在の CA のリストを取得する許可を付与	リスト	group*		
ListGroupVersions	グループのバージョンを一覧表示する許可を付与	リスト	group*		
ListGroups	グループのリストを取得する許可を付与	リスト			
ListLoggerDefinitionVersions	ロガー定義のバージョンを一覧表示する許可を付与	リスト	loggerDefinition*		
ListLoggerDefinitions	ロガー定義のリストを取得する許可を付与	リスト			
ListResourceDefinitionVersions	リソース定義のバージョンを一覧表示する許可を付与	リスト	resourceDefinition*		
ListResourceDefinitions	リソース定義のリストを取得する許可を付与	リスト			
ListSubscriptionDefinitionVersions	サブスクリプション定義のバージョンを一覧表示する許可を付与	リスト	subscriptionDefinition*		
ListSubscriptionDefinitions	サブスクリプション定義のリストを取得する許可を付与	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	Read	bulkDeployment		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			connectorDefinition		
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		
			resourceDefinition		
			subscriptionDefinition		
				aws:RequestTag/${TagKey} aws:TagKeys	
ResetDeployments	グループのデプロイをリセットする許可を付与	Write	group*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartBulkDeployment	1 回のオペレーションで複数のグループをデプロイする許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys	
StopBulkDeployment	一括デプロイの実行を停止する許可を付与	Write	bulkDeployment*		
TagResource	リソースにタグを追加するアクセス許可を付与します	タグ付け	bulkDeployment		
			connectorDefinition		
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		
			resourceDefinition		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			subscriptionDefinition		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	タグ付け	bulkDeployment		
			connectorDefinition		
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		
			resourceDefinition		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			subscriptionDefinition		
				aws:TagKeys	
UpdateConnectivityInfo	Greengrass コアの接続情報を更新する許可を付与。このコアを持つグループに属するすべてのデバイスは、コアの場所を見つけてそれに接続するためにこの情報を受け取ります。	Write	connectivityInfo*		
UpdateConnectorDefinition	コネクタ定義を更新する許可を付与	Write	connectorDefinition*		
UpdateCoreDefinition	コア定義を更新する許可を付与	Write	coreDefinition*		
UpdateDeviceDefinition	デバイス定義を更新する許可を付与	Write	deviceDefinition*		
UpdateFunctionDefinition	Lambda 関数定義を更新する許可を付与	Write	functionDefinition*		
UpdateGroup	グループを更新する許可を付与	Write	group*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateGroupCertificateConfiguration	グループの証明書の有効期限を更新する許可を付与	Write	group*		
UpdateLoggerDefinition	ロガー定義を更新する許可を付与	Write	loggerDefinition*		
UpdateResourceDefinition	リソース定義を更新する許可を付与	Write	resourceDefinition*		
UpdateSubscriptionDefinition	サブスクリプション定義を更新する許可を付与	Write	subscriptionDefinition*		
UpdateThingRuntimeConfiguration	モノのランタイム設定を更新する許可を付与	Write	thingRuntimeConfig*		

AWS IoT Greengrass で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
connectivityInfo	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/things/${ThingName}/connectivityInfo	
certificateAuthority	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/certificateauthorities/${CertificateAuthorityId}	
deployment	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/deployments/${DeploymentId}	
bulkDeployment	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/bulk/deployments/${BulkDeploymentId}	aws:ResourceTag/${TagKey}
group	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}	aws:ResourceTag/${TagKey}
groupVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/versions/${VersionId}	
coreDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/cores/${CoreDefinitionId}	aws:ResourceTag/${TagKey}
coreDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/cores/${CoreDefinitionId}/versions/${VersionId}	

リソースタイプ	ARN	条件キー
deviceDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/devices/${DeviceDefinitionId}	aws:ResourceTag/${TagKey}
deviceDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/devices/${DeviceDefinitionId}/versions/${VersionId}	
functionDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/functions/${FunctionDefinitionId}	aws:ResourceTag/${TagKey}
functionDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/functions/${FunctionDefinitionId}/versions/${VersionId}	
subscriptionDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/subscriptions/${SubscriptionDefinitionId}	aws:ResourceTag/${TagKey}
subscriptionDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/subscriptions/${SubscriptionDefinitionId}/versions/${VersionId}	
loggerDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/loggers/${LoggerDefinitionId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
loggerDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/loggers/${LoggerDefinitionId}/versions/${VersionId}	
resourceDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/resources/${ResourceDefinitionId}	aws:ResourceTag/${TagKey}
resourceDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/resources/${ResourceDefinitionId}/versions/${VersionId}	
connectorDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/connectors/${ConnectorDefinitionId}	aws:ResourceTag/${TagKey}
connectorDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/connectors/${ConnectorDefinitionId}/versions/${VersionId}	
thing	arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}	
thingRuntimeConfig	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/things/${ThingName}/runtimeconfig	

AWS IoT Greengrass の条件キー

AWS IoT Greengrass では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	各必須タグの許可された値のセットでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値に基づいて、アクセスをフィルタリングする	String
aws:TagKeys	リクエスト内の必須タグの存在でアクセスをフィルタリングします	ArrayOfString

AWS IoT Greengrass V2 のアクション、リソース、および条件キー

AWS IoT Greengrass V2 (サービスプレフィックス: `greengrass`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IoT Greengrass V2 で定義されるアクション
- AWS IoT Greengrass V2 で定義されるリソースタイプ
- AWS IoT Greengrass V2 の条件キー

AWS IoT Greengrass V2 で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateServiceRoleToAccount	ロールをアカウントに関連付けるアクセス許可を付与します。 AWS IoT Greengrass はこのロールを使用して Lambda 関数と AWS IoT リソースにアクセスします	権限の管理			iam:PassRole
BatchAssociateClientDeviceWithCoreDevice	クライアントデバイスのリストをコアデバイスに関連付けるアクセス許可を付与します。	書き込み	coreDevice*		
BatchDisassociateClientDeviceFromCoreDevice	コアデバイスからクライアントデバイスのリストの関連付けを解除するアクセス許可を付与します。	書き込み	coreDevice*		
CancelDeployment	デプロイをキャンセルする許可を付与	書き込み	deployment*		iot:CancelJob iot:DeleteThingShadow iot:DescribeJob iot:DescribeThing

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					iot:DescribeThingGroup iot:GetThingShadow iot:UpdateJob iot:UpdateThingShadow
CreateComponentVersion	コンポーネントを作成する許可を付与	書き込み	component *		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateDeployment	デプロイを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	iot:CancelJob iot:CreateJob iot:DeleteThingShadow iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow iot:UpdateJob iot:UpdateThingShadow
DeleteComponent	コンポーネントを削除する許可を付与	書き込み	componentVersion*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteCoreDevice	AWS IoT モノである AWS IoT Greengrass コアデバイスを削除するアクセス許可を付与します。この操作は、コアデバイスのリストからコアデバイスを削除します。このオペレーションでは、 AWS IoT モノは削除されません。	書き込み	coreDevice*		iot:DescribeJobExecution
DeleteDeployment	デプロイを削除するアクセス許可を付与。アクティブなデプロイを削除する前にキャンセルする必要があります	書き込み	deployment*		iot:DeleteJob
DescribeComponent	コンポーネントのバージョンのメタデータを取得する許可を付与	読み込み	componentVersion*		
DisassociateServiceRoleFromAccount	アカウントからサービスロールの関連付けを解除する許可を付与。サービスロールがない場合、デプロイは動作しません。	書き込み			
GetComponent	コンポーネントのバージョンの recipe を取得する許可を付与	読み込み	componentVersion*		
GetComponentVersionArtifact	パブリックコンポーネントアーティファクトをダウンロードするための署名付き URL を取得する許可を付与	読み込み	componentVersion*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetConnectivityInfo	Greengrass コアデバイスの接続情報を取得する許可を付与	読み取り	connectivityInfo*		iot:GetThingShadow
GetCoreDevice	AWS IoT Greengrass コアデバイスのメタデータを取得するアクセス許可を付与します	読み取り	coreDevice*		
GetDeployment	デプロイを取得する許可を付与	読み込み	deployment*		iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow
GetServiceRoleForAccount	アカウントにアタッチされているサービスのロールを取得する許可を付与	読み取り			
ListClientDevicesAssociatedWithCoreDevice	AWS IoT Greengrass コアデバイスに関連付けられたクライアントデバイスのページ分割されたリストを取得するアクセス許可を付与します	リスト	coreDevice*		
ListComponentVersions	コンポーネントのすべてのバージョンのページ分割されたリストを取得する許可を付与	リスト	component*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListComponents	コンポーネント概要のページ分割されたリストを取得する許可を付与	リスト			
ListCoreDevices	AWS IoT Greengrass コアデバイスのページ分割されたリストを取得する許可を付与	リスト			
ListDeployments	デプロイのページ分割されたリストを取得する許可を付与	リスト			iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListEffectiveDeployments	IoT Greengrass が AWS IoT AWS IoT Greengrass コアデバイスに送信するデプロイジョブのページ分割されたリストを取得するアクセス許可を付与します	リスト	coreDevice*		iot:DescribeJob iot:DescribeJobExecution iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow
ListInstalledComponents	AWS IoT Greengrass コアデバイスが実行するコンポーネントのページ分割されたリストを取得するアクセス許可を付与します	リスト	coreDevice*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み込み	component		
			componentVersion		
			coreDevice		
			deployment		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
ResolveComponentCandidates	デプロイのコンポーネント、バージョン、およびプラットフォームの要件を満たすコンポーネントを一覧表示する許可を付与	リスト	componentVersion*		
TagResource	リソースにタグを追加する許可を付与	タグ付け	component		
			componentVersion		
			coreDevice		
			deployment		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	タグ付け	component		
			componentVersion		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			coreDevice		
			deployment		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateConnectivityInfo	Greengrass コアの接続情報を更新する許可を付与。このコアを持つグループに属するすべてのデバイスは、コアの場所を見つけてそれに接続するためにこの情報を受け取ります。	書き込み	connectivityInfo*		iot:GetThingShadow iot:UpdateThingShadow

AWS IoT Greengrass V2 で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
connectivityInfo	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/things/${ThingName}/connectivityInfo	
component	arn:${Partition}:greengrass:${Region}:${Account}:components:${ComponentName}	aws:ResourceTag/${TagKey}
componentVersion	arn:${Partition}:greengrass:${Region}:${Account}:components:${ComponentName}:versions:${ComponentVersion}	aws:ResourceTag/${TagKey}
coreDevice	arn:${Partition}:greengrass:${Region}:${Account}:coreDevices:${CoreDeviceThingName}	aws:ResourceTag/${TagKey}
deployment	arn:${Partition}:greengrass:${Region}:${Account}:deployments:${DeploymentId}	aws:ResourceTag/${TagKey}

AWS IoT Greengrass V2 の条件キー

AWS IoT Greengrass V2 では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーおよび値のペアによってアクセスをフィルタリングします。	String

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	特定のリソースに関連付けられているタグのキーおよび値のペアをチェックして、アクセスをフィルタリングします。	String
aws:TagKeys	リクエストで渡されたタグキーをチェックして、アクセスをフィルタリングします。	ArrayOfString

AWS IoT Jobs DataPlane のアクション、リソース、および条件キー

AWS IoT Jobs DataPlane (サービスプレフィックス: `iotjobsdata`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IoT Jobs DataPlane で定義されるアクション
- AWS IoT Jobs DataPlane で定義されるリソースタイプ
- AWS IoT Jobs DataPlane の条件キー

AWS IoT Jobs DataPlane で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeJobExecution	ジョブ実行を記述する許可を付与	読み込み	thing*		
				iot:JobId	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetPendingJobExecutions	終端状態にないモノのすべてのジョブのリストを取得する許可を付与	読み込み	thing*		
StartNextPendingJobExecution	モノに対して保留中の次のジョブ実行を取得および開始する許可を付与	書き込み	thing*		
UpdateJobExecution	ジョブ実行を更新する許可を付与	書き込み	thing*		
				iot:JobId	

AWS IoT Jobs DataPlane で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
thing	`arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}`	

AWS IoT Jobs DataPlane の条件キー

AWS IoT Jobs DataPlane では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
iot:JobId	iotjobsdata:DescribeJobExecution API および iotjobsdata:UpdateJobExecution API の jobId でアクセスをフィルタリングします	String

AWS IoT Managed Integrations のアクション、リソース、および条件キー

AWS IoT Managed Integrations (サービスプレフィックス: `iotmanagedintegrations`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IoT Managed Integrations で定義されるアクション
- AWS IoT Managed Integrations で定義されるリソースタイプ
- AWS IoT マネージド統合の条件キー

AWS IoT Managed Integrations で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateAccountAssociation	新しいアカウントの関連付けを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:TagKeys iotmanagedintegrations:connectorDestinationId	
CreateCloudConnector	新しいクラウドコネクタを作成するアクセス許可を付与します	書き込み			
CreateConnectorDestination	新しいコネクタ送信先を作成するアクセス許可を付与します	書き込み		iotmanagedintegrations:cloudConnectorId	
CreateCredentialLocker	製品認証情報ロッカーを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDestination	新しい送信先を作成するアクセス許可を付与します	書き込み			
CreateEventLogConfiguration	新しいイベント設定を作成するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateManagedThing	新しいマネージドモノを作成するアクセス許可を付与します	書き込み	credential-locker		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNotification Configuration	新しい通知設定を作成するアクセス許可を付与します	書き込み			
CreateOtaTask	新しい ota タスクを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOtaTaskConfiguration	新しい ota タスク設定を作成するアクセス許可を付与します	書き込み			
CreateProvisioningProfile	新しいプロビジョニングプロファイルを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteAccountAssociation	アカウントの関連付けを削除するアクセス許可を付与します	書き込み	account-association*		
DeleteCloudConnector	クラウドコネクタを削除する許可を付与	書き込み		iotmanagedintegrations:cloudConnectorId	
DeleteConnectorDestination	コネクタの送信先を削除するアクセス許可を付与します	書き込み			
DeleteCredentialLocker	認証情報ロッカーを削除するアクセス許可を付与します	書き込み	credential-locker*		
DeleteDestination	送信先を削除するアクセス許可を付与します	書き込み			
DeleteEventLogConfiguration	イベントログ設定を削除するアクセス許可を付与します	書き込み			
DeleteManagedThing	マネージドモノを削除するアクセス許可を付与します	書き込み	managed-thing*		
DeleteNotificationConfiguration	通知設定を削除するアクセス許可を付与します	書き込み			
DeleteOtaTask	ota タスクを削除するアクセス許可を付与します	書き込み	ota-task*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteOtaTaskConfiguration	ota タスク設定を削除するアクセス許可を付与します	書き込み			
DeleteProvisioningProfile	プロビジョニングプロファイルを削除するアクセス許可を付与します	書き込み	provisioning-profile*		
DeregisterAccountAssociation	アカウントの関連付けを登録解除するアクセス許可を付与します	書き込み	account-association*		
			managed-thing*		
GetAccountAssociation	アカウントの関連付けに関する情報を取得するアクセス許可を付与します	読み取り	account-association*		
GetCloudConnector	クラウドコネクタに関する情報を取得する許可を付与	読み取り			
GetConnectorDestination	クラウド送信先に関する情報を取得するアクセス許可を付与します	読み取り			
GetCredentialLocker	認証情報ロッカーに関する情報を取得するアクセス許可を付与します	読み取り	credential-locker*		
GetCustomEndpoint	カスタムエンドポイントに関する情報を取得するアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetDefaultEncryptionConfiguration	デフォルトの暗号化設定に関する情報を取得するアクセス許可を付与します	読み取り			
GetDestination	送信先に関する情報を取得するアクセス許可を付与します	読み取り			
GetDeviceDiscovery	デバイス検出に関する情報を取得するアクセス許可を付与します	読み取り			
GetEventLogConfiguration	イベントログ設定に関する情報を取得するアクセス許可を付与します	読み取り			
GetHubConfiguration	ハブ設定に関する情報を取得するアクセス許可を付与します	読み取り			
GetManagedThing	マネージドモノに関する情報を取得するアクセス許可を付与します	読み取り	managed-thing*		
GetManagedThingCapabilities	マネージドモノの機能レポートを取得する許可を付与	読み取り	managed-thing*		
GetManagedThingConnectivityData	マネージドモノの接続データを取得する許可を付与	読み取り	managed-thing*		
GetManagedThingMetaData	マネージドモノのメタデータ情報を取得する許可を付与	読み取り	managed-thing*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetManagedThingState	マネージドモノのデバイス状態情報を取得する許可を付与	読み取り	managed-thing*		
GetNotificationConfiguration	通知設定の情報を取得するアクセス許可を付与します	読み取り			
GetOtaTask	ota タスクの情報を取得するアクセス許可を付与します	読み取り	ota-task*		
GetOtaTaskConfiguration	ota タスク設定の情報を取得するアクセス許可を付与します	読み取り			
GetProvisioningProfile	プロビジョニングプロファイルの情報を取得するアクセス許可を付与します	読み取り	provisioning-profile*		
GetRuntimeLogConfiguration	ランタイムログ設定の情報を取得するアクセス許可を付与します	読み取り			
GetSchemaVersion	スキーマのバージョンに関する情報を取得するアクセス許可を付与します	読み取り			
ListAccountAssociations	アカウント関連付けの情報を一覧表示するアクセス許可を付与します	リスト			
ListCloudConnectors	クラウドコネクタの情報を一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListConnectorDestinations	コネクタの送信先の情報を一覧表示するアクセス許可を付与します	リスト			
ListCredentialLockers	認証情報ロッカーの情報を一覧表示するアクセス許可を付与します	リスト			
ListDestinations	送信先の情報を一覧表示するアクセス許可を付与します	リスト			
ListDeviceDiscoveries	デバイス検出の情報を一覧表示するアクセス許可を付与します	リスト			
ListDiscoveredDevices	デバイス検出で検出されたデバイスの情報を一覧表示するアクセス許可を付与します	読み取り			
ListEventLogConfigurations	イベントログ設定の情報を一覧表示するアクセス許可を付与します	読み取り			
ListManagedThingAccountAssociations	マネージドモノとアカウントの関連付け間の関連付けに関する情報を一覧表示するアクセス許可を付与します	リスト			
ListManagedThingSchemas	マネージドモノに関連付けられたスキーマを一覧表示する許可を付与	読み取り	managed-thing*		
ListManagedThings	マネージドモノの情報を一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListNotificationConfigurations	通知設定の情報を一覧表示するアクセス許可を付与します	読み取り			
ListOtaTaskConfigurations	ota タスク設定の情報を一覧表示するアクセス許可を付与します	読み取り			
ListOtaTaskExecutions	ota タスク実行の情報を一覧表示するアクセス許可を付与します	読み取り	ota-task*		
ListOtaTasks	ota タスクの情報を一覧表示するアクセス許可を付与します	リスト			
ListProvisioningProfiles	プロビジョニングプロファイルの情報を一覧表示するアクセス許可を付与します	リスト			
ListSchemaVersions	スキーマの情報を一覧表示するアクセス許可を付与します	リスト			
ListTagsForResource	指定されたリソースのタグを一覧表示する許可を付与	読み取り	account-association		
			credential-locker		
			managed-thing		
			ota-task		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			provisioning-profile		
				aws:ResourceTag/${TagKey}	
PutDefaultEncryptionConfiguration	暗号化設定のデフォルト設定を更新する許可を付与	書き込み			
PutHubConfiguration	ハブ設定を更新するアクセス許可を付与します	書き込み			
PutRuntimeLogConfiguration	ランタイムログ設定を更新するアクセス許可を付与します	書き込み			
RegisterAccountAssociation	アカウントの関連付けを管理対象モノに登録するアクセス許可を付与します	書き込み	account-association*		
			managed-thing*		
RegisterCustomEndpoint	カスタムエンドポイントを登録するアクセス許可を付与します	書き込み			
ResetRuntimeLogConfiguration	ランタイムログ設定をリセットするアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SendConnectorEvent	コネクタイベントを送信するアクセス許可を付与します	書き込み			
SendManagedThingCommand	マネージドモノにコマンドを送信するアクセス許可を付与します	書き込み	managed-thing*		
			account-association		
StartAccountAssociationRefresh	アカウントの関連付けに関連付けられたアクセストークンの更新を開始するアクセス許可を付与します	書き込み	account-association*		
StartDeviceDiscovery	デバイス検出を開始するアクセス許可を付与します	書き込み	account-association		
			managed-thing		
TagResource	指定されたリソースにタグを追加するアクセス許可を付与します	Tagging	account-association		
			credential-locker		
			managed-thing		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			ota-task		
			provisioning-profile		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	指定されたリソースのタグを削除するアクセス許可を付与します	Tagging	account-association		
			credential-locker		
			managed-thing		
			ota-task		
			provisioning-profile		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateAccountAssociation	アカウントの関連付けを更新するアクセス許可を付与します	書き込み	account-association*		
UpdateCloudConnector	クラウドコネクタを更新する許可を付与	書き込み		iotmanagedintegrations:cloudConnectorId	
UpdateConnectorDestination	コネクタの送信先を更新する許可を付与	書き込み			
UpdateDestination	送信先を更新する許可を付与します。	書き込み			
UpdateEventLogConfiguration	イベントログ設定を更新する許可を付与	書き込み			
UpdateManagedThing	マネージドモノを更新するアクセス許可を付与します	書き込み	managed-thing*		
			credential-locker		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateNotification Configuration	通知設定を更新するアクセス許可を付与します	書き込み			
UpdateOtaTask	ota タスクを更新する許可を付与	書き込み	ota-task*		

AWS IoT Managed Integrations で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
account-association	arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:account-association/${AccountAssociationId}	aws:ResourceTag/${TagKey}
credential-locker	arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:credential-locker/${Identifier}	aws:ResourceTag/${TagKey}
managed-thing	arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:managed-thing/${Identifier}	aws:ResourceTag/${TagKey}
ota-task	arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:ota-task/${Identifier}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
provisioning-profile	arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:provisioning-profile/${Identifier}	aws:ResourceTag/${TagKey}

AWS IoT マネージド統合の条件キー

AWS IoT Managed Integrations では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーによりアクセスをフィルタリングします	ArrayOfString
iotmanagedintegrations:cloudConnectorId	CloudConnectorId でアクセスをフィルタリングします	String
iotmanagedintegrations:connectorDestinationId	ConnectorDestinationId でアクセスをフィルタリングします	String

AWS IoT SiteWise のアクション、リソース、および条件キー

AWS IoT SiteWise (サービスプレフィックス: iotsitewise) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IoT SiteWise で定義されるアクション
- AWS IoT SiteWise で定義されるリソースタイプ
- AWS IoT SiteWise の条件キー

AWS IoT SiteWise で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateAssets	階層によって子アセットを親アセットに関連付けるアクセス許可を付与	書き込み	asset*		
AssociateTimeSeriesToAssetProperty	時系列をアセットプロパティに関連付けるためのアクセス許可を付与	書き込み	asset*		
			time-series*		
BatchAssociateProjectAssets	アセットをプロジェクトに関連付けるアクセス許可を付与	書き込み	project*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchDisassociateProjectAssets	プロジェクトからアセットの関連付けを解除する許可を付与	書き込み	project*		
BatchGetAssetPropertyAggregates	複数のアセットプロパティの計算された集計を取得するための許可を付与	読み取り	asset		
			time-series		
BatchGetAssetPropertyValue	複数のアセットプロパティの最新値を取得する許可を付与	読み取り	asset		
			time-series		
BatchGetAssetPropertyValueHistory	複数のアセットプロパティの値履歴を取得する許可を付与	読み取り	asset		
			time-series		
BatchPutAssetPropertyValue	アセットプロパティのプロパティ値を付けるアクセス許可を付与	書き込み	asset		
			time-series		
CreateAccessPolicy	ポータルまたはプロジェクトのアクセスポリシーを作成する許可を付与	書き込み	portal		
			project		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateAsset	アセットモデルからアセットを作成する許可を付与	書き込み	asset-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssetModel	アセットモデルを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssetModelCompositeModel	アセットモデル内にアセットモデル複合モデルを作成する許可を付与	書き込み	asset-model*		
CreateBulkImportJob	バルクインポートジョブを作成するアクセス許可を付与	書き込み			
CreateComputationModel	計算モデルを作成するアクセス許可を付与します	書き込み	asset		
			asset-model		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDashboard	プロジェクト内でダッシュボードを作成する許可を付与	書き込み	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	データセットを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGateway	ゲートウェイを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreatePortal	ポータルを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	sso:CreateManagedApplicationInstance sso:DescribeRegisteredRegions
CreateProject	ポータルにプロジェクトを作成する許可を付与	書き込み	portal*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessPolicy	アクセスポリシーを削除する許可を付与	書き込み	access-policy*		
DeleteAsset	アセットを削除する許可を付与	書き込み	asset*		
DeleteAssetModel	アセットモデルを削除する許可を付与	書き込み	asset-model*		
DeleteAssetModelCompositeModel	アセットモデル複合モデルを削除する許可を付与	書き込み	asset-model*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteAssetModelInterfaceRelationship	アセットモデルとインターフェイス間の関係を削除するアクセス許可を付与します	書き込み	asset-model*		
DeleteComputationModel	計算モデルを削除するアクセス許可を付与します	書き込み	computation-model*		
DeleteDashboard	ダッシュボードを削除する許可を付与	書き込み	dashboard*		
DeleteDataset	データセットを削除する許可を付与	書き込み	dataset*		
DeleteGateway	ゲートウェイを削除する許可を付与	書き込み	gateway*		
DeletePortal	ポータルを削除する許可を付与	書き込み	portal*		sso:DeleteManagedApplicationInstance
DeleteProject	プロジェクトを削除する許可を付与	書き込み	project*		
DeleteTimeSeries	時系列を削除するアクセス許可を付与	書き込み	asset		
			time-series		
DescribeAccessPolicy	アクセスポリシーを記述する許可を付与	読み取り	access-policy*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeAction	アクションを記述する許可を付与	読み取り	asset		
			computation-model		
DescribeAsset	アセットを記述する許可を付与	読み取り	asset*		
DescribeAssetCompositeModel	アセット複合モデルを記述する許可を付与	読み取り	asset*		
DescribeAssetModel	アセットモデルを記述する許可を付与	読み取り	asset-model*		
DescribeAssetModelCompositeModel	アセットモデル複合モデルを記述する許可を付与	読み取り	asset-model*		
DescribeAssetModelInterfaceRelationship	アセットモデルとインターフェイスの関係を記述するアクセス許可を付与します	読み取り	asset-model*		
DescribeAssetProperty	アセットプロパティを記述する許可を付与	読み取り	asset*		
DescribeBulkImportJob	バルクインポートジョブを記述するアクセス許可を付与	読み取り			
DescribeComputationModel	計算モデルを記述するアクセス許可を付与します	読み取り	computation-model*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeComputationModelExecutionSummary	計算モデルの実行概要を記述するアクセス許可を付与します	読み取り	computation-model*		
			asset		
DescribeDashboard	ダッシュボードを記述する許可を付与	読み取り	dashboard*		
DescribeDataset	データセットを記述するアクセス許可を付与します	読み取り	dataset*		
DescribeDefaultEncryptionConfiguration	のデフォルトの暗号化設定を記述するアクセス許可を付与します AWS アカウント	読み取り			
DescribeExecution	実行を記述する許可を付与	読み取り			
DescribeGateway	ゲートウェイを記述する許可を付与	読み込み	gateway*		
DescribeGatewayCapabilityConfiguration	ゲートウェイの機能設定を記述する許可を付与	読み取り	gateway*		
DescribeLoggingOptions	のログ記録オプションを記述するアクセス許可を付与します AWS アカウント	読み取り			
DescribePortal	ポータルを記述する許可を付与	読み込み	portal*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeProject	プロジェクトを記述する許可を付与	読み取り	project*		
DescribeStorageConfiguration	のストレージ設定を記述するアクセス許可を付与しますAWS アカウント	読み取り			
DescribeTimeSeries	時系列を記述する許可を付与	読み込み	asset		
			time-series		
				aws:RequestTag/${TagKey} aws:TagKeys	
DisassociateAssets	子アセットを親アセットとの階層による関連付けから解除する許可を付与	書き込み	asset*		
DisassociateTimeSeriesFromAssetProperty	アセットプロパティから時系列の関連付けを解除する許可を付与	書き込み	asset*		
			time-series*		
EnableSiteWiseIntegration [アクセス許可のみ]	IoT SiteWise を他のサービスと統合できるようにする許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ExecuteAction	アクションを実行する許可を付与	書き込み	asset		
			computation-model		
ExecuteQuery	クエリを実行する許可を付与	読み取り			
GetAssetPropertyAggregates	アセットプロパティの計算された集計を取得するためのアクセス許可を付与	読み込み	asset		
			time-series		
GetAssetPropertyValue	アセットプロパティの最新値を取得する許可を付与	読み込み	asset		
			time-series		
GetAssetPropertyValueHistory	アセットプロパティの値履歴を取得する許可を付与	読み込み	asset		
			time-series		
GetInterpolatedAssetPropertyValues	アセットプロパティの補間値を取得する許可を付与	読み取り	asset		
			time-series		
InvokeAssistant	アシスタントを呼び出すアクセス許可を付与します	読み取り			
ListAccessPolicies	ID またはリソースのすべてのアクセスポリシーを一覧表示する許可を付与	リスト	portal		
			project		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListActions	アクションを一覧表示する許可を付与	リスト	asset		
			computation-model		
ListAssetModelCompositeModels	アセットモデル複合モデルを一覧表示する許可を付与	リスト	asset-model*		
ListAssetModelProperties	アセットモデルのプロパティを一覧表示する許可を付与	リスト	asset-model*		
ListAssetModels	すべてのアセットモデルを一覧表示する許可を付与	リスト			
ListAssetProperties	アセットプロパティを一覧表示する許可を付与	リスト	asset*		
ListAssetRelationships	アセットのアセットリレーションシップグラフを一覧表示する許可を付与	リスト	asset*		
ListAssets	すべてのアセットを一覧表示する許可を付与	リスト	asset-model		
ListAssociatedAssets	階層別にアセットに関連付けられているすべてのアセットを一覧表示する許可を付与	リスト	asset*		
ListBulkImportJobs	バルクインポートジョブを一覧表示するアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListCompositionRelationships	すべてのアセットモデル構成関係を一覧表示する許可を付与	リスト	asset-model*		
ListComputationModelDataBindingUsages	計算モデルデータバインディングの使用状況を一覧表示するアクセス許可を付与します	リスト	asset		
			asset-model		
ListComputationModelResolveToResources	リソースへの計算モデルの解決を一覧表示するアクセス許可を付与します	リスト	computation-model*		
ListComputationModels	すべての計算モデルを一覧表示するアクセス許可を付与します	リスト			
ListDashboards	プロジェクト内のすべてのダッシュボードを一覧表示する許可を付与	リスト	project*		
ListDatasets	すべてのデータセットを一覧表示するアクセス許可を付与	リスト			
ListExecutions	実行を一覧表示するアクセス許可を付与します	リスト	asset		
			computation-model		
ListGateways	すべてのゲートウェイを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListInterfaceRelationships	インターフェイスによって強制されるすべてのアセットモデルを一覧表示するアクセス許可を付与します	リスト	asset-model*		
ListPortals	すべてのポータルを一覧表示する許可を付与	リスト			
ListProjectAssets	プロジェクトに関連付けられているすべてのアセットを一覧表示する許可を付与	リスト	project*		
ListProjects	ポータル内のすべてのプロジェクトを一覧表示する許可を付与	リスト	portal*		
ListTagsForResource	リソースのすべてのタグを一覧表示する許可を付与	読み込み	access-policy		
			asset		
			asset-model		
			computation-model		
			dashboard		
			dataset		
			gateway		
			portal		
			project		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			time-series		
				aws:ResourceTag/${TagKey}	
ListTimeSeries	時系列を一覧表示するアクセス許可を付与	リスト	asset		
PutAssetModelInterfaceRelationship	アセットモデルとインターフェイス間の関係を作成するアクセス許可を付与します	書き込み	asset-model*		
PutDefaultEncryptionConfiguration	のデフォルトの暗号化設定を設定するアクセス許可を付与します AWS アカウント	書き込み			
PutLoggingOptions	の口グ記録オプションを設定するアクセス許可を付与します AWS アカウント	書き込み			
PutStorageConfiguration	のストレージ設定を構成するアクセス許可を付与します AWS アカウント	書き込み			
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	access-policy		
			asset		
			asset-model		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			computation-model		
			dashboard		
			dataset		
			gateway		
			portal		
			project		
			time-series		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	リソースのタグを解除する許可を付与	タグ付け	access-policy		
			asset		
			asset-model		
			computation-model		
			dashboard		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			dataset		
			gateway		
			portal		
			project		
			time-series		
				aws:TagKeys	
UpdateAccessPolicy	アクセスポリシーを更新する許可を付与	書き込み	access-policy*		
UpdateAsset	アセットを更新する許可を付与	書き込み	asset*		
UpdateAssetModel	アセットモデルを更新する許可を付与	書き込み	asset-model*		
UpdateAssetModelCompositeModel	アセットモデル複合モデルを更新する許可を付与	書き込み	asset-model*		
UpdateAssetModelPropertyRouting [アクセス許可のみ]	AssetModel プロパティルーティングを更新するアクセス許可を付与	書き込み	asset-model*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateAssetProperty	アセットプロパティを更新する許可を付与	書き込み	asset*		
UpdateComputationModel	計算モデルを更新するアクセス許可を付与します	書き込み	computation-model*		
			asset		
			asset-model		
UpdateDashboard	ダッシュボードを更新する許可を付与	書き込み	dashboard*		
UpdateDataset	データセットを更新するアクセス許可を付与	書き込み	dataset*		
UpdateGateway	ゲートウェイを更新する許可を付与	書き込み	gateway*		
UpdateGatewayCapabilityConfiguration	ゲートウェイの機能設定を更新する許可を付与	書き込み	gateway*		
UpdatePortal	ポータルを更新する許可を付与	書き込み	portal*		
UpdateProject	プロジェクトを更新する許可を付与	書き込み	project*		

AWS IoT SiteWise で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
asset	arn:${Partition}:iotsitewise:${Region}:${Account}:asset/${AssetId}	aws:ResourceTag/${TagKey}
asset-model	arn:${Partition}:iotsitewise:${Region}:${Account}:asset-model/${AssetModelId}	aws:ResourceTag/${TagKey}
time-series	arn:${Partition}:iotsitewise:${Region}:${Account}:time-series/${TimeSeriesId}	aws:ResourceTag/${TagKey}
gateway	arn:${Partition}:iotsitewise:${Region}:${Account}:gateway/${GatewayId}	aws:ResourceTag/${TagKey}
portal	arn:${Partition}:iotsitewise:${Region}:${Account}:portal/${PortalId}	aws:ResourceTag/${TagKey}
project	arn:${Partition}:iotsitewise:${Region}:${Account}:project/${ProjectId}	aws:ResourceTag/${TagKey}
dashboard	arn:${Partition}:iotsitewise:${Region}:${Account}:dashboard/${DashboardId}	aws:ResourceTag/${TagKey}
access-policy	arn:${Partition}:iotsitewise:${Region}:${Account}:access-policy/${AccessPolicyId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
dataset	arn:${Partition}:iotsitewise:${Region}:${Account}:dataset/${DatasetId}	aws:ResourceTag/${TagKey}
computation-model	arn:${Partition}:iotsitewise:${Region}:${Account}:computation-model/${ComputationModelId}	aws:ResourceTag/${TagKey}

AWS IoT SiteWise の条件キー

AWS IoT SiteWise では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアによるアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされたタグでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString
iotsitewise:assetHierarchyPath	アセットの階層内のアセット ID の文字列であるアセット階層パスでアクセスをフィルタリングします。各パスはスラッシュで区切られます	String
iotsitewise:childAssetId	親アセットに関連付けられている子アセットの ID でアクセスをフィルタリングします	String

条件キー	説明	タイプ
iotsitewise:group	AWS Single Sign-On グループの ID でアクセスをフィルタリングします	String
iotsitewise:iam	IAM アイデンティティの ID AWS でアクセスをフィルタリングします	String
iotsitewise:isAssociatedWithAssetProperty	アセットプロパティに関連付けられている、または関連付けられていないデータストリームによってアクセスをフィルタリングします	String
iotsitewise:portal	ポータルの ID でアクセスをフィルタリングします	文字列
iotsitewise:project	プロジェクトの ID でアクセスをフィルタリングします	String
iotsitewise:propertyAlias	プロパティエイリアスによってアクセスをフィルタリングします	String
iotsitewise:propertyId	アセットプロパティの ID でアクセスをフィルタリングします	String
iotsitewise:user	AWS シングルサインオンユーザーの ID でアクセスをフィルタリングします	String

AWS IoT TwinMakerの、アクション、リソース、および条件キー

AWS IoT TwinMaker (サービスプレフィックス: `iottwinmaker`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IoT TwinMakerで定義されるアクション
- AWS IoT TwinMakerで定義されるリソースタイプ
- AWS IoT TwinMaker条件キー

AWS IoT TwinMakerで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchPutPropertyValues	複数の時系列プロパティの値を設定するアクセス許可を付与	書き込み	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			entity		
CancelMetadataTransferJob	メタデータ転送ジョブをキャンセルする許可を付与	書き込み	metadataTransferJob*		
CreateComponentType	ComponentType を作成するアクセス許可を付与	書き込み	workspace*		
				aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
CreateEntity	エンティティを作成する許可を付与	書き込み	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMetadataTransferJob	メタデータ転送ジョブを作成する許可を付与	書き込み			
CreateScene	シーンを作成するアクセス許可を付与	書き込み	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSyncJob	同期ジョブを作成する許可を付与	書き込み	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateWorkspace	ワークスペースを作成するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComponentType	ComponentType を削除するアクセス許可を付与	書き込み	componentType*		
			workspace*		
DeleteEntity	エンティティを削除する許可を付与	書き込み	entity*		
			workspace*		
DeleteScene	シーン を削除する許可を付与	書き込み	scene*		
			workspace*		
DeleteSyncJob	同期ジョブを削除する許可を付与	書き込み	syncJob*		
			workspace*		
DeleteWorkspace	ワークスペースを削除するアクセス許可を付与	書き込み	workspace*		
ExecuteQuery	クエリを実行する許可を付与	読み取り	workspace*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetComponentType	コンポーネントタイプを取得するためのアクセス許可を付与	読み取り	componentType*		
			workspace*		
GetEntity	エンティティを取得するためのアクセス許可を付与	読み取り	entity*		
			workspace*		
GetMetadataTransferJob	メタデータ転送ジョブを取得する許可を付与	読み取り	metadataTransferJob*		
GetPricingPlan	料金設定プランを取得する許可を付与	読み取り			
GetPropertyValue	プロパティの最新値を取得する許可を付与	読み取り	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			componentType		
			entity		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetPropertyValueHistory	時系列の値履歴を取得する許可を付与	読み取り	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			componentType		
			entity		
GetScene	シーンを得るためのアクセス許可を付与	読み取り	scene*		
			workspace*		
GetSyncJob	同期ジョブを取得する許可を付与	読み取り	syncJob*		
			workspace*		
GetWorkspace	ワークスペースを取得する許可を付与	読み取り	workspace*		
ListComponentTypes	ワークスペース内のすべてのComponentTypes を一覧表示するアクセス許可を付与	リスト	workspace*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListComponents	エンティティにアタッチされているコンポーネントを一覧表示する許可を付与	リスト	entity*		
			workspace*		
ListEntities	ワークスペース内のすべてのエンティティを一覧表示するアクセス許可を付与	リスト	workspace*		
ListMetadataTransferJobs	メタデータ転送ジョブを一覧表示する許可を付与	リスト			
ListProperties	エンティティコンポーネントのプロパティを一覧表示する許可を付与	リスト	entity*		
			workspace*		
ListScenes	ワークスペース内のすべてのシーンを一覧表示するアクセス許可を付与	リスト	workspace*		
ListSyncJobs	ワークスペース内のすべての同期ジョブを一覧表示する許可を付与	リスト	workspace*		
ListSyncResources	同期ジョブのすべての同期リソースを一覧表示する許可を付与	リスト	syncJob*		
			workspace*		
ListTagsForResource	リソースのすべてのタグを一覧表示する許可を付与	リスト	componentType		
			entity		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			scene		
			syncJob		
			workspace		
				aws:ResourceTag/${TagKey}	
ListWorkspaces	全てのワークスペースを一覧表示するアクセス許可を付与	リスト			
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	componentType		
			entity		
			scene		
			syncJob		
			workspace		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースのタグを解除する許可を付与	Tagging	componentType		
			entity		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			scene		
			syncJob		
			workspace		
				aws:TagKeys	
UpdateComponentType	コンポーネントタイプを更新するためのアクセス許可を付与	書き込み	componentType*		
			workspace*		
UpdateEntity	エンティティを更新する許可を付与	書き込み	entity*		
			workspace*		
UpdatePricingPlan	料金設定プランを更新する許可を付与	書き込み			
UpdateScene	シーンを更新するアクセス許可を付与	書き込み	scene*		
			workspace*		
UpdateWorkspace	ワークスペースを更新するアクセス許可を付与	書き込み	workspace*		

AWS IoT TwinMakerで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアク

ションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
workspace	arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}	aws:ResourceTag/${TagKey}
entity	arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/entity/${EntityId}	aws:ResourceTag/${TagKey}
componentType	arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/component-type/${ComponentTypeId}	aws:ResourceTag/${TagKey}
scene	arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/scene/${SceneId}	aws:ResourceTag/${TagKey}
syncJob	arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/sync-job/${SyncJobId}	aws:ResourceTag/${TagKey}
metadataTransferJob	arn:${Partition}:iottwinmaker:${Region}:${Account}:metadata-transfer-job/${MetadataTransferJobId}	

AWS IoT TwinMaker条件キー

AWS IoT TwinMaker では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアによるアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされたタグでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString
iottwinmaker:destinationType	メタデータ転送ジョブの送信先のタイプでアクセスをフィルタリングします	ArrayOfString
iottwinmaker:linkedServices	サービスにリンクされたワークスペースでアクセスをフィルタリングします	ArrayOfString
iottwinmaker:sourceType	メタデータの転送ジョブのソース、タイプ別にアクセスをフィルタリングします	ArrayOfString

AWS IoT Wireless のアクション、リソース、および条件キー

AWS IoT Wireless (サービスプレフィックス: `iotwireless`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IoT Wireless によって定義されたアクション
- AWS IoT Wireless によって定義されたリソースタイプ
- AWS IoT Wireless の条件キー

AWS IoT Wireless によって定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateAwsAccountWithPartnerAccount	パートナーアカウントを にリンクするアクセス許可を付与します AWS アカウント	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
AssociateMulticastGroupWithFuotaTask	マルチキャストグループを FuotaTask に関連付けるためのアクセス許可を付与	書き込み	FuotaTask*		
			MulticastGroup*		
AssociateWirelessDeviceWithFuotaTask	ワイヤレスデバイスを FuotaTask に関連付けるためのアクセス許可を付与	書き込み	FuotaTask*		
			WirelessDevice*		
AssociateWirelessDeviceWithMulticastGroup	WirelessDevice Multicast Group を関連付けるためのアクセス許可を付与	書き込み	MulticastGroup*		
			WirelessDevice*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateWirelessDeviceWithThing	ワイヤレスデバイスを特定の wirelessDeviceId の AWS IoT モノに関連付けるアクセス許可を付与します	書き込み	WirelessDevice*		iot:DescribeThing
			thing*		
AssociateWirelessGatewayWithCertificate	WirelessGateway を IoT Core Identity 証明書に関連付けるアクセス許可を付与	書き込み	WirelessGateway*		
			cert*		
AssociateWirelessGatewayWithThing	ワイヤレスゲートウェイを特定の wirelessGatewayId の AWS IoT モノに関連付けるアクセス許可を付与します	書き込み	WirelessGateway*		iot:DescribeThing
			thing*		
CancelMulticastGroupSession	MulticastGroup セッションをキャンセルするアクセス許可を付与	書き込み	MulticastGroup*		
CreateDestination	送信先のリソースを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceProfile	DeviceProfile リソースを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateFuotaTask	ホストリソースを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMulticastGroup	MulticastGroup リソースを作成するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNetworkAnalyzerConfiguration	NetworkAnalyzerConfiguration リソースを作成する許可を付与	書き込み	MulticastGroup*		
			WirelessDevice*		
			WirelessGateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateServiceProfile	ServiceProfile リソースを作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWirelessDevice	指定された送信先で WirelessDevice リソースを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWirelessGateway	WirelessGateway リソースを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWirelessGatewayTask	指定された WirelessGateway のタスクを作成する許可を付与	書き込み	WirelessGateway*		
CreateWirelessGatewayTaskDefinition	WirelessGateway タスク定義を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDestination	送信先を削除する許可を付与	書き込み	Destination*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteDeviceProfile	DeviceProfile を削除する許可を付与	書き込み	DeviceProfile*		
DeleteFuotaTask	FuoTask を削除するアクセス許可を付与	書き込み	FuotaTask*		
DeleteMulticastGroup	MultiCastGroup を削除するアクセス許可を付与	書き込み	MulticastGroup*		
DeleteNetworkAnalyzerConfiguration	NetworkAnalyzerConfiguration を削除する許可を付与	書き込み	NetworkAnalyzerConfiguration*		
DeleteQueuedMessages	QueuedMessages を削除する許可を付与	書き込み			
DeleteServiceProfile	ServiceProfile を削除する許可を付与	書き込み	ServiceProfile*		
DeleteWirelessDevice	WirelessDevice を削除する許可を付与	書き込み	WirelessDevice*		
DeleteWirelessDeviceImportTask	ワイヤレスデバイスのインポートタスクを削除するための許可を付与します	書き込み	ImportTask*		
DeleteWirelessGateway	WirelessGateway を削除する許可を付与。	書き込み	WirelessGateway*		
DeleteWirelessGatewayTask	指定された WirelessGateway のタスクを削除する許可を付与	書き込み	WirelessGateway*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteWirelessGatewayTaskDefinition	WirelessGateway タスク定義を削除する許可を付与	書き込み	WirelessGatewayTaskDefinition*		
DeregisterWirelessDevice	ワイヤレスデバイスの登録を解除する許可を付与	書き込み	WirelessDevice*		
DisassociateAwsAccountFromPartnerAccount	パートナーアカウント AWS アカウント から の関連付けを解除するアクセス許可を付与します	書き込み	SidewalkAccount*		
DisassociateMulticastGroupFromFuotaTask	FuotaTask から Multicast Group の関連付けを解除するためのアクセス許可を付与	書き込み	FuotaTask*		
			MulticastGroup*		
DisassociateWirelessDeviceFromFuotaTask	IoT Thing からワイヤレスデバイスの関連付けを解除する許可を付与	書き込み	FuotaTask*		
			WirelessDevice*		
DisassociateWirelessDeviceFromMulticastGroup	IoT Thing からワイヤレスデバイスの関連付けを解除する許可を付与	書き込み	MulticastGroup*		
			WirelessDevice*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DisassociateWirelessDeviceFromThing	ワイヤレスデバイスを AWS IoT モノから関連付け解除するアクセス許可を付与します	書き込み	WirelessDevice*		iot:DescribeThing
			thing*		
DisassociateWirelessGatewayFromCertificate	IoT Core Identity 証明書から WirelessGateway の関連付けを解除する許可を付与	書き込み	WirelessGateway*		
			cert*		
DisassociateWirelessGatewayFromThing	IoT Core Thing から WirelessGateway の関連付けを解除する許可を付与	書き込み	WirelessGateway*		iot:DescribeThing
			thing*		
GetDestination	送信先を取得する許可を付与	読み取り	Destination*		
GetDeviceProfile	DeviceProfile を取得する許可を付与	読み取り	DeviceProfile*		
GetEventConfigurationByResourceTypes	リソースタイプ別にイベント設定を取得する許可を付与	読み取り			
GetFuotaTask	FuoTask を取得するアクセス許可を付与	読み取り	FuotaTask*		
GetLogLevelsByResourceTypes	リソースタイプ別にログレベルを取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetMetricConfiguration	メトリクス設定を取得する許可を付与する	読み取り			
GetMetrics	メトリクスを取得する許可を付与する	読み取り			
GetMulticastGroup	MultiCastGroup を取得するアクセス許可を付与	読み取り	MulticastGroup*		
GetMulticastGroupSession	MulticastGroup セッションを取得するアクセス許可を付与	読み取り	MulticastGroup*		
GetNetworkAnalyzerConfiguration	NetworkAnalyzer 設定を取得するアクセス許可を付与	読み取り	NetworkAnalyzerConfiguration*		
GetPartnerAccount	関連付けられた PartnerAccount を取得する許可を付与	読み取り	SidewalkAccount*		
GetPosition	特定リソースのポジションを取得する許可の付与	読み取り	WirelessDevice		
			WirelessGateway		
GetPositionConfiguration	特定リソースのポジション設定を取得する許可の付与	読み取り	WirelessDevice		
			WirelessGateway		
GetPositionEstimate	推測位置を取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetResourceEventConfiguration	識別子のイベント設定を取得するアクセス許可を付与	読み取り	SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
GetResourceLogLevel	リソースログレベルを取得する許可を付与	読み取り	WirelessDevice		
			WirelessGateway		
GetResourcePosition	特定リソースのポジションを取得する許可の付与	読み取り	WirelessDevice		
			WirelessGateway		
GetServiceEndpoint	CUPS プロトコル接続または LoRaWAN Network Server (LNS) プロトコル接続用のカスタマーアカウント固有のエンドポイントを取得し、必要に応じて PEM 形式のサーバー信頼証明書を取得する許可を付与	読み取り			
GetServiceProfile	ServiceProfile を取得する許可を付与	読み取り	ServiceProfile*		
GetWirelessDevice	WirelessDevice を取得する許可を付与	読み取り	WirelessDevice*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetWirelessDeviceImportTask	ワイヤレスデバイスのインポートタスクを取得するための許可を付与します	読み取り	ImportTask*		
GetWirelessDeviceStatistics	指定された WirelessDevice の統計情報を取得する許可を付与	読み取り	WirelessDevice*		
GetWirelessGateway	WirelessGateway を取得する許可を付与	読み取り	WirelessGateway*		
GetWirelessGatewayCertificate	WirelessGateway に関連付けられた IoT Core Identity 証明書 ID を取得する許可を付与	読み取り	WirelessGateway*		
GetWirelessGatewayFirmwareInformation	WirelessGateway の Current ファームウェアバージョンおよびその他の情報の取得する許可を付与	読み取り	WirelessGateway*		
GetWirelessGatewayStatistics	指定された WirelessGateway の統計情報を取得する許可を付与	読み取り	WirelessGateway*		
GetWirelessGatewayTask	指定された WirelessGateway のタスクを取得するためのアクセス許可を付与	読み取り	WirelessGateway*		
GetWirelessGatewayTaskDefinition	指定された WirelessGateway タスク定義を取得するためのアクセス許可を付与	読み取り	WirelessGatewayTaskDefinition*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListDestinations	に基づいて利用可能な送信先の情報を一覧表示するアクセス許可を付与します AWS アカウント	読み取り			
ListDeviceProfiles	に基づいて使用可能な DeviceProfiles の情報を一覧表示するアクセス許可を付与します AWS アカウント	読み取り			
ListDevicesForWirelessDeviceImportTask	に基づいて、ワイヤレスデバイスのインポートタスクによってデバイスの情報を一覧表示するアクセス許可を付与します AWS アカウント	読み取り	ImportTask*		
ListEventConfigurations	に基づいて使用可能なイベント設定の情報を一覧表示するアクセス許可を付与します AWS アカウント	読み取り			
ListFuotaTasks	に基づいて使用可能な FuotaTasks の情報を一覧表示するアクセス許可を付与します AWS アカウント	読み取り			
ListMulticastGroups	に基づいて使用可能な MulticastGroups の情報を一覧表示するアクセス許可を付与します AWS アカウント	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListMulticastGroupsByFuotaTask	に基づいてFuotaTask によって使用可能な MulticastGroups の情報を一覧表示するアクセス許可を付与します AWS アカウント	読み取り	FuotaTask *		
ListNetworkAnalyzerConfigurations	に基づいて使用可能な NetworkAnalyzerConfigurations の情報を一覧表示するアクセス許可を付与します AWS アカウント	読み取り			
ListPartnerAccounts	利用可能なパートナーアカウントを一覧表示する許可を付与	読み取り			
ListPositionConfigurations	に基づいて使用可能な位置設定の情報を一覧表示するアクセス許可を付与します AWS アカウント	読み取り			
ListQueuedMessages	QueuedMessages を一覧表示する許可を付与	読み取り			
ListServiceProfiles	に基づいて利用可能な ServiceProfiles の情報を一覧表示するアクセス許可を付与します AWS アカウント	読み取り			
ListTagsForResource	指定されたリソースのすべてのタグを一覧表示する許可を付与	読み取り	Destination		
			DeviceProfile		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			FuotaTask		
			ImportTask		
			MulticastGroup		
			NetworkAnalyzerConfiguration		
			ServiceProfile		
			SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
			WirelessGatewayTaskDefinition		
ListWirelessDeviceImportTasks	に基づいて のワイヤレスデバイスのインポートタスク情報を一覧表示するアクセス許可を付与します AWS アカウント	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListWirelessDevices	に基づいて使用可能な WirelessDevices の情報を一覧表示するアクセス許可を付与します AWS アカウント	読み取り			
ListWirelessGatewayTaskDefinitions	に基づいて利用可能な WirelessGateway タスク定義の情報を一覧表示するアクセス許可を付与します AWS アカウント	読み取り			
ListWirelessGateways	に基づいて利用可能な WirelessGateways の情報を一覧表示するアクセス許可を付与します AWS アカウント	読み取り			
PutPositionConfiguration	特定リソースのポジション設定を指定する許可の付与	書き込み	WirelessDevice		
			WirelessGateway		
PutResourceLogLevel	リソースログレベルを配置する許可を付与	書き込み	WirelessDevice		
			WirelessGateway		
ResetAllResourceLogLevels	すべてのリソースログレベルをリセットする許可を付与	書き込み			
ResetResourceLogLevel	リソースログレベルをリセットする許可を付与	書き込み	WirelessDevice		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			WirelessGateway		
SendDataToMulticastGroup	MulticastGroup にデータを送信するアクセス許可を付与	書き込み	MulticastGroup*		
SendDataToWirelessDevice	復号化されたアプリケーションデータフレームをターゲットデバイスに送信する許可を付与	書き込み	WirelessDevice*		
StartBulkAssociateWirelessDeviceWithMulticastGroup	ワイヤレスデバイスをマルチキャストグループに関連付けるためのアクセス許可を付与	書き込み	MulticastGroup*		
StartBulkDisassociateWirelessDeviceFromMulticastGroup	ワイヤレスデバイスを MulticastGroup から一括で関連付け解除する権限を付与	書き込み	MulticastGroup*		
StartFuotaTask	FuoTask を開始するアクセス許可を付与	書き込み	FuotaTask*		
StartMulticastGroupSession	MulticastGroup セッションを開始するアクセス許可を付与	書き込み	MulticastGroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartNetworkAnalyzerStream	NetworkAnalyzer ストリームを開始するアクセス許可を付与	書き込み	NetworkAnalyzerConfiguration*		
StartSingleWirelessDeviceImportTask	単一のワイヤレスデバイスのインポートタスクを開始するための許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
StartWirelessDeviceImportTask	ワイヤレスデバイスのインポートタスクを開始するための許可を付与します	書き込み	ImportTask*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	指定されたリソースにタグを付けるアクセス許可を付与	タグ付け	Destination		
			DeviceProfile		
			FuotaTask		
			ImportTask		
			MulticastGroup		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			NetworkAnalyzerConfiguration		
			ServiceProfile		
			SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
			WirelessGatewayTaskDefinition		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestWirelessDevice	プロビジョンドデバイスをシミュレートして、「Hello」のペイロードのアップリンクデータを送信する許可を付与	書き込み	WirelessDevice*		
UntagResource	指定されたタグをリソースから削除する許可を付与	タグ付け	Destination		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			DeviceProfile		
			FuotaTask		
			ImportTask		
			MulticastGroup		
			NetworkAnalyzerConfiguration		
			ServiceProfile		
			SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
			WirelessGatewayTaskDefinition		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateDestination	送信先のリソースを更新する許可を付与	書き込み	Destination*		
UpdateEventConfigurationByResourceTypes	リソースタイプ別にイベント設定を更新する許可を付与	書き込み			
UpdateFuotaTask	FuoTask を更新するアクセス許可を付与	書き込み	FuotaTask*		
UpdateLogLevelsByResourceTypes	リソースタイプ別にログレベルを更新する許可を付与	書き込み			
UpdateMetricConfiguration	メトリクス設定を更新する許可を付与する	書き込み			
UpdateMulticastGroup	MultiCastGroup を更新するアクセス許可を付与	書き込み	MulticastGroup*		
UpdateNetworkAnalyzerConfiguration	NetworkAnalyzer 設定を更新するアクセス許可を付与	書き込み	MulticastGroup*		
			NetworkAnalyzerConfiguration*		
			WirelessDevice*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			WirelessGateway*		
UpdatePartnerAccount	パートナーアカウントを更新する許可を付与	書き込み	SidewalkAccount*		
UpdatePosition	特定リソースのポジションを更新する許可の付与	書き込み	WirelessDevice		
			WirelessGateway		
UpdateResourceEventConfiguration	識別子のイベント設定を更新するアクセス許可を付与	書き込み	SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
UpdateResourcePosition	特定リソースのポジションを更新する許可の付与	書き込み	WirelessDevice		
			WirelessGateway		
UpdateWirelessDevice	WirelessDevice リソースを更新する許可を付与。	書き込み	WirelessDevice*		
UpdateWirelessDeviceImportTask	ワイヤレスデバイスのインポートタスクを更新するための許可を付与します	書き込み	ImportTask*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateWirelessGateway	WirelessGateway リソースを更新する許可を付与	書き込み	WirelessGateway*		

AWS IoT Wireless によって定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
WirelessDevice	arn:${Partition}:iotwireless:${Region}:${Account}:WirelessDevice/${WirelessDeviceId}	aws:ResourceTag/${TagKey}
WirelessGateway	arn:${Partition}:iotwireless:${Region}:${Account}:WirelessGateway/${WirelessGatewayId}	aws:ResourceTag/${TagKey}
DeviceProfile	arn:${Partition}:iotwireless:${Region}:${Account}:DeviceProfile/${DeviceProfileId}	aws:ResourceTag/${TagKey}
ServiceProfile	arn:${Partition}:iotwireless:${Region}:${Account}:ServiceProfile/${ServiceProfileId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
Destination	arn:${Partition}:iotwireless:${Region}:${Account}:Destination/${DestinationName}	aws:ResourceTag/${TagKey}
SidewalkAccount	arn:${Partition}:iotwireless:${Region}:${Account}:SidewalkAccount/${SidewalkAccountId}	aws:ResourceTag/${TagKey}
WirelessGatewayTaskDefinition	arn:${Partition}:iotwireless:${Region}:${Account}:WirelessGatewayTaskDefinition/${WirelessGatewayTaskDefinitionId}	aws:ResourceTag/${TagKey}
FuotaTask	arn:${Partition}:iotwireless:${Region}:${Account}:FuotaTask/${FuotaTaskId}	aws:ResourceTag/${TagKey}
MulticastGroup	arn:${Partition}:iotwireless:${Region}:${Account}:MulticastGroup/${MulticastGroupId}	aws:ResourceTag/${TagKey}
NetworkAnalyzerConfiguration	arn:${Partition}:iotwireless:${Region}:${Account}:NetworkAnalyzerConfiguration/${NetworkAnalyzerConfigurationName}	aws:ResourceTag/${TagKey}
thing	arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}	
cert	arn:${Partition}:iot:${Region}:${Account}:cert/${Certificate}	
ImportTask	arn:${Partition}:iotwireless:${Region}:${Account}:ImportTask/${ImportTaskId}	aws:ResourceTag/${TagKey}

AWS IoT Wireless の条件キー

AWS IoT Wireless では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	ユーザーが IoT Wireless に対して行うリクエストに含まれるタグキーによってアクセスをフィルタリング	文字列
aws:ResourceTag/${TagKey}	IoT Wireless リソースにアタッチされているタグのタグキーコンポーネントによってアクセスをフィルタリング	String
aws:TagKeys	リクエスト内のリソースに関連付けられているすべてのタグキー名のリストによりアクセスををフィルタリングします	ArrayOfString

AWS IQ のアクション、リソース、および条件キー

AWS IQ (サービスプレフィックス: iq) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IQ で定義されるアクション
- AWS IQ で定義されるリソースタイプ

- AWS IQ の条件キー

AWS IQ で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AcceptCall	着信音声/ビデオ通話を受け入れるための許可を付与します	書き込み	call*		
ApprovePaymentRequest	支払いリクエストを承認するための許可を付与します	書き込み	paymentRequest*		
ApproveProposal	提案を承認するための許可を付与します	書き込み	proposal*		
ArchiveConversation	会話をアーカイブするための許可を付与します	書き込み	conversation*		
CompleteProposal	提案を完了するための許可を付与します	書き込み	proposal*		
CreateConversation	リクエストに応答し、またはダイレクトメッセージを送信して会話を開始するための許可を付与します	書き込み			
CreateExpert	エキスパートプロファイルを作成するための許可を付与します	書き込み			
CreateListing	リスティングを作成するための許可を付与します	書き込み			
CreateMilestoneProposal	マイルストーン提案を作成するための許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreatePaymentRequest	支払いリクエストを作成するための許可を付与します	書き込み			
CreateProject	新しいリクエストを送信するための許可を付与します	書き込み			
CreateRequest	新しいリクエストを送信するための許可を付与します	書き込み			
CreateScheduledProposal	スケジュールされた提案を作成するための許可を付与します	書き込み			
CreateSeller	販売者プロファイルを作成するための許可を付与します	書き込み			
CreateUpfrontProposal	事前提案を作成するための許可を付与します	書き込み			
DeclineCall	着信音声/ビデオ通話を拒否するための許可を付与します	書き込み	call*		
DeleteAttachment	既存のアタッチメントを削除するための許可を付与します	書き込み	attachment*		
DisableIndividualPublicProfile	個々の公開プロフィールページを無効にするアクセス許可を付与します	書き込み	expert*		
DownloadAttachment	既存のアタッチメントをダウンロードする許可を付与	読み取り	attachment*		
EnableIndividualPublicProfile	個々の公開プロフィールページを有効にするアクセス許可を付与します	書き込み	expert*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
EndCall	音声/ビデオ通話を終了するための許可を付与します	書き込み	call*		
GetBuyer	購入者情報を読み取るための許可を付与します	読み取り	buyer*		
GetCall	音声/ビデオ通話の詳細を読み取るための許可を付与します	読み取り	call*		
GetChatInfo	会話に関するチャット環境の詳細を読み取るための許可を付与します	読み取り	conversation*		
GetChatMessages	会話でチャットメッセージを読み取るための許可を付与します	読み取り	conversation*		
GetChatToken	会話通知用の websocket トークンをリクエストするための許可を付与します	読み取り	token*		
GetCompanyChatMessages	会社の会話でチャットメッセージを読み取る許可を付与します	読み取り	conversation*		
GetCompanyProfile	会社プロファイルを読み取るための許可を付与します	読み取り	company*		
GetConversation	会話の詳細を読み取るための許可を付与します	読み取り	conversation*		
GetExpert	エキスパート情報を読み取るための許可を付与します	読み取り	expert*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetListing	リスティングを読み取るための許可を付与します	読み取り	listing*		
GetMarketplaceSeller	販売者プロファイル情報を読み取るための許可を付与します	読み取り	seller*		
GetPaymentRequest	支払いリクエストを読み取るための許可を付与します	読み取り	paymentRequest*		
GetProposal	提案を読み取るための許可を付与します	読み取り	proposal*		
GetRequest	作成されたリクエストを取得する許可を付与	読み取り	request*		
GetReview	エキスパートのレビューを読み取るための許可を付与します	読み取り	seller*		
HideRequest	リクエストを非表示にするための許可を付与します	書き込み	request*		
InitiateCall	音声/ビデオ通話を開始するための許可を付与します	書き込み			
LinkAwsCertification	AWS 証明書を個々のプロファイルにリンクする許可を付与	書き込み	expert*		
ListAttachments	既存のアタッチメントを一覧表示する許可を付与	リスト	attachment*		
ListConversations	既存の会話を一覧表示するための許可を付与します	読み取り	conversation*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListExpertAccessLogs	エキスパートの活動のアクセスログを一覧表示するアクセス許可を付与します	読み取り	permission*		
ListListings	リスティングを一覧表示するための許可を付与します	読み取り	listing*		
ListPaymentRequests	支払いリクエストを一覧表示するための許可を付与します	読み取り	paymentRequest		
			paymentSchedule		
ListProposals	提案を一覧表示するための許可を付与します	読み取り	proposal*		
ListRequests	作成されたリクエストを一覧表示するための許可を付与します	読み取り	request*		
ListReviews	エキスパートのレビューを一覧表示するための許可を付与します	読み取り	seller*		
MarkChatMessageRead	会話でメッセージを既読としてマークするための許可を付与します	書き込み	conversation*		
RejectPaymentRequest	支払いリクエストを拒否するための許可を付与します	書き込み	paymentRequest*		
RejectProposal	提案を拒否するための許可を付与します	書き込み	proposal*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SendCompanyChatMessage	会社として会話でメッセージを送信するための許可を付与します	書き込み	conversation*		
SendIndividualChatMessage	個人として会話でメッセージを送信するための許可を付与します	書き込み	conversation*		
UnarchiveConversation	会話をアーカイブ解除するための許可を付与します	書き込み	conversation*		
UnlinkAwsCertification	個々のプロファイルから AWS 証明書のリンクを解除する許可を付与	書き込み	expert*		
UpdateCompanyProfile	会社プロファイルを更新するための許可を付与します	書き込み	company*		
UpdateConversationMembers	会話に参加者をさらに追加するための許可を付与します	書き込み	conversation*		
UpdateExpert	エキスパート情報を更新するための許可を付与します	書き込み	expert*		
UpdateListing	リスティングを更新するための許可を付与します	書き込み	listing*		
UpdateRequest	リクエストを更新するための許可を付与します	書き込み	request*		
UploadAttachment	アタッチメントをアップロードするための許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
WithdrawPaymentRequest	支払いリクエストを撤回するための許可を付与します	書き込み	paymentRequest*		
WithdrawProposal	提案を撤回するための許可を付与します	書き込み	proposal*		
WriteReview	エキスパートのレビューを書き込むための許可を付与します	書き込み	seller*		

AWS IQ で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
conversation	`arn:${Partition}:iq:${Region}::conversation/${ConversationId}`	
buyer	`arn:${Partition}:iq:${Region}::buyer/${BuyerId}`	
expert	`arn:${Partition}:iq:${Region}::expert/${ExpertId}`	
call	`arn:${Partition}:iq:${Region}::call/${CallId}`	

リソースタイプ	ARN	条件キー
token	arn:${Partition}:iq:${Region}::token/${TokenId}	
proposal	arn:${Partition}:iq:${Region}::proposal/${ConversationId}/${ProposalId}	
paymentRequest	arn:${Partition}:iq:${Region}::paymentRequest/${ConversationId}/${ProposalId}/${PaymentRequestId}	
paymentSchedule	arn:${Partition}:iq:${Region}::paymentSchedule/${ConversationId}/${ProposalId}/${VersionId}	
seller	arn:${Partition}:iq:${Region}::seller/${SellerAwsAccountId}	
company	arn:${Partition}:iq:${Region}::company/${CompanyId}	
request	arn:${Partition}:iq:${Region}::request/${RequestId}	
listing	arn:${Partition}:iq:${Region}::listing/${ListingId}	
attachment	arn:${Partition}:iq:${Region}::attachment/${AttachmentId}	
permission	arn:${Partition}:iq-permission:${Region}::permission/${PermissionRequestId}	

AWS IQ の条件キー

IQ には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS IQ Permissions のアクション、リソース、および条件キー

AWS IQ Permissions (サービスプレフィックス: iq-permission) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS IQ Permissions で定義されるアクション
- AWS IQ Permissions で定義されるリソースタイプ
- AWS IQ Permissions の条件キー

AWS IQ Permissions で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ApproveAccessGrant	許可リクエストを承認するための許可を付与します	書き込み	permission*		
ApprovePermissionRequest	許可リクエストを承認するための許可を付与します	書き込み	permission*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssumePermissionRole	エキスパートが購入者の AWS リソースにアクセスするために使用できる一連の一時的なセキュリティ認証情報を取得するアクセス許可を付与します	書き込み	permission*		
CreatePermissionRequest	許可リクエストを作成するための許可を付与します	書き込み	permission*		
GetPermissionRequest	許可リクエストを取得するための許可を付与します	読み取り	permission*		
ListPermissionRequests	許可リクエストを一覧表示するための許可を付与します	読み取り	permission*		
RejectPermissionRequest	許可リクエストを拒否するための許可を付与します	書き込み	permission*		
RevokePermissionRequest	以前に承認された許可リクエストを取り消すための許可を付与します	書き込み	permission*		
WithdrawPermissionRequest	承認または拒否されていない許可リクエストを撤回するための許可を付与します	書き込み	permission*		

AWS IQ Permissions で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアク

ションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
permission	`arn:${Partition}:iq-permission:${Region}::permission/${PermissionRequestId}`	

AWS IQ Permissions の条件キー

IQ のアクセス許可には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Kendra のアクション、リソース、および条件キー

Amazon Kendra (サービスプレフィックス: kendra) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Kendra で定義されるアクション
- Amazon Kendra で定義されるリソースタイプ
- Amazon Kendra の条件キー

Amazon Kendra で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateEntitiesToExperience	インデックスにプリンシパルマッピングを配置する許可を付与	書き込み	experience*		
			index*		
AssociatePersonasToEntities	Amazon Kendra エクスペリエンスにアクセスできる AWS SSO ID ソース内のユーザーまたはグループの特定のアクセス許可を定義します。	書き込み	experience*		
			index*		
BatchDeleteDocument	ドキュメントを一括で削除する許可を付与	書き込み	index*		
BatchDeleteFeaturedResultsSet	主要な結果セットを削除する許可を付与	書き込み	featured-results-set*		
			index*		
BatchGetDocumentStatus	ドキュメントのステータスをバッチ取得する許可を付与	読み込み	index*		
BatchPutDocument	ドキュメントを一括で配置する許可を付与	書き込み	index*		
ClearQuerySuggestions	これまでに生成されたインデックスの候補をクリアする許可を付与	書き込み	index*		
CreateAccessControlConfiguration	アクセスコントロール設定を作成する許可を付与	書き込み	index*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateDataSource	データソースを作成するアクセス許可を付与	書き込み	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExperience	検索アプリケーションなどの Amazon Kendra エクスペリエンスを作成します	書き込み	index*		
CreateFaq	よくある質問を作成する許可を付与	書き込み	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFeaturedResultsSet	主要な結果セットを作成する許可を付与	書き込み	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateIndex	インデックスを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateQuerySuggestionsBlockList	QuerySuggestions ブロックリストを作成する許可を付与	書き込み	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateThesaurus	類語辞典を作成する許可を付与	書き込み	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessControlConfiguration	アクセスコントロール設定を削除する許可を付与	書き込み	access-control-configuration*		
			index*		
DeleteDataSource	データソースを削除するアクセス許可を付与	書き込み	data-source*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			index*		
DeleteExperience	検索アプリケーションなどの Amazon Kendra エクスペリエンスを削除します	書き込み	experience*		
			index*		
DeleteFaq	よくある質問を削除する許可を付与	書き込み	faq*		
			index*		
DeleteIndex	インデックスを削除する許可を付与	書き込み	index*		
DeletePrincipalMapping	インデックスからプリンシパルマッピングを削除する許可を付与	書き込み	index*		
			data-source		
DeleteQuerySuggestionsBlockList	QuerySuggestions ブロックリストを削除する許可を付与	書き込み	index*		
			query-suggestions-block-list*		
DeleteThesaurus	類語辞典を削除する許可を付与	書き込み	index*		
			thesaurus*		
DescribeAccessControlConfiguration	アクセスコントロール設定を記述する許可を付与	読み取り	access-control-configuration*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			index*		
DescribeDataSource	データソースを記述するアクセス許可を付与	読み込み	data-source*		
			index*		
DescribeExperience	検索アプリケーションなどの Amazon Kendra エクスペリエンスに関する情報を取得します	読み込み	experience*		
			index*		
DescribeFaq	よくある質問を記述する許可を付与	読み取り	faq*		
			index*		
DescribeFeaturedResultsSet	主要な結果セットを記述する許可を付与	読み取り	featured-results-set*		
			index*		
DescribeIndex	インデックスを記述する許可を付与	読み込み	index*		
DescribePrincipalMapping	インデックスからプリンシパルマッピングを記述する許可を付与	読み込み	index*		
			data-source		
DescribeQuerySuggestionsBlockList	QuerySuggestions ブロックリストを記述する許可を付与	読み込み	index*		
			query-suggestions-block-list*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeQuerySuggestionsConfig	インデックスのクエリ候補設定を記述する許可を付与	読み込み	index*		
DescribeThesaurus	類語辞典を記述する許可を付与	読み取り	index*		
			thesaurus*		
DisassociateEntitiesFromExperience	SSO ID AWS ソースのユーザーまたはグループが Amazon Kendra エクスペリエンスにアクセスできないようにします	書き込み	experience*		
			index*		
DisassociatePersonasFromEntities	Amazon Kendra エクスペリエンスにアクセスできる AWS SSO ID ソース内のユーザーまたはグループの特定のアクセス許可を削除します。	書き込み	experience*		
			index*		
GetQuerySuggestions	クエリプレフィックスの候補を取得する許可を付与	読み込み	index*		
GetSnapshots	検索メトリクスデータを取得します	読み取り	index*		
ListAccessControlConfigurations	オリジンアクセスコントロール設定を一覧表示する許可を付与	リスト	index*		
ListDataSourceSyncJobs	データソース同期ジョブの履歴を取得する許可を付与	リスト	data-source*		
			index*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListDataSources	データソースを一覧表示する許可を付与	リスト	index*		
ListEntityPersonas	Amazon Kendra エクスペリエンスへのアクセス権のあるユーザーおよびグループの特定の許可を一覧表示します	リスト	experience*		
			index*		
ListExperienceEntities	Amazon Kendra エクスペリエンスへのアクセスが許可されている AWS SSO ID ソース内のユーザーまたはグループを一覧表示します。	リスト	experience*		
			index*		
ListExperiences	1 つ以上の Amazon Kendra エクスペリエンスを一覧表示します。検索アプリケーションなどの Amazon Kendra エクスペリエンスを作成できます	リスト	index*		
ListFaqs	よくある質問を一覧表示する許可を付与	リスト	index*		
ListFeaturedResultsSets	主要な結果セットを一覧表示する許可を付与	リスト	index*		
ListGroupsOlderThanOrderingId	注文 ID よりも古いグループを一覧表示する許可を付与	リスト	index*		
			data-source		
ListIndices	インデックスを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListQuerySuggestionsBlockLists	QuerySuggestions ブロックリストを一覧表示する許可を付与	リスト	index*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み込み	data-source		
			faq		
			featured-results-set		
			index		
			query-suggestions-block-list		
			thesaurus		
ListThesauri	類語辞典を一覧表示する許可を付与	リスト	index*		
PutPrincipalMapping	インデックスにプリンシパルマッピングを配置する許可を付与	書き込み	index*		
			data-source		
Query	ドキュメントとよくある質問をクエリする許可を付与	読み取り	index*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
Retrieve	インデックスから関連コンテンツを取得するアクセス許可を付与します	読み取り	index*		
StartDataSourceSyncJob	データソース同期ジョブを開始する許可を付与	書き込み	data-source*		
			index*		
StopDataSourceSyncJob	データソース同期ジョブを停止する許可を付与	書き込み	data-source*		
			index*		
SubmitFeedback	クエリ結果に関するフィードバックを送信する許可を付与	書き込み	index*		
TagResource	指定されたキーと値のペアでリソースにタグを付けるアクセス許可を付与	Tagging	data-source		
			faq		
			featured-results-set		
			index		
			query-suggestions-block-list		
			thesaurus		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	所与のキーを持つタグをリソースから削除する許可を付与	Tagging	data-source		
			faq		
			featured-results-set		
			index		
			query-suggestions-block-list		
			thesaurus		
				aws:TagKeys	
UpdateAccessControlConfiguration	アクセスコントロール設定を更新する許可を付与	書き込み	access-control-configuration*		
			index*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateDataSource	データソースを更新する権限を付与	書き込み	data-source*		
			index*		
UpdateExperience	検索アプリケーションなどの Amazon Kendra エクスペリエンスを更新します	書き込み	index*		
UpdateFeaturedResultsSet	主要な結果セットを更新する許可を付与	書き込み	featured-results-set*		
			index*		
UpdateIndex	インデックスを更新する許可を付与	書き込み	index*		
UpdateQuerySuggestionsBlockList	QuerySuggestions ブロックリストを更新する許可を付与	書き込み	index*		
			query-suggestions-block-list*		
UpdateQuerySuggestionsConfig	インデックスのクエリ候補設定を更新する許可を付与	書き込み	index*		
UpdateThesaurus	類語辞典を更新する許可を付与	書き込み	index*		
			thesaurus*		

Amazon Kendra で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
index	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}	aws:ResourceTag/${TagKey}
data-source	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/data-source/${DataSourceId}	aws:ResourceTag/${TagKey}
faq	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/faq/${FaqId}	aws:ResourceTag/${TagKey}
experience	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/experience/${ExperienceId}	
thesaurus	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/thesaurus/${ThesaurusId}	aws:ResourceTag/${TagKey}
query-suggestions-block-list	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/query-suggestions-block-list/${QuerySuggestionsBlockListId}	aws:ResourceTag/${TagKey}
featured-results-set	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/featured-results-set/${FeaturedResultsSetId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
access-control-configuration	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/access-control-configuration/${AccessControlConfigurationId}	

Amazon Kendra の条件キー

Amazon Kendra では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon Kendra インテリジェントランキングのアクション、リソース、および条件キー

Amazon Kendra インテリジェントランキング (サービスプレフィックス: kendra-ranking) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Kendra インテリジェントランキングで定義されるアクション
- Amazon Kendra インテリジェントランキングで定義されるリソースタイプ
- Amazon Kendra インテリジェントランキングの条件キー

Amazon Kendra インテリジェントランキングで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateRescoreExecutionPlan	RescoreExecutionPlan を作成するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteRescoreExecutionPlan	RescoreExecutionPlan を削除するアクセス許可を付与	書き込み	rescore-execution-plan*		
DescribeRescoreExecutionPlan	RescoreExecutionPlan を説明するアクセス許可を付与	読み取り	rescore-execution-plan*		
ListRescoreExecutionPlans	すべての RescoreExecutionPlan を一覧表示するアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	rescore-execution-plan		
Rescore	Kendra インテリジェントランキングでドキュメントを再スコアリングするアクセス許可を付与	読み取り	rescore-execution-plan*		
TagResource	指定されたキーと値のペアでリソースにタグを付けるアクセス許可を付与	Tagging	rescore-execution-plan		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	所与のキーを持つタグをリソースから削除する許可を付与	Tagging	rescore-execution-plan		
				aws:TagKeys	
UpdateRescoreExecutionPlan	RescoreExecutionPlan を更新するアクセス許可を付与	書き込み	rescore-execution-plan*		

Amazon Kendra インテリジェントランキングで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
rescore-execution-plan	arn:${Partition}:kendra-ranking:${Region}:${Account}:rescore-execution-plan/${RescoreExecutionPlanId}	aws:ResourceTag/${TagKey}

Amazon Kendra インテリジェントランキングの条件キー

Amazon Kendra インテリジェントランキングは、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon Keyspaces (Apache Cassandra 向け) のアクション、リソース、および条件キー

Amazon Keyspaces (Apache Cassandra 向け) (サービスプレフィックス: `cassandra`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Keyspaces (Apache Cassandra 向け) で定義されるアクション
- Amazon Keyspaces (Apache Cassandra 向け) で定義されるリソースタイプ
- Amazon Keyspaces (Apache Cassandra 向け) の条件キー

Amazon Keyspaces (Apache Cassandra 向け) で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイ

プが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
Alter	キースペースまたはテーブルを変更する許可を付与。	書き込み	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AlterMultiRegionResource	マルチリージョンのキースペースまたはテーブルを変更する許可を付与	書き込み	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
Create	キースペースまたはテーブルを作成する許可を付与。	書き込み	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMultiRegionResource	マルチリージョンのキースペースまたはテーブルを作成する許可を付与	書き込み	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
Drop	キースペースまたはテーブルを削除する許可を付与。	書き込み	keyspace		
			table		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DropMultiRegionResource	マルチリージョンのキースペースまたはテーブルを削除する許可を付与	書き込み	keyspace		
			table		
GetRecords	特定のシャードから CDC ストリームレコードを取得する許可を付与	読み取り	stream*		
GetShardIterator	シャードイテレータを返すアクセス許可を付与します。	読み取り	stream*		
GetStream	シャードの構成など、CDC ストリームに関する情報を返すアクセス許可を付与します	読み取り	stream*		
ListStreams	現在のアカウントとエンドポイントに関連付けられた CDC ストリーム ARNs の配列を返すアクセス許可を付与します	リスト			
Modify	テーブル内のデータを挿入、更新、または削除する許可を付与。	書き込み	table*		
ModifyMultiRegionResource	マルチリージョンのテーブル内のデータに対し INSERT、UPDATE、または DELETE の処理を行う許可を付与	書き込み	table*		
Restore	バックアップからテーブルを復元する許可を付与	書き込み	table*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RestoreMultiRegionTable	バックアップからマルチリージョンのテーブルを復元する許可を付与	書き込み	table*		
Select	テーブルからデータを選択するためのアクセス許可を付与します。	読み取り	table*		
SelectMultiRegionResource	マルチリージョンのテーブルからデータを SELECT する許可を付与	読み取り	table*		
TagMultiRegionResource	マルチリージョンのキースペースまたはテーブルにタグを付ける許可を付与	Tagging	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	キースペース、テーブル、またはストリームにタグを付けるアクセス許可を付与します	Tagging	keyspace		
			stream		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UnTagMultiRegionResource	マルチリージョンのキースペースまたはテーブルのタグを削除する許可を付与	Tagging	keyspace		
			table		
				aws:TagKeys	
UntagResource	キースペース、テーブル、またはストリームのタグを解除するアクセス許可を付与します	Tagging	keyspace		
			stream		
			table		
				aws:TagKeys	
UpdatePartitioner	システムテーブル内のパーティショナーを更新するアクセス許可を付与します	書き込み	table*		

Amazon Keyspaces (Apache Cassandra 向け) で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
keyspace	`arn:${Partition}:cassandra:${Region}:${Account}:/keyspace/${KeyspaceName}/`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
table	arn:${Partition}:cassandra:${Region}:${Account}:/keyspace/${KeyspaceName}/table/${TableName}	aws:ResourceTag/${TagKey}
stream	arn:${Partition}:cassandra:${Region}:${Account}:/keyspace/${KeyspaceName}/table/${TableName}/stream/${StreamLabel}	aws:ResourceTag/${TagKey}

Amazon Keyspaces (Apache Cassandra 向け) の条件キー

Amazon Keyspaces (Apache Cassandra 向け) は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアのプレゼンスに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいてアクションをフィルタリングします	ArrayOfString

Amazon Kinesis Analytics のアクション、リソース、および条件キー

Amazon Kinesis Analytics (サービスプレフィックス: kinesisanalytics) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Kinesis Analytics で定義されるアクション
- Amazon Kinesis Analytics で定義されるリソースタイプ
- Amazon Kinesis Analytics の条件キー

Amazon Kinesis Analytics で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddApplicationInput	アプリケーションに入力を追加する許可を付与	書き込み	application*		
AddApplicationOutput	アプリケーションに出力を追加する許可を付与	Write	application*		
AddApplicationReferenceDataSource	アプリケーションにリファレンスデータソースを追加する許可を付与	書き込み	application*		
CreateApplication	アプリケーションを作成する許可を付与	書き込み		aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
DeleteApplication	アプリケーションを削除する許可を付与	書き込み	application*		
DeleteApplicationOutput	アプリケーションで指定した出力を削除する許可を付与	Write	application*		
DeleteApplicationReferenceDataSource	アプリケーションの指定されたリファレンスデータソースを削除する許可を付与	書き込み	application*		
DescribeApplication	指定されたアプリケーションを説明する許可を付与	読み取り	application*		
DiscoverInputSchema	アプリケーションの入力スキーマを検出する許可を付与	読み取り			
GetApplicationState [許可のみ]	Kinesis Data Analytics コンソールに、Kinesis Data Analytics SQL ランタイムアプリケーションのストリーム結果を表示するアクセス許可を付与	読み取り	application*		
ListApplications	アカウントのアプリケーションを一覧表示する許可を付与	リスト			
ListTagsForResource	アプリケーションに関連付けられているタグを取得する許可を付与	Read	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartApplication	アプリケーションを起動する許可を付与	Write	application*		
StopApplication	アプリケーションを停止する許可を付与	Write	application*		
TagResource	アプリケーションにタグを追加する許可を付与	タグ付け	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	アプリケーションから指定したタグを削除する許可を付与	タグ付け	application*		
				aws:TagKeys	
UpdateApplication	アプリケーションを更新する許可を付与	書き込み	application*		

Amazon Kinesis Analytics で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
application	arn:${Partition}:kinesisanalytics:${Region}:${Account}:application/${ApplicationName}	aws:ResourceTag/${TagKey}

Amazon Kinesis Analytics の条件キー

Amazon Kinesis Analytics は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	各タグの値のセットによってアクセスをフィルタリング	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値によってアクセスをフィルタリング	String
aws:TagKeys	リクエスト内の必須タグキーの存在によってアクセスをフィルタリング	ArrayOfString

Amazon Kinesis Analytics V2 のアクション、リソース、および条件キー

Amazon Kinesis Analytics V2 (サービスプレフィックス: kinesisanalytics) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Kinesis Analytics V2 で定義されるアクション
- Amazon Kinesis Analytics V2 で定義されるリソースタイプ
- Amazon Kinesis Analytics V2 の条件キー

Amazon Kinesis Analytics V2 で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddApplicationCloudWatchLoggingOption	アプリケーションに CloudWatch ログオプションを追加する許可を付与	Write	application*		
AddApplicationInput	アプリケーションに入力を追加する許可を付与	Write	application*		
AddApplicationInputProcessingConfiguration	アプリケーションに入力処理設定を追加する許可を付与	Write	application*		
AddApplicationOutput	アプリケーションに出力を追加する許可を付与	Write	application*		
AddApplicationRefe	アプリケーションにリファレンスデータソースを追加する許可を付与	Write	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
renceDataSource					
AddApplicationVpcConfiguration	アプリケーションに VPC 設定を追加する許可を付与	Write	application*		
CreateApplication	アプリケーションを作成する許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateApplicationPresignedUrl	アプリケーションの拡張機能に接続するために使用できる URL を作成して返すアクセス許可を付与する	Read	application*		
CreateApplicationSnapshot	アプリケーションのスナップショットを作成する許可を付与	Write	application*		
DeleteApplication	アプリケーションを削除する許可を付与	Write	application*		
DeleteApplicationCloudWatchLoggingOption	アプリケーションで指定した CloudWatch ログオプションを削除する許可を付与	Write	application*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteApplicationInputProcessingConfiguration	アプリケーションで指定した入力処理設定を削除する許可を付与	Write	application*		
DeleteApplicationOutput	アプリケーションで指定した出力を削除する許可を付与	Write	application*		
DeleteApplicationReferenceDataSource	アプリケーションの指定されたリファレンスデータソースを削除する許可を付与	Write	application*		
DeleteApplicationSnapshot	アプリケーションのスナップショットを削除する許可を付与	Write	application*		
DeleteApplicationVpcConfiguration	アプリケーションで指定した VPC 設定を削除する許可を付与	Write	application*		
DescribeApplication	指定されたアプリケーションを説明する許可を付与	読み取り	application*		
DescribeApplicationOperation	アプリケーションのアプリケーション操作を記述する許可を付与する	読み取り	application*		
DescribeApplicationSnapshot	アプリケーションのスナップショットを記述する許可を付与	読み取り	application*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeApplicationVersion	アプリケーションのアプリケーションバージョンを記述する許可を付与	読み取り	application*		
DiscoverInputSchema	アプリケーションの入力スキーマを検出する許可を付与	読み取り			iam:PassRole
ListApplicationOperations	アプリケーションのアプリケーション操作を一覧表示する許可を付与する	読み取り	application*		
ListApplicationSnapshots	アプリケーションのスナップショットを一覧表示する許可を付与	読み取り	application*		
ListApplicationVersions	アプリケーションのアプリケーションバージョンを一覧表示する許可を付与	読み取り	application*		
ListApplications	アカウントのアプリケーションを一覧表示する許可を付与	リスト			
ListTagsForResource	アプリケーションに関連付けられているタグを取得する許可を付与	読み取り	application*		
RollbackApplication	アプリケーションでロールバックオペレーションを実行する許可を付与	書き込み	application*		
StartApplication	アプリケーションを起動する許可を付与	Write	application*		
StopApplication	アプリケーションを停止する許可を付与	Write	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagResource	アプリケーションにタグを追加する許可を付与	タグ付け	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	アプリケーションから指定したタグを削除する許可を付与	タグ付け	application*		
				aws:TagKeys	
UpdateApplication	アプリケーションを更新する許可を付与	書き込み	application*		
UpdateApplicationMaintenanceConfiguration	アプリケーションのメンテナンス設定を更新する許可を付与	書き込み	application*		

Amazon Kinesis Analytics V2 で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
application	arn:${Partition}:kinesisanalytics:${Region}:${Account}:application/${ApplicationName}	aws:ResourceTag/${TagKey}

Amazon Kinesis Analytics V2 の条件キー

Amazon Kinesis Analytics V2 では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	各タグの値のセットによってアクセスをフィルタリング	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値によってアクセスをフィルタリング	String
aws:TagKeys	リクエスト内の必須タグキーの存在によってアクセスをフィルタリング	ArrayOfString

Amazon Kinesis Data Streams のアクション、リソース、および条件キー

Amazon Kinesis Data Streams (サービスプレフィックス: kinesis) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Kinesis Data Streams で定義されるアクション
- Amazon Kinesis Data Streams で定義されるリソースタイプ
- Amazon Kinesis Data Streams の条件キー

Amazon Kinesis Data Streams で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddTagsToStream	指定した Amazon Kinesis ストリームのタグを追加または更新する許可を付与します 各ストリームには最大 50 個のタグを含めることができます	Tagging	stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateStream	Amazon Kinesis ストリームを作成する許可を付与します	書き込み	stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DecreaseStreamRetentionPeriod	ストリームの保持期間 (データレコードがストリームに追加されてからアクセス可能な期間) を短縮する許可を付与します	書き込み	stream*	aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	指定されたストリームまたはコンシューマーに関連付けられたリソースポリシーを削除するためのアクセス許可を付与	書き込み	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	
DeleteStream	ストリーム、シャード、データを削除する許可を付与します	書き込み	stream*	aws:ResourceTag/${TagKey}	
DeregisterStreamConsumer	Kinesis データストリームでストリームコンシューマーの登録解除する許可を付与します	書き込み	consumer*	aws:ResourceTag/${TagKey}	
DescribeLimits	アカウントのシャード制限と使用状況を説明する許可を付与します	読み取り			
DescribeStream	指定されたストリームを説明する許可を付与します	読み取り	stream*	aws:ResourceTag/${TagKey}	
DescribeStreamConsumer	登録済みストリームコンシューマーの説明を取得する許可を付与します	読み取り	consumer*	aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeStreamSummary	指定された Kinesis データストリームの概要説明 (シャードリストなし) を提供する許可を付与します	読み取り	stream*	aws:ResourceTag/${TagKey}	
DisableEnhancedMonitoring	拡張モニタリングを無効にする許可を付与します	書き込み			
EnableEnhancedMonitoring	シャードレベルメトリクスの拡張 Kinesis データストリームモニタリングを有効にする許可を付与します	書き込み			
GetRecords	シャードからデータレコードを取得するための許可を付与します	読み取り	stream*	aws:ResourceTag/${TagKey}	
GetResourcePolicy	指定されたストリームまたはコンシューマーに関連付けられたリソースポリシーを取得するためのアクセス許可を付与	読み取り	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	
GetShardIterator	シャードイテレーターを取得する許可を付与します シャードイテレーターはリクエスタに返されてから 5 分後に有効期限が切れます	読み取り	stream*	aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
IncreaseStreamRetentionPeriod	ストリームの保持期間 (データレコードがストリームに追加されてからアクセス可能な期間) を延長する許可を付与します	書き込み	stream*	aws:ResourceTag/${TagKey}	
ListShards	ストリーム内のシャードを一覧表示する許可を付与し、各シャードに関する情報を提供します	リスト	stream*	aws:ResourceTag/${TagKey}	
ListStreamConsumers	拡張ファンアウトを使用して Kinesis ストリームからデータを受け取るために登録されたストリームコンシューマーを一覧表示する許可を付与し、各コンシューマーに関する情報を提供します	リスト	stream*	aws:ResourceTag/${TagKey}	
ListStreams	ストリームを一覧表示する許可を付与します	リスト			
ListTagsForResource	指定された Amazon Kinesis リソースのタグを一覧表示するアクセス許可を付与します	読み取り	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	
ListTagsForStream	指定済み Amazon Kinesis ストリームのタグを一覧表示する許可を付与します	読み取り	stream*	aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
MergeShards	ストリーム内で隣接する 2 つのシャードをマージし、それらを 1 つのシャードに結合して、データの取り込みと転送する場合のストリーム容量を減らす許可を付与します	書き込み	stream*	aws:ResourceTag/${TagKey}	
PutRecord	プロデューサーから Amazon Kinesis ストリームに単一のデータレコードを書き込む許可を付与します	書き込み	stream*	aws:ResourceTag/${TagKey}	
PutRecords	1 回の呼び出しで、プロデューサーから Amazon Kinesis ストリームに複数のデータレコードを書き込む許可を付与します (PutRecords リクエストとも呼びます)	書き込み	stream*	aws:ResourceTag/${TagKey}	
PutResourcePolicy	指定されたストリームまたはコンシューマーにリソースポリシーをアタッチするためのアクセス許可を付与	書き込み	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RegisterStreamConsumer	Kinesis データストリームでストリームコンシューマーを登録する許可を付与します	書き込み	stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
RemoveTagsFromStream	指定済み Kinesis データストリームからタグを削除する許可を付与します 削除済みタグは削除され、このオペレーションが正常に完了した後は復元できません	Tagging	stream*	aws:TagKeys aws:ResourceTag/${TagKey}	
SplitShard	データの取り込みと転送する場合のストリーム容量を増やすために、Kinesis データストリームでシャードを 2 つの新しいシャードに分割する許可を付与します	書き込み	stream*	aws:ResourceTag/${TagKey}	
StartStreamEncryption	指定されたストリームの KMS AWS キーを使用してサーバー側の暗号化を有効化または更新するアクセス許可を付与します	書き込み	kmsKey*		
			stream*	aws:ResourceTag/${TagKey}	
StopStreamEncryption	指定済ストリームに対するサーバー側の暗号化を無効にする許可を付与します	書き込み	kmsKey*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			stream*	aws:ResourceTag/${TagKey}	
SubscribeToShard	ファンアウトを拡張した特定のシャードのリスニング許可を付与します	読み取り	consumer*	aws:ResourceTag/${TagKey}	
TagResource	指定された Amazon Kinesis リソースのタグを追加または更新するアクセス許可を付与します。各リソースには最大 50 個のタグを含めることができます	Tagging	consumer*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	指定された Kinesis データリソースからタグを削除するアクセス許可を付与します。削除済みタグは削除され、このオペレーションが正常に完了した後は復元できません	Tagging	consumer*	aws:TagKeys aws:ResourceTag/${TagKey}	
			stream*	aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateShardCount	指定済みストリームのシャード数を指定済みシャード数に更新する許可を付与します	書き込み			
UpdateStreamMode	データストリームのキャパシティーモードを更新する許可を付与します	書き込み			

Amazon Kinesis Data Streams で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
stream	arn:${Partition}:kinesis:${Region}:${Account}:stream/${StreamName}	aws:ResourceTag/${TagKey}
consumer	arn:${Partition}:kinesis:${Region}:${Account}:${StreamType}/${StreamName}/consumer/${ConsumerName}:${ConsumerCreationTimpstamp}	
kmsKey	arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}	

Amazon Kinesis Data Streams の条件キー

Amazon Kinesis Data Streams は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

Amazon Kinesis Firehose のアクション、リソース、および条件キー

Amazon Kinesis Firehose (サービスプレフィックス: `firehose`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Kinesis Firehose で定義されるアクション
- Amazon Kinesis Firehose で定義されるリソースタイプ
- Amazon Kinesis Firehose の条件キー

Amazon Kinesis Firehose で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateDeliveryStream	配信ストリームを作成するアクセス許可を付与します	書き込み	deliverystream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDeliveryStream	配信ストリームとそのデータを削除する許可を付与。	書き込み	deliverystream*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeDeliveryStream	指定された配信ストリームを説明するアクセス許可を付与し、ステータスを取得します。	読み込み	deliverystream*		
ListDeliveryStreams	配信ストリームを一覧表示するアクセス許可を付与します	リスト			
ListTagsForDeliveryStream	指定した配信ストリームのタグを一覧表示するアクセス許可を付与します	リスト	deliverystream*		
PutRecord	Amazon Kinesis Firehose 配信ストリームに 1 つのデータレコードを書き込むアクセス許可を付与します	書き込み	deliverystream*		
PutRecordBatch	1 回の呼び出しで配信ストリームに複数のデータレコードを書き込むアクセス許可を付与します。これにより、単一のレコードを書き込むよりプロデューサーあたりのスループットが高くなります	書き込み	deliverystream*		
StartDeliveryStreamEncryption	配信ストリームのサーバー側暗号化 (SSE) を有効にするアクセス許可を付与します	書き込み	deliverystream*		
StopDeliveryStreamEncryption	指定された配信ストリームの指定された送信先を無効にするアクセス許可を付与します	書き込み	deliverystream*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagDeliveryStream	指定された配信ストリームのタグを追加または更新するアクセス許可を付与します	Tagging	deliverystream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagDeliveryStream	指定された配信ストリームからタグを削除するアクセス許可を付与します	Tagging	deliverystream*		
				aws:TagKeys	
UpdateDestination	指定された配信ストリームの指定された送信先を更新するアクセス許可を付与します	書き込み	deliverystream*		

Amazon Kinesis Firehose で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
deliverystream	arn:${Partition}:firehose:${Region}:${Account}:deliverystream/${DeliveryStreamName}	aws:ResourceTag/${TagKey}

Amazon Kinesis Firehose の条件キー

Amazon Kinesis Firehose では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon Kinesis Video Streams のアクション、リソース、および条件キー

Amazon Kinesis Video Streams (サービスプレフィックス: kinesisvideo) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Kinesis Video Streams で定義されるアクション
- Amazon Kinesis Video Streams で定義されるリソースタイプ
- Amazon Kinesis Video Streams の条件キー

Amazon Kinesis Video Streams で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ConnectAsMaster	エンドポイントで指定されたシグナリングチャネルにマスターとして接続する許可を付与。	書き込み	channel*		
ConnectAsViewer	エンドポイントで指定されたシグナリングチャネルに表示者として接続する許可を付与。	書き込み	channel*		
CreateSignalingChannel	シグナリングチャネルを作成する許可を付与。	書き込み	channel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStream	Kinesis ビデオストリームを作成する許可を付与。	書き込み	stream*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteEdgeConfiguration	Kinesis Video Stream のエッジ設定を削除するアクセス許可を付与します	書き込み	stream*		
DeleteSignalingChannel	既存のシグナリングチャネルを削除する許可を付与。	書き込み	channel*		
DeleteStream	既存の Kinesis ビデオストリームを削除する許可を付与。	書き込み	stream*		
DescribeEdgeConfiguration	Kinesis Video Stream のエッジ設定を記述する許可を付与	読み取り	stream*		
DescribeImageGenerationConfiguration	Kinesis Video Streams のイメージ生成設定を記述する許可を付与	読み取り	stream*		
DescribeMappedResourceConfiguration	Kinesis ビデオストリームにマッピングされたリソースを記述するための許可を付与します	リスト	stream*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeMediaStorageConfiguration	シグナリングチャネルのメディアストレージ設定を記述するための許可を付与します	読み取り	channel*		
DescribeNotificationConfiguration	Kinesis Video Streams の通知設定を記述する許可を付与	読み取り	stream*		
DescribeSignalingChannel	指定したシグナリングチャネルを記述する許可を付与。	リスト	channel*		
DescribeStream	指定した Kinesis ビデオストリームを記述する許可を付与。	リスト	stream*		
GetClip	ビデオストリームからメディアクリップを取得する許可を付与。	読み込み	stream*		
GetDASHStreamingSessionURL	MPEG-DASH ビデオストリーミング用の URL を作成する許可を付与。	読み込み	stream*		
GetDataEndpoint	Kinesis Video Streams のメディアデータの読み取りまたは書き込みを行うために、指定されたストリームのエンドポイントを取得する許可を付与。	読み込み	stream*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetHLSStreamingSessionURL	HLS ビデオストリーミング用の URL を作成する許可を付与。	読み込み	stream*		
GetIceServerConfig	ICE サーバー設定を取得する許可を付与。	読み取り	channel*		
GetImages	Kinesis Video Streams から生成された画像を取得する許可を付与	読み取り	stream*		
GetMedia	Kinesis ビデオストリームのメディアコンテンツを返すアクセス許可を付与します。	読み込み	stream*		
GetMediaForFragmentList	永続的ストレージからのみメディアデータを読み取って返すアクセス許可を付与します。	読み込み	stream*		
GetSignalingChannelEndpoint	シグナリングチャネルのプロトコルとロールの指定された組み合わせのエンドポイントを取得する許可を付与。	読み取り	channel*		
JoinStorageSession	チャネルのストレージセッションに参加するための許可を付与します	書き込み	channel*		
JoinStorageSessionAsViewer	ビュアーとしてチャネルのストレージセッションに参加するための許可を付与する	書き込み	channel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListEdgeAgentConfigurations	エッジエージェントの設定を一覧表示するアクセス許可を付与します	リスト			
ListFragments	指定された範囲で、ページ分割トークンまたはセレクタータイプに基づいてアーカイブストレージからのフラグメントを一覧表示する許可を付与。	リスト	stream*		
ListSignalingChannels	シグナリングチャネルを一覧表示する許可を付与。	リスト			
ListStreams	Kinesis ビデオストリームを一覧表示する許可を付与。	リスト			
ListTagsForResource	リソースに関連付けられているタグを取得する許可を付与。	読み込み	channel		
			stream		
ListTagsForStream	Kinesis ビデオストリームに関連付けられているタグを取得する許可を付与。	読み込み	stream*		
PutMedia	Kinesis ビデオストリームにメディアデータを送信する許可を付与。	書き込み	stream*		
SendAlexaOfferToMaster	Alexa SDP オファーをマスターに送信する許可を付与。	書き込み	channel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartEdgeConfigurationUpdate	Kinesis Video Stream のエッジ設定の更新を開始する許可を付与	書き込み	stream*		
TagResource	リソースにタグのセットをアタッチする許可を付与。	タグ付け	channel		
			stream		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagStream	Kinesis ビデオストリームにタグのセットをアタッチする許可を付与。	タグ付け	stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースから 1 つ以上のタグを削除する許可を付与。	タグ付け	channel		
			stream		
				aws:TagKeys	
UntagStream	Kinesis ビデオストリームから 1 つ以上のタグを削除する許可を付与。	タグ付け	stream*		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateDataRetention	Kinesis ビデオストリームのデータ保持期間を更新する許可を付与。	書き込み	stream*		
UpdateImageGenerationConfiguration	Kinesis Video Streams のイメージ生成設定を更新する許可を付与	書き込み	stream*		
UpdateMediaStorageConfiguration	シグナリングチャネルとストリーム間のマッピングを作成または更新するための許可を付与します	書き込み	channel*		
UpdateNotificationConfiguration	Kinesis Video Streams の通知設定を更新する許可を付与	書き込み	stream*		
UpdateSignalingChannel	既存のシグナリングチャネルを更新する許可を付与。	書き込み	channel*		
UpdateStream	既存の Kinesis ビデオストリームを更新する許可を付与。	書き込み	stream*		

Amazon Kinesis Video Streams で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
stream	arn:${Partition}:kinesisvideo:${Region}:${Account}:stream/${StreamName}/${CreationTime}	aws:ResourceTag/${TagKey}
channel	arn:${Partition}:kinesisvideo:${Region}:${Account}:channel/${ChannelName}/${CreationTime}	aws:ResourceTag/${TagKey}

Amazon Kinesis Video Streams の条件キー

Amazon Kinesis Video Streams は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	各タグで許可されている値のセットに基づいてリクエストをフィルタリングします。	String
aws:ResourceTag/${TagKey}	ストリームに関連付けられているタグ値に基づいてアクションをフィルタリングします。	String
aws:TagKeys	リクエスト内の必須のタグキーの存在に基づいてリクエストをフィルタリングします。	ArrayOfString

AWS Lake Formation のアクション、リソース、および条件キー

AWS Lake Formation (サービスプレフィックス: lakeformation) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Lake Formation で定義されるアクション
- AWS Lake Formation で定義されるリソースタイプ
- AWS Lake Formation の条件キー

AWS Lake Formation で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddLFTagsToResource	Lake Formation タグをカタログリソースにアタッチする許可を付与	Tagging			
BatchGrantPermissions	バッチ内の 1 つ以上のプリンシパルに対し、データレイクへのアクセス許可を付与する	権限の管理			
BatchRevokePermissions	バッチ内の 1 つ以上のプリンシパルにおいて、データレイクへのアクセス許可を取り消すためのアクセス許可を付与する	権限の管理			
CancelTransaction	指定されたトランザクションをキャンセルする許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CommitTransaction	指定されたトランザクションをコミットする許可を付与	書き込み			
CreateDataCellsFilter	Lake Formation データセルフィルターを作成する許可を付与	書き込み			
CreateLFTag	Lake Formation タグを作成する許可を付与	書き込み			
CreateLFTagExpression	Lake Formation タグ式を作成する許可を付与	書き込み			
CreateLakeFormationIdentityCenterConfiguration	Lake Formation と IAM Identity Center 接続を作成して、IAM Identity Center ユーザーとグループが Data Catalog リソースにアクセスする許可を付与する	書き込み			
CreateLakeFormationOptIn	指定されたデータベース、テーブル、プリンシパルに対して Lake Formation の許可を適用する許可を付与する	書き込み			
DeleteDataCellsFilter	Lake Formation データセルフィルターを削除する許可を付与	書き込み			
DeleteLFTag	Lake Formation タグを削除する許可を付与	書き込み			
DeleteLFTagExpression	Lake Formation 式を削除する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteLakeFormationIdentityCenterConfiguration	Lake Formation との IAM Identity Center 接続を削除する許可を付与する	書き込み			
DeleteLakeFormationOptIn	指定されたデータベース、テーブル、プリンシパルの Lake Formation の許可の適用を削除する許可を付与する	書き込み			
DeleteObjectsOnCancel	トランザクションがキャンセルされた場合に、指定されたオブジェクトを削除する許可を付与	書き込み			
DeregisterResource	登録された場所の登録を解除するためのアクセス許可を付与する	書き込み			
DescribeLakeFormationIdentityCenterConfiguration	Lake Formation との IAM Identity Center 接続を記述する許可を付与する	読み取り			
DescribeResource	登録された場所について詳細表示するためのアクセス許可を付与する	読み取り			
DescribeTransaction	指定されたトランザクションのステータスを取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ExtendTransaction	指定されたトランザクションのタイムアウトを延長する許可を付与	書き込み			
GetDataAccess	仮想データレイクへのアクセス許可を付与する	書き込み		lakeformation:EnabledOnlyForMetaDataAccess	
GetDataCellsFilter	Lake Formation データセルフィルターを取得するための許可を付与します	読み取り			
GetDataLakePrincipal	呼び出し元プリンシパルのアイデンティティを取得する許可を付与する	読み取り			
GetDataLakeSettings	データレイクの管理者や、データベースおよびテーブルでのデフォルトのアクセス許可のリストなど、データレイク設定を取得するためのアクセス許可を付与する	読み取り			
GetEffectivePermissionsForPath	指定されたパスのリソースにアタッチされた許可を取得する許可を付与	読み取り			
GetLFTag	Lake Formation タグを取得する許可を付与	読み取り			
GetLFTagExpression	Lake Formation タグ式を取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetQueryState	指定されたクエリの状態を取得する許可を付与	読み取り			lakeformation:StartQueryPlanning
GetQueryStatistics	指定されたクエリの統計を取得する許可を付与	読み取り			lakeformation:StartQueryPlanning
GetResourceLFTags	カタログリソースにおいてLakeFormation タグを取得するためのアクセス許可を付与する	読み取り			
GetTableObjects	テーブルからオブジェクトを取得する許可を付与	読み取り			
GetWorkUnitResults	指定されたワークユニットの結果を取得する許可を付与	読み取り			lakeformation:GetWorkUnits lakeformation:StartQueryPlanning
GetWorkUnits	指定されたクエリのワークユニットを取得する許可を付与	読み取り			lakeformation:StartQueryPlanning
GrantPermissions	プリンシパルにデータレイクへのアクセス許可を付与する	権限の管理			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListDataCellsFilter	セルのフィルターを一覧表示する許可を付与	リスト			
ListLFTagExpressions	Lake Foramtion タグ式を一覧表示する許可を付与	読み取り			
ListLFTags	Lake Formation タグを一覧表示する許可を付与	読み取り			
ListLakeFormationOptIns	Lake Formation の許可を適用するようオプトインされているリソースとプリンシパルの現在のリストを取得する許可を付与する	リスト			
ListPermissions	プリンシパルまたはリソースによってフィルタリングされたアクセス許可をリストするための許可を付与する。	リスト			
ListResources	登録された場所をリストするためのアクセス許可を付与する	リスト			
ListTableStorageOptimizers	管理テーブルのすべてのストレージオプティマイザーを一覧表示する許可を付与	リスト			
ListTransactions	システム内のすべてのトランザクションを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutDataLakeSettings	データレイク管理者や、データベースおよびテーブルでのデフォルトのアクセス許可のリストなど、データレイク設定を上書きするためのアクセス許可を付与する	権限の管理			
RegisterResource	Lake Formation によって管理される新しい場所を登録するためのアクセス許可を付与する	書き込み			
RegisterResourceWithPrivilegedAccess	Lake Formation が管理する新しい場所を特権アクセスで登録する許可を付与	書き込み			
RemoveLFTagsFromResource	カタログリソースから LakeFormation タグを削除するためのアクセス許可を付与する	Tagging			
RevokePermissions	プリンシパルにおいてデータレイクへのアクセス許可を取り消すためのアクセス許可を付与する	権限の管理			
SearchDatabasesByLFTags	Lake Formation タグが付いたカタログデータベースを一覧表示する許可を付与	読み取り			
SearchTablesByLFTags	Lake Formation タグが付いたカタログテーブルを一覧表示する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartQueryPlanning	指定されたクエリの計画を開始する許可を付与	書き込み			
StartTransaction	新しいトランザクションを開始する許可を付与	書き込み			
UpdateDataCellsFilter	Lake Formation データセルフィルターを更新するための許可を付与します	書き込み			
UpdateLFTag	Lake Formation タグを更新する許可を付与	書き込み			
UpdateLFTagExpression	Lake Formation 式を更新する許可を付与	書き込み			
UpdateLakeFormationIdentityCenterConfiguration	IAM Identity Center 接続パラメータを更新する許可を付与する	書き込み			
UpdateResource	登録された場所を更新するためのアクセス許可を付与する	書き込み			
UpdateTableObjects	指定されたオブジェクトをテーブルに追加する、またはテーブルから削除する許可を付与	書き込み			
UpdateTableStorageOptimizer	管理テーブルのストレージオプティマイザーの設定を更新する許可を付与	書き込み			

AWS Lake Formation で定義されるリソースタイプ

AWS Lake Formation は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Lake Formation へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Lake Formation の条件キー

AWS Lake Formation では、IAM ポリシーの `Condition`要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
lakeformation:EnabledOnlyForMetaDataAccess	ロールのアイデンティティベースのポリシー用に設定されたキーの存在によってアクセスをフィルタリングします	Bool

AWS Lambda のアクション、リソース、および条件キー

AWS Lambda (サービスプレフィックス: `lambda`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Lambda で定義されるアクション
- AWS Lambda で定義されるリソースタイプ
- AWS Lambda の条件キー

AWS Lambda で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AddLayerVersionPermission	AWS Lambda レイヤーのバージョンのリソースベースのポリシーにアクセス許可を追加するアクセス許可を付与します	権限の管理	layerVersion*		
AddPermission	AWS Lambda 関数を使用するアクセス許可を AWS サービスまたは別のアカウントに付与するアクセス許可を付与します	権限の管理	function*		
				lambda:Principal lambda:FunctionUrlAuthType	
CreateAlias	Lambda 関数バージョンのエイリアスを作成する許可を付与。	書き込み	function*		
CreateCodeSigningConfig	AWS Lambda コード署名設定を作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventSourceMapping	イベントソースと AWS Lambda 関数間のマッピング	書き込み		lambda:FunctionArn	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	を作成するアクセス許可を付与します			aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunction	AWS Lambda 関数を作成するアクセス許可を付与します	書き込み	function*		iam:PassRole
				lambda:Layer lambda:VpcIds lambda:SubnetIds lambda:SecurityGroupIds lambda:CodeSigningConfigArn aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateFunctionUrlConfig	Lambda 関数の関数 URL 設定を作成するアクセス許可を付与	書き込み	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	
DeleteAlias	AWS Lambda 関数エイリアスを削除する許可を付与	書き込み	function*		
DeleteCodeSigningConfig	AWS Lambda コード署名設定を削除する許可を付与	書き込み	codesigningconfig*		
DeleteEventSourceMapping	AWS Lambda イベントソースマッピングを削除する許可を付与	書き込み	eventSourceMapping*		
				lambda:FunctionArn	
DeleteFunction	AWS Lambda 関数を削除するアクセス許可を付与します	書き込み	function*		
DeleteFunctionCodeSigningConfig	AWS Lambda 関数からコード署名設定をデタッチするアクセス許可を付与します	書き込み	function*		
DeleteFunctionConcurrency	AWS Lambda 関数から同時実行制限を削除するアクセス許可を付与します	書き込み	function*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteFunctionEventInvokeConfig	AWS Lambda 関数、バージョン、またはエイリアスの非同期呼び出しの設定を削除するアクセス許可を付与します	書き込み	function*		
DeleteFunctionUrlConfig	Lambda 関数の関数 URL 設定を削除するアクセス許可を付与	書き込み	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	
DeleteLayerVersion	AWS Lambda レイヤーのバージョンを削除するアクセス許可を付与します	書き込み	layerVersion*		
DeleteProvisionedConcurrencyConfig	AWS Lambda 関数のプロビジョニングされた同時実行設定を削除するアクセス許可を付与します	書き込み	function alias		
			function version		
DisableReplication [アクセス許可のみ]	Lambda@Edge 関数のレプリケーションを無効にする許可を付与。	Permissions management	function*		
EnableReplication [許可のみ]	Lambda@Edge 関数のレプリケーションを有効にする許可を付与。	権限の管理	function*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetAccountSettings	アカウントの制限と使用状況に関する詳細を で表示するアクセス許可を付与します AWS リージョン	読み取り			
GetAlias	AWS Lambda 関数エイリアスの詳細を表示するアクセス許可を付与します	読み取り	function*		
GetCodeSigningConfig	AWS Lambda コード署名設定の詳細を表示するアクセス許可を付与します	読み取り	codesigningconfig*		
GetEventSourceMapping	AWS Lambda イベントソースマッピングの詳細を表示するアクセス許可を付与します	読み取り	eventSourceMapping*		
				lambda:FunctionArn	
GetFunction	AWS Lambda 関数の詳細を表示するアクセス許可を付与します	読み取り	function*		
GetFunctionCodeSigningConfig	AWS Lambda 関数にアタッチされたコード署名設定 ARN を表示する許可を付与	読み取り	function*		
GetFunctionConcurrency	関数の予約済み同時実行設定の詳細を表示する許可を付与。	読み取り	function*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetFunctionConfiguration	AWS Lambda 関数またはバージョンのバージョン固有の設定に関する詳細を表示するアクセス許可を付与します	読み取り	function*		
GetFunctionEventInvokeConfig	関数、バージョン、またはエイリアスの非同期呼び出しの設定を表示する許可を付与。	読み取り	function*		
GetFunctionRecursionConfig	AWS Lambda 関数の再帰設定を表示するアクセス許可を付与します	読み取り	function*		
GetFunctionUrlConfig	Lambda 関数の関数 URL 設定を読み取るアクセス許可を付与	読み取り	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	
GetLayerVersion	AWS Lambda レイヤーのバージョンに関する詳細を表示するアクセス許可を付与します。このアクションは、GetLayerVersionByArn API もサポートしていることに注意してください	読み取り	layerVersion*		
GetLayerVersionPolicy	AWS Lambda レイヤーのバージョンに対するリソースベースのポリシーを表示するアクセス許可を付与します	読み取り	layerVersion*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetPolicy	AWS Lambda 関数、バージョン、またはエイリアスのリソースベースのポリシーを表示するアクセス許可を付与します	読み取り	function*		
GetProvisionedConcurrencyConfig	AWS Lambda 関数のエイリアスまたはバージョンのプロビジョニングされた同時実行設定を表示するアクセス許可を付与します	読み取り	function alias		
			function version		
GetRuntimeManagementConfig	AWS Lambda 関数のランタイム管理設定を表示するアクセス許可を付与します	読み取り	function*		
InvokeAsync	(非推奨) 関数を非同期的に呼び出すアクセス許可を付与	書き込み	function*		
InvokeFunction	AWS Lambda 関数を呼び出すアクセス許可を付与します	書き込み	function*		
				lambda:EventSourceToken	
InvokeFunctionUrl [アクセス許可のみ]	URL を介して AWS Lambda 関数を呼び出すアクセス許可を付与します	書き込み	function*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				lambda:FunctionUrlAuthType lambda:FunctionArn lambda:EventSourceToken	
ListAliases	AWS Lambda 関数のエイリアスのリストを取得する許可を付与	リスト	function*		
ListCodeSigningConfigs	AWS Lambda コード署名設定のリストを取得する許可を付与	リスト			
ListEventSourceMappings	AWS Lambda イベントソースマッピングのリストを取得する許可を付与	リスト			
ListFunctionEventInvokeConfigs	関数の非同期呼び出しの設定リストを取得する許可を付与。	リスト	function*		
ListFunctionUrlConfigs	関数の関数 URL 設定を読み取るアクセス許可を付与	リスト	function*		
				lambda:FunctionUrlAuthType	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListFunctions	各関数のバージョン固有の設定を使用して、 AWS Lambda 関数のリストを取得するアクセス許可を付与します	リスト			
ListFunctionsByCodeSigningConfig	割り当てられたコード署名設定によって AWS Lambda 関数のリストを取得する許可を付与	リスト	codesigningconfig*		
ListLayerVersions	AWS Lambda レイヤーのバージョンのリストを取得するアクセス許可を付与します	リスト			
ListLayers	各レイヤーの最新バージョンの詳細を含む AWS Lambda レイヤーのリストを取得するアクセス許可を付与します	リスト			
ListProvisionedConcurrencyConfigs	AWS Lambda 関数のプロビジョニングされた同時実行設定のリストを取得するアクセス許可を付与します	リスト	function*		
ListTags	AWS Lambda 関数、イベントソースマッピング、またはコード署名設定リソースのタグのリストを取得するアクセス許可を付与します	読み取り	codesigningconfig		
			eventSourceMapping		
			function		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListVersionsByFunction	AWS Lambda 関数のバージョンのリストを取得するアクセス許可を付与します	リスト	function*		
PublishLayerVersion	AWS Lambda レイヤーを作成するアクセス許可を付与します	書き込み	layer*		
PublishVersion	AWS Lambda 関数バージョンを作成するアクセス許可を付与します	書き込み	function*		
PutFunctionCodeSigningConfig	AWS Lambda 関数にコード署名設定をアタッチするアクセス許可を付与します	書き込み	codesigningconfig*		
			function*		
				lambda:CodeSigningConfigArn	
PutFunctionConcurrency	AWS Lambda 関数の予約済み同時実行を設定するアクセス許可を付与します	書き込み	function*		
PutFunctionEventInvokeConfig	AWS Lambda 関数、バージョン、またはエイリアスで非同期呼び出しのオプションを設定するアクセス許可を付与します	書き込み	function*		
PutFunctionRecursionConfig	AWS Lambda 関数の再帰設定を更新する許可を付与	書き込み	function*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutProvisionedConcurrencyConfig	AWS Lambda 関数のエイリアスまたはバージョンのプロビジョニングされた同時実行を設定するアクセス許可を付与します	書き込み	function alias		
			function version		
PutRuntimeManagementConfig	AWS Lambda 関数のランタイム管理設定を更新する許可を付与	書き込み	function*		
RemoveLayerVersionPermission	AWS Lambda レイヤーのバージョンに対するアクセス許可ポリシーからステートメントを削除するアクセス許可を付与します	権限の管理	layerVersion*		
RemovePermission	AWS サービスまたは別のアカウントから関数使用のアクセス許可を取り消すアクセス許可を付与します	権限の管理	function*		
				lambda:Principal lambda:FunctionUrlAuthType	
TagResource	AWS Lambda 関数、イベントソースマッピング、またはコード署名設定リソースにタグを追加する許可を付与	Tagging	code signing config		
			eventSourceMapping		
			function		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	AWS Lambda 関数、イベントソースマッピング、またはコード署名設定リソースからタグを削除するアクセス許可を付与します	Tagging	codesigningconfig		
			eventSourceMapping		
			function		
				aws:TagKeys	
UpdateAlias	AWS Lambda 関数のエイリアスの設定を更新する許可を付与	書き込み	function*		
UpdateCodeSigningConfig	AWS Lambda コード署名設定を更新する許可を付与	書き込み	codesigningconfig*		
UpdateEventSourceMapping	AWS Lambda イベントソースマッピングの設定を更新する許可を付与	書き込み	eventSourceMapping*		
				lambda:FunctionArn	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateFunctionCode	AWS Lambda 関数のコードを更新する許可を付与	書き込み	function*		
UpdateFunctionCodeSigningConfig	AWS Lambda 関数のコード署名設定を更新する許可を付与	書き込み	code signing config*		
			function*		
UpdateFunctionConfiguration	AWS Lambda 関数のバージョン固有の設定を変更するアクセス許可を付与します	書き込み	function*		
				lambda:Layer lambda:VpcIds lambda:SubnetIds lambda:SecurityGroupIds	
UpdateFunctionEventInvokeConfig	AWS Lambda 関数、バージョン、またはエイリアスの非同期呼び出しの設定を変更するアクセス許可を付与します	書き込み	function*		
UpdateFunctionUrlConfig	Lambda 関数の関数 URL 設定を更新するアクセス許可を付与	書き込み	function*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				lambda:FunctionUrlAuthType lambda:FunctionArn	

AWS Lambda で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
code signing config	`arn:${Partition}:lambda:${Region}:${Account}:code-signing-config:${CodeSigningConfigId}`	aws:ResourceTag/${TagKey}
eventSourceMapping	`arn:${Partition}:lambda:${Region}:${Account}:event-source-mapping:${UUID}`	aws:ResourceTag/${TagKey}
function	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}`	aws:ResourceTag/${TagKey}
function alias	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Alias}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
function version	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Version}`	aws:ResourceTag/${TagKey}
layer	`arn:${Partition}:lambda:${Region}:${Account}:layer:${LayerName}`	
layerVersion	`arn:${Partition}:lambda:${Region}:${Account}:layer:${LayerName}:${LayerVersion}`	

AWS Lambda の条件キー

AWS Lambda は、IAM ポリシーの `Condition`要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
lambda:CodeSigningConfigArn	AWS Lambda コード署名設定の ARN でアクセスをフィルタリングします	ARN

条件キー	説明	タイプ
lambda:EventSourceToken	AWS Lambda 関数用に設定されたAWS イベント以外のソースからの ID でアクセスをフィルタリングします	String
lambda:FunctionArn	AWS Lambda 関数の ARN でアクセスをフィルタリングします	ARN
lambda:FunctionUrlAuthType	リクエストで指定された認可タイプでアクセスをフィルタリングします。CreateFunctionUrlConfig、UpdateFunctionUrlConfig、DeleteFunctionUrlConfig、GetFunctionUrlConfig、ListFunctionUrlConfig、AddPermission、および RemovePermission のオペレーション中に使用できます	String
lambda:Layer	AWS Lambda レイヤーのバージョン ARN でアクセスをフィルタリングします	ArrayOfString
lambda:Principal	関数を呼び出すことができる AWS サービスまたはアカウントを制限してアクセスをフィルタリングします	String
lambda:SecurityGroupIds	AWS Lambda 関数用に設定されたセキュリティグループの ID でアクセスをフィルタリングします	ArrayOfString
lambda:SourceFunctionArn	リクエスト元の AWS Lambda 関数の ARN でアクセスをフィルタリングします	ARN
lambda:SubnetIds	AWS Lambda 関数用に設定されたサブネットの ID でアクセスをフィルタリングします	ArrayOfString
lambda:VpcIds	AWS Lambda 関数用に設定された VPC の ID でアクセスをフィルタリングします	String

AWS Launch Wizard のアクション、リソース、および条件キー

AWS Launch Wizard (サービスプレフィックス: `launchwizard`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Launch Wizard によって定義されたアクション
- AWS Launch Wizard によって定義されるリソースタイプ
- AWS Launch Wizard の条件キー

AWS Launch Wizard によって定義されたアクション

IAM ポリシーステートメントの `Action` 要素では、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateAdditionalNode [アクセス許可のみ]	追加のノードを作成する許可を付与	書き込み			
CreateDeployment	デプロイを作成する許可を付与	書き込み	deployment*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateSettingsSet [アクセス許可のみ]	アプリケーションの設定セットを作成する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteAdditionalNode [アクセス許可のみ]	追加ノードを削除する許可を付与	書き込み			
DeleteApp [アクセス許可のみ]	アプリケーションを削除する許可を付与	書き込み			
DeleteDeployment	デプロイを削除する許可を付与	書き込み	deployment*	aws:ResourceTag/${TagKey}	
DeleteSettingsSet [アクセス許可のみ]	設定セットを削除する許可を付与	書き込み			
DescribeAdditionalNode [アクセス許可のみ]	追加ノードを記述する許可を付与	読み取り			
DescribeProvisionedApp [許可のみ]	プロビジョニングアプリケーションを記述するアクセス許可を付与	読み取り			
DescribeProvisioningEvents [許可のみ]	プロビジョニングイベントを記述するアクセス許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeSettingsSet [許可のみ]	アプリケーションの設定セットを記述する許可を付与	読み取り			
GetDeployment	デプロイを取得する許可を付与	読み取り	deployment*	aws:ResourceTag/${TagKey}	
GetInfrastructureSuggestion [許可のみ]	インフラストラクチャの提案を取得するアクセス許可を付与	読み取り			
GetIpAddress [許可のみ]	お客様の IP アドレスを取得するアクセス許可を付与	読み取り			
GetResourceCostEstimate [許可のみ]	リソースコストの見積りを取得するアクセス許可を付与	読み取り			
GetResourceRecommendation [許可のみ]	リソースに対する推奨事項を取得する許可を付与	読み取り			
GetSettingsSet [許可のみ]	設定セットを取得する許可を付与	読み取り			
GetWorkload	ワークロードを取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetWorkloadAsset [許可のみ]	ワークロードのアセットを取得する許可を付与	読み取り			
GetWorkloadAssets [許可のみ]	ワークロードのアセットを取得する許可を付与	読み取り			
GetWorkloadDeploymentPattern	デプロイパターンを取得する許可を付与する	読み取り			
ListAdditionalNodes [許可のみ]	追加ノードを一覧表示する許可を付与	リスト			
ListAllowedResources [許可のみ]	許可されているリソースを一覧表示する許可を付与	リスト			
ListDeploymentEvents	デプロイ中に発生したイベントを一覧表示する許可を付与	リスト			
ListDeployments	デプロイを一覧表示する許可を付与	リスト			
ListProvisionedApps [許可のみ]	プロビジョニングアプリケーションを一覧表示するアクセス許可を付与	リスト			
ListResourceCostEstimates [許可のみ]	リソースのコストの見積もりを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListSettingsSets [許可のみ]	設定セット (複数) を一覧表示する許可を付与	リスト			
ListTagsForResource	LaunchWizard リソースのタグ付けを一覧表示する許可を付与します。	読み取り	deployment	aws:ResourceTag/${TagKey}	
ListWorkloadDeploymentOptions [許可のみ]	特定のワークロードのデプロイオプションを一覧表示する許可を付与	リスト			
ListWorkloadDeploymentPatterns	ワークロードのデプロイパターンを一覧表示する許可を付与	リスト			
ListWorkloads	ワークロードを一覧表示する許可を付与	リスト			
PutSettingsSet [許可のみ]	設定セットを作成する許可を付与	書き込み			
StartProvisioning [アクセス許可のみ]	プロビジョニングを開始するアクセス許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
TagResource	LaunchWizard リソースをタグ付けする許可を付与します。	Tagging	deployment	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	LaunchWizard リソースのタグを解除する許可を付与します。	Tagging	deployment	aws:TagKeys	
UpdateSettingsSet [アクセス許可のみ]	アプリケーションの設定セットを更新する許可を付与	書き込み			

AWS Launch Wizard によって定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
deployment	`arn:${Partition}:launchwizard:${Region}:${Account}:deployment/${DeploymentId}`	aws:ResourceTag/${TagKey}

AWS Launch Wizard の条件キー

AWS Launch Wizard は、IAM ポリシーの `Condition`要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアのプレゼンスに基づいてアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアに基づいてアクセスをフィルタリングします。	文字列
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいてアクセスをフィルタリングします	ArrayOfString

Amazon Lex のアクション、リソース、および条件キー

Amazon Lex (サービスプレフィックス: `lex`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Lex で定義されるアクション
- Amazon Lex で定義されるリソースタイプ
- Amazon Lex の条件キー

Amazon Lex で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateBotVersion	指定されたボットの $LATEST バージョンに基づいて新しいバージョンを作成します	書き込み	bot version*		
CreateIntentVersion	指定されたインテントの $LATEST バージョンに基づいて新しいバージョンを作成します	書き込み	intent version*		
CreateSlotTypeVersion	指定されたスロットタイプの $LATEST バージョンに基づいて新しいバージョンを作成します	書き込み	slottype version*		
DeleteBot	ボットのすべてのバージョンを削除します	書き込み	bot version*		
DeleteBotAlias	指定されたボットのエイリアスを削除します	書き込み	bot alias*		
DeleteBotChannelAssociation	Amazon Lex ボットエイリアスとメッセージングプラットフォームの間の関連付けを削除します	書き込み	channel*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteBotVersion	ボットの特定のバージョンを削除します	書き込み	bot version*		
DeleteIntent	インテントのすべてのバージョンを削除します	書き込み	intent version*		
DeleteIntentVersion	インテントの特定のバージョンを削除します	書き込み	intent version*		
DeleteSession	指定されたボット、エイリアス、ユーザー ID のセッション情報を削除します	書き込み	bot alias		
			bot version		
DeleteSlotType	スロットタイプのすべてのバージョンを削除します	書き込み	slottype version*		
DeleteSlotTypeVersion	スロットタイプの特定のバージョンを削除します	書き込み	slottype version*		
DeleteUtterances	特定のボットおよび userId における発話のために Amazon Lex で維持されている情報を削除します	書き込み	bot version*		
GetBot	特定のボットの情報を返します。ボット名の他に、ボットバージョンまたはエイリアスが必要です	読み込み	bot alias		
			bot version		
GetBotAlias	Amazon Lex ボットエイリアスの情報を返します	読み込み	bot alias*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetBotAliases	特定の Amazon Lex ボットのエイリアスのリストを返します	リスト			
GetBotChannelAssociation	Amazon Lex ボットとメッセージングプラットフォームの関連付けに関する情報を返します	読み込み	channel*		
GetBotChannelAssociations	1 つのボットに関連付けられているすべてのチャネルのリストを返します	リスト	channel*		
GetBotVersions	特定のボットのすべてのバージョンの情報を返します	リスト	bot version*		
GetBots	すべてのボットの $LATEST バージョンについて、クライアントから提供されたフィルターに従って情報を返します	リスト			
GetBuiltinIntent	組み込みインテントの情報を返します	読み込み			
GetBuiltinIntents	指定された基準を満たす組み込みインテントのリストを取得します	読み込み			
GetBuiltinSlotTypes	指定された基準を満たす組み込みスロットタイプのリストを取得します	読み込み			
GetExport	Amazon Lex リソースをリクエストされた形式でエクスポートします	読み込み	bot version*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetImport	StartImport で開始されたインポートジョブの情報を取得します	読み込み			
GetIntent	特定のインテントの情報を返します。インテント名に加えて、インテントバージョンも指定する必要があります	読み込み	intent version*		
GetIntentVersions	特定のインテントのすべてのバージョンの情報を返します	リスト	intent version*		
GetIntents	すべてのインテントの $LATEST バージョンについて、クライアントから提供されたフィルターに従って情報を返します	リスト			
GetMigration	進行中または完了した移行を表示する許可を付与	読み込み			
GetMigrations	Amazon Lex v1 から Amazon Lex v2 への移行のリストを表示する許可を付与	リスト			
GetSession	指定されたボット、エイリアス、ユーザー ID のセッション情報を返します	読み込み	bot alias		
			bot version		
GetSlotType	スロットタイプの特定のバージョンに関する情報を返します。スロットタイプ名に加えて、スロットタイプバージョンも指定する必要があります	読み込み	slottype version*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetSlotTypeVersions	特定のスロットタイプのすべてのバージョンの情報を返します	リスト	slottype version*		
GetSlotTypes	すべてのスロットタイプの $LATEST バージョンについて、クライアントから提供されたフィルターに従って情報を返します	リスト			
GetUtterancesView	ボットのバージョンについて、最近の期間における発話の集計データを表示します	リスト	bot version*		
ListTagsForResource	Lex リソースのタグを一覧表示します。	読み込み	bot		
			bot alias		
			channel		
PostContent	ユーザー入力 (テキストまたは音声) を Amazon Lex に送信します	書き込み	bot alias		
			bot version		
PostText	ユーザー入力 (テキストのみ) を Amazon Lex に送信します	書き込み	bot alias		
			bot version		
PutBot	Amazon Lex 会話ボットの $LATEST バージョンを作成または更新します	書き込み	bot version*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
PutBotAlias	特定のボットのエイリアスを作成または更新します	書き込み	bot alias*		
				aws:TagKeys aws:RequestTag/${TagKey}	
PutIntent	インテントの $LATEST バージョンを作成または更新します	書き込み	intent version*		
PutSession	Amazon Lex ボットで新しいセッションを作成するか、既存のセッションを変更します	書き込み	bot alias		
			bot version		
PutSlotType	スロットタイプの $LATEST バージョンを作成または更新します	書き込み	slottype version*		
StartImport	リソースを Amazon Lex にインポートするジョブを開始します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartMigration	Amazon レックス v1 から Amazon Lex v2 にボットを移行する許可を付与	書き込み	bot version*		
TagResource	Lex リソースにタグを追加または上書きします。	タグ付け	bot		
			bot alias		
			channel		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Lex リソースからタグを削除します。	タグ付け	bot		
			bot alias		
			channel		
				aws:TagKeys aws:RequestTag/${TagKey}	

Amazon Lex で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
bot	arn:${Partition}:lex:${Region}:${Account}:bot:${BotName}	aws:ResourceTag/${TagKey}
bot version	arn:${Partition}:lex:${Region}:${Account}:bot:${BotName}:${BotVersion}	aws:ResourceTag/${TagKey}
bot alias	arn:${Partition}:lex:${Region}:${Account}:bot:${BotName}:${BotAlias}	aws:ResourceTag/${TagKey}
channel	arn:${Partition}:lex:${Region}:${Account}:bot-channel:${BotName}:${BotAlias}:${ChannelName}	aws:ResourceTag/${TagKey}
intent version	arn:${Partition}:lex:${Region}:${Account}:intent:${IntentName}:${IntentVersion}	
slottype version	arn:${Partition}:lex:${Region}:${Account}:slottype:${SlotName}:${SlotVersion}	

Amazon Lex の条件キー

Amazon Lex では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグに基づいてアクセスをフィルタリングする	文字列
aws:ResourceTag/${TagKey}	Lex リソースにアタッチされたタグでアクセスをフィルタリングする	String
aws:TagKeys	リクエスト内のタグキーのセットに基づいてアクセスをフィルタリングします	ArrayOfString
lex:associatedIntents	ユーザーに対し、リクエストに含まれるインテントに基づいたアクセスの制御を可能にします	ArrayOfString
lex:associatedSlotTypes	ユーザーに対し、リクエストに含まれるスロットタイプに基づいたアクセスの制御を可能にします	ArrayOfString
lex:channelType	ユーザーに対し、リクエストに含まれるチャネルタイプに基づいたアクセスの制御を可能にします	String

Amazon Lex V2 のアクション、リソース、および条件キー

Amazon Lex V2 (サービスプレフィックス: `lex`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Lex V2 で定義されるアクション
- Amazon Lex V2 で定義されるリソースタイプ

- Amazon Lex V2 の条件キー

Amazon Lex V2 で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchCreateCustomVocabularyItem	既存のカスタム語彙内に新しい項目を作成する許可を付与	書き込み	bot*		
BatchDeleteCustomVocabularyItem	既存のカスタム語彙内の既存の項目を削除する許可を付与	書き込み	bot*		
BatchUpdateCustomVocabularyItem	既存のカスタム語彙内の既存の項目を更新する許可を付与	書き込み	bot*		
BuildBotLocale	ボットに既存のボットロケールを構築する許可を付与	書き込み	bot*		
CreateBot	ドラフトボットバージョンを指す新しいボットとテストボットのエイリアスを作成する許可を付与	書き込み	bot*		
			bot alias*		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
CreateBotAlias	ボットに新しいボットエイリアスを作成する許可を付与	書き込み	bot alias*		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey}	
CreateBotChannel [アクセス許可のみ]	既存のボットでボットチャネルを作成する許可を付与	書き込み	bot*		
CreateBotLocale	既存のボットで新しいボットロケールを作成する許可を付与	書き込み	bot*		
CreateBotReplica	ボットのボットレプリカを作成する許可を付与する	書き込み	bot*		
CreateBotVersion	既存のボットの新しいバージョンを作成する許可を付与	書き込み	bot*		
CreateCustomVocabulary [アクセス許可のみ]	既存のボットロケールで新しいカスタム語彙を作成する許可を付与	書き込み	bot*		
CreateExport	既存のリソースのエクスポートを作成する許可を付与	書き込み	bot		
			test set		
CreateIntent	既存のボットロケールで新しいインテントを作成する許可を付与	書き込み	bot*		
CreateResourcePolicy	Lex リソースの新しいリソースポリシーを作成する許可を付与	書き込み	bot		
			bot alias		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateResourcePolicyStatement	Lex リソースの新しいリソースポリシーステートメントを作成するアクセス許可を付与します	書き込み	bot		
			bot alias		
CreateSlot	インテントに新しいスロットを作成する許可を付与	書き込み	bot*		
CreateSlotType	既存のボットロケールで新しいスロットタイプを作成する許可を付与	書き込み	bot*		
CreateTestSet [アクセス許可のみ]	新しいテストセットをインポートするアクセス許可を付与します	書き込み			
CreateTestSetDiscrepancyReport	テストセット不一致レポートを作成するアクセス許可を付与します	書き込み	test set*		
CreateUploadUrl	インポートファイルのアップロード URL を作成する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteBot	既存のボットを削除する許可を付与	書き込み	bot*		lex:DeleteBotAlias lex:DeleteBotChannel lex:DeleteBotLocale lex:DeleteBotVersion lex:DeleteIntent lex:DeleteSlot lex:DeleteSlotType
			bot alias*		
DeleteBotAlias	ボット内の既存のボットエイリアスを削除する許可を付与	書き込み	bot alias*		
DeleteBotChannel [アクセス許可のみ]	既存のボットチャネルを削除する許可を付与	書き込み	bot*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteBotLocale	ボットに既存のボットロケールを削除する許可を付与	書き込み	bot*		lex:DeleteIntent lex:DeleteSlot lex:DeleteSlotType
DeleteBotReplica	既存のボットレプリカを削除する許可を付与する	書き込み	bot*		
DeleteBotVersion	既存のボットバージョンを削除する許可を付与	書き込み	bot*		
DeleteCustomVocabulary	ボットロケールの既存のカスタム語彙を削除する許可を付与	書き込み	bot*		
DeleteExport	既存のエクスポートを削除する許可を付与	書き込み	bot		
			test set		
DeleteImport	既存のルートを削除するためのアクセス許可を付与	書き込み	bot		
			test set		
DeleteIntent	ボットロケールの既存のインテントを削除する許可を付与	書き込み	bot*		
DeleteResourcePolicy	Lex リソースの既存のリソースポリシーを削除する許可を付与	書き込み	bot		
			bot alias		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteResourcePolicyStatement	Lex リソースの既存のリソースポリシーステートメントを削除するアクセス許可を付与します	書き込み	bot		
			bot alias		
DeleteSession	ボットエイリアスとユーザー ID のセッション情報を削除する許可を付与	書き込み	bot alias*		
DeleteSlot	インテント内の既存のスロットを削除する許可を付与	書き込み	bot*		
DeleteSlotType	ボットロケールの既存のスロットタイプを削除する許可を付与	書き込み	bot*		
DeleteTestSet	既存のテストセットを削除するアクセス許可を付与します	書き込み	test set*		
DeleteUtterances	ボットの発話データを削除するアクセス許可を付与	書き込み	bot*		
DescribeBot	既存のボットを取得する許可を付与	読み込み	bot*		
DescribeBotAlias	既存のボットエイリアスを取得する許可を付与	読み込み	bot alias*		
DescribeBotChannel [許可のみ]	既存のボットチャネルを取得する許可を付与	読み込み	bot*		
DescribeBotLocale	既存のボットロケールを取得する許可を付与	読み込み	bot*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeBotRecommendation	bot推奨事項関するメタデータ情報を取得するためのアクセス許可を付与	読み取り	bot*		
DescribeBotReplica	既存のボットレプリカを取得する許可を付与する	読み取り	bot*		
DescribeBotResourceGeneration	ボットのリソース生成のメタデータ情報を取得する許可を付与	読み取り	bot*		
DescribeBotVersion	既存のbotバージョンを取得するためのアクセス許可を付与	読み込み	bot*		
DescribeCustomVocabulary [許可のみ]	既存のカスタム語彙を取得する許可を付与	読み込み	bot*		
DescribeCustomVocabularyMetadata	既存のカスタム語彙のメタデータを取得する許可を付与	読み込み	bot*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeExport	既存のエクスポートを取得する許可を付与	読み込み	bot		lex:DescribeBot lex:DescribeBotLocale lex:DescribeIntent lex:DescribeSlot lex:DescribeSlotType lex:ListBotLocales lex:ListIntents lex:ListSlotTypes lex:ListSlots
			test set		
DescribeImport	既存のインポートを取得する許可を付与	読み込み	bot		
			test set		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeIntent	既存のインテントを取得する許可を付与	読み込み	bot*		
DescribeResourcePolicy	Lex リソースの既存のリソースポリシーを取得する許可を付与	読み込み	bot		
			bot alias		
DescribeSlot	既存のスロットを取得する許可を付与	読み込み	bot*		
DescribeSlotType	既存のスロットタイプを取得する許可を付与	読み取り	bot*		
DescribeTestExecution	テスト実行メタデータを取得するアクセス許可を付与します	読み取り	test set*		
DescribeTestSet	既存のテストセットを取得するアクセス許可を付与します	読み取り	test set*		
DescribeTestSetDiscrepancyReport	テストセット不一致レポートのメタデータを取得するアクセス許可を付与します	読み取り	test set*		
DescribeTestSetGeneration	テストセット生成メタデータを取得するアクセス許可を付与します	読み取り	test set		
GenerateBotElement	ボット対応のフィールドまたは要素を生成する許可を付与	読み取り	bot*		
GetSession	ボットエイリアスとユーザー ID のセッション情報を取得する許可を付与	読み取り	bot alias*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetTestExecutionArtifactsUrl	テスト実行のアーティファクト URL を取得するアクセス許可を付与します	読み取り	test set*		
ListAggregatedUtterances	botの発話および統計を一覧表示するアクセス許可を付与	リスト	bot*		
ListBotAliasReplicas	ボットレプリカ内のエイリアスレプリカを一覧表示する許可を付与する	リスト	bot*		
ListBotAliases	ボットにボットのエイリアスを一覧表示する許可を付与	リスト	bot*		
ListBotChannels [許可のみ]	ボットチャネルを一覧表示する許可を付与	リスト	bot*		
ListBotLocales	ボット内のボットロケールを一覧表示する許可を付与	リスト	bot*		
ListBotRecommendations	指定された条件を満たすボット推奨のリストを取得するアクセス許可を付与	リスト	bot*		
ListBotReplicas	ボットのレプリカを一覧表示する許可を付与する	リスト	bot*		
ListBotResourceGenerations	ボットのリソース生成を一覧表示する許可を付与	リスト	bot*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListBotVersionReplicas	ボットレプリカ内のバージョンレプリカを一覧表示する許可を付与する	リスト	bot*		
ListBotVersions	既存のボットバージョンを一覧表示する許可を付与	リスト	bot*		
ListBots	既存のボットを一覧表示する許可を付与	リスト			
ListBuiltInIntents	組み込みインテントを一覧表示する許可を付与	リスト			
ListBuiltInSlotTypes	組み込みスロットタイプを一覧表示する許可を付与	リスト			
ListCustomVocabularyItems	既存のカスタム語彙の項目を一覧表示する許可を付与	リスト	bot*		
ListExports	既存のエクスポートを一覧表示する許可を付与	リスト			
ListImports	既存のインポートを一覧表示する許可を付与	リスト			
ListIntentMetrics	ボットのインテント分析メトリクスを一覧表示するための許可を付与します	リスト	bot*		
ListIntentPaths	ボットのインテントパス分析を一覧表示するための許可を付与します	リスト	bot*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListIntentStageMetrics	ボットの intentStage 分析メトリクスを一覧表示するための許可を付与します	リスト	bot*		
ListIntents	ボットにインテントを一覧表示する許可を付与	リスト	bot*		
ListRecommendedIntents	ボット推奨によって提供される推奨インテントのリストを取得するアクセス許可を付与	リスト	bot*		
ListSessionAnalyticsData	ボットのセッション分析データを一覧表示するための許可を付与します	リスト	bot*		
ListSessionMetrics	ボットのセッション分析メトリクスを一覧表示するための許可を付与します	リスト	bot*		
ListSlotTypes	ボット内のスロットタイプを一覧表示する許可を付与	リスト	bot*		
ListSlots	インテント内のスロットを一覧表示する許可を付与	リスト	bot*		
ListTagsForResource	Lex リソースのタグを一覧表示する許可を付与	読み取り	bot		
			bot alias		
			test set		
ListTestExecutionResultItems	テスト実行のテスト結果データを取得するアクセス許可を付与します	読み取り	test set*		lex:ListTestSetRecords

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTestExecutions	テスト実行を一覧表示するアクセス許可を付与します	リスト			
ListTestSetRecords	既存のテストセット内のレコードを取得するアクセス許可を付与します	読み取り	test set*		
ListTestSets	テストセットを一覧表示するアクセス許可を付与します	リスト			
PutSession	ボットエイリアスとユーザー ID に対して、新しいセッションを作成したり、既存のセッションを変更したりする許可を付与	書き込み	bot alias*		
RecognizeText	ユーザー入力 (テキストのみ) をボットエイリアスに送信する許可を付与	書き込み	bot alias*		
RecognizeUtterance	ユーザー入力 (テキストまたは音声) をボットエイリアスに送信する許可を付与	書き込み	bot alias*		
SearchAssociatedTranscripts	指定された条件を満たす関連するトランスクリプトを検索するアクセス許可を付与	リスト	bot*		
StartBotRecommendation	既存のボットロケールでボット推奨を開始するアクセス許可を付与	書き込み	bot*		
StartBotResourceGeneration	既存のボットロケールのリソース生成を開始する許可を付与	書き込み	bot*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartConversation	ユーザー入力 (音声/テキスト/DTMF) をボットエイリアスにストリームする許可を付与	書き込み	bot alias*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartImport	アップロードされたインポートファイルを使用して新しいインポートを開始する許可を付与	書き込み	bot		lex:CreateBot lex:CreateBotLocale lex:CreateCustomVocabulary lex:CreateIntent lex:CreateSlot lex:CreateSlotType lex:CreateTestSet lex:DeleteBotLocale lex:DeleteCustomVocabulary lex:DeleteIntent lex:DeleteSlot

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					lex:DeleteSlotType lex:UpdateBot lex:UpdateBotLocale lex:UpdateCustomVocabulary lex:UpdateIntent lex:UpdateSlot lex:UpdateSlotType lex:UpdateTestSet
			bot alias		
			test set		
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartTestExecution	テストセットを使用してテスト実行を開始するアクセス許可を付与します	書き込み	test set*		
StartTestSetGeneration	テストセットを生成するアクセス許可を付与します	書き込み	test set		
StopBotRecommendation	既存のボットロケールでボット推奨を停止する許可を付与	書き込み	bot*		
TagResource	Lex リソースのタグを追加または上書きする許可を付与	タグ付け	bot		
			bot alias		
			test set		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Lex リソースからタグを削除する許可を付与	タグ付け	bot		
			bot alias		
			test set		
				aws:TagKeys	
UpdateBot	既存のボットを更新する許可を付与	書き込み	bot*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateBotAlias	既存のボットエイリアスを更新する許可を付与	書き込み	bot alias*		
UpdateBotLocale	既存のボットロケールを更新する許可を付与	書き込み	bot*		
UpdateBotRecommendation	既存のボット推奨リクエストを更新するアクセス許可を付与	書き込み	bot*		
UpdateCustomVocabulary [アクセス許可のみ]	既存のカスタム語彙を更新する許可を付与	書き込み	bot*		
UpdateExport	既存のエクスポートを更新する許可を付与	書き込み	bot*		
UpdateIntent	既存のインテントを更新する許可を付与	書き込み	bot*		
UpdateResourcePolicy	Lex リソースの既存のリソースポリシーを更新する許可を付与	書き込み	bot		
			bot alias		
UpdateSlot	既存のスロットを更新する許可を付与	書き込み	bot*		
UpdateSlotType	既存のスロットタイプを更新する許可を付与	書き込み	bot*		
UpdateTestSet	既存のテストセットを更新するアクセス許可を付与します	書き込み	test set*		

Amazon Lex V2 で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
bot	arn:${Partition}:lex:${Region}:${Account}:bot/${BotId}	aws:ResourceTag/${TagKey}
bot alias	arn:${Partition}:lex:${Region}:${Account}:bot-alias/${BotId}/${BotAliasId}	aws:ResourceTag/${TagKey}
test set	arn:${Partition}:lex:${Region}:${Account}:test-set/${TestSetId}	aws:ResourceTag/${TagKey}

Amazon Lex V2 の条件キー

Amazon Lex V2 では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグでアクセスをフィルタリングする	String
aws:ResourceTag/${TagKey}	Lex リソースにアタッチされたタグでアクセスをフィルタリングする	String

条件キー	説明	[Type] (タイプ)
aws:TagKeys	リクエスト内のタグキーのセットでアクセスをフィルタリングします。	ArrayOfString

AWS License Manager のアクション、リソース、および条件キー

AWS License Manager (サービスプレフィックス: `license-manager`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS License Manager で定義されるアクション
- AWS License Manager で定義されるリソースタイプ
- AWS License Manager の条件キー

AWS License Manager で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptGrant	権限を受け入れるアクセス許可を付与します	書き込み	grant*		
CheckInLicense	ライセンスエンタイトルメントをプールに戻すチェックインをする許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CheckoutBorrowLicense	借用ユースケースのライセンスエンタイトルメントをチェックアウトする許可を付与	書き込み	license*		
CheckoutLicense	ライセンスエンタイトルメントをチェックアウトする許可を付与	書き込み			
CreateGrant	ライセンスの新しい許可を作成する許可を付与	書き込み	license*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateGrantVersion	権限の新しいバージョンを作成する許可を付与	書き込み	grant*		
CreateLicense	新しいライセンスを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseConfiguration	新しいライセンス設定を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateLicenseConversionTaskForResource	リソースのライセンス変換タスクを作成する許可を付与	書き込み			
CreateLicenseManagerReportGenerator	ライセンス設定のレポートジェネレータを作成するためのアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseVersion	ライセンスの新しいバージョンを作成するアクセス許可を付与します	書き込み	license*		
CreateToken	ライセンスの新しいトークンを作成する許可を付与	書き込み	license*		
DeleteGrant	権限を削除するアクセス許可を付与します	書き込み	grant*		
DeleteLicense	ライセンスを削除する許可を付与	書き込み	license*		
DeleteLicenseConfiguration	ライセンス設定を完全に削除する許可を付与	書き込み	license-configuration*		
DeleteLicenseManagerReportGenerator	レポートジェネレータを削除するためのアクセス許可を付与します。	書き込み	report-generator*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteToken	トークンを削除する許可を付与	書き込み			
ExtendLicenseConsumption	すでにチェックアウトしているライセンスエンタイトルメントの消費期間を延長する許可を付与	書き込み			
GetAccessToken	アクセストークンを取得する許可を付与	読み込み			
GetGrant	権限を得るためのアクセス許可を付与します	読み込み	grant*		
GetLicense	ライセンスを取得する許可を付与	読み込み	license*		
GetLicenseConfiguration	ライセンス設定を取得する許可を付与	読み込み	license-configuration*		
GetLicenseConversionTask	ライセンス変換タスクを取得する許可を付与	読み込み			
GetLicenseManagerReportGenerator	レポートジェネレータを取得するためのアクセス許可を付与します。	読み込み	report-generator*		
GetLicenseUsage	ライセンス使用法を取得する許可を付与	読み込み	license*		
GetServiceSettings	サービス設定を取得する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListAssociationsForLicenseConfiguration	選択したライセンス設定の関連付けを一覧表示する許可を付与	リスト	license-configuration*		
ListDistributedGrants	配布された権限を一覧表示する許可を付与	リスト			
ListFailuresForLicenseConfigurationOperations	失敗したライセンス設定オペレーションを一覧表示する許可を付与	リスト	license-configuration*		
ListLicenseConfigurations	ライセンス設定を一覧表示する許可を付与します	読み込み			
ListLicenseConversionTasks	ライセンス変換タスクを一覧表示する許可を付与	リスト			
ListLicenseManagerReportGenerators	レポートジェネレータを一覧表示するためのアクセス許可を付与します	リスト	license-configuration		
ListLicenseSpecificationsForResource	選択したリソースに関連付けられたライセンス仕様を一覧表示する許可を付与しますアクセス	リスト			
ListLicenseVersions	ライセンスバージョンを一覧表示する許可を付与	リスト	license*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListLicenses	ライセンスを一覧表示する許可を付与	読み込み			
ListReceivedGrants	受け取った権限を一覧表示する許可を付与	リスト			
ListReceivedGrantsForOrganization	組織が受け取った権限を一覧表示する許可を付与	リスト			
ListReceivedLicenses	受け取ったライセンスを一覧表示する許可を付与	リスト			
ListReceivedLicensesForOrganization	組織が受け取ったライセンスを一覧表示する許可を付与	リスト			
ListResourceInventory	リソースインベントリを一覧表示する許可を付与	リスト			
ListTagsForResource	選択したリソース用のタグを一覧表示する許可を付与	読み込み	grant		
			license		
			license-configuration		
			report-generator		
ListTokens	トークンを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListUsageForLicenseConfiguration	選択したライセンス設定の使用状況レコードを一覧表示する許可を付与	リスト	license-configuration*		
RejectGrant	権限を拒否する許可を付与	書き込み	grant*		
TagResource	選択したリソースをタグ付けする許可を付与	タグ付け	grant		
			license		
			license-configuration		
			report-generator		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	選択したリソースのタグを解除する許可を付与	タグ付け	grant		
			license		
			license-configuration		
			report-generator		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:TagKeys	
UpdateLicenseConfiguration	既存のライセンス設定を更新する許可を付与	書き込み	license-configuration*		
UpdateLicenseManagerReportGenerator	ライセンス設定のレポートジェネレータを更新するためのアクセス許可を付与します	書き込み	report-generator*		
UpdateLicenseSpecificationsForResource	選択したリソースのライセンス仕様を更新する許可を付与	書き込み	license-configuration*		
UpdateServiceSettings	サービス設定を更新する許可を付与	Permissions management			

AWS License Manager で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
license-configuration	arn:${Partition}:license-manager:${Region}:${Account}:license-configuration:${LicenseConfigurationId}	aws:ResourceTag/${TagKey} license-manager:ResourceTag/${TagKey}
license	arn:${Partition}:license-manager::${Account}:license:${LicenseId}	aws:ResourceTag/${TagKey}
grant	arn:${Partition}:license-manager::${Account}:grant:${GrantId}	aws:ResourceTag/${TagKey}
report-generator	arn:${Partition}:license-manager:${Region}:${Account}:report-generator:${ReportGeneratorId}	aws:ResourceTag/${TagKey} license-manager:ResourceTag/${TagKey}

AWS License Manager の条件キー

AWS License Manager は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	String

条件キー	説明	タイプ
aws:TagKeys	リクエストで渡されたタグキーによりアクセスをフィルタリングします	ArrayOfString
license-manager:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアでアクセスをフィルタリングします	String

AWS License Manager Linux Subscriptions Manager のアクション、リソース、および条件キー

AWS License Manager Linux Subscriptions Manager (サービスプレフィックス: `license-manager-linux-subscriptions`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS License Manager Linux Subscriptions Manager で定義されるアクション
- AWS License Manager Linux Subscriptions Manager で定義されるリソースタイプ
- AWS License Manager Linux Subscriptions Manager の条件キー

AWS License Manager Linux Subscriptions Manager で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーショ

ンへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeregisterSubscriptionProvider	AWS License Manager でサブスクリプションプロバイダーを完全に削除する許可を付与	書き込み	subscription-provider*		
GetRegisteredSubscriptionProvider	AWS License Manager でサブスクリプションプロバイダーを取得する許可を付与	読み取り	subscription-provider*		
GetServiceSettings	AWS License Manager で Linux サブスクリプションのサービス設定を取得する許可を付与	読み取り			
ListLinuxSubscriptionInstances	AWS License Manager で Linux サブスクリプションを持つすべてのインスタンスを一覧表示する許可を付与	読み取り			
ListLinuxSubscriptions	AWS License Manager ですべての Linux サブスクリプションを一覧表示する許可を付与	読み取り			
ListRegisteredSubscriptionProviders	AWS License Manager でサブスクリプションプロバイダーを一覧表示する許可を付与	読み取り			
ListTagsForResource	選択したリソース用のタグを一覧表示する許可を付与	読み取り	subscription-provider*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RegisterSubscriptionProvider	AWS License Manager で新しいサブスクリプションプロバイダーを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	選択したリソースをタグ付けする許可を付与	タグ付け	subscription-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	選択したリソースのタグを解除する許可を付与	Tagging	subscription-provider*		
				aws:TagKeys	
UpdateServiceSettings	AWS License Manager で Linux サブスクリプションのサービス設定を更新する許可を付与	書き込み			

AWS License Manager Linux Subscriptions Manager で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアク

ションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
subscription-provider	arn:${Partition}:license-manager-linux-subscriptions:${Region}:${Account}:subscription-provider/${SubscriptionProviderId}	aws:ResourceTag/${TagKey}

AWS License Manager Linux Subscriptions Manager の条件キー

AWS License Manager Linux Subscriptions Manager では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーによりアクセスをフィルタリングします	ArrayOfString

AWS License Manager User Subscriptions のアクション、リソース、および条件キー

AWS License Manager ユーザーサブスクリプション (サービスプレフィックス: `license-manager-user-subscriptions`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS License Manager User Subscriptions で定義されるアクション
- AWS License Manager User Subscriptions で定義されるリソースタイプ
- AWS License Manager User Subscriptions の条件キー

AWS License Manager User Subscriptions で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateUser	ライセンスマネージャーユーザーサブスクリプション製品で起動されたインスタンスに、サブスクライブ済みユーザーを関連付けるアクセス許可を付与	書き込み	identity-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseServerEndpoint	特定の ID プロバイダーの特定のサーバータイプのライセンスサーバーエンドポイントを	書き込み	identity-provider*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	作成するアクセス許可を付与します			aws:RequestTag/${TagKey} aws:TagKeys	
DeleteLicenseServerEndpoint	特定の ID プロバイダーの特定のサーバータイプのライセンスサーバーエンドポイントを削除するアクセス許可を付与します	書き込み	identity-provider*		
			license-server-endpoint*		
DeregisterIdentityProvider	製品のライセンスマネージャーユーザーサブスクリプションで Microsoft Active Directory を登録解除するアクセス許可を付与	書き込み	identity-provider*		
DisassociateUser	ライセンスマネージャーユーザーサブスクリプション製品で起動されたインスタンスからサブスクライブ済みユーザーの関連付けを解除するアクセス許可を付与	書き込み	identity-provider*		
			instance-user*		
ListIdentityProviders	ライセンスマネージャーユーザーサブスクリプションのすべての ID プロバイダーを一覧表示するアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListInstances	ライセンスマネージャーユーザーサブスクリプション製品を使用して起動されたすべてのインスタンスを一覧表示するアクセス許可を付与	リスト			
ListLicenseServerEndpoints	ライセンスサーバーエンドポイントを一覧表示する許可を付与	リスト			
ListProductSubscriptions	製品および ID プロバイダーのすべての製品サブスクリプションを一覧表示するアクセス許可を付与	リスト	identity-provider*		
ListTagsForResource	選択したリソース用のタグを一覧表示する許可を付与	読み取り	identity-provider*		
			instance-user*		
			license-server-endpoint*		
			product-subscription*		
ListUserAssociations	製品用に起動されたインスタンスに関連付けられているすべてのユーザーを一覧表示するアクセス許可を付与	リスト	identity-provider*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RegisterIdentityProvider	製品のライセンスマネージャーユーザーサブスクリプションに Microsoft Active Directory を登録するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
StartProductSubscription	製品の登録済みアクティブディレクトリでユーザーの製品サブスクリプションを開始するアクセス許可を付与	書き込み	identity-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StopProductSubscription	製品の登録済みアクティブディレクトリでユーザーの製品サブスクリプションを停止するアクセス許可を付与	書き込み	identity-provider*		
			product-subscription*		
TagResource	選択したリソースをタグ付けする許可を付与	タグ付け	identity-provider*		
			instance-user*		
			license-server-endpoint*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			product-subscription*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	選択したリソースのタグを解除する許可を付与	Tagging	identity-provider*		
			instance-user*		
			license-server-endpoint*		
			product-subscription*		
UpdateIdentityProviderSettings	ID プロバーダー設定を更新する許可を付与	書き込み	identity-provider*		

AWS License Manager User Subscriptions で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
identity-provider	arn:${Partition}:license-manager-user-subscriptions:${Region}:${Account}:identity-provider/${IdentityProviderId}	aws:ResourceTag/${TagKey}
product-subscription	arn:${Partition}:license-manager-user-subscriptions:${Region}:${Account}:product-subscription/${ProductSubscriptionId}	aws:ResourceTag/${TagKey}
instance-user	arn:${Partition}:license-manager-user-subscriptions:${Region}:${Account}:instance-user/${InstanceUserId}	aws:ResourceTag/${TagKey}
license-server-endpoint	arn:${Partition}:license-manager-user-subscriptions:${Region}:${Account}:license-server-endpoint/${LicenseServerEndpointId}	aws:ResourceTag/${TagKey}

AWS License Manager User Subscriptions の条件キー

AWS License Manager ユーザーサブスクリプションでは、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーによりアクセスをフィルタリングします	ArrayOfString

Amazon Lightsailのアクション、リソース、および条件キー

Amazon Lightsail (サービスプレフィックス: `lightsail`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Lightsailで定義されるアクション
- Amazon Lightsail で定義されるリソースタイプ
- Amazon Lightsail の条件キー

Amazon Lightsailで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AllocateStaticIp	インスタンスにアタッチできる静的 IP アドレスを作成する許可を付与	書き込み			
AttachCertificateToDistribution	Amazon Lightsail コンテンツ配信ネットワーク (CDN) ディストリビューションに SSL/TLS 証明書をアタッチする許可を付与する	書き込み	Certificate*		
			Distribution*		
AttachDisk	インスタンスにディスクをアタッチする許可を付与	書き込み	Disk*		
AttachInstancesToLoadBalancer	1 つ以上のインスタンスをロードバランサーにアタッチする許可を付与	書き込み	LoadBalancer*		
AttachLoadBalancerTlsCertificate	ロードバランサー TLS 証明書をアタッチする許可を付与	書き込み	LoadBalancer*		
AttachStaticIp	インスタンスに静的 IP アドレスをアタッチする許可を付与	書き込み	Instance*		
			StaticIp*		
CloseInstancePublicPorts	インスタンスのパブリックポートを閉じる許可を付与	書き込み	Instance*		
CopySnapshot	の 1 つの から別の にスナップショットをコピー AWS リージョン するアクセス許可を付与します Amazon Lightsail	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateBucket	Amazon Lightsail バケットを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateBucketAccessKey	指定したバケットの新しいアクセスキーを作成する許可を付与	書き込み	Bucket*		
CreateCertificate	SSL/TLS 証明書を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	lightsail:CreateDomainEntry lightsail:GetDomains
CreateCloudFormationStack	エクスポートされた Amazon Lightsail スナップショットから新しい Amazon EC2 インスタンスを作成する許可を付与する	書き込み			
CreateContactMethod	E メールまたは SMS テキストメッセージの連絡方法を作成する許可を付与	書き込み			
CreateContainerService	Amazon Lightsail コンテナサービスを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateContainerServiceDeployment	Amazon Lightsail コンテナサービスのデプロイを作成する許可を付与する	書き込み	ContainerService*		
CreateContainerServiceRegistryLogin	ローカルマシン上の Docker プロセスにログインするために使用できるログイン認証情報の一時的なセットを作成する許可を付与	書き込み			
CreateDisk	ディスクを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDiskFromSnapshot	スナップショットからディスクを作成する許可を付与	書き込み	DiskSnapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDiskSnapshot	ディスクのスナップショットを作成する許可を付与	書き込み	Disk		
			Instance		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDistribution	Amazon Lightsail コンテンツ配信ネットワーク (CDN) ディストリビューションを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateDomain	指定されたドメイン名のドメインリソースを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	route53:DeleteHostedZone route53:GetHostedZone route53:ListHostedZonesByName route53domains:GetDomainDetail route53domains:GetOperationDetail route53domains:ListDomains route53domains:ListOperations route53domains:UpdateDomain

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					Nameservers
CreateDomainEntry	ドメインリソースの 1 つ以上の DNS レコードエントリを作成する許可を付与: アドレス (A)、正規名 (CNAME)、メールエクスチェンジャー (MX)、ネームサーバー (NS)、Start of Authority (SOA)、サービスロケーター (SRV)、またはテキスト (TXT)	書き込み	Domain*		
CreateGUISessionAccessDetails	インスタンスのグラフィカルユーザーインターフェイス (GUI) セッションへのアクセスに使用される URL を作成するための許可を付与します	書き込み	Instance*		
CreateInstanceSnapshot	インスタンスのスナップショットを作成する許可を付与	書き込み	Instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInstances	1 つ以上のインスタンスを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateInstancesFromSnapshot	インスタンスのスナップショットに基づいて 1 つ以上のインスタンスを作成する許可を付与	書き込み	InstanceSnapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateKeyPair	インスタンスの認証と接続に使用するキーペアを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLoadBalancer	ロードバランサーを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	lightsail:CreateDomainEntry lightsail:GetDomains
CreateLoadBalancerTlsCertificate	ロードバランサー TLS 証明書を作成する許可を付与	書き込み	LoadBalancer*		lightsail:CreateDomainEntry lightsail:GetDomains

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateRelationalDatabase	新しいリレーショナルデータベースを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRelationalDatabaseFromSnapshot	スナップショットから新しいリレーショナルデータベースを作成する許可を付与	書き込み	RelationalDatabaseSnapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRelationalDatabaseSnapshot	リレーショナルデータベースのスナップショットを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlarm	アラームを削除する許可を付与	書き込み	Alarm*		
DeleteAutoSnapshot	インスタンスまたはディスクの自動スナップショットを削除する許可を付与	書き込み			
DeleteBucket	Amazon Lightsail バケットを削除する許可を付与する	書き込み	Bucket*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteBucketAccessKey	指定した Amazon Lightsail バケットのアクセスキーを削除する許可を付与する	書き込み	Bucket*		
DeleteCertificate	SSL/TLS 証明書を削除する許可を付与	書き込み	Certificate*		
DeleteContactMethod	連絡方法を削除する許可を付与	書き込み			
DeleteContainerImage	Amazon Lightsail コンテナサービスに登録されているコンテナイメージを削除する許可を付与する	書き込み	ContainerService*		
DeleteContainerService	Amazon Lightsail コンテナサービスを削除する許可を付与する	書き込み	ContainerService*		
DeleteDisk	ディスクを削除する許可を付与	書き込み	Disk*		
DeleteDiskSnapshot	ディスクスナップショットを削除する許可を付与	書き込み	DiskSnapshot*		
DeleteDistribution	Amazon Lightsail コンテンツ配信ネットワーク (CDN) ディストリビューションを削除する許可を付与する	書き込み	Distribution*		
DeleteDomain	ドメインリソースとそのすべての DNS レコードを削除する許可を付与	書き込み	Domain*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteDomainEntry	ドメインリソースの DNS レコードを削除する許可を付与	書き込み	Domain*		
DeleteInstance	インスタンスを削除する許可を付与	書き込み	Instance*		
DeleteInstanceSnapshot	インスタンスのスナップショットを削除する許可を付与	書き込み	InstanceSnapshot*		
DeleteKeyPair	インスタンスの認証と接続に使用するキーペアを削除する許可を付与	書き込み	KeyPair*		
DeleteKnownHostKeys	インスタンスを認証するために Amazon Lightsail のブラウザベースの SSH または RDP クライアントで使用される既知のホストキーまたは証明書を削除する許可を付与する	書き込み	Instance*		
DeleteLoadBalancer	ロードバランサーを削除する許可を付与	書き込み	LoadBalancer*		
DeleteLoadBalancerTlsCertificate	ロードバランサー TLS 証明書を削除する許可を付与	書き込み	LoadBalancer*		
DeleteRelationalDatabase	リレーショナルデータベースを削除する許可を付与	書き込み	RelationalDatabase*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteRelationalDatabaseSnapshot	リレーショナルデータベースのスナップショットを削除する許可を付与	書き込み	RelationalDatabaseSnapshot*		
DetachCertificateFromDistribution	Amazon Lightsail コンテンツ配信ネットワーク (CDN) ディストリビューションから SSL/TLS 証明書の接続を解除する許可を付与する	書き込み	Distribution*		
DetachDisk	インスタンスからディスクをデタッチする許可を付与	書き込み	Disk*		
DetachInstancesFromLoadBalancer	1 つ以上のインスタンスをロードバランサーからデタッチする許可を付与	書き込み	LoadBalancer*		
DetachStaticIp	静的 IP をアタッチ先のインスタンスからデタッチする許可を付与	書き込み	StaticIp*		
DisableAddOn	Amazon Lightsail リソースのアドオンを無効にする許可を付与する	書き込み			
DownloadDefaultKeyPair	特定の のインスタンスの認証と接続に使用されるデフォルトのキーペアをダウンロードするアクセス許可を付与します AWS リージョン	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
EnableAddOn	Amazon Lightsail リソースのアドオンを有効化または変更する許可を付与する	書き込み			
ExportSnapshot	Amazon Lightsail スナップショットを Amazon EC2 にエクスポートする許可を付与する	書き込み	DiskSnapshot		iam:CreateServiceLinkedRole iam:PutRolePolicy
			InstanceSnapshot		
GetActiveNames	すべてのアクティブな (削除されていない) リソースの名前を取得する許可を付与	読み込み			
GetAlarms	設定されたアラームに関する情報を表示する許可を付与。	読み込み			
GetAutoSnapshots	インスタンスまたはディスクで使用可能な自動スナップショットを表示する許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetBlueprints	インスタンスイメージまたは設計図のリストを取得する許可を付与 特定のオペレーティングシステムを実行している新しいインスタンスやプリインストールされているアプリケーション、または開発スタックを作成するには、設計図を使用します。インスタンスで実行されるソフトウェアは、インスタンスの作成時に定義した設計図によって異なります。	読み取り			
GetBucketAccessKeys	指定した Amazon Lightsail バケットの既存のアクセスキー ID を取得する許可を付与する	読み取り			
GetBucketBundles	Amazon Lightsail バケットに適用できるバンドルを取得する許可を付与する	読み取り			
GetBucketMetricData	Amazon Lightsail バケットの特定のメトリクスのデータポイントを取得する許可を付与する	読み取り			
GetBuckets	1 つまたは複数の Amazon Lightsail バケットの情報を取得する許可を付与する	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetBundles	インスタンスバンドルのリストを取得する許可を付与。バンドルを使用して、CPU 数、ディスクサイズ、RAM サイズ、ネットワーク転送枠など、一連のパフォーマンス仕様を持つ新しいインスタンスを作成できます。インスタンスのコストは、インスタンスの作成時に定義したバンドルによって異なります。	読み取り			
GetCertificates	1 つ以上の Amazon Lightsail SSL/TLS 証明書に関する情報を表示する許可を付与する	読み取り			
GetCloudFormationStackRecords	エクスポートされた Amazon Lightsail スナップショットから Amazon EC2 リソースを作成するために使用されるすべての CloudFormation スタックに関する情報を取得する許可を付与する	読み取り			
GetContactMethods	構成された連絡方法に関する情報を表示する許可を付与	読み取り			
GetContainerAPIMetadata	Lightsail コントロール (lightsailctl) プラグインの最新バージョンなど、Amazon Lightsail コンテナに関する情報を表示するアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetContainerImages	Amazon Lightsail コンテナサービスに登録されているコンテナイメージを表示する許可を付与する	読み取り			
GetContainerLog	Amazon Lightsail コンテナサービスのコンテナのログイベントを表示する許可を付与する	読み取り			
GetContainerServiceDeployments	Amazon Lightsail コンテナサービスのデプロイを表示する許可を付与する	読み取り			
GetContainerServiceMetricData	Amazon Lightsail コンテナサービスの指定されたメトリックのデータポイントを表示する許可を付与する	読み取り			
GetContainerServicePowers	Amazon Lightsail コンテナサービスに指定できる許可のリストを表示する許可を付与する	読み取り			
GetContainerServices	1 つ以上の Amazon Lightsail コンテナサービスに関する情報を表示する許可を付与する	読み取り			
GetCostEstimate	指定されたリソースのコスト見積りに関する情報を取得するための許可を付与します	読み取り	Disk		
			Instance		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetDisk	ディスクに関する情報を取得する許可を付与	読み込み			
GetDiskSnapshot	ディスクのスナップショットに関する情報を取得する許可を付与	読み込み			
GetDiskSnapshots	すべてのディスクのスナップショットに関する情報を取得する許可を付与	読み込み			
GetDisks	すべてのディスクに関する情報を取得する許可を付与	読み取り			
GetDistributionBundles	Amazon Lightsail コンテンツ配信ネットワーク (CDN) ディストリビューションに適用できるバンドルのリストを表示する許可を付与する	読み取り			
GetDistributionLatestCacheReset	指定された Amazon Lightsail コンテンツ配信ネットワーク (CDN) ディストリビューションの最終キャッシュリセット時のタイムスタンプとステータスを表示する許可を付与する	読み取り			
GetDistributionMetricData	Amazon Lightsail コンテンツ配信ネットワーク (CDN) ディストリビューションの指定されたメトリックのデータポイントを表示する許可を付与する	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetDistributions	1 つ以上の Amazon Lightsail コンテンツ配信ネットワーク (CDN) ディストリビューションに関する情報を表示する許可を付与する	読み取り			
GetDomain	ドメインリソースの DNS レコードを取得する許可を付与	読み込み			
GetDomains	すべてのドメインリソースの DNS レコードを取得する許可を付与	読み取り			
GetExportSnapshotRecords	Amazon EC2 にエクスポートされた Amazon Lightsail スナップショットのすべてのレコードに関する情報を取得する許可を付与する	読み取り			
GetInstance	インスタンスに関する情報を取得する許可を付与	読み込み			
GetInstanceAccessDetails	インスタンスを認証して接続するために使用できる一時キーを取得する許可を付与	書き込み	Instance*		
GetInstanceMetricData	インスタンスの指定されたメトリクスのデータポイントを取得する許可を付与	読み込み			
GetInstancePortStates	インスタンスのポートのステータスを取得する許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetInstanceSnapshot	インスタンスのスナップショットに関する情報を取得する許可を付与	読み込み			
GetInstanceSnapshots	すべてのインスタンスのスナップショットに関する情報を取得する許可を付与	読み込み			
GetInstanceState	インスタンスのステータスを取得する許可を付与	読み込み			
GetInstances	すべてのインスタンスに関する情報を取得する許可を付与	読み込み			
GetKeyPair	キーペアに関する情報を取得する許可を付与	読み込み			
GetKeyPairs	すべてのキーペアに関する情報を取得する許可を付与	読み取り			
GetLoadBalancer	ロードバランサーに関する情報を取得する許可を付与	読み取り			
GetLoadBalancerMetricData	ロードバランサーの指定されたメトリクスのデータポイントを取得する許可を付与	読み込み			
GetLoadBalancerTlsCertificates	ロードバランサーの TLS 証明書に関する情報を取得する許可を付与	読み取り			
GetLoadBalancerTlsPolicies	Lightsail ロードバランサーに適用できる TLS セキュリティポリシーのリストを取得する許可を付与する	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetLoadBalancers	ロードバランサーに関する情報を取得する許可を付与	読み込み			
GetOperation	オペレーションに関する情報を取得する許可を付与 オペレーションには、インスタンスの作成、静的 IP の割り当て、静的 IP のアタッチなどのイベントなどを含む	読み込み			
GetOperations	オペレーションに関する情報を取得する許可を付与。オペレーションには、インスタンスの作成、静的 IP の割り当て、静的 IP のアタッチなどのイベントなどを含む	読み込み			
GetOperationsForResource	リソースのオペレーションを取得する許可を付与	読み取り			
GetRegions	に有効なすべての のリストを取得するアクセス許可を付与 AWS リージョン します Amazon Lightsail	読み取り			
GetRelationalDatabase	リレーショナルデータベースに関する情報を取得する許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetRelationalDatabaseBlueprints	リレーショナルデータベースイメージまたは設計図のリストを取得する許可を付与 設計図を使用して、特定のデータベースエンジンを実行する新しいデータベースを作成できます。データベースで実行されるデータベースエンジンは、リレーショナルデータベースの作成時に定義した設計図によって異なります	読み込み			
GetRelationalDatabaseBundles	リレーショナルデータベースの設計図のリストを取得する許可を付与。バンドルを使用して、CPU 数、ディスクサイズ、RAM サイズ、ネットワーク転送許容量、高可用性の標準など、一連のパフォーマンス仕様を持つ新しいデータベースを作成できます。データベースのコストは、リレーショナルデータベースの作成時に定義したバンドルによって異なります	読み込み			
GetRelationalDatabaseEvents	リレーショナルデータベースのイベントを取得する許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetRelationalDatabaseLogEvents	リレーショナルデータベースの指定されたログストリームのイベントを取得する許可を付与	読み込み			
GetRelationalDatabaseLogStreams	リレーショナルデータベースで使用できるログストリームを取得する許可を付与	読み込み			
GetRelationalDatabaseMasterUserPassword	リレーショナルデータベースのマスターユーザーパスワードを取得する許可を付与	書き込み	RelationalDatabase*		
GetRelationalDatabaseMetricData	リレーショナルデータベースの指定されたメトリクスのデータポイントを取得する許可を付与	読み込み			
GetRelationalDatabaseParameters	リレーショナルデータベースのパラメータを取得する許可を付与	読み込み			
GetRelationalDatabaseSnapshot	リレーショナルデータベースのスナップショットに関する情報を取得する許可を付与	読み込み			
GetRelationalDatabaseSnapshots	すべてのリレーショナルデータベースのスナップショットに関する情報を取得する許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetRelationalDatabases	すべてのリレーショナルデータベースに関する情報を取得する許可を付与	読み取り			
GetSetupHistory	指定されたリソースで実行されたセットアップリクエストの詳細情報を取得する許可を付与する	読み取り	Instance		
GetStaticIp	静的 IP に関する情報を取得する許可を付与	読み込み			
GetStaticIps	すべての静的 IP に関する情報を取得する許可を付与	読み込み			
ImportKeyPair	キーペアからパブリックキーをインポートする許可を付与	書き込み			
IsVpcPeered	Amazon Lightsail 仮想プライベートクラウド (VPC) がピアリング接続されているかどうかを示すブール値を取得する許可を付与する	読み取り			
OpenInstancePublicPorts	インスタンスのパブリックポートを追加または開く許可を付与	書き込み	Instance*		
PeerVpc	Amazon Lightsail 仮想プライベートクラウド (VPC) をデフォルト VPC とピア接続する許可を付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutAlarm	アラームを作成または更新するアクセス許可を付与し、指定したメトリックに関連付け	書き込み	Alarm*		
PutInstancePublicPorts	インスタンスに指定された開いているポートを設定し、リクエストに含まれていないすべてのプロトコルのすべてのポートを閉じる許可を付与	書き込み	Instance*		
RebootInstance	実行状態のインスタンスを再起動する許可を付与	書き込み	Instance*		
RebootRelationalDatabase	実行状態のリレーショナルデータベースを再起動する許可を付与	書き込み	RelationalDatabase*		
RegisterContainerImage	コンテナイメージを Amazon Lightsail コンテナサービスに登録する許可を付与する	書き込み	ContainerService*		
ReleaseStaticIp	静的 IP を削除する許可を付与	書き込み	StaticIp*		
ResetDistributionCache	Amazon Lightsail コンテンツ配信ネットワーク (CDN) ディストリビューションから現在キャッシュされているコンテンツを削除する許可を付与する	書き込み	Distribution*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SendContactMethodVerification	検証リクエストを E メールの連絡方法に送信して、リクエスターが所有していることを確認する許可を付与	書き込み			
SetIpAddressType	Amazon Lightsail リソースの IP アドレスのタイプを設定する許可を付与する	書き込み	Distribution		
			Instance		
			LoadBalancer		
SetResourceAccessForBucket	指定された Amazon Lightsail バケットにアクセスできる Amazon Lightsail リソースを設定する許可を付与する	書き込み	Bucket*		
			Instance*		
SetupInstanceHttps	SSL/TLS 証明書を作成し、指定したインスタンスにインストールする許可を付与する	書き込み	Instance*		lightsail:GetInstanceAccessDetails
StartGUISession	インスタンスのオペレーティングシステムまたはアプリケーションへのアクセスに使用されるグラフィカルユーザーインターフェイス (GUI) セッションを開始するための許可を付与します	書き込み	Instance*		
StartInstance	停止状態のインスタンスを起動する許可を付与	書き込み	Instance*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartRelationalDatabase	停止状態のリレーショナルデータベースを起動する許可を付与	書き込み	RelationalDatabase*		
StopGUISession	インスタンスのオペレーティングシステムまたはアプリケーションへのアクセスに使用されるグラフィカルユーザーインターフェイス (GUI) セッションを終了するための許可を付与します	書き込み	Instance*		
StopInstance	実行状態のインスタンスを停止する許可を付与	書き込み	Instance*		
StopRelationalDatabase	実行状態のリレーショナルデータベースを停止する許可を付与	書き込み	RelationalDatabase*		
TagResource	リソースにタグを付けるアクセス許可を付与	Tagging	Bucket		
			Certificate		
			ContainerService		
			Disk		
			DiskSnapshot		
			Distribution		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			Domain		
			Instance		
			InstanceSnapshot		
			KeyPair		
			LoadBalancer		
			RelationalDatabase		
			RelationalDatabaseSnapshot		
			StaticIp		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TestAlarm	Amazon Lightsail コンソールにバナーを表示するか、指定したアラームに対して通知トリガーが設定されている場合は、通知プロトコルに通知を送信することにより、アラームをテストする許可を付与する	書き込み	Alarm*		
UnpeerVpc	Amazon Lightsail 仮想プライベートクラウド (VPC) をデフォルト VPC からピア接続解除しようとする許可を付与する	書き込み			
UntagResource	リソースのタグを解除する許可を付与	Tagging	Bucket		
			Certificate		
			ContainerService		
			Disk		
			DiskSnapshot		
			Distribution		
			Domain		
			Instance		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			InstanceSnapshot		
			KeyPair		
			LoadBalancer		
			RelationalDatabase		
			RelationalDatabaseSnapshot		
			StaticIp		
				aws:TagKeys	
UpdateBucket	既存の Amazon Lightsail バケットを更新する許可を付与する	書き込み	Bucket*		
UpdateBucketBundle	既存の Amazon Lightsail バケットのバンドルまたはストレージプランを更新する許可を付与する	書き込み	Bucket*		
UpdateContainerService	Amazon Lightsail コンテナサービス (パワー、スケール、パブリックドメイン名など) の設定を更新する許可を付与する	書き込み	ContainerService*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateDistribution	既存の Amazon Lightsail コンテンツ配信ネットワーク (CDN) ディストリビューションまたはその設定を更新する許可を付与	書き込み	Distribution*		
UpdateDistributionBundle	Amazon Lightsail コンテンツ配信ネットワーク (CDN) ディストリビューションのバンドルを更新する許可を付与する	書き込み	Distribution*		
UpdateDomainEntry	作成後、ドメインの RecordSet を更新する許可を付与	書き込み	Domain*		
UpdateInstanceMetadataOptions	インスタンスのメタデータオプションを更新するための許可を付与します	書き込み	Instance*		
UpdateLoadBalancerAttribute	ヘルスチェックパスやセッション維持などのロードバランサー属性を更新する許可を付与	書き込み	LoadBalancer*		
UpdateRelationalDatabase	リレーショナルデータベースを更新する許可を付与	書き込み	RelationalDatabase*		
UpdateRelationalDatabaseParameters	リレーショナルデータベースのパラメータを更新する許可を付与	書き込み	RelationalDatabase*		

Amazon Lightsail で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Domain	arn:${Partition}:lightsail:${Region}:${Account}:Domain/${Id}	aws:ResourceTag/${TagKey}
Instance	arn:${Partition}:lightsail:${Region}:${Account}:Instance/${Id}	aws:ResourceTag/${TagKey}
InstanceSnapshot	arn:${Partition}:lightsail:${Region}:${Account}:InstanceSnapshot/${Id}	aws:ResourceTag/${TagKey}
KeyPair	arn:${Partition}:lightsail:${Region}:${Account}:KeyPair/${Id}	aws:ResourceTag/${TagKey}
StaticIp	arn:${Partition}:lightsail:${Region}:${Account}:StaticIp/${Id}	aws:ResourceTag/${TagKey}
Disk	arn:${Partition}:lightsail:${Region}:${Account}:Disk/${Id}	aws:ResourceTag/${TagKey}
DiskSnapshot	arn:${Partition}:lightsail:${Region}:${Account}:DiskSnapshot/${Id}	aws:ResourceTag/${TagKey}
LoadBalancer	arn:${Partition}:lightsail:${Region}:${Account}:LoadBalancer/${Id}	aws:ResourceTag/${TagKey}
LoadBalancerTlsCertificate	arn:${Partition}:lightsail:${Region}:${Account}:LoadBalancerTlsCertificate/${Id}	

リソースタイプ	ARN	条件キー
ExportSnapshotRecord	arn:${Partition}:lightsail:${Region}:${Account}:ExportSnapshotRecord/${Id}	
CloudFormationStackRecord	arn:${Partition}:lightsail:${Region}:${Account}:CloudFormationStackRecord/${Id}	
RelationalDatabase	arn:${Partition}:lightsail:${Region}:${Account}:RelationalDatabase/${Id}	aws:ResourceTag/${TagKey}
RelationalDatabaseSnapshot	arn:${Partition}:lightsail:${Region}:${Account}:RelationalDatabaseSnapshot/${Id}	aws:ResourceTag/${TagKey}
Alarm	arn:${Partition}:lightsail:${Region}:${Account}:Alarm/${Id}	
Certificate	arn:${Partition}:lightsail:${Region}:${Account}:Certificate/${Id}	aws:ResourceTag/${TagKey}
ContactMethod	arn:${Partition}:lightsail:${Region}:${Account}:ContactMethod/${Id}	
ContainerService	arn:${Partition}:lightsail:${Region}:${Account}:ContainerService/${Id}	aws:ResourceTag/${TagKey}
Distribution	arn:${Partition}:lightsail:${Region}:${Account}:Distribution/${Id}	aws:ResourceTag/${TagKey}
Bucket	arn:${Partition}:lightsail:${Region}:${Account}:Bucket/${Id}	aws:ResourceTag/${TagKey}

Amazon Lightsail の条件キー

Amazon Lightsail では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString

Amazon Location のアクション、リソース、および条件キー

Amazon Location (サービスプレフィックス: geo) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Location で定義されるアクション
- Amazon Location で定義されるリソースタイプ

- Amazon Location の条件キー

Amazon Location で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateTrackerConsumer	ジオフェンスコレクションとトラッカーリソースの間の関連付けを作成する権限を付与します	Write	tracker*		
BatchDeleteDevicePositionHistory	トラッカーリソースからデバイス位置履歴のバッチを削除する許可を付与	Write	tracker*		
				geo:DeviceIds	
BatchDeleteGeofence	ジオフェンスのコレクションからジオフェンスのバッチを削除する権限を付与します	Write	geofence-collection*		
				geo:GeofenceIds	
BatchEvaluateGeofences	所与のジオフェンスコレクション内のジオフェンスの位置に照らしてデバイスの位置を評価する権限を付与します	Write	geofence-collection*		
BatchGetDevicePosition	デバイスの位置を取得するためのバッチリクエストを送信する権限を付与します	Read	tracker*		
				geo:DeviceIds	
BatchPutGeofence	所与のジオフェンスコレクションにジオフェンスを追加するバッチリクエストを送信する権限を付与します	Write	geofence-collection*		
				geo:GeofenceIds	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchUpdateDevicePosition	1 つ異常のデバイスの位置更新をトラッカーリソースにアップロードする権限を付与します	Write	tracker*		
				geo:DeviceIds	
CalculateRoute	指定されたルート計算リソースを使用してルートを計算する許可を付与	読み取り	route-calculator*		
CalculateRouteMatrix	指定済みルート計算リソースを使用して、ルートマトリクスを計算する許可を付与します	読み取り	route-calculator*		
CreateGeofenceCollection	ジオフェンスコレクションを作成する権限を付与します	書き込み	geofence-collection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateKey	API キーリソースを作成するための許可を付与します	書き込み	api-key*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateMap	マップリソースを作成する権限を付与します	Write	map*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePlaceIndex	場所インデックスリソースを作成する権限を付与します	Write	place-index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRouteCalculator	ルート計算リソースを作成する許可を付与	Write	route-calculator*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTracker	トラッカーリソースを作成する権限を付与します	Write	tracker*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGeofenceCollection	ジオフェンスコレクションを削除する許可を付与	書き込み	geofence-collection*		
DeleteKey	API キーリソースを削除するための許可を付与します	書き込み	api-key*		
DeleteMap	マップリソースを削除する権限を付与します	Write	map*		
DeletePlaceIndex	場所インデックスリソースを削除する権限を付与します	Write	place-index*		
DeleteRouteCalculator	ルート計算リソースを削除する許可を付与	Write	route-calculator*		
DeleteTracker	トラッカーリソースを削除する権限を付与します	Write	tracker*		
DescribeGeofenceCollection	ジオフェンスコレクションの詳細を取得する許可を付与	読み取り	geofence-collection*		
DescribeKey	API キーリソースの詳細とシークレットを取得するための許可を付与します	読み取り	api-key*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeMap	マップリソースの詳細を取得する許可を付与。	Read	map*		
DescribePlaceIndex	場所インデックスリソースの詳細を取得する許可を付与	Read	place-index*		
DescribeRouteCalculator	ルート計算リソースの詳細を取得する許可を付与	Read	route-calculator*		
DescribeTracker	トラッカーリソースの詳細を取得する権限を付与します	Read	tracker*		
DisassociateTrackerConsumer	トラッカーリソースとジオフェンスコレクションの間の関連付けを削除する権限を付与します。	書き込み	tracker*		
ForecastGeofenceEvents	特定のジオフェンスコレクションに保存されているジオフェンスのイベントを予測する許可を付与する	読み取り	geofence-collection*		
GetDevicePosition	最新のデバイス位置を取得する権限を付与します	読み取り	tracker*		
				geo:DeviceIds	
GetDevicePositionHistory	デバイス位置履歴を取得する許可を付与します	読み取り	tracker*		
				geo:DeviceIds	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetGeofence	ジオフェンスコレクションからジオフェンスの詳細を取得する許可を付与します	読み取り	geofence-collection*		
				geo:GeofenceIds	
GetMapGlyphs	マップリソースのグリフファイルを取得する権限を付与します	Read	map*		
GetMapSprites	マップリソースのスプライトファイルを取得する権限を付与します	Read	map*		
GetMapStyleDescriptor	マップリソースからマップスタイル記述子を取得するパーミッションを付与します	Read	map*		
GetMapTile	マップリソースからマップタイルを取得する権限を付与します	読み取り	map*		
GetPlace	ユニーク ID でその場所を検索する許可を付与	読み取り	place-index*		
ListDevicePositions	指定されたトラッカーリソースからデバイスのリストと最新の位置を取得する許可を付与	読み取り	tracker*		
ListGeofenceCollections	ジオフェンスコレクションを一覧表示する権限を付与します	リスト	geofence-collection*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListGeofences	所与のジオフェンスのコレクションに保存されているジオフェンスを一覧表示する権限を付与します	読み取り	geofence-collection*		
ListKeys	API キーリソースを一覧表示するための許可を付与します	リスト	api-key*		
ListMaps	マップリソースを一覧表示する権限を付与します	リスト	map*		
ListPlaceIndexes	場所インデックスリソースのリストを返す権限を付与します	リスト	place-index*		
ListRouteCalculators	ルート計算リソースのリストを返すアクセス許可を付与します	リスト	route-calculator*		
ListTagsForResource	リソースに割り当てたタグ (メタデータ) を一覧表示する許可を付与	Read	api-key		
			geofence-collection		
			map		
			place-index		
			route-calculator		
			tracker		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTrackerConsumers	所与のトラッカーリソースに現在関連付けられているジオフェンスコレクションのリストを取得する権限を付与します	Read	tracker*		
ListTrackers	トラッカーリソースのリストを返す権限を付与します	リスト	tracker*		
PutGeofence	新しいジオフェンスを追加したり、既存のジオフェンスを更新して所与のジオフェンスコレクションにする権限を付与します	Write	geofence-collection*		
				geo:GeofenceIds	
SearchPlaceIndexForPosition	所与の座標を逆ジオコーディングする権限を付与します	読み取り	place-index*		
SearchPlaceIndexForSuggestions	部分的またはスペルミスのある自由形式のテキストに基づいて、住所および対象となるポイントの候補を生成する許可を付与	読み取り	place-index*		
SearchPlaceIndexForText	住所、名前、都市、地域など自由形式のテキストをジオコーディングする権限を付与します	Read	place-index*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagResource	指定されたリソースのタグに追加するアクセス許可、またはタグを変更する許可を付与。タグは、リソースを管理するために使用できるメタデータです	タグ付け	api-key		
			geofence-collection		
			map		
			place-index		
			route-calculator		
			tracker		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	指定のタグ (メタデータ) をリソースから削除する許可を付与	Tagging	api-key		
			geofence-collection		
			map		
			place-index		
			route-calculator		
			tracker		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
UpdateGeofenceCollection	ジオフェンスコレクションを更新する許可を付与	書き込み	geofence-collection*		
UpdateKey	API キーリソースを更新するための許可を付与します	書き込み	api-key*		
UpdateMap	マップリソースを更新する許可を付与	書き込み	map*		
UpdatePlaceIndex	場所インデックスリソースを更新する許可を付与	書き込み	place-index*		
UpdateRouteCalculator	ルート計算リソースを更新する許可を付与	書き込み	route-calculator*		
UpdateTracker	トラッカーリソースを更新する許可を付与	書き込み	tracker*		
VerifyDevicePosition	デバイスの位置を確認する許可を付与する	読み取り	tracker*		
				geo:DeviceIds	

Amazon Location で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
api-key	arn:${Partition}:geo:${Region}:${Account}:api-key/${KeyName}	aws:ResourceTag/${TagKey}
geofence-collection	arn:${Partition}:geo:${Region}:${Account}:geofence-collection/${GeofenceCollectionName}	aws:ResourceTag/${TagKey} geo:GeofenceIds
map	arn:${Partition}:geo:${Region}:${Account}:map/${MapName}	aws:ResourceTag/${TagKey}
place-index	arn:${Partition}:geo:${Region}:${Account}:place-index/${IndexName}	aws:ResourceTag/${TagKey}
route-calculator	arn:${Partition}:geo:${Region}:${Account}:route-calculator/${CalculatorName}	aws:ResourceTag/${TagKey}
tracker	arn:${Partition}:geo:${Region}:${Account}:tracker/${TrackerName}	aws:ResourceTag/${TagKey} geo:DeviceIds

Amazon Location の条件キー

Amazon Location では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグのキーと値でアクセスをフィルター	String
aws:ResourceTag/${TagKey}	リクエスト内のタグキーおよび値のペアのプレゼンスによってアクションをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString
geo:DeviceIds	リクエスト内のデバイス ID の有無でアクセスをフィルタリング	ArrayOfString
geo:GeofenceIds	リクエスト内のジオフェンス ID の有無でアクセスをフィルタリング	ArrayOfString

Amazon Location Service Maps のアクション、リソース、および条件キー

Amazon Location Service Maps (サービスプレフィックス: geo-maps) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Location Service Maps で定義されるアクション
- Amazon Location Service Maps で定義されるリソースタイプ
- Amazon Location Service Maps の条件キー

Amazon Location Service Maps で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetStaticMap	静的マップを取得するアクセス許可を付与します	読み取り	provider*		
GetTile	マップタイルを取得するアクセス許可を付与します	読み取り	provider*		

Amazon Location Service Maps で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
provider	`arn:${Partition}:geo-maps:${Region}::provider/default`	

Amazon Location Service Maps の条件キー

Geo Maps には、ポリシーステートメントの Condition要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Location Service Places のアクション、リソース、および条件キー

Amazon Location Service Places (サービスプレフィックス: geo-places) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Location Service Places で定義されるアクション
- Amazon Location Service Places で定義されるリソースタイプ
- Amazon Location Service Places の条件キー

Amazon Location Service Places で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
Autocomplete	ユーザータイプとして潜在的な場所とアドレスを含むテキスト入力をオートコンプリートするアクセス許可を付与します	読み取り	provider*		
Geocode	テキストアドレスをジオコードしたり、地理的座標に配置するアクセス許可を付与します	読み取り	provider*		
GetPlace	unqiue place ID を使用して場所をクエリするアクセス許可を付与します	読み取り	provider*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ReverseGeocode	地理的座標を人間が読めるアドレスまたは場所に変換するアクセス許可を付与します	読み取り	provider*		
SearchNearby	場所によって提供されるカテゴリや食品タイプなど、ユーザー定義の一連の制限に一致する位置の近くの場所を取得するアクセス許可を付与します	読み取り	provider*		
SearchText	1 つの自由形式のテキスト入力を使用して場所をクエリするアクセス許可を付与します	読み取り	provider*		
Suggest	ユーザーの入力に基づいて潜在的な場所を提案するアクセス許可を付与します	読み取り	provider*		

Amazon Location Service Places で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
provider	`arn:${Partition}:geo-places:${Region}::provider/default`	

Amazon Location Service Places の条件キー

Geo Places には、ポリシーステートメントの Condition要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Location Service Routes のアクション、リソース、および条件キー

Amazon Location Service Routes (サービスプレフィックス: geo-routes) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Location Service Routes で定義されるアクション
- Amazon Location Service Routes で定義されるリソースタイプ
- Amazon Location Service Routes の条件キー

Amazon Location Service Routes で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にア

クションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
Calculate Isolines	指定された時間内に到達可能な送信先またはサービスエリアを決定するアクセス許可を付与します	読み取り	provider*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CalculateRouteMatrix	送信元と送信先のセット間の移動時間と距離を提供するルーティングマトリックスを計算するアクセス許可を付与します	読み取り	provider*		
CalculateRoutes	2 つ以上の口ケーション間のルートを計算するアクセス許可を付与します	読み取り	provider*		
OptimizeWaypoints	ルートに沿って複数のウェイポイントまたは口ケーションにアクセスするための最も効率的なシーケンスを計算するアクセス許可を付与します	読み取り	provider*		
SnapToRoads	GPS 座標をデジタルマップ上の最も近い道路セグメントに合わせることで、地理的配置の精度を高めるアクセス許可を付与します	読み取り	provider*		

Amazon Location Service Routes で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
provider	arn:${Partition}:geo-routes:${Region}::provider/default	

Amazon Location Service Routes の条件キー

Geo Routes には、ポリシーステートメントの Condition要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Lookout for Equipment のアクション、リソース、および条件キー

Amazon Lookout for Equipment (サービスプレフィックス: lookoutequipment) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Lookout for Equipment で定義されているアクション
- Amazon Lookout for Equipment で定義されているリソースタイプ
- Amazon Lookout for Equipment の条件キー

Amazon Lookout for Equipment で定義されているアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateDataset	データセットを作成する許可を付与	書き込み	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInferenceScheduler	トレーニングされたモデルの推論スケジューラを作成する許可を付与	書き込み	inference-scheduler*		
			model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLabel	ラベルを作成するアクセス許可を付与	書き込み	label-group*		
CreateLabelGroup	ラベルグループを作成するアクセス許可を付与	書き込み	label-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateModel	データセットでトレーニングされたモデルを作成する許可を付与	書き込み	dataset*		
			model*		
			label-group		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRetrainingScheduler	トレーニング済みモデルの再トレーニングスケジューラを作成する許可を付与	書き込み	model*		
DeleteDataset	データセットを削除する許可を付与	書き込み	dataset*		
DeleteInferenceScheduler	推論スケジューラを削除する許可を付与	書き込み	inference-scheduler*		
DeleteLabel	ラベルを削除するアクセス許可を付与	書き込み	label-group*		
DeleteLabelGroup	ラベルグループを削除するアクセス許可を付与	書き込み	label-group*		
DeleteModel	モデルを削除する許可を付与	書き込み	model*		
DeleteResourcePolicy	リソースポリシーを削除する許可を付与。	書き込み	dataset		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			model		
			model-version		
DeleteRetrainingScheduler	トレーニング済みモデルの再トレーニングスケジューラを削除する許可を付与	書き込み	model*		
DescribeDataIngestionJob	データ取り込みジョブを説明する許可を付与	読み込み			
DescribeDataset	データセットを記述するアクセス許可を付与	読み込み	dataset*		
DescribeInferenceScheduler	推論スケジューラを説明する許可を付与	読み取り	inference-scheduler*		
DescribeLabelGroup	ラベルグループを記述するアクセス許可を付与	読み取り	label-group*		
DescribeModel	モデルを記述する許可を付与	読み取り	model*		
DescribeModelVersion	モデルのバージョンを記述する許可を付与	読み取り	model-version*		
DescribeResourcePolicy	リソースポリシーを記述する許可を付与	読み取り	dataset		
			model		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			model-version		
DescribeRetrainingScheduler	トレーニング済みモデルの再トレーニングスケジューラを記述する許可を付与	読み取り	model*		
DescribeLabel	ラベルを記述するアクセス許可を付与	読み取り	label-group*		
ImportDataset	データセットをインポートする許可を付与	書き込み	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ImportModelVersion	モデルのバージョンをインポートする許可を付与	書き込み	dataset*		
			model*		
			label-group		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys lookoutequipment:IsImportingData	
ListDataIngestionJobs	アカウントまたは特定のデータセットのデータ取り込みジョブを一覧表示する許可を付与	リスト	dataset*		
ListDatasets	アカウント内のデータセットを一覧表示する許可を付与	リスト			
ListInferenceEvents	推論スケジューラの推論イベントを一覧表示する権限を付与する	読み取り	inference-scheduler*		
ListInferenceExecutions	推論スケジューラの推論実行を一覧表示する許可を付与	読み込み	inference-scheduler*		
ListInferenceSchedulers	アカウントに推論スケジューラを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListLabelGroups	アカウント内のラベルグループを一覧表示するアクセス許可を付与	リスト	label-group*		
ListLabels	アカウント内のラベルを一覧表示するアクセス許可を付与	リスト	label-group*		
ListModelVersions	アカウントのモデルバージョンを一覧表示する許可を付与	リスト	model*		
ListModels	アカウントのモデルを一覧表示する許可を付与	リスト			
ListRetrainingSchedulers	アカウントに再トレーニングスケジューラを一覧表示する許可を付与	リスト			
ListSensorStatistics	特定のデータセットまたは取り込みジョブのセンサー統計を一覧表示するアクセス許可を付与	リスト	dataset*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	dataset		
			inference-scheduler		
			label-group		
			model		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			model-version		
PutResourcePolicy	リソースポリシーを配置する許可を付与	書き込み	dataset		
			model		
			model-version		
StartDataIngestionJob	データセットのデータ取り込みジョブを開始する許可を付与	書き込み	dataset*		
StartInferenceScheduler	推論スケジューラを開始する許可を付与	書き込み	inference-scheduler*		
StartRetrainingScheduler	トレーニング済みモデルの再トレーニングスケジューラを開始する許可を付与	書き込み	model*		
StopInferenceScheduler	推論スケジューラを停止する許可を付与	書き込み	inference-scheduler*		
StopRetrainingScheduler	トレーニング済みモデルの再トレーニングスケジューラを停止する許可を付与	書き込み	model*		
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	dataset		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			inference-scheduler		
			label-group		
			model		
			model-version		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースのタグを解除する許可を付与	Tagging	dataset		
			inference-scheduler		
			label-group		
			model		
			model-version		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
UpdateActiveModelVersion	特定の機械学習モデルのアクティブなモデルバージョンを設定する許可を付与	書き込み	model*		
			model-version*		
UpdateInferenceScheduler	推論スケジューラを更新する許可を付与	書き込み	inference-scheduler*		
UpdateLabelGroup	ラベルグループを更新するアクセス許可を付与	書き込み	label-group*		
UpdateModel	トレーニング済みモデルを更新する許可を付与	書き込み	model*		
UpdateRetrainingScheduler	トレーニング済みモデルの再トレーニングスケジューラを更新する許可を付与	書き込み	model*		

Amazon Lookout for Equipment で定義されているリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
dataset	arn:${Partition}:lookoutequipment:${Region}:${Account}:dataset/${DatasetName}/${DatasetId}	aws:ResourceTag/${TagKey}
model	arn:${Partition}:lookoutequipment:${Region}:${Account}:model/${ModelName}/${ModelId}	aws:ResourceTag/${TagKey}
model-version	arn:${Partition}:lookoutequipment:${Region}:${Account}:model/${ModelName}/${ModelId}/model-version/${ModelVersionNumber}	aws:ResourceTag/${TagKey}
inference-scheduler	arn:${Partition}:lookoutequipment:${Region}:${Account}:inference-scheduler/${InferenceSchedulerName}/${InferenceSchedulerId}	aws:ResourceTag/${TagKey}
label-group	arn:${Partition}:lookoutequipment:${Region}:${Account}:label-group/${LabelGroupName}/${LabelGroupId}	aws:ResourceTag/${TagKey}

Amazon Lookout for Equipment の条件キー

Amazon Lookout for Equipment では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString
lookoutequipment:IsImportingData	基盤となるデータのインポート戦略でアクセスをフィルタリング	Bool

Amazon Lookout for Metrics のアクション、リソース、および条件キー

Amazon Lookout for Metrics (サービスプレフィックス: `lookoutmetrics`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Lookout for Metrics で定義されているアクション
- Amazon Lookout for Metrics で定義されているリソースタイプ
- Amazon Lookout for Metrics の条件キー

Amazon Lookout for Metrics で定義されているアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ActivateAnomalyDetector	異常検出器をアクティブ化する許可を付与	書き込み	AnomalyDetector*		
BackTestAnomalyDetector	異常検出器でバックテストを実行する許可を付与	書き込み	AnomalyDetector*		
CreateAlert	異常検出器のアラートを作成する許可を付与	書き込み	Alert*		
			AnomalyDetector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnomalyDetector	異常検出器を作成する許可を付与	書き込み	AnomalyDetector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMetricSet	データセットを作成する許可を付与	書き込み	AnomalyDetector*		
			MetricSet*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
DeactivateAnomalyDetector	異常検出器を無効にする許可を付与	書き込み	AnomalyDetector*		
DeleteAlert	アラートを削除する許可を付与	書き込み	Alert*		
DeleteAnomalyDetector	異常検出器を削除する許可を付与	書き込み	AnomalyDetector*		
DescribeAlert	アラートに関する詳細を取得する許可を付与	読み込み	Alert*		
DescribeAnomalyDetectionExecutions	異常検出ジョブに関する情報を取得する許可を付与	読み込み	AnomalyDetector*		
DescribeAnomalyDetector	異常検出器の詳細を取得する許可を付与	読み込み	AnomalyDetector*		
DescribeMetricSet	データセットに関する詳細を取得する許可を付与	読み込み	MetricSet*		
DetectMetricSetConfig	データソースからメトリクスセット設定を検出するアクセス許可を付与	書き込み	AnomalyDetector*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetAnomalyGroup	影響を受けるメトリクスのグループの詳細を取得する許可を付与	読み込み	AnomalyDetector*		
GetDataQualityMetrics	異常検出器のデータ品質メトリクスを取得する許可を付与	読み込み	AnomalyDetector*		
GetFeedback	異常グループの影響を受けるメトリクスに関するフィードバックを取得するためのアクセス許可を付与	読み込み	AnomalyDetector*		
GetSampleData	Amazon S3 データソースからサンプルレコードの選択を取得するためのアクセス許可を付与	読み込み			
ListAlerts	検出器のアラートのリストを取得する許可を付与	リスト	AnomalyDetector		
ListAnomalyDetectors	異常検出器のリストを取得する許可を付与	リスト			
ListAnomalyGroupRelatedMetrics	異常グループの関連測定値のリストを取得する許可を付与	リスト	AnomalyDetector*		
ListAnomalyGroupSummaries	異常グループのリストを取得する許可を付与	リスト	AnomalyDetector*		
ListAnomalyGroupTimeSeries	異常グループのメジャーに対して影響を受けるメトリクスのリストを取得するためのアクセス許可を付与	リスト	AnomalyDetector*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListMetricSets	データセットのリストを取得する許可を付与	リスト	AnomalyDetector		
ListTagsForResource	ディテクター、データセット、またはアラートのタグのリストを取得するためのアクセス許可を付与	読み込み	Alert		
			AnomalyDetector		
			MetricSet		
PutFeedback	異常グループの影響を受けるメトリクスのフィードバックを追加する許可を付与	書き込み	AnomalyDetector*		
TagResource	ディテクター、データセット、またはアラートにタグを追加する許可を付与	タグ付け	Alert		
			AnomalyDetector		
			MetricSet		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	ディテクター、データセット、アラートからタグを削除する許可を付与	Tagging	Alert		
			AnomalyDetector		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			MetricSet		
				aws:TagKeys	
UpdateAlert	異常検出器のアラートを更新する許可を付与	書き込み	Alert*		
UpdateAnomalyDetector	異常検出器を更新する許可を付与	書き込み	AnomalyDetector*		
UpdateMetricSet	データセットを更新するアクセス許可を付与	書き込み	MetricSet*		

Amazon Lookout for Metrics で定義されているリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
AnomalyDetector	`arn:${Partition}:lookoutmetrics:${Region}:${Account}:AnomalyDetector:${AnomalyDetectorName}`	aws:ResourceTag/${TagKey}
MetricSet	`arn:${Partition}:lookoutmetrics:${Region}:${Account}:MetricSet/${AnomalyDetectorName}/${MetricSetName}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
Alert	arn:${Partition}:lookoutmetrics:${Region}:${Account}:Alert:${AlertName}	aws:ResourceTag/${TagKey}

Amazon Lookout for Metrics の条件キー

Amazon Lookout for Metrics では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon Lookout for Vision のアクション、リソース、および条件キー

Amazon Lookout for Vision (サービスプレフィックス: lookoutvision) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Lookout for Vision で定義されているアクション
- Amazon Lookout for Vision で定義されているリソースタイプ
- Amazon Lookout for Vision の条件キー

Amazon Lookout for Vision で定義されているアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateDataset	データセットマニフェストを作成するアクセス許可を付与	書き込み			
CreateModel	新しい異常検出モデルを作成するアクセス許可を付与	書き込み	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProject	新しいプロジェクトを作成するアクセス許可を付与	書き込み	project*		
DeleteDataset	データセットを削除する許可を付与	書き込み			
DeleteModel	モデルおよび関連するすべてのアセットを削除するアクセス許可を付与	書き込み	model*		
DeleteProject	プロジェクトを完全に削除するアクセス許可を付与	書き込み	project*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeDataset	データセットマニフェストに関する詳細情報を表示するアクセス許可を付与	読み込み			
DescribeModel	モデルに関する詳細情報を表示するアクセス許可を付与	読み込み	model*		
DescribeModelPackagingJob	モデルパッケージングジョブに関する詳細情報を表示する許可を付与	読み込み			
DescribeProject	プロジェクトに関する詳細情報を表示するアクセス許可を付与	読み込み	project*		
DescribeTrialDetection [許可のみ]	実行中の異常検出ジョブに関するステータス情報を提供するアクセス許可を付与	読み込み			
DetectAnomalies	異常検出を呼び出すアクセス許可を付与	書き込み	model*		
ListDatasetEntries	データセットマニフェストの内容を一覧表示するアクセス許可を付与	読み込み			
ListModelPackagingJobs	プロジェクトに関連付けられているすべてのモデルパッケージングジョブを一覧表示する許可を付与	リスト			
ListModels	プロジェクトに関連付けられているすべてのモデルを一覧表示するアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListProjects	すべてのプロジェクトを一覧表示するアクセス許可を付与	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み込み	model		
ListTrialDetections [許可のみ]	すべての異常検出ジョブを一覧表示するアクセス許可を付与	リスト			
StartModel	異常検出モデルを開始するアクセス許可を付与	書き込み	model*		
StartModelPackagingJob	モデルパッケージングジョブを開始する許可を付与	書き込み	model*		
StartTrialDetection [アクセス許可のみ]	S3 バケットに保存された一連のイメージについて異常の一括検出を開始する剣健を付与	書き込み			
StopModel	異常検出モデルを停止する許可を付与	書き込み	model*		
TagResource	指定されたキーと値のペアでリソースにタグを付けるアクセス許可を付与	Tagging	model		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource		Tagging	model		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	所与のキーを持つタグをリソースから削除する許可を付与			aws:TagKeys	
UpdateDatasetEntries	トレーニングまたはテストデータセットのマニフェストを更新するアクセス許可を付与	書き込み			

Amazon Lookout for Vision で定義されているリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
model	arn:${Partition}:lookoutvision:${Region}:${Account}:model/${ProjectName}/${ModelVersion}	aws:ResourceTag/${TagKey}
project	arn:${Partition}:lookoutvision:${Region}:${Account}:project/${ProjectName}	

Amazon Lookout for Vision の条件キー

Amazon Lookout for Vision では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon Machine Learning のアクション、リソース、および条件キー

Amazon Machine Learning (サービスプレフィックス: `machinelearning`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Machine Learning で定義されるアクション
- Amazon Machine Learning で定義されるリソースタイプ
- Amazon Machine Learning の条件キー

Amazon Machine Learning で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddTags	1 つ以上のタグをオブジェクトに追加します (最大 10 個)。各タグはキーとオプションの値で構成されます。	タグ付け	batchprediction		
			datasource		
			evaluation		
			mlmodel		
CreateBatchPrediction	観測グループの予測を生成します。	Write	batchprediction*		
			datasource*		
			mlmodel*		
CreateDataSourceFromRDS	Amazon RDS から DataSource オブジェクトを作成します。	Write	datasource*		
CreateDataSourceFromRedshift	Amazon Redshift クラスターでホストされているデータベースから DataSource を作成します。	Write	datasource*		
CreateDataSourceFromS3	S3 から DataSource オブジェクトを作成します。	Write	datasource*		
CreateEvaluation	MLModel の新しい評価を作成します。	Write	datasource*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			evaluation*		
			mlmodel*		
CreateMLModel	新しい MLModel を作成します。	Write	datasource*		
			mlmodel*		
CreateRealtimeEndpoint	MLModel のリアルタイムエンドポイントを作成します。	Write	mlmodel*		
DeleteBatchPrediction	DELETED ステータスを BatchPrediction に割り当て、使用できない状態にします。	Write	batchprediction*		
DeleteDataSource	DELETED ステータスを DataSource に割り当て、使用できない状態にします。	Write	datasource*		
DeleteEvaluation	DELETED ステータスを Evaluation に割り当て、使用できない状態にします。	Write	evaluation*		
DeleteMLModel	DELETED ステータスを MLModel に割り当て、使用できない状態にします。	Write	mlmodel*		
DeleteRealtimeEndpoint	MLModel のリアルタイムエンドポイントを削除します。	Write	mlmodel*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteTags	ML オブジェクトに関連付けられている指定されたタグを削除します。このオペレーションが完了すると、削除されたタグを復旧することはできません。	タグ付け	batchprediction		
			datasource		
			evaluation		
			mlmodel		
DescribeBatchPredictions	リクエスト内の検索条件に一致する BatchPrediction オペレーションのリストを返します。	リスト			
DescribeDataSources	リクエスト内の検索条件に一致する DataSource のリストを返します。	リスト			
DescribeEvaluations	リクエスト内の検索条件に一致する DescribeEvaluations のリストを返します。	リスト			
DescribeMLModels	リクエスト内の検索条件に一致する MLModel のリストを返します。	リスト			
DescribeTags	1 つ以上の Amazon ML オブジェクトのタグについて説明します。	リスト	batchprediction		
			datasource		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			evaluation		
			mlmodel		
GetBatchPrediction	詳細なメタデータ、ステータス、およびデータファイル情報を含む BatchPrediction を返します。	Read	batchprediction*		
GetDataSource	メタデータやデータファイル情報、DataSource の現在のステータスを含む DataSource を返します。	Read	datasource*		
GetEvaluation	メタデータと Evaluation の現在のステータスを含む Evaluation を返します。	Read	datasource*		
GetMLModel	詳細なメタデータ、データソース情報、および MLModel の現在のステータスを含む MLModel を返します。	Read	mlmodel*		
Predict	指定した ML モデルを使用して観察の予測を生成します。	Write	mlmodel*		
UpdateBatchPrediction	BatchPrediction の BatchPredictionName を更新します。	Write	batchprediction*		
UpdateDataSource	DataSource の DataSourceName を更新します。	Write	datasource*		
UpdateEvaluation	Evaluation の EvaluationName を更新します。	Write	evaluation*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateMLModel	MLModel の MLModelName と ScoreThreshold を更新します。	Write	mlmodel*		

Amazon Machine Learning で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
batchprediction	`arn:${Partition}:machinelearning:${Region}:${Account}:batchprediction/${BatchPredictionId}`	
datasource	`arn:${Partition}:machinelearning:${Region}:${Account}:datasource/${DatasourceId}`	
evaluation	`arn:${Partition}:machinelearning:${Region}:${Account}:evaluation/${EvaluationId}`	
mlmodel	`arn:${Partition}:machinelearning:${Region}:${Account}:mlmodel/${MlModelId}`	

Amazon Machine Learning の条件キー

Machine Learning には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Macie のアクション、リソース、および条件キー

Amazon Macie (サービスプレフィックス: macie2) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Macie で定義されるアクション
- Amazon Macie で定義されるリソースタイプ
- Amazon Macie の条件キー

Amazon Macie で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

> **Note**
>
> DisassociateFromMasterAccount アクションと GetMasterAccount アクションは廃止されました。代わりに、DisassociateFromAdministratorAccount アクションと GetAdministratorAccount アクションをそれぞれ指定することをお勧めします。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptInvitation	Amazon Macie メンバーシップへの招待を承諾する許可を付与。	Write			
BatchGetCustomDataIdentifiers	1 つ以上のカスタムデータ識別子に関する情報を取得する許可を付与	読み取り	CustomDataIdentifier*		
BatchUpdateAutomatedDiscoveryAccounts	組織内の 1 つ以上のアカウントの機密データの自動検出のステータスを変更する許可を Amazon Macie 管理者に付与する	書き込み			
CreateAllowList	許可リストの設定を作成および定義するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateClassificationJob	機密データ検出ジョブの設定を作成および定義する許可を付与	Write	ClassificationJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomDataIdentifier	カスタムデータ識別子の設定を作成および定義する許可を付与	Write	CustomDataIdentifier*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingsFilter	結果フィルターの設定を作成および定義する許可を付与	Write	FindingsFilter*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInvitations	Amazon Macie メンバーシップ招待状を送信する許可を付与	Write			
CreateMember	アカウントを Amazon Macie 管理者アカウントに関連付けるアクセス許可を付与	Write	Member*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSampleFindings	サンプル結果を作成する許可を付与。	Write			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeclineInvitations	Amazon Macie メンバーシップへの招待を拒否する許可を付与	書き込み			
DeleteAllowList	許可リストを削除するアクセス許可を付与	書き込み	AllowList*		
DeleteCustomDataIdentifier	カスタムデータ識別子を削除する許可を付与	Write	CustomDataIdentifier*		
DeleteFindingsFilter	結果フィルターを削除する許可を付与	Write	FindingsFilter*		
DeleteInvitations	Amazon Macie メンバーシップの招待状を削除する許可を付与	Write			
DeleteMember	Amazon Macie 管理者アカウントとアカウント間の関連付けを削除する許可を付与	Write	Member*		
DescribeBuckets	Amazon Macie が監視および分析する S3 バケットに関する統計データおよびその他の情報を取得する許可を付与	Read			
DescribeClassificationJob	機密データ検出ジョブのステータスと設定に関する情報を取得する許可を付与	読み取り	ClassificationJob*		
DescribeOrganizationConfiguration	AWS 組織の Amazon Macie 設定に関する情報を取得するアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisableMacie	Amazon Macie アカウントを無効にする許可を付与。これにより、アカウントの Macie リソースも削除されます	書き込み			
DisableOrganizationAdminAccount	AWS 組織の委任 Amazon Macie 管理者アカウントとしてアカウントを無効にするアクセス許可を付与します	書き込み			
DisassociateFromAdministratorAccount	Macie 管理者アカウントとの関連付けを解除するアクセス許可を Amazon Macie メンバーアカウントに付与	書き込み			
DisassociateFromMasterAccount	Macie 管理者アカウントとの関連付けを解除するアクセス許可を Amazon Macie メンバーアカウントに付与	書き込み			
DisassociateMember	Macie メンバーアカウントとの関連付けを解除するアクセス許可を Amazon Macie 管理者アカウントに付与	書き込み	Member*		
EnableMacie	新しい Amazon Macie アカウントの設定を有効にして指定するためのアクセス許可を付与	書き込み			
EnableOrganizationAdminAccount	AWS 組織の委任 Amazon Macie 管理者アカウントとしてアカウントを有効にするアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetAdministratorAccount	Amazon Macie 管理者アカウントに関する情報を取得するアクセス許可をアカウントに付与	読み取り			
GetAllowList	許可リストの設定とステータスを取得するアクセス許可を付与	読み取り	AllowList*		
GetAutomatedDiscoveryConfiguration	Amazon Macie 管理者アカウント、組織、またはスタンドアロンアカウントの機密データ自動検出の設定とステータスを取得する許可を付与する	読み取り			
GetBucketStatistics	Amazon Macie が監視および分析するすべての S3 バケットの集計された統計データを取得する許可を付与	Read			
GetClassificationExportConfiguration	機密データ検出結果をエクスポートするための設定を取得する許可を付与	読み取り			
GetClassificationScope	アカウントにおける分類スコープ設定を取得する許可を付与	読み取り			
GetCustomDataIdentifier	カスタムデータ識別子の設定に関する情報を取得する許可を付与	Read	CustomDataIdentifier*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetFindingStatistics	結果に関する集計された統計データを取得する許可を付与	Read			
GetFindings	1 つまたは複数の結果の詳細を取得する許可を付与	Read			
GetFindingsFilter	結果フィルターの設定に関する情報を取得する許可を付与	読み取り	FindingsFilter*		
GetFindingsPublicationConfiguration	AWS Security Hub に結果を発行するための設定を取得するアクセス許可を付与します	読み取り			
GetInvitationsCount	アカウントで受け取った Amazon Macie メンバーシップの招待状の数を取得する許可を付与	Read			
GetMacieSession	Amazon Macie アカウントのステータスと構成設定に関する情報を取得する許可を付与	読み取り			
GetMasterAccount	Amazon Macie 管理者アカウントに関する情報を取得するアクセス許可をアカウントに付与	読み取り			
GetMember	Amazon Macie 管理者アカウントに関連付けられているアカウントに関する情報を取得する許可を付与	読み取り	Member*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetResourceProfile	S3 バケットの機密データ検出統計と機密性スコアを取得する許可を付与	読み取り			
GetRevealConfiguration	検出結果によって報告された機密データの出現の取得のために、ステータスと構成設定を取得する許可を付与	読み取り			
GetSensitiveDataOccurrences	検出結果によって報告された機密データの出現を取得する許可を付与	読み取り			
GetSensitiveDataOccurrencesAvailability	検出結果のために機密データの出現を取得できるかどうかを確認する許可を付与	読み取り			
GetSensitivityInspectionTemplate	アカウントの機密性検出テンプレート設定を取得する許可を付与	読み取り			
GetUsageStatistics	1 つ以上のアカウントのクォータと集計された使用状況データを取得する許可を付与	Read			
GetUsageTotals	アカウントの集計使用状況データを取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListAllowLists	アカウントのすべての許可リストに関する情報のサブセットを取得するアクセス許可を付与	リスト			
ListAutomatedDiscoveryAccounts	アカウントにおける機密データの自動検出ステータスを取得する許可を付与する	リスト			
ListClassificationJobs	1 つ以上の機密データ検出ジョブのステータスと設定に関する情報を取得する許可を付与	リスト			
ListClassificationScopes	アカウントの分類スコープに関する情報のサブセットを取得する許可を付与	リスト			
ListCustomDataIdentifiers	すべてのカスタムデータ識別子に関する情報を取得する許可を付与	リスト			
ListFindings	1 つ以上の結果に関する情報のサブセットを取得する許可を付与	リスト			
ListFindingsFilters	すべての結果フィルターに関する情報を取得する許可を付与	リスト			
ListInvitations	アカウントから受け取ったすべての Amazon Macie メンバーシップ招待状に関する情報を取得する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListManagedDataIdentifiers	マネージドデータ識別子に関する情報を取得する許可を付与	リスト			
ListMembers	Amazon Macie マスターアカウントに関連付けられている Macie 管理者アカウントに関する情報を取得する許可を付与	リスト			
ListOrganizationAdminAccounts	AWS 組織の委任 Amazon Macie 管理者アカウントに関する情報を取得する許可を付与	リスト			
ListResourceProfileArtifacts	機密データの自動検出用に S3 バケットから Amazon Macie が選択したオブジェクトに関する情報を取得する許可を付与する	リスト			
ListResourceProfileDetections	Amazon Macie が S3 バケットで見つけた機密データの種類と量に関する情報を取得する許可を付与	リスト			
ListSensitivityInspectionTemplates	アカウントの機密性検出テンプレートに関する情報のサブセットを取得する許可を付与	リスト			
ListTagsForResource	Amazon Macie リソースのタグを取得する許可を付与	Read	AllowList		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			ClassificationJob		
			CustomDataIdentifier		
			FindingsFilter		
			Member		
PutClassificationExportConfiguration	機密データ検出結果を保存するための設定を作成または更新する許可を付与	書き込み			
PutFindingsPublicationConfiguration	AWS Security Hub に結果を発行するための設定を更新するアクセス許可を付与します	書き込み			
SearchResources	Amazon Macie がモニタリングおよび分析する AWS リソースに関する統計データやその他の情報を取得する許可を付与	読み取り			
TagResource	Amazon Macie リソースのタグを追加または更新する許可を付与	タグ付け	AllowList		
			ClassificationJob		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			CustomDataIdentifier		
			FindingsFilter		
			Member		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestCustomDataIdentifier	カスタムデータ識別子をテストする許可を付与	Write			
UntagResource	Amazon Macie リソースからタグを削除する許可を付与。	Tagging	AllowList		
			ClassificationJob		
			CustomDataIdentifier		
			FindingsFilter		
			Member		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
UpdateAllowList	許可リストの設定を更新するアクセス許可を付与	書き込み	AllowList*		
UpdateAutomatedDiscoveryConfiguration	Amazon Macie 管理者アカウント、組織、またはスタンドアロンアカウントの機密データの自動検出のステータスを変更する許可を付与する	書き込み			
UpdateClassificationJob	機密データ検出ジョブのステータスを変更する許可を付与	書き込み	ClassificationJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateClassificationScope	アカウントにおける分類スコープ設定を更新する許可を付与	書き込み			
UpdateFindingsFilter	結果フィルターの設定を更新する許可を付与	書き込み	FindingsFilter*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateMacieSession	メンバーアカウントに対して Macie を一時停止または再有効化するアクセス許可を Amazon Macie 管理者アカウントに付与する	書き込み			
UpdateMemberSession	Macie メンバーアカウントを一時停止または再有効化するアクセス許可を Amazon Macie 管理者アカウントに付与	書き込み			
UpdateOrganizationConfiguration	AWS 組織の Amazon Macie 構成設定を更新する許可を付与	書き込み			
UpdateResourceProfile	S3 バケットの機密性スコアを更新する許可を付与	書き込み			
UpdateResourceProfileDetections	S3 バケットの機密性スコア設定を更新する許可を付与	書き込み			
UpdateRevealConfiguration	検出結果によって報告された機密データの出現の取得のために、ステータスと構成設定を更新する許可を付与	書き込み			
UpdateSensitivityInspectionTemplate	アカウントの機密性検出テンプレート設定を更新する許可を付与	書き込み			

Amazon Macie で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
AllowList	arn:${Partition}:macie2:${Region}:${Account}:allow-list/${ResourceId}	aws:ResourceTag/${TagKey}
ClassificationJob	arn:${Partition}:macie2:${Region}:${Account}:classification-job/${ResourceId}	aws:ResourceTag/${TagKey}
CustomDataIdentifier	arn:${Partition}:macie2:${Region}:${Account}:custom-data-identifier/${ResourceId}	aws:ResourceTag/${TagKey}
FindingsFilter	arn:${Partition}:macie2:${Region}:${Account}:findings-filter/${ResourceId}	aws:ResourceTag/${TagKey}
Member	arn:${Partition}:macie2:${Region}:${Account}:member/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon Macie の条件キー

Amazon Macie では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

AWS Mainframe Modernization アプリケーションテストのアクション、リソース、条件キー

AWS Mainframe Modernization アプリケーションテスト (サービスプレフィックス: apptest) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Mainframe Modernization アプリケーションテストで定義されるアクション
- AWS Mainframe Modernization アプリケーションテストで定義されるリソースタイプ
- AWS Mainframe Modernization アプリケーションテストの条件キー

AWS Mainframe Modernization アプリケーションテストで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateTestCase	テストケースを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTestConfiguration	テスト設定を作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTestSuite	テストスイートを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTestCase	テストケースを削除する許可を付与する	書き込み	TestCase*		
DeleteTestConfiguration	テスト設定を削除する許可を付与する	書き込み	TestConfiguration*		
DeleteTestRun	テスト実行を削除する許可を付与する	書き込み	TestRun*		s3:DeleteObject s3:ListBucket

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteTestSuite	テストスイートを削除する許可を付与する	書き込み	TestSuite*		
GetTestCase	テストケースを取得する許可を付与する	読み取り	TestCase*		
GetTestConfiguration	テスト設定を取得する許可を付与する	読み取り	TestConfiguration*		
GetTestRunStep	テスト実行ステップを取得する許可を付与する	読み取り	TestRun*		
GetTestSuite	テストスイートを取得する許可を付与する	読み取り	TestSuite*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り			
ListTestCases	テストケースを一覧表示する許可を付与する	リスト			
ListTestConfigurations	テスト設定を一覧表示する許可を付与する	リスト			
ListTestRunSteps	テスト実行のステップを一覧表示する許可を付与する	読み取り	TestRun*		
ListTestRunTestCases	テスト実行のテストケースを一覧表示する許可を付与する	読み取り	TestRun*		
ListTestRuns	テスト実行を一覧表示する許可を付与する	リスト			
ListTestSuites	テストスイーツを一覧表示する許可を付与する	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartTestRun	テスト実行を開始する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	cloudformation:CreateStack cloudformation:DeleteStack cloudformation:DescribeStacks dms:DescribeReplicationTasks dms:StartReplicationTask dms:StopReplicationTask ec2:DescribeAvailabilityZones ec2:DescribeVpcEndpointServ

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					iceConfigurations ec2:DescribeVpcEndpointServices m2:CreateDataSetImportTask m2:GetApplication m2:GetApplicationVersion m2:GetBatchJobExecution m2:GetDataSetDetails m2:GetDataSetImportTask m2:StartApplication m2:StartBatchJob

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					m2:StopApplication s3:CreateBucket s3:DeleteObject s3:GetObject s3:ListBucket s3:PutObject
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	TestCase		
			TestConfiguration		
			TestRun		
			TestSuite		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースのタグを解除する許可を付与	Tagging	TestCase		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			TestConfiguration		
			TestRun		
			TestSuite		
				aws:TagKeys	
UpdateTestCase	テストケースを更新する許可を付与する	書き込み	TestCase*		
UpdateTestConfiguration	テスト設定を更新する許可を付与する	書き込み	TestConfiguration*		
UpdateTestSuite	テストスイートを更新する許可を付与する	書き込み	TestSuite*		

AWS Mainframe Modernization アプリケーションテストで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
TestCase	`arn:${Partition}:apptest:${Region}:${Account}:testcase/${TestCaseId}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
TestConfiguration	arn:${Partition}:apptest:${Region}:${Account}:testconfiguration/${TestConfigurationId}	aws:ResourceTag/${TagKey}
TestRun	arn:${Partition}:apptest:${Region}:${Account}:testrun/${TestRunId}	aws:ResourceTag/${TagKey}
TestSuite	arn:${Partition}:apptest:${Region}:${Account}:testsuite/${TestSuiteId}	aws:ResourceTag/${TagKey}

AWS Mainframe Modernization アプリケーションテストの条件キー

AWS Mainframe Modernization アプリケーションテストでは、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString

AWS Mainframe Modernization サービスのアクション、リソース、条件キー

AWS Mainframe Modernization Service (サービスプレフィックス: m2) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Mainframe Modernization サービスで定義されるアクション
- AWS Mainframe Modernization サービスで定義されるリソースタイプ
- AWS Mainframe Modernization サービスの条件キー

AWS Mainframe Modernization サービスで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイ

プが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelBatchJobExecution	バッチジョブの実行をキャンセルする許可を付与	書き込み	Application*		
CreateApplication	アプリケーションを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject s3:ListBucket

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateDataSetExportTask	データセットのエクスポートタスクを作成するアクセス許可を付与します	書き込み	Application*		s3:GetObject
CreateDataSetImportTask	セットインポートタスクを作成する許可を付与	書き込み	Application*		s3:GetObject
CreateDeployment	デプロイを作成する許可を付与	書き込み	Application*		elasticloadbalancing:AddTags elasticloadbalancing:CreateListener elasticloadbalancing:CreateTargetGroup elasticloadbalancing:RegisterTargets
			Environment		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateEnvironment	環境を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcs ec2:ModifyNetworkInterfaceAttribute

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					elasticfilesystem:DescribeMountTargets elasticloadbalancing:AddTags elasticloadbalancing:CreateLoadBalancer fsx:DescribeFileSystems iam:CreateServiceLinkedRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteApplication	アプリケーションを削除する許可を付与	書き込み	Application*		elasticloadbalancing:DeleteListener elasticloadbalancing:DeleteTargetGroup
DeleteApplicationFromEnvironment	ランタイム環境からアプリケーションを削除する許可を付与	書き込み	Application*		elasticloadbalancing:DeleteListener elasticloadbalancing:DeleteTargetGroup
DeleteEnvironment	ランタイム環境を削除する許可を付与	書き込み	Environment*		elasticloadbalancing:DeleteLoadBalancer
GetApplication	アプリケーションを取得する許可を付与	読み取り	Application*		
GetApplicationVersion	アプリケーションバージョンを取得する許可を付与	読み取り	Application*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetBatchJobExecution	バッチジョブ実行を取得するアクセス許可を付与	読み取り	Application*		
GetDataSetDetails	データセットの詳細を取得する許可を付与	読み取り	Application*		
GetDataSetExportTask	指定された S3 ロケーションでデータセットをエクスポートするアクセス許可を付与します	読み取り	Application*		
GetDataSetImportTask	データセットのインポートタスクを取得する許可を付与	読み取り	Application*		
GetDeployment	デプロイを取得する許可を付与	読み取り	Application*		
GetEnvironment	ランタイム環境を取得する許可を付与	読み取り	Environment*		
GetSignedBluinsightsUrl	署名済みの Bluinsights URL を作成する許可を付与	読み取り			
ListApplicationVersions	アプリケーションのバージョンを一覧表示する許可を付与	読み取り	Application*		
ListApplications	アプリケーションを一覧表示する許可を付与	リスト			
ListBatchJobDefinitions	バッチジョブ定義を一覧表示する許可を付与	読み取り	Application*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListBatchJobExecutions	バッチジョブのジョブ実行を一覧表示する許可を付与	読み取り	Application*		
ListBatchJobRestartPoints	バッチジョブ実行を取得するアクセス許可を付与	読み取り	Application*		
ListDataSetExportHistory	データセットのエクスポート履歴を一覧表示する許可を付与	読み取り	Application*		
ListDataSetImportHistory	データセットインポート履歴を一覧表示する許可を付与	読み取り	Application*		
ListDataSets	データセットを一覧表示する許可を付与	読み取り	Application*		
ListDeployments	デプロイを一覧表示する許可を付与	読み取り	Application*		
ListEngineVersions	エンジンバージョンを一覧表示する許可を付与	読み取り			
ListEnvironments	ランタイム環境を一覧表示する許可を付与	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り			
StartApplication	アプリケーションを開始する許可を付与	書き込み	Application*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartBatchJob	バッチジョブを開始する許可を付与	書き込み	Application*		
StopApplication	アプリケーションを停止する許可を付与	書き込み	Application*		
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	Application		
			Environment		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースのタグを解除する許可を付与	タグ付け	Application		
			Environment		
				aws:TagKeys	
UpdateApplication	アプリケーションを更新する許可を付与	書き込み	Application*		s3:GetObject s3:ListBucket

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateEnvironment	ランタイム環境を更新する許可を付与	書き込み	Environment*		

AWS Mainframe Modernization サービスで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Application	`arn:${Partition}:m2:${Region}:${Account}:app/${ApplicationId}`	aws:ResourceTag/${TagKey}
Environment	`arn:${Partition}:m2:${Region}:${Account}:env/${EnvironmentId}`	aws:ResourceTag/${TagKey}

AWS Mainframe Modernization サービスの条件キー

AWS Mainframe Modernization Service では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString

Amazon Managed Blockchain のアクション、リソース、および条件キー

Amazon Managed Blockchain (サービスプレフィックス: `managedblockchain`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Managed Blockchain で定義されるアクション
- Amazon Managed Blockchain で定義されるリソースタイプ
- Amazon Managed Blockchain の条件キー

Amazon Managed Blockchain で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateAccessor	Amazon Managed Blockchain アクセサーを作成するための許可を付与します	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateMember	Amazon Managed Blockchain ネットワークのメンバーを作成する許可を付与	書き込み	network*		iam:CreateServiceLinkedRole
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNetwork	Amazon Managed Blockchain ネットワークを作成する許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateNode	Amazon Managed Blockchain ネットワークのメンバー内にノードを作成する許可を付与	書き込み	member		iam:CreateServiceLinkedRole
			network		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey}	
CreateProposal	Amazon Managed Blockchain ネットワークでメンバーを追加または削除するために、他のブロックチェーンネットワークのメンバーが投票できる提案を作成する許可を付与	書き込み	network*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteAccessor	Amazon Managed Blockchain アクセサーを削除するための許可を付与します	書き込み	accessor*		
DeleteMember	Amazon Managed Blockchain ネットワークからメンバーおよび関連付けられているすべてのリソースを削除する許可を付与	書き込み	member*		
DeleteNode	Amazon Managed Blockchain ネットワークのメンバーからノードを削除する許可を付与	書き込み	node*		
GET [アクセス許可のみ]	HTTP GET リクエストを Ethereum ノードに送信するための許可を付与します	権限の管理			
GetAccessor	Amazon Managed Blockchain アクセサーに関する詳細情報を返すための許可を付与します	読み取り	accessor*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetMember	Amazon Managed Blockchain ネットワークのメンバーに関する詳細情報を返すアクセス許可を付与する	読み込み	member*		
GetNetwork	Amazon Managed Blockchain ネットワークに関する詳細情報を返すアクセス許可を付与する	読み込み	network*		
GetNode	Amazon Managed Blockchain ネットワークのメンバー内のノードに関する詳細情報を返すアクセス許可を付与する	読み込み	node*		
GetProposal	Amazon Managed Blockchain ネットワークの提案に関する詳細情報を返すアクセス許可を付与する	読み取り	proposal*		
Invoke [許可のみ]	Ethereum ノードへの WebSocket 接続を作成するための許可を付与します	権限の管理			
InvokeRpcBitcoinMainnet	Bitcoin Mainnet RPC を呼び出すための許可を付与します	読み取り			
InvokeRpcBitcoinTestnet	Bitcoin Testnet RPC を呼び出すための許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
InvokeRpcPolygonMainnet	Polygon Mainnet RPC を呼び出すためのアクセス許可を付与	読み取り			
InvokeRpcPolygonMumbaiTestnet	Polygon Mumbai Testnet RPC を呼び出すためのアクセス許可を付与	読み取り			
ListAccessors	現在の が所有する Amazon Managed Blockchain アクセサーを一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListInvitations	Managed Blockchain ネットワーク AWS アカウント からアクティブな に拡張された招待を一覧表示するアクセス許可を付与します	リスト			
ListMembers	Amazon Managed Blockchain ネットワークのメンバーとそのメンバーシップのプロパティを一覧表示する許可を付与	リスト	network*		
ListNetworks	現在の が AWS アカウント 参加している Amazon Managed Blockchain ネットワークを一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListNodes	Amazon Managed Blockchain ネットワークのメンバー内のノードを一覧表示する許可を付与	リスト	member		
			network		
ListProposalVotes	投票の値、特定の Amazon Managed Blockchain ネットワークに対して票を投じるメンバーの一意の識別子など、提案に対するすべての投票を一覧表示する許可を付与	読み込み	proposal*		
ListProposals	特定の Amazon Managed Blockchain ネットワークの提案を一覧表示する許可を付与	リスト	network*		
ListTagsForResource	Amazon Managed Blockchain リソースに関連付けられたタグを表示する許可を付与	読み取り	accessor		
			invitation		
			member		
			network		
			node		
			proposal		
POST [許可のみ]	HTTP POST リクエストを Ethereum ノードに送信するための許可を付与します	権限の管理			
RejectInvitation	ブロックチェーンネットワークへの参加招待を拒否する許可を付与	書き込み	invitation*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagResource	Amazon Managed Blockchain リソースにタグを追加する許可を付与	タグ付け	accessor		
			invitation		
			member		
			network		
			node		
			proposal		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Amazon Managed Blockchain リソースからタグを削除する許可を付与	タグ付け	accessor		
			invitation		
			member		
			network		
			node		
			proposal		
				aws:TagKeys	
UpdateMember	Amazon Managed Blockchain ネットワークのメンバーを更新する許可を付与	書き込み	member*		iam:CreateServiceLinkedRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateNode	Amazon Managed Blockchain ネットワークのメンバーからノードを更新する許可を付与	書き込み	node*		iam:CreateServiceLinkedRole
VoteOnProposal	指定されたブロックチェーンネットワークメンバーに代わって提案に票を投じるアクセス許可を付与する	書き込み	proposal*		

Amazon Managed Blockchain で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
network	arn:${Partition}:managedblockchain:${Region}::networks/${NetworkId}	aws:ResourceTag/${TagKey}
member	arn:${Partition}:managedblockchain:${Region}:${Account}:members/${MemberId}	aws:ResourceTag/${TagKey}
node	arn:${Partition}:managedblockchain:${Region}:${Account}:nodes/${NodeId}	aws:ResourceTag/${TagKey}
proposal	arn:${Partition}:managedblockchain:${Region}::proposals/${ProposalId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
invitation	`arn:${Partition}:managedblockchain:${Region}:${Account}:invitations/${InvitationId}`	aws:ResourceTag/${TagKey}
accessor	`arn:${Partition}:managedblockchain:${Region}:${Account}:accessors/${AccessorId}`	aws:ResourceTag/${TagKey}

Amazon Managed Blockchain の条件キー

Amazon Managed Blockchain では、IAM ポリシーの `Condition` 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします。	文字列
aws:ResourceTag/${TagKey}	Amazon Managed Blockchain リソースに関連付けられたタグに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーに基づいてアクションをフィルタリングします。	ArrayOfString

Amazon Managed Blockchain Query のアクション、リソース、および条件キー

Amazon Managed Blockchain Query (サービスプレフィックス: managedblockchain-query) では、IAM 許可ポリシーで使用できるように、次のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Managed Blockchain Query によって定義されたアクション
- Amazon Managed Blockchain Query によって定義されたリソースタイプ
- Amazon Managed Blockchain Query の条件キー

Amazon Managed Blockchain Query によって定義されたアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchGetTokenBalance	GetTokenBalance API のバッチ呼び出しを実行するための許可を付与します	読み取り			
GetAssetContract	ブロックチェーン上の契約に関する情報を取得するアクセス許可を付与します	読み取り			
GetTokenBalance	ブロックチェーン上のアドレスについてのトークン残高を取得するための許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetTransaction	ブロックチェーン上のトランザクションを取得するための許可を付与します	読み取り			
ListAssetContracts	ブロックチェーン上の複数の契約を取得するためのアクセス許可を付与します	リスト			
ListFilteredTransactionEvents	追加のフィルターを使用してブロックチェーン上のイベントを取得する許可を付与する	リスト			
ListTokenBalances	ブロックチェーン上の複数の残高を取得するための許可を付与します	リスト			
ListTransactionEvents	ブロックチェーン上のトランザクション内のイベントを取得するための許可を付与します	リスト			
ListTransactions	ブロックチェーン上の複数のトランザクションを取得するための許可を付与します	リスト			

Amazon Managed Blockchain Query によって定義されたリソースタイプ

Amazon Managed Blockchain Query では、IAM ポリシーステートメントの `Resource` 要素でのリソース ARN の指定はサポートされていません。Amazon Managed Blockchain Query に対するアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

Amazon Managed Blockchain Query の条件キー

Managed Blockchain Query には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Managed Grafana のアクション、リソース、および条件キー

Amazon Managed Grafana (サービスプレフィックス: grafana) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Managed Grafana で定義されるアクション
- Amazon Managed Grafana で定義されるリソースタイプ
- Amazon Managed Grafana の条件キー

Amazon Managed Grafana で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
Associate License	ライセンスを使用してワークスペースをアップグレードする許可を付与	書き込み	workspace *		aws-marketplace:ViewSubscriptions

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateWorkspace	ワークスペースを作成するアクセス許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetManagedPrefixListEntries iam:CreateServiceLinkedRole organizations:DescribeOrganization sso:CreateManagedApplicationInstance sso:DescribeRegisteredRegions sso:GetSharedSsoCo

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					nfiguration
CreateWorkspaceApiKey	ワークスペースの API キーを作成するための許可を付与します	書き込み	workspace*		
CreateWorkspaceServiceAccount	ワークスペースのサービスアカウントを作成する許可を付与する	書き込み	workspace*		
CreateWorkspaceServiceAccountToken	ワークスペースのサービスアカウントトークンを作成する許可を付与する	書き込み	workspace*		
DeleteWorkspace	ワークスペースを削除するアクセス許可を付与	書き込み	workspace*		sso:DeleteManagedApplicationInstance
DeleteWorkspaceApiKey	ワークスペースから API キーを削除する許可を付与します	書き込み	workspace*		
DeleteWorkspaceServiceAccount	ワークスペースのサービスアカウントを削除する許可を付与する	書き込み	workspace*		
DeleteWorkspaceServiceAccountToken	ワークスペースのサービスアカウントトークンを削除する許可を付与する	書き込み	workspace*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeWorkspace	ワークスペースを記述する権限を付与します	読み込み	workspace*		
DescribeWorkspaceAuthentication	ワークスペースで認証プロバイダーを記述するアクセス許可を付与します	読み取り	workspace*		
DescribeWorkspaceConfiguration	指定されたワークスペースの現在の設定文字列を記述するための許可を付与します	読み取り	workspace*		
DisassociateLicense	ワークスペースからライセンスを削除する許可を付与	書き込み	workspace*		
ListPermissions	WorkSpace に対するアクセス許可を一覧表示する許可を付与	リスト	workspace*		
ListTagsForResource	ワークスペースに関連付けられているタグを一覧表示するアクセス許可を付与します	読み取り	workspace		
ListVersions	利用可能なサポートされているすべての Grafana バージョンを一覧表示するための許可を付与します オプションで、アップグレード可能なバージョンを一覧表示するワークスペースを含めます。	リスト	workspace		
ListWorkspaceServiceAccountTokens	ワークスペースのサービスアカウントトークンを一覧表示する許可を付与する	読み取り	workspace*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListWorkspaceServiceAccounts	ワークスペースのサービスアカウントを一覧表示する許可を付与する	読み取り	workspace*		
ListWorkspaces	ワークスペースを一覧表示する許可を付与します	読み込み			
TagResource	ワークスペースにタグを追加したり、タグ値を更新したりするアクセス許可を付与します	Tagging	workspace*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	ワークスペースからタグを削除するアクセス許可を付与します	Tagging	workspace*		
				aws:TagKeys	
UpdatePermissions	WorkSpace に対するアクセス許可を変更する許可を付与	Permissions management	workspace*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateWorkspace	WorkSpace を変更する許可を付与	書き込み	workspace*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetManagedPrefixListEntries iam:CreateServiceLinkedRole
UpdateWorkspaceAuthentication	ワークスペースで認証プロバイダーを変更するアクセス許可を付与します	書き込み	workspace*		
UpdateWorkspaceConfiguration	指定されたワークスペースの設定文字列を更新するための許可を付与します	書き込み	workspace*		

Amazon Managed Grafana で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
workspace	arn:${Partition}:grafana:${Region}:${Account}:/workspaces/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon Managed Grafana の条件キー

Amazon Managed Grafana では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーおよび値のペアのプレゼンスに基づいてアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアに基づいてアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいたアクションでアクセスをフィルタリングします	ArrayOfString

Amazon Managed Service for Prometheus のアクション、リソース、および条件キー

Amazon Managed Service for Prometheus (サービスプレフィックス: aps) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Managed Service for Prometheus で定義されるアクション
- Amazon Managed Service for Prometheus で定義されるリソースタイプ
- Amazon Managed Service for Prometheus の条件キー

Amazon Managed Service for Prometheus で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateAlertManagerAlerts	アラートを作成するためのアクセス許可を付与する	書き込み	workspace*		
				aws:ResourceTag/${TagKey}	
CreateAlertManagerDefinition	アラートマネージャ定義を作成するためのアクセス許可を付与する	書き込み	workspace*		
				aws:ResourceTag/${TagKey}	
CreateLoggingConfiguration	ログ記録設定を作成する許可を付与	書き込み	workspace*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateQueryLoggingConfiguration	クエリログ記録設定を作成するアクセス許可を付与します	書き込み	workspace*		
				aws:ResourceTag/${TagKey}	
CreateRuleGroupsNamespace	ルールグループ名前空間を作成するためのアクセス許可を付与する	書き込み	rulegroupsnamespace*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateScraper	スクレイパーを作成するためのアクセス許可を付与	書き込み	cluster*		aps:TagResource ec2:DescribeSecurityGroups ec2:DescribeSubnets eks:DescribeCluster iam:CreateServiceLinkedRole
			workspace*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateWorkspace	ワークスペースを作成するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlertManagerDefinition	アラートマネージャ定義を削除するためのアクセス許可を付与する	書き込み	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteAlertManagerSilence	サイレンス (silence) を削除するためのアクセス許可を付与する	書き込み	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteLoggingConfiguration	ログ記録設定を削除する許可を付与	書き込み	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteQueryLoggingConfiguration	クエリログ記録設定を削除するアクセス許可を付与します	書き込み	workspace*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteResourcePolicy	ワークスペースリソースポリシーを削除するアクセス許可を付与します	書き込み	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteRuleGroupsNamespace	ルールグループ名前空間を削除するためのアクセス許可を付与する	書き込み	rulegroupsnamespace*		
				aws:ResourceTag/${TagKey}	
DeleteScraper	スクレイパーを削除するためのアクセス許可を付与	書き込み	scraper*		
				aws:ResourceTag/${TagKey}	
DeleteWorkspace	ワークスペースを削除するアクセス許可を付与	書き込み	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeAlertManagerDefinition	アラートマネージャ定義を詳細表示するためのアクセス許可を付与する	読み取り	workspace*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeLoggingConfiguration	ログ記録設定を記述する許可を付与	読み取り	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeQueryLoggingConfiguration	クエリログ記録設定を記述するアクセス許可を付与します	読み取り	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeResourcePolicy	ワークスペースリソースポリシーを記述するアクセス許可を付与します	読み取り	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeRuleGroupsNamespace	ルールグループ名前空間を詳細表示するためのアクセス許可を付与する	読み取り	rulegroupsnamespace*		
				aws:ResourceTag/${TagKey}	
DescribeScraper	スクレイパーを記述するためのアクセス許可を付与	読み取り	scraper*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeWorkspace	ワークスペースを記述する権限を付与します	読み取り	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeWorkspaceConfiguration	ワークスペース設定を記述するアクセス許可を付与します	読み取り	workspace*		
				aws:ResourceTag/${TagKey}	
GetAlertManagerSilence	サイレンス (silence) を取得するためのアクセス許可を付与する	読み込み	workspace*		
				aws:ResourceTag/${TagKey}	
GetAlertManagerStatus	アラートマネージャの現在のステータスを取得するためのアクセス許可を付与する	読み取り	workspace*		
				aws:ResourceTag/${TagKey}	
GetDefaultScraperConfiguration	デフォルトのスクレイパー設定を取得するためのアクセス許可を付与	読み取り			
GetLabels	AMP ワークスペースラベルを取得する権限を付与します	読み込み	workspace*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
GetMetricMetadata	AMP ワークスペースメトリクスのメタデータを取得する権限を付与します	読み込み	workspace*		
				aws:ResourceTag/${TagKey}	
GetSeries	AMP ワークスペースの時系列データを取得する権限を付与します	読み込み	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerAlertGroups	グループを一覧表示するためのアクセス許可を付与する	読み込み	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerAlerts	アラートを一覧表示するためのアクセス許可を付与する	読み込み	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerReceivers	レシーバ を一覧表示するためのアクセス許可を付与する	読み込み	workspace*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
ListAlertManagerSilences	サイレンス (silence) を一覧表示するためのアクセス許可を付与する	読み込み	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlerts	アクティブなアラートを一覧表示するためのアクセス許可を付与する	読み込み	workspace*		
				aws:ResourceTag/${TagKey}	
ListRuleGroupsNamespaces	ルールグループ名前空間を一覧表示するためのアクセス許可を付与する	リスト	workspace*		
				aws:ResourceTag/${TagKey}	
ListRules	アラートとレコーディングのルールを一覧表示するためのアクセス許可を付与する	読み取り	workspace*		
				aws:ResourceTag/${TagKey}	
ListScrapers	スクレイパーを一覧表示するためのアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTagsForResource	AMP リソースのタグを一覧表示する許可を付与	読み込み	rulegroupsnamespace		
			scraper		
			workspace		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListWorkspaces	ワークスペースを一覧表示する権限を付与します	リスト			
PutAlertManagerDefinition	アラートマネージャ定義を更新するためのアクセス許可を付与する	書き込み	workspace*		
				aws:ResourceTag/${TagKey}	
PutAlertManagerSilences	サイレンス (silence) を作成または更新するためのアクセス許可を付与する	書き込み	workspace*		
				aws:ResourceTag/${TagKey}	
PutResourcePolicy	ワークスペースリソースポリシーを作成および更新するアクセス許可を付与します	書き込み	workspace*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
PutRuleGroupsNamespace	ルールグループ名前空間を更新するためのアクセス許可を付与する	書き込み	rulegroupsnamespace*		
				aws:ResourceTag/${TagKey}	
QueryMetrics	AMP ワークスペースメトリクスについてクエリを実行する権限を付与します	読み込み	workspace*		
				aws:ResourceTag/${TagKey}	
RemoteWrite	AMP ワークスペースへのメトリクスのストリーミングを開始するリモート書き込みを実行する権限を付与します	書き込み	workspace*		
				aws:ResourceTag/${TagKey}	
TagResource	AMP リソースにタグ付けする許可を付与	Tagging	rulegroupsnamespace		
			scraper		
			workspace		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	AMP リソースのタグ付けを解除する許可を付与	Tagging	rulegroupsnamespace		
			scraper		
			workspace		
				aws:TagKeys	
UpdateLoggingConfiguration	ログ記録設定を更新する許可を付与	書き込み	workspace*		
				aws:ResourceTag/${TagKey}	
UpdateQueryLoggingConfiguration	クエリログ記録設定を更新するアクセス許可を付与します	書き込み	workspace*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateScraper	スクレイパーを更新する許可を付与	書き込み	scraper*		aps:CreateScraper aps:TagResource
			workspace		
				aws:ResourceTag/${TagKey}	
UpdateWorkspaceAlias	既存の AMP ワークスペースのエイリアスを変更する権限を付与します	書き込み	workspace*		
				aws:ResourceTag/${TagKey}	
UpdateWorkspaceConfiguration	ワークスペース設定を更新するアクセス許可を付与します	書き込み	workspace*		
				aws:ResourceTag/${TagKey}	

Amazon Managed Service for Prometheus で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
workspace	arn:${Partition}:aps:${Region}:${Account}:workspace/${WorkspaceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
rulegroupsnamespace	arn:${Partition}:aps:${Region}:${Account}:rulegroupsnamespace/${WorkspaceId}/${Namespace}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
scraper	arn:${Partition}:aps:${Region}:${Account}:scraper/${ScraperId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
cluster	arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}	aws:ResourceTag/${TagKey}

Amazon Managed Service for Prometheus の条件キー

Amazon Managed Service for Prometheus は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられているタグに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーに基づいてアクションをフィルタリングします	ArrayOfString

Amazon Managed Streaming for Apache Kafka のアクション、リソース、および条件キー

Amazon Managed Streaming for Apache Kafka (サービスプレフィックス: kafka) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Managed Streaming for Apache Kafka で定義されるアクション
- Amazon Managed Streaming for Apache Kafka で定義されるリソースタイプ
- Amazon Managed Streaming for Apache Kafka の条件キー

Amazon Managed Streaming for Apache Kafka で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchAssociateScramSecret	Amazon MSK クラスターに 1 つ以上の Scram シークレットを関連付ける権限を付与します	書き込み	cluster*		kms:CreateGrant kms:RetireGrant
BatchDisassociateScramSecret	Amazon MSK クラスターから 1 つ以上の Scram シークレットの関連付けを解除する権限を付与します	書き込み	cluster*		kms:RetireGrant
CreateCluster	MSK クラスターを作成する権限を付与します	書き込み	cluster*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy kms:CreateGrant

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateClusterV2	MSK クラスターを作成する権限を付与します	書き込み	cluster*		ec2:CreateTags ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs iam:AttachRolePolicy

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					iam:CreateServiceLinkedRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguration	MSK 設定を作成する権限を付与します	書き込み	configuration*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateReplicator	MSK レプリケーターを作成するアクセス許可を付与します	書き込み	replicator*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PassRole iam:PutRolePolicy kafka:DescribeClusterV2 kafka:GetBootstrapBrokers

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateVpcConnection	MSK VPC 接続を作成するアクセス許可を付与	書き込み	cluster*		ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					iam:PutRolePolicy
			vpc-connection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCluster	MSK クラスターを削除する権限を付与します	書き込み	cluster*		ec2:DeleteVpcEndpoints ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints
DeleteClusterPolicy	クラスターのリソースベースポリシーを削除する許可を付与	書き込み	cluster*		
DeleteConfiguration	指定された MSK 設定を削除する権限を付与します	書き込み	configuration*		
DeleteReplicator	MSK レプリケーターを削除するアクセス許可を付与します	書き込み	replicator*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteVpcConnection	MSK VPC 接続を削除するアクセス許可を付与	書き込み	vpc-connection*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints
DescribeCluster	MSK クラスターを記述する権限を付与します	読み込み	cluster*		
DescribeClusterOperation	所与の ARN で指定されたクラスターオペレーションを記述する権限を付与します	読み取り			
DescribeClusterOperationV2	所与の ARN で指定されたクラスターオペレーションを記述する権限を付与します	読み込み			
DescribeClusterV2	MSK クラスターを記述する権限を付与します	読み込み	cluster*		
DescribeConfiguration	MSK 設定を記述する権限を付与します	読み込み	configuration*		
DescribeConfigurationRevision	MSK 設定リビジョンを記述する権限を付与します	読み取り	configuration*		
DescribeReplicator	MSK レプリケーターを記述するアクセス許可を付与します	読み取り	replicator*		
DescribeVpcConnection	MSK VPC 接続を記述する権限を付与	読み取り	vpc-connection*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetBootstrapBrokers	MSK クラスター内にあるブローカーノードについて接続の詳細を取得する権限を付与します	読み取り			
GetClusterPolicy	クラスターのリソースベースポリシーを記述する許可を付与	読み取り	cluster*		
GetCompatibleKafkaVersions	MSK クラスターを更新できる Apache Kafka バージョンのリストを取得する権限を付与します	リスト			
ListClientVpcConnections	クラスター用に作成されたすべての MSK VPC 接続を一覧表示する許可を付与	リスト	cluster*		
ListClusterOperations	指定された MSK クラスターで実行されたすべてのオペレーション一覧を返すアクセス許可を付与する	リスト	cluster*		
ListClusterOperationsV2	指定された MSK クラスターで実行されたすべてのオペレーション一覧を返すアクセス許可を付与する	リスト	cluster*		
ListClusters	このアカウント内のすべての MSK クラスターを一覧表示する権限を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListClustersV2	このアカウント内のすべてのMSK クラスターを一覧表示する権限を付与します	リスト			
ListConfigurationRevisions	このアカウント内の MSK 設定のすべてのリビジョンを一覧表示する権限を付与します	リスト	configuration*		
ListConfigurations	このアカウント内のすべてのMSK 設定を一覧表示する権限を付与します	リスト			
ListKafkaVersions	Amazon MSK でサポートされているすべての Apache Kafka バージョンを一覧表示する権限を付与します	リスト			
ListNodes	MSK クラスター内のブローカーを一覧表示する権限を付与します	リスト	cluster*		
ListReplicators	このアカウント内のすべてのMSK レプリケーションを一覧表示するアクセス許可を付与します	リスト			
ListScramSecrets	Amazon MSK クラスターに関連付けられた Scram シークレットを一覧表示する権限を付与します。	リスト	cluster*		
ListTagsForResource	MSK リソースのタグを一覧表示する権限を付与します	読み取り	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListVpcConnections	このアカウント内が使用するすべての MSK VPC 接続を一覧表示する許可を付与	リスト			
PutClusterPolicy	クラスター用のリソースベースポリシーを作成または更新する許可を付与	書き込み	cluster*		
RebootBroker	ブローカーを再起動する権限を付与します	書き込み	cluster*		
RejectClientVpcConnection	MSK VPC 接続を拒否する許可を付与	書き込み	cluster*		
			vpc-connection*		
TagResource	MSK リソースにタグを付ける権限を付与します	タグ付け	cluster		
			vpc-connection		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	MSK リソースからタグを削除する権限を付与します	タグ付け	cluster		
			vpc-connection		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
UpdateBrokerCount	MSK クラスターのブローカー数を更新する許可を付与	書き込み	cluster*		
UpdateBrokerStorage	MSK クラスターのブローカーのストレージサイズを更新する許可を付与	書き込み	cluster*		
UpdateBrokerType	Amazon MSK クラスターのブローカータイプを更新する許可を付与	書き込み	cluster*		
UpdateClusterConfiguration	MSK クラスターの設定を更新する権限を付与します	書き込み	cluster*		
			configuration*		
UpdateClusterKafkaVersion	MSK クラスター更新してを指定された Apache Kafka バージョンにする権限を付与します	書き込み	cluster*		
UpdateConfiguration	MSK 設定の新しいリビジョンを作成する権限を付与します。	書き込み	configuration*		
UpdateConnectivity	MSK クラスターのセキュリティ設定を更新する許可を付与	書き込み	cluster*		ec2:DescribeRouteTables ec2:DescribeSubnets

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				kafka:publicAccessEnabled	
UpdateMonitoring	MSK クラスターのモニタリング設定を更新する権限を付与します	書き込み	cluster*		
UpdateReplicationInfo	MSK レプリケーターのレプリケーション情報を更新するアクセス許可を付与します	書き込み	replicator*		
UpdateSecurity	MSK クラスターのセキュリティ設定を更新する許可を付与	書き込み	cluster*		kms:RetireGrant
UpdateStorage	MSK ブローカーに関連する EBS ストレージ (サイズまたはプロビジョニングされたスループット) を更新したり、クラスターストレージモードを TIERED に設定したりする許可を付与	書き込み	cluster*		

Amazon Managed Streaming for Apache Kafka で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
cluster	arn:${Partition}:kafka:${Region}:${Account}:cluster/${ClusterName}/${Uuid}	aws:ResourceTag/${TagKey}
configuration	arn:${Partition}:kafka:${Region}:${Account}:configuration/${ConfigurationName}/${Uuid}	
vpc-connection	arn:${Partition}:kafka:${Region}:${VpcOwnerAccount}:vpc-connection/${ClusterOwnerAccount}/${ClusterName}/${Uuid}	aws:ResourceTag/${TagKey}
replicator	arn:${Partition}:kafka:${Region}:${Account}:replicator/${ReplicatorName}/${Uuid}	aws:ResourceTag/${TagKey}
topic	arn:${Partition}:kafka:${Region}:${Account}:topic/${ClusterName}/${ClusterUuid}/${TopicName}	
group	arn:${Partition}:kafka:${Region}:${Account}:group/${ClusterName}/${ClusterUuid}/${GroupName}	
transactional-id	arn:${Partition}:kafka:${Region}:${Account}:transactional-id/${ClusterName}/${ClusterUuid}/${TransactionalId}	

Amazon Managed Streaming for Apache Kafka の条件キー

Amazon Managed Streaming for Apache Kafka では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条

件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString
kafka:publicAccessEnabled	リクエスト内に有効化された公開アクセスが存在するかで、アクセスでフィルタリング	Bool

Amazon Managed Streaming for Kafka Connect のアクション、リソース、および条件キー

Amazon Managed Streaming for Kafka Connect (サービスプレフィックス: kafkaconnect) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Managed Streaming for Kafka Connect で定義されるアクション
- Amazon Managed Streaming for Kafka Connect で定義されるリソースタイプ
- Amazon Managed Streaming for Kafka Connect の条件キー

Amazon Managed Streaming for Kafka Connect で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateConnector	MSK Connect コネクタを作成する許可を付与	書き込み			ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs firehose:TagDeliveryStream iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					iam:PutRolePolicy logs:CreateLogDelivery logs:DescribeLogGroups logs:DescribeResourcePolicies logs:GetLogDelivery logs:ListLogDeliveries logs:PutResourcePolicy s3:GetBucketPolicy s3:PutBucketPolicy

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateCustomPlugin	MSK Connect カスタムプラグインを作成する許可を付与	書き込み			s3:GetObject
CreateWorkerConfiguration	MSK Connect ワーカー設定を作成する許可を付与	書き込み			
DeleteConnector	MSK Connect コネクタを削除する許可を付与	書き込み	connector*		logs:DeleteLogDelivery logs:ListLogDeliveries
DeleteCustomPlugin	MSK Connect カスタムプラグインを削除する許可を付与	書き込み	customplugin*		
DeleteWorkerConfiguration	MSK Connect ワーカー設定を削除する許可を付与する	書き込み	workerconfiguration*		
DescribeConnector	MSK Connect コネクタを記述する許可を付与	読み取り	connector*		
DescribeConnectorOperation	MSK Connect コネクタオペレーションを記述するアクセス許可を付与します	読み取り	connectoroperation*		
DescribeCustomPlugin	MSK Connect カスタムプラグインを記述する許可を付与	読み取り	customplugin*		
DescribeWorkerConfiguration	MSK Connect ワーカー設定を記述する許可を付与	読み取り	workerconfiguration*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListConnectorOperations	特定の MSK Connect コネクタのすべてのオペレーションを一覧表示するアクセス許可を付与します	読み取り	connector *		
ListConnectors	このアカウント内のすべての MSK Connect コネクタを一覧表示する許可を付与	読み取り			
ListCustomPlugins	このアカウント内のすべての MSK Connect カスタムプラグインを一覧表示する許可を付与	読み取り			
ListTagsForResource	MSK Connect リソースのタグを一覧表示する許可を付与する	読み取り	connector	aws:ResourceTag/${TagKey}	
			custom plugin	aws:ResourceTag/${TagKey}	
			worker configuration	aws:ResourceTag/${TagKey}	
ListWorkerConfigurations	このアカウント内のすべての MSK Connect ワーカー設定を一覧表示する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
TagResource	MSK Connect リソースにタグ付けする許可を付与する	Tagging	connector	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			custom plugin	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			worker configuration	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	MSK Connect リソースからタグを削除する許可を付与する	Tagging	connector	aws:TagKeys	
			custom plugin	aws:TagKeys	
			worker configuration	aws:TagKeys	
				aws:TagKeys	
UpdateConnector	MSK Connect コネクタを更新する許可を付与	書き込み	connector *		

Amazon Managed Streaming for Kafka Connect で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
connector	arn:${Partition}:kafkaconnect:${Region}:${Account}:connector/${ConnectorName}/${UUID}	aws:ResourceTag/${TagKey}
custom plugin	arn:${Partition}:kafkaconnect:${Region}:${Account}:custom-plugin/${CustomPluginName}/${UUID}	aws:ResourceTag/${TagKey}
worker configuration	arn:${Partition}:kafkaconnect:${Region}:${Account}:worker-configuration/${WorkerConfigurationName}/${UUID}	aws:ResourceTag/${TagKey}
connector operation	arn:${Partition}:kafkaconnect:${Region}:${Account}:connector-operation/${ConnectorName}/${ConnectorUUID}/${UUID}	aws:ResourceTag/${TagKey}

Amazon Managed Streaming for Kafka Connect の条件キー

Amazon Managed Streaming for Kafka Connect では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

Amazon Managed Workflows for Apache Airflow のアクション、リソース、および条件キー

Amazon Managed Workflows for Apache Airflow (サービスプレフィックス: `airflow`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Managed Workflows for Apache Airflow で定義されるアクション
- Amazon Managed Workflows for Apache Airflow で定義されるリソースタイプ
- Amazon Managed Workflows for Apache Airflow の条件キー

Amazon Managed Workflows for Apache Airflow で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーショ

ンへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateCliToken	ユーザーが Apache Airflow Webserver のエンドポイント経由で Airflow CLI を呼び出せるように短命トークンを作成する権限を付与します	Write	environment*		
CreateEnvironment	Amazon MWAA 環境を作成する権限を付与します	Write	environment*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebLoginToken	ユーザーが Apache Airflow ウェブ UI にログインできるように短命トークンを作成する権限を付与します。	Write	rbac-role*		
DeleteEnvironment	Amazon MWAA 環境を削除する権限を付与します	Write	environment*		
				aws:ResourceTag/${TagKey}	
GetEnvironment	Amazon MWAA 環境の詳細を表示する権限を付与します	読み取り	environment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
InvokeRestApi	Apache Airflow Webserver のエンドポイントを介して Airflow REST API を呼び出す許可を付与する	書き込み	rbac-role*		
ListEnvironments	アカウント内の Amazon MWAA 環境を一覧表示する権限を付与します	リスト			
ListTagsForResource	Amazon MWAA 環境のタグを一覧表示する権限を付与します	Read	environment		
				aws:ResourceTag/${TagKey}	
PublishMetrics	Amazon MWAA 環境のメトリクスを公開する許可を付与します	Write	environment*		
TagResource	Amazon MWAA 環境にタグを付ける権限を付与します	タグ付け	environment		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Amazon MWAA 環境のタグを解除する権限を付与します	タグ付け	environment		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateEnvironment	Amazon MWAA 環境を変更する権限を付与します	Write	environment*		
				aws:ResourceTag/${TagKey}	

Amazon Managed Workflows for Apache Airflow で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
environment	`arn:${Partition}:airflow:${Region}:${Account}:environment/${EnvironmentName}`	
rbac-role	`arn:${Partition}:airflow:${Region}:${Account}:role/${EnvironmentName}/${RoleName}`	

Amazon Managed Workflows for Apache Airflow の条件キー

Amazon Managed Workflows for Apache Airflow では、IAM ポリシーの `Condition` 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Marketplaceのアクション、リソース、および条件キー

AWS Marketplace（ サービスプレフィックス: aws-marketplace) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Marketplaceで定義されるアクション
- AWS Marketplaceで定義されるリソースタイプ
- AWS Marketplaceの条件キー

AWS Marketplaceで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptAgreementApprovalRequest	受信した (サブスクリプションの検証が必要な製品を提供するプロバイダー向けの) サブスクリプションリクエストを承認するための、アクセス許可をユーザーに付与する	書き込み			
AcceptAgreementRequest	契約リクエストを受け入れる許可をユーザーに付与します。このアクションは Marketplace の購入には適用されないことに注意してください	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CancelAgreement	契約をキャンセルする許可をユーザーに付与します。このアクションは Marketplace の購入には適用されないことに注意してください	書き込み			
CancelAgreementRequest	サブスクリプションの検証が必要な製品において、保留中のサブスクリプションリクエストをキャンセルするためのアクセス許可をユーザーに付与する	書き込み			
CreateAgreementRequest	契約リクエストを作成する許可をユーザーに付与します。このアクションは Marketplace の購入には適用されないことに注意してください	書き込み			
DescribeAgreement	契約に関するメタデータを詳細表示するためのアクセス許可をユーザーに付与する	読み取り			
GetAgreementApprovalRequest	受信した (サブスクリプションの検証が必要な製品を提供するプロバイダー向け) サブスクリプションリクエストの詳細を表示するための、アクセス許可をユーザーに付与する	読み取り			
GetAgreementEntitlements	契約に関連付けられた使用権限を表示するアクセス許可をユーザーに付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetAgreementRequest	サブスクリプションの検証が必要なデータ製品において、サブスクリプションリクエストの詳細を表示するためのアクセス許可をユーザーに付与する	読み取り			
GetAgreementTerms	契約条件のリストを取得するためのアクセス許可をユーザーに付与する	リスト			
ListAgreementApprovalRequests	受信した (サブスクリプションの検証が必要な製品を提供するプロバイダー向けの) サブスクリプションリクエストを、リストするためのアクセス許可をユーザーに付与する	リスト			
ListAgreementCharges	契約に関連する料金を表示するアクセス許可をユーザーに付与します	リスト			
ListAgreementRequests	サブスクリプションの検証が必要な製品において、サブスクリプションリクエストをリストするためのアクセス許可をユーザーに付与する	リスト			
ListEntitlementDetails	契約に関連する資格の詳細を表示するアクセス許可をユーザーに付与します。このアクションは Marketplace の購入には適用されないことに注意してください	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RejectAgreementApprovalRequest	受信した (サブスクリプションの検証が必要な製品を提供するプロバイダー向けの) サブスクリプションリクエストを、拒否するためのアクセス許可をユーザーに付与する	書き込み			
SearchAgreements	契約を検索するためのアクセス許可をユーザーに付与する	リスト			
Subscribe	AWS Marketplace 製品をサブスクライブするアクセス許可をユーザーに付与します。サブスクリプションの検証が必要な製品のサブスクリプションリクエストを送信する機能が含まれています。既存のサブスクリプションの自動更新を有効にする機能が含まれています。	書き込み			
Unsubscribe	AWS Marketplace 製品のサブスクリプションを削除するアクセス許可をユーザーに付与します。既存のサブスクリプションの自動更新を無効にする機能が含まれています。	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateAgreementApprovalRequest	受信したサブスクリプションリクエストにおいて、将来のサブスクライバーの情報を削除する (サブスクリプションの検証が必要な製品を提供するプロバイダー向け) 機能などに対して変更を加えるための、アクセス許可をユーザーに付与する	書き込み			
UpdatePurchaseOrders	契約に関連する料金の発注書を更新するアクセス許可をユーザーに付与します	書き込み			
ViewSubscriptions	アカウントのサブスクリプションを表示するためのアクセス許可をユーザーに付与する	リスト			

AWS Marketplaceで定義されるリソースタイプ

AWS Marketplace では、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定はサポートされていません。 AWS Marketplaceへのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Marketplaceの条件キー

AWS Marketplace は、IAM ポリシーの `Condition`要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws-marketplace:AgreementType	契約のタイプによりアクセスをフィルタリング	ArrayOfString
aws-marketplace:PartyType	契約の当事者タイプによりアクセスをフィルタリング	String
aws-marketplace:ProductId	AWS Marketplace RedHat OpenShift および Bedrock 製品の製品 ID でアクセスをフィルタリングします。注: この条件キーを使用しても、 の製品へのアクセスは制限されません。 AWS Marketplace	ArrayOfString

AWS Marketplace Catalog のアクション、リソース、および条件キー

AWS Marketplace Catalog (サービスプレフィックス: `aws-marketplace`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Marketplace Catalog で定義されるアクション
- AWS Marketplace Catalog で定義されるリソースタイプ
- AWS Marketplace Catalog の条件キー

AWS Marketplace Catalog で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelChangeSet	実行中の変更セットをキャンセルする許可を付与	書き込み	ChangeSet*		
DeleteResourcePolicy	既存のエンティティのリソースポリシーを削除する許可を付与	権限の管理	Entity*		
DescribeAssessment	既存の評価の詳細を返す許可を付与する	読み取り			
DescribeChangeSet	既存の変更セットの詳細を返す許可を付与	読み取り	ChangeSet*		
DescribeEntity	既存のエンティティの詳細を返す許可を付与	読み取り	Entity*		
GetResourcePolicy	既存のエンティティのリソースポリシーを取得する許可を付与	読み取り	Entity*		
ListAssessments	既存の評価を一覧表示する許可を付与する	リスト			
ListChangeSets	既存の変更セットを一覧表示する許可を付与	リスト			
ListEntities	既存のエンティティを一覧表示する許可を付与	リスト			
ListTagsForResource	既存のエンティティまたは変更セットのタグを一覧表示する許可を付与	読み取り	ChangeSet		
			Entity		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutResourcePolicy	リソースポリシーを既存のエンティティにアタッチする許可を付与	権限の管理	Entity*		
StartChangeSet	新しい変更セットをリクエストするアクセス許可を付与します (注: このアクションのリソースレベルのアクセス許可とこのアクションの条件コンテキストキーは、Catalog API で使用する場合にのみサポートされ、 AWS Marketplace Management Portal で使用する場合はサポートされません)。	書き込み	Entity*		
				catalog:ChangeType aws-marketplace:Intent aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	既存のエンティティまたは変更セットをタグ付けする許可を付与	Tagging	ChangeSet		
			Entity		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	既存のエンティティまたは変更セットのタグを解除する許可を付与	Tagging	ChangeSet		
			Entity		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:TagKeys	

AWS Marketplace Catalog で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Entity	`arn:${Partition}:aws-marketplace:${Region}:${Account}:${Catalog}/${EntityType}/${ResourceId}`	aws:ResourceTag/${TagKey} catalog:ChangeType
ChangeSet	`arn:${Partition}:aws-marketplace:${Region}:${Account}:${Catalog}/ChangeSet/${ResourceId}`	aws:ResourceTag/${TagKey} catalog:ChangeType

AWS Marketplace Catalog の条件キー

AWS Marketplace Catalog では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws-marketplace:Intent	StartChangeSet リクエストの Intent パラメータによってアクセスをフィルタリングする	String
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
catalog:ChangeType	StartChangeSet リクエストの変更タイプでアクセスをフィルタリングします	String

AWS Marketplace Commerce Analytics Service のアクション、リソース、および条件キー

AWS Marketplace Commerce Analytics Service (サービスプレフィックス: `marketplacecommerceanalytics`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。

トピック

- AWS Marketplace Commerce Analytics Service で定義されるアクション
- AWS Marketplace Commerce Analytics Service で定義されるリソースタイプ
- AWS Marketplace Commerce Analytics Service の条件キー

AWS Marketplace Commerce Analytics Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GenerateDataSet	Amazon S3 バケットに発行されるデータセットをリクエストします。	Write			
StartSupportDataExport	Amazon S3 バケットに発行されるサポートデータセットをリクエストします。	Write			

AWS Marketplace Commerce Analytics Service で定義されるリソースタイプ

AWS Marketplace Commerce Analytics Service は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Marketplace Commerce Analytics Service へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Marketplace Commerce Analytics Service の条件キー

MCS には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Marketplace Deployment Service のアクション、リソース、および条件キー

AWS Marketplace Deployment Service (サービスプレフィックス: `aws-marketplace`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Marketplace Deployment Service で定義されるアクション
- AWS Marketplace Deployment Service で定義されるリソースタイプ
- AWS Marketplace Deployment Service の条件キー

AWS Marketplace Deployment Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTagsForResource	デプロイパラメータリソースのタグを一覧表示する許可を付与	読み取り	DeploymentParameter		
				aws:ResourceTag/${TagKey}	
PutDeploymentParameter	デプロイパラメータリソースを作成または更新する許可を付与	書き込み	DeploymentParameter*	aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	aws-marketplace:TagResource
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	デプロイパラメータリソースにタグ付けする許可を付与	Tagging	DeploymentParameter*	aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	デプロイパラメータリソースのタグを解除する許可を付与	Tagging	DeploymentParameter*	aws:ResourceTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:TagKeys	

AWS Marketplace Deployment Service で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
DeploymentParameter	`arn:${Partition}:aws-marketplace:${Region}:${Account}:DeploymentParameter:catalogs/${CatalogName}/products/${ProductId}/${ResourceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

AWS Marketplace Deployment Service の条件キー

AWS Marketplace Deployment Service では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストで渡されたタグによりアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグによりアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーによりアクセスをフィルタリングします	ArrayOfString

AWS Marketplace Discovery のアクション、リソース、および条件キー

AWS Marketplace Discovery (サービスプレフィックス: `aws-marketplace`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Marketplace Discovery によって定義されたアクション
- AWS Marketplace Discovery によって定義されたリソースタイプ
- AWS Marketplace Discovery の条件キー

AWS Marketplace Discovery によって定義されたアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListPrivateListings	プライベートオファーを一覧表示するための許可をユーザーに付与します	リスト			

AWS Marketplace Discovery によって定義されたリソースタイプ

AWS Marketplace Discovery は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Marketplace Discovery へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Marketplace Discovery の条件キー

Marketplace Discovery には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Marketplace Entitlement Service のアクション、リソース、および条件キー

AWS Marketplace Entitlement Service (サービスプレフィックス: `aws-marketplace`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Marketplace Entitlement Service で定義されるアクション

- AWS Marketplace Entitlement Service で定義されるリソースタイプ
- AWS Marketplace Entitlement Service の条件キー

AWS Marketplace Entitlement Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetEntitlements	特定の製品の使用権限管理の値を取得する許可を付与します。結果は、顧客 ID または製品ディメンションに基づいてフィルタリングできます。	Read			

AWS Marketplace Entitlement Service で定義されるリソースタイプ

AWS Marketplace Entitlement Service は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Marketplace Entitlement Service へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Marketplace Entitlement Service の条件キー

Marketplace Entitlement には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Marketplace Image Building Service のアクション、リソース、および条件キー

AWS Marketplace Image Building Service (サービスプレフィックス: `aws-marketplace`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Marketplace Image Building Service で定義されるアクション
- AWS Marketplace Image Building Service で定義されるリソースタイプ
- AWS Marketplace Image Building Service の条件キー

AWS Marketplace Image Building Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeBuilds [アクセス許可のみ]	ビルド ID によって識別されるイメージビルドについて説明します。	Read			
ListBuilds [許可のみ]	イメージビルドを一覧表示します。	Read			
StartBuild [許可のみ]	イメージビルドを開始します。	Write			

AWS Marketplace Image Building Service で定義されるリソースタイプ

AWS Marketplace Image Building Service は、IAM ポリシーステートメントの Resource要素でのリソース ARN の指定をサポートしていません。 AWS Marketplace Image Building Service へのアクセスを許可するには、ポリシーで "Resource": "*" を指定します。

AWS Marketplace Image Building Service の条件キー

Marketplace Image Build には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Marketplace Management Portal のアクション、リソース、および条件キー

AWS Marketplace Management Portal (サービスプレフィックス: aws-marketplace-management) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Marketplace Management Portal で定義されるアクション
- AWS Marketplace Management Portal で定義されるリソースタイプ
- AWS Marketplace Management Portal の条件キー

AWS Marketplace Management Portal で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にア

クションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetAdditionalSellerNotificationRecip	追加の販売者通知の受信者を表示する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ients [アクセス許可のみ]					
GetBankAccountVerificationDetails [許可のみ]	銀行口座の検証ステータスを表示する許可を付与	読み取り			
GetSecondaryUserVerificationDetails [許可のみ]	セカンダリユーザーアカウントの検証ステータスを表示する許可を付与	読み取り			
GetSellerVerificationDetails [許可のみ]	アカウント検証ステータスを表示する許可を付与	読み取り			
PutAdditionalSellerNotificationRecipients [許可のみ]	追加の販売者通知の受信者を更新する許可を付与	書き込み			
PutBankAccountVerificationDetails [アクセス許可のみ]	銀行口座の検証ステータスを更新する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutSecondaryUserVerificationDetails [アクセス許可のみ]	セカンダリユーザーアカウントの検証ステータスを更新する許可を付与	書き込み			
PutSellerVerificationDetails [アクセス許可のみ]	口座の検証ステータスを更新する許可を付与	書き込み			
uploadFiles [アクセス許可のみ]	AWS Marketplace 管理ポータル内のファイルアップロードページへのアクセスを許可します。	書き込み			
viewMarketing [アクセス許可のみ]	AWS Marketplace 管理ポータル内のマーケティングページへのアクセスを許可します。	リスト			
viewReports [許可のみ]	AWS Marketplace 管理ポータル内のレポートページへのアクセスを許可します。	リスト			
viewSettings [許可のみ]	AWS Marketplace 管理ポータル内の設定ページへのアクセスを許可します。	リスト			
viewSupport [許可のみ]	AWS Marketplace 管理ポータル内のカスタマーサポート適格性ページへのアクセスを許可します	リスト			

AWS Marketplace Management Portal で定義されるリソースタイプ

AWS Marketplace Management Portal は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Marketplace Management Portal へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Marketplace Management Portal の条件キー

Marketplace Portal には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Marketplace Metering Service のアクション、リソース、および条件キー

AWS Marketplace Metering Service (サービスプレフィックス: `aws-marketplace`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Marketplace Metering Service で定義されるアクション
- AWS Marketplace Metering Service で定義されるリソースタイプ
- AWS Marketplace Metering Service の条件キー

AWS Marketplace Metering Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchMeterUsage	SaaS アプリケーションの顧客のセットのメータリングレコードを投稿する許可を付与	Write			
MeterUsage	メータリングレコードを投稿する許可を付与	書き込み			
RegisterUsage	有料ソフトウェアを実行している顧客が製品をサブスクライブしていることを検証するためのアクセス許可を付与し AWS Marketplace、不正使用から保護できるようにします。1 時間あたりの ECS タスクごとのソフトウェア使用量を、1 秒単位に按分した使用量で計測します	Write			
ResolveCustomer	登録トークンを解決して CustomerIdentifier と製品コードを取得する許可を付与	Write			

AWS Marketplace Metering Service で定義されるリソースタイプ

AWS Marketplace Metering Service は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Marketplace Metering Service へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Marketplace Metering Service の条件キー

Marketplace Metering には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Marketplace Private Marketplace のアクション、リソース、および条件キー

AWS Marketplace Private Marketplace (サービスプレフィックス: aws-marketplace) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Marketplace Private Marketplace で定義されるアクション
- AWS Marketplace Private Marketplace で定義されるリソースタイプ
- AWS Marketplace Private Marketplace の条件キー

AWS Marketplace Private Marketplace で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateProductsWithPrivateMarketplace [アクセス許可のみ]	Private Marketplace に関連付ける製品のリクエストを承認する許可を付与 このアクションは、ユーザーがアクセス許可を持ち、 AWS 組織のサービスコントロールポリシーで許可されている場合、組織内の任意のアカウントで実行できます。	書き込み			
CreatePrivateMarke	Private Marketplace に関連付ける製品のリクエストを作	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
tplaceRequests [アクセス許可のみ]	成する許可を付与。このアクションは、ユーザーがアクセス許可を持ち、組織のサービスコントロールポリシーで許可されている場合、 AWS 組織内の の任意のアカウントで実行できます。				
DescribePrivateMarketplaceRequests [アクセス許可のみ]	Private Marketplace でのリクエストと関連商品について記述する許可を付与。このアクションは、ユーザーがアクセス許可を持ち、 AWS 組織のサービスコントロールポリシーで許可されている場合、組織内の任意のアカウントで実行できます。	リスト			
DisassociateProductsFromPrivateMarketplace [許可のみ]	Private Marketplace に関連付ける製品のリクエストを辞退する許可を付与 このアクションは、ユーザーがアクセス許可を持ち、 AWS 組織のサービスコントロールポリシーで許可されている場合、組織内の任意のアカウントで実行できます。	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListPrivateMarketplaceRequests [アクセス許可のみ]	Private Marketplace でのリクエストと関連商品のクエリ可能なリストを取得する許可を付与 このアクションは、ユーザーがアクセス許可を持ち、AWS 組織のサービスコントロールポリシーで許可されている場合、組織内の任意のアカウントで実行できます。	リスト			

AWS Marketplace Private Marketplace で定義されるリソースタイプ

AWS Marketplace Private Marketplace は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Marketplace Private Marketplace へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Marketplace Private Marketplace の条件キー

Private Marketplace には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Marketplace Procurement Systems Integration のアクション、リソース、および条件キー

AWS Marketplace 調達システム統合 (サービスプレフィックス: `aws-marketplace`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Marketplace Procurement Systems Integration で定義されるアクション
- AWS Marketplace Procurement Systems Integration で定義されるリソースタイプ
- AWS Marketplace Procurement Systems Integration の条件キー

AWS Marketplace Procurement Systems Integration で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeProcurementSystemConfiguration [アクセス許可のみ]	個々のアカウント、または存在する場合は AWS 組織全体の調達システム統合設定 (Coupa など) を記述するアクセス許可を付与します。このアクションは、 AWS Organization を使用している場合にのみ、マスターアカウントによって実行できます。	読み取り			
PutProcurementSystemConfiguration [許可のみ]	個々のアカウント、または AWS 組織全体の調達システム統合設定 (Coupa など) を作成または更新するアクセス許可を付与します。このアクションは、 AWS Organization を使用している場合にのみ、マスターアカウントによって実行できます。	書き込み			

AWS Marketplace Procurement Systems Integration で定義されるリソースタイプ

AWS Marketplace 調達システム統合では、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定はサポートされていません。 AWS Marketplace Procurement Systems Integration へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Marketplace Procurement Systems Integration の条件キー

Marketplace Procurement Integration には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Marketplace Reporting のアクション、リソース、および条件キー

AWS Marketplace レポート (サービスプレフィックス: `aws-marketplace`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Marketplace Reporting で定義されるアクション
- AWS Marketplace Reporting で定義されるリソースタイプ
- AWS Marketplace Reporting の条件キー

AWS Marketplace Reporting で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetBuyerDashboard	購入者 AWS Marketplace の購入データを表示するダッシュ	読み取り	Dashboard *		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	ボードを表示するアクセス許可を付与します				

AWS Marketplace Reporting で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Dashboard	`arn:${Partition}:aws-marketplace::${Account}:${Catalog}/ReportingData/${FactTable}/Dashboard/${DashboardName}`	

AWS Marketplace Reporting の条件キー

Marketplace Reporting には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Marketplace Seller Reporting のアクション、リソース、および条件キー

AWS Marketplace Seller Reporting (サービスプレフィックス: `aws-marketplace`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Marketplace Seller Reporting で定義されるアクション
- AWS Marketplace Seller Reporting で定義されるリソースタイプ
- AWS Marketplace Seller Reporting の条件キー

AWS Marketplace Seller Reporting で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetSellerDashboard	販売者ダッシュボードを表示する許可を付与	読み取り	SellerDashboard*		

AWS Marketplace Seller Reporting で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
SellerDashboard	`arn:${Partition}:aws-marketplace::${Account}:${Catalog}/ReportingData/${FactTable}/Dashboard/${DashboardName}`	

AWS Marketplace Seller Reporting の条件キー

Marketplace Seller Reporting には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Marketplace Vendor Insights のアクション、リソース、および条件キー

AWS Marketplace Vendor Insights (サービスプレフィックス: vendor-insights) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Marketplace Vendor Insights によって定義されたアクション
- AWS Marketplace Vendor Insights によって定義されたリソースの種類
- AWS Marketplace Vendor Insights の条件キー

AWS Marketplace Vendor Insights によって定義されたアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にア

クションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ActivateSecurityProfile	セキュリティプロファイルをアクティブ化する許可を付与	書き込み	SecurityProfile*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
AssociateDataSource	セキュリティプロファイルをデータソースに関連付ける許可を付与	書き込み	SecurityProfile*		vendor-insights:GetDataSource
				aws:ResourceTag/${TagKey}	
CreateDataSource	新しいデータソースを作成する許可を付与	書き込み		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	vendor-insights:TagResource
CreateSecurityProfile	新しいセキュリティプロファイルを作成する許可を付与	書き込み		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	vendor-insights:TagResource

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeactivateSecurityProfile	セキュリティプロファイルを非アクティブ化する許可を付与	書き込み	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
DeleteDataSource	データソースを削除するアクセス許可を付与	書き込み	DataSource*		
				aws:ResourceTag/${TagKey}	
DisassociateDataSource	データソースからセキュリティプロファイルの関連付けを解除する許可を付与	書き込み	SecurityProfile*		vendor-insights:GetDataSource
				aws:ResourceTag/${TagKey}	
GetDataSource	既存のデータソースの詳細を取得する許可を付与	読み取り	DataSource*		
				aws:ResourceTag/${TagKey}	
GetEntitledSecurityProfileSnapshot	リクエスタに読み取り権限が付与されている、セキュリティプロファイルスナップショットの詳細を返す許可を付与	読み取り	SecurityProfile*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetProfileAccessTerms	ベンダーインサイトプロファイルのアクセス条件を取得する許可を付与	読み取り			
GetSecurityProfile	既存のセキュリティプロファイルの詳細を返す許可を付与	読み取り	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
GetSecurityProfileSnapshot	セキュリティプロファイルスナップショットの詳細を返す許可を付与	読み取り	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
ListDataSources	既存のデータソースを一覧表示する許可を付与	リスト			
ListEntitledSecurityProfileSnapshots	リクエスタに一覧表示する権限が付与されている、既存のセキュリティプロファイルのスナップショットの概要のリストを返す許可を付与	リスト	SecurityProfile*		
ListEntitledSecurityProfiles	権限が付与されているセキュリティプロファイルを一覧表示する許可を付与	リスト			
ListSecurityProfileSnapshots	既存のセキュリティプロファイルのスナップショットの概要のリストを返す許可を付与	リスト	SecurityProfile*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
ListSecurityProfiles	既存のセキュリティプロファイルを一覧表示する許可を付与	リスト			
ListTagsForResource	ベンダーインサイトリソースのタグを一覧表示する許可を付与	読み取り	DataSource		
			SecurityProfile		
				aws:ResourceTag/${TagKey}	
TagResource	ベンダーインサイトリソースをタグ付けする許可を付与	Tagging	DataSource		
			SecurityProfile		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	ベンダーインサイトリソースのタグを解除する許可を付与	Tagging	DataSource		
			SecurityProfile		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateDataSource	既存のデータソースを更新する許可を付与	書き込み	DataSource*		
				aws:ResourceTag/${TagKey}	
UpdateSecurityProfile	セキュリティプロファイルを更新する許可を付与	書き込み	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
UpdateSecurityProfileSnapshotCreationConfiguration	セキュリティプロファイルスナップショット作成設定を更新する許可を付与	書き込み	SecurityProfile*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateSecurityProfileSnapshotReleaseConfiguration	セキュリティプロファイルスナップショット解除設定を更新する許可を付与	書き込み	SecurityProfile*		
				aws:ResourceTag/${TagKey}	

AWS Marketplace Vendor Insights によって定義されたリソースの種類

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
DataSource	arn:${Partition}:vendor-insights:::data-source:${ResourceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
SecurityProfile	arn:${Partition}:vendor-insights:::security-profile:${ResourceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

AWS Marketplace Vendor Insights の条件キー

AWS Marketplace Vendor Insights では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストで渡されたタグによりアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグによりアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーによりアクセスをフィルタリングします	ArrayOfString

Amazon Mechanical Turk のアクション、リソース、および条件キー

Amazon Mechanical Turk (サービスプレフィックス: mechanicalturk) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Mechanical Turk で定義されるアクション

- Amazon Mechanical Turk で定義されるリソースタイプ
- Amazon Mechanical Turk の条件キー

Amazon Mechanical Turk で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AcceptQualificationRequest	AcceptQualificationRequest オペレーションにより、資格に関するワーカーのリクエストが許可されます。	Write			
ApproveAssignment	ApproveAssignment オペレーションは、完了した割り当ての結果を承認します。	Write			
AssociateQualificationWithWorker	AssociateQualificationWithWorker オペレーションにより、ワーカーに資格が与えられます。	Write			
CreateAdditionalAssignmentsForHIT	CreateAdditionalAssignmentsForHIT オペレーションは、既存の HIT の最大割り当て数を増やします。	Write			
CreateHIT	CreateHIT オペレーションは、新しい HIT (Human Intelligence Task) を作成します。	Write			
CreateHITType	CreateHITType オペレーションは、新しい HIT タイプを作成します。	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateHITWithHITType	CreateHITWithHITType オペレーションは、CreateHITType オペレーションにより生成された既存の HITTypeID を使用して、新しい Human Intelligence Task (HIT) を作成します。	Write			
CreateQualificationType	CreateQualificationType オペレーションは、新しい資格タイプを作成します。これは、QualificationType のデータ構造で表されます。	Write			
CreateWorkerBlock	CreateWorkerBlock オペレーションを使用すると、ワーカーが HIT で作業するのを防ぐことができます。	Write			
DeleteHIT	DeleteHIT オペレーションは、不要になった HIT を破棄します。	Write			
DeleteQualificationType	DeleteQualificationType は、資格タイプを破棄し、資格タイプに関連付けられているすべての HIT タイプを破棄します。	Write			
DeleteWorkerBlock	DeleteWorkerBlock オペレーションを使用すると、ブロックされたワーカーを元に戻して HIT で作業することができます。	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisassociateQualificationFromWorker	DisassociateQualificationFromWorker は、以前に付与された資格をユーザーから取り消します。	Write			
GetAccountBalance	GetAccountBalance オペレーションは、Amazon Mechanical Turk アカウントの金額を取得します。	Read			
GetAssignment	GetAssignment は、AssignmentStatus 値が送信済み、承認済み、または却下の割り当てを、割り当ての ID を使用して取得します。	Read			
GetFileUploadURL	GetFileUploadURL オペレーションは、一時 URL を生成して返します。	Read			
GetHIT	GetHIT オペレーションは、指定した HIT の詳細を取得します。	Read			
GetQualificationScore	GetQualificationScore オペレーションは、指定した資格タイプのワーカーの資格の値を返します。	Read			
GetQualificationType	GetQualificationType オペレーションは、ID を使用して資格タイプに関する情報を取得します。	Read			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListAssignmentsForHIT	ListAssignmentsForHIT オペレーションは、HIT の完了した割り当てを取得します。	リスト			
ListBonusPayments	ListBonusPayments オペレーションは、特定の HIT または割り当てに対してワーカーに支払ったボーナスの金額を取得します。	リスト			
ListHITs	ListHITs オペレーションは、リクエスタの HIT をすべて返します。	リスト			
ListHITsForQualificationType	ListHITsForQualificationType オペレーションは、資格要件に指定された資格タイプを使用する HIT を返します。	リスト			
ListQualificationRequests	ListQualificationRequests オペレーションは、特定の資格タイプの資格のリクエストを取得します。	リスト			
ListQualificationTypes	ListQualificationTypes オペレーションは、指定された検索クエリを使用して資格タイプを検索し、資格タイプのリストを返します。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListReviewPolicyResultsForHIT	ListReviewPolicyResultsForHIT オペレーションは、計算結果と、CreateHIT オペレーション中にレビューポリシーを実行する過程で実行されたアクションを取得します。	リスト			
ListReviewableHITs	ListReviewableHITs オペレーションは、承認または拒否されていないリクエスタの HIT をすべて返します。	リスト			
ListWorkerBlocks	ListWorkersBlocks オペレーションは、HIT での作業がブロックされているワーカーのリストを取得します。	リスト			
ListWorkersWithQualificationType	ListWorkersWithQualificationType オペレーションは、指定された資格タイプを持つすべてのワーカーを返します。	リスト			
NotifyWorkers	NotifyWorkers オペレーションは、ワーカー ID で指定する 1 人または複数のワーカーに E メールを送信します。	Write			
RejectAssignment	RejectAssignment オペレーションは、完了した割り当ての結果を却下します。	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RejectQualificationRequest	RejectQualificationRequest オペレーションにより、資格に関するユーザーのリクエストが却下されます。	Write			
SendBonus	SendBonus オペレーションは、アカウントからワーカーにお金を支払います。	Write			
SendTestEventNotification	SendTestEventNotification オペレーションにより、Amazon Mechanical Turk は、HIT イベントが発生したかのように、指定された通知仕様に従って通知メッセージを送信します。	Write			
UpdateExpirationForHIT	UpdateExpirationForHIT オペレーションでは、HIT の有効期限を現在の有効期限を超えて延長したり、HIT をすぐに期限切れにしたりできます。	Write			
UpdateHITReviewStatus	UpdateHITReviewStatus オペレーションは、HIT のステータスを切り替えます。	Write			
UpdateHITTypeOfHIT	UpdateHITTypeOfHIT オペレーションでは、HIT の HITType プロパティを変更できます。	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateNotificationSettings	UpdateNotificationSettings オペレーションは、HIT タイプの通知を作成、更新、無効化、または再有効化します。	Write			
UpdateQualificationType	UpdateQualificationType オペレーションは、既存の資格タイプの属性を変更します。これは、QualificationType データ構造で表されます。	Write			

Amazon Mechanical Turk で定義されるリソースタイプ

Amazon Mechanical Turk では、IAM ポリシーステートメントの `Resource` 要素でのリソース ARN の指定はサポートされていません。Amazon Mechanical Turk へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

Amazon Mechanical Turk の条件キー

MechanicalTurk には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon MemoryDB のアクション、リソース、および条件キー

Amazon MemoryDB (サービスプレフィックス: `memorydb`) では、IAM 許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon MemoryDB で定義されるアクション
- Amazon MemoryDB で定義されるリソースタイプ
- Amazon MemoryDB の条件キー

Amazon MemoryDB で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

> **Note**
>
> IAM で MemoryDB for Redis ポリシーを作成する場合、リソースブロックでワイルドカード「*」を使用する必要があります。IAM ポリシーで Redis API アクションの以下の MemoryDB を使用する詳細については、「MemoryDB アクションと IAM」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchUpdateCluster	サービスの更新を適用する許可を付与	書き込み	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					ec2:DescribeVpcs s3:GetObject
				aws:ResourceTag/${TagKey}	
Connect	IAM ユーザーまたはロールが、指定された MemoryDB ユーザーとしてクラスター内のノードに接続することを許可	書き込み	cluster*		
			user*		
				aws:ResourceTag/${TagKey}	
CopySnapshot	既存のスナップショットのコピーを作成する許可を付与	書き込み	snapshot*		memorydb:TagResource s3:DeleteObject s3:GetBucketAcl s3:PutObject

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateAcl	新しいアクセスコントロールリストを作成する許可を付与	書き込み	user*		memorydb:TagResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateCluster	クラスターを作成する許可を付与	書き込み	acl*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs memorydb:TagResource s3:GetObject
			parametergroup*		
			subnetgroup*		
			multiregioncluster		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			snapshot		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys memorydb:TLSEnabled	
CreateMultiRegionCluster	マルチリージョンクラスターを作成するアクセス許可を付与します	書き込み	multiregionparametergroup*		memorydb:TagResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys memorydb:TLSEnabled	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateParameterGroup	新しいパラメータグループを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	memorydb:TagResource
CreateSnapshot	現在の時点でクラスターのバックアップを作成する許可を付与	書き込み	cluster*		memorydb:TagResource s3:DeleteObject s3:GetBucketAcl s3:PutObject
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSubnetGroup	新しいサブネットグループを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	memorydb:TagResource
CreateUser	新しいユーザーを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys memorydb:UserAuthenticationMode	memorydb:TagResource
DeleteAcl	アクセスコントロールリストを削除する許可を付与	書き込み	acl*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteCluster	以前にプロビジョニングされたクラスターを削除する許可を付与	書き込み	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			multiregioncluster		
			snapshot		
				aws:ResourceTag/${TagKey}	
DeleteMultiRegionCluster	マルチリージョンクラスターを削除するアクセス許可を付与します	書き込み	multiregioncluster*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
DeleteParameterGroup	パラメータグループを削除する許可を付与	書き込み	parametergroup*		
				aws:ResourceTag/${TagKey}	
DeleteSnapshot	スナップショットを削除する許可を付与	書き込み	snapshot*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteSubnetGroup	サブネットグループを削除する許可を付与	書き込み	subnetgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
DeleteUser	ユーザーを削除する許可を付与	書き込み	user*		
				aws:ResourceTag/${TagKey}	
DescribeAcls	アクセスコントロールリストに関する情報を取得する許可を付与	読み取り	acl*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeClusters	クラスター識別子が指定されていない場合はすべてのプロビジョニングされたクラスターに関する情報を取得し、クラスター識別子が指定されている場合は特定のクラスターについての情報を取得する許可を付与	読み取り	cluster*		
				aws:ResourceTag/${TagKey}	
DescribeEngineVersions	利用可能なエンジンとそのバージョンのリストを表示する許可を付与	読み取り			
DescribeEvents	クラスター、サブネットグループ、およびパラメータグループに関連するイベントを取得する許可を付与	読み取り			
DescribeMultiRegionClusters	クラスター識別子が指定されていない場合はすべてのマルチリージョンクラスターに関する情報、クラスター識別子が指定されている場合は特定のマルチリージョンクラスターに関する情報を取得するアクセス許可を付与します	読み取り	multiregioncluster*		
				aws:ResourceTag/${TagKey}	
DescribeMultiRegionParameterGroups	マルチリージョンパラメータグループに関する情報を取得するアクセス許可を付与します	読み取り	multiregionparametergroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeMultiRegionParameters	特定のマルチリージョンパラメータグループの詳細なパラメータリストを取得するアクセス許可を付与します	読み取り	multiregionparametergroup*		
DescribeParameterGroups	パラメータグループに関する情報を取得する許可を付与	読み取り	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeParameters	特定のパラメータグループの詳細なパラメータリストを取得する許可を付与	読み取り	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeReservedNodes	リザーブドノードを取得するアクセス許可を付与	読み取り	reservednode*		
				aws:ResourceTag/${TagKey}	
DescribeReservedNodesOfferings	リザーブドノードオファリングを取得するアクセス許可を付与	読み取り			
DescribeServiceUpdates	サービス更新の詳細を取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeSnapshots	クラスターのスナップショットに関する情報を取得する許可を付与	読み取り	snapshot*		
				aws:ResourceTag/${TagKey}	
DescribeSubnetGroups	サブネットグループのリストを取得する許可を付与	読み取り	subnetgroup*		
				aws:ResourceTag/${TagKey}	
DescribeUsers	ユーザーに関する情報を取得する許可を付与	読み取り	user*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
FailoverShard	クラスター内の指定されたシャードで自動フェイルオーバーをテストする許可を付与	書き込み	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
ListAllowedMultiRegionClusterUpdates	使用可能なマルチリージョンクラスターの更新を一覧表示するアクセス許可を付与します	読み取り	multiregioncluster*		
				aws:ResourceTag/${TagKey}	
ListAllowedNodeTypeUpdates	利用可能なノードタイプの更新を一覧表示する許可を付与	読み取り	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
ListTags	コスト割り当てタグを一覧表示する許可を付与	読み取り	acl		
			cluster		
			multiregioncluster		
			parametergroup		
			snapshot		
			subnetgroup		
			user		
				aws:ResourceTag/${TagKey}	
PauseMultiRegionClusterReplication [許可のみ]	マルチリージョンクラスターのレプリケーションを一時停止するアクセス許可を付与します	書き込み	multiregioncluster*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PurchaseReservedNodesOffering	新しいリザーブドノードを購入するアクセス許可を付与	書き込み	reservednode*		memorydb:TagResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
ResetParameterGroup	パラメータグループのパラメータをエンジンまたはシステムのデフォルト値に変更する許可を付与	書き込み	parametergroup*		
				aws:ResourceTag/${TagKey}	
TagResource	名前のついたリソースに最大 10 個のコスト割り当てタグを追加する許可を付与	Tagging	acl		
			cluster		
			multiregioncluster		
			parametergroup		
			reservednode		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			snapshot		
			subnetgroup		
			user		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	TagKeys リストによって識別されたタグをリソースから削除する許可を付与	Tagging	acl		
			cluster		
			multiregioncluster		
			parametergroup		
			snapshot		
			subnetgroup		
			user		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAcl	アクセスコントロールリストを更新する許可を付与	書き込み	acl*		
			user*		
				aws:ResourceTag/${TagKey}	
UpdateCluster	クラスターの設定を更新する許可を付与	書き込み	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			acl		
			parameter group		
				aws:ResourceTag/${TagKey}	
UpdateMultiRegionCluster	マルチリージョンクラスターの設定を更新するアクセス許可を付与します	書き込み	multiregioncluster *		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			multiregionparametergroup		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
UpdateParameterGroup	パラメータグループのパラメータを更新する許可を付与	書き込み	parametergroup*		
				aws:ResourceTag/${TagKey}	
UpdateSubnetGroup	サブネットグループを更新する許可を付与	書き込み	subnetgroup*		
				aws:ResourceTag/${TagKey}	
UpdateUser	ユーザーを更新する許可を付与	書き込み	user*		
				aws:ResourceTag/${TagKey} memorydb:UserAuthenticationMode	

Amazon MemoryDB で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
multiregionparametergroup	arn:${Partition}:memorydb::${Account}:multiregionparametergroup/${MultiRegionParameterGroupName}	
parametergroup	arn:${Partition}:memorydb:${Region}:${Account}:parametergroup/${ParameterGroupName}	aws:ResourceTag/${TagKey}
subnetgroup	arn:${Partition}:memorydb:${Region}:${Account}:subnetgroup/${SubnetGroupName}	aws:ResourceTag/${TagKey}
multiregioncluster	arn:${Partition}:memorydb::${Account}:multiregioncluster/${ClusterName}	aws:ResourceTag/${TagKey} memorydb:TLSEnabled
cluster	arn:${Partition}:memorydb:${Region}:${Account}:cluster/${ClusterName}	aws:ResourceTag/${TagKey}
snapshot	arn:${Partition}:memorydb:${Region}:${Account}:snapshot/${SnapshotName}	aws:ResourceTag/${TagKey}
user	arn:${Partition}:memorydb:${Region}:${Account}:user/${UserName}	aws:ResourceTag/${TagKey}
acl	arn:${Partition}:memorydb:${Region}:${Account}:acl/${AclName}	aws:ResourceTag/${TagKey}
reservednode	arn:${Partition}:memorydb:${Region}:${Account}:reservednode/${ReservationID}	aws:ResourceTag/${TagKey}

Amazon MemoryDB の条件キー

Amazon MemoryDB は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします。	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられているタグに基づいてアクションをフィルタリングします。	文字列
aws:TagKeys	リクエストで渡されたタグキーに基づいてアクションをフィルタリングします。	ArrayOfString
memorydb:TLSEnabled	リクエスト内に存在する TLSEnabled パラメータによってアクセスをフィルタリングするか、パラメータが存在しない場合はデフォルトで true 値に設定する	Bool
memorydb:UserAuthenticationMode	リクエスト内の UserAuthenticationMode.Type パラメータでアクセスをフィルタリングする	String

Amazon Message Delivery Service のアクション、リソース、および条件キー

Amazon Message Delivery Service (サービスプレフィックス: ec2messages) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Message Delivery Service で定義されるアクション
- Amazon Message Delivery Service で定義されるリソースタイプ
- Amazon Message Delivery Service の条件キー

Amazon Message Delivery Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcknowledgeMessage	メッセージを承認するアクセス権限を付与し、再度配信されないようにします	Write			
DeleteMessage	メッセージを削除するアクセス権限を付与します	Write			
FailMessage	メッセージに失敗し、メッセージが正常に処理されなかったこと、返信または再送信できないことを示すアクセス権限を付与します	Write			
GetEndpoint	メッセージの指定された宛先に基づき、正しいエンドポイントにトラフィックをルーティングするアクセス権限を付与します	Read			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetMessages	ロングポーリングを使用してクライアント/インスタンスにメッセージを配信するアクセス権限を付与します	Read		ssm:SourceInstanceARN ec2:SourceInstanceARN	
SendReply	クライアント/インスタンスからアップストリームサービスへの応答を送信するアクセス権限を付与します	Write		ssm:SourceInstanceARN ec2:SourceInstanceARN	

Amazon Message Delivery Service で定義されるリソースタイプ

Amazon Message Delivery Service では、IAM ポリシーステートメントの `Resource` 要素でのリソース ARN の指定はサポートされていません。Amazon Message Delivery Service へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

Amazon Message Delivery Service の条件キー

Amazon Message Delivery Service は、IAM ポリシーの `Condition` 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
ec2:SourceInstanceARN	リクエストが発生したインスタンスの ARN によってアクセスをフィルタリングします	ARN
ssm:SourceInstanceARN	リクエスト元の AWS Systems Manager マネージドインスタンスの Amazon リソースネーム (ARN) を検証してアクセスをフィルタリングします。EC2 インスタンスプロファイルに関連付けられた IAM ロールで認証されたマネージドインスタンスからリクエストが送信された場合、このキーは存在しません。	ARN

Amazon Message Gateway Service のアクション、リソース、および条件キー

Amazon Message Gateway Service (サービスプレフィックス: `ssmmessages`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Message Gateway Service で定義されるアクション
- Amazon Message Gateway Service で定義されるリソースタイプ
- Amazon Message Gateway Service の条件キー

Amazon Message Gateway Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateControlChannel	インスタンスが Systems Manager サービスにコントロールメッセージを送信するためのコントロールチャネルを登録するアクセス権限を付与します	Write		ssm:SourceInstanceARN ec2:SourceInstanceARN	
CreateDataChannel	インスタンスが Systems Manager サービスにデータメッセージを送信するためのデータチャネルを登録するアクセス権限を付与します	Write			
OpenControlChannel	インスタンスから Systems Manager サービスへの登録済みコントロールチャネルストリームの WebSocket 接続を開くアクセス権限を付与します	Write			
OpenDataChannel	インスタンスから Systems Manager サービスへの登録済みデータチャネルストリームの WebSocket 接続を開くアクセス権限を付与します	書き込み			

Amazon Message Gateway Service で定義されるリソースタイプ

Amazon Message Gateway Service では、IAM ポリシーステートメントの `Resource` 要素でのリソース ARN の指定はサポートされていません。Amazon Message Gateway Service へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

Amazon Message Gateway Service の条件キー

Amazon Message Gateway Service では、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
ec2:SourceInstanceARN	リクエストが発生したインスタンスの ARN によってアクセスをフィルタリングします	ARN
ssm:SourceInstanceARN	リクエスト元の AWS Systems Manager マネージドインスタンスの Amazon リソースネーム (ARN) を検証してアクセスをフィルタリングします。EC2 インスタンスプロファイルに関連付けられた IAM ロールで認証されたマネージドインスタンスからリクエストが送信された場合、このキーは存在しません。	ARN

AWS .NET 用Microservice Extractorのアクション、リソースおよび条件キー

AWS Microservice Extractor for .NET (サービスプレフィックス: serviceextract) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS .NET 用Microservice Extractorで定義されるアクション
- AWS .NET 用Microservice Extractorで定義されるリソースタイプ
- AWS .NET用Microservice Extractorの条件キー

AWS .NET 用Microservice Extractorで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベルの列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetConfig [アクセス許可のみ]	AWS Microservice Extractor for .NET デスクトップクライアントに必要な設定を取得する許可を付与	読み取り			

AWS .NET 用Microservice Extractorで定義されるリソースタイプ

AWS Microservice Extractor for .NET では、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定はサポートされていません。 AWS `."Resource": "*"`のポリシーで、Microservice Extractorへアクセスするためには、

AWS .NET用Microservice Extractorの条件キー

Microservice Extractor for .NET には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Migration Acceleration Program クレジットのアクション、リソース、および条件キー

AWS Migration Acceleration Program Credits (サービスプレフィックス: `mapcredits`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Migration Acceleration Program クレジットで定義されるアクション
- AWS Migration Acceleration Program クレジットで定義されるリソースタイプ
- AWS Migration Acceleration Program クレジットの条件キー

AWS Migration Acceleration Program クレジットで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListAssociatedPrograms [アクセス許可のみ]	ユーザーの関連付られている Migration Acceleration Program 契約を表示する許可を付与	リスト	agreement*		
ListQuarterCredits [許可のみ]	ユーザーの支払人アカウントに関連付けられている Migration Acceleration Program 契約クレジットを表示する許可を付与	リスト	agreement*		
ListQuarterSpend [許可のみ]	ユーザーの支払人アカウントに関連付けられている Migration Acceleration Program 契約の対象となる支出を閲覧する許可を付与	リスト	agreement*		

AWS Migration Acceleration Program クレジットで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
agreement	`arn:${Partition}:mapcredits:::${Agreement}/${AgreementId}`	

AWS Migration Acceleration Program クレジットの条件キー

MapCredits には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Migration Hub のアクション、リソース、および条件キー

AWS Migration Hub (サービスプレフィックス: mgh) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Migration Hub で定義されるアクション
- AWS Migration Hub で定義されるリソースタイプ
- AWS Migration Hub の条件キー

AWS Migration Hub で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptConnection	接続を受け入れるアクセス許可を付与します	書き込み	ConnectionResource*		
				aws:TagKeys aws:RequestTag/${TagKey}	
AssociateAutomationUnitRole	IAM ロールをオートメーションユニットに関連付けるアクセス許可を付与します	書き込み	AutomationUnitResource*		
AssociateCreatedArtifact	特定の AWS アーティファクトを MigrationTask に関連付けるアクセス許可を付与します	書き込み	migrationTask*		
AssociateDiscoveredResource	特定の ADS リソースを MigrationTask に関連付けるアクセス許可を付与します	書き込み	migrationTask*		
AssociateSourceResource	ソースリソースを関連付けるアクセス許可を付与します	書き込み	migrationTask*		
BatchAssociateIamRoleWithConnection	IAM ロールを接続にバッチ関連付けするアクセス許可を付与します	書き込み	ConnectionResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchDisassociateIamRoleFromConnection	接続から IAM ロールをバッチで関連付け解除するアクセス許可を付与します	書き込み	ConnectionResource*		
CreateAutomationRun	オートメーションユニット実行を作成するアクセス許可を付与します	書き込み			
CreateAutomationUnit	オートメーションユニットを作成するアクセス許可を付与します	書き込み			
CreateHomeRegionControl	Migration Hub ホームリージョンコントロールを作成するアクセス許可を付与します	書き込み			
CreateProgressUpdateStream	ProgressUpdateStream を作成するアクセス許可を付与します	書き込み	progressUpdateStream*		
DeleteAutomationRun	オートメーションユニット実行を削除するアクセス許可を付与します	書き込み	AutomationRunResource*		
DeleteAutomationUnit	オートメーションユニットを削除するアクセス許可を付与します	書き込み	AutomationUnitResource*		
DeleteConnection	接続を削除する許可を付与。	書き込み	ConnectionResource*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteHomeRegionControl	Migration Hub ホームリージョンコントロールを削除するアクセス許可を付与します	書き込み			
DeleteProgressUpdateStream	ProgressUpdateStream を削除するアクセス許可を付与します	書き込み	progressUpdateStream*		
DescribeApplicationState	アプリケーション変換サービスのアプリケーションの状態を取得するアクセス許可を付与します	読み取り			
DescribeAutomationRun	オートメーションユニットの実行を記述するアクセス許可を付与します	読み取り	AutomationRunResource*		
DescribeAutomationUnit	オートメーションユニットを記述するアクセス許可を付与します	読み取り	AutomationUnitResource*		
DescribeHomeRegionControls	ホームリージョンコントロールを一覧表示するアクセス許可を付与します	リスト			
DescribeMigrationTask	MigrationTask を説明するアクセス許可を付与します	読み取り	migrationTask*		
DisassociateAutomationUnitRole	オートメーションユニットから IAM ロールの関連付けを解除するアクセス許可を付与します	書き込み	AutomationUnitResource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisassociateCreatedArtifact	MigrationTask から特定の AWS アーティファクトの関連付けを解除するアクセス許可を付与します	書き込み	migrationTask*		
DisassociateDiscoveredResource	MigrationTask から特定の ADS リソースの関連付けを解除するアクセス許可を付与します	書き込み	migrationTask*		
DisassociateSourceResource	ソースリソースの関連付けを解除するアクセス許可を付与します	書き込み	migrationTask*		
GetConnection	接続を取得するためアクセス許可を付与	読み取り	ConnectionResource* -		
GetHomeRegion	Migration Hub ホームリージョンを取得するアクセス許可を付与します	読み取り			
ImportMigrationTask	MigrationTask をインポートするアクセス許可を付与します	書き込み	migrationTask*		
ListApplicationStates	アプリケーションのステータスを一覧表示するアクセス許可を付与します	リスト			
ListAutomationRuns	自動化ユニットの実行を一覧表示するアクセス許可を付与します	リスト			
ListAutomationUnits	自動化ユニットを一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListConnectionRoles	接続ロールを一覧表示するアクセス許可を付与します	リスト	ConnectionResource*		
ListConnections	接続を一覧表示するアクセス許可を付与します	リスト			
ListCreatedArtifacts	MigrationTask に関連付けられた作成済みのアーティファクトを一覧表示するアクセス許可を付与します	リスト	migrationTask*		
ListDiscoveredResources	MigrationTask から関連付けられた ADS リソースを一覧表示するアクセス許可を付与します	リスト	migrationTask*		
ListMigrationTaskUpdates	移行タスクの更新を一覧表示するアクセス許可を付与します	リスト	migrationTask*		
ListMigrationTasks	MigrationTask を一覧表示するアクセス許可を付与します	リスト			
ListProgressUpdateStreams	ProgressUpdateStream を一覧表示するアクセス許可を付与します	リスト			
ListSourceResources	ソースリソースを一覧表示するアクセス許可を付与します	リスト	migrationTask*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
NotifyApplicationState	アプリケーション変換サービスのアプリケーションの状態を更新するアクセス許可を付与します	書き込み			
NotifyMigrationTaskState	MigrationTask の最新の状態を通知するアクセス許可を付与します	書き込み	migrationTask*		
PutResourceAttributes	ResourceAttribute を配置するアクセス許可を付与します	書き込み	migrationTask*		
RejectConnection	接続を拒否するアクセス許可を付与します	書き込み	ConnectionResource*		
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け		aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	リソースのタグを解除する許可を付与	Tagging		aws:TagKeys	

AWS Migration Hub で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
progressUpdateStream	arn:${Partition}:mgh:${Region}:${Account}:progressUpdateStream/${Stream}	
migrationTask	arn:${Partition}:mgh:${Region}:${Account}:progressUpdateStream/${Stream}/migrationTask/${Task}	
AutomationRunResource	arn:${Partition}:mgh:${Region}:${Account}:automation-run/${RunID}	mgh:AutomationRunResourceRunID
AutomationUnitResource	arn:${Partition}:mgh:${Region}:${Account}:automation-unit/${AutomationUnitId}	mgh:AutomationUnitResourceAutomationUnitArn
ConnectionResource	arn:${Partition}:mgh:${Region}:${Account}:${ConnectionArn}	aws:ResourceTag/${TagKey} mgh:ConnectionResourceConnectionArn

AWS Migration Hub の条件キー

AWS Migration Hub では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします	文字列

条件キー	説明	タイプ
aws:ResourceTag/${TagKey}	リソースに関連付けられているタグに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーに基づいてアクションをフィルタリングします	ArrayOfString
mgh:AutomationRunResourceRunID	AutomationRunResource リソース runID 識別子	String
mgh:AutomationUnitResourceAutomationUnitArn	AutomationUnitResource リソース automationUnitArn 識別子	ARN
mgh:ConnectionResourceConnectionArn	ConnectionResource リソース connectionArn 識別子	String

AWS Migration Hub Orchestrator のアクション、リソース、および条件キー

AWS Migration Hub Orchestrator (サービスプレフィックス: `migrationhub-orchestrator`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Migration Hub Orchestrator で定義されるアクション
- AWS Migration Hub Orchestrator で定義されるリソースタイプ
- AWS Migration Hub Orchestrator の条件キー

AWS Migration Hub Orchestrator で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateTemplate	カスタムテンプレートを作成する許可を付与する	書き込み			
CreateWorkflow	選択したテンプレートに基づいてワークフローを作成するアクセス許可を付与します	書き込み	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkflowStep	ワークフローおよび特定のステップグループの下にステップを作成するアクセス許可を付与します	書き込み	workflow*		
CreateWorkflowStepGroup	特定のワークフローのカスタムステップグループを作成するアクセス許可を付与します	書き込み	workflow*		
DeleteTemplate	カスタムテンプレートを削除する許可を付与する	書き込み	template*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteWorkflow	ワークフローにアクセス許可を付与します	書き込み	workflow*		
DeleteWorkflowStep	ワークフロー内の特定のステップグループからステップを削除するアクセス許可を付与します	書き込み	workflow*		
DeleteWorkflowStepGroup	ワークフローに関連付けられたステップグループを削除するアクセス許可を付与します	書き込み	workflow*		
GetMessage	サービスから情報を受信するアクセス許可をプラグインに付与します	読み込み			
GetTemplate	テンプレート用のメタデータを取得するアクセス許可を付与します	読み込み	template*		
GetTemplateStep	テンプレートおよびステップグループに関連付けられたステップの詳細を取得するアクセス許可を付与します	読み込み	template*		
GetTemplateStepGroup	テンプレート内のステップグループのメタデータを取得するアクセス許可を付与します	読み込み	template*		
GetWorkflow	ワークフローに関連付けられたメタデータを取得するアクセス許可を付与します	読み込み	workflow*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetWorkflowStep	ワークフローおよびステップグループに関連付けられたステップの詳細を取得するアクセス許可を付与します	読み込み	workflow*		
GetWorkflowStepGroup	ワークフローに関連付けられたステップグループの詳細を取得するアクセス許可を付与します	読み込み	workflow*		
ListPlugins	登録されているすべてのプラグインのリストを取得するアクセス許可を付与します	リスト			
ListTagsForResource	リソースに関連付けられているすべてのタグのリストを取得するアクセス許可を付与します	読み込み	template* workflow*		
ListTemplateStepGroups	テンプレートのステップグループを一覧表示するアクセス許可を付与します	リスト	template*		
ListTemplateSteps	ステップグループ内のステップのリストを取得するアクセス許可を付与します	リスト	template*		
ListTemplates	顧客が利用できるすべてのテンプレートのリストを取得するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListWorkflowStepGroups	ワークフローに関連付けられたステップグループのリストを取得するアクセス許可を付与します	リスト	workflow*		
ListWorkflowSteps	ワークフローに関連付けられたステップグループ内のステップのリストを取得するアクセス許可を付与します	リスト	workflow*		
ListWorkflows	全てのワークフローを一覧表示するアクセス許可を付与します	リスト			
RegisterPlugin	プラグインを登録して、ID を受信し、サービスからのメッセージの受信を開始するアクセス許可を付与します	書き込み			
RetryWorkflowStep	ワークフロー内で失敗したステップを再試行するアクセス許可を付与します	書き込み	workflow*		
SendMessage	サービスに情報を送信するアクセス許可をプラグインに付与します	書き込み			
StartWorkflow	ワークフローを開始したり、停止したワークフローを再開したりするアクセス許可を付与します	書き込み	workflow*		
StopWorkflow	ワークフローを停止するアクセス許可を付与します	書き込み	workflow*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagResource	リソースにタグを追加するアクセス許可を付与します	タグ付け	template		
			workflow		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	リソースからタグを削除する許可を付与	Tagging	template		
			workflow		
				aws:TagKeys	
UpdateTemplate	カスタムテンプレートを更新する許可を付与する	書き込み	template*		
UpdateWorkflow	ワークフローに関連付けられたメタデータを更新するアクセス許可を付与します	書き込み	workflow*		
UpdateWorkflowStep	ワークフロー内のカスタムステップのメタデータとステータスを更新するアクセス許可を付与します	書き込み	workflow*		
UpdateWorkflowStepGroup	特定のワークフロー内のステップグループに関連付けられたメタデータを更新するアクセス許可を付与します	書き込み	workflow*		

AWS Migration Hub Orchestrator で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
workflow	arn:${Partition}:migrationhub-orchestrator:${Region}:${Account}:workflow/${ResourceId}	aws:ResourceTag/${TagKey}
template	arn:${Partition}:migrationhub-orchestrator:${Region}:${Account}:template/${ResourceId}	aws:ResourceTag/${TagKey}

AWS Migration Hub Orchestrator の条件キー

AWS Migration Hub Orchestrator では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列

条件キー	説明	タイプ
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Migration Hub Refactor Spacesのアクション、リソース、および条件キー

AWS Migration Hub Refactor Spaces (サービスプレフィックス: `refactor-spaces`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Migration Hub Refactor Spacesで定義されるアクション
- AWS Migration Hub Reactor Spacesで定義されるリソースタイプ
- AWS Migration Hub Refactor Spacesの条件キー

AWS Migration Hub Refactor Spacesで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にア

クションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateApplication	環境内のアプリケーションを作成する許可を付与します。	書き込み		refactor-spaces:ApplicationCreatedByAccount	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				refactor-spaces:CreatedByAccountIds aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironment	環境を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateRoute	アプリケーションのルートを作成する許可を付与します。	書き込み		refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateService	アプリケーション内のサービスを作成する許可を付与します。	書き込み		refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:CreatedByAccountIds aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	環境内のアプリケーションを削除する許可を付与します。	書き込み	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
DeleteEnvironment	環境を削除する許可を付与します	書き込み	environment*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	リソースポリシーを削除する許可を付与。	書き込み			
DeleteRoute	アプリケーションのルートを削除する許可を付与します。	書き込み	route*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:ResourceTag/${TagKey}	
DeleteService	アプリケーションからのサービスを削除する許可を付与します。	書き込み	service*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
GetApplication	アプリケーション関する情報を取得する許可を付与します。	読み取り	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
GetEnvironment	開発環境に関する詳細を取得する許可を付与します。	読み取り	environment*		
				aws:ResourceTag/${TagKey}	
GetResourcePolicy	リソースポリシーに関する詳細を取得する許可を付与します。	読み取り			
GetRoute	ルートに関する情報を取得するためのアクセス許可を付与します。	読み取り	route*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:ResourceTag/${TagKey}	
GetService	サービスに関する情報を取得するためのアクセス許可を付与します。	読み取り	service*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
ListApplications	環境内のすべてのアプリケーションを一覧表示する許可を付与します。	読み取り	application*		
ListEnvironmentVpcs	環境のすべてのVPC一覧表示する許可を付与します。	読み取り	environment*		
ListEnvironments	すべての環境を一覧表示する許可を付与します。	読み取り			
ListRoutes	アプリケーション内のすべてのルートを一覧表示する許可を付与します。	読み取り	route*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListServices	環境内にあるすべてのサービスを一覧表示するアクセス許可を付与します。	読み取り	environment*		
ListTagsForResource	指定されたリソースのすべてのタグを一覧表示する許可を付与します。	読み取り			
PutResourcePolicy	リソースポリシーを追加する許可を付与します。	書き込み			
TagResource	リソースにタグを付けるアクセス許可を付与	Tagging	application		
			environment		
			route		
			service		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
UntagResource	リソースからタグを削除する許可を付与	Tagging	application		
			environment		
			route		
			service		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
UpdateRoute	アプリケーションのルートを更新する許可を付与します。	書き込み	route*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:ResourceTag/${TagKey}	

AWS Migration Hub Reactor Spacesで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
environment	arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}	aws:ResourceTag/${TagKey}
application	arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}/application/${ApplicationId}	aws:ResourceTag/${TagKey} refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds
service	arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}/application/${ApplicationId}/service/${ServiceId}	aws:ResourceTag/${TagKey} refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:ServiceCreatedByAccount

リソースタイプ	ARN	条件キー
route	arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}/application/${ApplicationId}/route/${RouteId}	aws:ResourceTag/${TagKey} refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:RouteCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:SourcePath

AWS Migration Hub Refactor Spacesの条件キー

AWS Migration Hub リファクタリングスペースは、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString
refactor-spaces:ApplicationCreatedByAccount	環境内でアプリケーションを作成したアカウントのみにアクションを制限して、アクセスをフィルタリングします。	String
refactor-spaces:CreatedByAccountIds	リソースを作成したアカウントでアクセスをフィルタリングします。	ArrayOfString
refactor-spaces:RouteCreatedByAccount	アプリケーション内でルートを作成したアカウントのみに制限して、アクセスをフィルタリングします。	String
refactor-spaces:ServiceCreatedByAccount	アプリケーション内でサービスを作成したアカウントのみにアクションを制限して、アクセスをフィルタリングします。	String
refactor-spaces:SourcePath	ルートのパス によってアクセスをフィルタリングします。	String

AWS Migration Hub Strategy Recommendations のアクション、リソース、および条件キー

AWS Migration Hub Strategy Recommendations (サービスプレフィックス: `migrationhub-strategy`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Migration Hub Strategy Recommendations で定義されるアクション
- AWS Migration Hub Strategy Recommendations で定義されるリソースタイプ
- AWS Migration Hub Strategy Recommendations の条件キー

AWS Migration Hub Strategy Recommendations で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetAntiPattern	顧客の環境でコレクターが参照すべき各アンチパターンの詳細を、取得するためのアクセス許可を付与する	読み込み			
GetApplicationComponentDetails	アプリケーションの詳細を取得するためのアクセス許可を付与する	読み込み			
GetApplicationComp	サーバーで実行されているアプリケーションに対し推奨される、すべての戦略とツール	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
onentStrategies	のリストを取得するためのアクセス許可を付与する				
GetAssessment	進行中の評価についてのステータスを取得するためのアクセス許可を付与する	読み込み			
GetImportFileTask	特定のインポートタスクの詳細を取得するためのアクセス許可を付与する	読み取り			
GetLatestAssessmentId	最新の評価 ID を取得するための許可を付与します	読み取り			
GetMessage	サービスから情報を受信するためのアクセス許可をコレクターに付与する	読み込み			
GetPortfolioPreferences	顧客の移行/モダナイゼーションに関する設定を取得するためのアクセス許可を付与する	読み込み			
GetPortfolioSummary	全体的な概要 (リホストするサーバの数、アンチパターンの総数など) を取得するためのアクセス許可を付与する	読み込み			
GetRecommendationReportDetails	推奨事項のレポートに関する詳細情報を取得するためのアクセス許可を付与する	読み込み			
GetServerDetails	特定のサーバーに関する情報を取得するためのアクセス許可を付与する	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetServerStrategies	特定のサーバーに対し推奨される戦略とツールを取得するためのアクセス許可を付与する	読み取り			
ListAnalyzableServers	お客様の vcenter 環境内にある分析可能なすべてのサーバーのリストを取得するアクセス許可を付与する	リスト			
ListAntiPatterns	顧客の環境でコレクターが検索すべきすべてのアンチパターンのリストを、取得するためのアクセス許可を付与する	リスト			
ListApplicationComponents	顧客のサーバー上で実行されているすべてのアプリケーションのリストを取得するためのアクセス許可を付与する	リスト			
ListCollectors	顧客によってインストールされたすべてのコレクターのリストを取得するためのアクセス許可を付与する	リスト			
ListImportFileTask	顧客により実行されたすべてのインポートのリストを取得するためのアクセス許可を付与する	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListJarArtifacts	コレクターによる評価の対象となるバイナリのリストを、取得するためのアクセス許可を付与する	リスト			
ListServers	顧客の環境内にある、すべてのサーバーのリストを取得するためのアクセス許可を付与する	リスト			
PutLogData	サービスにログを送信する許可をコレクタに付与する	書き込み			
PutMetricData	サービスにメトリクスを送信する許可をコレクタに付与する	書き込み			
PutPortfolioPreferences	顧客における移行/モダナイゼーションの設定を保存するためのアクセス許可を付与する	書き込み			
RegisterCollector	ID を受信し、サービスからのメッセージの受信を開始するために登録を行う許可をコレクタに付与する	書き込み			
SendMessage	サービスに情報を送信するための許可をコレクタに付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartAssessment	顧客の環境で (すべてのサーバからデータを収集し、推奨事項を提供する) 評価を開始するためのアクセス許可を付与する	書き込み			
StartImportFileTask	顧客から提供されたファイルからのデータのインポートを開始するためのアクセス許可を付与する	書き込み			
StartRecommendationReportGeneration	推奨事項レポートの生成を開始するためのアクセス許可を付与する	書き込み			
StopAssessment	進行中の評価を停止するためのアクセス許可を付与する	書き込み			
UpdateApplicationComponentConfig	アプリケーションの詳細を更新するためのアクセス許可を付与する	書き込み			
UpdateCollectorConfiguration	サービスに設定情報を送信するための許可をコレクターに付与します	書き込み			
UpdateServerConfig	推奨される戦略を含めたサーバー上の情報を更新するためのアクセス許可を付与する	書き込み			

AWS Migration Hub Strategy Recommendations で定義されるリソースタイプ

AWS Migration Hub Strategy Recommendations は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Migration Hub Strategy Recommendations へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Migration Hub Strategy Recommendations の条件キー

Migration Hub Strategy Recommendations には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Mobile Analytics のアクションとリソース、条件キー

Amazon Mobile Analytics (サービスプレフィックス: `mobileanalytics`) では、以下のサービス固有のリソースやアクション、条件コンテキストキーを IAM アクセス許可ポリシーで使用できます。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Mobile Analytics で定義されるアクション
- Amazon Mobile Analytics で定義されるリソースタイプ
- Amazon Mobile Analytics の条件キー

Amazon Mobile Analytics で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetFinancialReports	アプリの財務メトリクスへのアクセスを許可します。	Read			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetReports	アプリの標準メトリクスへのアクセスを許可します。	Read			
PutEvents	PutEvents オペレーションは、1 つ以上のイベントを記録します。	Write			

Amazon Mobile Analytics で定義されるリソースタイプ

Amazon Mobile Analytics では、IAM ポリシーステートメントの `Resource` 要素でのリソース ARN の指定はサポートされていません。Amazon Mobile Analytics へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

Amazon Mobile Analytics の条件キー

Mobile Analytics には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS「グローバル条件コンテキストキー」を参照してください。

Amazon Monitron のアクション、リソース、および条件キー

Amazon Monitron (サービスプレフィックス: `monitron`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Monitron で定義されるアクション

- Amazon Monitron で定義されるリソースタイプ
- Amazon Monitron の条件キー

Amazon Monitron で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateProjectAdminUser [アクセス許可のみ]	ユーザーを管理者としてプロジェクトに関連付けるアクセス許可を付与	Permissions management	project*		sso-directory:DescribeUsers sso:AssociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateProject [許可のみ]	プロジェクトを作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole kms:CreateGrant sso:CreateManagedApplicationInstance sso:DeleteManagedApplicationInstance sso:DescribeRegisteredRegions

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateProjectUserAssociation [アクセス許可のみ]	ユーザーをプロジェクトに関連付けるアクセス許可を付与	権限の管理	project*		sso-directory:DescribeUsers sso:AssociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateUserAccessRoleAssociation [許可のみ]	ユーザーにアクセスロールを関連付ける許可を付与	権限の管理	project*		sso-directory:DescribeUsers sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles
DeleteProject [許可のみ]	プロジェクトを削除する許可を付与	書き込み	project*		sso:DeleteManagedApplicationInstance

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteProjectUserAssociation [アクセス許可のみ]	プロジェクトからユーザーの関連付けを解除する許可を付与	権限の管理	project*		sso-directory:DescribeUsers sso:DisassociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfiles
DeleteUserAccessRoleAssociation [許可のみ]	ユーザーからアクセスロールの関連付けを解除する許可を付与。	権限の管理	project*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisassociateProjectAdminUser [許可のみ]	プロジェクトと管理者の関連付けを解除するアクセス許可を付与	Permissions management	project*		sso-directory:DescribeUsers sso:DisassociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfiles
GetProject [許可のみ]	プロジェクトに関する情報を取得するアクセス許可を付与	読み込み	project*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetProjectAdminUser [許可のみ]	プロジェクトに関連付けられている管理者を記述するアクセス許可を付与	読み込み	project*		sso-directory:DescribeUsers sso:GetManagedApplicationInstance sso:ListProfileAssociations
ListProjectAdminUsers [許可のみ]	プロジェクトに関連付けられているすべての管理者を一覧表示するアクセス許可を付与	Permissions management	project*		sso-directory:DescribeUsers sso:GetManagedApplicationInstance

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListProjectUserAssociations [許可のみ]	プロジェクトに関連付けられているすべてのユーザーを一覧表示する許可を付与	リスト	project*		sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles
ListProjects [許可のみ]	すべてのプロジェクトを一覧表示するアクセス許可を付与	リスト			
ListTagsForResource [許可のみ]	リソースのすべてのタグを一覧表示する許可を付与	読み込み	project		
ListUserAccessRoleAssociations [許可のみ]	ユーザーに関連付けられたすべてのアクセスロールを一覧表示する許可を付与	リスト	project*		
TagResource [許可のみ]	リソースにタグを付けるアクセス許可を付与	タグ付け	project		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [アクセス許可のみ]	リソースのタグを解除する許可を付与	タグ付け	project		
				aws:TagKeys	
UpdateProject [アクセス許可のみ]	プロジェクトを更新する許可を付与	書き込み	project*		

Amazon Monitron で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
project	arn:${Partition}:monitron:${Region}:${Account}:project/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon Monitron の条件キー

Amazon Monitron では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアによるアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされたタグでアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon MQ のアクション、リソース、および条件キー

Amazon MQ (サービスプレフィックス: mq) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件キーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon MQ で定義されるアクション
- Amazon MQ で定義されるリソースタイプ

- Amazon MQ の条件キー

Amazon MQ で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateBroker	ブローカーを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:CreateVpcEndpoint ec2:DescribeInternetGateways ec2:DescribeNetworkInterfacePermissions ec2:DescribeNetworkInterfaces

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyNetworkInterfaceAttribute iam:CreateServiceLinkedRole route53:AssociateVPCWithHostedZone
CreateConfiguration	指定した設定名の新しい設定を作成する許可を付与。Amazon MQ では、デフォルトの設定 (エンジンのタイプとエンジンのバージョン) が使用されます	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateReplicaBroker [アクセス許可のみ]	レプリカブローカーを作成する許可を付与	書き込み	brokers*		
CreateTags	タグを作成する許可を付与	タグ付け	brokers		
			configurations		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUser	ActiveMQ ユーザーを作成する許可を付与	書き込み	brokers*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteBroker	ブローカーを削除する許可を付与	書き込み	brokers*		ec2:DeleteNetworkInterface ec2:DeleteNetworkInterfacePermission ec2:DeleteVpcEndpoints ec2:DetachNetworkInterface
DeleteConfiguration	設定を削除するアクセス許可を付与します	書き込み	configurations*		
DeleteTags	タグを削除する許可を付与	タグ付け	brokers		
			configurations		
				aws:TagKeys	
DeleteUser	ActiveMQ ユーザーを削除する許可を付与	書き込み	brokers*		
DescribeBroker	指定したブローカーに関する情報を返すアクセス許可を付与する	読み込み	brokers*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeBrokerEngineTypes	ブローカーエンジンに関する情報を返すアクセス許可を付与する	読み込み			
DescribeBrokerInstanceOptions	ブローカーインスタンスオプションに関する情報を返すアクセス許可を付与します。	読み込み			
DescribeConfiguration	指定した設定に関する情報を返すアクセス許可を付与する	読み込み	configurations*		
DescribeConfigurationRevision	指定した設定の指定した設定リビジョンを返すアクセス許可を付与する	読み込み	configurations*		
DescribeUser	ActiveMQ ユーザーに関する情報を返すアクセス許可を付与する	読み込み	brokers*		
ListBrokers	すべてのブローカーのリストを返すアクセス許可を付与する	リスト			
ListConfigurationRevisions	指定した設定の既存のすべてのリビジョンのリストを返すアクセス許可を付与する	リスト	configurations*		
ListConfigurations	すべての設定のリストを返すアクセス許可を付与する	リスト			
ListTags	タグのリストを返すアクセス許可を付与する	リスト	brokers		
			configurations		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListUsers	すべての ActiveMQ ユーザーのリストを返すアクセス許可を付与する	リスト	brokers*		
Promote	ブローカーを昇格させる許可を付与します	書き込み	brokers*		
RebootBroker	ブローカーを再起動する許可を付与	書き込み	brokers*		
UpdateBroker	ブローカーに保留中の設定変更を追加する許可を付与	書き込み	brokers*		
UpdateConfiguration	指定した設定を更新する許可を付与	書き込み	configurations*		
UpdateUser	ActiveMQ ユーザーに関する情報を更新する許可を付与	書き込み	brokers*		

Amazon MQ で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
brokers	`arn:${Partition}:mq:${Region}:${Account}:broker:${BrokerName}:${BrokerId}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
configurations	arn:${Partition}:mq:${Region}:${Account}:configuration:${ConfigurationId}	aws:ResourceTag/${TagKey}

Amazon MQ の条件キー

Amazon MQ では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

マルチパーティー承認のアクション、リソース、および条件キー

マルチパーティー承認 (サービスプレフィックス: mpa) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- マルチパーティー承認で定義されるアクション
- マルチパーティー承認で定義されるリソースタイプ
- マルチパーティー承認の条件キー

マルチパーティー承認で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelSession	承認セッションをキャンセルするアクセス許可を付与します	書き込み	session*		
				aws:ResourceTag/${TagKey} mpa:RequestedOperation mpa:ProtectedResourceAccount	
CreateApprovalTeam	承認チームを作成するアクセス許可を付与します	書き込み	approval-team*		
				aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:TagKeys	
CreateIdentitySource	ID ソースを作成するアクセス許可を付与します	書き込み	identity-source*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteIdentitySource	ID ソースを削除するアクセス許可を付与します	書き込み	identity-source*		
				aws:ResourceTag/${TagKey}	
DeleteInactiveApprovalTeamVersion	非アクティブな承認チームを削除するアクセス許可を付与します	書き込み	approval-team*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteResourcePolicy [アクセス許可のみ]	リソースポリシーを削除する許可を付与。	権限の管理			
GetApprovalTeam	承認チームの詳細を取得するアクセス許可を付与します	読み取り	approval-team*		
				aws:ResourceTag/${TagKey}	
GetIdentitySource	ID ソースの詳細を取得するアクセス許可を付与します	読み取り	identity-source*		
				aws:ResourceTag/${TagKey}	
GetPolicyVersion	ポリシーの詳細を取得するアクセス許可を付与します	読み取り			
GetResourcePolicy	特定のリソースの詳細を取得するアクセス許可を付与します	読み取り			
GetSession	承認セッションの詳細を取得するアクセス許可を付与します	読み取り	session*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} mpa:RequestedOperation mpa:ProtectedResourceAccount	
ListApprovalTeams	承認チームを一覧表示する許可を付与	リスト			
ListIdentitySources	ID ソースを一覧表示するアクセス許可を付与します	リスト			
ListPolicies	ポリシーを一覧表示するアクセス許可を付与します	リスト			
ListPolicyVersions	ポリシーのバージョンを一覧表示するアクセス許可を付与します	リスト			
ListResourcePolicies	リソースのポリシーを一覧表示するアクセス許可を付与します	リスト			
ListSessions	承認セッションを一覧表示するアクセス許可を付与します	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutResourcePolicy [許可のみ]	リソースのポリシーを作成または更新するアクセス許可を付与します	権限の管理			
StartActiveApprovalTeamDeletion	アクティブな承認チームの削除プロセスを開始するアクセス許可を付与します	書き込み	approval-team*		
				aws:ResourceTag/${TagKey}	
StartSession [アクセス許可のみ]	承認セッションを開始するアクセス許可を付与します		session*		
				aws:ResourceTag/${TagKey} mpa:RequestedOperation mpa:ProtectedResourceAccount	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	リソースのタグを解除する許可を付与	Tagging		aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateApprovalTeam	承認チームを更新する許可を付与	書き込み	approval-team*		
				aws:ResourceTag/${TagKey}	

マルチパーティー承認で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
approval-team	arn:${Partition}:mpa:${Region}:${Account}:approval-team/${ApprovalTeamId}	aws:ResourceTag/${TagKey}
identity-source	arn:${Partition}:mpa:${Region}:${Account}:identity-source/${IdentitySourceId}	aws:ResourceTag/${TagKey}
session	arn:${Partition}:mpa:${Region}:${Account}:session/${SessionId}	aws:ResourceTag/${TagKey}

マルチパーティー承認の条件キー

マルチパーティー承認では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString
mpa:ProtectedResourceAccount	承認が必要なオペレーションのターゲットであるリソースを所有するアカウントでアクセスをフィルタリングします	String

条件キー	説明	タイプ
mpa:RequestedOperation	実行する前にチームの承認を必要とするリクエストされたオペレーションでアクセスをフィルタリングします	String

Amazon Neptune のアクション、リソース、および条件キー

Amazon Neptune (サービスプレフィックス: neptune-db) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Neptune で定義されるアクション
- Amazon Neptune で定義されるリソースタイプ
- Amazon Neptune の条件キー

Amazon Neptune で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelLoaderJob	ローダージョブをキャンセルする許可を付与	書き込み	database*		
CancelMLDataProcessingJob	ML データ処理ジョブをキャンセルする許可を付与	書き込み	database*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelMLModelTrainingJob	ML モデルトレーニングジョブをキャンセルする許可を付与	書き込み	database*		
CancelMLModelTransformJob	ML モデルの変換ジョブをキャンセルする許可を付与	書き込み	database*		
CancelQuery	クエリをキャンセルする許可を付与	書き込み	database*		
CreateMLEndpoint	ML エンドポイントを作成する許可を付与	書き込み	database*		
DeleteDataViaQuery	データベース上のクエリ API を介してデータ削除を実行する許可を付与	書き込み	database*		
				neptune-db:QueryLanguage	
DeleteMLEndpoint	ML エンドポイントを削除する許可を付与	書き込み	database*		
DeleteStatistics	データベースのすべての統計を削除する許可を付与	書き込み	database*		
GetEngineStatus	Neptune エンジンのステータスを確認する許可を付与	読み取り	database*		
GetGraphSummary	データベースからグラフの概要を取得するための許可を付与します	読み取り	database*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetLoaderJobStatus	ローダージョブのステータスを確認する許可を付与	読み取り	database*		
GetMLDataProcessingJobStatus	ML データ処理ジョブのステータスを確認する許可を付与	読み取り	database*		
GetMLEndpointStatus	ML エンドポイントのステータスを確認する許可を付与	読み取り	database*		
GetMLModelTrainingJobStatus	ML モデルトレーニングジョブのステータスを確認する許可を付与	読み取り	database*		
GetMLModelTransformJobStatus	ML モデル変換ジョブのステータスを確認する許可を付与	読み取り	database*		
GetQueryStatus	すべてのアクティブなクエリのステータスを確認する許可を付与	読み取り	database*		
				neptune-db:QueryLanguage	
GetStatisticsStatus	データベースの統計のステータスを確認する許可を付与	読み取り	database*		
GetStreamRecords	Neptune からストリームレコードを取得する許可を付与	読み取り	database*		
				neptune-db:QueryLanguage	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListLoaderJobs	すべてのローダージョブを一覧表示する許可を付与	リスト	database*		
ListMLDataProcessingJobs	すべての ML データ処理ジョブを一覧表示する許可を付与	リスト	database*		
ListMLEndpoints	すべての ML エンドポイントを一覧表示する許可を付与	リスト	database*		
ListMLModelTrainingJobs	すべての ML モデルトレーニングジョブを一覧表示する許可を付与	リスト	database*		
ListMLModelTransformJobs	すべての ML モデル変換ジョブを一覧表示する許可を付与	リスト	database*		
ManageStatistics	データベース内の統計を管理する許可を付与	書き込み	database*		
ReadDataViaQuery	データベース上のクエリ API を介してデータの読み取りを実行する許可を付与	読み取り	database*		
				neptune-db:QueryLanguage	
ResetDatabase	リセットに必要なトークンを取得する許可を付与し、Neptune データベースをリセットします	書き込み	database*		
StartLoaderJob	ローダージョブを開始する許可を付与	書き込み	database*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartMLDataProcessingJob	ML データ処理ジョブを開始する許可を付与	書き込み	database*		
StartMLModelTrainingJob	ML モデルトレーニングジョブを開始する許可を付与	書き込み	database*		
StartMLModelTransformJob	ML モデルの変換を開始する許可を付与	書き込み	database*		
WriteDataViaQuery	データベース上のクエリ API を介してデータの書き込みを実行する許可を付与	書き込み	database*		
				neptune-db:QueryLanguage	
connect	1.2.0.0 より前のエンジンバージョンのすべてのデータアクセスアクションに対してアクセス許可を付与	書き込み	database*		

Amazon Neptune で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
database	arn:${Partition}:neptune-db:${Region}:${Account}:${ClusterResourceId}/*	

Amazon Neptune の条件キー

Amazon Neptune は、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
neptune-db:QueryLanguage	グラフモデルでアクセスをフィルタリング	String

Amazon Neptune Analytics のアクション、リソース、および条件キー

Amazon Neptune Analytics (サービスプレフィックス: neptune-graph) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Neptune Analytics で定義されるアクション
- Amazon Neptune Analytics で定義されるリソースタイプ
- Amazon Neptune Analytics の条件キー

Amazon Neptune Analytics で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

Note

「ReadDataViaQuery」、「WriteDataViaQuery」、「DeleteDataViaQuery」を除くすべての IAM アクションには、対応する API オペレーションがあります

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelExportTask	進行中のエクスポートタスクをキャンセルするアクセス許可を付与します	書き込み	export-task*		
				aws:ResourceTag/${TagKey}	
CancelImportTask	進行中のインポートタスクをキャンセルするためのアクセス許可を付与	書き込み	import-task*		
CancelQuery	クエリをキャンセルする許可を付与	書き込み	graph*		
				aws:ResourceTag/${TagKey}	
CreateGraph	新しいグラフを作成するためのアクセス許可を付与	書き込み	graph*		iam:CreateServiceLinkedRole kms:CreateGrant

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					kms:Decrypt kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys neptune-graph:PublicConnectivity	
CreateGraphSnapshot	既存のグラフから新しいスナップショットを作成するためのアクセス許可を付与	書き込み	graph* graph-snapshot*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateGraphUsingImportTask	新しいグラフへのデータをインポートしながら新しいグラフを作成するアクセス許可を付与	書き込み	graph*		iam:CreateServiceLinkedRole iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey
			import-task*		
				aws:RequestTag/${TagKey} aws:TagKeys neptune-graph:PublicConnectivity	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreatePrivateGraphEndpoint	VPC 内からグラフにアクセスするための新しいプライベートグラフエンドポイントを作成するためのアクセス許可を付与	書き込み	graph*		ec2:CreateVpcEndpoint ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint route53:AssociateV

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					PCWithHostedZone
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteDataViaQuery	グラフ上のクエリ API を介してデータを削除するためのアクセス許可を付与	書き込み	graph*		
				aws:ResourceTag/${TagKey}	
DeleteGraph	グラフを削除するためのアクセス許可を付与	書き込み	graph*		
				aws:ResourceTag/${TagKey}	
DeleteGraphSnapshot	スナップショットを削除するためのアクセス許可を付与	書き込み	graph-snapshot*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeletePrivateGraphEndpoint	グラフのプライベートグラフエンドポイントを削除するためのアクセス許可を付与	書き込み	graph*		ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint route53:DisassociateVPCFrom

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					HostedZone
				aws:ResourceTag/${TagKey}	
GetEngineStatus	グラフのエンジンステータスを取得するためのアクセス許可を付与	読み取り	graph*		
				aws:ResourceTag/${TagKey}	
GetExportTask	エクスポートタスクの詳細を取得するアクセス許可を付与します	読み取り	export-task*		
				aws:ResourceTag/${TagKey}	
GetGraph	グラフに関する詳細を取得するためのアクセス許可を付与	読み取り	graph*		
				aws:ResourceTag/${TagKey}	
GetGraphSnapshot	スナップショットに関する詳細を取得するためのアクセス許可を付与	読み取り	graph-snapshot*		
				aws:ResourceTag/${TagKey}	
GetGraphSummary		読み取り	graph*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	グラフ内のデータの概要を取得するためのアクセス許可を付与			aws:ResourceTag/${TagKey}	
GetImportTask	インポートタスクに関する詳細を取得するためのアクセス許可を付与	読み取り	import-task*		
GetPrivateGraphEndpoint	グラフのプライベートグラフエンドポイントに関する詳細を取得するためのアクセス許可を付与	読み取り	graph*		
				aws:ResourceTag/${TagKey}	
GetQueryStatus	特定のクエリのステータスを確認するためのアクセス許可を付与	読み取り	graph*		
				aws:ResourceTag/${TagKey}	
GetStatisticsStatus	グラフ内のデータの統計を取得するためのアクセス許可を付与	読み取り	graph*		
				aws:ResourceTag/${TagKey}	
ListExportTasks	アカウントのエクスポートタスクを一覧表示するアクセス許可を付与します	読み取り	export-task*		
ListGraphSnapshots	アカウント内のスナップショットを一覧表示するためのアクセス許可を付与	読み取り	graph-snapshot*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListGraphs	アカウント内のグラフを一覧表示するためのアクセス許可を付与	読み取り	graph*		
ListImportTasks	アカウント内のインポートタスクを一覧表示するためのアクセス許可を付与	読み取り	import-task*		
ListPrivateGraphEndpoints	特定のグラフのプライベートグラフエンドポイントを一覧表示するためのアクセス許可を付与	読み取り	graph*		
				aws:ResourceTag/${TagKey}	
ListQueries	すべてのアクティブなクエリのステータスを確認する許可を付与	読み取り	graph*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	Neptune Analytics リソースのタグを一覧表示するためのアクセス許可を付与	読み取り	graph		
			graph-snapshot		
				aws:ResourceTag/${TagKey}	
ReadDataViaQuery	グラフ上のクエリ API を介してデータを読み込むためのアクセス許可を付与	読み取り	graph*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ResetGraph	グラフ内のすべてのデータを削除してグラフをリセットするためのアクセス許可を付与	書き込み	graph*		
				aws:ResourceTag/${TagKey}	
RestoreGraphFromSnapshot	既存のスナップショットから新しいグラフを作成するためのアクセス許可を付与	書き込み	graph*		kms:CreateGrant kms:Decrypt kms:DescribeKey
			graph-snapshot*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys neptune-graph:PublicConnectivity	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartExportTask	既存のグラフからデータをエクスポートする許可を付与	書き込み	export-task*		iam:PassRole
			graph*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
StartImportTask	既存のグラフにデータをインポートする許可を付与する	書き込み	graph*		iam:PassRole
			import-task*		
TagResource	Neptune Analytics リソースにタグを付けるためのアクセス許可を付与	Tagging	graph		
			graph-snapshot		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource		Tagging	graph		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	Neptune Analytics リソースのタグを解除するためのアクセス許可を付与		graph-snapshot		
				aws:TagKeys	
UpdateGraph	グラフを変更するためのアクセス許可を付与	書き込み	graph*		
				aws:ResourceTag/${TagKey} neptune-graph:PublicConnectivity	
WriteDataViaQuery	グラフ上のクエリ API を介してデータを書き込むためのアクセス許可を付与	書き込み	graph*		
				aws:ResourceTag/${TagKey}	

Amazon Neptune Analytics で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
graph	arn:${Partition}:neptune-graph:${Region}:${Account}:graph/${ResourceId}	aws:ResourceTag/${TagKey}
graph-snapshot	arn:${Partition}:neptune-graph:${Region}:${Account}:graph-snapshot/${ResourceId}	aws:ResourceTag/${TagKey}
import-task	arn:${Partition}:neptune-graph:${Region}:${Account}:import-task/${ResourceId}	
export-task	arn:${Partition}:neptune-graph:${Region}:${Account}:export-task/${ResourceId}	

Amazon Neptune Analytics の条件キー

Amazon Neptune Analytics は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグのキーと値でアクセスをフィルター	String
aws:ResourceTag/${TagKey}	リクエスト内のタグキーおよび値のペアのプレゼンスによってアクションをフィルタリングします	String

条件キー	説明	タイプ
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString
neptune-graph:PublicConnectivity	リクエストで指定されたパブリック接続パラメータの値、または指定されていない場合はデフォルト値によってアクセスをフィルタリングします。グラフへのすべてのアクセスは IAM 認証されています	Bool

AWS Network Firewall のアクション、リソース、および条件キー

AWS Network Firewall (サービスプレフィックス: `network-firewall`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Network Firewall で定義されるアクション
- AWS Network Firewall で定義されるリソースタイプ
- AWS Network Firewall の条件キー

AWS Network Firewall で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptNetworkFirewallTransi	トランジットゲートウェイで保留中の Network Firewall ア	書き込み	Firewall*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
tGatewayAttachment	タッチメントを受け入れるアクセス許可を付与します				
AssociateAvailabilityZones	アベイラビリティーゾーンをファイアウォールに関連付けるアクセス許可を付与します	書き込み	Firewall*		
AssociateFirewallPolicy	ファイアウォールポリシーとファイアウォール間の関連付けを作成する許可を付与	書き込み	Firewall*		
			FirewallPolicy*		
AssociateSubnets	VPC サブネットをファイアウォールに関連付けるアクセス許可を付与します	書き込み	Firewall*		
CreateFirewall	AWS Network Firewall ファイアウォールを作成するアクセス許可を付与します	書き込み	Firewall*		iam:CreateServiceLinkedRole
			FirewallPolicy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallPolicy	AWS Network Firewall ファイアウォールポリシーを作成するアクセス許可を付与します	書き込み	FirewallPolicy*		
			StatefulRuleGroup		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			StatelessRuleGroup		
			TLSInspectionConfiguration		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	AWS Network Firewall ルールグループを作成するアクセス許可を付与します	書き込み	StatefulRuleGroup		
			StatelessRuleGroup		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTLSInspectionConfiguration	AWS Network Firewall tls 検査設定を作成するアクセス許可を付与します	書き込み	TLSInspectionConfiguration*		iam:CreateServiceLinkedRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVpcEndpointAssociation	AWS Network Firewall vpc エンドポイントの関連付けを作成するアクセス許可を付与します	書き込み	Firewall*		iam:CreateServiceLinkedRole
			VpcEndpointAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFirewall	ファイアウォールを削除する許可を付与	書き込み	Firewall*		
DeleteFirewallPolicy	ファイアウォールポリシーを削除する許可を付与	書き込み	FirewallPolicy*		
DeleteNetworkFirewallTransitGatewayAttachment	トランジットゲートウェイの Network Firewall アタッチメントを削除するアクセス許可を付与します	書き込み	Firewall*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteResourcePolicy	ファイアウォールポリシー、ルールグループ、またはファイアウォールのリソースポリシーを削除するアクセス許可を付与します	書き込み	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
DeleteRuleGroup	ルールグループを削除する許可を付与	書き込み	StatefulRuleGroup*		
			StatelessRuleGroup*		
DeleteTLSInspectionConfiguration	TLS の検査設定を削除するアクセス許可を付与	書き込み	TLSInspectionConfiguration*		
DeleteVpcEndpointAssociation	vpc エンドポイントの関連付けを削除するアクセス許可を付与します	書き込み	VpcEndpointAssociation*		
DescribeFirewall	ファイアウォールを定義するデータオブジェクトを取得する許可を付与	読み取り	Firewall*		
DescribeFirewallMetadata	ファイアウォールに関する大まかな情報を取得するアクセス許可を付与します	読み取り	Firewall*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeFirewallPolicy	ファイアウォールポリシーを定義するデータオブジェクトを取得する許可を付与	読み取り	FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
DescribeFlowOperation	ファイアウォールで実行されるフローオペレーションを記述するアクセス許可を付与します	読み取り	Firewall*		
DescribeLoggingConfiguration	ファイアウォールのログ設定を記述する許可を付与	読み取り	Firewall*		logs:GetLogDelivery logs:ListLogDeliveries
DescribeResourcePolicy	ファイアウォールポリシー、ルールグループ、またはファイアウォールのリソースポリシーを記述するアクセス許可を付与します	読み取り	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			StatelessRuleGroup		
DescribeRuleGroup	ルールグループを定義するデータオブジェクトを取得する許可を付与	読み込み	StatefulRuleGroup		
			StatelessRuleGroup		
DescribeRuleGroupMetadata	ルールグループの概要を取得する許可を付与	読み取り	StatefulRuleGroup		
			StatelessRuleGroup		
DescribeRuleGroupSummary	ルールグループに関する概要情報を取得するアクセス許可を付与します	読み取り	StatefulRuleGroup		
			StatelessRuleGroup		
DescribeTLSInspectionConfiguration	TLS の検査設定を定義しているデータオブジェクトを取得する許可を付与	読み取り	TLSInspectionConfiguration*		
DescribeVpcEndpointAssociation	vpc エンドポイントの関連付けを定義するデータオブジェクトを取得する許可を付与	読み取り	VpcEndpointAssociation*		
DisassociateAvailabilityZones	アベイラビリティーゾーンとファイアウォールの関連付けを解除するアクセス許可を付与します	書き込み	Firewall*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisassociateSubnets	ファイアウォールから VPC サブネットの関連付けを解除する許可を付与	書き込み	Firewall*		
GetAnalysisReportResults	ファイアウォールの分析レポート結果を取得するアクセス許可を付与します	読み取り	Firewall*		
ListAnalysisReports	ファイアウォール分析レポートを一覧表示する許可を付与	リスト	Firewall*		
ListFirewallPolicies	ファイアウォールポリシー用のメタデータを取得する許可を付与	リスト	FirewallPolicy*		
ListFirewalls	ファイアウォール用のメタデータを取得する許可を付与	リスト	Firewall*		
ListFlowOperationResults	ファイアウォールで実行されたフローオペレーションの結果を一覧表示するアクセス許可を付与します	読み取り	Firewall*		
ListFlowOperations	ファイアウォールで実行されたフローオペレーションを一覧表示するアクセス許可を付与します	リスト	Firewall*		
ListRuleGroups	ルールグループ用のメタデータを取得する許可を付与	リスト			
ListTLSInspectionConfigurations	TLS の検査設定に関するメタデータを取得する許可を付与	リスト	TLSInspectionConfiguration*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTagsForResource	リソースのタグを取得する許可を付与	リスト	Firewall*		
			FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
			VpcEndpointAssociation		
ListVpcEndpointAssociations	vpc エンドポイントの関連付けのメタデータを取得する許可を付与	リスト	VpcEndpointAssociation*		
PutResourcePolicy	ファイアウォールポリシー、ルールグループ、またはファイアウォールのリソースポリシーを配置するアクセス許可を付与します	書き込み	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RejectNetworkFirewallTransitGatewayAttachment	トランジットゲートウェイで保留中の Network Firewall アタッチメントを拒否するアクセス許可を付与します	書き込み	Firewall*		
StartAnalysisReport	ファイアウォールで分析レポートを開始する許可を付与	書き込み	Firewall*		
StartFlowCapture	ファイアウォールでキャプチャオペレーションを開始するアクセス許可を付与します	書き込み	Firewall*		
StartFlowFlush	ファイアウォールでフラッシュオペレーションを開始する許可を付与	書き込み	Firewall*		
TagResource	リソースにタグを追加する許可を付与	タグ付け	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
			VpcEndpointAssociation		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	Tagging	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
			VpcEndpointAssociation		
				aws:TagKeys	
UpdateAvailabilityZoneChangeProtection	ファイアウォールのアベイラビリティーゾーン変更保護を追加または削除するためのアクセス許可を付与します	書き込み	Firewall*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateFirewallAnalysisSettings	ファイアウォールのファイアウォール分析設定を変更するアクセス許可を付与します	書き込み	Firewall*		
UpdateFirewallDeleteProtection	ファイアウォールの削除保護を追加または削除する許可を付与	書き込み	Firewall*		
UpdateFirewallDescription	ファイアウォールの説明を変更する許可を付与	書き込み	Firewall*		
UpdateFirewallEncryptionConfiguration	ファイアウォールの暗号化設定を修正する許可の付与	書き込み	Firewall*		
UpdateFirewallPolicy	ファイアウォールポリシーを変更する許可を付与	書き込み	FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
UpdateFirewallPolicyChangeProtection	ファイアウォールのファイアウォールポリシー変更保護を追加または削除する許可を付与	書き込み	Firewall*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateLoggingConfiguration	ファイアウォールのログ設定を変更する許可を付与	書き込み	Firewall*		
UpdateRuleGroup	ルールグループを変更する許可を付与	書き込み	StatefulRuleGroup		
			StatelessRuleGroup		
UpdateSubnetChangeProtection	ファイアウォールのサブネット変更保護を追加または削除する許可を付与	書き込み	Firewall*		
UpdateTLSInspectionConfiguration	TLS の検査設定を変更する許可を付与	書き込み	TLSInspectionConfiguration*		

AWS Network Firewall で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Firewall	`arn:${Partition}:network-firewall:${Region}:${Account}:firewall/${Name}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
FirewallPolicy	arn:${Partition}:network-firewall:${Region}:${Account}:firewall-policy/${Name}	aws:ResourceTag/${TagKey}
StatefulRuleGroup	arn:${Partition}:network-firewall:${Region}:${Account}:stateful-rulegroup/${Name}	aws:ResourceTag/${TagKey}
StatelessRuleGroup	arn:${Partition}:network-firewall:${Region}:${Account}:stateless-rulegroup/${Name}	aws:ResourceTag/${TagKey}
TLSInspectionConfiguration	arn:${Partition}:network-firewall:${Region}:${Account}:tls-configuration/${Name}	aws:ResourceTag/${TagKey}
VpcEndpointAssociation	arn:${Partition}:network-firewall:${Region}:${Account}:vpc-endpoint-association/${Name}	aws:ResourceTag/${TagKey}

AWS Network Firewall の条件キー

AWS Network Firewall では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	各タグの許可された値のセットでアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値に基づいて、アクセスをフィルタリングする	String
aws:TagKeys	リクエスト内の必須タグの存在でアクセスをフィルタリングします	ArrayOfString

Network Flow Monitor のアクション、リソース、および条件キー

Network Flow Monitor (サービスプレフィックス: `networkflowmonitor`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Network Flow Monitor で定義されるアクション
- Network Flow Monitor で定義されるリソースタイプ
- Network Flow Monitor の条件キー

Network Flow Monitor で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateMonitor	モニターを作成するための許可を付与します	書き込み	monitor*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScope	スコープを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMonitor	モニターを削除するための許可を付与します	書き込み	monitor*		
DeleteScope	スコープを削除するアクセス許可を付与します	書き込み	scope*		
GetMonitor	モニターに関する情報を取得するための許可を付与します	読み取り	monitor*		
GetQueryResultsMonitorTopContributors	モニターの上位寄与要因データを取得するクエリの結果を取得するアクセス許可を付与します	読み取り	monitor*		
GetQueryResultsWorkloadInsightsTopContributors	ワークロードインサイトの上位寄与要因を取得するクエリの結果を取得するアクセス許可を付与します	読み取り	scope*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetQueryResultsWorkloadInsightsTopContributorsData	ワークロードインサイトの上位寄与要因データポイントを取得するクエリの結果を取得するアクセス許可を付与します	読み取り	scope*		
GetQueryStatusMonitorTopContributors	モニターの上位寄与要因データを取得するクエリのステータスを取得するアクセス許可を付与します	読み取り	monitor*		
GetQueryStatusWorkloadInsightsTopContributors	ワークロードインサイトの上位寄与要因を取得するクエリのステータスを取得するアクセス許可を付与します	読み取り	scope*		
GetQueryStatusWorkloadInsightsTopContributorsData	ワークロードインサイトの上位寄与要因データポイントを取得するクエリのステータスを取得するアクセス許可を付与します	読み取り	scope*		
GetScope	スコープに関する情報を取得するアクセス許可を付与します	読み取り	scope*		
ListMonitors	アカウント内のすべてのモニターとそのステータスを一覧表示するための許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListScopes	アカウントのすべてのスコープを取得するアクセス許可を付与します	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	monitor		
			scope		
Publish	レポートを公開するアクセス許可を付与します	書き込み			
StartQueryMonitorTopContributors	モニターの上位寄与要因データを取得するためのクエリを開始するアクセス許可を付与します	書き込み	monitor*		
StartQueryWorkloadInsightsTopContributors	ワークロードインサイトの上位寄与要因データを取得するためのクエリを開始するアクセス許可を付与します	書き込み	scope*		
StartQueryWorkloadInsightsTopContributorsData	ワークロードインサイトの上位寄与要因データポイントを取得するためのクエリを開始するアクセス許可を付与します	書き込み	scope*		
StopQueryMonitorTopContributors	モニターの上位寄与要因データを取得するためのクエリを停止するアクセス許可を付与します	書き込み	monitor*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StopQueryWorkloadInsightsTopContributors	ワークロードインサイトの上位寄与要因を取得するためのクエリを停止するアクセス許可を付与します	書き込み	scope*		
StopQueryWorkloadInsightsTopContributorsData	ワークロードインサイトの上位寄与要因データポイントを取得するためのクエリを停止するアクセス許可を付与します	書き込み	scope*		
TagResource	リソースにタグを追加するアクセス許可を付与します	タグ付け	monitor		
			scope		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	Tagging	monitor		
			scope		
				aws:TagKeys	
UpdateMonitor	モニターを更新するための許可を付与します	書き込み	monitor*		
UpdateScope	スコープを更新するアクセス許可を付与します	書き込み	scope*		

Network Flow Monitor で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
monitor	arn:${Partition}:networkflowmonitor:${Region}:${Account}:monitor/${MonitorName}	aws:ResourceTag/${TagKey}
scope	arn:${Partition}:networkflowmonitor:${Region}:${Account}:scope/${ScopeId}	aws:ResourceTag/${TagKey}

Network Flow Monitor の条件キー

Network Flow Monitor は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアによるアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアでアクセスをフィルタリングします	String

条件キー	説明	タイプ
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Network Manager のアクション、リソース、条件キー

AWS Network Manager (サービスプレフィックス: networkmanager) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Network Manager が定義するアクション
- AWS Network Manager が定義するリソースタイプ
- AWS Network Manager の条件キー

AWS Network Manager が定義するアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptAttachment	コアネットワーク内の送信元と宛先間の添付ファイルの作成を許可する権限を付与します。	書き込み	attachment*		ec2:DescribeRegions
AssociateConnectPeer	Connect ピアを関連付けるアクセス許可を付与します。	書き込み	device*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			global-network*		
AssociateCustomerGateway	カスタマーゲートウェイをデバイスに関連付けるアクセス許可を付与します。	書き込み	device*		
			global-network*		
			link		
				networkmanager:cgwArn	
AssociateLink	リンクをデバイスに関連付けるアクセス許可を付与します。	書き込み	device*		
			global-network*		
			link*		
AssociateTransitGatewayConnectPeer	Transit Gateway 接続ピアをデバイスに関連付けるアクセス許可を付与します	書き込み	device*		
			global-network*		
			link		
				networkmanager:tgwConnectPeerArn	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateConnectAttachment	接続アタッチメントを作成する許可を付与します。	書き込み	attachment*		ec2:DescribeRegions networkmanager:TagResource
			core-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectPeer	Connect Peer connectionを作成する許可を付与します。	書き込み	attachment*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateConnection	新しい接続を作成する許可を付与	書き込み	global-network*		networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCoreNetwork	新しいコアネットワークを作成する許可を付与します。	書き込み	global-network*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDevice	新しいデバイスを作成する許可を付与	書き込み	global-network*		networkmanager:TagResource

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDirectConnectGatewayAttachment	Direct Connect ゲートウェイアタッチメントを作成するアクセス許可を付与します	書き込み	core-network*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:directConnectGatewayArn networkmanager:edgeLocations	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateGlobalNetwork	新しいグローバルネットワークを作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole networkmanager:TagResource
CreateLink	新しいリンクを作成する許可を付与	書き込み	global-network*		networkmanager:TagResource
			site		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSite	新しいサイトを作成する許可を付与	書き込み	global-network*		networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSiteToSiteVpnAttachment	Site-to-Site VPN アタッチメントを作成するアクセス許可を付与します	書き込み	core-network*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:vpnConnectionArn	
CreateTransitGatewayPeering	トランジット ゲートウェイ ピアリングを作成する許可の付与	書き込み	core-network*		ec2:DescribeRegions networkmanager:TagResource

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:tgwArn	
CreateTransitGatewayRouteTableAttachment	TGW RTB アタッチメントを作成する許可の付与	書き込み	peering*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:tgwRtbArn	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateVpcAttachment	VPC アタッチメントを作成する許可を付与します。	書き込み	core-network*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:vpcArn networkmanager:subnetArns	
DeleteAttachment	アタッチメントを削除するアクセス許可を付与します。	書き込み	attachment*		ec2:DescribeRegions
DeleteConnectPeer	Connect Peerを削除する許可を付与します。	書き込み	connect-peer*		ec2:DescribeRegions
DeleteConnection	接続を削除する許可を付与。	書き込み	connection*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			global-network*		
DeleteCoreNetwork	コアネットワーク を削除する許可を付与します。	書き込み	core-network*		ec2:DescribeRegions
DeleteCoreNetworkPolicyVersion	コアネットワークポリシーバージョンを削除するアクセス許可を付与します。	書き込み	core-network*		
DeleteDevice	デバイスを削除する許可を付与	書き込み	device*		
			global-network*		
DeleteGlobalNetwork	グローバルネットワークを削除する許可を付与。	書き込み	global-network*		
DeleteLink	リンクを削除する許可を付与	書き込み	global-network*		
			link*		
DeletePeering	ピアリングを削除する許可の付与	書き込み	peering*		ec2:DescribeRegions
DeleteResourcePolicy	リソースを削除するためのアクセス許可を付与します。	書き込み	core-network*		
DeleteSite	サイトを削除する許可を付与	書き込み	global-network*		
			site*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeregisterTransitGateway	グローバルネットワークから転送ゲートウェイを登録解除する許可を付与。	書き込み	global-network*		
				networkmanager:tgwArn	
DescribeGlobalNetworks	グローバルネットワークを記述する許可を付与。	リスト	global-network		
DisassociateConnectPeer	Connect ピアの関連付けを解除するアクセス許可を付与します。	書き込み	global-network*		
DisassociateCustomerGateway	カスタマーゲートウェイとデバイスの関連付けを解除する許可を付与。	書き込み	global-network*		
				networkmanager:cgwArn	
DisassociateLink	リンクとデバイスの関連付けを解除する許可を付与。	書き込み	device*		
			global-network*		
			link*		
DisassociateTransitGatewayConnectPeer	トランジットゲートウェイ接続ピアをデバイスから解除する許可を付与します	書き込み	global-network*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				networkmanager:tgwConnectPeerArn	
ExecuteCoreNetworkChangeSet	コアネットワークに変更を適用するアクセス許可を付与します。	書き込み	core-network*		ec2:DescribeRegions
GetConnectAttachment	コネクトアタッチメントを取得する許可を付与します。	読み込み	attachment*		
GetConnectPeer	Connectピアを取得する許可を付与します。	読み込み	connect-peer*		
GetConnectPeerAssociations	Connectピアアソシエーションを記述する許可を付与します。	読み込み	global-network*		
GetConnections	接続を記述する許可を付与	リスト	global-network*		
			connection		
GetCoreNetwork	コアネットワークを取得するアクセス許可を付与します。	読み取り	core-network*		
GetCoreNetworkChangeEvents	コアネットワーク変更セットのリストを取得する許可の付与	読み取り	core-network*		
GetCoreNetworkChangeSet	コアネットワーク変更セットのリストを取得するアクセス許可を付与します。	読み込み	core-network*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetCoreNetworkPolicy	コアネットワークポリシーを取得するアクセス許可を付与します。	読み込み	core-network*		
GetCustomerGatewayAssociations	カスタマーゲートウェイの関連付けを記述する許可を付与。	リスト	global-network*		
GetDevices	デバイスを記述する許可を付与。	リスト	global-network*		
			device		
GetDirectConnectGatewayAttachment	Direct Connect ゲートウェイアタッチメントを取得する許可を付与	読み取り	attachment*		
GetLinkAssociations	リンクの関連付けを記述する許可を付与。	リスト	global-network*		
			device		
			link		
GetLinks	リンクを記述する許可を付与。	リスト	global-network*		
			link		
GetNetworkResourceCounts	タイプ別にグループ化されたグローバルネットワークのリソースの数を返すアクセス許可を付与します。	読み込み	global-network*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetNetworkResourceRelationships	グローバルネットワーク内のリソースの関連リソースを取得する権限を付与します。	読み込み	global-network*		
GetNetworkResources	グローバルネットワークリソースを取得するアクセス許可を付与します。	読み込み	global-network*		
GetNetworkRoutes	グローバルネットワーク内のルート表のルートを取得する権限を付与します。	読み込み	global-network*		
GetNetworkTelemetry	グローバルネットワークのネットワークテレメトリオブジェクトを取得する権限を付与します。	読み込み	global-network*		
GetResourcePolicy	リソースポリシーを取得する許可を付与。	読み込み	core-network*		
GetRouteAnalysis	ルート解析設定および結果を取得するアクセス許可を付与します。	読み込み	global-network*		
GetSiteToSiteVpnAttachment	Site-to-Site VPN アタッチメントを取得するアクセス許可を付与します。	読み込み	attachment*		
GetSites	グローバルネットワークを記述する許可を付与。	リスト	global-network*		
			site		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetTransitGatewayConnectPeerAssociations	トランジットゲートウェイ接続ピアアソシエーションを記述する許可を付与	リスト	global-network*		
GetTransitGatewayPeering	トランジット ゲートウェイ ピアリングを取得する許可の付与	読み取り	peering*		
GetTransitGatewayRegistrations	転送ゲートウェイの登録を記述する許可を付与。	リスト	global-network*		
GetTransitGatewayRouteTableAttachment	TGW RTB アタッチメントを取得する許可の付与	読み取り	attachment*		
GetVpcAttachment	VPC アタッチメントを取得するアクセス許可を付与します。	読み込み	attachment*		
ListAttachments	アタッチメントを記述するアクセス許可を付与します。	リスト	attachment*		
ListConnectPeers	Connetピアを記述する許可を付与します。	リスト	connect-peer*		
ListCoreNetworkPolicyVersions	コアネットワークポリシーのバージョンを一覧表示するアクセス許可を付与します。	リスト	core-network*		
ListCoreNetworks	コアネットワークを一覧表示するアクセス許可を付与します。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListOrganizationServiceAccessStatus	組織サービスのアクセスステータスを一覧表示するアクセス許可を付与します	リスト			
ListPeerings	ピアリングを記述する許可の付与	リスト			
ListTagsForResource	Network Manager リソースのリストタグにアクセス許可を付与します。	読み込み	attachment		
			connect-peer		
			connection		
			core-network		
			device		
			global-network		
			link		
			peering		
			site		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutCoreNetworkPolicy	コアネットワークポリシーを作成する許可を付与します。	書き込み	core-network*		ec2:DescribeRegions
PutResourcePolicy	リソースポリシーを作成または更新する許可を付与します。	書き込み	core-network*		
RegisterTransitGateway	グローバルネットワークに転送ゲートウェイを登録する許可を付与します	書き込み	global-network*		
				networkmanager:tgwArn	
RejectAttachment	アタッチメントリクエストを拒否する権限を付与します。	書き込み	attachment*		
RestoreCoreNetworkPolicyVersion	コアネットワークポリシーを以前のバージョンに復元する権限を付与します。	書き込み	core-network*		ec2:DescribeRegions
StartOrganizationServiceAccessUpdate	組織サービスアクセス更新を開始するアクセス許可を付与します	書き込み			
StartRouteAnalysis	ルート解析を開始し、解析構成を保存する権限を付与します。	書き込み	global-network*		
TagResource	Network Manager リソースにタグを付けるアクセス許可を付与します。	タグ付け	attachment		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			connect-peer		
			connection		
			core-network		
			device		
			global-network		
			link		
			peering		
			site		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Network Manager リソースのタグを解除する許可を付与。	タグ付け	attachment		
			connect-peer		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			connection		
			core-network		
			device		
			global-network		
			link		
			peering		
			site		
				aws:TagKeys	
UpdateConnection	接続を更新する許可を付与。	書き込み	connection*		
			global-network*		
UpdateCoreNetwork	コアネットワークを更新する許可を付与します。	書き込み	core-network*		
UpdateDevice	デバイスを更新する許可を付与	書き込み	device*		
			global-network*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateDirectConnectGatewayAttachment	Direct Connect ゲートウェイアタッチメントを更新する許可を付与	書き込み	attachment*		ec2:DescribeRegions
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:edgeLocations	
UpdateGlobalNetwork	グローバルネットワークを更新する許可を付与。	書き込み	global-network*		
UpdateLink	リンクを更新する許可を付与	書き込み	global-network*		
			link*		
UpdateNetworkResourceMetadata	ネットワークリソースでメタデータのキーおよび値のペアを追加または更新するアクセス許可を付与します。	書き込み	global-network*		
UpdateSite	サイトを更新する許可を付与	書き込み	global-network*		
			site*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateVpcAttachment	VPCアタッチメントを更新する権限を付与します。	書き込み	attachment*		ec2:DescribeRegions
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:subnetArns	

AWS Network Manager が定義するリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
global-network	`arn:${Partition}:networkmanager::${Account}:global-network/${ResourceId}`	aws:ResourceTag/${TagKey}
site	`arn:${Partition}:networkmanager::${Account}:site/${GlobalNetworkId}/${ResourceId}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
link	arn:${Partition}:networkmanager::${Account}:link/${GlobalNetworkId}/${ResourceId}	aws:ResourceTag/${TagKey}
device	arn:${Partition}:networkmanager::${Account}:device/${GlobalNetworkId}/${ResourceId}	aws:ResourceTag/${TagKey}
connection	arn:${Partition}:networkmanager::${Account}:connection/${GlobalNetworkId}/${ResourceId}	aws:ResourceTag/${TagKey}
core-network	arn:${Partition}:networkmanager::${Account}:core-network/${ResourceId}	aws:ResourceTag/${TagKey}
attachment	arn:${Partition}:networkmanager::${Account}:attachment/${ResourceId}	aws:ResourceTag/${TagKey}
connect-peer	arn:${Partition}:networkmanager::${Account}:connect-peer/${ResourceId}	aws:ResourceTag/${TagKey}
peering	arn:${Partition}:networkmanager::${Account}:peering/${ResourceId}	aws:ResourceTag/${TagKey}

AWS Network Manager の条件キー

AWS Network Manager は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
networkmanager:cgwArn	関連付けまたは関連付け解除できるカスタマーゲートウェイによってアクセスをフィルタリングします。	ARN
networkmanager:directConnectGatewayArn	Direct Connect ゲートウェイを添付ファイルの作成/更新に使用できるアクセスをフィルタリングします	ARN
networkmanager:edgeLocations	Direct Connect ゲートウェイアタッチメントからエッジロケーションを追加または削除できるアクセスをフィルタリングします	ArrayOfString
networkmanager:subnetArns	VPC サブネットを VPC アタッチメントに追加または削除できるアクセスをフィルタリングします。	ArrayOfARN
networkmanager:tgwArn	トランジットゲートウェイが登録、登録解除、ピアリングされる対象のアクセスのフィルタリング	ARN
networkmanager:tgwConnectPeerArn	トランジットゲートウェイ接続ピアを関連付けまたは関連付け解除できるアクセスをフィルタリングします	ARN
networkmanager:tgwRtbArn	トランジット ゲートウェイ ルート テーブルを使用してアタッチメントを作成する対象のアクセスのフィルタリング	ARN

条件キー	説明	タイプ
networkmanager:vpcArn	アタッチメントの作成/更新に VPC を使用できるアクセスをフィルタリングします。	ARN
networkmanager:vpnConnectionArn	添付ファイルの作成/更新にSite-to-Site VPN を使用できるアクセスをフィルタリングします。	ARN

AWS Network Manager Chat のアクション、リソース、条件キー

AWS Network Manager Chat (サービスプレフィックス: `networkmanager-chat`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Network Manager Chat が定義するアクション
- AWS Network Manager Chat が定義するリソースタイプ
- AWS Network Manager Chat を指定 の条件キー

AWS Network Manager Chat が定義するアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelMessageRespo	メッセージへの応答をキャンセルする許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
nse [アクセス許可のみ]					
CreateConversation [アクセス許可のみ]	会話を作成する許可を付与	書き込み			
DeleteConversation [アクセス許可のみ]	会話を削除するためのアクセス許可を付与	書き込み			
ListConversationMessages [アクセス許可のみ]	会話メッセージを一覧表示する許可を付与	リスト			
ListConversations [許可のみ]	会話を一覧表示する許可を付与	リスト			
NotifyConversationIsActive [許可のみ]	会話にアクティビティがあるかどうかを通知する許可を付与	書き込み			
SendConversationMessage [アクセス許可のみ]	会話メッセージを送信する許可を付与	書き込み			

AWS Network Manager Chat が定義するリソースタイプ

AWS Network Manager Chat は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Network Manager Chat にアクセスするには、ポリシーで `"Resource": "*"` を指定してください。

AWS Network Manager Chat を指定 の条件キー

Network Manager Chat には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS「グローバル条件コンテキストキー」を参照してください。

Amazon Nimble Studio のアクション、リソース、条件キー

Amazon Nimble Studio (サービスプレフィックス: `nimble`) では、IAM 許可ポリシーで使用できるように、次のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Nimble Studio によって定義されたアクション
- Amazon Nimble Studio で定義されたリソースタイプ
- Amazon Nimble Studio の条件キー

Amazon Nimble Studio によって定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptEulas	EULA を承諾するためのアクセス許可を付与	Write	eula*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateLaunchProfile	起動プロファイルを作成するためのアクセス許可を付与	Write	studio*		ec2:CreateNetworkInterface ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeRouteTables ec2:DescribeSubnets ec2:DescribeVpcEndpoints ec2:RunInstances
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateStreamingImage	ストリーミングイメージを作成するためのアクセス許可を付与	Write	studio*		ec2:DescribeImages ec2:DescribeSnapshots ec2:ModifyInstanceAttribute ec2:ModifySnapshotAttribute ec2:RegisterImage
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateStreamingSession	ストリーミングセッションを作成するためのアクセス許可を付与	Write	launch-profile*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission nimble:GetLaunchProfile nimble:GetLaunchProfileInitialization nimble:ListEulaAcceptances
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStreamingSessionStream	StreamingSessionStream を作成するためのアクセス許可を付与	Write	streaming-session*		
				nimble:requesterPrincipalId	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateStudio	スタジオを作成するためのアクセス許可を付与	Write	studio*		iam:PassRole sso:CreateManagedApplicationInstance
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStudioComponent	スタジオコンポーネントを作成するためのアクセス許可を付与 スタジオコンポーネントは、起動プロファイルがアクセスを提供するネットワークリソースを指定します	Write	studio*		ds:AuthorizeApplication ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteLaunchProfile	起動プロファイルを削除するためのアクセス許可を付与	Write	launch-profile*		
DeleteLaunchProfileMember	起動プロファイルメンバーを削除するためのアクセス許可を付与	Write	launch-profile*		
DeleteStreamingImage	ストリーミングイメージを削除するためのアクセス許可を付与	Write	streaming-image*		ec2:DeleteSnapshot ec2:DeregisterImage ec2:ModifyInstanceAttribute ec2:ModifySnapshotAttribute
DeleteStreamingSession	ストリーミングセッションを削除するためのアクセス許可を付与	Write	streaming-session*		ec2:DeleteNetworkInterface

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				nimble:requesterPrincipalId	
DeleteStudio	スタジオを削除するためのアクセス許可を付与	Write	studio*		sso:DeleteManagedApplicationInstance
DeleteStudioComponent	スタジオコンポーネントを削除するためのアクセス許可を付与	Write	studio-component*		ds:UnauthorizeApplication
DeleteStudioMember	スタジオメンバーを削除するためのアクセス許可を付与	Write	studio*		
GetEula	EULA を取得するためのアクセス許可を付与	Read	eula*		
GetFeatureMap [許可のみ]	Nimble Studio ポータルがこのアカウントに適切な機能を表示できるようにするためのアクセス許可を付与	Read			
GetLaunchProfile	起動プロファイルを取得するためのアクセス許可を付与	Read	launch-profile*		
GetLaunchProfileDetails	起動プロファイルによって使用されるスタジオコンポーネントとストリーミングイメージの概要を含む、起動プロファイルの詳細を取得するためのアクセス許可を付与	Read	launch-profile*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetLaunchProfileInitialization	起動プロファイルの初期化を取得するためのアクセス許可を付与 起動プロファイルの初期化は、アタッチされたスタジオコンポーネントの接続情報を含む、起動プロファイルの参照解除されたバージョンです	Read	launch-profile*		ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems
GetLaunchProfileMember	起動プロファイルメンバーを取得するためのアクセス許可を付与	Read	launch-profile*		
GetStreamingImage	ストリーミングイメージを取得するためのアクセス許可を付与	Read	streaming-image*		
GetStreamingSession	ストリーミングセッションを取得するためのアクセス許可を付与	読み取り	streaming-session*		
				nimble:requesterPrincipalId	
GetStreamingSessionBackup	ストリーミングセッションバックアップを取得するアクセス許可を付与	読み取り	streaming-session-backup*		
				nimble:requesterPrincipalId	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetStreamingSessionStream	ストリーミングセッションストリームを取得するためのアクセス許可を付与	Read	streaming-session*		
				nimble:requesterPrincipalId	
GetStudio	スタジオを取得するためのアクセス許可を付与	Read	studio*		
GetStudioComponent	スタジオコンポーネントを取得するためのアクセス許可を付与	Read	studio-component*		
GetStudioMember	スタジオメンバーを取得するためのアクセス許可を付与	Read	studio*		
ListEulaAcceptances	EULA 承認を一覧表示するためのアクセス許可を付与	Read	eula-acceptance*		
ListEulas	EULA を一覧表示する許可を付与	Read	eula*		
ListLaunchProfileMembers	起動プロファイルメンバーを一覧表示するためのアクセス許可を付与	Read	launch-profile*		
ListLaunchProfiles	起動プロファイルを一覧表示するためのアクセス許可を付与	Read	studio*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				nimble:principalId nimble:requesterPrincipalId	
ListStreamingImages	ストリーミングイメージを一覧表示するためのアクセス許可を付与	読み取り	studio*		
ListStreamingSessionBackups	ストリーミングセッションバックアップを一覧表示するアクセス許可を付与	読み取り	studio*		
				nimble:requesterPrincipalId	
ListStreamingSessions	ストリーミングセッションを一覧表示するためのアクセス許可を付与	Read	studio*		
				nimble:createdBy nimble:ownedBy nimble:requesterPrincipalId	
ListStudioComponents	スタジオコンポーネントを一覧表示するためのアクセス許可を付与	Read	studio*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListStudioMembers	スタジオメンバーを一覧表示するためのアクセス許可を付与	Read	studio*		
ListStudios	すべてのスタジオを一覧表示するためのアクセス許可を付与	Read			
ListTagsForResource	Nimble Studio リソースのすべてのタグを一覧表示するためのアクセス許可を付与	Read	launch-profile		
			streaming-image		
			streaming-session		
			streaming-session-backup		
			studio		
			studio-component		
PutLaunchProfileMembers	起動プロファイルメンバーを追加/更新するためのアクセス許可を付与	Write	launch-profile*		sso-directory:DescribeUsers
PutStudioLogEvents [アクセス許可のみ]	Nimble Studio ポータルのメトリクスとログをレポートし、アプリケーションの正常性を監視するためのアクセス許可を付与	Write	studio*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutStudioMembers	スタジオメンバーを追加/更新するためのアクセス許可を付与	書き込み	studio*		sso-directory:DescribeUsers
StartStreamingSession	ストリーミングセッションを開始するためのアクセス許可を付与	書き込み	streaming-session*		nimble:GetLaunchProfile nimble:GetLaunchProfileMember
			streaming-session-backup		
				nimble:requesterPrincipalId	
StartStudioSSOConfigurationRepair	スタジオの IAM Identity Center AWS 設定を修復するアクセス許可を付与します	書き込み	studio*		sso:CreateManagedApplicationInstance sso:GetManagedApplicationInstance
StopStreamingSession	ストリーミングセッションを停止するためのアクセス許可を付与	書き込み	streaming-session*		nimble:GetLaunchProfile

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				nimble:requesterPrincipalId	
TagResource	指定された Nimble Studio リソースの 1 つ以上のタグを追加または上書きするためのアクセス許可を付与	タグ付け	launch-profile		
			streaming-image		
			streaming-session		
			streaming-session-backup		
			studio		
			studio-component		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UntagResource	指定された Nimble Studio リソースから 1 つまたは複数のタグの関連付けを解除するためのアクセス許可を付与	タグ付け	launch-profile		
			streaming-image		
			streaming-session		
			streaming-session-backup		
			studio		
			studio-component		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateLaunchProfile	起動プロファイルを更新するためのアクセス許可を付与	Write	launch-profile*		ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeRouteTables ec2:DescribeSubnets ec2:DescribeVpcEndpoints
UpdateLaunchProfileMember	起動プロファイルメンバーを更新するためのアクセス許可を付与	Write	launch-profile*		
UpdateStreamingImage	ストリーミングイメージを更新するためのアクセス許可を付与	Write	streaming-image*		
UpdateStudio	スタジオを更新するためのアクセス許可を付与	Write	studio*		iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateStudioComponent	スタジオコンポーネントを更新するためのアクセス許可を付与	Write	studio-component*		ds:AuthorizeApplication ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems iam:PassRole

Amazon Nimble Studio で定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
studio	`arn:${Partition}:nimble:${Region}:${Account}:studio/${StudioId}`	aws:RequestTag/${TagKey}

リソースタイプ	ARN	条件キー
		aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId
streaming-image	arn:${Partition}:nimble:${Region}:${Account}:streaming-image/${StreamingImageId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId
studio-component	arn:${Partition}:nimble:${Region}:${Account}:studio-component/${StudioComponentId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId
launch-profile	arn:${Partition}:nimble:${Region}:${Account}:launch-profile/${LaunchProfileId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId

リソースタイプ	ARN	条件キー
streaming-session	arn:${Partition}:nimble:${Region}:${Account}:streaming-session/${StreamingSessionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:createdBy nimble:ownedBy
streaming-session-backup	arn:${Partition}:nimble:${Region}:${Account}:streaming-session-backup/${StreamingSessionBackupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:ownedBy
eula	arn:${Partition}:nimble:${Region}:${Account}:eula/${EulaId}	
eula-acceptance	arn:${Partition}:nimble:${Region}:${Account}:eula-acceptance/${EulaAcceptanceId}	nimble:studioId

Amazon Nimble Studio の条件キー

Amazon Nimble Studio では、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString
nimble:createdBy	createdBy リクエストパラメータもしくはリソースの作成者の ID に基づいてアクセスをフィルタリングします。	String
nimble:ownedBy	ownedBy リクエストパラメータもしくはリソースの所有者の ID に基づいてアクセスをフィルタリングします。	String
nimble:principalId	principalId リクエストパラメータに基づいてアクセスをフィルタリングします。	String
nimble:requesterPrincipalId	ログインしているユーザーの ID でアクセスをフィルタリングします。	String
nimble:studioId	特定のスタジオでアクセスをフィルタリングします。	ARN

Amazon One Enterprise のアクション、リソース、および条件キー

Amazon One Enterprise (サービスプレフィックス: one) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon One Enterprise で定義されるアクション
- Amazon One Enterprise で定義されるリソースタイプ
- Amazon One Enterprise の条件キー

Amazon One Enterprise で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateDeviceActivationQrCode	デバイスインスタンスの QR コードを作成するためのアクセス許可を付与	書き込み	device-instance*		
				aws:ResourceTag/${TagKey}	
CreateDeviceConfigurationTemplate	デバイス設定テンプレートを作成するためのアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceInstance	デバイスインスタンスを作成するためのアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceInstanceConfiguration	デバイスインスタンス設定を作成するためのアクセス許可を付与	書き込み	device-instance*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
CreateSite	サイトを作成するためのアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAssociatedDevice	デバイスとデバイスインスタンスの関連付けを解除するためのアクセス許可を付与	書き込み	device-instance*		
				aws:ResourceTag/${TagKey}	
DeleteDeviceConfigurationTemplate	デバイス設定テンプレートを削除するためのアクセス許可を付与	書き込み	device-configuration-template*		
				aws:ResourceTag/${TagKey}	
DeleteDeviceInstance	デバイスインスタンスを削除するためのアクセス許可を付与	書き込み	device-instance*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteSite	サイトを削除するためのアクセス許可を付与	書き込み	site*		
				aws:ResourceTag/${TagKey}	
DeleteUserV1	ユーザーを削除するためのアクセス許可を付与	書き込み	user*		
GetDeviceConfigurationTemplate	デバイス設定テンプレートを表示するためのアクセス許可を付与	読み取り	device-configuration-template*		
				aws:ResourceTag/${TagKey}	
GetDeviceInstance	デバイスインスタンスを表示するためのアクセス許可を付与	読み取り	device-instance*		
				aws:ResourceTag/${TagKey}	
GetDeviceInstanceConfiguration	デバイスインスタンス設定を表示するためのアクセス許可を付与	読み取り	configuration*		
				aws:ResourceTag/${TagKey}	
GetSite	サイトを表示するためのアクセス許可を付与	読み取り	site*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
GetSiteAddress	サイトのアドレスを表示するためのアクセス許可を付与	読み取り	site*		
				aws:ResourceTag/${TagKey}	
ListDeviceConfigurationTemplates	デバイス設定テンプレートのリストを取得するためのアクセス許可を付与	リスト			
ListDeviceInstances	デバイスインスタンスのリストを取得するためのアクセス許可を付与	リスト			
ListSites	サイトのリストを表示するためのアクセス許可を付与	リスト			
ListTagsForResource	Amazon One Enterprise リソースのタグを一覧表示するためのアクセス許可を付与	読み取り	device-configuration-template		
			device-instance		
			site		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListUsersV1	ユーザーのリストを表示するためのアクセス許可を付与	リスト			
RebootDevice	デバイスインスタンスに関連付けられたデバイスを再起動するためのアクセス許可を付与	書き込み	device-instance*		
				aws:ResourceTag/${TagKey}	
TagResource	Amazon One Enterprise リソースにタグを追加するためのアクセス許可を付与	Tagging	device-configuration-template		
			device-instance		
			site		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Amazon One Enterprise リソースからタグを削除するためのアクセス許可を付与	Tagging	device-configuration-template		
			device-instance		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			site		
				aws:TagKeys	
UpdateDeviceConfigurationTemplate	デバイス設定テンプレートを更新するためのアクセス許可を付与	書き込み	device-configuration-template*		
				aws:ResourceTag/${TagKey}	
UpdateDeviceInstance	デバイスインスタンスを更新するためのアクセス許可を付与	書き込み	device-instance*		
				aws:ResourceTag/${TagKey}	
UpdateSite	サイトを更新するためのアクセス許可を付与	書き込み	site*		
				aws:ResourceTag/${TagKey}	
UpdateSiteAddress	サイトのアドレスを更新するためのアクセス許可を付与	書き込み	site*		
				aws:ResourceTag/${TagKey}	

Amazon One Enterprise で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
device-instance	arn:${Partition}:one:${Region}:${Account}:device-instance/${DeviceInstanceId}	aws:ResourceTag/${TagKey}
configuration	arn:${Partition}:one:${Region}:${Account}:device-instance/${DeviceInstanceId}/configuration/${Version}	
device-configuration-template	arn:${Partition}:one:${Region}:${Account}:device-configuration-template/${TemplateId}	aws:ResourceTag/${TagKey}
site	arn:${Partition}:one:${Region}:${Account}:site/${SiteId}	aws:ResourceTag/${TagKey}
user	arn:${Partition}:one:${Region}:${Account}:user/${UserId}	

Amazon One Enterprise の条件キー

Amazon One Enterprise は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアによってアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアによってアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon OpenSearch のアクション、リソース、および条件キー

Amazon OpenSearch (サービスプレフィックス: opensearch) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon OpenSearch で定義されるアクション
- Amazon OpenSearch で定義されるリソースタイプ
- Amazon OpenSearch の条件キー

Amazon OpenSearch で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ApplicationAccessAll [アクセス許可のみ]	OpenSearch Application にアクセスする許可を付与	権限の管理	application*		
CancelDirectQuery	OpenSearch DataSource リソースで送信されたクエリをキャンセルするアクセス許可を付与します	書き込み	datasource*		
GetDirectQuery	OpenSearch DataSource リソースで実行されるクエリステータスを取得する許可を付与	読み取り	datasource*		
GetDirectQueryResult	OpenSearch DataSource リソースで実行されるクエリの結果を取得するアクセス許可を付与します	読み取り	datasource*		
StartDirectQuery	提供された OpenSearch DataSource ARN で直接クエリを開始するアクセス許可を付与します	書き込み	datasource*		

Amazon OpenSearch で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
application	arn:${Partition}:opensearch:${Region}:${Account}:application/${AppId}	
datasource	arn:${Partition}:opensearch:${Region}:${Account}:datasource/${DataSourceName}	

Amazon OpenSearch の条件キー

OpenSearch には、ポリシーステートメントの Condition要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon OpenSearch Ingestion のアクション、リソース、および条件キー

Amazon OpenSearch Ingestion (サービスプレフィックス: osis) には、IAM 許可ポリシーで使用できるように、次のサービス固有のリソース、アクション、および条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon OpenSearch Ingestion で定義されるアクション
- Amazon OpenSearch Ingestion で定義されるリソースタイプ
- Amazon OpenSearch Ingestion の条件キー

Amazon OpenSearch Ingestion で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreatePipeline	OpenSearch Ingestion のパイプラインを作成する許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole iam:PassRole kms:DescribeKey kms:GenerateDataKeyWithoutPlaintext logs:CreateLogDelivery
DeletePipeline	OpenSearch Ingestion のパイプラインを削除する許可を付与	書き込み	pipeline*		logs:DeleteLogDelivery logs:GetLogDelivery logs:ListLogDeliveries
GetPipeline	OpenSearch Ingestion のパイプラインから設定情報を取得する許可を付与	読み取り	pipeline*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetPipelineBlueprint	OpenSearch Ingestion のパイプラインからブループリントの内容を取得する許可を付与	読み取り	pipeline-blueprint*		
GetPipelineChangeProgress	OpenSearch Ingeestion のパイプラインに関する詳細度情報を取得する許可を付与	読み取り	pipeline*		
Ingest	OpenSearch Ingestion のパイプラインを通じてデータを取り込む許可を付与	書き込み	pipeline*		
ListPipelineBlueprints	OpenSearch Ingestion のパイプライン設定で使用可能なブループリントの名前を一覧表示する許可を付与	リスト			
ListPipelines	現在のアカウントとリージョンにある、各 OpenSearch Ingestion のパイプラインの基本設定を一覧表示する許可を付与	リスト			
ListTagsForResource	OpenSearch Ingestion のパイプラインに関連付けられたすべてのリソースタグを一覧表示する許可を付与	読み取り	pipeline*		
StartPipeline	OpenSearch Ingestion のパイプラインを開始する許可を付与	書き込み	pipeline*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StopPipeline	OpenSearch Ingestion のパイプラインを停止する許可を付与	書き込み	pipeline*		
TagResource	OpenSearch Ingestion のパイプラインにリソースタグをアタッチする許可を付与	Tagging	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	OpenSearch Ingestion Service パイプラインからリソースタグを削除する許可を付与	Tagging	pipeline*		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdatePipeline	OpenSearch Ingestion のパイプラインの設定を変更する許可を付与	書き込み	pipeline*		iam:PassRole kms:DescribeKey kms:GenerateDataKeyWithoutPlaintext logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery
ValidatePipeline	OpenSearch Ingestion のパイプラインの設定を検証する許可を付与	読み取り			

Amazon OpenSearch Ingestion で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
pipeline	arn:${Partition}:osis:${Region}:${Account}:pipeline/${PipelineName}	aws:ResourceTag/${TagKey}
pipeline-blueprint	arn:${Partition}:osis:${Region}:${Account}:blueprint/${BlueprintName}	

Amazon OpenSearch Ingestion の条件キー

Amazon OpenSearch Ingestion では、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義しています。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon OpenSearch Serverless のアクション、リソース、および条件キー

Amazon OpenSearch Serverless (サービスプレフィックス: aoss) では、IAM 許可ポリシーで使用できるように、次のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon OpenSearch Serverless で定義されるアクション
- Amazon OpenSearch Serverless で定義されるリソースタイプ
- Amazon OpenSearch Serverless の条件キー

Amazon OpenSearch Serverless で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
APIAccessAll	サポートされているすべての Opensearch API に許可を付与	書き込み	Collection*		
				aoss:collection aoss:CollectionId	
BatchGetCollection	1 つまたは複数のコレクションの属性を取得する許可を付与	読み取り		aoss:collection	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchGetEffectiveLifecyclePolicy	1 つ以上の AOSS リソースに適用されるライフサイクルポリシーに関する情報を取得するアクセス許可を付与	読み取り			
BatchGetLifecyclePolicy	1 つまたは複数のライフサイクルポリシーの情報を取得するアクセス許可を付与	読み取り			
BatchGetVpcEndpoint	1 つまたは複数の VPC エンドポイントの属性を取得する許可を付与	読み取り			
CreateAccessPolicy	データアクセスポリシーを作成する許可を付与	書き込み		aoss:collection aoss:index	
CreateCollection	サーバーレスコレクションを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateIndex	オープンサーチインデックスを作成するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateLifecyclePolicy	ライフサイクルポリシーを作成するアクセス許可を付与	書き込み		aoss:index	
CreateSecurityConfig	サーバーレスセキュリティ設定を作成する許可を付与	書き込み			
CreateSecurityPolicy	ネットワークまたは暗号化ポリシーを作成する許可を付与	書き込み		aoss:collection	
CreateVpcEndpoint	OpenSearch Serverless マネージド VPC エンドポイントを作成する許可を付与	書き込み			
DashboardsAccessAll	Opensearch Serverless ダッシュボードに許可を付与	書き込み	Dashboards*		
				aoss:collection aoss:CollectionId	
DeleteAccessPolicy	データアクセスポリシーを削除する許可を付与	書き込み		aoss:collection aoss:index	
DeleteCollection	サーバーレスコレクションを削除する許可を付与	書き込み	Collection*		
DeleteIndex	オープンサーチインデックスを削除するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteLifecyclePolicy	ライフサイクルポリシーを削除するアクセス許可を付与	書き込み		aoss:index	
DeleteSecurityConfig	セキュリティ設定を削除する許可を付与。	書き込み			
DeleteSecurityPolicy	セキュリティポリシーを削除する許可を付与	書き込み		aoss:collection	
DeleteVpcEndpoint	OpenSearch Serverless マネージドインターフェース VPC エンドポイントを削除する許可を付与	書き込み			
GetAccessPolicy	データアクセスポリシーに関する情報を取得する許可を付与	読み取り		aoss:collection aoss:index	
GetAccountSettings	容量設定を含むアカウント設定を取得する許可を付与	読み取り			
GetIndex	オープンサーチインデックスを取得するアクセス許可を付与します	読み取り			
GetPoliciesStats	アカウント内のセキュリティポリシーに関する統計を取得する許可を付与	読み取り			
GetSecurityConfig	サーバーレスセキュリティ設定に関する情報を取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetSecurityPolicy	セキュリティポリシーに関する情報を取得する許可を付与	読み取り		aoss:collection	
ListAccessPolicies	データアクセスポリシーを一覧表示する許可を付与	リスト			
ListCollections	コレクションを一覧表示する許可を付与	リスト			
ListLifecyclePolicies	ライフサイクルポリシーを一覧表示するアクセス許可を付与	リスト			
ListSecurityConfigs	セキュリティ設定を一覧表示する許可を付与	リスト			
ListSecurityPolicies	セキュリティポリシーを一覧表示する許可を付与	リスト			
ListTagsForResource	コレクションのタグを一覧表示する許可を付与	リスト			
ListVpcEndpoints	OpenSearch Serverless マネージド VPC エンドポイントを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagResource	サーバーレスコレクションをタグ付けする許可を付与	書き込み		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	コレクションからタグを削除する許可を付与	書き込み		aws:TagKeys	
UpdateAccessPolicy	データアクセスポリシーを更新する許可を付与	書き込み		aoss:collection aoss:index	
UpdateAccountSettings	容量設定を含むアカウント設定を更新する許可を付与	書き込み			
UpdateCollection	コレクションを更新する許可を付与	書き込み	Collection*		
UpdateIndex	オープンサーチインデックスを更新する許可を付与	書き込み			
UpdateLifecyclePolicy	ライフサイクルポリシーを更新するアクセス許可を付与	書き込み		aoss:index	
UpdateSecurityConfig	セキュリティ設定を更新する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateSecurityPolicy	セキュリティポリシーを更新する許可を付与	書き込み		aoss:collection	
UpdateVpcEndpoint	OpenSearch Serverless マネージド VPC エンドポイントを更新する許可を付与	書き込み			

Amazon OpenSearch Serverless で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Collection	arn:${Partition}:aoss:${Region}:${Account}:collection/${CollectionId}	aws:ResourceTag/${TagKey}
Dashboards	arn:${Partition}:aoss:${Region}:${Account}:dashboards/default	

Amazon OpenSearch Serverless の条件キー

Amazon OpenSearch Serverless では、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aoss:CollectionId	コレクションの識別子でアクセスをフィルタリング	String
aoss:collection	コレクション名でアクセスをフィルタリング	String
aoss:index	索引でアクセスをフィルタリング	String
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられているタグに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーに基づいてアクションをフィルタリングします	ArrayOfString

Amazon OpenSearch Service のアクション、リソース、および条件キー

Amazon OpenSearch Service (サービスプレフィックス: es) では、IAM 許可ポリシーで使用できるように、次のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon OpenSearch Service で定義されるアクション
- Amazon OpenSearch Service で定義されるリソースタイプ
- Amazon OpenSearch Service の条件キー

Amazon OpenSearch Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AcceptInboundConnection	インバウンドクロスクラスター検索接続リクエストを受け入れるためのアクセス許可を送信先ドメイン所有者に付与します	書き込み			
AcceptInboundCrossClusterSearchConnection	クロスクラスターでの検索接続に関するインバウンドリクエストを受け入れるためのアクセス許可を、送信先ドメインの所有者に付与する このアクセス許可は廃止されました。代わりに AcceptInboundConnection を使用してください。	書き込み			
AddDataSource	OpenSearch Service ドメインのデータソースを追加するためのアクセス許可を付与	書き込み	domain*		
AddDirectQueryDataSource	提供された OpenSearch ARN のデータソースを追加する許可を付与	書き込み	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
AddTags	OpenSearch Service ドメイン、データソース、またはアプリケーションにリソースタ	Tagging	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	グをアタッチするアクセス許可を付与します		datasource*		
			domain*		
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociatePackage	パッケージを OpenSearch Service ドメインに関連付けるためのアクセス許可を付与する	書き込み	domain*		
AssociatePackages	複数のパッケージを OpenSearch Service ドメインに関連付けるアクセス許可を付与します	書き込み	domain*		
AuthorizeVpcEndpointAccess	インターフェイス VPC エンドポイントを使用して Amazon OpenSearch Service ドメインへのアクセスを提供するアクセス許可を付与	書き込み			
CancelDomainConfigChange	OpenSearch Service ドメインの変更をキャンセルするためのアクセス許可を付与	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelElasticsearchServiceSoftwareUpdate	ドメインのサービスソフトウェアに対する更新をキャンセルするためのアクセス許可を付与する このアクセス許可は廃止されました。代わりに CancelServiceSoftwareUpdate を使用してください。	書き込み	domain*		
CancelServiceSoftwareUpdate	ドメインのサービスソフトウェアに対する更新をキャンセルするためのアクセス許可を付与する	書き込み	domain*		
CreateApplication	OpenSearch アプリケーションを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDomain	Amazon OpenSearch Service ドメインを作成する許可を付与	書き込み	domain		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateElasticsearchDomain	OpenSearch Service ドメインを作成するためのアクセス許可を付与する このアクセス許可は廃止されました。代わりにCreateDomain を使用してください。	書き込み	domain		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateElasticsearchServiceRole	VPC アクセスを使用する OpenSearch Service ドメインに必要な、サービスにリンクされたロールを作成するためのアクセス許可を付与する このアクセス許可は廃止されました。サービスにリンクされたロールは OpenSearch Service によって自動的に作成されます	書き込み			
CreateOutboundConnection	送信元ドメインから送信先ドメインへの新しいクロスクラスター検索接続を作成するためのアクセス許可を付与します	書き込み	domain*		
CreateOutboundCrossClusterSearchConnection	送信元ドメインから送信先ドメインに対する、クロスクラスターでの新しい検索接続を作成するためのアクセス許可を付与する このアクセス許可は廃止されました。代わりにCreateOutboundConnection を使用してください。	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreatePackage	OpenSearch Service ドメインで使用するパッケージを追加するためのアクセス許可を付与する	書き込み			
CreateServiceRole	VPC アクセスを使用する Amazon OpenSearch Service ドメインに必要な、サービスにリンクされたロールを作成するためのアクセス許可を付与する	書き込み			
CreateVpcEndpoint	Amazon OpenSearch Service マネージド VPC エンドポイントを作成するアクセス許可を付与	書き込み			
DeleteApplication	OpenSearch アプリケーションを削除するアクセス許可を付与します	書き込み	application*		
DeleteDataSource	OpenSearch Service ドメインのデータソースを削除するためのアクセス許可を付与	書き込み	domain*		
DeleteDirectQueryDataSource	提供された OpenSearch ARN のデータソースを削除するアクセス許可を付与します	書き込み	datasource*		
DeleteDomain	Amazon OpenSearch Service ドメインとそのすべてのデータを削除するためのアクセス許可を付与する	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteElasticsearchDomain	OpenSearch Service ドメインとそのすべてのデータを削除するためのアクセス許可を付与する このアクセス許可は廃止されました。代わりに DeleteDomain を使用してください。	書き込み	domain*		
DeleteElasticsearchServiceRole	VPC アクセスを使用する OpenSearch Service ドメインが使用している、サービスにリンクされたロールを削除するためのアクセス許可を付与する このアクセス許可は廃止されました。サービスにリンクされたロールを削除するには、IAM API を使用します。	書き込み			
DeleteInboundConnection	既存のインバウンドクロスクラスター検索接続を削除するためのアクセス許可を送信先ドメインの所有者に付与します	書き込み			
DeleteInboundCrossClusterSearchConnection	既存のクロスクラスターでのインバウンド検索接続を削除するためのアクセス許可を、送信先ドメインの所有者に付与する このアクセス許可は廃止されました。代わりに DeleteInboundConnection を使用してください。	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteOutboundConnection	既存のアウトバウンドクロスクラスター検索接続を削除するためのアクセス許可をソースドメイン所有者に付与します。	書き込み			
DeleteOutboundCrossClusterSearchConnection	既存のクロスクラスターでのアウトバウンド検索接続を削除するためのアクセス許可を、送信元のドメイン所有者に付与する このアクセス許可は廃止されました。代わりに DeleteOutboundConnection を使用してください。	書き込み			
DeletePackage	OpenSearch Service からパッケージを削除するためのアクセス許可を付与する パッケージは、どのドメインとも関連付けることはできません。	書き込み			
DeleteVpcEndpoint	Amazon OpenSearch Service マネージドインターフェース VPC エンドポイントを削除するアクセス許可を付与	書き込み			
DescribeDomain	指定された OpenSearch Service ドメインについて、そのドメインの設定 (ドメインの ID、サービスエンドポイント、ARN など) を詳細表示するためのアクセス許可を付与する	読み取り	domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeDomainAutoTunes	指定された OpenSearch Service ドメインについて、ドメインの Auto-Tune 設定 (Auto-Tune の状態やメンテナンススケジュールなど) を表示するためのアクセス許可を付与する	読み取り	domain*		
DescribeDomainChangeProgress	OpenSearch Service ドメインの詳細ステージの進行状況を表示する許可を付与	読み取り	domain*		
DescribeDomainConfig	OpenSearch Service ドメインの設定オプションおよびステータスを詳細表示するためのアクセス許可を付与する	読み取り	domain*		
DescribeDomainHealth	ドメインとノードの状態、スタンバイアベイラビリティーゾーン、アベイラビリティーゾーンごとのノード数、ノードごとのシャード数に関する情報を表示するアクセス許可を付与します	読み取り	domain*		
DescribeDomainNodes	ドメインに設定されたノードと、その設定に関する情報 (ノード ID、ノードのタイプ、ノードのステータス、アベイラビリティーゾーン、インスタンスタイプ、ストレージ) を表示する許可を付与	読み取り	domain*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeDomains	指定された OpenSearch Service ドメイン (最大 5 個) についてドメイン設定を詳細表示するためのアクセス許可を付与する	リスト	domain*		
DescribeDryRunProgress	OpenSearch Service ドメインの更新前検証チェックのステータスを記述するアクセス許可を付与	読み取り	domain*		
DescribeElasticsearchDomain	指定された OpenSearch Service ドメインについて、ドメイン設定 (ドメインの ID、サービスエンドポイント、および ARN など) を詳細表示するためのアクセス許可を付与する このアクセス許可は廃止されました。代わりに DescribeDomain を使用してください。	読み取り	domain*		
DescribeElasticsearchDomainConfig	OpenSearch Service ドメインの設定とステータスを詳細表示するためのアクセス許可を付与する このアクセス許可は廃止されました。代わりに DescribeDomainConfig を使用してください。	読み取り	domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeElasticsearchDomains	指定された Amazon OpenSearch ドメイン (最大 5 個) について、ドメイン設定を詳細表示するためのアクセス許可を付与する このアクセス許可は廃止されました。代わりに DescribeDomains を使用してください。	リスト	domain*		
DescribeElasticsearchInstanceTypeLimits	特定の OpenSearch バージョンとインスタンスタイプについて、インスタンス数、ストレージ、マスターノードの制限を表示するためのアクセス許可を付与する このアクセス許可は廃止されました。代わりに DescribeInstanceTypeLimits を使用してください。	リスト			
DescribeInboundConnections	送信先ドメインのすべてのインバウンドクロスクラスター検索接続を一覧表示するためのアクセス許可を付与します	リスト			
DescribeInboundCrossClusterSearchConnections	送信先ドメインにおけるクロスクラスターでのすべてのインバウンド検索接続を、一覧表示するためのアクセス許可を付与する このアクセス許可は廃止されました。代わりに DescribeInboundConnections を使用してください。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeInstanceTypeLimits	特定エンジンバージョンとインスタンスタイプについて、インスタンス数、ストレージ、マスターノードの制限を表示するためのアクセス許可を付与する	リスト			
DescribeOutboundConnections	送信元ドメインのすべてのアウトバウンドクロスクラスター検索接続を一覧表示するためのアクセス許可を付与します	リスト			
DescribeOutboundCrossClusterSearchConnections	送信元ドメインでの、クロスクラスターによるすべてのアウトバウンド検索接続を一覧表示するためのアクセス許可を付与する このアクセス許可は廃止されました。代わりに DescribeOutboundConnections を使用してください。	リスト			
DescribePackages	OpenSearch Service ドメインで利用可能な、すべてのパッケージについて詳細表示するためのアクセス許可を付与する	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeReservedElasticsearchInstanceOfferings	Amazon OpenSearch Service 向けに、リザーブドインスタンスのサービスを取得するためのアクセス許可を付与するこのアクセス許可は廃止されました。代わりに DescribeReservedInstanceOfferings を使用してください。	リスト			
DescribeReservedElasticsearchInstances	既に購入済みの OpenSearch Service リザーブドインスタンスを取得するためのアクセス許可を付与する このアクセス許可は廃止されました。代わりに DescribeReservedInstances を使用してください。	リスト			
DescribeReservedInstanceOfferings	OpenSearch Service 向けに、リザーブドインスタンスのサービスを取得するためのアクセス許可を付与する	リスト			
DescribeReservedInstances	既に購入済みの OpenSearch Service リザーブドインスタンスを取得するためのアクセス許可を付与する	リスト			
DescribeVpcEndpoints	1 つ以上の Amazon OpenSearch Service マネージド VPC エンドポイントを記述するアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DissociatePackage	指定された OpenSearch Service ドメインに対するパッケージの関連付けを、解除するためのアクセス許可を付与する	書き込み	domain*		
DissociatePackages	指定された OpenSearch Service ドメインから複数のパッケージの関連付けを解除するアクセス許可を付与します	書き込み	domain*		
ESCrossClusterGet	クラスター間リクエストをターゲットドメインに送信する許可を付与	Read	domain		
ESHttpDelete	OpenSearch API に HTTP DELETE リクエストを送信する許可を付与	Write	domain		
ESHttpGet	OpenSearch API に HTTP GET リクエストを送信する許可を付与	Read	domain		
ESHttpHead	OpenSearch API に HTTP HEAD リクエストを送信する許可を付与	Read	domain		
ESHttpPatch	OpenSearch API に HTTP PATCH リクエストを送信する許可を付与	Write	domain		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ESHttpPost	OpenSearch API に HTTP POST リクエストを送信する許可を付与	Write	domain		
ESHttpPut	OpenSearch API に HTTP PUT リクエストを送信する許可を付与	書き込み	domain		
GetApplication	OpenSearch アプリケーションに関する情報を取得するアクセス許可を付与します	読み取り	application*		
GetCompatibleElasticsearchVersions	OpenSearch Service ドメインをアップグレードできる互換性を持つ、OpenSearch と Elasticsearch バージョンのリストを取得するためのアクセス許可を付与する このアクセス許可は廃止されました。代わりに GetCompatibleVersions を使用してください。	リスト	domain*		
GetCompatibleVersions	OpenSearch Service ドメインをアップグレードできる互換性を持つ、エンジンバージョンのリストを取得するためのアクセス許可を付与する	リスト	domain*		
GetDataSource	OpenSearch Service ドメインのデータソースを取得するためのアクセス許可を付与	読み取り	domain*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetDirectQueryDataSource	提供された OpenSearch ARN のデータソースを取得する許可を付与	読み取り	datasource*		
GetDomainMaintenanceStatus	ノードのメンテナンスアクションのステータスを取得するアクセス許可を付与します	読み取り	domain*		
GetPackageVersionHistory	パッケージのバージョン履歴を取得するためのアクセス許可を付与します	読み取り			
GetUpgradeHistory	特定の OpenSearch Service ドメインの、アップグレードに関する履歴を取得するためのアクセス許可を付与する	読み取り	domain*		
GetUpgradeStatus	特定の OpenSearch Service ドメインのアップグレード状況を取得するためのアクセス許可を付与する	読み取り	domain*		
ListApplications	OpenSearch アプリケーションを一覧表示する許可を付与	リスト	application*		
ListDataSources	OpenSearch Service ドメインのデータソースのリストを取得するためのアクセス許可を付与	リスト	domain*		
ListDirectQueryDataSources	提供された OpenSearch ARN のデータソースのリストを取得する許可を付与	リスト	datasource*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListDomainMaintenances	OpenSearch Service ドメインのメンテナンスアクションのリストを取得するアクセス許可を付与します	リスト	domain*		
ListDomainNames	現在のユーザーが所有している、すべての OpenSearch Service ドメインの名前を表示するためのアクセス許可を付与する	リスト			
ListDomainsForPackage	パッケージが関連付けられている、すべての OpenSearch Service ドメインを一覧表示するためのアクセス許可を付与する	リスト			
ListElasticsearchInstanceTypeDetails	特定の OpenSearch バージョンの、すべてのインスタンスタイプと使用可能な機能を一覧表示するためのアクセス許可を付与する このアクセス許可は廃止されました。代わりに ListInstanceTypeDetails を使用してください。	リスト			
ListElasticsearchInstanceTypes	特定の OpenSearch バージョンでサポートされている、すべての EC2 インスタンスタイプを一覧表示するためのアクセス許可を付与する	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListElasticsearchVersions	Amazon OpenSearch Service でサポートされている、すべての OpenSearch バージョンを一覧表示するためのアクセス許可を付与する このアクセス許可は廃止されました。代わりに ListVersions を使用してください。	リスト			
ListInstanceTypeDetails	特定の OpenSearch もしくは Elasticsearch バージョンの、すべてのインスタンスタイプと使用可能な機能を一覧表示するためのアクセス許可を付与する	リスト			
ListPackagesForDomain	OpenSearch Service ドメインに関連付けられている、すべてのパッケージを一覧表示するためのアクセス許可を付与する	リスト	domain*		
ListScheduledActions	OpenSearch Service ドメインのためにスケジュールされている設定変更のリストを取得するための許可を付与します	リスト	domain*		
ListTags	OpenSearch Service ドメイン、データソース、またはアプリケーションのすべてのリソースタグを表示するアクセス許可を付与します	読み取り	application*		
			datasource*		
			domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListVersions	Amazon OpenSearch Service でサポートされている、すべての OpenSearch および Elasticsearch のバージョンを一覧表示するためのアクセス許可を付与する	リスト			
ListVpcEndpointAccess	インターフェイス VPC エンドポイントを使用して、特定の Amazon OpenSearch Service ドメインへのアクセスが許可されている各 AWS プリンシパルに関する情報を取得するアクセス許可を付与します	リスト			
ListVpcEndpoints	現在の AWS アカウント およびリージョン内のすべての Amazon OpenSearch Service マネージド VPC エンドポイントを取得するアクセス許可を付与します	リスト			
ListVpcEndpointsForDomain	特定のドメインに関連付けられているすべての Amazon OpenSearch Service マネージド VPC エンドポイントを取得するアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PurchaseReservedElasticsearchInstanceOffering	OpenSearch Service リザーブドインスタンスを購入するためのアクセス許可を付与するこのアクセス許可は廃止されました。代わりに PurchaseReservedInstanceOffering を使用してください。	書き込み			
PurchaseReservedInstanceOffering	OpenSearch リザーブドインスタンスを購入する許可を付与	Write			
RejectInboundConnection	インバウンドクロスクラスター検索接続リクエストを拒否するためのアクセス許可を送信先ドメインの所有者に付与します	書き込み			
RejectInboundCrossClusterSearchConnection	クロスクラスターでの検索接続に関するインバウンドリクエストを拒否するためのアクセス許可を、送信先ドメインの所有者に対し付与する このアクセス許可は廃止されました。代わりに RejectInboundConnection を使用してください。	書き込み			
RemoveTags	OpenSearch Service ドメイン、データソース、またはアプリケーションからリソースタグを削除する許可を付与	Tagging	application*		
			datasource*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			domain*		
				aws:TagKeys	
RevokeVpcEndpointAccess	インターフェイス VPC エンドポイントを使用して提供された Amazon OpenSearch Service ドメインへのアクセスを取り消すアクセス許可を付与	書き込み			
StartDomainMaintenance	ノードのメンテナンスを開始するアクセス許可を付与します	書き込み	domain*		
StartElasticsearchServiceSoftwareUpdate	ドメインのサービスソフトウェアの更新を開始するためのアクセス許可を付与する。このアクセス許可は廃止されました。代わりに StartServiceSoftwareUpdate を使用してください。	書き込み	domain*		
StartServiceSoftwareUpdate	ドメインのサービスソフトウェアの更新を開始するためのアクセス許可を付与する	書き込み	domain*		
UpdateApplication	OpenSearch アプリケーションを更新する許可を付与	書き込み	application*		
UpdateDataSource	OpenSearch Service ドメインのデータソースを更新するためのアクセス許可を付与	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateDirectQueryDataSource	提供された OpenSearch ARN のデータソースを更新する許可を付与	書き込み	datasource*		
UpdateDomainConfig	OpenSearch Service ドメインの設定 (インスタンスタイプやインスタンス数など) を変更するためのアクセス許可を付与する	書き込み	domain*		
UpdateElasticsearchDomainConfig	OpenSearch Service ドメインの設定 (インスタンスタイプやインスタンス数など) を変更するためのアクセス許可を付与する このアクセス許可は廃止されました。代わりに UpdateDomainConfig を使用してください。	書き込み	domain*		
UpdatePackage	OpenSearch Service ドメインで使用するパッケージを更新するためのアクセス許可を付与する	書き込み			
UpdatePackageScope	パッケージの範囲を更新するアクセス許可を付与します	書き込み			
UpdateScheduledAction	計画された OpenSearch Service ドメイン設定の変更を再スケジュールして遅らせるための許可を付与します	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateVpcEndpoint	Amazon OpenSearch Service マネージドインターフェース VPC エンドポイントを変更するアクセス許可を付与	書き込み			
UpgradeDomain	OpenSearch Service ドメインにおいて、特定のバージョンへのアップグレードを開始するためのアクセス許可を付与する	書き込み	domain*		
UpgradeElasticsearchDomain	OpenSearch Service ドメインにおいて、指定されたバージョンへのアップグレードを開始するためのアクセス許可を付与する このアクセス許可は廃止されました。代わりに UpgradeDomain を使用してください。	書き込み	domain*		

Amazon OpenSearch Service で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
domain	arn:${Partition}:es:${Region}:${Account}:domain/${DomainName}	aws:ResourceTag/${TagKey}
application	arn:${Partition}:opensearch:${Region}:${Account}:application/${AppId}	aws:ResourceTag/${TagKey}
es_role	arn:${Partition}:iam::${Account}:role/aws-service-role/es.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService	aws:ResourceTag/${TagKey}
opensearchservice_role	arn:${Partition}:iam::${Account}:role/aws-service-role/opensearchservice.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService	aws:ResourceTag/${TagKey}
datasource	arn:${Partition}:opensearch:${Region}:${Account}:datasource/${DataSourceName}	aws:ResourceTag/${TagKey}

Amazon OpenSearch Service の条件キー

Amazon OpenSearch Service では、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします	文字列

条件キー	説明	タイプ
aws:ResourceTag/${TagKey}	リソースに関連付けられているタグに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーに基づいてアクションをフィルタリングします	ArrayOfString

AWS OpsWorks のアクション、リソース、および条件キー

AWS OpsWorks (サービスプレフィックス: opsworks) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS OpsWorks で定義されるアクション
- AWS OpsWorks で定義されるリソースタイプ
- AWS OpsWorks の条件キー

AWS OpsWorks で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssignInstance	登録されたインスタンスをレイヤーに割り当てるアクセス許可を付与します	書き込み	stack		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssignVolume	スタックの登録された Amazon EBS ボリュームの 1 つを指定されたインスタンスに割り当てるアクセス許可を付与します	書き込み	stack		
AssociateElasticIp	スタックの登録されている Elastic IP アドレスの 1 つを指定されたインスタンスに関連付けるアクセス許可を付与します	書き込み	stack		
AttachElasticLoadBalancer	Elastic Load Balancing のロードバランサーを指定されたレイヤーにアタッチするアクセス許可を付与します	書き込み	stack		
CloneStack	指定されたスタックのクローンを作成するアクセス許可を付与します	書き込み	stack		
CreateApp	指定されたスタックのアプリケーションを作成するアクセス許可を付与します	書き込み	stack		
CreateDeployment	デプロイコマンドまたはスタックコマンドを実行するアクセス許可を付与します	書き込み	stack		
CreateInstance	指定されたスタックにインスタンスを作成するアクセス許可を付与します	書き込み	stack		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateLayer	レイヤーを作成するアクセス許可を付与します	書き込み	stack		
CreateStack	新しいスタックを作成するアクセス許可を付与します	書き込み			
CreateUserProfile	新しいユーザープロファイルを作成するアクセス許可を付与します	書き込み			
DeleteApp	指定されたアプリケーションを削除するアクセス許可を付与します	書き込み	stack		
DeleteInstance	指定されたインスタンスを削除するアクセス許可を付与します。これにより、関連付けられている Amazon EC2 インスタンスが終了します	書き込み	stack		
DeleteLayer	指定されたレイヤーを削除するアクセス許可を付与します	書き込み	stack		
DeleteStack	指定されたスタックを削除するアクセス許可を付与	書き込み	stack		
DeleteUserProfile	ユーザープロファイルを削除するアクセス許可を付与します	書き込み			
DeregisterEcsCluster	ユーザープロファイルを削除するアクセス許可を付与します	書き込み	stack		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeregisterElasticIp	指定された Elastic IP アドレスを登録解除するアクセス許可を付与します	書き込み	stack		
DeregisterInstance	登録されている Amazon EC2 インスタンスまたはオンプレミスインスタンスを登録解除するアクセス許可を付与します	書き込み	stack		
DeregisterRdsDbInstance	Amazon RDS インスタンスを登録解除するアクセス許可を付与します	書き込み	stack		
DeregisterVolume	Amazon EBS ボリュームを登録解除するアクセス許可を付与します	書き込み	stack		
DescribeAgentVersions	利用可能な AWS OpsWorks エージェントバージョンを記述するアクセス許可を付与します	リスト	stack		
DescribeApps	指定された一連のアプリケーションの説明をリクエストするアクセス許可を付与します	リスト	stack		
DescribeCommands	指定されたコマンドの結果を記述するアクセス許可を付与します	リスト	stack		
DescribeDeployments	指定された一連のデプロイの説明をリクエストするアクセス許可を付与します	リスト	stack		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeEcsClusters	スタックに登録されているAmazon ECS クラスターを記述するアクセス許可を付与します	リスト	stack		
DescribeElasticIps	Elastic IP アドレスを記述するアクセス許可を付与します	リスト	stack		
DescribeElasticLoadBalancers	スタックの Elastic Load Balancing インスタンスを記述するアクセス許可を付与します	リスト	stack		
DescribeInstances	一連のインスタンスの説明をリクエストするアクセス許可を付与します	リスト	stack		
DescribeLayers	指定されたスタックの 1 つまたは複数のレイヤーの説明をリクエストするアクセス許可を付与します	リスト	stack		
DescribeLoadBasedAutoScaling	指定されたレイヤーの負荷ベースのオートスケーリング設定を記述するアクセス許可を付与します	リスト	stack		
DescribeMyUserProfile	ユーザーの SSH 情報を記述するアクセス許可を付与します	リスト			
DescribeOperatingSystems	AWS OpsWorks スタックでサポートされているオペレーティングシステムを記述するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribePermissions	指定されたスタックのアクセス許可を記述するアクセス許可を付与します	リスト	stack		
DescribeRaidArrays	インスタンスの RAID 配列を記述するアクセス許可を付与します	リスト	stack		
DescribeRdsDbInstances	Amazon RDS インスタンスを記述するアクセス許可を付与します	リスト	stack		
DescribeServiceErrors	AWS OpsWorks サービスエラーを記述する許可を付与	リスト	stack		
DescribeStackProvisioningParameters	スタックのプロビジョニングパラメータの説明をリクエストするアクセス許可を付与します	リスト	stack		
DescribeStackSummary	指定されたスタックのレイヤーとアプリケーションの数、および各状態 (running_setup や online など) のインスタンスの数を記述するアクセス許可を付与します	リスト	stack		
DescribeStacks	1 つまたは複数のスタックの説明をリクエストするアクセス許可を付与します	リスト	stack		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeTimeBasedAutoScaling	指定されたインスタンスの時間ベースのオートスケーリング設定を記述するアクセス許可を付与します	リスト	stack		
DescribeUserProfiles	指定されたユーザーを記述するアクセス許可を付与します	リスト			
DescribeVolumes	インスタンスの Amazon EBS ボリュームを記述するアクセス許可を付与します	リスト	stack		
DetachElasticLoadBalancer	指定された Elastic Load Balancing インスタンスをそのレイヤーからデタッチするアクセス許可を付与します	書き込み	stack		
DisassociateElasticIp	インスタンスから Elastic IP アドレスの関連付けを解除するアクセス許可を付与します	書き込み	stack		
GetHostnameSuggestion	現在のホスト名のテーマに基づいて、指定されたレイヤーの生成されたホスト名を取得するアクセス許可を付与します	読み込み	stack		
GrantAccess	指定された期間の Windows インスタンスへの RDP アクセスを許可するアクセス許可を付与します	書き込み	stack		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTags	指定されたスタックまたはレイヤーに適用されるタグのリストを返すアクセス許可を付与します	リスト	stack		
RebootInstance	指定されたインスタンスを再起動するアクセス許可を付与します	書き込み	stack		
RegisterEcsCluster	指定された Amazon ECS クラスターをスタックに登録するアクセス許可を付与します	書き込み	stack		
RegisterElasticIp	Elastic IP アドレスを指定されたスタックに登録するアクセス許可を付与します	書き込み	stack		
RegisterInstance	AWS OpsWorks の外部で作成された指定されたスタックにインスタンスを登録する許可を付与	書き込み	stack		
RegisterRdsDbInstance	Amazon RDS インスタンスをスタックに登録するアクセス許可を付与します	書き込み	stack		
RegisterVolume	Amazon EBS ボリュームを指定されたスタックに登録するアクセス許可を付与します	書き込み	stack		
SetLoadBasedAutoScaling	指定されたレイヤーの負荷ベースのオートスケーリング設定を指定するアクセス許可を付与します	書き込み	stack		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SetPermission	ユーザーのアクセス許可を指定するアクセス許可を付与します	権限の管理	stack		
SetTimeBasedAutoScaling	指定されたインスタンスの時間ベースのオートスケーリング設定を指定するアクセス許可を付与します	書き込み	stack		
StartInstance	指定されたインスタンスを起動するアクセス許可を付与します	書き込み	stack		
StartStack	スタックのインスタンスを起動するアクセス許可を付与します	書き込み	stack		
StopInstance	指定されたインスタンスを停止するアクセス許可を付与します	書き込み	stack		
StopStack	指定されたスタックを停止するアクセス許可を付与します	書き込み	stack		
TagResource	指定されたスタックまたはレイヤーにタグを適用するアクセス許可を付与します	Tagging	stack		
UnassignInstance	すべてのレイヤーから登録されたインスタンスを割り当て解除するアクセス許可を付与します	書き込み	stack		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UnassignVolume	割り当てられている Amazon EBS ボリュームを割り当て解除するアクセス許可を付与します	書き込み	stack		
UntagResource	指定したスタックまたはレイヤーからタグを削除するアクセス許可を付与します	Tagging	stack		
UpdateApp	指定されたアプリケーションを更新するアクセス許可を付与します	書き込み	stack		
UpdateElasticIp	登録された Elastic IP アドレスの名前を更新するアクセス許可を付与します	書き込み	stack		
UpdateInstance	指定されたインスタンスを更新するアクセス許可を付与します	書き込み	stack		
UpdateLayer	指定されたレイヤーを更新するアクセス許可を付与します	書き込み	stack		
UpdateMyUserProfile	ユーザーの SSH 公開鍵を更新するアクセス許可を付与します	書き込み			
UpdateRdsDbInstance	Amazon RDS インスタンスを更新するアクセス許可を付与します	書き込み	stack		
UpdateStack	指定されたスタックを更新するアクセス許可を付与します	書き込み	stack		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateUserProfile	指定されたユーザープロファイルを更新するアクセス許可を付与します	権限の管理			
UpdateVolume	Amazon EBS ボリュームの名前またはマウントポイントを更新するアクセス許可を付与します	書き込み	stack		

AWS OpsWorks で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
stack	`arn:${Partition}:opsworks:${Region}:${Account}:stack/${StackId}/`	

AWS OpsWorks の条件キー

OpsWorks には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS OpsWorks Configuration Management のアクション、リソース、および条件キー

AWS OpsWorks Configuration Management (サービスプレフィックス: opsworks-cm) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS OpsWorks Configuration Management で定義されるアクション
- AWS OpsWorks Configuration Management で定義されるリソースタイプ
- AWS OpsWorks Configuration Management の条件キー

AWS OpsWorks Configuration Management で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateNode	ノードを設定管理サーバーに関連付けるためのアクセス許可を付与	Write			
CreateBackup	指定したサーバーのバックアップを作成するためのアクセス許可を付与	Write			
CreateServer	新しいサーバーを作成するためのアクセス許可を付与	Write			
DeleteBackup	指定されたバックアップと、場合によってはその S3 バ	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	ケットを削除するためのアクセス許可を付与				
DeleteServer	対応する CloudFormation スタック、および場合によっては S3 バケットを使用して、指定されたサーバーを削除するためのアクセス許可を付与	Write			
DescribeAccountAttributes	ユーザーのアカウントのサービスの制限を記述するためのアクセス許可を付与	リスト			
DescribeBackups	単一のバックアップ、指定したサーバーのすべてのバックアップ、またはユーザーのアカウントのすべてのバックアップを記述するためのアクセス許可を付与	リスト			
DescribeEvents	指定したサーバーのすべてのイベントを記述するためのアクセス許可を付与	リスト			
DescribeNodeAssociationStatus	指定されたノードトークンと指定されたサーバーの関連付けステータスを記述するためのアクセス許可を付与	リスト			
DescribeServers	指定したサーバーまたはユーザーアカウントのすべてのサーバーを記述するためのアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisassociateNode	サーバーから指定されたノードの関連付けを解除するためのアクセス許可を付与	Write			
ExportServerEngineAttribute	サーバーからエンジン属性をエクスポートするためのアクセス許可を付与	Read			
ListTagsForResource	指定したサーバーまたはバックアップに適用されているタグを一覧表示するためのアクセス許可を付与	Read			
RestoreServer	指定されたサーバーにバックアップを適用するためのアクセス許可を付与 指定されている場合は、ec2-instance をスワップアウトする可能性があります	Write			
StartMaintenance	サーバーのメンテナンスをすぐに開始するためのアクセス許可を付与	Write			
TagResource	指定されたサーバーまたはバックアップにタグを適用するためのアクセス許可を付与	タグ付け			
UntagResource	指定されたサーバーまたはバックアップからタグを削除するためのアクセス許可を付与	タグ付け			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateServer	一般的なサーバー設定を更新するためのアクセス許可を付与	Write			
UpdateServerEngineAttributes	設定管理タイプに固有のサーバー設定を更新するためのアクセス許可を付与	Write			

AWS OpsWorks Configuration Management で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
server	`arn:${Partition}:opsworks-cm::${Account}:server/${ServerName}/${UniqueId}`	
backup	`arn:${Partition}:opsworks-cm::${Account}:backup/${ServerName}-{Date-and-Time-Stamp-of-Backup}`	

AWS OpsWorks Configuration Management の条件キー

OpsworksCM には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Organizations のアクション、リソース、および条件キー

AWS Organizations (サービスプレフィックス: `organizations`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Organizations で定義されるアクション
- AWS Organizations で定義されるリソースタイプ
- AWS Organizations の条件キー

AWS Organizations で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptHandshake	ハンドシェイクリクエストによって提案されたアクションに同意したハンドシェイクの発行者に応答を送信する許可を付与	書き込み	handshake*		iam:CreateServiceLinkedRole
AttachPolicy	ルート、組織単位、または個々のアカウントにポリシーをアタッチする許可を付与	書き込み	policy*		
			account		
			organizationalunit		
			root		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				organizations:PolicyType	
CancelHandshake	ハンドシェイクをキャンセルする許可を付与	書き込み	handshake*		
CloseAccount	組織内で作成されたか、組織に参加するように招待 AWS アカウント された、組織の一部になった を閉じるアクセス許可を付与します	書き込み	account*		
CreateAccount	リクエストを行った認証情報を使用して、自動的に組織のメンバー AWS アカウント である を作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateGovCloudAccount	AWS GovCloud (米国) アカウントを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateOrganization	組織を作成する許可を付与 CreateOrganization オペレーションを呼び出す認証情報を持つアカウントは、自動的に新しい組織の管理アカウントになります	書き込み			iam:CreateServiceLinkedRole
CreateOrganizationalUnit	ルートまたは親 OU 内に組織単位 (OU) を作成する許可を付与	書き込み	organizationalunit		
			root		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePolicy	ルート、組織単位 (OU)、または個人にアタッチできるポリシーを作成するアクセス許可を付与します AWS アカウント	書き込み		organizations:PolicyType aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeclineHandshake	ハンドシェイクリクエストを拒否する許可を付与 これにより、ハンドシェイクの状態が DECLINED に設定され、効果的にリクエストが非アクティブ化されます	書き込み	handshake*		
DeleteOrganization	組織を削除する許可を付与	書き込み			
DeleteOrganizationalUnit	ルートまたは別の OU から組織単位を削除する許可を付与	書き込み	organizationalunit*		
DeletePolicy	組織からポリシーを削除する許可を付与	書き込み	policy*		
				organizations:PolicyType	
DeleteResourcePolicy	組織からリソースポリシーを削除するための許可を付与します	書き込み			
DeregisterDelegatedAdministrator	ServicePrincipal によって指定された AWS サービスの委任管理者 AWS アカウント として指定されたメンバーの登録を解除するアクセス許可を付与します	書き込み	account*		
				organizations:ServicePrincipal	
DescribeAccount	指定したアカウントに関する Organizations 関連の詳細を取得する許可を付与	読み込み	account*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeCreateAccountStatus	アカウントを作成するための非同期リクエストの現在のステータスを取得する許可を付与	読み込み			
DescribeEffectivePolicy	アカウントの有効なポリシーを取得する許可を付与	読み込み	account*		
				organizations:PolicyType	
DescribeHandshake	以前にリクエストされたハンドシェイクに関する詳細を取得する許可を付与	読み取り	handshake*		
DescribeOrganization	呼び出し元の認証情報が属する組織に関する詳細を取得するアクセス許可を付与します	読み取り			
DescribeOrganizationalUnit	組織単位 (OU) の詳細を取得する許可を付与	読み取り	organizationalunit*		
DescribePolicy	ポリシーの詳細を取得するアクセス許可を付与します	読み取り	policy*		
				organizations:PolicyType	
DescribeResourcePolicy	リソースポリシーに関する情報を取得するための許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DetachPolicy	ターゲットのルート、組織単位、または個々のアカウントからポリシーをデタッチする許可を付与	書き込み	policy*		
			account		
			organizationalunit		
			root		
				organizations:PolicyType	
DisableAWSServiceAccess	AWS サービス (ServicePrincipal によって指定されたサービス) と AWS Organizations の統合を無効にするアクセス許可を付与します	書き込み		organizations:ServicePrincipal	
DisablePolicyType	ルートの組織ポリシータイプを無効にする許可を付与	書き込み	root*		
				organizations:PolicyType	
EnableAWSServiceAccess	AWS サービス (ServicePrincipal によって指定されたサービス) と AWS Organizations の統合を有効にするアクセス許可を付与します	書き込み		organizations:ServicePrincipal	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
EnableAllFeatures	一括請求機能のみをサポートする設定からアップグレードするために、組織内のすべての機能を有効にするプロセスを開始する許可を付与	書き込み			
EnablePolicyType	ルートのポリシータイプを有効にする許可を付与	書き込み	root*		
				organizations:PolicyType	
InviteAccountToOrganization	別の に招待を送信し AWS アカウント、メンバーアカウントとして組織に参加するように依頼するアクセス許可を付与します	書き込み	account		
				aws:RequestTag/${TagKey} aws:TagKeys	
LeaveOrganization	親組織からメンバーアカウントを削除する許可を付与	書き込み			
ListAWSServiceAccessForOrganization	組織との統合を有効にした AWS サービスのリストを取得するアクセス許可を付与します	リスト			
ListAccounts	組織内のすべてのアカウントを一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListAccountsForParent	ルートまたは組織単位 (OU) に含まれる組織内のアカウントを一覧表示する許可を付与	リスト	organizationalunit		
			root		
ListChildren	親 OU またはルートに含まれるすべての OU またはアカウントを一覧表示する許可を付与	リスト	organizationalunit		
			root		
ListCreateAccountStatus	現在組織で追跡中の非同期アカウント作成リクエストを一覧表示する許可を付与	リスト			
ListDelegatedAdministrators	この組織で委任管理者として指定されている AWS アカウントを一覧表示するアクセス許可を付与します	リスト		organizations:ServicePrincipal	
ListDelegatedServicesForAccount	指定されたアカウントがこの組織の委任管理者である AWS サービスを一覧表示するアクセス許可を付与します	リスト	account*		
ListHandshakesForAccount	アカウントに関連付けられているすべてのハンドシェイクを一覧表示する許可を付与	リスト			
ListHandshakesForOrganization	組織に関連付けられているハンドシェイクを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListOrganizationalUnitsForParent	親組織単位またはルート内のすべての組織単位 (OUs) を一覧表示するアクセス許可を付与します	リスト	organizationalunit		
			root		
ListParents	子 OU またはアカウントの直接の親として機能するルートまたは組織単位 (OU) を一覧表示する許可を付与	リスト	account		
			organizationalunit		
ListPolicies	組織内のすべてのポリシーを一覧表示する許可を付与	リスト		organizations:PolicyType	
ListPoliciesForTarget	ルート、組織単位 (OU)、またはアカウントに直接アタッチされているすべてのポリシーを一覧表示する許可を付与	リスト	account		
			organizationalunit		
			root		
				organizations:PolicyType	
ListRoots	組織内で定義されているすべてのルートを一覧表示する許可を付与	リスト			
ListTagsForResource	指定したリソースのすべてのタグを一覧表示する許可を付与	リスト	account		
			organizationalunit		
			policy		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			resourcepolicy		
			root		
ListTargetsForPolicy	ポリシーがアタッチされているすべてのルーツ、OU、およびアカウントを一覧表示する許可を付与	リスト	policy*		
				organizations:PolicyType	
MoveAccount	アカウントを現在のルートまたは OU から別の親ルートまたは OU に移動する許可を付与	書き込み	account*		
			organizationalunit*		
			root*		
PutResourcePolicy	リソースポリシーを作成または更新する許可を付与します。	書き込み	resourcepolicy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RegisterDelegatedAdministrator	ServicePrincipal によって指定された AWS サービスの Organizations 機能を管理するために、指定されたメンバーアカウントを登録するアクセス許可を付与します	書き込み	account*		
				organizations:ServicePrincipal	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RemoveAccountFromOrganization	指定されたアカウントを組織から削除するアクセス許可を付与します	書き込み	account*		
TagResource	指定されたリソースに 1 つ以上のタグを追加する権限を付与します	タグ付け	account		
			organizationalunit		
			policy	organizations:PolicyType	
			resourcepolicy		
			root		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	指定されたリソースから 1 つ以上のタグを削除する権限を付与します	Tagging	account		
			organizationalunit		
			policy		
			resourcepolicy		
			root		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:TagKeys	
UpdateOrganizationalUnit	組織単位 (OU) の名前を変更する許可を付与します	書き込み	organizationalunit*		
UpdatePolicy	既存のポリシーを新しい名前、説明、またはコンテンツで更新する許可を付与します	書き込み	policy*		
				organizations:PolicyType	

AWS Organizations で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource 工レメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
account	arn:${Partition}:organizations::${Account}:account/o-${OrganizationId}/${AccountId}	aws:ResourceTag/${TagKey}
handshake	arn:${Partition}:organizations::${Account}:handshake/o-${OrganizationId}/${HandshakeType}/h-${HandshakeId}	

リソースタイプ	ARN	条件キー
organization	arn:${Partition}:organizations::${Account}:organization/o-${OrganizationId}	
organizationalunit	arn:${Partition}:organizations::${Account}:ou/o-${OrganizationId}/ou-${OrganizationalUnitId}	aws:ResourceTag/${TagKey}
policy	arn:${Partition}:organizations::${Account}:policy/o-${OrganizationId}/${PolicyType}/p-${PolicyId}	aws:ResourceTag/${TagKey}
resourcepolicy	arn:${Partition}:organizations::${Account}:resourcepolicy/o-${OrganizationId}/rp-${ResourcePolicyId}	aws:ResourceTag/${TagKey}
awspolicy	arn:${Partition}:organizations::aws:policy/${PolicyType}/p-${PolicyId}	
root	arn:${Partition}:organizations::${Account}:root/o-${OrganizationId}/r-${RootId}	aws:ResourceTag/${TagKey}

AWS Organizations の条件キー

AWS Organizations では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
organizations:PolicyType	指定したポリシータイプ名でアクセスをフィルタリングする	String
organizations:ServicePrincipal	指定したサービスプリンシパル名でアクセスをフィルタリングする	String

AWS Outposts のアクション、リソース、および条件キー

AWS Outposts (サービスプレフィックス: outposts) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Outposts で定義されるアクション
- AWS Outposts で定義されるリソースタイプ
- AWS Outposts の条件キー

AWS Outposts で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelCapacityTask	キャパシティタスクをキャンセルするアクセス許可を付与します	書き込み	outpost*		
CancelOrder	注文をキャンセルする許可を付与	書き込み			
CreateOrder	順序を作成する許可を付与します。	書き込み	outpost*		
CreateOutpost	Outpost を作成する許可を付与	書き込み	site*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreatePrivateConnectivityConfig	プライベート接続設定を作成するアクセス許可を付与します	書き込み	outpost*		
CreateSite	サイトを作成する許可を付与します。	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
DeleteOutpost	Outpost を削除する許可を付与	書き込み	outpost*		
DeleteSite	サイトを削除する許可を付与	書き込み	site*		
GetCapacityTask	指定されたキャパシティタスクに関する情報を取得するアクセス許可を付与します	読み取り	outpost*		
GetCatalogItem	カタログ項目を取得する許可を付与	読み取り			
GetConnection	Outpost サーバーの接続に関する情報を取得する許可を付与	読み取り			
GetOrder	オーダーに関する情報を取得する許可を付与	読み取り			
GetOutpost	指定された Outpost に関する情報を取得する許可を付与。	読み取り	outpost*		
GetOutpostBillingInformation	指定された Outpost の Outpost 請求情報を取得する許可を付与	読み取り	outpost*		
GetOutpostInstanceTypes	指定された Outpost のインスタンスタイプを取得する許可を付与	読み取り	outpost*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetOutpostSupportedInstanceTypes	指定された Outpost のサポートされたインスタンスタイプを取得する許可を付与する	読み取り	outpost*		
GetPrivateConnectivityConfig	プライベート接続設定を取得するアクセス許可を付与します	読み取り	outpost*		
GetSite	サイト を取得するためのアクセス許可を付与します。	読み取り	site*		
GetSiteAddress	サイトアドレスを取得する許可を付与	読み取り	site*		
ListAssetInstances	指定された Outpost で実行中のすべてのインスタンスを一覧表示するアクセス許可を付与します	リスト	outpost*		
ListAssets	Outpost のアセットを一覧表示する許可を付与する	リスト	outpost*		
ListBlockingInstancesForCapacityTask	指定された Outpost に対してキャパシティタスクの実行をブロックしている実行中のすべてのインスタンスを一覧表示するアクセス許可を付与します	リスト	outpost*		
ListCapacityTasks	のキャパシティタスクを一覧表示するアクセス許可を付与します AWS アカウント	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListCatalogItems	すべてのカタログ項目を一覧表示する許可を付与	リスト			
ListOrders	の注文を一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListOutposts	の Outposts を一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListSites	のサイトを一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り			
StartCapacityTask	キャパシティタスクを作成するアクセス許可を付与します	書き込み	outpost*		
StartConnection	Outpost サーバーへの接続を開始する許可を付与	書き込み			
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	outpost		
			site		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	リソースのタグを解除する許可を付与	Tagging	outpost		
			site		
				aws:TagKeys	
UpdateOutpost	Outpost を更新する許可を付与	書き込み	outpost*		
UpdateSite	サイトを更新する許可を付与	書き込み	site*		
UpdateSiteAddress	サイトアドレスを更新する許可を付与	書き込み	site*		
UpdateSiteRackPhysicalProperties	サイトのラックの物理プロパティを更新する許可を付与	書き込み	site*		

AWS Outposts で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
outpost	`arn:${Partition}:outposts:${Region}:${Account}:outpost/${OutpostId}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
site	arn:${Partition}:outposts:${Region}:${Account}:site/${SiteId}	aws:ResourceTag/${TagKey}

AWS Outposts の条件キー

AWS Outposts は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Panorama のアクション、リソース、および条件キー

AWS Panorama (サービスプレフィックス: panorama) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Panorama で定義されるアクション
- AWS Panorama で定義されるリソースタイプ
- AWS Panorama の条件キー

AWS Panorama で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateApplicationInstance	AWS Panorama アプリケーションインスタンスを作成するアクセス許可を付与します	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateJobForDevices	AWS Panorama アプライアンスのジョブを作成するアクセス許可を付与します	書き込み			
CreateNodeFromTemplateJob	AWS Panorama ノードを作成するアクセス許可を付与します	書き込み			
CreatePackage	AWS Panorama パッケージを作成するアクセス許可を付与します	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreatePackageImportJob	AWS Panorama パッケージを作成するアクセス許可を付与します	書き込み			
DeleteDevice	AWS Panorama アプライアンスの登録を解除する許可を付与	書き込み	device*		
DeletePackage	AWS Panorama パッケージを削除するアクセス許可を付与します	書き込み	package*		
DeregisterPackageVersion	AWS Panorama パッケージバージョンの登録を解除する許可を付与	書き込み	package*		
DescribeApplicationInstance	AWS Panorama アプリケーションインスタンスの詳細を表示するアクセス許可を付与します	読み取り	applicationInstance*		
DescribeApplicationInstanceDetails	AWS Panorama アプリケーションインスタンスの詳細を表示するアクセス許可を付与します	読み取り	applicationInstance*		
DescribeDevice	AWS Panorama アプライアンスの詳細を表示するアクセス許可を付与します	読み取り	device*		
DescribeDeviceJob	AWS Panorama アプライアンスのジョブの詳細を表示するアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeNode	AWS Panorama アプリケーションノードの詳細を表示するアクセス許可を付与します	読み取り			
DescribeNodeFromTemplateJob	AWS Panorama アプリケーションノードの詳細を表示するアクセス許可を付与します	読み取り			
DescribePackage	AWS Panorama パッケージの詳細を表示するアクセス許可を付与します	読み取り	package*		
DescribePackageImportJob	AWS Panorama パッケージの詳細を表示するアクセス許可を付与します	読み取り			
DescribePackageVersion	AWS Panorama パッケージバージョンの詳細を表示するアクセス許可を付与します	読み取り	package*		
DescribeSoftware [許可のみ]	AWS Panorama アプライアンスのソフトウェアバージョンに関する詳細を表示するアクセス許可を付与します	読み取り			
GetWebSocketURL [許可のみ]	AWS Panorama との通信用に WebSocket エンドポイントを生成するアクセス許可を付与します	読み取り			
ListApplicationInstanceDependencies	AWS Panorama でアプリケーションインスタンスの依存関係のリストを取得する許可を付与	リスト	applicationInstance*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListApplicationInstanceNodeInstances	AWS Panorama のアプリケーションインスタンスのノードインスタンスのリストを取得するアクセス許可を付与します	リスト	applicationInstance*		
ListApplicationInstances	AWS Panorama のアプリケーションインスタンスのリストを取得するアクセス許可を付与します	リスト	device		
ListDevices	AWS Panorama でアプライアンスのリストを取得するアクセス許可を付与します	リスト			
ListDevicesJobs	AWS Panorama アプライアンスのジョブのリストを取得するアクセス許可を付与します	リスト	device		
ListNodeFromTemplateJobs	AWS Panorama アプライアンスのノードのリストを取得するアクセス許可を付与します	リスト			
ListNodes	AWS Panorama のノードのリストを取得するアクセス許可を付与します	リスト			
ListPackageImportJobs	AWS Panorama でパッケージのリストを取得する許可を付与	リスト			
ListPackages	AWS Panorama でパッケージのリストを取得する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTagsForResource	AWS Panorama のリソースのタグのリストを取得するアクセス許可を付与します	読み取り	applicationInstance		
			device		
			package		
ProvisionDevice	AWS Panorama アプライアンスを登録する許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
RegisterPackageVersion	AWS Panorama パッケージバージョンを登録する許可を付与	書き込み	package*		
RemoveApplicationInstance	AWS Panorama アプリケーションインスタンスを削除するアクセス許可を付与します	書き込み	applicationInstance*		
SignalApplicationInstanceNodeInstances	アプリケーションインスタンス内のカメラノードに信号を送信して、一時停止または再開するための許可を付与します	書き込み	applicationInstance*		
TagResource	AWS Panorama のリソースにタグを追加する許可を付与	Tagging	applicationInstance		
			device		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			package		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	AWS Panorama のリソースからタグを削除する許可を付与	Tagging	applicationInstance		
			device		
			package		
				aws:TagKeys	
UpdateDeviceMetadata	AWS Panorama アプライアンスの基本設定を変更するアクセス許可を付与します	書き込み	device*		

AWS Panorama で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
device	arn:${Partition}:panorama:${Region}:${Account}:device/${DeviceId}	aws:ResourceTag/${TagKey}
package	arn:${Partition}:panorama:${Region}:${Account}:package/${PackageId}	aws:ResourceTag/${TagKey}
applicationInstance	arn:${Partition}:panorama:${Region}:${Account}:applicationInstance/${ApplicationInstanceId}	aws:ResourceTag/${TagKey}

AWS Panorama の条件キー

AWS Panorama では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS パラレルコンピューティングサービスのアクション、リソース、および条件キー

AWS Parallel Computing Service (サービスプレフィックス: pcs) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS パラレルコンピューティングサービスで定義されるアクション
- AWS パラレルコンピューティングサービスで定義されるリソースタイプ
- AWS パラレルコンピューティングサービスの条件キー

AWS パラレルコンピューティングサービスで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイ

プが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AllowVendedLogDeliveryForResource [アクセス許可のみ]	AWS PCS クラスターログの供給ログ配信を設定するアクセス許可を付与します	書き込み	cluster*		
CreateCluster	クラスターを作成する許可を付与する	書き込み		aws:ResourceTag/${TagKey}	ec2:CreateNetworkInterface

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateNetworkInterfacePermission ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:GetSecurityGroupsForVpc iam:CreateServiceLinkedRole secretsmanager:CreateSecret

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					secretsmanager:TagResource

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateComputeNodeGroup	コンピューティングノードグループを作成する許可を付与する	書き込み	cluster*		ec2:CreateFleet ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateTags ec2:DescribeImages ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:RunInstances iam:GetInstanceProfile iam:PassRole
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateQueue	キューを作成する許可を付与する	書き込み	cluster*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCluster	クラスターを削除する許可を付与する	書き込み	cluster*		ec2:DeleteNetworkInterface secretsmanager:DeleteSecret
DeleteComputeNodeGroup	コンピューティングノードグループを削除する許可を付与する	書き込み	cluster*		ec2:DeleteLaunchTemplate ec2:TerminateInstances
			computenodegroup*		
DeleteQueue	キューを削除する許可を付与する	書き込み	cluster*		
			queue*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetCluster	クラスターのプロパティを取得する許可を付与する	読み取り	cluster*		
GetComputeNodeGroup	コンピューティングノードグループのプロパティを取得する許可を付与する	読み取り	cluster*		
			computenodegroup*		
GetQueue	キューのプロパティを取得する許可を付与する	読み取り	cluster*		
			queue*		
ListClusters	クラスターを一覧表示するためのアクセス許可を付与	リスト			
ListComputeNodeGroups	コンピューティングノードグループを一覧表示する許可を付与する	リスト	cluster*		
ListQueues	キューを一覧表示する許可を付与する	リスト	cluster*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り			
RegisterComputeNodeGroupInstance	コンピューティングノードグループにコンピューティングインスタンスを登録する許可を付与する	書き込み	cluster*		secretsmanager:GetSecretValue
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	cluster	aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			computenodegroup	aws:ResourceTag/${TagKey}	
			queue	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースのタグを解除する許可を付与	Tagging	cluster	aws:ResourceTag/${TagKey}	
			computenodegroup	aws:ResourceTag/${TagKey}	
			queue	aws:ResourceTag/${TagKey}	
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateComputeNodeGroup	コンピューティングノードグループのプロパティを更新する許可を付与する	書き込み	cluster*		ec2:CreateFleet ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateTags ec2:DescribeImages ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:RunInstances iam:GetInstanceProfile iam:PassRole
			computenodegroup*		
UpdateQueue	キューのプロパティを更新する許可を付与する	書き込み	cluster*		
			queue*		

AWS パラレルコンピューティングサービスで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
cluster	arn:${Partition}:pcs:${Region}:${Account}:cluster/${ClusterIdentifier}	aws:ResourceTag/${TagKey}
computenodegroup	arn:${Partition}:pcs:${Region}:${Account}:cluster/${ClusterIdentifier}/computenodegroup/${ComputeNodeGroupIdentifier}	aws:ResourceTag/${TagKey}
queue	arn:${Partition}:pcs:${Region}:${Account}:cluster/${ClusterIdentifier}/queue/${QueueIdentifier}	aws:ResourceTag/${TagKey}

AWS パラレルコンピューティングサービスの条件キー

AWS Parallel Computing Service では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列

条件キー	説明	タイプ
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS パートナーセントラルのアカウント管理用のアクション、リソース、および条件キー

AWS Partner Central Account Management (サービスプレフィックス: `partnercentral-account-management`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS パートナーセントラルのアカウント管理によって定義されているアクション
- AWS パートナーセントラルのアカウント管理によって定義されているリソースタイプ
- AWS パートナーセントラルのアカウント管理用の条件キー

AWS パートナーセントラルのアカウント管理によって定義されているアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーショ

ンへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociatePartnerAccount [アクセス許可のみ]	パートナーアカウントを に関連付けるアクセス許可を付与します AWS アカウント	書き込み			
AssociatePartnerUser	パートナーユーザーを IAM ロールに関連付ける許可を付与	書き込み			
DisassociatePartnerUser	パートナーユーザーの IAM ロールへの関連付けを解除する許可を付与	書き込み			

AWS パートナーセントラルのアカウント管理によって定義されているリソースタイプ

AWS パートナーセントラルアカウント管理では、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定はサポートされていません。 AWS パートナーセントラルのアカウント管理へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS パートナーセントラルのアカウント管理用の条件キー

パートナーセントラルのアカウント管理には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーがありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Partner Central Selling のアクション、リソース、および条件キー

AWS Partner Central Selling (サービスプレフィックス: `partnercentral`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Partner Central Selling で定義されるアクション
- AWS Partner Central Selling で定義されるリソースタイプ
- AWS Partner Central Selling の条件キー

AWS Partner Central Selling で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptEngagementInvitation	AWS Partner Central でエンゲージメント招待を受け入れるアクセス許可を付与します	書き込み	engagement-invitation*		
				partnercentral:Catalog	
AssignOpportunity	AWS Partner Central に Opportunities を割り当てるアクセス許可を付与します	書き込み	Opportunity*		
				partnercentral:Catalog	
AssociateOpportunity	AWS Partner Central の Opportunities を他のエンティティに関連付けるアクセス許可を付与します	書き込み	Opportunity*		
				partnercentral:Catalog	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				partnercentral:RelatedEntityType	
CreateEngagement	AWS Partner Central でエンゲージメントを作成するアクセス許可を付与します	書き込み	Engagement*		
				partnercentral:Catalog	
CreateEngagementInvitation	AWS Partner Central でエンゲージメントの招待を作成するアクセス許可を付与します	書き込み	engagement-invitation*		
				partnercentral:Catalog	
CreateOpportunity	AWS Partner Central で新しい Opportunities を作成するアクセス許可を付与します	書き込み	Opportunity*		
				aws:RequestTag/${TagKey} aws:TagKeys partnercentral:Catalog	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateResourceSnapshot	AWS Partner Central でリソーススナップショットを作成する許可を付与	書き込み	ResourceSnapshot*		
				partnercentral:Catalog	
CreateResourceSnapshotJob	AWS Partner Central でリソーススナップショットジョブを作成するアクセス許可を付与します	書き込み	resource-snapshot-job*		
				aws:RequestTag/${TagKey} aws:TagKeys partnercentral:Catalog	
DeleteResourceSnapshotJob	AWS Partner Central でリソーススナップショットジョブを削除する許可を付与	書き込み	resource-snapshot-job*		
				partnercentral:Catalog	
DisassociateOpportunity	AWS Partner Central の Opportunities と他のエンティティの関連付けを解除するアクセス許可を付与します	書き込み	Opportunity*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				partnercentral:Catalog partnercentral:RelatedEntityType	
GetAwsOpportunitySummary	AWS Partner Central AWS で Opportunities の機会概要を取得する許可を付与	読み取り	Opportunity*		
				partnercentral:Catalog	
GetEngagement	AWS Partner Central でエンゲージメントの詳細を取得する許可を付与	読み取り	Engagement*		
				partnercentral:Catalog	
GetEngagementInvitation	AWS Partner Central でエンゲージメント招待の詳細を取得するアクセス許可を付与します	読み取り	engagement-invitation*		
				partnercentral:Catalog	
GetOpportunity	AWS Partner Central で Opportunities の詳細を取得するアクセス許可を付与します	読み取り	Opportunity*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				partnercentral:Catalog	
GetResourceSnapshot	AWS Partner Central でリソーススナップショットの詳細を取得する許可を付与	読み取り	ResourceSnapshot*		
				partnercentral:Catalog	
GetResourceSnapshotJob	AWS Partner Central でリソーススナップショットジョブの詳細を取得する許可を付与	読み取り	resource-snapshot-job*		
				partnercentral:Catalog	
GetSellingSystemSettings	AWS Partner Central でシステム設定を取得する許可を付与	読み取り		partnercentral:Catalog	
ListEngagementByAcceptingInvitationTasks	AWS Partner Central で招待タスクを受け入れてエンゲージメントを一覧表示する許可を付与	リスト		partnercentral:Catalog	
ListEngagementFromOpportunityTasks	AWS Partner Central のオポチュニティタスクからエンゲージメントを一覧表示する許可を付与	リスト		partnercentral:Catalog	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListEngagementInvitations	AWS Partner Central でエンゲージメント招待を一覧表示する許可を付与	リスト		partnercentral:Catalog	
ListEngagementMembers	AWS Partner Central でエンゲージメントメンバーを一覧表示するアクセス許可を付与します	読み取り	Engagement*		
				partnercentral:Catalog	
ListEngagementResourceAssociations	AWS Partner Central でエンゲージメントリソースの関連付けを一覧表示する許可を付与	読み取り	ResourceSnapshot*		
				partnercentral:Catalog	
ListEngagements	AWS Partner Central でエンゲージメントを一覧表示する許可を付与	リスト		partnercentral:Catalog	
ListOpportunities	AWS Partner Central で Opportunities を一覧表示する許可を付与	リスト		partnercentral:Catalog	
ListResourceSnapshotJobs	AWS Partner Central でリソーススナップショットジョブを一覧表示する許可を付与	リスト		partnercentral:Catalog	
ListResourceSnapshots	AWS Partner Central でリソーススナップショットを一覧表示する許可を付与	読み取り	ResourceSnapshot*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				partnercentral:Catalog	
ListSolutions	AWS Partner Central でソリューションを一覧表示するアクセス許可を付与します	リスト		partnercentral:Catalog	
ListTagsForResource	リソースにリストタグを追加するアクセス許可を付与します。サポートされているリソース: ResourceSnapshotJob	読み取り		aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
PutSellingSystemSettings	AWS Partner Central にシステム設定を配置するアクセス許可を付与します	書き込み			
RejectEngagementInvitation	AWS Partner Central でエンゲージメントの招待を拒否するアクセス許可を付与します	書き込み	engagement-invitation*		
				partnercentral:Catalog	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartEngagementByAcceptingInvitationTask	エンゲージメント招待を受け入れて AWS Partner Central でエンゲージメントを開始するタスクを開始するアクセス許可を付与します	書き込み	engagement-by-accepting-invitation-task*		partnercentral:AcceptEngagementInvitation partnercentral:CreateOpportunity partnercentral:CreateResourceSnapshotJob partnercentral:GetEngagementInvitation partnercentral:StartResourceSnapshotJob partnercentral:SubmitOpportunity

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartEngagementFromOpportunityTask	AWS Partner Central の Opportunities からエンゲージメントを開始するタスクを開始するアクセス許可を付与します	書き込み	engagement-from-opportunity-task*		partnercentral:CreateEngagement partnercentral:CreateEngagementInvitation partnercentral:CreateResourceSnapshotJob partnercentral:GetOpportunity partnercentral:StartResourceSnapshotJob partnercentral:SubmitOpportunity

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
StartResourceSnapshotJob	AWS Partner Central でリソーススナップショットジョブを開始する許可を付与	書き込み	resource-snapshot-job*		
				partnercentral:Catalog	
StopResourceSnapshotJob	AWS Partner Central でリソーススナップショットジョブを停止する許可を付与	書き込み	resource-snapshot-job*		
				partnercentral:Catalog	
SubmitOpportunity	AWS Partner Central で Opportunities を送信する許可を付与	書き込み	Opportunity*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				partnercentral:Catalog	
TagResource	リソースに新しいタグを追加するアクセス許可を付与します。サポートされているリソース: ResourceSnapshotJob	Tagging	Opportunity		
			resource-snapshot-job		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
UntagResource	リソースからタグを削除するアクセス許可を付与します。サポートされているリソース: ResourceSnapshotJob	Tagging	Opportunity		
			resource-snapshot-job		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
UpdateOpportunity	AWS Partner Central で Opportunities を更新する許可を付与	書き込み	Opportunity*		
				partnercentral:Catalog	

AWS Partner Central Selling で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Engagement	arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/engagement/${Identifier}	

リソースタイプ	ARN	条件キー
engagement-by-accepting-invitation-task	arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/engagement-by-accepting-invitation-task/${TaskId}	
engagement-from-opportunity-task	arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/engagement-from-opportunity-task/${TaskId}	
engagement-invitation	arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/engagement-invitation/${Identifier}	
Opportunity	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/opportunity/${Identifier}	aws:ResourceTag/${TagKey}
resource-snapshot-job	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/resource-snapshot-job/${Identifier}	aws:ResourceTag/${TagKey}
ResourceSnapshot	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/engagement/${EngagementIdentifier}/resource/${ResourceType}/${ResourceIdentifier}/template/${TemplateIdentifier}/resource-snapshot/${SnapshotRevision}	
Solution	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/solution/${Identifier}	

AWS Partner Central Selling の条件キー

AWS Partner Central Selling では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
partnercentral:Catalog	特定のカタログでアクセスをフィルタリングします。使用できる値: [AWS、サンドボックス〕	String
partnercentral:RelatedEntityType	オポチュニティの関連付けのためにエンティティタイプでアクセスをフィルタリングします。使用できる値: [Solutions、AwsProducts、AwsMarketplaceOffers]	String

AWS Payment Cryptography のアクション、リソース、および条件キー

AWS Payment Cryptography (サービスプレフィックス: payment-cryptography) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Payment Cryptography によって定義されているアクション
- AWS Payment Cryptography で定義されるリソースタイプ
- AWS Payment Cryptography の条件キー

AWS Payment Cryptography によって定義されているアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateAlias	キーにわかりやすい名前を作成するアクセス許可を付与します	書き込み	alias*		
			key*		
CreateKey	発信者の AWS アカウント およびリージョンに一意のカスタマーマネージドキーを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	payment-cryptography:TagResource
DecryptData	対称、非対称、または DUKPT データ暗号化キーを使用して、暗号テキストデータをプレーンテキストに復号化する許可を付与します	書き込み	alias*		
			key*		
DeleteAlias	指定された エイリアスを削除するアクセス許可を付与	書き込み	alias*		
				aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
DeleteKey	キーの削除をスケジュールするアクセス許可を付与します。	書き込み	key*		
EncryptData	対称、非対称、または DUKPT データ暗号化キーを使用して、プレーンテキストデータを暗号テキストに暗号化する許可を付与します	書き込み	alias*		
			key*		
ExportKey	サービスからキーをエクスポートする許可を付与します	書き込み	key*		
GenerateCardValidationData	磁気ストライプカードの有効性をチェックする、カード検証値 (CVV/CVV2)、動的カード検証値 (dCVV/dCVV2)、カードセキュリティコード (CSC) などのアルゴリズムを使用して、カード関連データを生成するアクセス許可を付与します	書き込み	alias*		
			key*		
GenerateMac	MAC (メッセージ認証コード) 暗号文を生成するアクセス許可を付与します	書き込み	alias*		
			key*		
GenerateMacEmvPinChange	MAC (メッセージ認証コード) 暗号文を生成するアクセス許可を付与します	書き込み	alias*		
			key*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GeneratePinData	新規カード発行またはカード再発行時に、PIN、PIN 検証値 (PVV)、PIN ブロック、PIN オフセットなどの PIN 関連データを生成する許可を付与します	書き込み	alias*		
			key*		
GetAlias	aliasName に関連付けられた keyArn を返すアクセス許可を付与します	読み取り	alias*		
			key*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetKey	指定されたキーに関する詳細情報を返すアクセス許可を付与します	読み取り	key*		
GetParametersForExport	TR-34 キーエクスポートを開始するためのエクスポートトークンと署名キー証明書を取得する許可を付与します	読み取り			
GetParametersForImport	TR-34 キーのインポートを開始するためのインポートトークンとラッピングキー証明書を取得する許可を付与します	読み取り			
GetPublicKeyCertificate	PUBLIC_KEY クラスのキーからパブリックキーを返すアクセス許可を付与します	読み取り	key*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ImportKey	キーと公開キー証明書をインポートするアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	payment-cryptography:TagResource
ListAliases	発信者と AWS アカウントリージョンのすべてのキー用に作成されたエイリアスのリストを返すアクセス許可を付与します	リスト			
ListKeys	発信者の AWS アカウント およびリージョンで作成されたキーのリストを返すアクセス許可を付与します	リスト			
ListTagsForResource	発信者の AWS アカウント およびリージョンで作成されたタグのリストを返すアクセス許可を付与します	読み取り	key		
ReEncryptData	DUKPT、対称および非対称データ暗号化キーを使用して暗号文を再暗号化するアクセス許可を付与します	書き込み	alias* key*		
RestoreKey	待機期間中にキーを復活させる必要が生じた場合に、予定されていたキー削除をキャンセルするアクセス許可を付与します。	書き込み	key*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartKeyUsage	無効になっているキーを有効にするアクセス許可を付与します	書き込み	key*		
StopKeyUsage	有効になっているキーを無効にするアクセス許可を付与します	書き込み	key*		
TagResource	指定したリソースの 1 つ以上のタグを追加または上書きするアクセス許可を付与します	Tagging	key*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TranslatePinData	暗号化された PIN ブロックを ISO 9564 形式 0,1,3,4 から、および ISO 9564 形式 0,1,3,4 へ変換するアクセス許可を付与します	書き込み	alias*		
			key*		
UntagResource	指定されたリソースから指定されたタグを削除するアクセス許可を付与します	Tagging	key*		
				aws:TagKeys	
UpdateAlias	エイリアスが割り当てられているキーを変更したり、現在のキーから割り当てを解除したりする許可を付与します	書き込み	alias*		
			key*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
VerifyAuthRequestCryptogram	EMV チップ決済カード認可用の認可リクエストクリプトグラム (ARQC) を検証するアクセス許可を付与します	書き込み	alias*		
			key*		
VerifyCardValidationData	カード検証値 (CVV/CVV2)、動的カード検証値 (dCVV/dCVV2)、カードセキュリティコード (CSC) などのアルゴリズムを使用して、カード関連の検証データを検証する許可を付与します	書き込み	alias*		
			key*		
VerifyMac	提供された MAC に対して入力データの MAC (メッセージ認証コード) を検証する許可を付与します	書き込み	alias*		
			key*		
VerifyPinData	VISA PVV や IBM3624 などのアルゴリズムを使用して、PIN や PIN オフセットなどのピン関連データを検証する許可を付与します	書き込み	alias*		
			key*		

AWS Payment Cryptography で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
key	arn:${Partition}:payment-cryptography:${Region}:${Account}:key/${KeyId}	aws:ResourceTag/${TagKey} payment-cryptography:ResourceAliases
alias	arn:${Partition}:payment-cryptography:${Region}:${Account}:alias/${Alias}	payment-cryptography:ResourceAliases

AWS Payment Cryptography の条件キー

AWS Payment Cryptography では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	指定された操作のリクエストでタグのキーと値の両方によりアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	指定された操作のキーに割り当てられたタグによりアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
aws:TagKeys	指定された操作のリクエストで、タグキーによりアクセスをフィルタリングします	ArrayOfString
payment-cryptography:CertificateAuthorityPublicKeyIdentifier	リクエストで指定された CertificateAuthorityPublicKeyIdentifier、または ImportKey、および ExportKey 操作によりアクセスをフィルタリングします	String
payment-cryptography:ImportKeyMaterial	ImportKey 操作において、インポートされるキーマテリアルのタイプ [RootCertificatePublicKey、TrustedCertificatePublicKey、Tr34KeyBlock、Tr31KeyBlock] によってアクセスをフィルタリングします	String
payment-cryptography:KeyAlgorithm	CreateKey 操作のリクエストで指定された KeyAlgorithm によりアクセスをフィルタリングします	String
payment-cryptography:KeyClass	CreateKey 操作のリクエストで指定された KeyClass でアクセスをフィルタリングします	String
payment-cryptography:KeyUsage	リクエストで指定された、または CreateKey 操作のキーに関連付けられた KeyClass でアクセスをフィルタリングします	String
payment-cryptography:RequestAlias	指定された操作のリクエスト内のエイリアスでアクセスをフィルタリングします	String
payment-cryptography:ResourceAliases	指定された操作のキーに関連付けられたエイリアスによりアクセスをフィルタリングします	ArrayOfString

条件キー	説明	[Type] (タイプ)
payment-cryptography:WrappingKeyIdentifier	ImportKey および ExportKey 操作のリクエストで指定された WrappingKeyIdentifier でアクセスをフィルタリングします。	String

AWS 支払いのアクション、リソース、および条件キー

AWS 支払い (サービスプレフィックス: payments) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS 支払いで定義されるアクション
- AWS 支払いで定義されるリソースタイプ
- AWS 支払いの条件キー

AWS 支払いで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にア

クションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptFinancingApplicationTerms	レンダーが提供する資金調達申請条件を受け入れる許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateFinancingApplication	資金調達アプリケーションを作成するアクセス許可を付与します	書き込み			
CreatePaymentInstrument	支払い方法を作成するアクセス許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
DeletePaymentInstrument [アクセス許可のみ]	支払い方法を削除するアクセス許可を付与	書き込み			
GetFinancingApplication	資金調達アプリケーションに関する情報を取得する許可を付与	読み取り			
GetFinancingLine	資金調達ラインに関する情報を取得する許可を付与	読み取り			
GetFinancingLineWithdrawal	資金調達ラインの引き出しに関する情報を取得するアクセス許可を付与します	読み取り			
GetFinancingOption	資金調達オプションに関する情報を取得する許可を付与	読み取り			
GetPaymentInstrument	支払い方法に関する情報を取得するアクセス許可を付与	リスト	payment-instrument		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetPaymentStatus [許可のみ]	請求書の支払い状況を取得するアクセス許可を付与	読み取り			
ListFinancingApplications	資金調達アプリケーションメタデータを一覧表示する許可を付与	リスト			
ListFinancingLineWithdrawals	資金調達ラインリダクションメタデータを一覧表示するアクセス許可を付与します	リスト			
ListFinancingLines	資金調達ラインメタデータを一覧表示する許可を付与	リスト			
ListPaymentInstruments [許可のみ]	支払い手段メタデータを一覧表示する許可を付与する	リスト			
ListPaymentPreferences [許可のみ]	支払い設定（優先支払い通貨、優先支払い方法など）を取得するアクセス許可を付与	リスト			
ListPaymentProgramOptions	支払いオプションに関する情報を一覧表示するアクセス許可を付与します	リスト			
ListPaymentProgramStatus	支払いプログラムの適格性と登録ステータスに関する情報を一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTagsForResource	ペイメントリソースのタグを一覧表示する許可を付与する	リスト	payment-instrument		
MakePayment [許可のみ]	支払い、支払いの認証、支払い方法の検証、および前払いの資金請求書類の作成を行うアクセス許可を付与	書き込み			
TagResource	ペイメントリソースにタグを付ける許可を付与する	Tagging	payment-instrument		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	ペイメントリソースのタグを解除する許可を付与する	Tagging	payment-instrument		
				aws:TagKeys	
UpdateFinancingApplication	資金調達アプリケーションを更新する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdatePaymentInstrument [アクセス許可のみ]	支払い手段を更新する許可を付与する	書き込み			
UpdatePaymentPreferences [アクセス許可のみ]	支払い設定 (優先支払い通貨、優先支払い方法など) を更新するアクセス許可を付与	書き込み			

AWS 支払いで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource 工レメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
payment-instrument	`arn:${Partition}:payments::${Account}:payment-instrument:${ResourceId}`	aws:ResourceTag/${TagKey}

AWS 支払いの条件キー

AWS 支払いでは、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Performance Insights のアクション、リソース、および条件キー

AWS Performance Insights (サービスプレフィックス: pi) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Performance Insights で定義されるアクション
- AWS Performance Insights で定義されるリソースタイプ
- AWS Performance Insights の条件キー

AWS Performance Insights で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreatePerformanceAnalysisReport	CreatePerformanceAnalysisReport API を呼び出して、指定した DB インスタンスのパフォーマンス分析レポートを作成する許可を付与	書き込み	perf-reports-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePerformanceAnalysisReport	DeletePerformanceAnalysisReport API を呼び出して、指定した DB インスタンスのパフォーマンス分析レポートを削除する許可を付与	書き込み	perf-reports-resource*		
DescribeDimensionKeys	特定の期間にメトリクスの上位 N 個のディメンションキーを取得する DescribeDimensionKeys API を呼び出す許可を付与	読み取り	metric-resource*		
				pi:Dimensions	
GetDimensionKeyDetails	指定のディメンショングループの属性を取得する GetDimensionKeyDetails API を呼び出す許可を付与	読み取り	metric-resource*		
				pi:Dimensions	
GetPerformanceAnalysisReport	GetPerformanceAnalysisReport API を呼び出して、指定した DB インスタンスのパフォーマンス分析レポートを取得する許可を付与	読み取り	perf-reports-resource*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetResourceMetadata	各種機能のメタデータを取得する GetResourceMetadata API を呼び出す許可を付与	読み取り	metric-resource*		
GetResourceMetrics	一定期間中に一連のデータソースの PI メトリクスを取得する GetResourceMetrics API を呼び出す許可を付与	読み取り	metric-resource*		
				pi:Dimensions	
ListAvailableResourceDimensions	指定された DB インスタンスの指定された各メトリクスタイプに対してクエリ可能なディメンションを取得する ListAvailableResourceDimensions API を呼び出す許可を付与	読み取り	metric-resource*		
ListAvailableResourceMetrics	指定された DB インスタンスに対してクエリ可能な指定されたタイプのメトリクスを取得する ListAvailableResourceMetrics API を呼び出す許可を付与	読み取り	metric-resource*		
ListPerformanceAnalysisReports	ListPerformanceAnalysisReports API を呼び出して、指定した DB インスタンスのパフォーマンス分析レポートを一覧表示する許可を付与	リスト	perf-reports-resource*		
ListTagsForResource	ListTagsForResource API を呼び出してリソースのタグを一覧表示する許可を付与	リスト	perf-reports-resource*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagResource	TagResource API を呼び出してリソースにタグを付ける許可を付与	Tagging	perf-reports-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	UntagResource API を呼び出してリソースのタグを解除する許可を付与	Tagging	perf-reports-resource*		
				aws:TagKeys	

AWS Performance Insights で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
metric-resource	`arn:${Partition}:pi:${Region}:${Account}:metrics/${ServiceType}/${Identifier}`	

リソースタイプ	ARN	条件キー
perf-reports-resource	arn:${Partition}:pi:${Region}:${Account}:perf-reports/${ServiceType}/${Identifier}/${ReportId}	aws:ResourceTag/${TagKey}

AWS Performance Insights の条件キー

AWS Performance Insights では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
pi:Dimensions	リクエストされたディメンションでアクセスをフィルタリングする	ArrayOfString

Amazon Personalize のアクション、リソース、および条件キー

Amazon Personalize (サービスプレフィックス: personalize) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Personalize で定義されるアクション
- Amazon Personalize で定義されるリソースタイプ
- Amazon Personalize の条件キー

Amazon Personalize で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateBatchInferenceJob	バッチ推論ジョブを作成する許可を付与	書き込み	batchInferenceJob*		
CreateBatchSegmentJob	バッチセグメントジョブを作成するためのアクセス許可を付与します。	書き込み	batchSegmentJob*		
CreateCampaign	キャンペーンを作成する許可を付与	書き込み	campaign*		
CreateDataDeletionJob	データ削除ジョブを作成する許可を付与する	書き込み	dataDeletionJob*		
CreateDataInsightsJob	データインサイトジョブを作成するアクセス許可を付与	書き込み	dataInsightsJob*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateDataset	データセットを作成する許可を付与	書き込み	dataset*		
CreateDatasetExportJob	データセットエクスポートジョブを作成する許可を付与	書き込み	datasetExportJob*		
CreateDatasetGroup	データセットグループを無効にするアクセス許可を付与	書き込み	datasetGroup*		
CreateDatasetImportJob	データセットインポートジョブを作成するアクセス許可を付与	Write	datasetImportJob*		
CreateEventTracker	イベントトラッカーを作成する許可を付与	Write	eventTracker*		
CreateFilter	フィルターを作成する許可を付与	書き込み	filter*		
CreateMetricAttribution	メトリクス属性を作成するための許可を付与します	書き込み	metricAttribution*		
CreateRecommender	レコメンダーを作成する許可を付与します。	書き込み	recommender*		
CreateSchema	スキーマを作成する許可を付与	Write	schema*		
CreateSolution	ソリューションを作成する許可を付与	Write	solution*		
CreateSolutionVersion	ソリューションバージョンを作成する許可を付与	Write	solution*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteCampaign	キャンペーンを削除する許可を付与	Write	campaign*		
DeleteDataset	データセットを削除する許可を付与	書き込み	dataset*		
DeleteDatasetGroup	データセットグループを削除するアクセス許可を付与	Write	datasetGroup*		
DeleteEventTracker	イベントトラッカーを削除する許可を付与	Write	eventTracker*		
DeleteFilter	フィルターを削除する許可を付与	書き込み	filter*		
DeleteMetricAttribution	メトリクス属性を削除するための許可を付与します	書き込み	metricAttribution*		
DeleteRecommender	レコメンダーを削除する権限を付与します。	書き込み	recommender*		
DeleteSchema	スキーマを削除する許可を付与	Write	schema*		
DeleteSolution	ソリューションのすべてのバージョンを含むソリューションを削除する許可を付与	Write	solution*		
DescribeAlgorithm	アルゴリズムを記述する許可を付与	Read	algorithm*		
DescribeBatchInferenceJob	バッチ推論ジョブを記述する許可を付与	読み取り	batchInferenceJob*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeBatchSegmentJob	バッチセグメントジョブを記述するアクセス権限を付与します。	読み取り	batchSegmentJob*		
DescribeCampaign	キャンペーンを記述する許可を付与	読み取り	campaign*		
DescribeDataDeletionJob	データ削除ジョブを記述する許可を付与する	読み取り	dataDeletionJob*		
DescribeDataInsightsJob	データインサイトジョブを記述するアクセス許可を付与	読み取り	dataInsightsJob*		
DescribeDataset	データセットを記述するアクセス許可を付与	読み取り	dataset*		
DescribeDatasetExportJob	データセットエクスポートジョブを記述する許可を付与	読み取り	datasetExportJob*		
DescribeDatasetGroup	データセットグループを記述するアクセス許可を付与	読み込み	datasetGroup*		
DescribeDatasetImportJob	データセットインポートジョブを記述するアクセス許可を付与	Read	datasetImportJob*		
DescribeEventTracker	イベントトラッカーを記述する許可を付与	Read	eventTracker*		
DescribeFeatureTransformation	機能変換を記述する許可を付与	Read	featureTransformation*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeFilter	フィルターを記述する許可を付与	読み取り	filter*		
DescribeMetricAttribution	メトリクス属性を記述するための許可を付与します	読み取り	metricAttribution*		
DescribeRecipe	recipe を記述するアクセス許可を付与	読み取り	recipe*		
DescribeRecommender	レコメンダーを記述するアクセス権限を付与します。	読み取り	recommender*		
DescribeSchema	スキーマを記述する許可を付与	Read	schema*		
DescribeSolution	ソリューションを記述する許可を付与	Read	solution*		
DescribeSolutionVersion	ソリューションのバージョンを記述する許可を付与	読み取り	solution*		
GetActionRecommendations	推奨されるアクションのリストを取得するためのアクセス許可を付与	読み取り	campaign*		
GetDataInsights	データインサイトジョブからデータインサイトを取得するアクセス許可を付与	読み取り	dataInsightsJob*		
GetPersonalizedRanking	推奨事項の再ランクリストを取得するためのアクセス許可を付与します	Read	campaign*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetRecommendations	キャンペーンから推奨事項のリストを取得するためのアクセス許可を付与します	Read	campaign*		
GetSolutionMetrics	ソリューションバージョンのメトリクスを取得するためのアクセス許可を付与します	Read	solution*		
ListBatchInferenceJobs	バッチ推論ジョブを一覧表示する許可を付与	リスト			
ListBatchSegmentJobs	バッチセグメントジョブを一覧表示する許可を付与します。	リスト			
ListCampaigns	キャンペーンを一覧表示する許可を付与	リスト			
ListDataDeletionJobs	データ削除ジョブを一覧表示する許可を付与する	リスト			
ListDataInsightsJobs	データインサイトジョブを一覧表示するアクセス許可を付与	リスト			
ListDatasetExportJobs	すべてのデータセットエクスポートジョブを一覧表示する許可を付与	リスト			
ListDatasetGroups	データセットグループを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListDatasetImportJobs	すべてのデータセットインポートジョブを一覧表示する許可を付与	リスト			
ListDatasets	データセットを一覧表示する許可を付与	リスト			
ListEventTrackers	イベントトラッカーを一覧表示する許可を付与	リスト			
ListFilters	フィルターを一覧表示する許可を付与	リスト			
ListMetricAttributionMetrics	メトリクス属性メトリクスを一覧表示するための許可を付与します	リスト			
ListMetricAttributions	メトリクス属性を一覧表示するための許可を付与します	リスト			
ListRecipes	recipe を一覧表示する許可を付与	リスト			
ListRecommenders	レコメンダーを一覧表示するアクセス許可を付与します。	リスト			
ListSchemas	スキーマを一覧表示する許可を付与	リスト			
ListSolutionVersions	ソリューションのバージョンを一覧表示する許可を付与	リスト			
ListSolutions	ソリューションを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTagsForResource	リソースのタグを一覧表示する許可を付与。	リスト			
PutActionInteractions	リアルタイムアクションインタラクションデータを入力するためのアクセス許可を付与	書き込み			
PutActions	アクションデータを取り込むためのアクセス許可を付与	書き込み	dataset*		
PutEvents	リアルタイムイベントデータを入力する許可を付与	Write			
PutItems	アイテムデータを取り込むアクセス許可を付与します	Write	dataset*		
PutUsers	ユーザーデータを取り込むアクセス許可を付与します	書き込み	dataset*		
StartRecommender	レコメンダーを開始する権限を付与する	書き込み	recommender*		
StopRecommender	レコメンダーを停止する権限を付与する	書き込み	recommender*		
StopSolutionVersionCreation	ソリューションバージョンの作成を停止する許可を付与	書き込み	solution*		
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け			
UntagResource	リソースのタグを解除する許可を付与	Tagging			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateCampaign	キャンペーンを更新する許可を付与	書き込み	campaign*		
UpdateDataset	データセットを更新するアクセス許可を付与	書き込み	dataset*		
UpdateMetricAttribution	メトリクス属性を更新するための許可を付与します	書き込み	metricAttribution*		
UpdateRecommender	レコメンダーを更新するアクセス許可を付与します。	書き込み	recommender*		
UpdateSolution	ソリューションを更新する許可を付与する	書き込み	solution*		

Amazon Personalize で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
schema	`arn:${Partition}:personalize:${Region}:${Account}:schema/${ResourceId}`	
featureTransformation	`arn:${Partition}:personalize:::feature-transformation/${ResourceId}`	
dataset	`arn:${Partition}:personalize:${Region}:${Account}:dataset/${ResourceId}`	

リソースタイプ	ARN	条件キー
datasetGroup	arn:${Partition}:personalize:${Region}:${Account}:dataset-group/${ResourceId}	
datasetImportJob	arn:${Partition}:personalize:${Region}:${Account}:dataset-import-job/${ResourceId}	
dataInsightsJob	arn:${Partition}:personalize:${Region}:${Account}:data-insights-job/${ResourceId}	
datasetExportJob	arn:${Partition}:personalize:${Region}:${Account}:dataset-export-job/${ResourceId}	
dataDeletionJob	arn:${Partition}:personalize:${Region}:${Account}:data-deletion-job/${ResourceId}	
solution	arn:${Partition}:personalize:${Region}:${Account}:solution/${ResourceId}	
campaign	arn:${Partition}:personalize:${Region}:${Account}:campaign/${ResourceId}	
eventTracker	arn:${Partition}:personalize:${Region}:${Account}:event-tracker/${ResourceId}	
recipe	arn:${Partition}:personalize:::recipe/${ResourceId}	
algorithm	arn:${Partition}:personalize:::algorithm/${ResourceId}	

リソースタイプ	ARN	条件キー
batchInferenceJob	arn:${Partition}:personalize:${Region}:${Account}:batch-inference-job/${ResourceId}	
filter	arn:${Partition}:personalize:${Region}:${Account}:filter/${ResourceId}	
recommender	arn:${Partition}:personalize:${Region}:${Account}:recommender/${ResourceId}	
batchSegmentJob	arn:${Partition}:personalize:${Region}:${Account}:batch-segment-job/${ResourceId}	
metricAttribution	arn:${Partition}:personalize:${Region}:${Account}:metric-attribution/${ResourceId}	

Amazon Personalize の条件キー

Personalize には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Pinpoint のアクション、リソース、および条件キー

Amazon Pinpoint (サービスプレフィックス: mobiletargeting) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Pinpoint で定義されるアクション
- Amazon Pinpoint で定義されるリソースタイプ
- Amazon Pinpoint の条件キー

Amazon Pinpoint で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateApp	アプリケーションを作成する許可を付与します。	書き込み	apps*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateCampaign	アプリケーションのキャンペーンを作成する許可を付与します。	書き込み	app*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateEmailTemplate	E メールテンプレートを作成する許可を付与	書き込み	template*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateExportJob	エンドポイントの定義を Amazon S3 にエクスポートするためのエクスポートジョブを作成する許可を付与します。	書き込み	app*		
CreateImportJob	エンドポイント定義をインポートしてセグメントを作成する許可を付与します。	書き込み	app*		
CreateInAppTemplate	インアプリメッセージテンプレートを作成する許可を付与	書き込み	template*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateJourney	アプリケーション のジャーニーを作成するためのアクセス許可を付与します。	書き込み	journeys*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreatePushTemplate	プッシュ通知テンプレートを作成するアクセス許可を付与します。	書き込み	template*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateRecommenderConfiguration	推奨モデル用の Amazon Pinpoint 設定を作成する許可を付与します。	書き込み	recommenders*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSegment	アプリケーションによって Pinpoint に報告されたエンドポイントデータに基づくセグメントを作成する許可を付与します。ユーザーが Pinpoint の外部からエンドポイントデータをインポートしてセグメントを作成することを許可するには、mobiletargeting:CreateImportJob アクションを許可します。	書き込み	app*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateSmsTemplate	SMSメッセージテンプレートを作成する許可を付与します。	書き込み	template*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateVoiceTemplate	ボイスメッセージテンプレートを作成する許可を付与します。	書き込み	template*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteAdmChannel	アプリケーションの ADM チャネルを削除するアクセス許可を付与します。	書き込み	channel*		
DeleteApnsChannel	アプリケーションの APN チャネルを削除するアクセス許可を付与します。	書き込み	channel*		
DeleteApnsSandboxChannel	appの APN サンドボックスチャネルを削除する許可を付与します。	書き込み	channel*		
DeleteApnsVoipChannel	アプリケーションの APN VoIP チャネルを削除するアクセス許可を付与します。	書き込み	channel*		
DeleteApnsVoipSandboxChannel	アプリケーションの APN VoIP サンドボックスチャネルを削除する許可を付与します。	書き込み	channel*		
DeleteApp	特定のキャンペーンを削除する許可を付与します。	書き込み	app*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteBaiduChannel	アプリケーションの Baidu チャネルを削除するアクセス許可を付与します。	書き込み	channel*		
DeleteCampaign	特定のキャンペーンを削除する許可を付与します。	書き込み	campaign*		
DeleteEmailChannel	アプリケーションの電子メールチャネルを削除するアクセス許可を付与します。	書き込み	channel*		
DeleteEmailTemplate	E メールテンプレートもしくは E メールテンプレートバージョンを削除する許可を付与します。	書き込み	template*		
DeleteEndpoint	エンドポイントを削除する許可を付与	書き込み	endpoint*		
DeleteEventStream	アプリケーションのイベントストリームを削除するアクセス許可を付与します。	書き込み	event-stream*		
DeleteGcmChannel	アプリケーションの GCM チャネルを削除するアクセス許可を付与します。	書き込み	channel*		
DeleteInAppTemplate	インアプリメッセージテンプレートまたはインアプリメッセージテンプレートバージョンを削除する許可を付与	書き込み	template*		
DeleteJourney	特定のジャーニーを削除するアクセス許可を付与します。	書き込み	journey*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeletePushTemplate	プッシュ通知テンプレートもしくはプッシュ通知テンプレートバージョンを削除する許可を付与します。	書き込み	template*		
DeleteRecommenderConfiguration	推奨モデルの Amazon Pinpoint 設定を削除する許可を付与します。	書き込み	recommender*		
DeleteSegment	特定のセグメントを削除するアクセス許可を付与します。	書き込み	segment*		
DeleteSmsChannel	アプリケーションの SMS チャネルを削除するアクセス許可を付与します。	書き込み	channel*		
DeleteSmsTemplate	SMS メッセージテンプレートもしくは SMS メッセージテンプレートバージョンを削除する許可を付与します。	書き込み	template*		
DeleteUserEndpoints	ユーザー ID に関連付けられているすべてのエンドポイントを削除する許可を付与します。	書き込み	user*		
DeleteVoiceChannel	アプリケーションの音声チャネルを削除するアクセス許可を付与します。	書き込み	channel*		
DeleteVoiceTemplate	ボイスメッセージテンプレートもしくはボイスメッセージテンプレートバージョンを削除する許可を付与します。	書き込み	template*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetAdmChannel	アプリケーションの Amazon Device Messaging (ADM) チャネルに関する情報を取得する許可を付与します。	読み込み	channel*		
GetApnsChannel	アプリケーションの APN チャネルについての情報を取得する許可を付与します。	読み込み	channel*		
GetApnsSandboxChannel	アプリケーションの APN サンドボックスチャネルに関する情報を取得する許可を付与します。	読み込み	channel*		
GetApnsVoipChannel	アプリケーションの APN VoIP チャネルに関する情報を取得する許可を付与します。	読み込み	channel*		
GetApnsVoipSandboxChannel	アプリケーションの APN VoIP サンドボックスチャネルに関する情報を取得する許可を付与します。	読み込み	channel*		
GetApp	Amazon Pinpoint アカウントのアプリケーションに関する情報を取得する許可を付与します。	読み込み	app*		
GetApplicationDateRangeKpi	アプリケーションに適用される標準的なメトリクスの事前集計データを取得 (クエリ) する許可を付与します。	読み込み	application-metrics*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetApplicationSettings	アプリケーションのデフォルト設定を取得するアクセス許可を付与します。	リスト	app*		
GetApps	Amazon Pinpoint アカウント内のアプリケーションのリストを取得する許可を付与します。	読み込み	apps*		
GetBaiduChannel	アプリケーションの Baidu チャンネルに関する情報を取得する許可を付与します。	読み込み	channel*		
GetCampaign	特定のキャンペーンについての情報を返すアクセス許可を付与します。	読み込み	campaign*		
GetCampaignActivities	キャンペーンによって実行されたアクティビティに関する情報を取得する許可を付与します。	リスト	campaign*		
GetCampaignDateRangeKpi	キャンペーンに適用される標準的なメトリクスの事前集計データを取得 (クエリ) する許可を付与します。	読み込み	campaign-metrics*		
GetCampaignVersion	特定のキャンペーンのバージョンに関する情報を取得する許可を付与します。	読み込み	campaign*		
GetCampaignVersions	現在および以前のキャンペーンのバージョンに関する情報を取得する許可を付与します。	リスト	campaign*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetCampaigns	アプリケーションのすべてのキャンペーンに関する情報を取得する許可を付与します。	リスト	app*		
GetChannels	アプリケーションのすべてのチャネル情報を取得するアクセス許可を付与します。	リスト	channels*		
GetEmailChannel	アプリケーションの E メールチャネルに関する情報を取得する許可を付与します。	読み込み	channel*		
GetEmailTemplate	E メールテンプレートの特定のバージョンもしくはアクティブバージョンに関する情報を取得する許可を付与します。	読み込み	template*		
GetEndpoint	特定のエンドポイントについての情報を取得するアクセス許可を付与します。	読み込み	endpoint*		
GetEventStream	アプリケーションのイベントストリームに関する情報を取得する許可を付与します。	読み込み	event-stream*		
GetExportJob	特定のエクスポートジョブに関する情報を取得する許可を付与します。	読み込み	export-job*		
GetExportJobs	アプリケーションのすべてのエクスポートジョブのリストを取得する許可を付与します。	リスト	app*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetGcmChannel	アプリケーションの GCM チャネルについての情報を取得する許可を付与します。	読み込み	channel*		
GetImportJob	特定のインポートジョブについての情報を返すアクセス許可を付与します。	読み込み	import-job*		
GetImportJobs	アプリケーションのすべてのインポートジョブに関する情報を取得する許可を付与します。	リスト	app*		
GetInAppMessages	指定されたエンドポイント ID のアプリ内メッセージを取得する権限を付与します。	読み込み	app*		
GetInAppTemplate	インアプリメッセージテンプレートの特定のバージョンもしくはアクティブバージョンに関する情報を取得する許可を付与	読み込み	template*		
GetJourney	特定のジャーニーについての情報を取得するアクセス許可を付与します。	読み込み	journey*		
GetJourneyDateRangeKpi	ジャーニーに適用される標準的なエンゲージメントメトリクスの事前集計データを取得(クエリ)する許可を付与します。	読み込み	journey-metrics*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetJourneyExecutionActivityMetrics	ジャーニーアクティビティに適用される標準的な実行メトリクスの事前集計データを取得 (クエリ)する許可を付与します。	読み込み	journey-execution-activity-metrics*		
GetJourneyExecutionMetrics	ジャーニーに適用される標準的な実行メトリクスの事前集計データを取得 (クエリ) する許可を付与します。	読み取り	journey-execution-metrics*		
GetJourneyRunExecutionActivityMetrics	単一のジャーニー実行のジャーニーアクティビティに適用される標準的な実行メトリクスの事前集計データを取得 (クエリ) するための許可を付与します	読み取り	journey*		
GetJourneyRunExecutionMetrics	単一のジャーニー実行のジャーニーに適用される標準的な実行メトリクスの事前集計データを取得 (クエリ) するための許可を付与します	読み取り	journey*		
GetJourneyRuns	ジャーニーのすべてのジャーニー実行に関する情報を取得するための許可を付与します	リスト	journey*		
GetPushTemplate	プッシュ通知テンプレートの特定のバージョンもしくはアクティブバージョンに関する情報を取得する許可を付与します。	読み込み	template*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetRecommenderConfiguration	推奨モデルの Amazon Pinpoint 設定に関する情報を取得する許可を付与します。	読み込み	recommender*		
GetRecommenderConfigurations	Amazon Pinpoint アカウントに関連付けられているすべての推奨モデルの設定に関する情報を取得する許可を付与します。	リスト	recommenders*		
GetReports [許可のみ]	mobiletargeting:GetReports の許可を付与	読み込み	reports*		
GetSegment	特定のセグメントについての情報を取得するアクセス許可を付与します。	読み込み	segment*		
GetSegmentExportJobs	エンドポイント定義をセグメントから Amazon S3 にエクスポートするジョブに関する情報を取得する許可を付与します。	リスト	segment*		
GetSegmentImportJobs	エンドポイント定義をインポートしてセグメントを作成するジョブに関する情報を取得する許可を付与します。	リスト	segment*		
GetSegmentVersion	特定のセグメントバージョンに関する情報を取得する許可を付与します。	読み込み	segment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetSegmentVersions	現在および以前のセグメントのバージョンに関する情報を取得する許可を付与します。	リスト	segment*		
GetSegments	アプリケーションのセグメントについての情報を取得する許可を付与します。	リスト	app*		
GetSmsChannel	アプリケーションの SMS チャネルに関する情報を取得する許可を付与します。	読み込み	channel*		
GetSmsTemplate	SMS メッセージテンプレートの特定のバージョンもしくはアクティブバージョンに関する情報を取得する許可を付与します。	読み込み	template*		
GetUserEndpoints	ユーザー ID に関連付けられているエンドポイントに関する情報を取得する許可を付与します。	読み込み	user*		
GetVoiceChannel	アプリケーションの音声チャネルに関する情報を取得する許可を付与します。	読み込み	channel*		
GetVoiceTemplate	ボイスメッセージテンプレートの特定のバージョンもしくはアクティブバージョンに関する情報を取得する許可を付与します。	読み込み	template*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListJourneys	アプリケーションのすべてのジャーニーに関する情報を取得する許可を付与します。	リスト	app*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み込み	app		
			campaign		
			journey		
			segment		
			template		
ListTemplateVersions	特定のテンプレートに関するすべてのバージョンを取得する許可を付与します。	リスト	template*		
ListTemplates	クエリしたテンプレートに関するメタデータを取得する許可を付与します。	リスト	templates*		
PhoneNumberValidate	電話番号のメタデータを取得する許可を付与します。たとえば、番号のタイプ (携帯電話、固定電話、VoIP)、場所およびプロバイダーなどです。	読み込み	phone-number-validate*		
PutEventStream	アプリケーションのイベントストリームを作成または更新する許可を付与します。	書き込み	event-stream*		
PutEvents	アプリケーションのイベントタイプを作成または更新する許可を付与します。	書き込み	events*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RemoveAttributes	アプリケーションの属性を削除するアクセス許可を付与します。	書き込み	attribute*		
SendMessages	特定のエンドポイントに SMS メッセージもしくはプッシュ通知を送信する許可を付与します。	書き込み	messages*		
SendOTPMessage	アプリケーションのユーザーに OTP コードを送信する許可を付与	書き込み	otp*		
SendUsersMessages	特定のユーザー ID に関連付けられているすべてのエンドポイントに、SMS メッセージまたはプッシュ通知を送信する許可を付与します。	書き込み	messages*		
TagResource	リソースにタグを追加するアクセス許可を付与します	タグ付け	app		
			campaign		
			journey		
			segment		
			template		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	リソースからタグを削除する許可を付与	Tagging	app		
			campaign		
			journey		
			segment		
			template		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateAdmChannel	アプリケーションの Amazon Device Messaging (ADM) チャネルを更新する許可を付与します。	書き込み	channel*		
UpdateApnsChannel	アプリケーションの Apple Push Notification Service (APNS) チャネルを更新する許可を付与します。	書き込み	channel*		
UpdateApnsSandboxChannel	アプリケーションの Apple Push Notification Service (APNS) サンドボックスチャネルを更新する許可を付与します。	書き込み	channel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateApnsVoipChannel	アプリケーションの Apple Push Notification Service (APNS) VoIP チャネルを更新する許可を付与します。	書き込み	channel*		
UpdateApnsVoipSandboxChannel	アプリケーションの Apple Push Notification Service (APNS) VoIP サンドボックスチャネルを更新する許可を付与します。	書き込み	channel*		
UpdateApplicationSettings	アプリケーションのデフォルト設定 の詳細を更新する権限を付与します。	書き込み	app*		
UpdateBaiduChannel	アプリケーションのBaiduチャンネルを更新する権限を付与します。	書き込み	channel*		
UpdateCampaign	特定されたキャンペーンを更新する許可を付与します。	書き込み	campaign*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateEmailChannel	アプリケーションのEメールチャンネルを更新する権限を付与します。	書き込み	channel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateEmailTemplate	同じバージョンで特定の E メールテンプレートを更新するか、新しいバージョンを生成する許可を付与します。	書き込み	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateEndpoint	エンドポイントの作成またはエンドポイントの情報を更新するアクセス許可を付与します。	書き込み	endpoint*		
UpdateEndpointsBatch	バッチオペレーションとしてエンドポイントを作成または更新する許可を付与します。	書き込み	app*		
UpdateGcmChannel	Firebase Cloud Messaging (FCM) もしくは Google Cloud Messaging (GCM) の API キーを更新して、Android アプリにプッシュ通知を送信する許可を付与します。	書き込み	channel*		
UpdateInAppTemplate	同じバージョンで特定のインアプリメッセージテンプレートを更新するか、新しいバージョンを生成する許可を付与	書き込み	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateJourney	特定のジャーニーを更新するアクセス許可を付与します。	書き込み	journey*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateJourneyState	特定のジャーニーステートを更新するアクセス許可を付与します。	書き込み	journey*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdatePushTemplate	同じバージョンで特定のプッシュ通知テンプレートを更新するか、新しいバージョンを生成する許可を付与します。	書き込み	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateRecommenderConfiguration	推奨モデルの Amazon Pinpoint 設定を更新する許可を付与します。	書き込み	recommender*		
UpdateSegment	特定のセグメントを更新するアクセス許可を付与します。	書き込み	segment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateSmsChannel	アプリケーションのSMSチャンネル の詳細を更新する権限を付与します。	書き込み	channel*		
UpdateSmsTemplate	同じバージョンで特定の SMS メッセージテンプレートを更新するか、新しいバージョンを生成する許可を付与します。	書き込み	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTemplateActiveVersion	特定のテンプレートのアクティブバージョンパラメータを更新する許可を付与します。	書き込み	template*		
UpdateVoiceChannel	アプリケーションの音声チャンネル の詳細を更新する権限を付与します。	書き込み	channel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateVoiceTemplate	同じバージョンで特定のボイスメッセージテンプレートを更新するか、新しいバージョンを生成する許可を付与します。	書き込み	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
VerifyOTPMessage	ワンタイムパスワード (OTP) の有効性を確認する許可を付与	書き込み	verify-otp*		

Amazon Pinpoint で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
app	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}	aws:ResourceTag/${TagKey}
apps	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/*	
campaign	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/campaigns/${CampaignId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
journey	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}	aws:ResourceTag/${TagKey}
journeys	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys	
segment	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/segments/${SegmentId}	aws:ResourceTag/${TagKey}
template	arn:${Partition}:mobiletargeting:${Region}:${Account}:templates/${TemplateName}/${TemplateType}	aws:ResourceTag/${TagKey}
templates	arn:${Partition}:mobiletargeting:${Region}:${Account}:templates	
recommender	arn:${Partition}:mobiletargeting:${Region}:${Account}:recommenders/${RecommenderId}	
recommenders	arn:${Partition}:mobiletargeting:${Region}:${Account}:recommenders/*	
phone-number-validate	arn:${Partition}:mobiletargeting:${Region}:${Account}:phone/number/validate	
channels	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/channels	

リソースタイプ	ARN	条件キー
channel	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/channels/${ChannelType}	
event-stream	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/eventstream	
events	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/events	
messages	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/messages	
verify-otp	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/verify-otp	
otp	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/otp	
attribute	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/attributes/${AttributeType}	
user	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/users/${UserId}	
endpoint	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/endpoints/${EndpointId}	

リソースタイプ	ARN	条件キー
import-job	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/jobs/import/${JobId}	
export-job	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/jobs/export/${JobId}	
application-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/kpis/daterange/${KpiName}	
campaign-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/campaigns/${CampaignId}/kpis/daterange/${KpiName}	
journey-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}/kpis/daterange/${KpiName}	
journey-execution-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}/execution-metrics	
journey-execution-activity-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}/activities/${JourneyActivityId}/execution-metrics	
reports	arn:${Partition}:mobiletargeting:${Region}:${Account}:reports	

Amazon Pinpoint の条件キー

Amazon Pinpoint では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	ユーザーが Pinpoint サービスに対して行うリクエストに含まれるキーによってアクセスをフィルタリングします。	String
aws:ResourceTag/${TagKey}	タグキーおよび値のペアでアクセスをフィルタリングします。	String
aws:TagKeys	ユーザーが Pinpoint サービスに対して行うリクエストに含まれるすべてのタグキー名のリストでアクセスをフィルタリングします。	ArrayOfString

Amazon Pinpoint Email Service のアクション、リソース、および条件キー

Amazon Pinpoint Email Service (サービスプレフィックス: ses) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Pinpoint Email Service で定義されるアクション
- Amazon Pinpoint Email Service で定義されるリソースタイプ
- Amazon Pinpoint Email Service の条件キー

Amazon Pinpoint Email Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateConfigurationSet	設定セットを作成する許可を付与	書き込み		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateConfigurationSetEventDestination	設定セットイベントの宛先を作成する許可を付与	書き込み	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateDedicatedIpPool	専用 IP アドレスの新しいプールを作成する許可を付与	書き込み		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateDeliverabilityTestReport	新しい予測受信箱配置テストを作成する許可を付与	書き込み	identity*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateEmailIdentity	E メール ID の検証プロセスを開始する許可を付与	書き込み		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
DeleteConfigurationSet	既存の設定セットを削除する許可を付与	書き込み	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteConfigurationSetEventDestination	イベントの送信先を削除するアクセス権限を付与します	書き込み	configuration-set*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteDedicatedIpPool	専用 IP プールを削除する許可を付与	書き込み	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailIdentity	以前に検証した E メール ID を削除する許可を付与	書き込み	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetAccount	E メールの送信ステータスと機能に関する情報を取得するためのアクセス許可を付与します	読み込み		ses:ApiVersion	
GetBlacklistReports	専用 IP アドレスが表示される拒否リストの一覧を取得するためのアクセス許可を付与します	読み込み		ses:ApiVersion	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetConfigurationSet	既存の設定セットに関する情報を取得するためのアクセス許可を付与します	読み込み	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetConfigurationSetEventDestinations	設定セットに関連付けられているイベント送信先のリストを取得する許可を付与	読み込み	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDedicatedIp	専用 IP アドレスに関する情報を取得するためのアクセス許可を付与します	読み込み		ses:ApiVersion	
GetDedicatedIps	アカウントに関連付けられている専用 IP アドレスを一覧表示する許可を付与	読み込み	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetDeliverabilityDashboardOptions	配信性能ダッシュボードのステータスを取得するためのアクセス許可を付与します	読み込み		ses:ApiVersion	
GetDeliverabilityTestReport	受信箱配置の予測テストの結果を取得するためのアクセス許可を付与します	読み込み	deliverability-test-report*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDomainDeliverabilityCampaign	特定のキャンペーンのすべての配信性能データを取得するためのアクセス許可を付与します	読み込み		ses:ApiVersion	
GetDomainStatisticsReport	E メールの送信に使用するドメインの受信箱配置とエンゲージメント率を取得する許可を付与	読み込み	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetEmailIdentity	アカウントに関連付けられた特定の ID に関する情報を取得するためのアクセス許可を付与します	読み込み	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListConfigurationSets	アカウントに関連付けられているすべての設定セットを一覧表示する許可を付与	リスト		ses:ApiVersion	
ListDedicatedIpPools	アカウント内に存在するすべての専用 IP プールを一覧表示する許可を付与	リスト		ses:ApiVersion	
ListDeliverabilityTestReports	ステータスに関係なく、実行した受信箱配置の予測テストのリストを取得する許可を付与	リスト		ses:ApiVersion	
ListDomainDeliverabilityCampaigns	指定した期間内に特定のドメインを使用して E メールを送信したすべてのキャンペーンの配信性能データを取得するためのアクセス許可を付与します	読み込み		ses:ApiVersion	
ListEmailIdentities	アカウントに関連付けられているすべての E メール ID の一覧を表示する許可を付与	リスト		ses:ApiVersion	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTagsForResource	特定のリソースに関連付けられているタグ (キーと値) のリストを取得する許可を付与	読み込み	configuration-set		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
				ses:ApiVersion	
PutAccountDedicatedIpWarmupAttributes	専用 IP アドレスの自動ウォームアップ機能を有効または無効にする許可を付与	書き込み		ses:ApiVersion	
PutAccountSendingAttributes	アカウントの E メール送信機能を有効または無効にする許可を付与	書き込み		ses:ApiVersion	
PutConfigurationSetDeliveryOptions	設定セットを専用 IP プールに関連付けるアクセス許可を付与します	書き込み	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutConfigurationSetReputationOptions	特定の設定セットを使用して送信する E メールの評価メトリクスの収集を有効または無効にする許可を付与	書き込み	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetSendingOptions	特定の設定セットを使用するメッセージの E メール送信を有効または無効にする許可を付与	書き込み	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetTrackingOptions	特定の設定セットを使用して送信する E メールの開封とクリックの追跡要素に使用するカスタムドメインを指定する許可を付与	書き込み	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpInPool	専用 IP アドレスを既存の専用 IP プールに移動する許可を付与	書き込み	dedicated-ip-pool*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpWarmupAttributes	専用 IP ウォームアップ属性を有効にする許可を付与	書き込み		ses:ApiVersion	
PutDeliverabilityDashboardOption	配信性能ダッシュボードを有効または無効にする許可を付与	書き込み		ses:ApiVersion	
PutEmailIdentityDkimAttributes	E メール ID の DKIM 認証を有効または無効にする許可を付与	書き込み	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityFeedbackAttributes	ID のフィードバック転送を有効または無効にする許可を付与	書き込み	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutEmailIdentityMailFromAttributes	E メール ID のカスタム MAIL FROM ドメイン設定を有効または無効にする許可を付与	書き込み	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
SendEmail	E メールメッセージを送信する許可を付与	書き込み	identity*		
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
TagResource	指定したリソースに 1 つ以上のタグ (キーと値) を追加する許可を付与	タグ付け	configuration-set		
			dedicated-ip-pool		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			deliverability-test-report		
			identity		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	指定したリソースから 1 つ以上のタグ (キーと値) を削除する許可を付与	タグ付け	configuration-set		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
				ses:ApiVersion aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateConfigurationSetEventDestination	設定セットのイベント送信先の設定を更新する許可を付与	書き込み	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Amazon Pinpoint Email Service で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
configuration-set	arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}	aws:ResourceTag/${TagKey}
dedicated-ip-pool	arn:${Partition}:ses:${Region}:${Account}:dedicated-ip-pool/${DedicatedIPPool}	aws:ResourceTag/${TagKey}
deliverability-test-report	arn:${Partition}:ses:${Region}:${Account}:deliverability-test-report/${ReportId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
identity	arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}	aws:ResourceTag/${TagKey}

Amazon Pinpoint Email Service の条件キー

Amazon Pinpoint Email Service は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアのプレゼンスに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいてアクションをフィルタリングします	ArrayOfString
ses:ApiVersion	SES API バージョンに基づいてアクションをフィルタリング	String
ses:FeedbackAddress	E メールフィードバック転送によって送信されたバウンスおよび苦情の場所を指定する「リターンパス」アドレスに基づくアクションをフィルタリングします	文字列
ses:FromAddress	メッセージの「From」アドレスに基づいてアクションをフィルタリングします	文字列

条件キー	説明	タイプ
ses:FromDisplayName	メッセージの表示名として使用される「From」アドレスに基づいてアクションをフィルタリングします	文字列
ses:Recipients	「To」、「CC」、「BCC」アドレスを含むメッセージの受取人アドレスに基づくアクションをフィルタリングします	ArrayOfString

Amazon Pinpoint SMS and Voice Service のアクション、リソース、および条件キー

Amazon Pinpoint SMS and Voice Service (サービスプレフィックス: `sms-voice`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Pinpoint SMS and Voice Service で定義されるアクション
- Amazon Pinpoint SMS and Voice Service で定義されるリソースタイプ
- Amazon Pinpoint SMS and Voice Service の条件キー

Amazon Pinpoint SMS and Voice Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーショ

ンへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateConfigurationSet	新しい設定セットを作成します。設定セットを作成したら、そのセットに 1 つ以上のイベント送信先を追加できます。	Write			
CreateConfigurationSetEventDestination	設定セット内に新しいイベント送信先を作成します。	Write			iam:PassRole
DeleteConfigurationSet	既存の設定セットを削除します。	Write			
DeleteConfigurationSetEventDestination	設定セットに含まれるイベント送信先を削除します。	Write			
GetConfigurationSetEventDestinations	報告されるイベントのタイプ、送信先の Amazon リソースネーム (ARN)、イベント送信先の名前など、イベント送信先に関する情報を取得します。	Read			
ListConfigurationSets	設定セットのリストを返します。このオペレーションは、現在の AWS リージョンに存在するアカウントに関連付けられている設定セットのみを返します。	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SendVoiceMessage	新しい音声メッセージを作成し、受信者の電話番号に送信します。	Write			
UpdateConfigurationSetEventDestination	設定セットに含まれるイベント送信先を更新します。イベント送信先は、音声通話に関する情報を公開する先です。たとえば、通話が失敗したときにイベントを Amazon CloudWatch 送信先に記録できます。	Write			iam:PassRole

Amazon Pinpoint SMS and Voice Service で定義されるリソースタイプ

Amazon Pinpoint SMS and Voice Service は、IAM ポリシーステートメントの `Resource` 要素でのリソース ARN の指定をサポートしていません。Amazon Pinpoint SMS and Voice Service へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

Amazon Pinpoint SMS and Voice Service の条件キー

Pinpoint SMS Voice には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS「グローバル条件コンテキストキー」を参照してください。

Amazon Polly のアクション、リソース、および条件キー

Amazon Polly (サービスプレフィックス: `polly`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Polly で定義されるアクション
- Amazon Polly で定義されるリソースタイプ
- Amazon Polly の条件キー

Amazon Polly で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteLexicon	に保存されている指定された発音レキシコンを削除するアクセス許可を付与します AWS リージョン	書き込み	lexicon*		
DescribeVoices	音声合成をリクエストするときに使用可能な音声のリストを記述するための許可を付与します	リスト			
GetLexicon	に保存されている指定された発音レキシコンのコンテンツを取得するアクセス許可を付与します AWS リージョン	読み取り	lexicon*		
GetSpeechSynthesisTask	特定の音声合成タスクに関する情報を取得するための許可を付与します	読み取り			
ListLexicons	に保存されている発音レキシコンを一覧表示するアクセス許可を付与します AWS リージョン	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListSpeechSynthesisTasks	リクエストされた音声合成タスクを一覧表示するための許可を付与します	リスト			
PutLexicon	発音レキシコンを に保存するためのアクセス許可を付与します AWS リージョン	書き込み	lexicon*		
StartSpeechSynthesisTask	指定された S3 の場所に長い入力を合成するための許可を付与します	書き込み	lexicon		s3:PutObject
SynthesizeSpeech	音声を合成するための許可を付与します	読み取り	lexicon		

Amazon Polly で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
lexicon	`arn:${Partition}:polly:${Region}:${Account}:lexicon/${LexiconName}`	

Amazon Polly の条件キー

Polly には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Price List のアクション、リソース、および条件キー

AWS Price List (サービスプレフィックス: pricing) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Price List で定義されるアクション
- AWS Price List で定義されるリソースタイプ
- AWS Price List の条件キー

AWS Price List で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeServices	すべての (分割された) サービスの詳細 (serviceCode が設定されていない場合)、または特定のサービスの詳細 (serviceCode が設定されている場合) を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetAttributeValues	指定の属性のすべての (分割された) 値を取得する許可を付与	読み取り			
GetPriceListFileUrl	特定のパラメータの料金格表ファイルの URL を取得するための許可を付与します	読み取り			
GetProducts	指定の検索条件を満たすすべての製品を取得する許可を付与	読み取り			
ListPriceLists	特定のパラメータのすべての (ページ分割された) 適格な料金表を一覧表示するための許可を付与します	読み取り			

AWS Price List で定義されるリソースタイプ

AWS Price List では、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定はサポートされていません。 AWS Price List へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Price List の条件キー

Price List には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

アクティブディレクトリ用の AWS プライベート CA コネクタのアクション、リソース、条件キー

AWS Private CA Connector for Active Directory (サービスプレフィックス: `pca-connector-ad`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- アクティブディレクトリ用の AWS プライベート CA コネクタによって定義されたアクション
- アクティブディレクトリ用の AWS プライベート CA コネクタによって定義されるリソースタイプ
- アクティブディレクトリ用の AWS プライベート CA コネクタの条件キー

アクティブディレクトリ用の AWS プライベート CA コネクタによって定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアク

ションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateConnector	アカウントでコネクタを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	acm-pca:DescribeCertificateAuthority acm-pca:GetCertificate acm-pca:GetCertificateAutho

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					rityCertificate acm-pca:IssueCertificate ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeVpcEndpoints
CreateDirectoryRegistration	アカウントに Directory Registration を作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	ds:AuthorizeApplication ds:DescribeDirectories
CreateServicePrincipalName	DirectoryRegistration の ServicePrincipalName を作成するアクセス許可を付与します	書き込み	Directory Registration*		ds:UpdateAuthorizedApplication

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateTemplate	コネクタのテンプレートを作成するアクセス許可を付与します	書き込み	Connector*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateTemplateGroupAccessControlEntry	テンプレートの TemplateGroupAccessControlEntry を作成するアクセス許可を付与します	書き込み	Template*		
DeleteConnector	アカウント内のコネクタを削除するアクセス許可を付与します	書き込み	Connector*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints
DeleteDirectoryRegistration	アカウントの Directory Registration を削除するアクセス許可を付与します	書き込み	DirectoryRegistration*		ds:UnauthorizeApplication ds:UpdateAuthorizedApplication

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteServicePrincipalName	DirectoryRegistration の ServicePrincipalName を削除するアクセス許可を付与します	書き込み	DirectoryRegistration*		ds:UpdateAuthorizedApplication
DeleteTemplate	コネクタのテンプレートを削除するアクセス許可を付与します	書き込み	Template*		
DeleteTemplateGroupAccessControlEntry	テンプレートの TemplateGroupAccessControlEntry を削除するアクセス許可を付与します	書き込み	Template*		
GetConnector	アカウントでコネクタを取得するアクセス許可を付与します	読み取り	Connector*		
GetDirectoryRegistration	アカウントの Directory Registration を取得するアクセス許可を付与します	読み取り	DirectoryRegistration*		
GetServicePrincipalName	DirectoryRegistration の ServicePrincipalName を取得するアクセス許可を付与します	読み取り	DirectoryRegistration*		
GetTemplate	コネクタのテンプレートを取得するアクセス許可を付与します	読み取り	Template*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetTemplateGroupAccessControlEntry	テンプレートの TemplateGroupAccessControlEntry を取得するアクセス許可を付与します	読み取り	Template*		
ListConnectors	アカウントでコネクタを一覧表示するアクセス許可を付与します	リスト			
ListDirectoryRegistrations	アカウントで Directory Registrations を一覧表示するアクセス許可を付与します	リスト			
ListServicePrincipalNames	DirectoryRegistration の ServicePrincipalNames を一覧表示するアクセス許可を付与します	リスト	DirectoryRegistration*		
ListTagsForResource	アカウント内の pca-connector-ad リソースのタグを一覧表示するアクセス許可を付与します	読み取り			
ListTemplateGroupAccessControlEntries	テンプレートの TemplateGroupAccessControlEntries を一覧表示するアクセス許可を付与します	リスト	Template*		
ListTemplates	コネクタのテンプレートを一覧表示するアクセス許可を付与します	リスト	Connector*		
TagResource	アカウントで pca-connector-ad リソースにタグ付けするアクセス許可を付与します	Tagging	Connector		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			Directory Registration		
			Template		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	アカウントで pca-connector-ad リースにタグ付けを解除するアクセス許可を付与します	Tagging	Connector		
			Directory Registration		
			Template		
				aws:TagKeys	
UpdateTemplate	コネクタでテンプレートを更新するアクセス許可を付与します	書き込み	Template*		
UpdateTemplateGroupAccessControlEntry	テンプレートの TemplateGroupAccessControlEntry を更新するアクセス許可を付与します	書き込み	Template*		

アクティブディレクトリ用の AWS プライベート CA コネクタによって定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Connector	`arn:${Partition}:pca-connector-ad:${Region}:${Account}:connector/${ConnectorId}`	aws:ResourceTag/${TagKey}
Directory Registration	`arn:${Partition}:pca-connector-ad:${Region}:${Account}:directory-registration/${DirectoryId}`	aws:ResourceTag/${TagKey}
Template	`arn:${Partition}:pca-connector-ad:${Region}:${Account}:connector/${ConnectorId}/template/${TemplateId}`	aws:ResourceTag/${TagKey}

アクティブディレクトリ用の AWS プライベート CA コネクタの条件キー

AWS Private CA Connector for Active Directory では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリング	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリング	String
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリング	ArrayOfString

AWS Private CA Connector for SCEP のアクション、リソース、条件キー

AWS Private CA Connector for SCEP (サービスプレフィックス: `pca-connector-scep`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Private CA Connector for SCEP によって定義されたアクション
- AWS Private CA Connector for SCEP によって定義されるリソースタイプ
- AWS Private CA Connector for SCEP の条件キー

AWS Private CA Connector for SCEP によって定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateChallenge	コネクタのチャレンジを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnector	アカウントで SCEP コネクタを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	acm-pca:DescribeCertificateAuthority acm-pca:GetCertificate acm-pca:GetCertificateAuthorityCertificate acm-pca:IssueCertificate
DeleteChallenge	コネクタのチャレンジを削除する許可を付与する	書き込み	Challenge*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteConnector	アカウント内の SCEP コネクタを削除する許可を付与する	書き込み	Connector*		
GetChallengeMetadata	コネクタのチャレンジを取得する許可を付与する	読み取り	Challenge*		
GetChallengePassword	コネクタのチャレンジパスワードを取得する許可を付与する	読み取り	Challenge*		
GetConnector	アカウントで SCEP コネクタを取得する許可を付与する	読み取り	Connector*		
ListChallengeMetadata	コネクタのチャレンジを一覧表示する許可を付与する	リスト			
ListConnectors	アカウントで SCEP コネクタを一覧表示する許可を付与する	リスト			
ListTagsForResource	アカウント内の pca-connector-scep リソースのタグを一覧表示する許可を付与する	読み取り			
TagResource	アカウントで pca-connector-scep リソースにタグ付けする許可を付与する	Tagging	Challenge		
			Connector		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	アカウントで pca-connector-scep リースのタグ付けを解除する許可を付与する	Tagging	Challenge		
			Connector		
				aws:TagKeys	

AWS Private CA Connector for SCEP によって定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource 工レメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Challenge	arn:${Partition}:pca-connector-scep:${Region}:${Account}:connector/${ConnectorId}/challenge/${ChallengeId}	aws:ResourceTag/${TagKey}
Connector	arn:${Partition}:pca-connector-scep:${Region}:${Account}:connector/${ConnectorId}	aws:ResourceTag/${TagKey}

AWS Private CA Connector for SCEP の条件キー

AWS Private CA Connector for SCEP では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Private Certificate Authority のアクション、リソース、条件キー

AWS Private Certificate Authority (サービスプレフィックス: acm-pca) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Private Certificate Authority で定義されたアクション
- AWS Private Certificate Authority で定義されたリソースタイプ
- AWS Private Certificate Authority の条件キー

AWS Private Certificate Authority で定義されたアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateCertificateAuthority	プライベート CA AWS および関連するプライベートキーと設定を作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCertificateAuthorityAuditReport	プライベート CA AWS の監査レポートを作成する許可を付与	書き込み	certificate-authority*		
CreatePermission	プライベート CA AWS のアクセス許可を作成するアクセス許可を付与します	権限の管理	certificate-authority*		
DeleteCertificateAuthority	プライベート CA AWS および関連するプライベートキーと設定を削除するアクセス許可を付与します	書き込み	certificate-authority*		
DeletePermission	プライベート CA AWS のアクセス許可を削除するアクセス許可を付与します	権限の管理	certificate-authority*		
DeletePolicy	プライベート CA AWS のポリシーを削除するアクセス許可を付与します	権限の管理	certificate-authority*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeCertificateAuthority	指定された AWS プライベート CA に含まれる設定フィールドとステータスフィールドのリストを返すアクセス許可を付与します	読み取り	certificate-authority*		
DescribeCertificateAuthorityAuditReport	AWS プライベート CA 監査レポートのステータスと情報を返すアクセス許可を付与します	読み取り	certificate-authority*		
GetCertificate	ARN で指定された認証機関の AWS プライベート CA 証明書と証明書チェーンを取得するアクセス許可を付与します	読み取り	certificate-authority*		
GetCertificateAuthorityCertificate	ARN で指定された認証機関の AWS プライベート CA 証明書と証明書チェーンを取得するアクセス許可を付与します	読み取り	certificate-authority*		
GetCertificateAuthorityCsr	ARN で指定された証明書権限の AWS プライベート CA 証明書署名リクエスト (CSR) を取得する許可を付与	読み取り	certificate-authority*		
GetPolicy	プライベート CA AWS でポリシーを取得するアクセス許可を付与します	読み取り	certificate-authority*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ImportCertificateAuthorityCertificate	SSL/TLS 証明書を AWS プライベート CA にインポートして、プライベート CA の CA AWS 証明書として使用する許可を付与	書き込み	certificate-authority*		
IssueCertificate	AWS プライベート CA 証明書を発行するアクセス許可を付与します	書き込み	certificate-authority*		
				acm-pca:TemplateArn	
ListCertificateAuthorities	プライベート CA AWS 認証機関 ARNs のリストと、呼び出し元のアカウントの各 CA のステータスの概要を取得するアクセス許可を付与します	リスト			
ListPermissions	プライベート CA AWS 認証機関に適用されたアクセス許可を一覧表示するアクセス許可を付与します	読み取り	certificate-authority*		
ListTags	プライベート CA AWS 認証機関に適用されたタグを一覧表示するアクセス許可を付与します	読み取り	certificate-authority*		
PutPolicy	プライベート CA AWS にポリシーを配置するアクセス許可を付与します	権限の管理	certificate-authority*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RestoreCertificateAuthority	AWS プライベート CA を削除時の状態に復元するアクセス許可を付与します	書き込み	certificate-authority*		
RevokeCertificate	AWS プライベート CA によって発行された証明書を取り消すアクセス許可を付与します	書き込み	certificate-authority*		
TagCertificateAuthority	プライベート CA に 1 AWS つ以上のタグを追加するアクセス許可を付与します	Tagging	certificate-authority*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagCertificateAuthority	プライベート CA から 1 AWS つ以上のタグを削除するアクセス許可を付与します	Tagging	certificate-authority*	aws:RequestTag/${TagKey}	
				aws:TagKeys	
UpdateCertificateAuthority	プライベート CA AWS の設定を更新するアクセス許可を付与します	書き込み	certificate-authority*		

AWS Private Certificate Authority で定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアク

ションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
certificate-authority	`arn:${Partition}:acm-pca:${Region}:${Account}:certificate-authority/${CertificateAuthorityId}`	aws:ResourceTag/${TagKey}

AWS Private Certificate Authority の条件キー

AWS Private Certificate Authority は、IAM ポリシーの `Condition`要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
acm-pca:TemplateArn	証明書発行リクエストで使用した証明書テンプレートの ARN でアクセスをフィルタリングします	ARN
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS PrivateLink のアクション、リソース、および条件キー

AWS PrivateLink (サービスプレフィックス: vpce) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS PrivateLink で定義されるアクション
- AWS PrivateLink で定義されるリソースタイプ
- AWS PrivateLink の条件キー

AWS PrivateLink で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AllowMultiRegion [アクセス許可のみ]	マルチリージョン VPC エンドポイントと VPC エンドポイントサービス設定を管理するアクセス許可を付与します	書き込み			

AWS PrivateLink で定義されるリソースタイプ

AWS PrivateLink は、IAM ポリシーステートメントの Resource要素でのリソース ARN の指定をサポートしていません。 AWS PrivateLink へのアクセスを許可するには、ポリシー"Resource": "*"で を指定します。

AWS PrivateLink の条件キー

VPC エンドポイントには、ポリシーステートメントの Condition要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Proton のアクション、リソース、および条件キー

AWS Proton (サービスプレフィックス: proton) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Proton で定義されるアクション
- AWS Proton で定義されるリソースタイプ
- AWS Proton の条件キー

AWS Proton で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptEnvironmentAccountConnection	別の環境アカウントからの環境アカウント接続要求を拒否する許可を付与	書き込み	environment-account-connection*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelComponentDeployment	コンポーネントのデプロイをキャンセルする許可の付与	書き込み	component*		
CancelEnvironmentDeployment	環境デプロイをキャンセルする許可を付与	書き込み	environment*		
				proton:EnvironmentTemplate	
CancelServiceInstanceDeployment	サービスインスタンスデプロイをキャンセルする許可を付与	書き込み	service-instance*		
				proton:ServiceTemplate	
CancelServicePipelineDeployment	サービスパイプラインデプロイをキャンセルする許可を付与	書き込み	service*		
				proton:ServiceTemplate	
CreateComponent	コンポーネントを作成する許可の付与	書き込み	component*		
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateEnvironment	環境を作成する許可を付与	書き込み	environment*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey} proton:EnvironmentTemplate	
CreateEnvironmentAccountConnection	環境アカウント接続を作成する許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironmentTemplate	環境テンプレートを作成する許可を付与	書き込み	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateEnvironmentTemplateMajorVersion	環境テンプレートのメジャーバージョンを作成する許可を付与。非推奨-代わりに CreateEnvironmentTemplateVersion を使用してください	書き込み	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironmentTemplateMinorVersion	環境テンプレートのマイナーバージョンを作成する許可を付与。非推奨-代わりに CreateEnvironmentTemplateVersion を使用してください	書き込み	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironmentTemplateVersion	環境テンプレートのバージョンを作成する許可を付与	書き込み	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRepository	リポジトリを作成する許可を付与。	書き込み	repository*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateService	サービスを作成する許可を付与	書き込み	service*		codestar-connections:PassConnection
				aws:TagKeys aws:RequestTag/${TagKey} proton:ServiceTemplate	
CreateServiceInstance	サービスインスタンスを作成する許可を付与	書き込み	service-instance*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey} proton:ServiceTemplate	
CreateServiceSyncConfig	サービス同期設定を作成する許可を付与	書き込み			
CreateServiceTemplate	サービステンプレートを作成する許可を付与	書き込み	service-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceTemplateMajorVersion	サービステンプレートのメジャーバージョンを作成する許可を付与。非推奨-代わりにCreateServiceTemplateVersion を使用してください	書き込み	service-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateServiceTemplateMinorVersion	サービステンプレートのマイナーバージョンを作成する許可を付与。非推奨-代わりに CreateServiceTemplateVersion を使用してください	書き込み	service-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceTemplateVersion	サービステンプレートのバージョンを作成する許可を付与	書き込み	service-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateTemplateSyncConfig	テンプレート同期設定を作成する許可を付与。	書き込み			
DeleteAccountRoles	アカウントロールを削除する許可を付与。非推奨-代わりに UpdateAccountSettings を使用してください	書き込み			
DeleteComponent	コンポーネントを削除する許可の付与	書き込み	component*		
DeleteDeployment	デプロイを削除する許可を付与	書き込み	deployment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteEnvironment	環境を削除する許可を付与します	書き込み	environment*		
				proton:EnvironmentTemplate	
DeleteEnvironmentAccountConnection	環境アカウント接続を削除する許可を付与	書き込み	environment-account-connection*		
DeleteEnvironmentTemplate	環境テンプレートを削除する許可を付与	書き込み	environment-template*		
DeleteEnvironmentTemplateMajorVersion	環境テンプレートのメジャーバージョンを削除する許可を付与。非推奨-代わりに DeleteEnvironmentTemplateVersion を使用してください	書き込み	environment-template*		
DeleteEnvironmentTemplateMinorVersion	環境テンプレートのマイナーバージョンを削除する許可を付与。非推奨-代わりに DeleteEnvironmentTemplateVersion を使用してください	書き込み	environment-template*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteEnvironmentTemplateVersion	環境テンプレートのバージョンを削除する許可を付与	書き込み	environment-template*		
DeleteRepository	リポジトリを削除する許可を付与	書き込み	repository*		
DeleteService	サービスを削除する許可を付与	書き込み	service*		
				proton:ServiceTemplate	
DeleteServiceSyncConfig	サービス同期設定を削除する許可を付与	書き込み			
DeleteServiceTemplate	サービステンプレートを削除する許可を付与	書き込み	service-template*		
DeleteServiceTemplateMajorVersion	サービステンプレートのメジャーバージョンを削除する許可を付与。非推奨-代わりに DeleteServiceTemplateVersion を使用してください	書き込み	service-template*		
DeleteServiceTemplateMinorVersion	サービステンプレートのマイナーバージョンを削除する許可を付与。非推奨-代わりに DeleteServiceTemplateVersion を使用してください	書き込み	service-template*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteServiceTemplateVersion	サービステンプレートのバージョンを削除する許可を付与	書き込み	service-template*		
DeleteTemplateSyncConfig	TemplateSyncConfig を削除する許可を付与。	書き込み			
GetAccountRoles	アカウントロールを取得する許可を付与。非推奨-代わりに GetAccountSettings を使用してください	読み込み			
GetAccountSettings	アカウント設定を記述する許可を付与	読み取り			
GetComponent	コンポーネントを記述する許可を付与	読み取り	component*		
GetDeployment	デプロイを記述する許可を付与	読み取り	deployment*		
GetEnvironment	環境を記述する許可を付与	読み込み	environment*		
GetEnvironmentAccountConnection	環境アカウント接続を記述する許可を付与	読み込み	environment-account-connection*		
GetEnvironmentTemplate	環境テンプレートを記述する許可を付与	読み込み	environment-template*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetEnvironmentTemplateMajorVersion	環境テンプレートのメジャーバージョンを取得する許可を付与。非推奨-代わりに GetEnvironmentTemplateVersion を使用してください	読み込み	environment-template*		
GetEnvironmentTemplateMinorVersion	環境テンプレートのマイナーバージョンを取得する許可を付与。非推奨-代わりに GetEnvironmentTemplateVersion を使用してください	読み込み	environment-template*		
GetEnvironmentTemplateVersion	環境テンプレートのバージョンを記述する許可を付与	読み込み	environment-template*		
GetRepository	リポジトリの詳細を取得する許可を付与。	読み込み	repository*		
GetRepositorySyncStatus	リポジトリの最新の同期ステータスを取得する許可を付与。	読み取り			
GetResourceTemplateVersionStatusCounts	リソーステンプレートのバージョンステータスカウントを一覧表示する許可を付与	読み取り			
GetResourcesSummary	リソース概要を取得する許可を付与	読み取り			
GetService	サービスを記述する許可を付与	読み込み	service*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetServiceInstance	サービスインスタンスを記述する許可を付与	読み取り	service-instance*		
GetServiceInstanceSyncStatus	サービスインスタンスの同期ステータスを記述する許可を付与	読み取り			
GetServiceSyncBlockerSummary	サービスまたはサービスインスタンスについて、サービス同期の阻害要因の詳細を表示する許可を付与	読み取り			
GetServiceSyncConfig	サービス同期設定を記述する許可を付与	読み取り			
GetServiceTemplate	サービステンプレートを記述する許可を付与	読み込み	service-template*		
GetServiceTemplateMajorVersion	サービステンプレートのメジャーバージョンを取得する許可を付与。非推奨-代わりにGetServiceTemplateVersionを使用してください	読み込み	service-template*		
GetServiceTemplateMinorVersion	サービステンプレートのマイナーバージョンを取得する許可を付与。非推奨-代わりにGetServiceTemplateVersionを使用してください	読み込み	service-template*		
GetServiceTemplateVersion	サービステンプレートのバージョンを記述する許可を付与	読み込み	service-template*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetTemplateSyncConfig	TemplateSyncConfig の詳細を取得する許可を付与。	読み込み			
GetTemplateSyncStatus	テンプレートの同期ステータスの詳細を取得する許可を付与。	読み取り			
ListComponentOutputs	コンポーネント出力を一覧表示する許可の付与	リスト	component *		
			deployment		
ListComponentProvisionedResources	コンポーネント プロビジョニング リソースを一覧表示する許可の付与	リスト	component *		
ListComponents	コンポーネントを一覧表示する許可の付与	リスト	environment		
			service		
			service-instance		
ListDeployments	デプロイを一覧表示する許可を付与	リスト			
ListEnvironmentAccountConnections	環境アカウント接続を一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListEnvironmentOutputs	環境を一覧表示する許可を付与します	リスト	environment*		
			deployment		
ListEnvironmentProvisionedResources	環境プロビジョニングリソースを一覧表示する許可を付与します	リスト	environment*		
ListEnvironmentTemplateMajorVersions	環境テンプレートのメジャーバージョンを一覧表示する許可を付与。非推奨-代わりに ListenVironmentTemplateVersions を使用してください	リスト	environment-template*		
ListEnvironmentTemplateMinorVersions	環境テンプレートのマイナーバージョンを一覧表示する許可を付与。非推奨-代わりに ListenVironmentTemplateVersions を使用してください	リスト	environment-template*		
ListEnvironmentTemplateVersions	環境テンプレートのバージョンを一覧表示する許可を付与	リスト	environment-template*		
ListEnvironmentTemplates	環境テンプレートを一覧表示する許可を付与	リスト			
ListEnvironments	環境を一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListRepositories	リポジトリを一覧表示する許可を付与。	リスト			
ListRepositorySyncDefinitions	リポジトリ同期定義を一覧表示する許可を付与。	リスト			
ListServiceInstanceOutputs	サービスインスタンス出力を一覧表示する許可を付与します	リスト	service*		
			service-instance*		
			deployment		
ListServiceInstanceProvisionedResources	サービスインスタンスのプロビジョニングリソースを一覧表示する許可を付与します	リスト	service*		
			service-instance*		
ListServiceInstances	サービスインスタンスを一覧表示する許可を付与	リスト			
ListServicePipelineOutputs	サービスパイプライン出力を一覧表示する許可を付与します	リスト	service*		
			deployment		
ListServicePipelineProvisionedResources	サービスパイプラインのプロビジョニングリソースを一覧表示する許可を付与します	リスト	service*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListServiceTemplateMajorVersions	サービステンプレートのメジャーバージョンを一覧表示する許可を付与。非推奨-代わりに ListServiceTemplateVersions を使用してください	リスト	service-template*		
ListServiceTemplateMinorVersions	サービステンプレートのマイナーバージョンを一覧表示する許可を付与。非推奨-代わりに ListServiceTemplateVersions を使用してください	リスト	service-template*		
ListServiceTemplateVersions	サービステンプレートのバージョンを一覧表示する許可を付与	リスト	service-template*		
ListServiceTemplates	サービステンプレートを一覧表示する許可を付与	リスト			
ListServices	サービスを一覧表示する許可を付与	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与。	読み込み	component		
			environment		
			environment-account-connection		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			environment-template		
			environment-template-major-version		
			environment-template-minor-version		
			environment-template-version		
			repository		
			service		
			service-instance		
			service-template		
			service-template-major-version		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			service-template-minor-version		
			service-template-version		
NotifyResourceDeploymentStatusChange	Proton にリソースデプロイのステータスの変更を通知する許可を付与	書き込み	environment		
			service-instance		
RejectEnvironmentAccountConnection	別の環境アカウントからの環境アカウント接続要求を拒否する許可を付与	書き込み	environment-account-connection*		
TagResource	リソースにタグを追加するアクセス許可を付与します	タグ付け	component		
			environment		
			environment-account-connection		
			environment-template		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			environment-template-major-version		
			environment-template-minor-version		
			environment-template-version		
			repository		
			service		
			service-instance		
			service-template		
			service-template-major-version		
			service-template-minor-version		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			service-template-version		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	リソースからタグを削除する許可を付与	Tagging	component		
			environment		
			environment-account-connection		
			environment-template		
			environment-template-major-version		
			environment-template-minor-version		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			environment-template-version		
			repository		
			service		
			service-instance		
			service-template		
			service-template-major-version		
			service-template-minor-version		
			service-template-version		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateAccountRoles	アカウントロールを更新する許可を付与。非推奨-代わりに UpdateAccountSettings を使用してください	書き込み			iam:PassRole
UpdateAccountSettings	アカウント設定を更新する許可を付与	書き込み			iam:PassRole
UpdateComponent	コンポーネントを更新する許可の付与	書き込み	component*		
UpdateEnvironment	環境を更新する許可を付与	書き込み	environment*		iam:PassRole
				proton:EnvironmentTemplate	
UpdateEnvironmentAccountConnection	環境アカウント接続を更新する許可を付与	書き込み	environment-account-connection*		
UpdateEnvironmentTemplate	環境テンプレートを更新する許可を付与	書き込み	environment-template*		
UpdateEnvironmentTemplateMajorVersion	環境テンプレートのメジャーバージョンを更新する許可を付与。非推奨-代わりに UpdateEnvironmentTemplateVersion を使用してください	書き込み	environment-template*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateEnvironmentTemplateMinorVersion	環境テンプレートのマイナーバージョンを更新する許可を付与。非推奨-代わりに UpdateEnvironmentTemplateVersion を使用してください	書き込み	environment-template*		
UpdateEnvironmentTemplateVersion	環境テンプレートのバージョンを更新する許可を付与	書き込み	environment-template*		
UpdateService	サービスを更新する許可を付与	書き込み	service*		
				proton:ServiceTemplate	
UpdateServiceInstance	サービスインスタンスを更新する許可を付与	書き込み	service-instance*		
				proton:ServiceTemplate	
UpdateServicePipeline	サービスパイプラインを更新する許可を付与	書き込み	service*		
				proton:ServiceTemplate	
UpdateServiceSyncBlocker	サービス同期の阻害要因を更新する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateServiceSyncConfig	サービス同期設定を更新するアクセス許可を付与	書き込み			
UpdateServiceTemplate	サービステンプレートを更新する許可を付与。	書き込み	service-template*		
UpdateServiceTemplateMajorVersion	サービステンプレートのメジャーバージョンを更新する許可を付与。非推奨-代わりにUpdateServiceTemplateVersion を使用してください	書き込み	service-template*		
UpdateServiceTemplateMinorVersion	サービステンプレートのマイナーバージョンを作成する許可を付与。非推奨-代わりにUpdateServiceTemplateVersion を使用してください	書き込み	service-template*		
UpdateServiceTemplateVersion	サービステンプレートのバージョンを更新する許可を付与	書き込み	service-template*		
UpdateTemplateSyncConfig	TemplateSyncConfig を更新する許可を付与。	書き込み			

AWS Proton で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
environment-template	arn:${Partition}:proton:${Region}:${Account}:environment-template/${Name}	aws:ResourceTag/${TagKey}
environment-template-version	arn:${Partition}:proton:${Region}:${Account}:environment-template/${TemplateName}:${MajorVersion}.${MinorVersion}	aws:ResourceTag/${TagKey}
environment-template-major-version	arn:${Partition}:proton:${Region}:${Account}:environment-template/${TemplateName}:${MajorVersionId}	aws:ResourceTag/${TagKey}
environment-template-minor-version	arn:${Partition}:proton:${Region}:${Account}:environment-template/${TemplateName}:${MajorVersionId}.${MinorVersionId}	aws:ResourceTag/${TagKey}
service-template	arn:${Partition}:proton:${Region}:${Account}:service-template/${Name}	aws:ResourceTag/${TagKey}
service-template-version	arn:${Partition}:proton:${Region}:${Account}:service-template/${TemplateName}:${MajorVersion}.${MinorVersion}	aws:ResourceTag/${TagKey}
service-template-major-version	arn:${Partition}:proton:${Region}:${Account}:service-template/${TemplateName}:${MajorVersionId}	aws:ResourceTag/${TagKey}
service-template-minor-version	arn:${Partition}:proton:${Region}:${Account}:service-template/${TemplateName}:${MajorVersionId}.${MinorVersionId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
environment	arn:${Partition}:proton:${Region}:${Account}:environment/${Name}	aws:ResourceTag/${TagKey}
service	arn:${Partition}:proton:${Region}:${Account}:service/${Name}	aws:ResourceTag/${TagKey}
service-instance	arn:${Partition}:proton:${Region}:${Account}:service/${ServiceName}/service-instance/${Name}	aws:ResourceTag/${TagKey}
environment-account-connection	arn:${Partition}:proton:${Region}:${Account}:environment-account-connection/${Id}	aws:ResourceTag/${TagKey}
repository	arn:${Partition}:proton:${Region}:${Account}:repository/${Provider}:${Name}	aws:ResourceTag/${TagKey}
component	arn:${Partition}:proton:${Region}:${Account}:component/${Id}	aws:ResourceTag/${TagKey}
deployment	arn:${Partition}:proton:${Region}:${Account}:deployment/${Id}	aws:ResourceTag/${TagKey}

AWS Proton の条件キー

AWS Proton は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString
proton:EnvironmentTemplate	リソースに関連する指定された環境テンプレートによって、アクセスをフィルタリング	String
proton:ServiceTemplate	リソースに関連する指定されたサービステンプレートによって、アクセスをフィルタリング	String

AWS Purchase Orders Console のアクション、リソース、条件キー

AWS Purchase Orders Console (サービスプレフィックス: `purchase-orders`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Purchase Orders Console で定義されるアクション
- AWS Purchase Orders Console で定義されるリソースタイプ
- AWS Purchase Orders Console の条件キー

AWS Purchase Orders Console で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddPurchaseOrder [アクセス許可のみ]	新しい発注書を追加する許可を付与	書き込み	purchase-order*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePurchaseOrder [アクセス許可のみ]	発注書を削除する許可を付与	書き込み	purchase-order*		
				aws:ResourceTag/${TagKey}	
GetConsoleActionSetEnforced [アクセス許可のみ]	Billing、Cost Management、および Account コンソールに対する承認を制御するために、既存またはきめ細かい IAM アクションを使用するかどうかを表示するための許可を付与します	読み取り			
GetPurchaseOrder [許可のみ]	発注書を取得する許可を付与	読み取り	purchase-order*		
				aws:ResourceTag/${TagKey}	
ListPurchaseOrderI	発注書に対する請求書を一覧表示する許可を付与	リスト	purchase-order*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
nvoices [許可のみ]				aws:ResourceTag/${TagKey}	
ListPurchaseOrders [許可のみ]	アカウントのすべての発注書を一覧表示する許可を付与します	リスト			
ListTagsForResource [許可のみ]	発注書のタグを一覧表示する許可を付与します	読み取り	purchase-order		
				aws:ResourceTag/${TagKey}	
ModifyPurchaseOrders [許可のみ]	発詳細および詳細を変更するアクセス許可を付与	書き込み	purchase-order*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
TagResource [アクセス許可のみ]	指定されたキーと値のペアで発注書にタグ付けする許可を付与します	Tagging	purchase-order*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource [アクセス許可のみ]	発注書からタグを削除するアクセス許可を付与します	Tagging	purchase-order*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateConsoleActionSetEnforced [アクセス許可のみ]	Billing、Cost Management、および Account コンソールに対する承認を制御するために、既存またはきめ細かい IAM アクションを使用するかどうかを変更するための許可を付与します	書き込み			
UpdatePurchaseOrder [アクセス許可のみ]	既存の発注書を更新する許可を付与	書き込み	purchase-order*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdatePurchaseOrderStatus [アクセス許可のみ]	発注書のステータスを設定する許可を付与	書き込み	purchase-order*		
				aws:ResourceTag/${TagKey}	
ViewPurchaseOrders [アクセス許可のみ]	発詳細および詳細を表示するアクセス許可を付与	読み取り	purchase-order		
				aws:ResourceTag/${TagKey}	

AWS Purchase Orders Console で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource 工レメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
purchase-order	`arn:${Partition}:purchase-orders::${Account}:purchase-order/${ResourceName}`	aws:ResourceTag/${TagKey}

AWS Purchase Orders Console の条件キー

AWS Purchase Orders Console では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに

絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグのキーと値でアクセスをフィルター	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーおよび値のペアによってアクセスをフィルタリングします。	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon Q のアクション、リソース、および条件キー

Amazon Q (サービスプレフィックス: q) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Q で定義されるアクション
- Amazon Q で定義されるリソースタイプ
- Amazon Q の条件キー

Amazon Q で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateConnectorResource [アクセス許可のみ]	AWS リソースを Amazon Q コネクタに関連付けるアクセス許可を付与します	書き込み			
CreateAssignment [アクセス許可のみ]	Amazon Q Developer プロファイルのユーザーまたはグループ割り当てを作成する許可を付与する	書き込み	profile*		
				identitystore:UserId identitystore:GroupId	
CreateAuthGrant [アクセス許可のみ]	Amazon Q で OAuth ユーザーを作成するアクセス許可を付与します	書き込み			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
CreateOAuthAppConnection [アクセス許可のみ]	Amazon Q に OAuth アプリケーションを登録する許可を付与	書き込み			kms:Decrypt kms:GenerateDataKe

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					yWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
CreatePlugin [アクセス許可のみ]	Amazon Q でサードパーティープラグインを作成および設定するアクセス許可を付与します	書き込み	plugin*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteAssignment [アクセス許可のみ]	Amazon Q Developer プロファイルのユーザーまたはグループ割り当てを削除する許可を付与する	書き込み	profile*		
				identitystore:UserId identitystore:GroupId	
DeleteConversation [アクセス許可のみ]	Amazon Q との会話を削除するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteOAuthAppConnection [アクセス許可のみ]	Amazon Q で OAuth アプリケーションを削除するアクセス許可を付与します	書き込み			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
DeletePlugin [アクセス許可のみ]	Amazon Q で設定されたプラグインを削除するアクセス許可を付与します	書き込み	plugin*		
				aws:ResourceTag/${TagKey}	
GenerateCodeFromCommands [アクセス許可のみ]	Amazon Q の CLI コマンドからコードを生成する許可を付与する	読み取り			
GenerateCodeRecommendations [許可のみ]	Amazon Q でコードレコメンデーションを生成するアクセス許可を付与します	読み取り			
GetConnector [許可のみ]	特定の Amazon Q コネクタに関する情報を表示するアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetConversation [許可のみ]	Amazon Q との特定の会話に関連付けられた個々のメッセージを取得するためのアクセス許可を付与	読み取り			
GetIdentityMetadata [許可のみ]	ID メタデータを取得するための許可を Amazon Q に付与する	読み取り			
GetPlugin [許可のみ]	設定された特定の Amazon Q プラグインに関する情報を表示するアクセス許可を付与します	読み取り	plugin*		
				aws:ResourceTag/${TagKey}	
GetTroubleshootingResults [許可のみ]	Amazon Q でトラブルシューティングの結果を取得するためのアクセス許可を付与	読み取り			
ListConversations [許可のみ]	特定の Amazon Q ユーザーに関連付けられた個々の会話を一覧表示する許可を付与する	読み取り			
ListDashboardMetrics [許可のみ]	Amazon Q ダッシュボードに入力するメトリクスを読み取るアクセス許可を付与します	リスト			
ListPluginProviders [許可のみ]	Amazon Q で使用可能なプラグインを一覧表示する許可を付与	リスト			
ListPlugins [許可のみ]	Amazon Q で設定されたプラグインを一覧表示するアクセス許可を付与します	リスト	plugin*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTagsForResource [許可のみ]	Amazon Q リソースに関連付けられているすべてのタグを一覧表示するアクセス許可を付与します	リスト	plugin	aws:ResourceTag/${TagKey}	
PassRequest [許可のみ]	Amazon Q がユーザーに代わってアクションを実行することを許可する許可を付与する	書き込み			
RejectConnector [アクセス許可のみ]	Amazon Q コネクタの接続リクエストを拒否するアクセス許可を付与します	書き込み			
SendEvent [アクセス許可のみ]	非同期 Amazon Q アクションをトリガーするアクセス許可を付与します	書き込み			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
SendMessage [アクセス許可のみ]	Amazon Q にメッセージを送信するためのアクセス許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartConversation [アクセス許可のみ]	Amazon Q との会話を開始するためのアクセス許可を付与	書き込み			
StartTroubleshootingAnalysis [アクセス許可のみ]	Amazon Q でトラブルシューティング分析を開始するためのアクセス許可を付与	書き込み			
StartTroubleshootingResolutionExplanation [アクセス許可のみ]	Amazon Q でトラブルシューティングの解決策の説明を開始するためのアクセス許可を付与	書き込み			
TagResource [アクセス許可のみ]	タグを Amazon Q リソースに関連付けるアクセス許可を付与します	Tagging	plugin		
				aws:ResourceTag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [アクセス許可のみ]	Amazon Q リソースに関連付けられたタグを削除するアクセス許可を付与します	Tagging	plugin		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateAuthGrant [アクセス許可のみ]	Amazon Q で OAuth ユーザーを更新する許可を付与	書き込み			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
UpdateConversation [アクセス許可のみ]	Amazon Q との会話を更新する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateOAuthAppConnection [アクセス許可のみ]	Amazon Q で OAuth アプリケーションを更新する許可を付与	書き込み			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
UpdatePlugin [アクセス許可のみ]	Amazon Q でサードパーティープラグインを更新する許可を付与	書き込み	plugin*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateTroubleshootingCommandResult [アクセス許可のみ]	Amazon Q でトラブルシューティングコマンドの結果を更新する許可を付与する	書き込み			
UsePlugin [アクセス許可のみ]	Amazon Q プラグインを使用するアクセス許可を付与します	書き込み	plugin*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
VerifyOAuthAppConnection [アクセス許可のみ]	Amazon Q で OAuth アプリケーションを検証するアクセス許可を付与します	書き込み			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo

Amazon Q で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
profile	`arn:${Partition}:codewhisperer:${Region}:${Account}:profile/${Identifier}`	
plugin	`arn:${Partition}:qdeveloper:${Region}:${Account}:plugin/${Identifier}`	aws:ResourceTag/${TagKey}

Amazon Q の条件キー

Amazon Q は、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	Amazon Q リソースに関連付けられたタグでアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
identitystore:GroupId	IAM Identity Center ユーザー ID でアクセスをフィルタリングする	ArrayOfString
identitystore:UserId	IAM Identity Center ユーザー ID でアクセスをフィルタリングします	ArrayOfString

Amazon Q Business のアクション、リソース、および条件キー

Amazon Q Business (サービスプレフィックス: qbusiness) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Q Business で定義されるアクション
- Amazon Q Business で定義されるリソースタイプ
- Amazon Q Business の条件キー

Amazon Q Business で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AllowVendedLogDeliveryForResource [アクセス許可のみ]	Amazon Q Business アプリケーションリソースの vended log 配信を設定する許可を付与する	権限の管理	application*		
				aws:ResourceTag/${TagKey}	
AssociatePermission	リソースベースのポリシーステートメントをアプリケーションに関連付けるアクセス許可を付与します	書き込み	application*		qbusiness:PutResourcePolicy
BatchDeleteDocument	ドキュメントを一括で削除する許可を付与	書き込み	application*		
			index*		
BatchPutDocument	ドキュメントを一括で配置する許可を付与	書き込み	application*		
			index*		
CancelSubscription	サブスクリプションをキャンセルする許可を付与する	書き込み	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			subscription*		
Chat	アプリケーションを使用してチャットするためのアクセス許可を付与	読み取り	application*		
ChatSync	アプリケーションを使用して同期的にチャットするためのアクセス許可を付与	読み取り	application*		
CheckDocumentAccess	ユーザーがドキュメントにアクセスできるかどうかを確認するアクセス許可を付与します	読み取り	application*		
			index*		
CreateAnonymousWebExperienceUrl	匿名の Amazon Q Business ウェブエクスペリエンス用の一意の URL を作成するアクセス許可を付与します	書き込み	application*		
			web-experience*		
CreateApplication	アプリケーションを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateChatResponseConfiguration	アプリケーションにチャットレスポンス設定を作成するアクセス許可を付与します	書き込み	application*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataAccessor	DataAccessor を作成するアクセス許可をアプリケーションに付与します	書き込み	application*		qbusiness:CreateDataAccessorWithTti
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataAccessorWithTti [アクセス許可のみ]	AWS IAM Identity Center Trusted Token Issuer based DataAccessor を作成するアクセス許可をアプリケーションに付与します	書き込み	application*		
CreateDataSource	特定のアプリケーションとインデックスのデータソースを作成するためのアクセス許可を付与	書き込み	application*		
			index*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIndex	特定のアプリケーションのインデックスを作成するためのアクセス許可を付与	書き込み	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIntegration	Q Business アプリケーションの新しい統合を作成するアクセス許可を付与します	書き込み	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePlugin	特定のアプリケーションのプラグインを作成するためのアクセス許可を付与	書き込み	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRetriever	特定のアプリケーションのレトリバーを作成するためのアクセス許可を付与	書き込み	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscription	サブスクリプションを作成する許可を付与する	書き込み	application*		
				identitystore:UserId identitystore:GroupId	
CreateUser	ユーザーを作成する許可を付与	書き込み	application*		
CreateWebExperience	特定のアプリケーションのウェブエクスペリエンスを作成するためのアクセス許可を付与	書き込み	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	アプリケーションを削除する許可を付与	書き込み	application*		
DeleteAttachment	現在のチャットコンテキストで添付ファイルを削除するアクセス許可を付与します	書き込み	application*		
DeleteChatControlsConfiguration	アプリケーションのチャットコントロール設定を削除するためのアクセス許可を付与	書き込み	application*		
DeleteChatResponseConfiguration	チャットレスポンス設定を削除するアクセス許可を付与します	書き込み	application*		
			chat-response-configuration*		
DeleteConversation	会話を削除するためのアクセス許可を付与	書き込み	application*		
DeleteDataAccessor	DataAccessor を削除する許可を付与	書き込み	application*		
			data-accessor*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteDataSource	データソースを削除するためのアクセス許可を付与	書き込み	application*		
			data-source*		
			index*		
DeleteGroup	グループを削除するアクセス許可を付与	書き込み	application*		
			index*		
DeleteIndex	インデックスを削除するためのアクセス許可を付与	書き込み	application*		
			index*		
DeleteIntegration	Q Business アプリケーションの統合を削除するアクセス許可を付与します	書き込み	application*		
			integration*		
DeletePlugin	プラグインを削除するためのアクセス許可を付与	書き込み	application*		
			plugin*		
DeleteRetriever	レトリバーを削除するためのアクセス許可を付与	書き込み	application*		
			retriever*		
DeleteUser	ユーザーを削除する許可を付与	書き込み	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteWebExperience	ウェブエクスペリエンスを削除するためのアクセス許可を付与	書き込み	application*		
			web-experience*		
DisableAclOnDataSource [アクセス許可のみ]	Amazon Q Business データソースリソースの作成中に ACL クロールを無効にする許可を付与する	書き込み	application*		
DisassociatePermission	リソースベースのポリシーステートメントのアプリケーションへの関連付けを解除するアクセス許可を付与します	書き込み	application*		qbusiness:PutResourcePolicy
GetApplication	アプリケーションを取得する許可を付与	読み取り	application*		
GetChatControlsConfiguration	アプリケーションのチャットコントロール設定を取得するためのアクセス許可を付与	リスト	application*		
GetChatResponseConfiguration	チャットレスポンス設定を取得するアクセス許可を付与します	読み取り	application*		
			chat-response-configuration*		
GetDataAccessor	DataAccessor を取得する許可を付与	読み取り	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			data-accessor*		
GetDataSource	データソースを取得するためのアクセス許可を付与	読み取り	application*		
			data-source*		
			index*		
GetDocumentContent	ドキュメントコンテンツを取得するアクセス許可を付与します	読み取り	application*		
			index*		
GetGroup	グループを取得するためのアクセス許可を付与	読み取り	application*		
			index*		
GetIndex	インデックスを取得するためのアクセス許可を付与	読み取り	application*		
			index*		
GetIntegration	Q Business アプリケーションの統合を取得する許可を付与	読み取り	application*		
			integration*		
GetMedia	システムメッセージに関連付けられたメディアを取得するアクセス許可を付与します	読み取り	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetPlugin	プラグインを取得するためのアクセス許可を付与	読み取り	application*		
			plugin*		
GetPolicy	アプリケーションのリソースベースのポリシーを取得するアクセス許可を付与します	読み取り	application*		
GetRetriever	レトリバーを取得するためのアクセス許可を付与	読み取り	application*		
			retriever*		
GetUser	ユーザーを取得するためのアクセス許可を付与	読み取り	application*		
GetWebExperience	ウェブエクスペリエンスを取得するためのアクセス許可を付与	読み取り	application*		
			web-experience*		
ListApplications	アプリケーションを一覧表示するためのアクセス許可を付与	リスト			
ListAttachments	現在のチャットコンテキストで添付ファイルを一覧表示するアクセス許可を付与します	リスト	application*		
ListChatResponseConfigurations	アプリケーションのチャットレスポンス設定を一覧表示するアクセス許可を付与します	リスト	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListConversations	アプリケーションのすべての会話を一覧表示するためのアクセス許可を付与	リスト	application*		
ListDataAccessors	アプリケーションの DataAccessors を一覧表示する許可を付与	リスト	application*		
ListDataSourceSyncJobs	データソース同期ジョブの履歴を取得する許可を付与	リスト	application*		
			data-source*		
			index*		
ListDataSources	アプリケーションとインデックスのデータソースを一覧表示するためのアクセス許可を付与	リスト	application*		
			index*		
ListDocuments	すべてのドキュメントを一覧表示するためのアクセス許可を付与	リスト	application*		
			index*		
ListGroups	グループを一覧表示するためのアクセス許可を付与する	リスト	application*		
			index*		
ListIndices	アプリケーションのインデックスを一覧表示するためのアクセス許可を付与	リスト	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListIntegrations	Q Business アプリケーションのすべての統合を一覧表示するアクセス許可を付与します	リスト	application*		
ListMessages	すべてのメッセージを一覧表示するためのアクセス許可を付与	リスト	application*		
ListPluginActions	アプリケーション内のプラグインのプラグインアクションを一覧表示するアクセス許可を付与します	読み取り	application*		
			plugin*		
ListPluginTypeActions	プラグインタイプのすべてのアクションを一覧表示するアクセス許可を付与します	読み取り			
ListPluginTypeMetadata	すべてのプラグインタイプのメタデータを一覧表示するアクセス許可を付与します	読み取り			
ListPlugins	アプリケーションのプラグインを一覧表示するためのアクセス許可を付与	リスト	application*		
ListRetrievers	アプリケーションのレトリバーを一覧表示するためのアクセス許可を付与	リスト	application*		
ListSubscriptions	サブスクリプションを一覧表示する許可を付与	リスト	application*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	application		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			chat-response-configuration		
			data-accessor		
			data-source		
			index		
			integration		
			plugin		
			retriever		
			web-experience		
ListWebExperiences	アプリケーションのウェブエクスペリエンスを一覧表示するためのアクセス許可を付与	リスト	application*		
PutFeedback	会話メッセージに関するフィードバックを入力するためのアクセス許可を付与	書き込み	application*		
PutGroup	ユーザーのグループを入力するためのアクセス許可を付与	書き込み	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			index*		
PutResourcePolicy [アクセス許可のみ]	リソースベースのポリシーステートメントをアプリケーションに配置するアクセス許可を付与します	書き込み	application*		
SearchRelevantContent	Amazon Q Business Application から関連コンテンツを検索する許可を付与	読み取り	application*		
StartDataSourceSyncJob	データソース同期ジョブを開始する許可を付与	書き込み	application*		
			data-source*		
			index*		
StartDeployment	統合のデプロイを開始する許可を付与	書き込み	application*		
			integration*		
StopDataSourceSyncJob	データソース同期ジョブを停止する許可を付与	書き込み	application*		
			data-source*		
			index*		
TagResource	指定されたキーと値のペアでリソースにタグを付けるアクセス許可を付与	Tagging	application		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			chat-response-configuration		
			data-accessor		
			data-source		
			index		
			integration		
			plugin		
			retriever		
			web-experience		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	所与のキーを持つタグをリソースから削除する許可を付与	Tagging	application		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			chat-response-configuration		
			data-accessor		
			data-source		
			index		
			integration		
			plugin		
			retriever		
			web-experience		
				aws:TagKeys	
UpdateApplication	アプリケーションを更新するためのアクセス許可を付与	書き込み	application*		
UpdateChatControlsConfiguration	アプリケーションのチャットコントロール設定を更新するためのアクセス許可を付与	書き込み	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateChatResponseConfiguration	チャットレスポンス設定を更新するアクセス許可を付与します	書き込み	application*		
			chat-response-configuration*		
UpdateDataAccessor	DataAccessor を更新する許可を付与	書き込み	application*		
			data-accessor*		
UpdateDataSource	データソースを更新するためのアクセス許可を付与	書き込み	application*		
			data-source*		
			index*		
UpdateIndex	インデックスを更新するためのアクセス許可を付与	書き込み	application*		
			index*		
UpdateIntegration	Q Business アプリケーションの統合を更新する許可を付与	書き込み	application*		
			integration*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdatePlugin	プラグインを更新するためのアクセス許可を付与	書き込み	application*		
			plugin*		
UpdateRetriever	レトリバーを更新するためのアクセス許可を付与	書き込み	application*		
			retriever*		
UpdateSubscription	サブスクリプションを更新する許可を付与する	書き込み	application*		
			subscription*		
UpdateUser	ユーザーを更新するためのアクセス許可を付与	書き込み	application*		
UpdateWebExperience	ウェブエクスペリエンスを更新するためのアクセス許可を付与	書き込み	application*		
			web-experience*		

Amazon Q Business で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
application	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}	aws:ResourceTag/${TagKey}
integration	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/integration/${IntegrationId}	aws:ResourceTag/${TagKey}
retriever	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/retriever/${RetrieverId}	aws:ResourceTag/${TagKey}
index	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/index/${IndexId}	aws:ResourceTag/${TagKey}
data-source	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/index/${IndexId}/data-source/${DataSourceId}	aws:ResourceTag/${TagKey}
plugin	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/plugin/${PluginId}	aws:ResourceTag/${TagKey}
web-experience	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/web-experience/${WebExperienceId}	aws:ResourceTag/${TagKey}
subscription	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/subscription/${SubscriptionId}	

リソースタイプ	ARN	条件キー
data-accessor	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/data-accessor/${DataAccessorId}	aws:ResourceTag/${TagKey}
chat-response-configuration	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/chat-response-configuration/${ChatResponseConfigurationId}	aws:ResourceTag/${TagKey}

Amazon Q Business の条件キー

Amazon Q Business は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
identitystore:GroupId	IAM Identity Center ユーザー ID でアクセスをフィルタリングする	ArrayOfString
identitystore:UserId	IAM Identity Center ユーザー ID でアクセスをフィルタリングします	ArrayOfString

Amazon Q Business Q Apps のアクション、リソース、および条件キー

Amazon Q Business Q Apps (サービスプレフィックス: qapps) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Q Business Q Apps で定義されるアクション
- Amazon Q Business Q Apps で定義されるリソースタイプ
- Amazon Q Business Q Apps の条件キー

Amazon Q Business Q Apps で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateLibraryItemReview	Q Business アプリケーション環境でライブラリ項目レビューを関連付ける許可を付与する	書き込み	qapp*		
				qapps:UserIsAppOwner qapps:AppIsPublished	
AssociateQAppWithUser	Q Business アプリケーション環境でユーザーと Q App を関連付ける許可を付与する	書き込み	application		
			qapp		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				qapps:UserIsAppOwner qapps:AppIsPublished	
BatchCreateCategory	Q Business アプリケーション環境でライブラリのカテゴリを作成するアクセス許可を付与します	書き込み	application*		
BatchDeleteCategory	Q Business アプリケーション環境でライブラリのカテゴリを削除するアクセス許可を付与します	書き込み	application*		
BatchUpdateCategory	Q Business アプリケーション環境でライブラリのカテゴリを更新する許可を付与	書き込み	application*		
CopyQApp [アクセス許可のみ]	Q Business アプリケーション環境で Q App をコピーする許可を付与する	書き込み	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateLibraryItem	Q Business アプリケーション環境でライブラリ項目を作成する許可を付与する	書き込み	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
CreateLibraryItemReview [アクセス許可のみ]	Q Business アプリケーション環境でライブラリ項目レビューを作成する許可を付与する	書き込み	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
CreateQApp	Q Business アプリケーション環境で Q App を作成する許可を付与する	書き込み	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSubscriptionToken [アクセス許可のみ]	Q Business アプリケーション環境で Q App イベントバストピックをサブスクライブする許可を付与する	書き込み	application*		
DeleteLibraryItem	Q Business アプリケーション環境でライブラリ項目を削除する許可を付与する	書き込み	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
DeleteQApp	Q Business アプリケーション環境で Q App を削除する許可を付与する	書き込み	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
DescribeQAppPermissions	Q Business アプリケーション環境で Q App 共有許可を取得する許可を付与	読み取り	application		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
DisassociateLibraryItemReview	Q Business アプリケーション環境でライブラリ項目レビューの関連付けを解除する許可を付与する	書き込み	qapp*		
				qapps:UserIsAppOwner qapps:AppIsPublished	
DisassociateQAppFromUser	Q Business アプリケーション環境でユーザーと Q App の関連付けを解除する許可を付与する	書き込み	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ExportQAppSessionData	Q Business アプリケーション環境で Q App セッションデータをエクスポートする許可を付与する	書き込み	qapp-session*		
GetLibraryItem	Q Business アプリケーション環境でライブラリ項目を取得する許可を付与する	読み取り	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
GetQApp	Q Business アプリケーション環境で Q App を取得する許可を付与する	読み取り	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
GetQAppSession	Q Business アプリケーション環境で Q App セッションを取得する許可を付与する	読み取り	qapp-session*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	
GetQAppSessionMetadata	Q Business アプリケーション環境で Q App セッションメタデータを取得する許可を付与する	読み取り	qapp-session*		
ImportDocument	Q Business アプリケーション環境で Q App または Q App セッションにドキュメントをインポートする許可を付与する	書き込み	qapp		
			qapp-session		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	
ListCategories	Q Business アプリケーション環境のカテゴリを一覧表示するアクセス許可を付与します	リスト	application*		
ListLibraryItems	Q Business アプリケーション環境でライブラリアイテムを一覧表示する許可を付与する	リスト	application*		
ListQAppSessionData	Q Business アプリケーション環境で Q App セッションデータを取得する許可を付与する	読み取り	qapp-session*		
ListQApps	Q Business アプリケーション環境で Q App を一覧表示する許可を付与する	リスト	application*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み込み	qapp		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			qapp-session		
PredictProblemStatementFromConversation [許可のみ]	Q Business アプリケーション環境の会話ログから問題ステートメントを予測する許可を付与する	書き込み	application*		
PredictQApp	Q Business アプリケーション環境の会話ログまたは問題ステートメントから Q App を予測する許可を付与する	書き込み	application*		
PredictQAppFromProblemStatement [アクセス許可のみ]	Q Business アプリケーション環境の問題ステートメントから Q App メタデータを予測する許可を付与する	書き込み	application*		
StartQAppSession	Q Business アプリケーション環境で Q App セッションを開始する許可を付与する	書き込み	application		
			qapp		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				qapps:UserIsAppOwner qapps:AppIsPublished aws:RequestTag/${TagKey} aws:TagKeys	
StopQAppSession	Q Business アプリケーション環境で Q App セッションを停止する許可を付与する	書き込み	application		
			qapp-session		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	
TagResource	指定されたキーと値のペアでリソースにタグを付けるアクセス許可を付与	Tagging	qapp		
			qapp-session		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	所与のキーを持つタグをリソースから削除する許可を付与	Tagging	qapp		
			qapp-session		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
UpdateLibraryItem	Q Business アプリケーション環境でライブラリ項目を更新する許可を付与する	書き込み	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
UpdateLibraryItemMetadata	Q Business アプリケーション環境のライブラリ項目のメタデータを更新する許可を付与する	書き込み	qapp*		
				qapps:AppIsPublished	
UpdateQApp	Q Business アプリケーション環境で Q App を更新する許可を付与する	書き込み	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateQAppPermissions	Q Business アプリケーション環境で Q App 共有アクセス許可を更新するアクセス許可を付与します	書き込み	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
UpdateQAppSession	Q Business アプリケーション環境で Q App セッションを更新する許可を付与する	書き込み	qapp-session*		
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateQAppSessionMetadata	Q Business アプリケーション環境で Q App セッションメタデータを更新する許可を付与する	書き込み	qapp-session*		

Amazon Q Business Q Apps で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
application	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}`	
qapp	`arn:${Partition}:qapps:${Region}:${Account}:application/${ApplicationId}/qapp/${AppId}`	aws:ResourceTag/${TagKey}
qapp-session	`arn:${Partition}:qapps:${Region}:${Account}:application/${ApplicationId}/qapp/${AppId}/session/${SessionId}`	aws:ResourceTag/${TagKey}

Amazon Q Business Q Apps の条件キー

Amazon Q Business Q Apps は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
qapps:AppIsPublished	Q App が公開されているかどうかによってアクセスをフィルタリングする	String
qapps:SessionIsShared	Q App セッションが共有されているかどうかによってアクセスをフィルタリングする	String
qapps:UserIsAppOwner	リクエスタが Q App 所有者であるかどうかによってアクセスをフィルタリングする	String
qapps:UserIsSessionModerator	リクエスタが Q App セッションモデレーターであるかどうかによってアクセスをフィルタリングする	String

Amazon Q Developer のアクション、リソース、および条件キー

Amazon Q Developer (サービスプレフィックス: qdeveloper) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Q Developer で定義されるアクション
- Amazon Q Developer で定義されるリソースタイプ
- Amazon Q Developer の条件キー

Amazon Q Developer で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ExportArtifact	Amazon Q Developer からアーティファクトをエクスポートする許可を付与	書き込み	codeTransformation		
ImportArtifact	Amazon Q Developer にアーティファクトをインポートする許可を付与	書き込み	codeTransformation		
ListTagsForResource [アクセス許可のみ]	Amazon Q Developer リソースに関連付けられているすべてのタグを一覧表示するアクセス許可を付与します	リスト	codeTransformation		
StartAgentSession	Amazon Q Developer とのエージェントセッションを開始するアクセス許可を付与します	書き込み		aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey}	
TagResource [アクセス許可のみ]	タグを Amazon Q Developer リソースに関連付けるアクセス許可を付与します	Tagging	codeTransformation		
				aws:TagKeys aws:RequestTag/${TagKey}	
TransformCode	Amazon Q Developer Transform Agent を使用してコードを変換するアクセス許可を付与します	書き込み	codeTransformation		
UntagResource [アクセス許可のみ]	Amazon Q Developer リソースに関連付けられたタグを削除するアクセス許可を付与します	Tagging	codeTransformation		
				aws:TagKeys	

Amazon Q Developer で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
codeTransformation	arn:${Partition}:qdeveloper:${Region}:${Account}:codeTransformation/${Identifier}	aws:ResourceTag/${TagKey}

Amazon Q Developer の条件キー

Amazon Q Developer では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	Amazon Q Developer リソースに関連付けられたタグでアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon Q in Connect のアクション、リソース、および条件キー

Amazon Q in Connect (サービスプレフィックス: wisdom) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Q in Connect で定義されるアクション
- Amazon Q in Connect で定義されるリソースタイプ
- Amazon Q in Connect の条件キー

Amazon Q in Connect で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ActivateMessageTemplate	メッセージテンプレートをアクティブ化する許可を付与する	書き込み	KnowledgeBase*		
			MessageTemplate*		
AllowVendedLogDeliveryForResource [アクセス許可のみ]	アシスタント用の vended log 配信を設定する許可を付与する	権限の管理	Assistant		
CreateAIAgent	AI エージェントを作成する許可を付与する	書き込み	Assistant*		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey}	
CreateAIAgentVersion	AI エージェントバージョンを作成する許可を付与する	書き込み	AIAgent*		
			Assistant*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIGuardrail	ai ガードレールを作成するアクセス許可を付与します	書き込み	Assistant*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIGuardrailVersion	ai ガードレールバージョンを作成するアクセス許可を付与します	書き込み	AIGuardrail*		
			Assistant*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIPrompt	AI プロンプトを作成する許可を付与する	書き込み	Assistant*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIPromptVersion	AI プロンプトのバージョンを作成する許可を付与する	書き込み	AIPrompt*		
			Assistant*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAssistant	アシスタントを作成するためのアクセス許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateAssistantAssociation	アシスタントと他のリソース間の関連付けを作成するためのアクセス許可を付与	書き込み	Assistant*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateContent	コンテンツを作成するためのアクセス許可を付与	書き込み	KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateContentAssociation	コンテンツの関連付けを作成する許可を付与する	書き込み	Content*		
			KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateKnowledgeBase	ナレッジベースを作成するためのアクセス許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateMessageTemplate	メッセージテンプレートを作成する許可を付与する	書き込み	KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateMessageTemplateAttachment	メッセージテンプレートに添付ファイルを作成する許可を付与する	書き込み	KnowledgeBase*		
			MessageTemplate*		
CreateMessageTemplateVersion	メッセージテンプレートのバージョンを作成する許可を付与する	書き込み	KnowledgeBase*		
			MessageTemplate*		
CreateQuickResponse	クイックレスポンスを作成するアクセス許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSession	セッションを作成するためのアクセス許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
DeactivateMessageTemplate	メッセージテンプレートを非アクティブ化する許可を付与する	書き込み	KnowledgeBase*		
			MessageTemplate*		
DeleteAIAgent	AI エージェントを削除する許可を付与する	書き込み	AIAgent*		
			Assistant*		
DeleteAIAgentVersion	AI エージェントのバージョンを削除する許可を付与する	書き込み	AIAgent*		
			Assistant*		
DeleteAIGuardrail	ai ガードレールを削除するアクセス許可を付与します	書き込み	AIGuardrail*		
			Assistant*		
DeleteAIGuardrailVersion	ai ガードレールバージョンを削除するアクセス許可を付与します	書き込み	AIGuardrail*		
			Assistant*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteAIPrompt	AI プロンプトを削除する許可を付与する	書き込み	AIPrompt*		
			Assistant*		
DeleteAIPromptVersion	AI プロンプトバージョンを削除する許可を付与する	書き込み	AIPrompt*		
			Assistant*		
DeleteAssistant	アシスタントを削除するためのアクセス許可を付与	書き込み	Assistant*		
DeleteAssistantAssociation	アシスタントの関連付けを削除するためのアクセス許可を付与	書き込み	Assistant*		
			AssistantAssociation*		
DeleteContent	コンテンツを削除するためのアクセス許可を付与	書き込み	Content*		
			KnowledgeBase*		
DeleteContentAssociation	コンテンツの関連付けを削除する許可を付与する	書き込み	Content*		
			ContentAssociation*		
			KnowledgeBase*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteImportJob	ナレッジベースのインポートジョブを削除するアクセス許可を付与	書き込み	KnowledgeBase*		
DeleteKnowledgeBase	ナレッジベースを削除するためのアクセス許可を付与	書き込み	KnowledgeBase*		
DeleteMessageTemplate	メッセージテンプレートを削除する許可を付与する	書き込み	KnowledgeBase*		
			MessageTemplate*		
DeleteMessageTemplateAttachment	メッセージテンプレートから添付ファイルを削除する許可を付与する	書き込み	KnowledgeBase*		
			MessageTemplate*		
DeleteQuickResponse	クイックレスポンスを削除するアクセス許可を付与	書き込み	KnowledgeBase*		
			QuickResponse*		
GetAIAgent	AI エージェントに関する情報を取得する許可を付与する	読み取り	AIAgent*		
			Assistant*		
GetAIGuardrail	ai ガードレールに関する情報を取得するアクセス許可を付与します	読み取り	AIGuardrail*		
			Assistant*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetAIPrompt	プロンプトについての情報を取得する許可を付与する	読み取り	AIPrompt*		
			Assistant*		
GetAssistant	アシスタントに関する情報を取得するためのアクセス許可を付与	読み取り	Assistant*		
GetAssistantAssociation	アシスタントの関連付けに関する情報を取得するためにアクセス許可を付与	読み取り	Assistant*		
			AssistantAssociation*		
GetContent	コンテンツ (コンテンツをダウンロードするための署名付き URL を含む) を取得するためのアクセス許可を付与	読み取り	Content*		
			KnowledgeBase*		
GetContentAssociation	コンテントの関連付けに関する情報を取得する許可を付与する	読み取り	Content*		
			ContentAssociation*		
			KnowledgeBase*		
GetContentSummary	コンテンツの概要に関する情報を取得するためのアクセス許可を付与	読み取り	Content*		
			KnowledgeBase*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetImportJob	特定のインポートジョブに関する情報を取得するアクセス許可を付与	読み取り	KnowledgeBase*		
GetKnowledgeBase	ナレッジベースに関する情報を取得するためのアクセス許可を付与	読み取り	KnowledgeBase*		
GetMessageTemplate	メッセージテンプレートを取得する許可を付与する	読み取り	KnowledgeBase*		
			MessageTemplate*		
				wisdom:MessageTemplate/RoutingProfileArn	
GetNextMessage	セッション内の次のメッセージの を取得するアクセス許可を付与します	読み取り	Assistant*		
			Session*		
GetQuickResponse	コンテンツを取得するアクセス許可を付与	読み取り	KnowledgeBase*		
			QuickResponse*		
GetRecommendations	指定されたセッションについての推奨事項を取得するためのアクセス許可を付与	読み取り	Assistant*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetSession	指定されたセッションの情報を取得するためのアクセス許可を付与	読み取り	Assistant*		
			Session*		
ListAIAgentVersions	AI エージェントのバージョンに関する情報を一覧表示する許可を付与する	リスト	AIAgent*		
			Assistant*		
ListAIAgents	AI エージェントに関する情報を一覧表示する許可を付与する	リスト	Assistant*		
ListAIGuardrailVersions	ai ガードレールのバージョンに関する情報を一覧表示するアクセス許可を付与します	リスト	AIGuardrail*		
			Assistant*		
ListAIGuardrails	ai ガードレールに関する情報を一覧表示するアクセス許可を付与します	リスト	Assistant*		
ListAIPromptVersions	AI プロンプトバージョンに関する情報を一覧表示する許可を付与する	リスト	AIPrompt*		
			Assistant*		
ListAIPrompts	プロンプトに関する情報を一覧表示する許可を付与する	リスト	Assistant*		
ListAssistantAssociations	アシスタントの関連付けに関する情報を一覧表示するためのアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListAssistants	アシスタントに関する情報を一覧表示するためのアクセス許可を付与	リスト			
ListContentAssociations	コンテンツの関連付けに関する情報を一覧表示する許可を付与する	リスト	Content*		
			KnowledgeBase*		
ListContents	ナレッジベースのコンテンツを一覧表示するためのアクセス許可を付与	リスト	KnowledgeBase*		
ListImportJobs	ナレッジベースに関する情報を一覧表示するためのアクセス許可を付与	リスト	KnowledgeBase*		
ListKnowledgeBases	ナレッジベースに関する情報を一覧表示するためのアクセス許可を付与	リスト			
ListMessageTemplateVersions	指定されたメッセージテンプレートのメッセージテンプレートバージョンを一覧表示する許可を付与する	リスト	KnowledgeBase*		
			MessageTemplate*		
ListMessageTemplates	ナレッジベースのメッセージテンプレートを一覧表示する許可を付与する	リスト	KnowledgeBase*		
ListMessages	セッション内のメッセージを一覧表示するアクセス許可を付与します	リスト	Assistant*		
			Session*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListQuickResponses	クイックレスポンスをナレッジベースとともに一覧表示するアクセス許可を付与	リスト	KnowledgeBase*		
ListTagsForResource	指定されたリソースのタグを一覧表示するためのアクセス許可を付与	読み取り			
NotifyRecommendationsReceived	新しく利用可能になった推奨事項において、指定されたアシスタントのキューから、指定された推奨事項を削除するためのアクセス許可を付与	書き込み			
PutFeedback	フィードバックを送信する許可を付与	書き込み	Assistant*		
QueryAssistant	指定されたアシスタントに対して手動検索を実行するためのアクセス許可を付与	読み取り	Assistant*		
RemoveAssistantAIAgent	アシスタントから AI エージェントを削除する許可を付与する	書き込み	Assistant*		
RemoveKnowledgeBaseTemplateUri	ナレッジベースから URI テンプレートを削除するためのアクセス許可を付与	書き込み	KnowledgeBase*		
RenderMessageTemplate	メッセージテンプレートをレンダリングする許可を付与する	読み取り	KnowledgeBase*		wisdom:GetMessageTemplate
			MessageTemplate*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				wisdom:MessageTemplate/RoutingProfileArn	
SearchContent	指定されたナレッジベースを参照しながらコンテンツを検索するためのアクセス許可を付与 特定のコンテンツリソースを、その名前で取得する際に使用します。	読み取り	KnowledgeBase*		
SearchMessageTemplates	指定されたナレッジベースを参照するメッセージテンプレートを検索する許可を付与する	読み取り	KnowledgeBase*		
				wisdom:SearchFilter/RoutingProfileArn wisdom:SearchFilter/Qualifier	
SearchQuickResponses	指定されたナレッジベースを参照しながらクイックレスポンスを検索するアクセス許可を付与	読み取り	KnowledgeBase*		wisdom:GetQuickResponse

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				wisdom:SearchFilter/RoutingProfileArn	
SearchSessions	指定されたアシスタントを参照しながらセッションを検索するためのアクセス許可を付与 特定のセッションリソースを、その名前で取得する際に使用します。	読み取り			
SendMessage	メッセージを送信するアクセス許可を付与します	書き込み	Assistant*		
			Session*		
StartContentUpload	ナレッジベースにコンテンツをアップロードする際の URL を取得するためのアクセス許可を付与	書き込み	KnowledgeBase*		
StartImportJob	複数のクイックレスポンスを作成するアクセス許可を付与	書き込み	KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource		Tagging	Assistant		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	指定されたタグを指定されたリソースに追加するためのアクセス許可を付与		AssistantAssociation		
			Content		
			ContentAssociation		
			KnowledgeBase		
			MessageTemplate		
			QuickResponse		
			Session		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	指定されたリソースから指定されたタグを削除するためのアクセス許可を付与	Tagging	Assistant		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			AssistantAssociation		
			Content		
			ContentAssociation		
			KnowledgeBase		
			MessageTemplate		
			QuickResponse		
			Session		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAIAgent	AI エージェントに関する情報を更新する許可を付与する	書き込み	AIAgent*		
			Assistant*		
UpdateAIGuardrail	ai ガードレールに関する情報を更新するアクセス許可を付与します	書き込み	AIGuardrail*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			Assistant*		
UpdateAIPrompt	AI プロンプトに関する情報を更新する許可を付与する	書き込み	AIPrompt*		
			Assistant*		
UpdateAssistantAIAgent	AI エージェントに関するアシスタント情報を更新する許可を付与する	書き込み	Assistant*		
UpdateContent	コンテンツに関する情報を更新するためのアクセス許可を付与	書き込み	Content*		
			KnowledgeBase*		
UpdateKnowledgeBaseTemplateUri	ナレッジベースのテンプレート URI を更新するためのアクセス許可を付与	書き込み	KnowledgeBase*		
UpdateMessageTemplate	メッセージテンプレートの内容を更新する許可を付与する	書き込み	KnowledgeBase*		
			MessageTemplate*		
UpdateMessageTemplateMetadata	メッセージテンプレートのメタデータを更新する許可を付与する	書き込み	KnowledgeBase*		
			MessageTemplate*		
UpdateQuickResponse	クイックレスポンスのコンテンツに関する情報を更新するアクセス許可を付与	書き込み	KnowledgeBase*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			QuickResponse*		
UpdateSession	セッションを更新する許可を付与する	書き込み	Assistant*		
			Session*		
UpdateSessionData	セッションに保存されたデータを更新する許可を付与する	書き込み	Assistant*		
			Session*		

Amazon Q in Connect で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
AIAgent	arn:${Partition}:wisdom:${Region}:${Account}:ai-agent/${AssistantId}/${AIAgentId}	aws:ResourceTag/${TagKey}
AIPrompt	arn:${Partition}:wisdom:${Region}:${Account}:ai-prompt/${AssistantId}/${AIPromptId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
AIGuardrail	arn:${Partition}:wisdom:${Region}:${Account}:ai-guardrail/${AssistantId}/${AIGuardrailId}	aws:ResourceTag/${TagKey}
Assistant	arn:${Partition}:wisdom:${Region}:${Account}:assistant/${AssistantId}	aws:ResourceTag/${TagKey}
Assistant Association	arn:${Partition}:wisdom:${Region}:${Account}:association/${AssistantId}/${AssistantAssociationId}	aws:ResourceTag/${TagKey}
Content	arn:${Partition}:wisdom:${Region}:${Account}:content/${KnowledgeBaseId}/${ContentId}	aws:ResourceTag/${TagKey}
ContentAssociation	arn:${Partition}:wisdom:${Region}:${Account}:content-association/${KnowledgeBaseId}/${ContentId}/${ContentAssociationId}	aws:ResourceTag/${TagKey}
KnowledgeBase	arn:${Partition}:wisdom:${Region}:${Account}:knowledge-base/${KnowledgeBaseId}	aws:ResourceTag/${TagKey}
MessageTemplate	arn:${Partition}:wisdom:${Region}:${Account}:message-template/${KnowledgeBaseId}/${MessageTemplateId}	aws:ResourceTag/${TagKey} wisdom:MessageTemplate/RoutingProfileArn
Session	arn:${Partition}:wisdom:${Region}:${Account}:session/${AssistantId}/${SessionId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
QuickResponse	arn:${Partition}:wisdom:${Region}:${Account}:quick-response/${KnowledgeBaseId}/${QuickResponseId}	aws:ResourceTag/${TagKey}

Amazon Q in Connect の条件キー

Amazon Q in Connect は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
wisdom:MessageTemplate/RoutingProfileArn	リソースに関連付けられた接続ルーティングプロファイルの ARN によってアクセスをフィルタリングする	ArrayOfARN
wisdom:SearchFilter/Qualifier	リクエストで渡された修飾子によってアクセスをフィルタリングする	ArrayOfString

条件キー	説明	タイプ
wisdom:SearchFilter/RoutingProfileArn	リクエストで渡された接続ルーティングプロファイルの ARN でアクセスをフィルタリングします	ARN

Amazon QLDB のアクション、リソース、および条件キー

Amazon QLDB (サービスプレフィックス: qldb) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon QLDB で定義されるアクション
- Amazon QLDB で定義されるリソースタイプ
- Amazon QLDB の条件キー

Amazon QLDB で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にア

クションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelJournalKinesisStream	ジャーナル Kinesis ストリームをキャンセルする許可を付与	書き込み	stream*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateLedger	台帳を作成する許可を付与。	書き込み	ledger*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteLedger	台帳を削除する許可を付与。	書き込み	ledger*		
DescribeJournalKinesisStream	ジャーナル Kinesis ストリームに関する情報を記述する許可を付与。	読み込み	stream*		
DescribeJournalS3Export	ジャーナルエクスポートジョブに関する情報を記述する許可を付与。	読み込み	ledger*		
DescribeLedger	台帳を記述する許可を付与。	読み取り	ledger*		
ExecuteStatement [許可のみ]	コンソール経由で台帳にコマンドを送信する許可を付与。	書き込み	ledger*		
ExportJournalToS3	ジャーナルコンテンツを Amazon S3 バケットにエクスポートする許可を付与。	書き込み	ledger*		
GetBlock	指定された BlockAddress の台帳からブロックを取得する許可を付与。	読み込み	ledger*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetDigest	指定された BlockAddress の台帳からダイジェストを取得する許可を付与。	読み込み	ledger*		
GetRevision	指定されたドキュメント ID および指定された BlockAddress のリビジョンを取得する許可を付与。	読み取り	ledger*		
InsertSampleData [許可のみ]	コンソール経由でサンプルアプリケーションデータを挿入する許可を付与。	書き込み	ledger*		
ListJournalKinesisStreamsForLedger	指定した台帳のジャーナル kinesis ストリームを一覧表示する許可を付与	リスト	stream*		
ListJournalS3Exports	すべての台帳のジャーナルエクスポートジョブを一覧表示する許可を付与。	リスト			
ListJournalS3ExportsForLedger	指定された台帳のジャーナルエクスポートジョブを一覧表示する許可を付与。	リスト	ledger*		
ListLedgers	既存の台帳を一覧表示する許可を付与。	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み込み	catalog		
			ledger		
			stream		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			table		
PartiQLCreateIndex	テーブルにインデックスを作成するためのアクセス許可を付与します	書き込み	table*		
PartiQLCreateTable	テーブルを作成する許可を付与。	書き込み	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PartiQLDelete	テーブルからドキュメントを削除する許可を付与	書き込み	table*		
PartiQLDropIndex	テーブルからインデックスを削除する許可を付与	書き込み	table*		
				qldb:Purge	
PartiQLDropTable	テーブルを削除する許可を付与。	書き込み	table*		
				qldb:Purge	
PartiQLHistoryFunction	テーブルで履歴関数を使用する許可を付与	読み込み	table*		
PartiQLInsert	テーブルにドキュメントを挿入する許可を付与	書き込み	table*		
PartiQLRedact	履歴リビジョンを編集する許可を付与	書き込み	table*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PartiQLSelect	テーブルからドキュメントを選択する許可を付与	読み込み	catalog		
			table		
PartiQLUndropTable	テーブルの削除を取り消すアクセス許可を付与します	書き込み	table*		
PartiQLUpdate	テーブル内の既存のドキュメントを更新する許可を付与	書き込み	table*		
SendCommand	台帳にコマンドを送信する許可を付与。	書き込み	ledger*		
ShowCatalog [アクセス許可のみ]	コンソールを介して台帳のカタログを表示する許可を付与。	書き込み	ledger*		
StreamJournalToKinesis	Kinesis データストリームにジャーナルのコンテンツをストリーミングする許可を付与	書き込み	stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	リソースに 1 つ以上のタグを追加する許可を付与	タグ付け	catalog		
			ledger		
			stream		
			table		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースから 1 つ以上のタグを削除する許可を付与	タグ付け	catalog		
			ledger		
			stream		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateLedger	台帳のプロパティを更新する許可を付与。	書き込み	ledger*		
UpdateLedgerPermissionsMode	台帳のアクセス許可モードを更新する許可を付与	書き込み	ledger*		

Amazon QLDB で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
ledger	arn:${Partition}:qldb:${Region}:${Account}:ledger/${LedgerName}	aws:ResourceTag/${TagKey}
stream	arn:${Partition}:qldb:${Region}:${Account}:stream/${LedgerName}/${StreamId}	aws:ResourceTag/${TagKey}
table	arn:${Partition}:qldb:${Region}:${Account}:ledger/${LedgerName}/table/${TableId}	aws:ResourceTag/${TagKey}
catalog	arn:${Partition}:qldb:${Region}:${Account}:ledger/${LedgerName}/information_schema/user_tables	aws:ResourceTag/${TagKey}

Amazon QLDB の条件キー

Amazon QLDB では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	文字列

条件キー	説明	タイプ
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString
qldb:Purge	PartiQL DROP ステートメントで指定されたパージの値でアクセスをフィルターします。	文字列

Amazon QuickSight のアクション、リソース、および条件キー

Amazon QuickSight (サービスプレフィックス: quicksight) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件キーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon QuickSight で定義されるアクション
- Amazon QuickSight で定義されるリソースタイプ
- Amazon QuickSight の条件キー

Amazon QuickSight で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AccountConfigurations	AWS リソースへのデフォルトアクセスの設定を有効にするアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
[アクセス許可のみ]					
BatchCreateTopicReviewedAnswer	トピックのレビュー済み回答を作成する許可を付与する	書き込み	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
BatchDeleteTopicReviewedAnswer	トピックのレビュー済み回答を削除する許可を付与する	書き込み	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CancelIngestion	データセットの SPICE 取り込みをキャンセルするアクセス許可を付与	書き込み	ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateAccountCustomization	QuickSight アカウントまたは名前空間のアカウントのカスタマイズを作成するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAccountSubscription	QuickSight にサブスクライブする許可の付与	書き込み		quicksight:Edition quicksight:DirectoryType	
CreateAdmin [アクセス許可のみ]	ユーザーが Amazon QuickSight 管理者、作成者、閲覧者をプロビジョンできるようにアクセス許可を付与	書き込み	user*		
CreateAnalysis	テンプレートから解析を作成するアクセス許可を付与	書き込み	analysis*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBrand	Amazon QuickSight ブランドを作成するアクセス許可を付与します	書き込み	brand*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomPermissions	QuickSight カスタムアクセス許可リソースを作成するアクセス許可を付与します	書き込み	custompermissions*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDashboard	QuickSight ダッシュボードを作成するアクセス許可を付与	書き込み	dashboard*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSet	データセットを作成する許可を付与	書き込み	datasource*		quicksight:PassDataSource

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	データソースを作成するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateEmailCustomizationTemplate [アクセス許可のみ]	QuickSight検証 E メールかストマイゼーションを作成する許可を付与	書き込み	emailCustomizationTemplate*		
CreateFolder	QuickSight フォルダを作成するmobiletargeting:GetReports	書き込み	folder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFolderMembership	QuickSight ダッシュボード、分析、またはデータセットを QuickSight フォルダに追加する許可を付与	書き込み	folder*		
			analysis		
			dashboard		
			dataset		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateGroup	QuickSight グループを作成するアクセス許可を付与	書き込み	group*		
CreateGroupMembership	QuickSight ユーザーを QuickSight グループに追加するアクセス許可を付与	書き込み	group*	quicksight:UserName	
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateIAMPolicyAssignment	指定された IAM ポリシー ARN を 1 つ持つ割り当てを作成するアクセス許可を付与この割り当ては、QuickSight の指定されたグループまたはユーザーに割り当てられます。	書き込み	assignment*		
CreateIngestion	データセットの SPICE 取り込みを開始するアクセス許可を付与	書き込み	ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateNamespace	QuickSight 名前空間を作成するアクセス許可を付与	書き込み	namespace*		ds:CreateIdentityPoolDirectory
CreateReader [アクセス許可のみ]	Amazon QuickSight リーダーをプロビジョニングするアクセス許可を付与	書き込み	user*		
CreateRefreshSchedule	データセットの更新スケジュールを作成する許可を付与	書き込み	refreshschedule*		
CreateRoleMembership	グループメンバーをロールに追加するためのアクセス許可を付与	書き込み		quicksight:Group	
CreateTemplate	テンプレートを作成するアクセス許可を付与	書き込み	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTemplateAlias	テンプレートエイリアスを作成するアクセス許可を付与	書き込み	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateTheme	テーマを作成するアクセス許可を付与	書き込み	theme*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateThemeAlias	テーマバージョンのエイリアスを作成するアクセス許可を付与	書き込み	theme*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTopic	トピックを作成する許可を付与	書き込み	dataset*		quicksight:PassDataSet
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTopicRefreshSchedule	トピックの更新スケジュールを作成する許可を付与	書き込み	topic*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateUser [アクセス許可のみ]	ユーザーが Amazon QuickSight の作成者や閲覧者をプロビジョンするアクセス許可を付与	書き込み	user*		
CreateVPCConnection	VPC 接続を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
DeleteAccountCustomization	QuickSight アカウントまたは名前空間のアカウントのカスタマイズを削除するアクセス許可を付与	書き込み	customization*		
DeleteAccountSubscription	QuickSight アカウントを削除する許可の付与	書き込み	account*		
DeleteAnalysis	分析を削除するアクセス許可を付与	書き込み	analysis*		
DeleteBrand	Amazon QuickSight ブランドを削除するアクセス許可を付与します	書き込み	brand*		
DeleteBrandAssignment	ブランド割り当てを削除するアクセス許可を付与します	書き込み			
DeleteCustomPermissions	QuickSight カスタムアクセス許可リソースを削除するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteDashboard	QuickSight ダッシュボードを削除するアクセス許可を付与	書き込み	dashboard*		
DeleteDataSet	データセットを削除する許可を付与	書き込み	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDataSetRefreshProperties	データセットの更新プロパティを削除する許可を付与	書き込み	dataset*		
DeleteDataSource	データソースを削除するアクセス許可を付与	書き込み	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDefaultQBusinessApplication	QuickSight アカウントのリンクされた QBusiness アプリケーションを削除する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteEmailCustomizationTemplate [アクセス許可のみ]	QuickSight メールカスタマイズテンプレートを削除するアクセス許可を付与	書き込み	emailCustomizationTemplate*		
DeleteFolder	QuickSight フォルダを削除する許可を付与	書き込み	folder*		
DeleteFolderMembership	QuickSight ダッシュボード、分析、またはデータセットを QuickSight フォルダから削除する許可を付与	書き込み	folder*		
			analysis		
			dashboard		
			dataset		
DeleteGroup	QuickSight からユーザーグループを削除するアクセス許可を付与	書き込み	group*		
DeleteGroupMembership	ユーザーをグループから削除するアクセス許可を付与削除するとそのユーザーはそのグループのメンバーではなくなります。	書き込み	group*	quicksight:UserName	
DeleteIAMPolicyAssignment	既存の割り当てを更新するアクセス許可を付与	書き込み	assignment*		
DeleteIdentityPropagationConfig	QuickSight で信頼できる ID 伝達 AWS のサービスを削除する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteNamespace	QuickSight 名前空間を削除するアクセス許可を付与	書き込み	namespace*		ds:DeleteDirectory
DeleteRefreshSchedule	データセットの更新スケジュールを削除する許可を付与	書き込み	refreshschedule*		
DeleteRoleCustomPermission	ロールに関連付けられたカスタムアクセス許可を削除するためのアクセス許可を付与	書き込み			
DeleteRoleMembership	ロールからグループメンバーを削除するためのアクセス許可を付与	書き込み		quicksight:Group	
DeleteTemplate	テンプレートを削除するアクセス許可を付与	書き込み	template*		
DeleteTemplateAlias	テンプレートエイリアスを削除するアクセス許可を付与	書き込み	template*		
DeleteTheme	テーマを削除するアクセス許可を付与	書き込み	theme*		
DeleteThemeAlias	テーマのエイリアスを削除するアクセス許可を付与	書き込み	theme*		
DeleteTopic	トピックを削除する許可を付与	書き込み	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteTopicRefreshSchedule	トピックの更新スケジュールを削除する許可を付与	書き込み	topic*		
DeleteUser	ユーザー名を指定して QuickSight ユーザーを削除するアクセス許可を付与	書き込み	user*		
DeleteUserByPrincipalId	プリンシパル ID で識別されるユーザーを削除するアクセス許可を付与	書き込み	user*		
DeleteUserCustomPermission	ユーザーに関連付けられたカスタムアクセス許可を削除するアクセス許可を付与します	書き込み	user*		
DeleteVPCConnection	VPC 接続を削除する許可を付与	書き込み	vpcconnection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeAccountCustomization	QuickSight アカウントまたは名前空間のアカウントのカスタマイズを記述するアクセス許可を付与	読み込み	customization*		
DescribeAccountSettings	QuickSight アカウントの管理者アカウント設定を説明するアクセス許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeAccountSubscription	QuickSight アカウントを記述する許可の付与	読み取り	account*		
DescribeAnalysis	分析を記述するアクセス許可を付与	読み込み	analysis*		
DescribeAnalysisPermissions	分析のアクセス許可を記述するアクセス許可を付与	読み取り	analysis*		
DescribeAssetBundleExportJob	アセットバンドルのエクスポートジョブを記述する許可を付与	読み取り	assetBundleExportJob*		
DescribeAssetBundleImportJob	アセットバンドルのインポートジョブを記述する許可を付与	読み取り	assetBundleImportJob*		
DescribeBrand	ブランドを記述するアクセス許可を付与します	読み取り	brand*		
DescribeBrandAssignment	ブランド割り当てを記述するアクセス許可を付与します	読み取り			
DescribeBrandPublishedVersion	ブランドの公開バージョンを記述するアクセス許可を付与します	読み取り	brand*		
DescribeCustomPermissions	QuickSight アカウントのカスタム権限リソースを記述するアクセス許可を付与	読み取り	custompermissions*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeDashboard	QuickSight ダッシュボードを記述するアクセス許可を付与	読み込み	dashboard*		
DescribeDashboardPermissions	QuickSight ダッシュボードのアクセス許可を記述するアクセス許可を付与	読み取り	dashboard*		
DescribeDashboardSnapshotJob	ダッシュボードスナップショットジョブを記述するための許可を付与します	読み取り	dashboardSnapshotJob*		
DescribeDashboardSnapshotJobResult	ダッシュボードスナップショットジョブの結果を記述するための許可を付与します	読み取り	dashboardSnapshotJob*		
DescribeDashboardsQAConfiguration	ダッシュボードの QA 設定を記述するアクセス許可を付与します	読み取り			
DescribeDataSet	データセットを記述するアクセス許可を付与	読み込み	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDataSetPermissions	データセットのリソースポリシーを記述するアクセス許可を付与	権限の管理	dataset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDataSetRefreshProperties	データセットの更新プロパティを記述する許可を付与	読み取り	dataset*		
DescribeDataSource	データソースを記述するアクセス許可を付与	読み込み	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDataSourcePermissions	データソースのリソースポリシーを記述するアクセス許可を付与	権限の管理	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeDefaultQBusinessApplication	QuickSight アカウントのリンクされた QBusiness アプリケーション ID を記述する許可を付与	読み取り			
DescribeEmailCustomizationTemplate [許可のみ]	QuickSight メールカスタマイゼーションテンプレートを記述するアクセス許可を付与	読み込み	emailCustomizationTemplate*		
DescribeFolder	QuickSight フォルダを記述する許可を付与	読み込み	folder*		
DescribeFolderPermissions	QuickSight ダッシュボードの許可を記述する許可を付与	読み込み	folder*		
DescribeFolderResolvedPermissions	QuickSight ダッシュボードの解決済みの許可を記述する許可を付与	読み込み	folder*		
DescribeGroup	QuickSight グループを記述するアクセス許可を付与	読み込み	group*		
DescribeGroupMembership	QuickSight グループメンバーを記述するアクセス許可を付与	読み込み	group*	quicksight:UserName	
DescribeIAMPolicyAssignment	既存の関連付けを記述するアクセス許可を付与	読み込み	assignment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeIngestion	データセットの SPICE 取り込みを記述するアクセス許可を付与	読み込み	ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeIpRestriction	QuickSight アカウントでの IP 制限を記述するアクセス許可を付与	読み取り			
DescribeKeyRegistration	QuickSight キー登録を記述する許可を付与する	読み取り			
DescribeNamespace	QuickSight 名前空間を記述するアクセス許可を付与	読み取り	namespace*		
DescribeQPersonalizationConfiguration	パーソナライズ設定を記述する許可を付与する	読み取り			
DescribeQuickSightQSearchConfiguration	QuickSight Q Search 設定を記述する許可を付与	読み取り			
DescribeRefreshSchedule	データセットの更新スケジュールを記述する許可を付与します	読み取り	refreshschedule*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeRoleCustomPermission	ロールに関連付けられたカスタムアクセス許可を記述するためのアクセス許可を付与	読み取り			
DescribeTemplate	テンプレートを記述するアクセス許可を付与	読み込み	template*		
DescribeTemplateAlias	テンプレートエイリアスを記述するアクセス許可を付与	読み込み	template*		
DescribeTemplatePermissions	テンプレートのアクセス許可を記述するアクセス許可を付与	読み込み	template*		
DescribeTheme	テーマを記述するアクセス許可を付与	読み込み	theme*		
DescribeThemeAlias	テーマエイリアスを記述するアクセス許可を付与	読み込み	theme*		
DescribeThemePermissions	テーマのアクセス許可を記述するアクセス許可を付与	読み取り	theme*		
DescribeTopic	トピックを記述する許可を付与	読み取り	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicPermissions	トピックのリソースポリシーを記述する許可を付与	権限の管理	topic*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicRefresh	トピックの更新ステータスを記述する許可を付与	読み取り	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicRefreshSchedule	トピックの更新スケジュールを記述する許可を付与	読み取り	topic*		
DescribeUser	ユーザー名を指定して QuickSight ユーザーを記述するアクセス許可を付与	読み取り	user*		
DescribeVPCConnection	VPC 接続を記述する許可を付与	読み取り	vpcconnection*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GenerateEmbedUrlForAnonymousUser	QuickSight に登録されていないユーザーのための QuickSight ダッシュボードまたは Q トピックを埋め込むために使用される URL を取得する許可を付与	書き込み	namespace*		
			dashboard		
			theme		
			topic		
				quicksight:AllowedEmbeddingDomains	
GenerateEmbedUrlForRegisteredUser	QuickSight に登録されていないユーザーのために QuickSight ダッシュボードを埋め込むために使用される URL を生成する許可を付与	書き込み	user*		
				quicksight:AllowedEmbeddingDomains	
GenerateEmbedUrlForRegisteredUserWithIdentity	ID 拡張ロールセッションを使用して QuickSight に登録されたユーザーの QuickSight エクスペリエンスを埋め込むために使用される URL を生成するアクセス許可を付与します	書き込み		quicksight:AllowedEmbeddingDomains	
GetAnonymousUserEmbedUrl [アクセス許可のみ]	QuickSight に登録されていないユーザーのために QuickSight ダッシュボードを埋め込むために使用される URL を取得する許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetAuthCode [許可のみ]	QuickSight ユーザーを表す認証コードを取得するアクセス許可を付与	読み込み	user*		
GetDashboardEmbedUrl	QuickSight ダッシュボードの埋め込みに使用する URL を取得するアクセス許可を付与	読み込み	dashboard*		
GetGroupMapping [許可のみ]	Amazon QuickSight を Enterprise Edition で使用して Amazon QuickSight のロールにマップされている Microsoft Active Directory (Microsoft Active Directory) ディレクトリグループを識別して表示するアクセス許可を付与	読み込み			
GetSessionEmbedUrl	QuickSight コンソールエクスペリエンスを埋め込むための URL を取得するアクセス許可を付与	読み込み			
ListAnalyses	アカウント内のすべての分析を一覧表示するアクセス許可を付与	リスト	analysis*		
ListAssetBundleExportJobs	すべてのアセットバンドルのエクスポートジョブを一覧表示する許可を付与	リスト	assetBundleExportJob*		
ListAssetBundleImportJobs	すべてのアセットバンドルのインポートジョブを一覧表示する許可を付与	リスト	assetBundleImportJob*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListBrands	Amazon QuickSight アカウントのすべてのブランドを一覧表示する許可を付与	リスト			
ListCustomPermissions	QuickSight アカウントのカスタム権限リソースを一覧表示するアクセス許可を付与	リスト			
ListCustomerManagedKeys [許可のみ]	登録されているすべてのカスタマーマネージドキーを一覧表示する許可を付与	リスト			
ListDashboardVersions	QuickSight ダッシュボードのすべてのバージョンを一覧表示するアクセス許可を付与	リスト	dashboard*		
ListDashboards	QuickSight アカウント内のすべてのダッシュボードを一覧表示するアクセス許可を付与	リスト	dashboard*		
ListDataSets	すべてのデータセットを一覧表示するアクセス許可を付与	リスト		aws:RequestTag/${TagKey} aws:TagKeys	
ListDataSources	すべてのデータソースを一覧表示するアクセス許可を付与	リスト		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListFolderMembers	フォルダのすべてのメンバーを一覧表示する許可を付与	読み込み	folder*		
ListFolders	QuickSight アカウント内のすべてのフォルダを一覧表示する許可を付与	リスト	folder*		
ListFoldersForResource	QuickSight リソースがメンバーであるすべてのフォルダを一覧表示する許可を付与する	リスト	analysis		
			dashboard		
			dataset		
			datasource		
			topic		
ListGroupMemberships	グループのメンバーユーザーを一覧表示するアクセス許可を付与	リスト	group*		
ListGroups	QuickSight ですべてのユーザーグループを一覧表示するアクセス許可を付与	リスト	group*		
ListIAMPolicyAssignments	現在の Amazon QuickSight アカウントのすべての割り当てを一覧表示するアクセス許可を付与	リスト	assignment*		
ListIAMPolicyAssignmentsForUser	ユーザーに割り当てられたすべての割り当てとそのユーザーが属するグループを一覧表示するアクセス許可を付与	リスト	assignment*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListIdentityPropagationConfigs	QuickSight で信頼できる ID の伝播が有効になっている AWS サービスを一覧表示するアクセス許可を付与します	リスト			
ListIngestions	データセットのすべての SPICE 取り込みを一覧表示するアクセス許可を付与	リスト		aws:RequestTag/${TagKey} aws:TagKeys	
ListKMSKeysForUser [許可のみ]	ユーザーの KMS キーを一覧表示する許可を付与	リスト			
ListNamespaces	QuickSight アカウント内のすべての名前空間を一覧表示するアクセス許可を付与	リスト			
ListRefreshSchedules	データセットのすべての更新スケジュールを一覧表示する許可を付与	リスト			
ListRoleMemberships	ロールのメンバーを一覧表示するためのアクセス許可を付与	リスト			
ListTagsForResource	QuickSight リソースのタグを一覧表示するアクセス許可を付与	読み込み	analysis		
			brand		
			customization		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			custompermissions		
			dashboard		
			dataset		
			datasource		
			folder		
			template		
			theme		
			topic		
			vpcconnection		
ListTemplateAliases	テンプレートのすべてのエイリアスを一覧表示するアクセス許可を付与	リスト	template*		
ListTemplateVersions	テンプレートのすべてのバージョンを一覧表示するアクセス許可を付与	リスト	template*		
ListTemplates	QuickSight アカウント内のすべてのテンプレートを一覧表示するアクセス許可を付与	リスト	template*		
ListThemeAliases	テーマのすべてのエイリアスを一覧表示するアクセス許可を付与	リスト	theme*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListThemeVersions	テーマのすべてのバージョンを一覧表示するアクセス許可を付与	リスト	theme*		
ListThemes	アカウント内のすべてのテーマを一覧表示するアクセス許可を付与	リスト	theme*		
ListTopicRefreshSchedules	トピックのすべての更新スケジュールを一覧表示する許可を付与	リスト			
ListTopicReviewedAnswers	トピックのレビュー済み回答をすべて一覧表示する許可を付与する	リスト		aws:RequestTag/${TagKey} aws:TagKeys	
ListTopics	すべてのトピックを一覧表示する許可を付与	リスト		aws:RequestTag/${TagKey} aws:TagKeys	
ListUserGroups	指定されたユーザーがメンバーになっているグループを一覧表示するアクセス許可を付与	リスト	user*		
ListUsers	このアカウントに属するすべての QuickSight ユーザーを一覧表示するアクセス許可を付与	リスト	user*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListVPCConnections	すべての VPC 接続を一覧表示する許可を付与	リスト		aws:RequestTag/${TagKey} aws:TagKeys	
PassDataSet [許可のみ]	テンプレートのデータセットを使用するアクセス許可を付与	読み込み	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PassDataSource [許可のみ]	データセットのデータソースを使用するアクセス許可を付与	読み取り	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PredictQAResults	QA 結果を予測するためのアクセス許可を付与します	読み取り	dashboard		
			topic		
PutDataSetRefreshProperties	データセットにデータセット更新プロパティを配置する許可を付与	書き込み	dataset*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RegisterCustomerManagedKey [アクセス許可のみ]	カスタマーマネージドキーを削除する許可を付与	書き込み			
RegisterUser	QuickSight ユーザーを作成するアクセス許可を付与そのユーザーの ID は、リクエストで指定された IAM ID/ロールに関連付けられます。	書き込み	user*	quicksight:IamArn quicksight:SessionName	
RemoveCustomerManagedKey [アクセス許可のみ]	カスタマーマネージドキーを削除する許可を付与	書き込み			
RestoreAnalysis	削除した解析を復元するアクセス許可を付与	書き込み	analysis*		
ScopeDownPolicy [アクセス許可のみ]	AWS リソースへのアクセス許可のスコープポリシーを管理するアクセス許可を付与します	書き込み			
SearchAnalyses	解析のサブセットを検索するアクセス許可を付与	リスト	analysis*		
SearchDashboards	QuickSight ダッシュボードのサブセットを検索するアクセス許可を付与	リスト	dashboard*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SearchDataSets	QuickSight データセットのサブセットを検索する許可を付与	リスト	dataset*		
SearchDataSources	QuickSight データソースのサブセットを検索する許可を付与	リスト	datasource*		
SearchDirectoryGroups [許可のみ]	Amazon QuickSight を Enterprise Edition で使用して Microsoft Active Directory ディレクトリグループを表示でき、Amazon QuickSight でロールにマップするものを選択するアクセス許可を付与	リスト			
SearchFolders	QuickSight フォルダのサブセットを検索する許可を付与	読み込み	folder*		
SearchGroups	QuickSight グループのサブセットを検索するアクセス許可を付与	リスト	group*		
SearchTopics	トピックのサブセットを検索するアクセス許可を付与します	リスト	topic*		
SearchUsers [許可のみ]	このアカウントに属する QuickSight ユーザーを検索するための許可を付与します	リスト	user*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SetGroupMapping [許可のみ]	Amazon QuickSight を Enterprise Edition で使用して Microsoft Active Directory ディレクトリグループを表示でき、Amazon QuickSight でロールにマップするものを選択するアクセス許可を付与	書き込み			
StartAssetBundleExportJob	アセットバンドルのエクスポートジョブを開始する許可を付与	書き込み	assetBundleExportJob*		
StartAssetBundleImportJob	アセットバンドルのインポートジョブを開始する許可を付与	書き込み	assetBundleImportJob*		
StartDashboardSnapshotJob	ダッシュボードスナップショットジョブを開始するための許可を付与します	書き込み	dashboardSnapshotJob*		
StartDashboardSnapshotJobSchedule	ダッシュボードスナップショットジョブのスケジュールを開始する許可を付与する	書き込み			
Subscribe [アクセス許可のみ]	Amazon QuickSight をサブスクライブするアクセス許可を付与し、ユーザーがサブスクリプションを Enterprise Edition にアップグレードできるようにします	書き込み		quicksight:Edition quicksight:DirectoryType	
TagResource	QuickSight リソースにタグを追加するアクセス許可を付与	タグ付け	analysis		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			brand		
			customization		
			custompermissions		
			dashboard		
			dataset		
			datasource		
			folder		
			ingestion		
			template		
			theme		
			topic		
			vpcconnection		
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
Unsubscribe [アクセス許可のみ]	Amazon QuickSight のサブスクリプションを解除して、すべてのユーザーとそのリソースを Amazon QuickSight から完全に削除するアクセス許可を付与	書き込み			
UntagResource	QuickSight リソースからタグを削除するアクセス許可を付与	タグ付け	analysis		
			brand		
			customization		
			custompermissions		
			dashboard		
			dataset		
			datasource		
			folder		
			ingestion		
			template		
			theme		
			topic		
			vpcconnection		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
UpdateAccountCustomization	QuickSight アカウントまたは名前空間のアカウントのカスタマイズを更新するアクセス許可を付与	書き込み	customization*		
UpdateAccountSettings	QuickSight アカウントの管理者アカウント設定を更新するアクセス許可を付与	書き込み			
UpdateAnalysis	分析を更新するアクセス許可を付与	書き込み	analysis*		
UpdateAnalysisPermissions	分析のアクセス許可を更新するアクセス許可を付与	権限の管理	analysis*		
UpdateApplicationWithTokenExchangeGrant	トークン交換許可を使用して QuickSight IAM Identity Center アプリケーションを更新する許可を付与	書き込み			
UpdateBrand	ブランドを更新するアクセス許可を付与します	書き込み	brand*		
UpdateBrandAssignment	ブランド割り当てを更新する許可を付与	書き込み			
UpdateBrandPublishedVersion	ブランドの公開バージョンを更新するアクセス許可を付与します	書き込み	brand*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateCustomPermissions	QuickSight カスタムアクセス許可リソースを更新するアクセス許可を付与します	書き込み	custompermissions*		
UpdateDashboard	QuickSight ダッシュボードを更新するアクセス許可を付与	書き込み	dashboard*		
UpdateDashboardLinks	QuickSight ダッシュボードのリンクを更新する許可を付与する	書き込み	dashboard*		
UpdateDashboardPermissions	QuickSight ダッシュボードのアクセス許可を更新するアクセス許可を付与	権限の管理	dashboard*		
UpdateDashboardPublishedVersion	QuickSight ダッシュボードの公開バージョンを更新する許可を付与する	書き込み	dashboard*		
UpdateDashboardsQAConfiguration	ダッシュボード Qa 設定を更新するアクセス許可を付与します	書き込み			
UpdateDataSet	データセットを更新するアクセス許可を付与	書き込み	dataset*		quicksight:PassDataSource
			datasource		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSetPermissions	データセットのリソースポリシーを更新するアクセス許可を付与	Permissions management	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSource	データソースを更新するアクセス許可を付与	書き込み	datasource*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSourcePermissions	データソースのリソースポリシーを更新するアクセス許可を付与	権限の管理	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateDefaultQBusinessApplication	QuickSight アカウントのリンクされた QBusiness アプリケーション ID を更新する許可を付与	書き込み			
UpdateEmailCustomizationTemplate [アクセス許可のみ]	QuickSight メールカスタマイゼーションテンプレートを更新するアクセス許可を付与	書き込み	emailCustomizationTemplate*		
UpdateFolder	QuickSight フォルダを更新する許可を付与	書き込み	folder*		
UpdateFolderPermissions	QuickSight フォルダの許可を更新する許可を付与	権限の管理	folder*		
UpdateGroup	グループの説明を変更するアクセス許可を付与	書き込み	group*		
UpdateIAMPolicyAssignment	既存の割り当てを更新するアクセス許可を付与	書き込み	assignment*		
UpdateIdentityPropagationConfig	QuickSight で信頼できる ID 伝達 AWS のサービスを追加および更新するアクセス許可を付与します	書き込み			
UpdateIpRestriction	QuickSight アカウントでの IP 制限を更新するためのアクセス許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateKeyRegistration	QuickSight キー登録を更新する許可を付与する	書き込み			
UpdatePublicSharingSettings	アカウントのパブリック共有を有効または無効にするアクセス許可を付与	書き込み			
UpdateQPersonalizationConfiguration	パーソナライズ設定を更新する許可を付与する	書き込み			
UpdateQuickSightQSearchConfiguration	QuickSight Q Search 設定を更新する許可を付与	書き込み			
UpdateRefreshSchedule	データセットの更新スケジュールを更新する許可を付与	書き込み	refreshschedule*		
UpdateResourcePermissions [アクセス許可のみ]	QuickSight でリソースレベルアクセス許可を更新するアクセス許可を付与	書き込み			
UpdateRoleCustomPermission	ロールに関連付けられたカスタムアクセス許可を更新するためのアクセス許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateSPICECapacityConfiguration	QuickSight SPICE キャパシティ設定を更新する許可を付与する	書き込み			
UpdateTemplate	テンプレートを更新するアクセス許可を付与	書き込み	template*		
UpdateTemplateAlias	テンプレートエイリアスを更新するアクセス許可を付与	書き込み	template*		
UpdateTemplatePermissions	テンプレートのアクセス許可を更新するアクセス許可を付与	Permissions management	template*		
UpdateTheme	テーマを更新するアクセス許可を付与	書き込み	theme*		
UpdateThemeAlias	テーマのエイリアスを更新するアクセス許可を付与	書き込み	theme*		
UpdateThemePermissions	テーマのアクセス許可を更新するアクセス許可を付与	権限の管理	theme*		
UpdateTopic	トピックを更新する許可を付与	書き込み	topic*		quicksight:PassDataSet
			dataset		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTopicPermissions	トピックのリソースポリシーを更新する許可を付与	権限の管理	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTopicRefreshSchedule	トピックの更新スケジュールを更新する許可を付与	書き込み	topic*		
UpdateUser	Amazon QuickSight ユーザーを更新するアクセス許可を付与	書き込み	user*		
UpdateUserCustomPermission	ユーザーに関連付けられたカスタムアクセス許可を更新するアクセス許可を付与します	書き込み	user*		
UpdateVPCConnection	VPC 接続を更新する許可を付与	書き込み	vpcconnection*		iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	

Amazon QuickSight で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
account	arn:${Partition}:quicksight:${Region}:${Account}:account/${ResourceId}	
user	arn:${Partition}:quicksight:${Region}:${Account}:user/${ResourceId}	
group	arn:${Partition}:quicksight:${Region}:${Account}:group/${ResourceId}	
analysis	arn:${Partition}:quicksight:${Region}:${Account}:analysis/${ResourceId}	aws:ResourceTag/${TagKey}
dashboard	arn:${Partition}:quicksight:${Region}:${Account}:dashboard/${ResourceId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
template	arn:${Partition}:quicksight:${Region}:${Account}:template/${ResourceId}	aws:ResourceTag/${TagKey}
vpcconnection	arn:${Partition}:quicksight:${Region}:${Account}:vpcConnection/${ResourceId}	aws:ResourceTag/${TagKey}
assetBundleExportJob	arn:${Partition}:quicksight:${Region}:${Account}:asset-bundle-export-job/${ResourceId}	
assetBundleImportJob	arn:${Partition}:quicksight:${Region}:${Account}:asset-bundle-import-job/${ResourceId}	
datasource	arn:${Partition}:quicksight:${Region}:${Account}:datasource/${ResourceId}	aws:ResourceTag/${TagKey}
dataset	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${ResourceId}	aws:ResourceTag/${TagKey}
ingestion	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${DatasetId}/ingestion/${ResourceId}	aws:ResourceTag/${TagKey}
refreshschedule	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${DatasetId}/refresh-schedule/${ResourceId}	
theme	arn:${Partition}:quicksight:${Region}:${Account}:theme/${ResourceId}	aws:ResourceTag/${TagKey}
assignment	arn:${Partition}:quicksight::${Account}:assignment/${ResourceId}	

リソースタイプ	ARN	条件キー
customization	arn:${Partition}:quicksight:${Region}:${Account}:customization/${ResourceId}	aws:ResourceTag/${TagKey}
namespace	arn:${Partition}:quicksight:${Region}:${Account}:namespace/${ResourceId}	
folder	arn:${Partition}:quicksight:${Region}:${Account}:folder/${ResourceId}	aws:ResourceTag/${TagKey}
emailCustomizationTemplate	arn:${Partition}:quicksight:${Region}:${Account}:email-customization-template/${ResourceId}	
topic	arn:${Partition}:quicksight:${Region}:${Account}:topic/${ResourceId}	aws:ResourceTag/${TagKey}
dashboardSnapshotJob	arn:${Partition}:quicksight:${Region}:${Account}:dashboard/${DashboardId}/snapshot-job/${ResourceId}	aws:ResourceTag/${TagKey}
brand	arn:${Partition}:quicksight:${Region}:${Account}:brand/${ResourceId}	aws:ResourceTag/${TagKey}
custompermissions	arn:${Partition}:quicksight:${Region}:${Account}:custompermissions/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon QuickSight の条件キー

Amazon QuickSight では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	文字列
aws:TagKeys	タグキーでアクセスをフィルタリングします	ArrayOfString
quicksight:AllowedEmbeddingDomains	許可された埋め込みドメインでアクセスのフィルタリング	ArrayOfString
quicksight:DirectoryType	ユーザー管理オプションに基づいてアクセスをフィルタリングします。	String
quicksight:Edition	QuickSight のエディションに基づいてアクセスをフィルタリングします。	String
quicksight:Group	QuickSight グループ ARN でアクセスをフィルタリングします	ARN
quicksight:IamArn	IAM ユーザーまたはロール ARN によってアクセスをフィルタリングします	ARN
quicksight:KmsKeyArns	KMS キー ARN によってアクセスをフィルタリングする	ArrayOfARN
quicksight:SessionName	セッション名でアクセスをフィルタリングします	文字列
quicksight:UserName	ユーザー名でアクセスをフィルタリングします	文字列

Amazon RDS Data API のアクション、リソース、および条件キー

Amazon RDS Data API (サービスプレフィックス: `rds-data`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon RDS Data API で定義されるアクション
- Amazon RDS Data API で定義されるリソースタイプ
- Amazon RDS Data API の条件キー

Amazon RDS Data API で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchExecuteStatement	データの配列に対してバッチ SQL ステートメントを実行する権限を付与します。	書き込み	cluster*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
BeginTransaction	SQL トランザクションを開始する権限を付与します。	書き込み	cluster*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
CommitTransaction	BeginTransaction オペレーションで開始された SQL トランザクションを終了し、変更を確定する権限を付与します。	書き込み	cluster*		rds-data:BeginTransaction
				aws:ResourceTag/${TagKey} aws:TagKeys	
ExecuteSql	1 つ以上の SQL ステートメントを実行する権限を付与します。このオペレーションは非推奨です。BatchExecuteStatement または ExecuteStatement オペレーションを使用します。	書き込み	cluster*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ExecuteStatement	データベースに対して SQL 文を実行する権限を付与します。	書き込み	cluster*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RollbackTransaction	トランザクションのロールバックを実行する権限を付与します。トランザクションをロールバックすると変更はキャンセルされます。	書き込み	cluster*		rds-data:BeginTransaction
				aws:ResourceTag/${TagKey} aws:TagKeys	

Amazon RDS Data API で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
cluster	arn:${Partition}:rds:${Region}:${Account}:cluster:${DbClusterInstanceName}	aws:ResourceTag/${TagKey} aws:TagKeys

Amazon RDS Data API の条件キー

Amazon RDS Data API では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	String
aws:TagKeys	リソースに関連付けられたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon RDS IAM 認証のアクション、リソース、条件キー

Amazon RDS IAM 認証 (サービスプレフィックス: `rds-db`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon RDS IAM 認証によって定義されたアクション
- Amazon RDS IAM 認証で定義されるリソースタイプ
- Amazon RDS IAM 認証の条件キー

Amazon RDS IAM 認証によって定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
connect	IAM ロールまたはユーザーが RDS データベースに接続することを許可する	Permissions management	db-user*		

Amazon RDS IAM 認証で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
db-user	`arn:${Partition}:rds-db:${Region}:${Account}:dbuser:${DbiResourceId}/${DbUserName}`	

Amazon RDS IAM 認証の条件キー

RDS IAM 認証には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS ごみ箱 のアクション、リソース、および条件キー

AWS ごみ箱 (サービスプレフィックス: rbin) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS ごみ箱で定義されるアクション
- AWS ごみ箱で定義されるリソースタイプ
- AWS ごみ箱の条件キー

AWS ごみ箱で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateRule	ごみ箱の保持ルールを作成する許可を付与	書き込み	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys rbin:Request/ResourceType	
DeleteRule	ごみ箱保持ルールを削除するアクセス許可を付与	書き込み	rule*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				rbin:Attribute/ResourceType	
GetRule	ごみ箱保持ルールに関する詳細情報を取得するアクセス許可を付与	読み込み	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
ListRules	リージョン内のごみ箱保持ルールを一覧表示するアクセス許可を付与	読み込み		rbin:Request/ResourceType	
ListTagsForResource	リソースに関連付けられているタグを一覧表示する許可を付与	読み取り	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
LockRule	既存のごみ箱保持ルールをロックする許可を付与	書き込み	rule*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
TagResource	リソースのタグを追加または更新する許可を付与	Tagging	rule*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys rbin:Attribute/ResourceType	
UnlockRule	既存のごみ箱保持ルールのロックを解除する許可を付与	書き込み	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	リソースに関連付けられているタグを削除する許可を付与	Tagging	rule*		
				aws:ResourceTag/${TagKey} aws:TagKeys rbin:Attribute/ResourceType	
UpdateRule	既存のごみ箱保持ルールを更新するアクセス許可を付与	書き込み	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	

AWS ごみ箱で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
rule	arn:${Partition}:rbin:${Region}:${Account}:rule/${ResourceName}	aws:ResourceTag/${TagKey}

AWS ごみ箱の条件キー

AWS ごみ箱は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグのキーと値でアクセスをフィルター	String
aws:ResourceTag/${TagKey}	リクエスト内のタグキーおよび値のペアのプレゼンスによってアクションをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString
rbin:Attribute/ResourceType	既存のルールのリソースタイプでアクセスをフィルタリング	String
rbin:Request/ResourceType	リクエスト内のリソースでアクセスをフィルタリング	String

Amazon Redshift のアクション、リソース、および条件キー

Amazon Redshift (サービスプレフィックス: `redshift`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Redshift で定義されるアクション
- Amazon Redshift で定義されるリソースタイプ
- Amazon Redshift の条件キー

Amazon Redshift で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptReservedNodeExchange	設定を変更せずに DC1 リザーブドノードを DC2 リザーブドノードと交換する許可を付与	書き込み			
AddPartner	パートナー統合をクラスターに追加する許可を付与	書き込み			
AssociateDataShareConsumer	コンシューマーをデータシェアに関連付ける許可を付与	書き込み	datashare*		
				redshift:ConsumerArn	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				redshift:AllowWrites	
AuthorizeClusterSecurityGroupIngress	Amazon Redshift セキュリティグループにインバウンド（進入）ルールを追加する許可を付与	書き込み	securitygroup*		
			securitygroupingress-ec2securitygroup*		
AuthorizeDataShare	指定されたデータシェアのコンシューマーにデータシェアの使用を許可する許可を付与	権限の管理	datashare*		
				redshift:ConsumerIdentifier redshift:AllowWrites	
AuthorizeEndpointAccess	redshift マネージド vpc エンドポイントのエンドポイント関連のアクティビティを認可する許可を付与	権限の管理			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AuthorizeInboundIntegration [許可のみ]	Amazon Redshift に、ターゲットデータウェアハウスがソース ARN からレプリケートされたデータを受信できるかどうかを継続的に検証する許可を付与する	書き込み	integration*		
AuthorizeSnapshotAccess	スナップショットを復元 AWS アカウント するためのアクセス許可を指定された に付与します	権限の管理	snapshot*		
BatchDeleteClusterSnapshots	最大 100 サイズのバッチでスナップショットを削除する許可を付与	書き込み	snapshot*		
BatchModifyClusterSnapshots	スナップショットのリストの設定を変更する許可を付与	書き込み	snapshot*		
CancelQuery [アクセス許可のみ]	Amazon Redshift コンソールを使用してクエリをキャンセルする許可を付与	書き込み			
CancelQuerySession [アクセス許可のみ]	Amazon Redshift コンソールでクエリを確認する許可を付与	書き込み			
CancelResize	サイズ変更操作をキャンセルする許可を付与	書き込み	cluster*		
CopyClusterSnapshot	クラスタースナップショットをコピーする許可を付与	書き込み	snapshot*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAuthenticationProfile	Amazon Redshift 認証プロファイルを作成する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateCluster	クラスターを作成する許可を付与	書き込み	cluster*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterParameterGroup	Amazon Redshift パラメータグループを作成する許可を付与	書き込み	parametergroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSecurityGroup	Amazon Redshift セキュリティグループを作成する許可を付与	書き込み	securitygroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSnapshot	指定したクラスターの手動スナップショットを作成する許可を付与	書き込み	snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSubnetGroup	Amazon Redshift サブネットグループを作成する許可を付与	書き込み	subnetgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterUser	指定された Amazon Redshift ユーザーが存在しない場合に、自動的に作成する許可を付与	権限の管理	dbuser*		
				redshift:DbUser	
CreateCustomDomainAssociation	クラスターのカスタムドメイン名を作成するための許可を付与します	書き込み	cluster*		acm:DescribeCertificate

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateEndpointAccess	redshift マネージドエンドポイントを作成する許可を付与	書き込み			
CreateEventSubscription	Amazon Redshift イベント通知サブスクリプションを作成する許可を付与	書き込み	eventsubscription*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHsmClientCertificate	クラスターが HSM への接続に使用する HSM クライアント証明書を作成する許可を付与	書き込み	hsmclientcertificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHsmConfiguration	ハードウェアセキュリティモジュール (HSM) においてクラスターがデータベース暗号化キーを保存または使用する際に必要とする情報を含んだ HSM 設定を作成する許可を付与。	書き込み	hsmconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateInboundIntegration [アクセス許可のみ]	ソースからターゲットデータウェアハウスにデータをレプリケートするためのインバウンド統合を作成する許可をソースプリンシパルに付与する	書き込み			
CreateIntegration	Amazon Redshift ゼロ ETL 統合を作成する許可を付与する	書き込み	integration*		kms:CreateGrant kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys redshift:IntegrationSourceArn redshift:IntegrationTargetArn	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateQev2IdcApplication [アクセス許可のみ]	QEV2 IDC アプリケーションを作成する許可を付与する	書き込み			sso:CreateApplication sso:PutApplicationAccessScope sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateRedshiftIdcApplication	Redshift IDC アプリケーションを作成するためのアクセス許可を付与	書き込み			sso:CreateApplication sso:PutApplicationAccessScope sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant
CreateSavedQuery [アクセス許可のみ]	Amazon Redshift コンソールを使用して、保存された SQL クエリを作成する許可を付与	書き込み			
CreateScheduledAction	Amazon Redshift のスケジュールされたアクションを作成する許可を付与	書き込み			
CreateSnapshotCopyGrant	スナップショットコピー許可を作成し、コピー先のスナップショットを暗号化するアクセス許可を付与します AWS リージョン	権限の管理	snapshotcopygrant*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotSchedule	スナップショットスケジュールを作成する許可を付与	書き込み	snapshotschedule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTags	指定したリソースに 1 つ以上のタグを追加する許可を付与	タグ付け	cluster		
			eventsubscription		
			hsmclientcertificate		
			hsmconfiguration		
			integration		
			parametergroup		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			securitygroup		
			securitygroupingress-cidr		
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		
			usagelimit		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateUsageLimit	使用制限を作成するためのアクセス許可を付与	書き込み	usagelimit*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeauthorizeDataShare	指定したデータ共有のコンシューマーからデータ共有を使用する許可を削除する許可を付与	権限の管理	datashare*		
				redshift:ConsumerIdentifier	
DeleteAuthenticationProfile	Amazon Redshift 認証プロファイルを削除する許可を付与	書き込み			
DeleteCluster	以前にプロビジョニングされたクラスターを削除する許可を付与	書き込み	cluster*		
DeleteClusterParameterGroup	Amazon Redshift パラメータグループを削除する許可を付与	書き込み	parametergroup*		
DeleteClusterSecurityGroup	Amazon Redshift セキュリティグループを削除する許可を付与	書き込み	securitygroup*		
DeleteClusterSnapshot	手動スナップショットを削除する許可を付与	書き込み	snapshot*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteClusterSubnetGroup	クラスターサブネットグループを削除する許可を付与	書き込み	subnetgroup*		
DeleteCustomDomainAssociation	クラスターのカスタムドメイン名を削除するための許可を付与します	書き込み	cluster*		
DeleteEndpointAccess	redshift マネージドエンドポイントを削除する許可を付与	書き込み			
DeleteEventSubscription	Amazon Redshift イベント通知サブスクリプションを削除する許可を付与	書き込み	eventsubscription*		
DeleteHsmClientCertificate	HSM クライアント証明書を削除する許可を付与	書き込み	hsmclientcertificate*		
DeleteHsmConfiguration	Amazon Redshift HSM 設定を削除する許可を付与	書き込み	hsmconfiguration*		
DeleteIntegration	Amazon Redshift ゼロ ETL 統合を削除する許可を付与する	書き込み	integration*		
				aws:ResourceTag/${TagKey}	
DeletePartner	クラスターからパートナー統合を削除する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteQev2IdcApplication [アクセス許可のみ]	QEV2 IDC アプリケーションを削除するための許可を付与する	書き込み	qev2idcapplication*		sso:DeleteApplication
DeleteRedshiftIdcApplication	Redshift IDC アプリケーションを削除するためのアクセス許可を付与	書き込み	redshiftidcapplication*		sso:DeleteApplication
DeleteResourcePolicy	指定されたリソースのリソースポリシーを削除する許可を付与	権限の管理	namespace*		
DeleteSavedQueries [許可のみ]	Amazon Redshift コンソールを介して保存された SQL クエリを削除する許可を付与	書き込み			
DeleteScheduledAction	Amazon Redshift のスケジュールされたアクションを削除する許可を付与	書き込み			
DeleteSnapshotCopyGrant	スナップショットコピー許可を削除する許可を付与	書き込み	snapshotcopygrant*		
DeleteSnapshotSchedule	スナップショットスケジュールを削除する許可を付与	書き込み	snapshotschedule*		
DeleteTags	リソースから 1 つまたは複数のタグを削除する許可を付与	タグ付け	cluster		
			eventsubscription		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			hsmclientcertificate		
			hsmconfiguration		
			integration		
			parametergroup		
			securitygroup		
			securitygroupingress-cidr		
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			subnetgroup		
			usagelimit		
				aws:TagKeys	
DeleteUsageLimit	使用制限を削除するためのアクセス許可を付与	書き込み	usagelimit*		
DeregisterNamespace	指定された名前空間をコンシューマーから登録解除するアクセス許可を付与します	書き込み			
DescribeAccountAttributes	指定された にアタッチされた属性を記述するアクセス許可を付与します AWS アカウント	読み取り			
DescribeAuthenticationProfiles	作成された Amazon Redshift 認証プロファイルの詳細を取得する許可を付与	読み取り			
DescribeClusterDbRevisions	クラスターのデータベースリビジョンを記述する許可を付与	リスト			
DescribeClusterParameterGroups	Amazon Redshift パラメータグループ (自分で作成したパラメータグループとデフォルトのパラメータグループを含む) を記述する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeClusterParameters	Amazon Redshift パラメータグループに含まれるパラメータを記述する許可を付与	読み取り	parametergroup*		
DescribeClusterSecurityGroups	Amazon Redshift セキュリティグループを記述する許可を付与	読み取り			
DescribeClusterSnapshots	クラスタースナップショットに関するメタデータを含む 1 つ以上のスナップショットオブジェクトを記述する許可を付与	読み取り			
DescribeClusterSubnetGroups	クラスターサブネットグループに関するメタデータを含む 1 つまたは複数のクラスターサブネットグループオブジェクトを記述する許可を付与	読み取り			
DescribeClusterTracks	使用可能なメンテナンストラックを記述する許可を付与	リスト			
DescribeClusterVersions	利用可能な Amazon Redshift クラスターのバージョンを記述する許可を付与	読み取り			
DescribeClusters	プロビジョニングされたクラスターのプロパティを記述する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeCustomDomainAssociations	クラスターのカスタムドメイン名を記述するための許可を付与します	リスト			
DescribeDataShares	クラスターによって作成および消費されるデータシェアを記述する許可を付与	読み取り			
DescribeDataSharesForConsumer	クラスターによって消費されるデータシェアのみを記述する許可を付与	読み取り			
DescribeDataSharesForProducer	クラスターによって作成されるデータシェアのみを記述する許可を付与	読み取り			
DescribeDefaultClusterParameters	パラメータグループファミリーのパラメータ設定を記述する許可を付与	読み取り			
DescribeEndpointAccess	redshift マネージド VPC エンドポイントを記述する許可を付与	読み取り			
DescribeEndpointAuthorization	redshift マネージド VPC エンドポイントのアクティビティの記述を承認する許可を付与	リスト			
DescribeEventCategories	すべてのイベントソースタイプ、または指定されたソースタイプのイベントカテゴリを記述する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeEventSubscriptions	指定された の Amazon Redshift イベント通知サブスクリプションを記述するアクセス許可を付与します AWS アカウント	読み取り			
DescribeEvents	クラスター、セキュリティグループ、スナップショット、パラメータグループに関連する過去 14 日間のイベントを記述する許可を付与	リスト			
DescribeHsmClientCertificates	HSM クライアント証明書を記述する許可を付与	読み取り			
DescribeHsmConfigurations	Amazon Redshift HSM の設定を記述する許可を付与	読み取り			
DescribeInboundIntegrations	インバウンド統合を一覧表示する許可を付与	リスト		redshift:InboundIntegrationArn	
DescribeIntegrations	Amazon Redshift ゼロ ETL 統合を記述する許可を付与する	リスト	integration*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeLoggingStatus	クエリや接続試行などの情報がクラスターでログに記録されているかどうかを記述する許可を付与	読み取り	cluster*		
DescribeNodeConfigurationOptions	指定されたアクションタイプのノードタイプ、ノード数、ディスク使用量など、可能なノード設定のプロパティを記述する許可を付与	リスト			
DescribeOrderableClusterOptions	順序設定可能なクラスターオプションを記述する許可を付与	読み取り			
DescribePartners	クラスターに対して定義されたパートナー統合に関する情報を取得する許可を付与	読み取り			
DescribeQev2IdcApplications [許可のみ]	QEV2 IDC アプリケーションを記述する許可を付与する	リスト			
DescribeQuery [許可のみ]	Amazon Redshift コンソールを介してクエリを記述する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeRedshiftIdcApplications	Redshift IDC アプリケーションを記述するためのアクセス許可を付与	リスト			sso:GetApplicationGrant sso:ListApplicationAccessScopes
DescribeReservedNodeExchangeStatus	予約済みノード交換の交換ステータスの詳細と関連するメタデータを記述するアクセス許可を付与。ステータスには、進行中やリクエスト済みなどの値があります	読み取り			
DescribeReservedNodeOfferings	Amazon Redshift で利用可能なリザーブドノードサービスを記述する許可を付与	読み取り			
DescribeReservedNodes	リザーブドノードを記述する許可を付与	読み取り			
DescribeResize	クラスターの直近のサイズ変更操作を記述する許可を付与	読み取り	cluster*		
DescribeSavedQueries [許可のみ]	Amazon Redshift コンソールを介して保存されたクエリを記述する許可を付与	読み取り			
DescribeScheduledActions	作成された Amazon Redshift のスケジュールされたアクションを記述する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeSnapshotCopyGrants	送信先 AWS アカウント で指定された が所有するスナップショットコピー許可を記述するアクセス許可を付与します AWS リージョン	読み取り			
DescribeSnapshotSchedules	スナップショットスケジュールを記述する許可を付与	読み取り	snapshotschedule*		
DescribeStorage	アカウントレベルのバックアップのストレージサイズと暫定ストレージを記述する許可を付与	読み取り			
DescribeTable [許可のみ]	Amazon Redshift コンソールを使用してテーブルを記述する許可を付与	読み取り			
DescribeTableRestoreStatus	RestoreTableFromClusterSnapshot API アクションを使用して行われた 1 つまたは複数のテーブル復元リクエストのステータスを記述する許可を付与	読み取り			
DescribeTags	タグを記述する許可を付与	読み取り	cluster		
			eventsubscription		
			hsmclientcertificate		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			hsmconfiguration		
			integration		
			parametergroup		
			securitygroup		
			securitygroupingress-cidr		
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			usagelimit		
DescribeUsageLimits	使用制限を記述するためのアクセス許可を付与	読み取り	usagelimit*		
DisableLogging	クラスターのログ記録情報（クエリや接続の試行など）を無効にする許可を付与	書き込み	cluster*		
DisableSnapshotCopy	クラスターのスナップショットの自動コピーを無効にする許可を付与	書き込み	cluster*		
DisassociateDataShareConsumer	コンシューマーとデータシェアの関連付けを解除する許可を付与	書き込み	datashare*		
				redshift:ConsumerArn	
EnableLogging	クラスターのログ記録情報（クエリや接続の試行など）を有効にする許可を付与	書き込み	cluster*		
EnableSnapshotCopy	クラスターのスナップショットの自動コピーを有効にする許可を付与	書き込み	cluster*		
ExecuteQuery [許可のみ]	Amazon Redshift コンソールを介してクエリを実行する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
FailoverPrimaryCompute	マルチ AZ クラスターのプライマリコンピューティングを別の AZ にフェイルオーバーするアクセス許可を付与	書き込み	cluster*		
FetchResults [許可のみ]	Amazon Redshift コンソールを介してクエリ結果を取得する許可を付与	読み取り			
GetClusterCredentials	指定された によって Amazon Redshift データベースにアクセスするための一時的な認証情報を取得するアクセス許可を付与します AWS アカウント	書き込み	dbuser*		
			dbname		
				redshift:DbName redshift:DbUser redshift:DurationSeconds	
GetClusterCredentialsWithIAM	指定された によって Amazon Redshift データベースにアクセスするための拡張一時認証情報を取得するアクセス許可を付与します AWS アカウント	書き込み	dbname		
				redshift:DbName redshift:DurationSeconds	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetReservedNodeExchangeConfigurationOptions	予約済みノード交換の設定オプションを取得するアクセス許可を付与	読み取り			
GetReservedNodeExchangeOfferings	指定された DC1 リザーブドノードの支払いタイプ、期間、および使用料金に一致する DC2 ReservedNodeOfferings の配列を取得する許可を付与	読み取り			
GetResourcePolicy	指定されたリソースのリソースポリシーを取得する許可を付与	読み取り	namespace*		
JoinGroup	指定された Amazon Redshift グループに参加する許可を付与	Permissions management	dbgroup*		
ListDatabases [許可のみ]	Amazon Redshift コンソールを介してデータベースを一覧表示する許可を付与	リスト			
ListRecommendations	Advisor レコメンデーションを一覧表示する許可を付与する	リスト			
ListSavedQueries [許可のみ]	Amazon Redshift コンソールを介して、保存されたクエリを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListSchemas [許可のみ]	Amazon Redshift コンソールを介してスキーマを一覧表示する許可を付与	リスト			
ListTables [許可のみ]	Amazon Redshift コンソールを介してテーブルを一覧表示する許可を付与	リスト			
ModifyAquaConfiguration	クラスターの AQUA 設定を変更する許可を付与	書き込み	cluster*		
ModifyAuthenticationProfile	既存の Amazon Redshift 認証プロファイルを変更する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ModifyCluster	クラスターの設定を変更する許可を付与	書き込み	cluster*		acm:DescribeCertificate kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:Get

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					RandomPassword secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
ModifyClusterDbRevision	クラスターのデータベースリビジョンを変更する許可を付与	書き込み	cluster*		
ModifyClusterIamRoles	クラスターが他の AWS サービスにアクセスするために使用できる AWS Identity and Access Management (IAM) ロールのリストを変更するアクセス許可を付与します	権限の管理	cluster*		
ModifyClusterMaintenance	クラスターのメンテナンス設定を変更する許可を付与	書き込み			
ModifyClusterParameterGroup	パラメータグループのパラメータを変更する許可を付与	書き込み	parametergroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ModifyClusterSnapshot	スナップショットの設定を変更する許可を付与	書き込み	snapshot*		
ModifyClusterSnapshotSchedule	クラスターのスナップショットスケジュールを変更する許可を付与	書き込み	cluster*		
ModifyClusterSubnetGroup	VPC サブネットの指定リストを含めるためにクラスターサブネットグループを変更する許可を付与	書き込み	subnetgroup*		
ModifyCustomDomainAssociation	クラスターのカスタムドメイン名を変更するための許可を付与します	書き込み	cluster*		acm:DescribeCertificate
ModifyEndpointAccess	Redshift マネージド VPC エンドポイントを変更する許可を付与	書き込み			
ModifyEventSubscription	既存の Amazon Redshift イベント通知サブスクリプションを変更する許可を付与	書き込み	eventsubscription*		
ModifyIntegration	Amazon Redshift ゼロ ETL 統合を変更する許可を付与する	書き込み	integration*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ModifyQev2IdcApplication [アクセス許可のみ]	QEV2 IDC アプリケーションを変更する許可を付与する	書き込み	qev2idcapplication*		sso:UpdateApplication

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ModifyRedshiftIdcApplication	Redshift IDC アプリケーションを変更するためのアクセス許可を付与	書き込み	redshiftidcapplication*		sso:DeleteApplicationAccessScope sso:DeleteApplicationGrant sso:GetApplicationGrant sso:ListApplicationAccessScopes sso:PutApplicationAccessScope sso:PutApplicationGrant sso:UpdateApplication
ModifySavedQuery [許可のみ]	Amazon Redshift コンソールを介して、既存の保存されたクエリを変更する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ModifyScheduledAction	既存の Amazon Redshift のスケジュールされたアクションを変更する許可を付与	書き込み			
ModifySnapshotCopyRetentionPeriod	ソースからコピー AWS リージョン されたスナップショットを送信先に保持する日数を変更するアクセス許可を付与します AWS リージョン	書き込み	cluster*		
ModifySnapshotSchedule	スナップショットスケジュールを変更する許可を付与	書き込み	snapshotschedule*		
ModifyUsageLimit	使用制限を変更するためのアクセス許可を付与	書き込み	usagelimit*		
PauseCluster	クラスターを一時停止する許可を付与	書き込み	cluster*		
PurchaseReservedNodeOffering	リザーブドノードを購入する許可を付与	書き込み			
PutResourcePolicy	指定されたリソースのリソースポリシーを更新する許可を付与	権限の管理	namespace*		
RebootCluster	クラスターを再起動する許可を付与	書き込み	cluster*		
RegisterNamespace	指定された名前空間をコンシューマーに登録するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RejectDataShare	別のアカウントから共有されたデータシェアを拒否する許可を付与	Permissions management	datashare*		
ResetClusterParameterGroup	パラメータグループの 1 つまたは複数のパラメータをデフォルト値に設定し、パラメータのソース値を「エンジンのデフォルト」に設定する許可を付与	書き込み	parametergroup*		
ResizeCluster	クラスターのサイズを変更する許可を付与	書き込み	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RestoreFromClusterSnapshot	スナップショットからクラスターを作成する許可を付与	書き込み	cluster*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
			snapshot*		
				aws:TagKeys	
RestoreTableFromClusterSnapshot	Amazon Redshift クラスタースナップショットのテーブルからテーブルを作成する許可を付与	書き込み	cluster*		
			snapshot*		
ResumeCluster	クラスターを再開する許可を付与	書き込み	cluster*		
RevokeClusterSecurityGroupIngress	以前に承認された IP 範囲または Amazon EC2 セキュリティグループに対し、Amazon Redshift セキュリティグループ内の進入ルールを取り消すアクセス許可を付与	書き込み	securitygroup*		
			securitygroupingress-ec2securitygroup*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RevokeEndpointAccess	redshift マネージド vpc エンドポイントのエンドポイント関連アクティビティへのアクセスを取り消す許可を付与	権限の管理			
RevokeSnapshotAccess	スナップショットを復元 AWS アカウント するために指定された からアクセスを取り消すアクセス許可を付与します	権限の管理	snapshot*		
RotateEncryptionKey	クラスターの暗号化キーをローテーションする許可を付与	書き込み	cluster*		
UpdatePartnerStatus	パートナー統合のステータスを更新する許可を付与	書き込み			
ViewQueriesFromConsole [許可のみ]	Amazon Redshift コンソールを介してクエリ結果を表示する許可を付与	リスト			
ViewQueriesInConsole [許可のみ]	Amazon Redshift コンソールを介して、実行中のクエリとロードを終了する許可を付与	リスト			

Amazon Redshift で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
cluster	arn:${Partition}:redshift:${Region}:${Account}:cluster:${ClusterName}	aws:ResourceTag/${TagKey}
datashare	arn:${Partition}:redshift:${Region}:${Account}:datashare:${ProducerClusterNamespace}/${DataShareName}	aws:ResourceTag/${TagKey}
dbgroup	arn:${Partition}:redshift:${Region}:${Account}:dbgroup:${ClusterName}/${DbGroup}	
dbname	arn:${Partition}:redshift:${Region}:${Account}:dbname:${ClusterName}/${DbName}	
dbuser	arn:${Partition}:redshift:${Region}:${Account}:dbuser:${ClusterName}/${DbUser}	
eventsubscription	arn:${Partition}:redshift:${Region}:${Account}:eventsubscription:${EventSubscriptionName}	aws:ResourceTag/${TagKey}
hsmclientcertificate	arn:${Partition}:redshift:${Region}:${Account}:hsmclientcertificate:${HSMClientCertificateId}	aws:ResourceTag/${TagKey}
hsmconfiguration	arn:${Partition}:redshift:${Region}:${Account}:hsmconfiguration:${HSMConfigurationId}	aws:ResourceTag/${TagKey}
integration	arn:${Partition}:redshift:${Region}:${Account}:integration:${IntegrationIdentifier}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
namespace	arn:${Partition}:redshift:${Region}:${Account}:namespace:${ClusterNamespace}	
parametergroup	arn:${Partition}:redshift:${Region}:${Account}:parametergroup:${ParameterGroupName}	aws:ResourceTag/${TagKey}
securitygroup	arn:${Partition}:redshift:${Region}:${Account}:securitygroup:${SecurityGroupName}/ec2securitygroup/${Owner}/${Ec2SecurityGroupId}	aws:ResourceTag/${TagKey}
securitygroupingress-cidr	arn:${Partition}:redshift:${Region}:${Account}:securitygroupingress:${SecurityGroupName}/cidrip/${IpRange}	aws:ResourceTag/${TagKey}
securitygroupingress-ec2securitygroup	arn:${Partition}:redshift:${Region}:${Account}:securitygroupingress:${SecurityGroupName}/ec2securitygroup/${Owner}/${Ece2SecuritygroupId}	aws:ResourceTag/${TagKey}
snapshot	arn:${Partition}:redshift:${Region}:${Account}:snapshot:${ClusterName}/${SnapshotName}	aws:ResourceTag/${TagKey}
snapshotcopygrant	arn:${Partition}:redshift:${Region}:${Account}:snapshotcopygrant:${SnapshotCopyGrantName}	aws:ResourceTag/${TagKey}
snapshotschedule	arn:${Partition}:redshift:${Region}:${Account}:snapshotschedule:${ScheduleIdentifier}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
subnetgroup	arn:${Partition}:redshift:${Region}:${Account}:subnetgroup:${SubnetGroupName}	aws:ResourceTag/${TagKey}
usagelimit	arn:${Partition}:redshift:${Region}:${Account}:usagelimit:${UsageLimitId}	aws:ResourceTag/${TagKey}
redshiftidcapplication	arn:${Partition}:redshift:${Region}:${Account}:redshiftidcapplication:${RedshiftIdcApplicationId}	
qev2idcapplication	arn:${Partition}:redshift:${Region}:${Account}:qev2idcapplication:${Qev2IdcApplicationId}	

Amazon Redshift の条件キー

Amazon Redshift では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	各タグで許可されている値のセットに基づいて、アクションでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値に基づいて、アクションでアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
aws:TagKeys	リクエスト内の必須タグのプレゼンスに基づいて、アクションでアクセスをフィルタリングします	ArrayOfString
redshift:AllowWrites	allowWrites 入力パラメータでアクセスをフィルタリングします	Bool
redshift:ConsumerArn	データ共有コンシューマの ARN によるアクセスをフィルタリングします	ARN
redshift:ConsumerIdentifier	データシェアコンシューマーによるアクセスをフィルタリングします	文字列
redshift:DbName	データベース名でアクセスをフィルタリングします	文字列
redshift:DbUser	データベースユーザー名でアクセスをフィルタリングします	文字列
redshift:DurationSeconds	一時的な認証情報のセットが有効期限になるまで秒数によりアクセスをフィルタリングします	String
redshift:InboundIntegrationArn	インバウンドゼロ ETL 統合リソースの ARN でアクセスをフィルタリングします	ARN
redshift:IntegrationSourceArn	ゼロ ETL 統合リソースの ARN でアクセスをフィルタリングする	ARN
redshift:IntegrationTargetArn	ゼロ ETL 統合ターゲットの ARN でアクセスをフィルタリングする	ARN

Amazon Redshift Data API のアクション、リソース、および条件キー

Amazon Redshift Data API (サービスプレフィックス: `redshift-data`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Redshift Data API で定義されるアクション
- Amazon Redshift Data API で定義されるリソースタイプ
- Amazon Redshift Data API の条件キー

Amazon Redshift Data API で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchExecuteStatement	1 つの接続で複数のクエリを実行する許可を付与	書き込み	cluster		
			workgroup		
				redshift-data:session-owner-iam-user id redshift-data:glue-catalog-arn	
CancelStatement	実行中のクエリをキャンセルする許可を付与。	Write		redshift-data:stat	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ement-owner-iam-userid	
DescribeStatement	文の実行に関する詳細情報を取得する許可を付与。	Read		redshift-data:statement-owner-iam-userid	
DescribeTable	特定のテーブルに関するメタデータを取得する許可を付与。	Read	cluster*		
			workgroup*		
ExecuteStatement	クエリを実行する許可を付与	書き込み	cluster		
			workgroup		
				redshift-data:session-owner-iam-userid redshift-data:glue-catalog-arn	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetStagingBucketLocation	特定のマネージドワークグループのステージングバケットの場所を取得するアクセス許可を付与します	読み取り	managed-workgroup*		
GetStatementResult	クエリの結果を取得するためのアクセス許可を付与	Read		redshift-data:statement-owner-iam-userid	
ListDatabases	特定のクラスターのデータベースを一覧表示する許可を付与	Read	cluster*		
			workgroup*		
ListSchemas	特定のクラスターのスキーマを一覧表示する許可を付与。	Read	cluster*		
			workgroup*		
ListStatements	指定されたプリンシパルのクエリをリストする許可を付与	リスト		redshift-data:statement-owner-iam-userid	
ListTables	特定のクラスターのテーブルを一覧表示する許可を付与	リスト	cluster*		
			workgroup*		

Amazon Redshift Data API で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
cluster	`arn:${Partition}:redshift:${Region}:${Account}:cluster:${ClusterName}`	aws:ResourceTag/${TagKey}
workgroup	`arn:${Partition}:redshift-serverless:${Region}:${Account}:workgroup/${WorkgroupId}`	aws:ResourceTag/${TagKey}
managed-workgroup	`arn:${Partition}:redshift-serverless:${Region}:${Account}:managed-workgroup/${ManagedWorkgroupId}`	

Amazon Redshift Data API の条件キー

Amazon Redshift Data API では、IAM ポリシーの Condition 要素で使用できる以下の条件キーが定義されます。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値でアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
redshift-data:glue-catalog-arn	Glue Catalog ARN でアクセスをフィルタリングします	ARN
redshift-data:session-owner-iam-userid	セッション所有者の IAM ユーザー ID でアクセスをフィルタリングする	String
redshift-data:statement-owner-iam-userid	ステートメント所有者の IAM ユーザー ID でアクセスをフィルタリングします	String

Amazon Redshift Serverless のアクション、リソース、条件キー

Amazon Redshift Serverless (サービスプレフィックス:「`redshift-serverless`」) は、IAM 許可ポリシーで使用する次のサービス固有のリソース、アクション、条件コンテキストキーを提供します。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Redshift Serverless で定義されたアクション
- Amazon Redshift Serverless で定義されたリソースタイプ
- Amazon Redshift Serverless の条件キー

Amazon Redshift Serverless で定義されたアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ConvertRecoveryPointToSnapshot	復旧ポイントをスナップショットに変換する許可の付与	書き込み	recoveryPoint*		
			snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomDomainAssociation	Amazon Redshift Serverless でカスタムドメインの関連付けを作成するアクセス許可を付与	書き込み	workgroup*		acm:DescribeCertificate
CreateEndpointAccess	Amazon Redshift Serverless マネージド VPC エンドポイントを作成するアクセス許可の付与	書き込み	endpointAccess*		
CreateNamespace	Amazon Redshift Serverless 名前空間を作成する許可の付与	書き込み	namespace*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateReservation	指定された数の RPUs	書き込み			
CreateScheduledAction	指定された Amazon Redshift Serverless 名前空間にスケジュールされたアクションを作成するためのアクセス許可を付与	書き込み	namespace*		
CreateSnapshot	名前空間にあるすべてのデータベースのスナップショットを作成する許可の付与	書き込み	snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotCopyConfiguration	指定された Amazon Redshift Serverless 名前空間にスナップショットコピー設定を作成するためのアクセス許可を付与	書き込み	namespace*		
CreateUsageLimit	指定された Amazon Redshift Serverless の使用タイプに対して使用制限を作成する許可の付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateWorkgroup	Amazon Redshift Serverless でワークグループを作成する許可の付与	書き込み	workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCustomDomainAssociation	カスタムドメインの関連付けを削除するアクセス許可を付与	書き込み	workgroup*		
DeleteEndpointAccess	Amazon Redshift Serverless マネージ VCP ドエンドポイントを削除する許可の付与	書き込み	endpointAccess*		
DeleteNamespace	Amazon Redshift Serverless から名前空間を削除する許可の付与	書き込み	namespace*		kms:DescribeKey kms:RetireGrant secretsmanager:DeleteSecret secretsmanager:DescribeSecret
DeleteResourcePolicy	指定したリソースポリシーを削除する許可の付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteScheduledAction	Amazon Redshift Serverless からスケジュールされたアクションを削除するためのアクセス許可を付与	書き込み			
DeleteSnapshot	Amazon Redshift Serverless からスナップショットを削除する許可の付与	書き込み	snapshot*		
DeleteSnapshotCopyConfiguration	Amazon Redshift Serverless 名前空間のスナップショットコピー設定を削除するためのアクセス許可を付与	書き込み			
DeleteUsageLimit	Amazon Redshift Serverless から使用制限を削除する許可の付与	書き込み			
DeleteWorkgroup	ワークグループを削除する許可を付与	書き込み	workgroup*		
DescribeOneTimeCredit [アクセス許可のみ]	Amazon Redshift Serverless コンソールで、無料トライアルクレジットの残数と有効期限を確認するアクセス許可を付与します	読み取り			
GetCredentials	Amazon Redshift Serverless にログオンするため、一時的な権限を備えたデータベースユーザー名と一時的なパスワードを取得する許可の付与	書き込み	workgroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetCustomDomainAssociation	特定のカスタムドメインの関連付けに関する情報を取得するアクセス許可の付与	読み取り	workgroup*		
GetEndpointAccess	Amazon Redshift Serverless マネージド VPC エンドポイントを作成するアクセス許可の付与	読み取り	endpointAccess*		
GetManagedWorkgroup	指定された設定で Amazon Redshift Managed Serverless ワークグループを作成するアクセス許可を付与します	読み取り	managed-workgroup*		
GetNamespace	Amazon Redshift Serverless の名前空間に関する情報を取得する許可の付与	読み取り	namespace*		
GetRecoveryPoint	リカバリポイントに関する情報を取得する許可の付与	読み取り	recoveryPoint*		
GetReservation	特定の予約オブジェクトを取得するアクセス許可を付与します	読み取り			
GetReservationOffering	特定の予約サービスを取得する許可を付与	読み取り			
GetResourcePolicy	リソースポリシーを取得する許可の付与	読み取り			
GetScheduledAction	特定のスケジュールされたアクションに関する情報を取得するためのアクセス許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetSnapshot	特定のスナップショットに関する情報を取得する許可の付与	読み取り	snapshot*		
GetTableRestoreStatus	特定のスナップショットに関する情報を取得するアクセス許可を付与	読み取り			
GetTrack	Amazon Redshift Serverless のトラックに関する情報を取得するアクセス許可を付与します	読み取り			
GetUsageLimit	Amazon Redshift Serverless の使用制限に関する情報を取得する許可の付与	読み取り			
GetWorkgroup	特定のワークグループに関する情報を取得する許可の付与	読み取り	workgroup*		
ListCustomDomainAssociations	Amazon Redshift Serverless でカスタムドメインの関連付けを一覧表示するアクセス許可の付与	リスト			
ListEndpointAccess	EndpointAccess オブジェクトと関連情報を一覧表示する許可の付与	リスト	endpointAccess*		
ListManagedWorkgroups	Amazon Redshift Serverless でマネージドワークグループを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListNamespaces	Amazon Redshift Serverless の名前空間を一覧表示する許可の付与	リスト			
ListRecoveryPoints	リカバリポイントの配列を一覧表示する許可の付与	リスト	namespace		
ListReservationOfferings	使用可能なすべてのキャパシティ予約サービスを一覧表示するアクセス許可を付与します	リスト			
ListReservations	すべての予約を一覧表示するアクセス許可を付与します	リスト			
ListScheduledActions	スケジュールされたアクションを一覧表示するためのアクセス許可を付与	リスト			
ListSnapshotCopyConfigurations	SnapshotCopyConfiguration オブジェクトと関連情報を一覧表示するためのアクセス許可を付与	リスト	namespace		
ListSnapshots	スナップショットを一覧表示する許可の付与	リスト	snapshot*		
ListTableRestoreStatus	テーブルの復元ステータスを一覧表示するアクセス許可を付与	リスト			
ListTagsForResource	リソースに割り当てられたタグを一覧表示する許可の付与	リスト	namespace workgroup		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
ListTracks	Amazon Redshift Serverless で利用可能なトラックを一覧表示する許可を付与	リスト			
ListUsageLimits	Amazon Redshift Serverless のすべての使用制限を一覧表示する許可の付与	リスト			
ListWorkgroups	Amazon Redshift Serverless のワークグループを一覧表示する許可の付与	リスト			
PutResourcePolicy	リソースポリシーを作成または更新する許可を付与します。	書き込み			
RestoreFromRecoveryPoint	リカバリポイントからデータを復元する許可の付与	書き込み	recoveryPoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RestoreFromSnapshot	スナップショットから名前空間を復元する許可の付与	書き込み	snapshot*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
RestoreTableFromRecoveryPoint	リカバリポイントからテーブルを復元するためのアクセス許可を付与	書き込み	namespace*		
			recoveryPoint*		
RestoreTableFromSnapshot	スナップショットからテーブルを復元するアクセス許可を付与	書き込み	namespace*		
			snapshot*		
TagResource	リソースに 1 つ以上のタグを割り当てる許可の付与	Tagging	namespace		
			recoveryPoint		
			snapshot		
			workgroup		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	リソースから 1 つのタグまたは一連のタグを削除する許可の付与	Tagging	namespace		
			recoveryPoint		
			snapshot		
			workgroup		
				aws:TagKeys	
UpdateCustomDomainAssociation	カスタムドメインに関連付けられた証明書を更新するアクセス許可の付与	書き込み	workgroup*		acm:DescribeCertificate
UpdateEndpointAccess	Amazon Redshift Serverless マネージド VPC エンドポイントを更新する許可の付与	書き込み	endpointAccess*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateNamespace	指定された設定セッティングで名前空間を更新する許可の付与	書き込み	namespace*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
UpdateScheduledAction	スケジュールされたアクションを更新するためのアクセス許可を付与	書き込み			
UpdateSnapshot	スナップショットを更新する許可の付与	書き込み	snapshot*		
UpdateSnapshotCopyConfiguration	Amazon Redshift Serverless 名前空間のスナップショットコピー設定を更新するためのアクセス許可を付与	書き込み			
UpdateUsageLimit	Amazon Redshift Serverless の使用制限を更新する許可の付与	書き込み			
UpdateWorkgroup	指定された設定セッティングで Amazon Redshift Serverless ワークグループを更新するアクセス許可の付与	書き込み	workgroup*		

Amazon Redshift Serverless で定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
namespace	arn:${Partition}:redshift-serverless:${Region}:${Account}:namespace/${NamespaceId}	aws:ResourceTag/${TagKey}
snapshot	arn:${Partition}:redshift-serverless:${Region}:${Account}:snapshot/${SnapshotId}	aws:ResourceTag/${TagKey}
workgroup	arn:${Partition}:redshift-serverless:${Region}:${Account}:workgroup/${WorkgroupId}	aws:ResourceTag/${TagKey}
managed-workgroup	arn:${Partition}:redshift-serverless:${Region}:${Account}:managed-workgroup/${ManagedWorkgroupName}	
recoveryPoint	arn:${Partition}:redshift-serverless:${Region}:${Account}:recoverypoint/${RecoveryPointId}	aws:ResourceTag/${TagKey}
endpointAccess	arn:${Partition}:redshift-serverless:${Region}:${Account}:managedvpcendpoint/${EndpointAccessId}	

Amazon Redshift Serverless の条件キー

Amazon Redshift Serverless は、IAM ポリシーの 「Condition」 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
redshift-serverless:endpointAccessId	エンドポイントのアクセス識別子でアクセスのフィルタリング	String
redshift-serverless:managedWorkgroupName	マネージドワークグループ識別子でアクセスをフィルタリングします	String
redshift-serverless:namespaceId	名前空間の識別子でアクセスのフィルタリング	String
redshift-serverless:recoveryPointId	リカバリポイントで識別子でアクセスのフィルタリング	String

条件キー	説明	タイプ
redshift-serverless:snapshotId	スナップショットで識別子でアクセスのフィルタリング	String
redshift-serverless:tableRestoreRequestId	テーブル復元リクエスト ID でアクセスをフィルタリングします	String
redshift-serverless:workgroupId	ワークグループの識別子でアクセスのフィルタリング	String

Amazon Rekognition のアクション、リソース、および条件キー

Amazon Rekognition (サービスプレフィックス: `rekognition`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Rekognition で定義されるアクション
- Amazon Rekognition で定義されるリソースタイプ
- Amazon Rekognition の条件キー

Amazon Rekognition で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateFaces	1 人のユーザーに複数の顔を個別の関連付ける許可を付与	書き込み	collection*		
CompareFaces	ソース入力イメージ内の顔とターゲット入力イメージ内で検出された各顔を比較する許可を付与します。	読み取り			
CopyProjectVersion	既存のモデルバージョンを新しいモデルバージョンにコピーする許可を付与	書き込み	project*		
			projectversion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCollection	でコレクションを作成するアクセス許可を付与します AWS リージョン	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	新しい Amazon Rekognition Custom Labels データセットを作成するためのアクセス許可を付与します。	書き込み	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateFaceLivenessSession	Face Liveness セッションを作成する許可を付与	書き込み			
CreateProject	Amazon Rekognition Custom Labels プロジェクトを作成するためのアクセス許可を付与します。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProjectVersion	モデルの新しいバージョントレーニングを開始するアクセス許可を付与します。	書き込み	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStreamProcessor	Amazon Rekognition ストリームプロセッサを作成するアクセス許可を付与します。	書き込み	collection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUser	提供した一意のユーザー ID を使用して、コレクション内に新しいユーザー作成する許可を付与	書き込み	collection*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteCollection	指定されたコレクションを削除するためのアクセス許可を付与します。	書き込み	collection*		
DeleteDataset	既存の Amazon Rekognition Custom Labels データセットを削除するアクセス許可を付与します。	書き込み	dataset*		
DeleteFaces	コレクションから顔を削除する許可を付与します。	書き込み	collection*		
DeleteProject	プロジェクトを削除する許可を付与	書き込み	project*		
DeleteProjectPolicy	プロジェクトにアタッチされたリソースポリシーを削除する許可を付与	書き込み	project*		
DeleteProjectVersion	モデルを削除する許可を付与	書き込み	projectversion*		
DeleteStreamProcessor	指定された ストリープロセッサーを削除する許可を付与します。	書き込み	streamprocessor*		
DeleteUser	提供されたユーザー ID に基づいて、コレクションからユーザーを削除する許可を付与	書き込み	collection*		
DescribeCollection	コレクションに関する詳細を読み取るためのアクセス許可を付与します。	読み込み	collection*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeDataset	Amazon Rekognition Custom Labels データセットを記述するアクセス許可を付与します。	読み込み	dataset*		
DescribeProjectVersions	Amazon Rekognition Custom Labels プロジェクトでモデルのバージョンを一覧表示するアクセス許可を付与します。	読み込み	project*		
DescribeProjects	Amazon Rekognition Custom Labels プロジェクトを一覧表示するアクセス許可を付与します。	読み込み			
DescribeStreamProcessor	指定されたストリームプロセッサーに関する情報を取得する許可を付与します。	読み込み	streamprocessor*		
DetectCustomLabels	提供された画像内のカスタムラベルを検出する権限を付与します。	読み込み	projectversion*		
DetectFaces	入力として提供されるイメージ内の人間の顔を検出するアクセス許可を付与します。	読み込み			
DetectLabels	入力として提供されるイメージ内の実社会ラベルのインスタンスを検出する許可を付与します。	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DetectModerationLabels	入力画像内のモデレーションラベルを検出する権限を付与します。	読み込み	projectversion		
DetectProtectiveEquipment	入力画像内の個人用保護具を検出するアクセス許可を付与します。	読み込み			
DetectText	入力イメージ内のテキストを検出し、コンピュータが読み取り可能なテキストに変換する許可を付与します。	読み取り			
DisassociateFaces	ユーザー ID と顔 ID の関連付けを削除する許可を付与	書き込み	collection*		
DistributeDatasetEntries	トレーニングデータセット内のエントリを、プロジェクトのトレーニングデータセットおよびテストデータセット全体に分散する権限を付与します。	書き込み	dataset*		
GetCelebrityInfo	有名人の名前と追加情報を読む権限を付与します。	読み込み			
GetCelebrityRecognition	非同期有名人認識ジョブによって保存されたビデオで見つかった有名人認識の結果を読み取る権限を付与します。	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetContentModeration	非同期コンテンツモデレーションジョブによって保存された動画で見つかったコンテンツモデレーション分析結果を読み取る権限を付与します。	読み込み			
GetFaceDetection	非同期顔検出ジョブによって保存されたビデオで見つかった顔検出結果を読み取る権限を付与します。	読み取り			
GetFaceLivenessSessionResults	Face Liveness セッションの結果を取得する許可を付与	読み取り			
GetFaceSearch	非同期顔検索ジョブによって保存されたビデオで見つかった一致するコレクション顔を読み取る権限を付与します。	読み込み			
GetLabelDetection	非同期ラベル検出ジョブによって保存されたビデオで見つかったラベル検出結果を読み取る権限を付与します。	読み取り			
GetMediaAnalysisJob	S3 内のジョブ結果への参照とメディア分析ジョブに関する追加情報を読み取るアクセス許可を付与します。	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetPersonTracking	非同期の人物追跡ジョブによって保存されたビデオで検出された人物のリストを読み取る権限を付与します。	読み込み			
GetSegmentDetection	非同期セグメント検出ジョブによって、保存されたビデオで見つかったビデオセグメントを取得する権限を付与します。	読み込み			
GetTextDetection	非同期テキスト検出ジョブによって保存されたビデオで見つかったテキストを取得する権限を付与します。	読み込み			
IndexFaces	入力イメージで検出された顔で既存のコレクションを更新するアクセス許可を付与します。	書き込み	collection*		
ListCollections	アカウント内のコレクション ID を読み取る権限を付与します。	読み込み			
ListDatasetEntries	既存の Amazon Rekognition Custom Labels データセット内のデータセットエントリを一覧表示する権限を付与します。	読み込み	dataset*		
ListDatasetLabels	データセットのラベルを一覧表示する権限を付与します。	読み込み	dataset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListFaces	指定したコレクション内の顔のメタデータを読み込むアクセス許可を付与します。	読み取り	collection*		
ListMediaAnalysisJobs	メディア分析ジョブのリストを読み取るアクセス許可を付与します。	読み取り			
ListProjectPolicies	プロジェクトにアタッチされたリソースポリシーを一覧表示する許可を付与	読み取り	project*		
ListStreamProcessors	ストリームプロセッサのリストを取得するアクセス許可を付与します。	リスト			
ListTagsForResource	リソースに関連付けられたタグのリストを返す許可を付与します。	読み取り	collection		
			dataset		
			project		
			projectversion		
			streamprocessor		
ListUsers	UserId および UserStatus を一覧表示する許可を付与	読み取り	collection*		
PutProjectPolicy	リソースポリシーをプロジェクトにアタッチする許可を付与	書き込み	project*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RecognizeCelebrities	入力画像内の有名人を検出するアクセス許可を付与します。	読み込み			
SearchFaces	提供された顔IDに、指定されたコレクションを検索する権限を付与します。	読み込み	collection*		
SearchFacesByImage	入力画像内の最大の顔の特定されたコレクションを検索するアクセス許可を付与します。	読み取り	collection*		
SearchUsers	指定されたコレクション内で、特定の顔 ID またはユーザー ID に一致するユーザーを検索する許可を付与	読み取り	collection*		
SearchUsersByImage	入力画像内の最大の顔を使用して、指定されたコレクションで一致するユーザーを検索する許可を付与	読み取り	collection*		
StartCelebrityRecognition	保存した動画内の有名人の非同期認識を開始する許可を付与します。	書き込み			
StartContentModeration	保存した動画の明示的もしくは暗示的なアダルトコンテンツの非同期検出を開始する許可を付与します。	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartFaceDetection	保存したビデオの顔の非同期検出を開始するアクセス許可を付与します。	書き込み			
StartFaceLivenessSession	Face Liveness のセッションの動画ストリーミングを開始する許可を付与	書き込み			
StartFaceSearch	保存した動画で検出された人物の顔に一致するコレクションの顔の非同期検索を開始する許可を付与します。	書き込み	collection*		
StartLabelDetection	保存した動画内のラベルの非同期検出を開始するアクセス許可を付与します。	書き込み			
StartMediaAnalysisJob	メディア分析ジョブを開始するアクセス許可を付与します。	書き込み	projectversion		
StartPersonTracking	保存した動画内の人の非同期トラッキングを開始する許可を付与します。	書き込み			
StartProjectVersion	モデルのバージョンを実行する許可を付与します。	書き込み	projectversion*		
StartSegmentDetection	保存したビデオのセグメントの非同期検出を開始するアクセス許可を付与します。	書き込み			
StartStreamProcessor	ストリームプロセッサの実行を開始するアクセス許可を付与します。	書き込み	streamprocessor*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartTextDetection	保存したビデオのテキストの非同期検出を開始するアクセス許可を付与します。	書き込み			
StopProjectVersion	モデルのバージョンの実行を停止する許可を付与します。	書き込み	projectversion*		
StopStreamProcessor	実行中のストリームプロセッサを停止するアクセス許可を付与します。	書き込み	streamprocessor*		
TagResource	リソースに 1 つ以上のタグを追加する許可を付与	タグ付け	collection		
			dataset		
			project		
			projectversion		
			streamprocessor		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースから 1 つ以上のタグを削除する許可を付与	Tagging	collection		
			dataset		
			project		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			projectversion		
			streamprocessor		
				aws:TagKeys	
UpdateDatasetEntries	データセット内の 1 つ以上の JSON 行 (エントリ) を追加または更新する権限を付与します。	書き込み	dataset*		
UpdateStreamProcessor	ストリームプロセッサのプロパティを修正する許可の付与	書き込み	streamprocessor*		

Amazon Rekognition で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
collection	`arn:${Partition}:rekognition:${Region}:${Account}:collection/${CollectionId}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
streamprocessor	arn:${Partition}:rekognition:${Region}:${Account}:streamprocessor/${StreamprocessorId}	aws:ResourceTag/${TagKey}
project	arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/${CreationTimestamp}	aws:ResourceTag/${TagKey}
projectversion	arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/version/${VersionName}/${CreationTimestamp}	aws:ResourceTag/${TagKey}
dataset	arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/dataset/${DatasetType}/${CreationTimestamp}	aws:ResourceTag/${TagKey}

Amazon Rekognition の条件キー

Amazon Rekognition では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストで渡されたタグによりアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグによりアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーによりアクセスをフィルタリングします	ArrayOfString

AWS rePost Private のアクション、リソース、および条件キー

AWS rePost Private (サービスプレフィックス: `repostspace`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS rePost Private で定義されるアクション
- AWS rePost Private で定義されるリソースタイプ
- AWS rePost Private の条件キー

AWS rePost Private で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchAddChannelRol	アカウントのプライベート re:Post チャネルのユーザーと	書き込み	space*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
eToAccessors	グループにロールを追加するアクセス許可を付与します				
BatchAddRole	アカウントのプライベート re:Post のユーザーとグループにロールを追加するアクセス許可を付与します	書き込み	space*		
BatchRemoveChannelRoleFromAccessors	アカウントのプライベート re:Post チャネルのユーザーとグループからロールを削除するアクセス許可を付与します	書き込み	space*		
BatchRemoveRole	アカウントのプライベート re:Post のユーザーとグループからロールを削除するアクセス許可を付与します	書き込み	space*		
CreateChannel	アカウントのプライベート re:Post に新しいチャネルを作成するアクセス許可を付与します	書き込み	space*		
CreateSpace	アカウントに新しいプライベート re:Post を作成する許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteSpace	アカウントからプライベート re:Post を削除する許可を付与	書き込み	space*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeregisterAdmin	アカウントのプライベート re:POST に管理者を削除する許可を付与	書き込み	space*		
GetChannel	アカウントのプライベート re:Post のチャネルの説明を取得するアクセス許可を付与します	読み取り	space*		
GetSpace	アカウントのプライベート re:Post の説明を取得する許可を付与する	読み取り	space*		
ListChannels	アカウントのプライベート re:Post 内のすべてのチャネルを一覧表示するアクセス許可を付与します	読み取り	space*		
ListSpaces	アカウント内のすべてのプライベート re:Post を一覧表示する許可を付与	読み取り			
ListTagsForResource	リソースに関連付けられているタグを一覧表示する許可を付与	読み取り	space*		
				aws:TagKeys aws:RequestTag/${TagKey}	
RegisterAdmin	アカウントのプライベート re:Post に管理者を追加するアクセス許可を付与します	書き込み	space*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SendInvites	アカウント内のプライベート re:Post のユーザーに招待を送信する許可を付与	書き込み	space*		
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	space*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	リソースのタグを解除する許可を付与	Tagging	space*		
				aws:TagKeys	
UpdateChannel	アカウントのプライベート re:Post でチャネルを更新する許可を付与	書き込み	space*		
UpdateSpace	アカウント内のプライベート re:Post を更新する許可を付与	書き込み	space*		

AWS rePost Private で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
space	arn:${Partition}:repostspace:${Region}:${Account}:space/${ResourceId}	aws:ResourceTag/${TagKey}

AWS rePost Private の条件キー

AWS rePost Private では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

AWS Resilience Hub のアクション、リソースおよび条件キー

AWS Resilience Hub (サービスプレフィックス: resiliencehub) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Resilience Hub で定義されるアクション
- AWS Resilience Hub で定義されるリソースタイプ
- AWS Resilience Hub の条件キー

AWS Resilience Hub で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptResourceGroupingRecommendations	リソースのグループ化の推奨事項を受け入れる許可を付与する	書き込み	application*		
AddDraftAppVersionResourceMappings	ドラフトアプリケーションバージョンリソースマッピングを追加するアクセス許可を付与します。	書き込み	application*		cloudformation:DescribeStacks cloudformation:ListStackResources resource-groups:GetGroup resource-groups:ListGroupResources

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					servicecatalog:GetApplication servicecatalog:ListAssociatedResources
BatchUpdateRecommendationStatus	1 つ以上のオペレーションに関するレコメンデーションを含めたり除外したりする許可を付与します	書き込み	application*		
CreateApp	アプリケーションを作成する許可を付与します。	書き込み	application*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAppVersionAppComponent	アプリケーションのアプリコンポーネントを作成するための許可を付与します	書き込み	application*		
CreateAppVersionResource	アプリケーションリソースを作成するための許可を付与します	書き込み	application*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateRecommendationTemplate	推奨テンプレートを作成するためのアクセス許可を付与します。	書き込み	application*		s3:CreateBucket s3:ListBucket s3:PutObject
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResiliencyPolicy	回復力 ポリシーを作成する許可を付与します。	書き込み	resiliency-policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApp	アプリケーションを一括で削除する許可を付与します。	書き込み	application*		
DeleteAppAssessment	アプリケーション評価を一括で削除するアクセス許可を付与します。	書き込み	application*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteAppInputSource	アプリケーションの入力ソースを削除するための許可を付与します	書き込み	application*		
DeleteAppVersionAppComponent	アプリケーションのアプリコンポーネントを削除するための許可を付与します	書き込み	application*		
DeleteAppVersionResource	アプリケーションリソースを削除するための許可を付与します	書き込み	application*		
DeleteRecommendationTemplate	レコメンデーションテンプレートを一括で削除するアクセス許可を付与します。	書き込み	application*		
DeleteResiliencyPolicy	回復力ｂポリシーを一括で削除する許可を付与します。	書き込み	resiliency-policy*		
DescribeApp	アプリケーションを記述する許可を付与します。	読み取り	application*		
DescribeAppAssessment	アプリケーション評価を記述する許可を付与します。	読み取り	application*		
DescribeAppVersion	アプリケーションバージョンを記述するための許可を付与します	読み取り	application*		
DescribeAppVersionAppComponent	アプリケーションバージョンのアプリコンポーネントを記述するための許可を付与します	読み取り	application*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeAppVersionResource	アプリケーションバージョンリソースを記述するための許可を付与します	読み取り	application*		
DescribeAppVersionResourcesResolutionStatus	アプリケーション決意を記述する許可を付与します。	読み取り	application*		
DescribeAppVersionTemplate	アプリケーションバージョンテンプレートを記述する許可を付与します。	読み取り	application*		
DescribeDraftAppVersionResourcesImportStatus	ドラフトアプリケーションバージョンリソースのインポートステータスを記述する権限を付与します。	読み取り	application*		
DescribeMetricsExport	メトリクスのエクスポートを記述する許可を付与	読み取り			
DescribeResiliencyPolicy	回復力ポリシーを記述する許可を付与します。	読み取り	resiliency-policy*		
DescribeResourceGroupingRecommendationTask	グループ化の推奨事項プロセスの最新のステータスを記述する許可を付与する	読み取り	application*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ImportResourcesToDraftAppVersion	ドラフトアプリケーションバージョンにリソースをインポートするアクセス許可を付与します。	書き込み	application*		cloudformation:DescribeStacks cloudformation:ListStackResources resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources
ListAlarmRecommendations	アラームレコメンデーションを一覧表示するアクセス許可を付与します。	リスト	application*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListAppAssessmentComplianceDrifts	評価の実行中に検出されたコンプライアンスドリフトを一覧表示する許可を付与します	リスト	application*		
ListAppAssessmentResourceDrifts	評価の実行中に検出されたリソースドリフトを一覧表示する許可を付与する	リスト	application*		
ListAppAssessments	アプリケーション評価を一覧表示する許可を付与します。	リスト			
ListAppComponentCompliances	appのコンポーネントコンプライアンスを一覧表示する許可を付与します。	リスト	application*		
ListAppComponentRecommendations	appコンポーネントレコメンデーションを一覧表示するアクセス許可を付与します。	リスト	application*		
ListAppInputSources	アプリケーションの入力ソースを一覧表示するための許可を付与します	リスト	application*		
ListAppVersionAppComponents	アプリケーションバージョンのアプリコンポーネントを一覧表示するための許可を付与します	リスト	application*		
ListAppVersionResourceMappings	アプリケーションのバージョンリソースマッピングにアクセス権限を付与します。	リスト	application*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListAppVersionResources	アプリケーションリソースを一覧表示するためのアクセス権限を付与します。	リスト	application*		
ListAppVersions	アプリケーションのバージョンを一覧表示するためのアクセス許可を付与します。	リスト	application*		
ListApps	アプリケーションを一覧表示する許可を付与します。	リスト			
ListMetrics	メトリクスを一覧表示するアクセス許可を付与します	リスト			
ListRecommendationTemplates	推奨テンプレートを一覧表示する許可を付与します。	リスト	application*		
ListResiliencyPolicies	回復ポリシーを一覧表示する許可を付与します。	リスト			
ListResourceGroupingRecommendations	リソースのグループ化の推奨事項を一覧表示する許可を付与する	リスト	application*		
ListSopRecommendations	SOPレコメンデーションを一覧表示するアクセス許可を付与します。	リスト	application*		
ListSuggestedResiliencyPolicies	推奨される回復力ポリシーを一覧表示するアクセス許可を付与します。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り			
ListTestRecommendations	テストレコメンデーションを一覧表示するアクセス許可を付与します。	リスト	application*		
ListUnsupportedAppVersionResources	サポートされていないアプリケーションバージョンリソースを一覧表示するアクセス許可を付与します。	リスト	application*		
PublishAppVersion	アプリケーションバージョンを発行するアクセス許可を付与します。	書き込み	application*		
PutDraftAppVersionTemplate	アプリケーションバージョンテンプレートの下書きを配置するアクセス許可を付与します。	書き込み	application*		
RejectResourceGroupingRecommendations	リソースのグループ化の推奨事項を拒否する許可を付与する	書き込み	application*		
RemoveDraftAppVersionResourceMappings	ドラフトアプリケーションバージョンマッピングを削除するアクセス許可を付与します。	書き込み	application*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ResolveAppVersionResources	アプリケーションバージョンリソースを解決するアクセス許可を付与します。	書き込み	application*		cloudformation:DescribeStacks cloudformation:ListStackResources resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartAppAssessment	アプリケーション評価を作成するアクセス許可を付与します。	書き込み	application*		cloudformation:DescribeStacks cloudformation:ListStackResources cloudwatch:DescribeAlarms cloudwatch:GetMetricData cloudwatch:GetMetricStatistics cloudwatch:PutMetricData ec2:DescribeRegions fis:GetExperimentTemplate

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					fis:ListExperimentTemplates fis:ListExperiments resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources ssm:GetParametersByPath

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
StartMetricsExport	メトリクスのエクスポートを開始するアクセス許可を付与します	書き込み			
StartResourceGroupingRecommendationTask	グループ化の推奨事項生成プロセスを開始する許可を付与する	書き込み	application*		
TagResource	リソースタグを割り当てるアクセス許可を付与	Tagging	app-assessment		
			application		
			recommendation-template		
			resiliency-policy		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースのタグを解除する許可を付与	Tagging	app-assessment		
			application		
			recommendation-template		
			resiliency-policy		
				aws:TagKeys	
UpdateApp	アプリケーションを更新する許可を付与します。	書き込み	application*		iam:PassRole
UpdateAppVersion	アプリケーションバージョンを更新するための許可を付与します	書き込み	application*		
UpdateAppVersionAppComponent	アプリケーションのアプリコンポーネントを更新するための許可を付与します	書き込み	application*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateAppVersionResource	アプリケーションリソースを更新するための許可を付与します	書き込み	application*		
UpdateResiliencyPolicy	回復力ポリシーを更新する許可を付与します。	書き込み	resiliency-policy*		

AWS Resilience Hub で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
resiliency-policy	arn:${Partition}:resiliencehub:${Region}:${Account}:resiliency-policy/${ResiliencyPolicyId}	aws:ResourceTag/${TagKey}
application	arn:${Partition}:resiliencehub:${Region}:${Account}:app/${AppId}	aws:ResourceTag/${TagKey}
app-assessment	arn:${Partition}:resiliencehub:${Region}:${Account}:app-assessment/${AppAssessmentId}	aws:ResourceTag/${TagKey}
recommendation-template	arn:${Partition}:resiliencehub:${Region}:${Account}:recommendation-template/${RecommendationTemplateId}	aws:ResourceTag/${TagKey}

AWS Resilience Hub の条件キー

AWS Resilience Hub では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Resource Access Manager (RAM) のアクション、リソース、および条件キー

AWS Resource Access Manager (RAM) (サービスプレフィックス: ram) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Resource Access Manager (RAM) で定義されるアクション

- AWS Resource Access Manager (RAM) で定義されるリソースタイプ
- AWS Resource Access Manager (RAM) の条件キー

AWS Resource Access Manager (RAM) で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AcceptResourceShareInvitation	指定されたリソース共有の招待を受け入れるアクセス許可を付与します。	Write	resource-share-invitation*		
				ram:ShareOwnerAccountId ram:ResourceShareName	
AssociateResourceShare	リソースやプリンシパルをリソース共有に関連付けるアクセス許可を付与します	Write	resource-share*		
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ram:AllowsExternalPrincipals ram:Principal ram:RequestedResourceType ram:ResourceArn	
AssociateResourceSharePermission	アクセス許可をリソース共有に関連付けるアクセス許可を付与します	書き込み	customer-managed-permission*		
			permission*		
			resource-share*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreatePermission	リソース共有に関連付けるアクセス許可を作成するアクセス許可を付与します	書き込み		ram:PermissionArn ram:PermissionResourceType aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	ram:TagResource
CreatePermissionVersion	リソース共有に関連付けるアクセス許可の新しいバージョンを作成するアクセス許可を付与します	書き込み	customer-managed-permission *		
				ram:PermissionArn ram:PermissionResourceType	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateResourceShare	指定されたリソースやプリンシパルでリソース共有を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys ram:RequestedResourceType ram:ResourceArn ram:RequestedAllowsExternalPrincipals ram:Principal ram:AllowsExternalPrincipals	
DeletePermission	指定されたアクセス許可を削除するアクセス許可を付与します	書き込み	customer-managed-permission*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} ram:PermissionArn ram:PermissionResourceType	
DeletePermissionVersion	指定されたアクセス許可のバージョンを削除するアクセス許可を付与します	書き込み	customer-managed-permission*		
				ram:PermissionArn ram:PermissionResourceType	
DeleteResourceShare	リソース共有を削除する許可を付与	Write	resource-share*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals	
DisassociateResourceShare	リソース共有からリソースやプリンシパルの関連付けを解除する許可を付与	Write	resource-share*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:Principal ram:RequestedResourceType ram:ResourceArn	
DisassociateResourceSharePermission	リソース共有からのアクセス許可の関連付けを解除する許可を付与	Write	customer-managed-permission*		
			permission*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			resource-share*		
EnableSharingWithAwsOrganization	お客様の組織へのアクセス許可を付与し、お客様のアカウントで SLR を作成します。	権限の管理			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess
GetPermission	RAM AWS アクセス許可の内容を取得するアクセス許可を付与します	読み取り	customer-managed-permission*		
			permission*		
				ram:PermissionArn	
GetResourcePolicies	ユーザーが所有し、共有している、指定されたリソースのポリシーを取得する許可を付与	Read			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetResourceShareAssociations	提供されたリストからまたは指定されたタイプの指定されたステータスを使用して、一連のリソースの共有の関連付けを取得する許可を付与	Read			
GetResourceShareInvitations	指定された招待 arn によるリソースの共有の招待、またはリソースの共有のためのリソースの共有の招待を取得する許可を付与	Read			
GetResourceShares	提供されたリストからまたは指定されたステータスを使用して、一連のリソースの共有を取得する許可を付与	Read		aws:RequestTag/${TagKey} aws:TagKeys	
ListPendingInvitationResources	ユーザーと共有されていますが、招待が保留中であるリソースの共有のリソースを一覧表示する許可を付与	読み取り	resource-share-invitation*		
				ram:ResourceShareName	
ListPermissionAssociations	アクセス許可と、その関連付けに関する情報を一覧表示する許可を付与	リスト	customer-managed-permission*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			permission*		
				ram:PermissionArn ram:PermissionResourceType	
ListPermissionVersions	AWS RAM アクセス許可のバージョンを一覧表示するアクセス許可を付与します	リスト			
ListPermissions	RAM AWS アクセス許可を一覧表示するアクセス許可を付与します	リスト			
ListPrincipals	リソースを共有しているプリンシパル、または共有リソースを持つプリンシパルを一覧表示する許可を付与	リスト			
ListReplacePermissionAssociationsWork	非同期アクセス許可置換のステータスを取得するアクセス許可を付与します	リスト			
ListResourceSharePermissions	リソース共有に関連付けられているアクセス許可の一覧を表示する許可を付与	リスト	resource-share*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals	
ListResourceTypes	RAM AWS でサポートされている共有可能なリソースタイプを一覧表示するアクセス許可を付与します	リスト			
ListResources	リソース共有に追加したリソース、または自分と共有しているリソースを一覧表示する許可を付与	リスト			
PromotePermissionCreatedFromPolicy	完全に管理可能な個別のカスタマー管理アクセス許可を作成するアクセス許可を付与します	書き込み	customer-managed-permission*		
				ram:PermissionArn ram:PermissionResourceType	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PromoteResourceShareCreatedFromPolicy	指定されたリソース共有を昇格する許可を付与	Write	resource-share*		
RejectResourceShareInvitation	指定されたリソース共有の招待を拒否する許可を付与	書き込み	resource-share-invitation*		
				ram:ShareOwnerAccountId ram:ResourceShareName	
ReplacePermissionAssociations	すべてのリソース共有を新しいアクセス許可に更新する許可を付与	書き込み	customer-managed-permission*		
			permission*		
				ram:PermissionArn ram:PermissionResourceType	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SetDefaultPermissionVersion	各カスタマー管理アクセス許可のデフォルトバージョンとしてバージョン番号を指定するアクセス許可を付与します	書き込み	customer-managed-permission *		
				ram:PermissionArn ram:PermissionResourceType	
TagResource	指定されたリソースまたはアクセス許可にタグを付けるアクセス許可を付与します	Tagging	customer-managed-permission		
			resource-share		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	指定されたリソース共有またはアクセス許可のタグを解除するアクセス許可を付与します	Tagging	customer-managed-permission		
			resource-share		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
UpdateResourceShare	リソース共有の属性を更新する許可を付与	書き込み	resource-share*		
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:RequestedAllowsExternalPrincipals	

AWS Resource Access Manager (RAM) で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
resource-share	arn:${Partition}:ram:${Region}:${Account}:resource-share/${ResourcePath}	aws:ResourceTag/${TagKey} ram:AllowsExternalPrincipals ram:ResourceShareName
resource-share-invitation	arn:${Partition}:ram:${Region}:${Account}:resource-share-invitation/${ResourcePath}	ram:ShareOwnerAccountId
permission	arn:${Partition}:ram::${Account}:permission/${ResourcePath}	ram:PermissionArn ram:PermissionResourceType
customer-managed-permission	arn:${Partition}:ram:${Region}:${Account}:permission/${ResourcePath}	aws:ResourceTag/${TagKey} ram:PermissionArn ram:PermissionResourceType

AWS Resource Access Manager (RAM) の条件キー

AWS Resource Access Manager (RAM) では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リソース共有を作成またはタグ付けする際にリクエストで渡されたタグで、アクセスをフィルタリングします。ユーザーがこれらのタグを渡さないか、タグをまったく指定しない場合、リクエストは失敗します	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	String
aws:TagKeys	リソース共有を作成またはタグ付けする際に渡されたタグキーで、アクセスをフィルタリング	ArrayOfString
ram:AllowsExternalPrincipals	外部プリンシパルとの共有を許可または拒否するリソース共有で、アクセスをフィルタリングします。たとえば、外部プリンシパルとの共有を許可または拒否するリソースの共有でのみアクションを実行できる場合は true を指定します。外部プリンシパルは AWS 、組織外の AWS アカウントです	Bool
ram:PermissionArn	指定されたアクセス許可 ARN でアクセスをフィルタリング	ARN
ram:PermissionResourceType	指定されたリソースタイプのアクセス許可でアクセスをフィルタリング	String
ram:Principal	指定されたプリンシパルの形式でアクセスをフィルタリング	String
ram:RequestedAllowsExternalPrincipals	'allowExternalPrincipals' に対し指定された値でアクセスをフィルタリングします。外部プリンシパルは AWS 、組織外の AWS アカウントです	Bool

条件キー	説明	[Type] (タイプ)
ram:RequestedResourceType	指定されたリソースタイプでアクセスをフィルタリング	String
ram:ResourceArn	指定された ARN でアクセスをフィルタリング	ARN
ram:ResourceShareName	指定された名前を持つリソース共有でアクセスをフィルタリング	String
ram:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	String
ram:ShareOwnerAccountId	特定のアカウントが所有するリソース共有でアクセスをフィルタリングします。例えば、この条件キーを使用して、リソース共有の所有者アカウント ID に基づいて、招待を承認または却下するリソースの共有を指定できます	String

AWS Resource Explorer のアクション、リソース、および条件キー

AWS Resource Explorer (サービスプレフィックス: `resource-explorer-2`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Resource Explorer で定義されるアクション
- AWS Resource Explorer で定義されるリソースタイプ

- AWS Resource Explorer の条件キー

AWS Resource Explorer で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateDefaultView	指定したビューをこの AWS リージョン のデフォルトとして設定するアクセス許可を付与します AWS アカウント	書き込み			
BatchGetView	ARN のリストで指定するビューに関するア詳細を取得する許可を付与	読み取り			resource-explorer-2:GetView
CreateIndex	インデックスを作成してこのオペレーションを呼び出した AWS リージョン で Resource Explorer を有効にするアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateManagedView [アクセス許可のみ]	マネージドビューを作成するアクセス許可を付与します	書き込み			
CreateView	ユーザーがクエリできるビューを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteIndex	インデックスを削除 AWS リージョン して、指定されたで Resource Explorer をオフ	書き込み	index*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	にするアクセス許可を付与します				
DeleteResourcePolicy [アクセス許可のみ]	指定したビューのリソースポリシーを削除する許可を付与する	権限の管理	view*		
DeleteView	ビューを削除する許可を付与	書き込み	view*		
DisassociateDefaultView	このオペレーションを呼び出す AWS リージョン のデフォルトビューを削除するアクセス許可を付与します	書き込み			
GetAccountLevelServiceConfiguration	AWS 組織内のアカウントレベルのデータにアクセスするためのアクセス許可を Resource Explorer に付与します	読み取り			
GetDefaultView	このオペレーションを呼び出す AWS リージョン のデフォルトであるビューの Amazon リソースネーム (ARN) を取得するアクセス許可を付与します	読み取り			
GetIndex	このオペレーションを呼び出す AWS リージョン のインデックスに関する情報を取得するアクセス許可を付与します	読み取り			
GetManagedView	マネージドビューを取得する許可を付与	読み取り	managed-view*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetResourcePolicy [許可のみ]	指定されたビューのリソースポリシーに関する情報を取得する許可を付与する	読み取り	view*		
GetView	指定したビューに関する情報を取得する許可を付与	読み取り	view*		
ListIndexes	すべての のインデックスを一覧表示するアクセス許可を付与します AWS リージョン	リスト			
ListIndexesForMembers	すべての で組織メンバーアカウントのインデックスを一覧表示するアクセス許可を付与します AWS リージョン	リスト			
ListManagedViews	マネージドビューを一覧表示する許可を付与	リスト			
ListSupportedResourceTypes	Resource Explorer で現在サポートされているすべてのリソースタイプのリストを取得する許可を付与	リスト			
ListTagsForResource	指定されたリソースにアタッチされているタグを一覧表示する許可を付与	読み取り	index view		
ListViews	このオペレーションを呼び出す AWS リージョン で使用可能なすべてのビューの Amazon リソースネーム (ARNs) を一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutResourcePolicy [許可のみ]	指定されたビューのリソースポリシーを更新する許可を付与する	権限の管理	view*		
Search	リソースを検索し、指定された条件に一致するすべてのリソースの詳細を表示する許可を付与	読み取り	view*		
				resource-explorer-2:Operation	
TagResource	指定されたリソースに 1 つ以上のタグキーと値のペアを追加する許可を付与	Tagging	index		
			view		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	指定したリソースに 1 つ以上のタグ (キーと値) を削除する許可を付与	Tagging	index		
			view		
				aws:TagKeys	
UpdateIndexType	項目のタイプを LOCAL から AGGREGATOR に、またはその逆に変更する許可を付与	書き込み	index*		
UpdateView	ビューのいくつかの詳細を変更する許可を付与	書き込み	view*		

AWS Resource Explorer で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
view	arn:${Partition}:resource-explorer-2:${Region}:${Account}:view/${ViewName}/${ViewUuid}	aws:ResourceTag/${TagKey}
index	arn:${Partition}:resource-explorer-2:${Region}:${Account}:index/${IndexUuid}	aws:ResourceTag/${TagKey}
managed-view	arn:${Partition}:resource-explorer-2:${Region}:${Account}:managed-view/${ManagedViewName}/${ManagedViewUuid}	

AWS Resource Explorer の条件キー

AWS Resource Explorer では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストで渡されたタグキーでアクセスをフィルタリングする	String

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	リソースにアタッチされたタグキーによりアクセスをフィルタリング	String
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
resource-explorer-2:Operation	呼び出されている実際のオペレーション、使用可能な値でアクセスをフィルタリングします: Search、ListResources	String

Amazon リソースグループのタグ付け API のアクション、リソース、および条件キー

Amazon リソースグループのタグ付け API (サービスプレフィックス: `tag`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon リソースグループのタグ付け API で定義されるアクション
- Amazon リソースグループのタグ付け API で定義されるリソースタイプ
- Amazon リソースグループのタグ付け API の条件キー

Amazon リソースグループのタグ付け API で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeReportCreation	StartReportCreation オペレーションのステータスを記述する許可を付与	読み取り			
GetComplianceSummary	有効なタグポリシーに準拠していないリソースの数についての概要を取得する許可を付与	読み取り			
GetResources	呼び出し元のアカウントに指定された で、タグ付けされたリソースまたは以前にタグ付けされたリソースを返 AWS リージョン すアクセス許可を付与します	読み取り			
GetTagKeys	呼び出し元のアカウントに指定された で現在使用されているタグキーを返 AWS リージョン すアクセス許可を付与します	読み取り			
GetTagValues	呼び出し元のアカウントに指定された で使用される指定されたキー AWS リージョン のタグ値を返すアクセス許可を付与します	読み取り			
StartReportCreation	組織全体のアカウントにあるすべてのタグ付けされたリソースと、各リソースが有効なタグポリシーに準拠しているかどうかを一覧表示するレ	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	ポートの生成を開始する許可を付与				
TagResources	指定されたリソースに 1 つ以上のタグを適用する許可を付与	Tagging			
UntagResources	指定されたリソースから指定されたタグを削除する許可を付与	Tagging			

Amazon リソースグループのタグ付け API で定義されるリソースタイプ

Amazon リソースグループのタグ付け API では、IAM ポリシーステートメントの `Resource` 要素でのリソース ARN の指定はサポートされていません。Amazon リソースグループのタグ付け API へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

Amazon リソースグループのタグ付け API の条件キー

リソースグループのタグ付けには、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Resource Groups のアクション、リソース、および条件キー

AWS Resource Groups (サービスプレフィックス: `resource-groups`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Resource Groups で定義されるアクション
- AWS Resource Groups で定義されるリソースタイプ
- AWS Resource Groups の条件キー

AWS Resource Groups で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateResource [アクセス許可のみ]	リソースをアプリケーションに関連付ける許可を付与	書き込み	group*		
CancelTagSyncTask	アプリケーショングループのタグ同期タスクをキャンセルする許可を付与する	書き込み	group*		resource-groups:DeleteGroup
CreateGroup	指定した名前、記述、リソースクエリでリソースグループを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	cloudformation:DescribeStacks
DeleteGroup	指定されたリソースグループを削除する許可を付与	書き込み	group*		tag:GetResources
DeleteGroupPolicy [アクセス許可のみ]	指定されたグループのリソースベースのポリシーを削除する許可を付与する	書き込み	group*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisassociateResource [アクセス許可のみ]	リソースのアプリケーションへの関連付けを解除する許可を付与	書き込み	group*		
GetAccountSettings	リソースグループのオプション機能の現在のステータスを取得するための許可を付与します	読み取り			
GetGroup	指定されたリソースグループの情報を取得する許可を付与	読み込み	group*		
GetGroupConfiguration	指定されたリソースグループに関連付けられたサービス設定を取得する許可を付与	読み取り	group*		
GetGroupPolicy [許可のみ]	指定されたグループのリソースベースのポリシーを取得する許可を付与する	読み取り	group*		
GetGroupQuery	指定されたリソースグループに関連付けられたクエリを取得する許可を付与	読み取り	group*		
GetTagSyncTask	指定されたタグ同期タスクの情報を取得する許可を付与する	読み取り	group*		
GetTags	指定されたリソースグループに関連付けられたタグを取得する許可を付与	読み込み	group*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GroupResources	指定されたリソースを指定されたグループに追加する許可を付与	書き込み	group*		resource-groups:Tag tag:TagResources
ListGroupResources	指定されたリソースグループのメンバーであるリソースを一覧表示する許可を付与	リスト	group*		cloudformation:DescribeStacks cloudformation:ListStackResources tag:GetResources
ListGroupingStatuses	指定されたアプリケーショングループのグループ化ステータスを一覧表示する許可を付与する	リスト	group*		
ListGroups	アカウント内のすべての Resource Groups を一覧表示する許可を付与	リスト			
ListResourceTypes [許可のみ]	サポートされているリソースタイプを一覧表示する許可を付与する	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTagSyncTasks	アカウントですべてのタグ同期タスクを一覧表示する許可を付与する	リスト	group*		
PutGroupConfiguration	指定された Resource Groups に関連付けられたサービス設定を配置する許可を付与	書き込み	group*		
PutGroupPolicy [アクセス許可のみ]	指定されたグループにリソースベースのポリシーを追加する許可を付与	書き込み	group*		
SearchResources	指定されたクエリに一致する AWS リソースを検索するアクセス許可を付与します	リスト			cloudformation:DescribeStacks cloudformation:ListStackResources tag:GetResources
StartTagSyncTask	アプリケーショングループのタグ同期タスクを作成する許可を付与する	書き込み	group*		iam:PassRole resource-groups:CreateGroup
Tag	指定されたリソースグループにタグを付けるアクセス許可を付与	タグ付け	group*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UngroupResources	指定されたグループから指定されたリソースを削除する許可を付与	書き込み	group*		resource-groups:Untag tag:UntagResources
Untag	指定されたリソースグループに関連付けられたタグを削除する許可を付与	Tagging	group*		
				aws:TagKeys	
UpdateAccountSettings	リソースグループのオプション機能を更新するための許可を付与します	書き込み			
UpdateGroup	指定されたリソースグループを更新する許可を付与	書き込み	group*		
UpdateGroupQuery	指定されたリソースグループに関連付けられたクエリを更新する許可を付与	書き込み	group*		cloudformation:DescribeStacks

AWS Resource Groups で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアク

ションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
group	arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}	aws:ResourceTag/${TagKey}
tagSyncTask	arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}/tag-sync-task/${TaskId}	aws:ResourceTag/${TagKey}

AWS Resource Groups の条件キー

AWS Resource Groups は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

Amazon RHEL ナレッジベースポータルのアクション、リソース、条件キー

Amazon RHEL ナレッジベースポータル (サービスプレフィックス: rhelkb) では、IAM アクセス許可ポリシーで使用するための、以下のサービス固有のリソース、アクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon RHEL ナレッジベースポータルで定義されるアクション
- Amazon RHEL ナレッジベースポータルで定義されるリソースタイプ
- Amazon RHEL ナレッジベースポータルの条件キー

Amazon RHEL ナレッジベースポータルで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイ

プが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetRhelURL	Red Hat ナレッジベースポータルへのアクセス許可を付与	読み取り			

Amazon RHEL ナレッジベースポータルで定義されるリソースタイプ

Amazon RHEL ナレッジベースポータルでは、IAM ポリシーステートメントの Resource 要素でのリソース ARN の指定はサポートされていません。Amazon RHEL ナレッジベースポータルへのアクセスを許可するには、ポリシーで "Resource": "*" を指定します。

Amazon RHEL ナレッジベースポータルの条件キー

RHEL KB には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS RoboMaker のアクション、リソース、および条件キー

AWS RoboMaker (サービスプレフィックス: robomaker) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS RoboMaker で定義されるアクション
- AWS RoboMaker で定義されるリソースタイプ
- AWS RoboMaker の条件キー

AWS RoboMaker で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchDeleteWorlds	バッチオペレーションで 1 つまたは複数のワールドを削除します	書き込み			
BatchDescribeSimulationJob	複数のシミュレーションジョブについて説明します	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelDeploymentJob	展開ジョブをキャンセルします	書き込み	deploymentJob*		
CancelSimulationJob	シミュレーションジョブをキャンセルする	書き込み	simulationJob*		
CancelSimulationJobBatch	シミュレーションジョブバッチをキャンセルします	書き込み	simulationJobBatch*		
CancelWorldExportJob	ワールドのエクスポートジョブをキャンセルします	書き込み	worldExportJob*		
CancelWorldGenerationJob	ワールドの生成ジョブをキャンセルします	書き込み	worldGenerationJob*		
CreateDeploymentJob	デプロイジョブを作成する	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateFleet	同じロボットアプリケーションを実行しているロボットの論理グループを表すデプロイフリートを作成します	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateRobot	フリートに登録できるロボットを作成します	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateRobotApplication	ロボットアプリケーションを作成する	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateRobotApplicationVersion	ロボットアプリケーションのスナップショットを作成します	書き込み	robotApplication*		s3:GetObject
CreateSimulationApplication	シミュレーションアプリケーションの作成	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateSimulationApplicationVersion	シミュレーションアプリケーションのスナップショットを作成します	書き込み	simulationApplication*		s3:GetObject

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSimulationJob	シミュレーションジョブの作成	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateWorldExportJob	ワールドのエクスポートジョブを作成します	書き込み	world*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateWorldGenerationJob	ワールドの生成ジョブを作成します	書き込み	worldTemplate*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateWorldTemplate	ワールドテンプレートを作成します	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteFleet	デプロイフリートの削除	書き込み	deploymentFleet*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteRobot	ロボットを削除する	書き込み	robot*		
DeleteRobotApplication	ロボットアプリケーションを削除する	書き込み	robotApplication*		
DeleteSimulationApplication	シミュレーションアプリケーションを削除する	書き込み	simulationApplication*		
DeleteWorldTemplate	ワールドテンプレートを削除します	書き込み	worldTemplate*		
DeregisterRobot	フリートからロボットを登録解除します	書き込み	deploymentFleet*		
			robot*		
DescribeDeploymentJob	デプロイジョブについて説明します	読み込み	deploymentJob*		
DescribeFleet	デプロイフリートについて説明します	読み込み	deploymentFleet*		
DescribeRobot	ロボットについて説明します	読み込み	robot*		
DescribeRobotApplication	ロボットアプリケーションについて説明します	読み込み	robotApplication*		
DescribeSimulationApplication	シミュレーションアプリケーションの説明	読み込み	simulationApplication*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeSimulationJob	シミュレーションジョブについて説明します	読み込み	simulationJob*		
DescribeSimulationJobBatch	シミュレーションジョブバッチについて説明します	読み込み	simulationJobBatch*		
DescribeWorld	ワールドについて説明します	読み込み	world*		
DescribeWorldExportJob	ワールドのエクスポートジョブについて説明します	読み込み	worldExportJob*		
DescribeWorldGenerationJob	ワールドの生成ジョブについて説明します	読み込み	worldGenerationJob*		
DescribeWorldTemplate	ワールドテンプレートについて説明します	読み込み	worldTemplate*		
GetWorldTemplateBody	ワールドテンプレートの本文を取得します	読み込み	worldTemplate*		
ListDeploymentJobs	デプロイジョブを一覧表示します	リスト			
ListFleets	フリートを一覧表示します	リスト			
ListRobotApplications	ロボットアプリケーションを一覧表示します	リスト			
ListRobots	ロボットを一覧表示します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListSimulationApplications	シミュレーションアプリケーションを一覧表示します	リスト			
ListSimulationJobBatches	シミュレーションジョブバッチを一覧表示します	リスト			
ListSimulationJobs	シミュレーションジョブを一覧表示します	リスト			
ListSupportedAvailabilityZones [許可のみ]	サポートされているアベイラビリティーゾーンを一覧表示します	リスト			
ListTagsForResource	RoboMaker リソースのタグを一覧表示します	リスト	deploymentFleet		
			deploymentJob		
			robot		
			robotApplication		
			simulationApplication		
			simulationJob		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			simulationJobBatch		
			world		
			worldExportJob		
			worldGenerationJob		
			worldTemplate		
ListWorldExportJobs	ワールドのエクスポートジョブを一覧表示します	リスト			
ListWorldGenerationJobs	ワールドの生成ジョブを一覧表示します	リスト			
ListWorldTemplates	ワールドテンプレートを一覧表示します	リスト			
ListWorlds	ワールドを一覧表示します	リスト			
RegisterRobot	フリートにロボットを登録します	書き込み	deploymentFleet*		
			robot*		
RestartSimulationJob	実行中のシミュレーションジョブを再開します	書き込み	simulationJob*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartSimulationJobBatch	シミュレーションジョブバッチを作成します	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
SyncDeploymentJob	フリート内のすべてのロボットに最近デプロイされたロボットアプリケーションがデプロイされるようにします	書き込み	deploymentFleet*		iam:CreateServiceLinkedRole
TagResource	RoboMaker リソースにタグを追加します	Tagging	deploymentFleet		
			deploymentJob		
			robot		
			robotApplication		
			simulationApplication		
			simulationJob		
			simulationJobBatch		
			world		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			worldExportJob		
			worldGenerationJob		
			worldTemplate		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	RoboMaker リソースからタグを削除します	Tagging	deploymentFleet		
			deploymentJob		
			robot		
			robotApplication		
			simulationApplication		
			simulationJob		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			simulationJobBatch		
			world		
			worldExportJob		
			worldGenerationJob		
			worldTemplate		
				aws:TagKeys	
UpdateRobotApplication	ロボットアプリケーションを更新する	書き込み	robotApplication*		
UpdateRobotDeployment [アクセス許可のみ]	個々のロボットのデプロイ状況を報告します	書き込み			
UpdateSimulationApplication	シミュレーションアプリケーションを更新する	書き込み	simulationApplication*		
UpdateWorldTemplate	ワールドテンプレートを更新します	書き込み	worldTemplate*		

AWS RoboMaker で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
robotApplication	arn:${Partition}:robomaker:${Region}:${Account}:robot-application/${ApplicationName}/${CreatedOnEpoch}	aws:ResourceTag/${TagKey}
simulationApplication	arn:${Partition}:robomaker:${Region}:${Account}:simulation-application/${ApplicationName}/${CreatedOnEpoch}	aws:ResourceTag/${TagKey}
simulationJob	arn:${Partition}:robomaker:${Region}:${Account}:simulation-job/${SimulationJobId}	aws:ResourceTag/${TagKey}
simulationJobBatch	arn:${Partition}:robomaker:${Region}:${Account}:simulation-job-batch/${SimulationJobBatchId}	aws:ResourceTag/${TagKey}
deploymentJob	arn:${Partition}:robomaker:${Region}:${Account}:deployment-job/${DeploymentJobId}	aws:ResourceTag/${TagKey}
robot	arn:${Partition}:robomaker:${Region}:${Account}:robot/${RobotName}/${CreatedOnEpoch}	aws:ResourceTag/${TagKey}
deploymentFleet	arn:${Partition}:robomaker:${Region}:${Account}:deployment-fleet/${FleetName}/${CreatedOnEpoch}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
worldGenerationJob	arn:${Partition}:robomaker:${Region}:${Account}:world-generation-job/${WorldGenerationJobId}	aws:ResourceTag/${TagKey}
worldExportJob	arn:${Partition}:robomaker:${Region}:${Account}:world-export-job/${WorldExportJobId}	aws:ResourceTag/${TagKey}
worldTemplate	arn:${Partition}:robomaker:${Region}:${Account}:world-template/${WorldTemplateJobId}	aws:ResourceTag/${TagKey}
world	arn:${Partition}:robomaker:${Region}:${Account}:world/${WorldId}	aws:ResourceTag/${TagKey}

AWS RoboMaker の条件キー

AWS RoboMaker では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられているタグに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーに基づいてアクションをフィルタリングします	ArrayOfString

Amazon Route 53 のアクション、リソース、および条件キー

Amazon Route 53 (サービスプレフィックス: route53) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Route 53 で定義されるアクション
- Amazon Route 53 で定義されるリソースタイプ
- Amazon Route 53 の条件キー

Amazon Route 53 で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ActivateKeySigningKey	DNSSEC による署名に使用できるように、キー署名キーをアクティブ化する許可を付与	書き込み	hostedzone*		
AssociateVPCWithHostedZone	追加の Amazon VPC をプライベートホストゾーンに関連付けるアクセス許可を付与	書き込み	hostedzone		ec2:DescribeVpcs
				route53:VPCs	
ChangeCidrCollection	CIDR コレクション内の CIDR ブロックを作成または削除する許可を付与	書き込み	cidrcollection*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ChangeResourceRecordSets	レコードを作成、更新、または削除する許可を付与。このアクセス許可には、指定されたドメインやサブドメイン名の正式な DNS 情報を含む	書き込み	hostedzone*		
				route53:ChangeResourceRecordSetsNormalizedRecordNames route53:ChangeResourceRecordSetsRecordTypes route53:ChangeResourceRecordSetsActions	
ChangeTagsForResource	ヘルスチェックまたはホストゾーンのタグを追加、編集、または削除する許可を付与	Tagging	healthcheck*		
			hostedzone*		
CreateCidrCollection	新しい CIDR コレクションを作成する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateHealthCheck	新しいヘルスチェックを作成する許可を付与。これにより、ウェブアプリケーションやウェブサーバーなどのリソースの状態やパフォーマンスをモニタリング	書き込み			
CreateHostedZone	パブリックホストゾーンを作成する許可を付与。このアクセス許可を使用して、ドメインネームシステム (DNS) で example.com などのドメインやそのサブドメインのインターネットトラフィックをルーティングする方法を指定	書き込み		route53:VPCs	ec2:DescribeVpcs
CreateKeySigningKey	ホストゾーンに関連付けられた新しいキー署名キーを作成する許可を付与	書き込み	hostedzone*		
CreateQueryLoggingConfig	DNS クエリログ記録の設定を作成する許可を付与	書き込み	hostedzone*		
CreateReusableDelegationSet	複数のホストゾーンで再利用できる委任セット (4 つのネームサーバーのグループ) を作成する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateTrafficPolicy	トラフィックポリシーを作成する許可を付与。このアクセス許可を使用して、1 つのドメイン名 (例: example.com) または 1 つのサブドメイン名 (例: www.example.com) に対して複数の DNS レコードを作成	書き込み			
CreateTrafficPolicyInstance	指定されたトラフィックポリシーバージョンの設定に基づき、指定されたホストゾーンにレコードを作成する許可を付与	書き込み	hostedzone* trafficpolicy*		
CreateTrafficPolicyVersion	既存のトラフィックポリシーの新しいバージョンを作成する許可を付与	書き込み	trafficpolicy*		
CreateVPCAssociationAuthorization	指定された VPC AWS アカウント を作成した が AssociateVPCWithHostedZone リクエストを送信することを許可するアクセス許可を付与します。このリクエストは、VPC を別のアカウントによって作成された指定されたホストゾーンに関連付けます。	書き込み	hostedzone* 	 route53:VPCs	
DeactivateKeySigningKey	DNSSEC による署名に使用されないように、キー署名キーを非アクティブ化する許可を付与	書き込み	hostedzone*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteCidrCollection	CIDR コレクションを削除する許可を付与	書き込み	cidrcollection*		
DeleteHealthCheck	ヘルスチェックを削除する許可を付与	書き込み	healthcheck*		
DeleteHostedZone	ホストゾーンを削除する許可を付与。	書き込み	hostedzone*		
DeleteKeySigningKey	キー署名キーを削除する許可を付与	書き込み	hostedzone*		
DeleteQueryLoggingConfig	DNS クエリログ記録の設定を削除する許可を付与。	書き込み	queryloggingconfig*		
DeleteReusableDelegationSet	再利用可能な委任セットを削除する許可を付与	書き込み	delegationset*		
DeleteTrafficPolicy	トラフィックポリシーを削除する許可を付与	書き込み	trafficpolicy*		
DeleteTrafficPolicyInstance	トラフィックポリシーインスタンスと、インスタンスの作成時に Route 53 で作成されたすべてのレコードを削除する許可を付与	書き込み	trafficpolicyinstance*		
DeleteVPCAssociationAuthorization	Amazon Virtual Private Cloud を Route 53 プライベートホストゾーンに関連付ける認可を削除する許可を付与	書き込み	hostedzone*		
				route53:VPCs	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DisableHostedZoneDNSSEC	特定のホストゾーンで DNSSEC サインインを無効にする許可を付与	書き込み	hostedzone*		
DisassociateVPCFromHostedZone	Route 53 プライベートホストゾーンから Amazon Virtual Private Cloud の関連付けを解除する許可を付与	書き込み	hostedzone		ec2:DescribeVpcs
				route53:VPCs	
EnableHostedZoneDNSSEC	特定のホストゾーンで DNSSEC サインインを有効にする許可を付与	書き込み	hostedzone*		
GetAccountLimit	現在のアカウントの指定された制限 (例: アカウントを使用して作成できるヘルスチェックの最大数) を取得する許可を付与	読み込み			
GetChange	1 つ以上のレコードを作成、更新、または削除するリクエストの現在のステータスを取得する許可を付与	リスト	change*		
GetCheckerIpRanges	リソースの状態を確認するために Route 53 ヘルスチェッカーで使用される IP 範囲のリストを取得する許可を付与	リスト			
GetDNSSEC	ホストゾーンのキー署名キーを含む、特定のホストゾーンの DNSSEC に関する情報を取得する許可を付与	読み込み	hostedzone*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetGeoLocation	指定された地理的な場所が Route 53 位置情報レコードでサポートされているかどうかに関する情報を取得する許可を付与	リスト			
GetHealthCheck	指定されたヘルスチェックに関する情報を取得する許可を付与	読み取り	healthcheck*		
GetHealthCheckCount	現在の に関連付けられているヘルスチェックの数を取得する許可を付与 AWS アカウント	リスト			
GetHealthCheckLastFailureReason	指定されたヘルスチェックが最近失敗した理由を取得する許可を付与	リスト	healthcheck*		
GetHealthCheckStatus	指定されたヘルスチェックのステータスを取得する許可を付与	リスト	healthcheck*		
GetHostedZone	指定されたホストゾーンに関する情報 (例: Route 53 によってホストゾーンに割り当てられた 4 つのネームサーバー) を取得する許可を付与	リスト	hostedzone*		
GetHostedZoneCount	現在の に関連付けられているホストゾーンの数を取得するアクセス許可を付与します AWS アカウント	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetHostedZoneLimit	指定されたホストゾーンに対して指定された制限を取得する許可を付与	読み込み	hostedzone*		
GetQueryLoggingConfig	DNS クエリログ記録の指定された設定に関する情報を取得する許可を付与	読み込み	queryloggingconfig*		
GetReusableDelegationSet	指定された再利用可能な委任セット (例: 委任セットに割り当てられた 4 つのネームサーバー) を取得する許可を付与	リスト	delegationset*		
GetReusableDelegationSetLimit	指定した再利用可能な委任セットに関連付けることができるホストゾーンの最大数を取得する許可を付与。	読み込み	delegationset*		
GetTrafficPolicy	指定されたトラフィックポリシーバージョンに関する情報を取得する許可を付与。	読み込み	trafficpolicy*		
GetTrafficPolicyInstance	指定されたトラフィックポリシーインスタンスに関する情報を取得する許可を付与	読み取り	trafficpolicyinstance*		
GetTrafficPolicyInstanceCount	現在の に関連付けられているトラフィックポリシーインスタンスの数を取得するアクセス許可を付与します AWS アカウント	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListCidrBlocks	指定された CIDR コレクション内の CIDR ブロックのリストを取得する許可を付与	リスト	cidrcollection*		
ListCidrCollections	現在の に関連付けられている CIDR コレクションのリストを取得する許可を付与 AWS アカウント	リスト			
ListCidrLocations	指定された CIDR コレクションに属する CIDR ロケーションのリストを取得する許可を付与	リスト	cidrcollection*		
ListGeoLocations	Route 53 がサポートする地理的な場所のリストを取得する許可を付与	読み取り			
ListHealthChecks	現在の に関連付けられているヘルスチェックのリストを取得するアクセス許可を付与します AWS アカウント	読み取り			
ListHostedZones	現在の に関連付けられているパブリックホストゾーンとプライベートホストゾーンのリストを取得するアクセス許可を付与します AWS アカウント	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListHostedZonesByName	辞書式順序でホストゾーンのリストを取得する許可を付与ホストゾーンは、ラベルを逆にして名前でソートされます (例: com.example.www)。	リスト			
ListHostedZonesByVPC	指定した VPC が関連付けられているすべてのプライベートホストゾーンのリストを取得する許可を付与	リスト		route53:VPCs	ec2:DescribeVpcs
ListQueryLoggingConfigs	現在の に関連付けられている DNS クエリログ記録の設定、AWS アカウント または指定されたホストゾーンに関連付けられている設定を一覧表示するアクセス許可を付与します	リスト	hostedzone		
ListResourceRecordSets	指定されたホストゾーンのレコードを一覧表示する許可を付与	リスト	hostedzone*		
ListReusableDelegationSets	現在の AWS アカウントに関連付けられた再利用可能な委託セットを一覧表示するアクセス許可を付与	読み取り			
ListTagsForResource	1 つのヘルスチェックまたはホストゾーンのタグを一覧表示する許可を付与	読み込み	healthcheck		
			hostedzone		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTagsForResources	最大 10 のヘルスチェックまたはホストゾーンのタグを一覧表示する許可を付与	読み取り	healthcheck		
			hostedzone		
ListTrafficPolicies	現在の AWS アカウントに関連付けられているすべてのトラフィックポリシーの最新バージョンの情報を取得するアクセス許可を付与。ポリシーは、作成された順に一覧表示	リスト			
ListTrafficPolicyInstances	現在の を使用して作成したトラフィックポリシーインスタンスに関する情報を取得するアクセス許可を付与します AWS アカウント	読み取り			
ListTrafficPolicyInstancesByHostedZone	指定されたホストゾーンで作成したトラフィックポリシーインスタンスに関する情報を取得する許可を付与	リスト	hostedzone*		
ListTrafficPolicyInstancesByPolicy	指定されたトラフィックポリシーバージョンを使用して作成したトラフィックポリシーインスタンスに関する情報を取得する許可を付与	リスト	trafficpolicy*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTrafficPolicyVersions	指定されたトラフィックポリシーのすべてのバージョンに関する情報を取得する許可を付与	リスト	trafficpolicy*		
ListVPCAssociationAuthorizations	他のアカウントによって作成され、指定されたホストゾーンに関連付けることができるVPC のリストを取得する許可を付与	リスト	hostedzone*		
TestDNSAnswer	指定されたレコード名とタイプの DNS クエリに応答して Route 53 によって返される値を取得する許可を付与	読み込み			
UpdateHealthCheck	既存のヘルスチェックを更新する許可を付与	書き込み	healthcheck*		
UpdateHostedZoneComment	指定されたホストゾーンのコメントを更新する許可を付与	書き込み	hostedzone*		
UpdateTrafficPolicyComment	指定されたトラフィックポリシーバージョンのコメントを更新する許可を付与	書き込み	trafficpolicy*		
UpdateTrafficPolicyInstance	指定されたトラフィックポリシーバージョンの設定に基づき作成された、指定のホストゾーンのレコードを更新する許可を付与	書き込み	trafficpolicyinstance*		

Amazon Route 53 で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
cidrcollection	arn:${Partition}:route53:::cidrcollection/${Id}	
change	arn:${Partition}:route53:::change/${Id}	
delegationset	arn:${Partition}:route53:::delegationset/${Id}	
healthcheck	arn:${Partition}:route53:::healthcheck/${Id}	
hostedzone	arn:${Partition}:route53:::hostedzone/${Id}	
trafficpolicy	arn:${Partition}:route53:::trafficpolicy/${Id}	
trafficpolicyinstance	arn:${Partition}:route53:::trafficpolicyinstance/${Id}	
queryloggingconfig	arn:${Partition}:route53:::queryloggingconfig/${Id}	
vpc	arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}	

Amazon Route 53 の条件キー

Amazon Route 53 では、IAM ポリシーの `Condition` 要素で使用できる以下の条件キーが定義されます。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
route53:ChangeResourceRecordSetsActions	ChangeResourceRecordSets リクエスト内の変更アクション (CREATE、UPSERT、または DELETE) でアクセスをフィルタリングします	ArrayOfString
route53:ChangeResourceRecordSetsNormalizedRecordNames	ChangeResourceRecordSets リクエスト内の正規化された DNS レコード名でアクセスをフィルタリングします	ArrayOfString
route53:ChangeResourceRecordSetsRecordTypes	ChangeResourceRecordSets リクエスト内の DNS レコードタイプでアクセスをフィルタリングします	ArrayOfString
route53:VPCs	リクエスト内の VPCs でアクセスをフィルタリングします	String

Amazon Route 53 Domains のアクション、リソース、および条件キー

Amazon Route 53 Domains (サービスプレフィックス: `route53domains`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Route 53 Domains によって定義されるアクション
- Amazon Route 53 Domains によって定義されるリソースタイプ
- Amazon Route 53 Domains の条件キー

Amazon Route 53 Domains によって定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptDomainTransferFromAnotherAwsAccount	別の から現在の AWS アカウント へのドメインの移管を受け入れるアクセス許可を付与します AWS アカウント	書き込み			
AssociateDelegationSignerToDomain	ドメインに新しい委任署名者を関連付けるアクセス許可を付与	書き込み			
CancelDomainTransferToAnotherAwsAccount	現在の から別の へのドメインの移管をキャンセル AWS アカウント するアクセス許可を付与します AWS アカウント	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CheckDomainAvailability	1 つのドメイン名が使用可能かどうかを確認する許可を付与。	Read			
CheckDomainTransferability	ドメイン名を Amazon Route 53 に移行できるかどうかを確認する許可を付与	読み取り			
DeleteDomain	ドメインを削除する許可を付与	書き込み			
DeleteTagsForDomain	ドメインの指定されたタグを削除する許可を付与。	タグ付け			
DisableDomainAutoRenew	ドメイン登録の有効期限が切れる前に、指定したドメインを自動的に更新するように Amazon Route 53 を設定する許可を付与。	Write			
DisableDomainTransferLock	ドメインの転送ロック (特に clientTransferProhibited ステータス) を削除してドメイン転送を許可する許可を付与。	書き込み			
DisassociateDelegationSignerFromDomain	ドメインから、既存の委任署名者の関連付けを解除するアクセス許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
EnableDomainAutoRenew	ドメイン登録の有効期限が切れる前に、指定したドメインを自動的に更新するように Amazon Route 53 を設定する許可を付与。	Write			
EnableDomainTransferLock	ドメイン転送を阻止するようにドメインの転送ロック (特に clientTransferProhibited ステータス) を設定する許可を付与。	書き込み			
GetContactReachabilityStatus	新しいドメインの登録など、登録者の連絡先の E メールアドレスが有効であることの確認が必要なオペレーションの場合は、登録者の連絡先が応答したかどうかに関する情報を取得する許可を付与。	読み取り			
GetDomainDetail	ドメインに関する詳細情報を取得する許可を付与。	Read			
GetDomainSuggestions	文字列を指定して、提案されたドメイン名のリストを取得する許可を付与。文字列は、ドメイン名でも、単に単語またはフレーズ (スペースなし) でも構いません。	Read			
GetOperationDetail	完了していないオペレーションの現在のステータスを取得する許可を付与。	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListDomains	現在の の Amazon Route 53 に登録されているすべてのドメイン名を一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListOperations	まだ完了していないオペレーションのオペレーション ID を一覧表示する許可を付与。	リスト			
ListPrices	TLD に対するオペレーションの料金を一覧表示する許可を付与	リスト			
ListTagsForDomain	指定したドメインに関連付けられているすべてのタグを一覧表示する許可を付与。	読み取り			
PushDomain	.uk ドメインの IPS タグを変更して Route 53 から別のレジストラへの移管プロセスを開始するアクセス許可を付与	書き込み			
RegisterDomain	ドメインを登録する許可を付与。	書き込み			
RejectDomainTransferFromAnotherAwsAccount	別の から現在の へのドメインの移管を拒否 AWS アカウント するアクセス許可を付与します AWS アカウント	書き込み			
RenewDomain	指定した年数の期間中にドメインを更新する許可を付与。	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ResendContactReachabilityEmail	新しいドメインの登録など、登録者の連絡先の E メールアドレスが有効であることの確認が必要なオペレーションの場合は、登録者の連絡先の現在の E メールアドレスに確認メールを再送信する許可を付与	書き込み			
ResendOperationAuthorization	操作権限を再送信するアクセス許可を付与	書き込み			
RetrieveDomainAuthCode	ドメインの AuthCode を取得する許可を付与。	Write			
TransferDomain	別の登録者から Amazon Route 53 にドメインを移行する許可を付与。	書き込み			
TransferDomainToAnotherAwsAccount	現在の から別の にドメインを移管 AWS アカウント するアクセス許可を付与します AWS アカウント	書き込み			
UpdateDomainContact	ドメインの連絡先情報を更新する許可を付与。	Write			
UpdateDomainContactPrivacy	ドメイン連絡先のプライバシー設定を更新する許可を付与。	Write			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateDomainNameservers	ドメインの現在のネームサーバーのセットを、指定したネームサーバーのセットに置き換えるアクセス許可を付与	Write			
UpdateTagsForDomain	指定したドメインのタグを追加または更新する許可を付与。	Tagging			
ViewBilling	AWS アカウント 指定された期間における現在の のすべてのドメイン関連の請求レコードを取得するアクセス許可を付与します	読み取り			

Amazon Route 53 Domains によって定義されるリソースタイプ

Amazon Route 53 Domains では、IAM ポリシーステートメントの `Resource` 要素でのリソース ARN の指定はサポートされていません。Amazon Route 53 Domains へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

Amazon Route 53 Domains の条件キー

Route 53 Domains には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS「グローバル条件コンテキストキー」を参照してください。

Amazon Route 53 プロファイルのアクション、リソース、および条件キー

Amazon Route 53 プロファイル (サービスプレフィックス: `route53profiles`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Route 53 プロファイルで定義されるアクション
- Amazon Route 53 プロファイルで定義されるリソースタイプ
- Amazon Route 53 プロファイルの条件キー

Amazon Route 53 プロファイルで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateProfile	プロファイルをカスタマー VPC に関連付ける許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeVpcs
AssociateResourceToProfile	DNS Firewall ルールグループ、プライベートホストゾーン、リゾルバールールなどのリソースを指定されたプロファイルに関連付ける許可を付与する	書き込み			
CreateProfile	新しいプロファイルリソースを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteProfile	ProfileId で指定されたプロファイルを削除する許可を付与する	書き込み			
DisassociateProfile	カスタマー VPC と指定されたプロファイル間の関連付けを削除する許可を付与する	書き込み			
DisassociateResourceFromProfile	DNS Firewall ルールグループ、プライベートホストゾーン、リゾルバールールなど、リソースと指定されたプロファイル間の関連付けを削除する許可を付与する	書き込み			
GetProfile	プロファイルを取得する許可を付与する	読み取り			
GetProfileAssociation	プロファイル関連付け ID で指定された VPC 関連付けにプロファイルを取得する許可を付与する	読み取り			
GetProfilePolicy [許可のみ]	プロファイルの RAM アクセス制御ポリシーを読み取る許可を付与する	読み取り	profile*		
GetProfileResourceAssociation	ProfileResourceAssociationId に基づいて Profile リソースの関連付けを取得する許可を付与する	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListProfileAssociations	指定されたプロファイルが関連付けられているすべてのVPC を一覧表示する許可を付与する	リスト			
ListProfileResourceAssociations	特定のプロファイル ID の DNS Firewall ルールグループ、プライベートホストゾーン、リゾルバールールなど、リソース間のすべての関連付けを一覧表示する許可を付与する	リスト			
ListProfiles	顧客が作成し共有したすべてのプロフィールを一覧表示する許可を付与する	リスト			
ListTagsForResource	リソースに関連付けられたすべてのタグを一覧表示する許可を付与する	リスト			
PutProfilePolicy [許可のみ]	プロファイルの RAM アクセス制御ポリシーを定義する許可を付与する	書き込み	profile*		
TagResource	指定されたリソースにタグを追加する許可を付与する	Tagging	profile		
			profile-association		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	指定されたリソースからタグを削除する許可を付与する	Tagging	profile		
			profile-association		
				aws:TagKeys	
UpdateProfileResourceAssociation	プロファイルリソースの関連付け名、リソースプロパティ、またはその両方を更新する許可を付与し、名前とリソースプロパティの両方が null の場合には、API は既存のプロファイルリソースの関連付けを返す	書き込み			

Amazon Route 53 プロファイルで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
profile	arn:${Partition}:route53profiles:${Region}:${Account}:profile/${ResourceId}	aws:ResourceTag/${TagKey}
profile-association	arn:${Partition}:route53profiles:${Region}:${Account}:profile-association/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon Route 53 プロファイルの条件キー

Amazon Route 53 プロファイルでは、IAM ポリシーの Condition 要素で使用できる以下の条件キーが定義されます。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアによってアクセスをフィルタリングする	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

Amazon Route 53 Recovery クラスターのアクション、リソース、および条件キー

Amazon Route 53 Recovery クラスター (サービスプレフィックス: `route53-recovery-cluster`) では、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されており、IAM 許可ポリシーでの使用が可能です。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Route 53 Recovery クラスターで定義されるアクション
- Amazon Route 53 Recovery クラスターで定義されるリソースタイプ
- Amazon Route 53 Recovery クラスターの条件キー

Amazon Route 53 Recovery クラスターで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイ

プが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetRoutingControlState	ルーティングの制御状態を取得するためのアクセス許可を付与する	読み込み	routingcontrol*		
ListRoutingControls	ルーティング制御を一覧表示するためのアクセス許可を付与	読み込み			
UpdateRoutingControlState	ルーティングの制御状態を更新するためのアクセス許可を付与する	書き込み	routingcontrol*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				route53-recovery-cluster:AllowSafetyRulesOverrides	
UpdateRoutingControlStates	一連のルーティングの制御状態を更新するためのアクセス許可を付与する	書き込み	routingcontrol*		
				route53-recovery-cluster:AllowSafetyRulesOverrides	

Amazon Route 53 Recovery クラスターで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
routingcontrol	arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}/routingcontrol/${RoutingControlId}	

Amazon Route 53 Recovery クラスターの条件キー

Amazon Route 53 Recovery Cluster では、以下の条件キーを定義しており、IAM ポリシーの Condition 要素での使用が可能です。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
route53-recovery-cluster:AllowSafetyRulesOverrides	安全ルールを上書きして、ルーティング制御状態の更新を許可する	Bool

Amazon Route 53 Recovery コントロールのアクション、リソース、および条件キー

Amazon Route 53 Recovery コントロール (サービスプレフィックス: route53-recovery-control-config) では、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されており、IAM 許可ポリシーでの使用が可能です。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Route 53 Recovery コントロールで定義されるアクション
- Amazon Route 53 Recovery コントロールで定義されるリソースタイプ
- Amazon Route 53 Recovery コントロールの条件キー

Amazon Route 53 Recovery コントロールで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateCluster	クラスターを作成する許可を付与	書き込み	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateControlPanel	コントロールパネルを作成するためのアクセス許可を付与	書き込み	controlpanel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRoutingControl	ルーティング制御を作成するためのアクセス許可を付与	書き込み	routingcontrol*		
CreateSafetyRule	安全ルールを作成するためのアクセス許可を付与	書き込み	safetyrule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCluster	クラスターを削除するためのアクセス許可を付与	書き込み	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteControlPanel	コントロールパネルを削除するためのアクセス許可を付与	書き込み	controlpanel*		
DeleteResourcePolicy [アクセス許可のみ]	クラスターの RAM アクセスコントロールポリシーを削除するアクセス許可を付与します	書き込み	cluster*		
DeleteRoutingControl	ルーティング制御を削除するためのアクセス許可を付与	Write	routingcontrol*		
DeleteSafetyRule	安全ルールを削除するためのアクセス許可を付与	Write	safetyrule*		
DescribeCluster	クラスターを詳細表示するためのアクセス許可を付与	Read	cluster*		
DescribeControlPanel	コントロールパネルについて詳細表示するためのアクセス許可を付与	Read	controlpanel*		
DescribeRoutingControl	ルーティング制御を詳細表示するためのアクセス許可を付与	Read	routingcontrol*		
DescribeRoutingControlByName	ルーティング制御を詳細表示するためのアクセス許可を付与	Read	routingcontrol*		
DescribeSafetyRule	安全ルールを詳細表示するためのアクセス許可を付与	読み取り	safetyrule*		
GetResourcePolicy	クラスターのリソースポリシーを更新するアクセス許可を付与	読み取り	cluster*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListAssociatedRoute53HealthChecks	関連付けられた Route 53 ヘルスチェックを一覧表示するためのアクセス許可を付与	リスト			
ListClusters	クラスターを一覧表示するためのアクセス許可を付与	読み取り			
ListControlPanels	コントロールパネルを一覧表示するためのアクセス許可を付与	Read			
ListRoutingControls	ルーティング制御を一覧表示するためのアクセス許可を付与	読み取り			
ListSafetyRules	安全ルールを一覧表示するためのアクセス許可を付与	読み取り	controlpanel*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み込み			
PutResourcePolicy [許可のみ]	クラスターの RAM アクセスコントロールポリシーを定義するアクセス許可を付与します	書き込み	cluster*		
TagResource	リソースにタグを付けるアクセス許可を付与	Tagging	cluster		
			controlpanel		
			safetyrule		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	リソースからタグを削除する許可を付与	Tagging	cluster		
			controlpanel		
			safetyrule		
				aws:TagKeys	
UpdateCluster	クラスターを更新するためのアクセス許可を付与	書き込み	cluster*		
UpdateControlPanel	クラスターを更新するためのアクセス許可を付与	書き込み	controlpanel*		
UpdateRoutingControl	ルーティング制御を更新するためのアクセス許可を付与	書き込み	routingcontrol*		
UpdateSafetyRule	安全ルールを更新するためのアクセス許可を付与	書き込み	safetyrule*		

Amazon Route 53 Recovery コントロールで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
cluster	arn:${Partition}:route53-recovery-control::${Account}:cluster/${ResourceId}	aws:ResourceTag/${TagKey}
controlpanel	arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}	aws:ResourceTag/${TagKey}
routingcontrol	arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}/routingcontrol/${RoutingControlId}	
safetyrule	arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}/safetyrule/${SafetyRuleId}	aws:ResourceTag/${TagKey}

Amazon Route 53 Recovery コントロールの条件キー

Amazon Route 53 Recovery Controls では、以下の条件キーを定義しており、IAM ポリシーの Condition 要素での使用が可能です。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグのキーと値でアクセスをフィルター	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

Amazon Route 53 Recovery Readiness のアクション、リソース、および条件キー

Amazon Route 53 Recovery Readiness (サービスプレフィックス: `route53-recovery-readiness`) では、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されており、IAM 許可ポリシーでの使用が可能です。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Route 53 Recovery Readiness で定義されるアクション
- Amazon Route 53 Recovery Readiness で定義されるリソースタイプ
- Amazon Route 53 Recovery Readiness の条件キー

Amazon Route 53 Recovery Readiness で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateCell	新しいセルを作成するためのアクセス許可を付与	書き込み	cell*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCrossAccountAuthorization	クロスアカウント認可を作成するためのアクセス許可を付与	書き込み			
CreateReadinessCheck	準備状況チェックを作成するためのアクセス許可を付与	書き込み	readinesscheck*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRecoveryGroup	リカバリグループを作成するためのアクセス許可を付与	書き込み	recoverygroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResourceSet	リソースセットを作成するためのアクセス許可を付与	書き込み	resourceset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCell	セルを削除するためのアクセス許可を付与	書き込み	cell*		
DeleteCrossAccountAuthorization	クロスアカウント認可を削除するためのアクセス許可を付与	書き込み			
DeleteReadinessCheck	準備状況チェックを削除するためのアクセス許可を付与	書き込み	readinesscheck*		
DeleteRecoveryGroup	リカバリグループを削除するためのアクセス許可を付与	書き込み	recoverygroup*		
DeleteResourceSet	リソースセットを削除するためのアクセス許可を付与	書き込み	resourceset*		
GetArchitectureRecommendations	リカバリグループのアーキテクチャに関する推奨事項を取得するためのアクセス許可を付与	読み取り	recoverygroup*		
GetCell	セルに関する情報を取得するためのアクセス許可を付与	読み取り	cell*		
GetCellReadinessSummary	セルの準備状況の概要を取得するためのアクセス許可を付与	読み取り	cell*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetReadinessCheck	準備状況チェックに関する情報を取得するためのアクセス許可を付与	読み取り	readinesscheck*		
GetReadinessCheckResourceStatus	個別リソースについて準備状況を取得するためのアクセス許可を付与	読み取り	readinesscheck*		
GetReadinessCheckStatus	準備状況チェックのステータスを取得するためのアクセス許可を付与 (リソースセット用)	読み取り	readinesscheck*		
GetRecoveryGroup	リカバリグループに関する情報を取得するためのアクセス許可を付与	読み取り	recoverygroup*		
GetRecoveryGroupReadinessSummary	リカバリグループの準備状況の概要を取得するためのアクセス許可を付与	読み取り	recoverygroup*		
GetResourceSet	リソースセットに関する情報を取得するためのアクセス許可を付与	読み取り	resourceset*		
ListCells	セルを一覧表示するためのアクセス許可を付与	読み取り			
ListCrossAccountAuthorizations	クロスアカウント認証を一覧表示するためのアクセス許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListReadinessChecks	準備状況チェックを一覧表示するためのアクセス許可を付与	読み取り			
ListRecoveryGroups	リカバリグループを一覧表示するためのアクセス許可を付与	読み取り			
ListResourceSets	リソースセットを一覧表示するためのアクセス許可を付与	読み取り			
ListRules	準備状況ルールを一覧表示するためのアクセス許可を付与	Read			
ListTagsForResources	リソースのタグを一覧表示する許可を付与	Read			
TagResource	リソースにタグを追加する許可を付与	タグ付け	cell		
			readinesscheck		
			recoverygroup		
			resourceset		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	リソースからタグを削除する許可を付与	Tagging	cell		
			readinesscheck		
			recoverygroup		
			resourceset		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateCell	セルを更新するためのアクセス許可を付与	書き込み	cell*		
				aws:TagKeys	
UpdateReadinessCheck	準備状況チェックを更新するためのアクセス許可を付与	書き込み	readinesscheck*		
				aws:TagKeys	
UpdateRecoveryGroup	リカバリグループを更新するためのアクセス許可を付与	書き込み	recoverygroup*		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateResourceSet	リソースセットを更新するためのアクセス許可を付与	書き込み	resourceset*		
				aws:TagKeys	

Amazon Route 53 Recovery Readiness で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
readinesscheck	arn:${Partition}:route53-recovery-readiness::${Account}:readiness-check/${ResourceId}	aws:ResourceTag/${TagKey}
resourceset	arn:${Partition}:route53-recovery-readiness::${Account}:resource-set/${ResourceId}	aws:ResourceTag/${TagKey}
cell	arn:${Partition}:route53-recovery-readiness::${Account}:cell/${ResourceId}	aws:ResourceTag/${TagKey}
recoverygroup	arn:${Partition}:route53-recovery-readiness::${Account}:recovery-group/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon Route 53 Recovery Readiness の条件キー

Amazon Route 53 Recovery Readiness では、以下の条件キーを定義しており、IAM ポリシーの Condition 要素での使用が可能です。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon Route 53 Resolver のアクション、リソース、および条件キー

Amazon Route 53 Resolver (サービスプレフィックス: route53resolver) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Route 53 Resolver で定義されるリソース

- Amazon Route 53 Resolver で定義されるリソースタイプ
- Amazon Route 53 Resolver の条件キー

Amazon Route 53 Resolver で定義されるリソース

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateFirewallRuleGroup	Amazon VPC を指定されたファイアウォールのルールグループに関連付けるアクセス許可を付与します。	Write	firewall-rule-group-association*		ec2:DescribeVpcs
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateResolverEndpointIpAddress	指定した IP アドレスを Resolver エンドポイントに関連付けるアクセス許可を付与します。これは、DNS クエリがネットワーク (アウトバウンド) または VPC (インバウンド) に到達するまでに経由する IP アドレスです。	Write	resolver-endpoint*		ec2:CreateNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets
AssociateResolverQ	指定されたクエリログ設定に Amazon VPC を関連付けるアクセス許可を付与します	Write	resolver-query-log-config*		ec2:DescribeVpcs

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ueryLogConfig					
AssociateResolverRule	指定した Resolver ルールを、指定した VPC に関連付けるアクセス許可を付与します	Write	resolver-rule*		ec2:DescribeVpcs
CreateFirewallDomainList	ファイアウォールのドメインリストを作成するためのアクセス許可を付与します	Write	firewall-domain-list*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallRule	ファイアウォールルールグループ内にファイアウォールルールを作成するためのアクセス許可を付与します	Write	firewall-domain-list*		
			firewall-rule-group*		
CreateFirewallRuleGroup	ファイアウォールルールグループを作成するためのアクセス許可を付与します	書き込み	firewall-rule-group*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOutpostResolver	Route 53 Resolver on Outposts を作成するための許可を付与します	書き込み	outpost-resolver*		outposts:GetOutpost
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateResolverEndpoint	Resolver エンドポイントを作成する許可を付与。Resolver エンドポイントには、インバウンドとアウトバウンドの 2 つのタイプがあります	Write	resolver-endpoint*		ec2:CreateNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResolverQueryLogConfig	Resolver クエリログ設定を作成する許可を付与。これは、Resolver が VPC から生成される DNS クエリログを保存する場所を定義します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateResolverRule	VPC で作成された DNS クエリについて、VPC からクエリをルーティングする方法を定義する許可を付与	書き込み	resolver-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFirewallDomainList	ファイアウォールのドメインリストを削除するためのアクセス許可を付与します	Write	firewall-domain-list*		
DeleteFirewallRule	ファイアウォールルールグループ内のファイアウォールルールを削除するためのアクセス許可を付与します	Write	firewall-domain-list*		
			firewall-rule-group*		
DeleteFirewallRuleGroup	ファイアウォールルールグループを削除するためのアクセス許可を付与します	書き込み	firewall-rule-group*		
DeleteOutpostResolver	Route 53 Resolver on Outposts を削除するための許可を付与します	書き込み	outpost-resolver*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteResolverEndpoint	Resolver エンドポイントを削除する許可を付与。Resolver エンドポイントを削除する効果は、エンドポイントがインバウンドであるかアウトバウンドであるかによって異なります	Write	resolver-endpoint*		ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces
DeleteResolverQueryLogConfig	Resolver クエリログ設定を削除する許可を付与	Write	resolver-query-log-config*		
DeleteResolverRule	Resolver ルールを削除する許可を付与	Write	resolver-rule*		
DisassociateFirewallRuleGroup	指定したファイアウォールのルールグループと指定した VPC の関連付けを削除する許可を付与。	Write	firewall-rule-group-association*		
DisassociateResolverEndpointIpAddress	指定した IP アドレスを Resolver エンドポイントから削除する許可を付与。これは、DNS クエリがネットワーク (アウトバウンド) または VPC (インバウンド) に到達するまでに経由する IP アドレスです。	Write	resolver-endpoint*		ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces
DisassociateResolverQueryLogConfig	指定した Resolver クエリログ設定と指定した VPC との関連付けを削除する許可を付与	Write	resolver-query-log-config*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisassociateResolverRule	指定した Resolver ルールと指定した VPC の関連付けを削除する許可を付与	Write	resolver-rule*		
GetFirewallConfig	指定されたファイアウォール設定に関する情報を取得するためのアクセス許可を付与します	Read	firewall-config*		ec2:DescribeVpcs
GetFirewallDomainList	指定されたファイアウォールドメインリストに関する情報を取得するためのアクセス許可を付与します	Read	firewall-domain-list*		
GetFirewallRuleGroup	指定したファイアウォールルールグループに関する情報を取得するためのアクセス許可を付与します	Read	firewall-rule-group*		
GetFirewallRuleGroupAssociation	指定したファイアウォールのルールグループと VPC の間の関連付けに関する情報を取得する許可を付与。	読み取り	firewall-rule-group-association*		
GetFirewallRuleGroupPolicy	別のユーザーに使用を許可するファイアウォールルールグループのオペレーションとリソースを指定する、指定されたファイアウォールルールグループポリシーに関する情報を取得するアクセス許可を付与 AWS アカウント します	読み取り	firewall-rule-group*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetOutpostResolver	指定された Route 53 Resolver on Outposts に関する情報を取得するための許可を付与します	読み取り	outpost-resolver*		
GetResolverConfig	指定されたリソース内の Resolver Config ステータスを取得するアクセス許可を付与します	読み取り	resolver-config*		ec2:DescribeVpcs
GetResolverDnssecConfig	指定されたリソース内の DNS クエリの DNSSEC 検証サポートステータスを取得する権利を付与します。	Read	resolver-dnssec-config*		
GetResolverEndpoint	指定した Resolver エンドポイントに関する情報 (エンドポイントがインバウンドであるかアウトバウンドであるか、および DNS クエリが VPC への送受信の過程で転送される VPC 内の IP アドレスなど) を取得するためのアクセス許可を付与します	Read	resolver-endpoint*		
GetResolverQueryLogConfig	指定した Resolver クエリの口グ設定に関する情報を取得するためのアクセス許可を付与します (設定がクエリを口グに記録している VPC の数や、口グの送信先など)	Read	resolver-query-log-config*		ec2:DescribeVpcs

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetResolverQueryLogConfigAssociation	Resolver クエリのログ設定と Amazon VPC の間の、指定された関連付けに関する情報を取得する許可を付与。VPC をクエリのログ設定に関連付けると、Resolver はその VPC で生成された DNS クエリをログに記録します	読み取り			
GetResolverQueryLogConfigPolicy	指定された Resolver クエリログ記録ポリシーに関する情報を取得するアクセス許可を付与します。このポリシーは、別のユーザーに AWS アカウント 使用を許可する Resolver クエリログ記録オペレーションとリソースを指定します。	読み取り	resolver-query-log-config*		
GetResolverRule	指定した Resolver ルールに関する情報 (ルールが DNS クエリを転送するドメイン名、クエリの転送先 IP アドレスなど) を取得するためのアクセス許可を付与します	Read	autodefined-rule		
			resolver-rule		
GetResolverRuleAssociation	指定した Resolver ルールと VPC の間の関連付けに関する情報を取得する許可を付与	読み取り	autodefined-rule		
			resolver-rule		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetResolverRulePolicy	Resolver ルールポリシーに関する情報を取得するアクセス許可を付与します。このポリシーは、別のユーザーに AWS アカウント 使用を許可する Resolver オペレーションとリソースを指定します。	読み取り	resolver-rule*		
ImportFirewallDomains	ファイアウォールドメインの一覧にファイアウォールドメインを追加、削除、または置換するためのアクセス許可を付与します	書き込み	firewall-domain-list*		
ListFirewallConfigs	現在の AWS アカウント がチェックできるすべてのファイアウォール設定を一覧表示するアクセス許可を付与します	リスト			ec2:DescribeVpcs
ListFirewallDomainLists	現在使用できるすべての Firewall AWS アカウント ドメインリストを一覧表示するアクセス許可を付与します	リスト			
ListFirewallDomains	指定された Firewall ドメインリストのすべての Firewall ドメインを一覧表示するアクセス許可を付与します	リスト	firewall-domain-list*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListFirewallRuleGroupAssociations	Amazon VPC とファイアウォールルールグループ間の関連付けに関する情報を一覧表示するためのアクセス許可を付与します	リスト			
ListFirewallRuleGroups	現在使用できるすべてのファイアウォールルールグループを一覧表示 AWS アカウントするアクセス許可を付与します	リスト			
ListFirewallRules	指定されたファイアウォールルールグループのすべてのファイアウォールルールを一覧表示するアクセス許可を付与します	リスト	firewall-rule-group*		
ListOutpostResolvers	現在の を使用して作成された Route 53 Resolver on Outposts のすべてのインスタンスを一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListResolverConfigs	リゾルバConfig ステータスを一覧表示するアクセス許可を付与します	リスト	resolver-config*		ec2:DescribeVpcs
ListResolverDnssecConfigs	DNS クエリの DNSSEC 検証サポートステータスを一覧表示する許可を付与。	リスト	resolver-dnssec-config*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListResolverEndpointIpAddresses	指定した Resolver エンドポイントについて、DNS クエリがネットワーク (アウトバウンド) または VPC (インバウンド) に到達するまでに経由する IP アドレスを一覧表示する許可を付与	リスト	resolver-endpoint*		
ListResolverEndpoints	現在の を使用して作成されたすべての Resolver エンドポイントを一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListResolverQueryLogConfigAssociations	Amazon VPC とクエリログ設定の間の関連付けに関する情報を一覧表示する許可を付与	リスト			ec2:DescribeVpcs
ListResolverQueryLogConfigs	指定したクエリログ設定に関する情報を一覧表示する許可を付与。この設定は、Resolver が DNS クエリログを保存する場所を定義し、クエリを口グに記録する VPC を指定します	リスト			ec2:DescribeVpcs
ListResolverRuleAssociations	現在の を使用してリゾルバールールと VPCs の間で作成された関連付けを一覧表示するアクセス許可を付与します AWS アカウント	リスト			ec2:DescribeVpcs

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListResolverRules	現在の を使用して作成されたリゾルバールールを一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListTagsForResource	指定したリソースに関連付けたタグを一覧表示する許可を付与	読み取り	firewall-domain-list		
			firewall-rule-group		
			firewall-rule-group-association		
			outpost-resolver		
			resolver-endpoint		
			resolver-query-log-config		
			resolver-rule		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutFirewallRuleGroupPolicy	Firewall ルールグループ AWS アカウント を共有する 、共有する Firewall ルールグループ、およびアカウントが設定で実行できるオペレーションを指定するアクセス許可を付与します	権限の管理	firewall-rule-group*		
PutResolverQueryLogConfigPolicy	クエリログ記録設定 AWS アカウント を共有する 、共有するクエリログ記録設定、およびアカウントが設定で実行できるようにするオペレーションを指定するアクセス許可を付与します	権限の管理	resolver-query-log-config*		
PutResolverRulePolicy	ルール AWS アカウント を共有する 、共有するリゾルバールール、およびアカウントがそれらのルールに対して実行できるようにするオペレーションを指定するアクセス許可を付与します	権限の管理	resolver-rule*		
TagResource	指定したリソースに 1 つ以上のタグを追加する許可を付与	タグ付け	firewall-config		
			firewall-domain-list		
			firewall-rule-group		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			firewall-rule-group-association		
			outpost-resolver		
			resolver-dnssec-config		
			resolver-endpoint		
			resolver-query-log-config		
			resolver-rule		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	指定したリソースから 1 つ以上のタグを削除する許可を付与	タグ付け	firewall-config		
			firewall-domain-list		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			firewall-rule-group		
			firewall-rule-group-association		
			outpost-resolver		
			resolver-dnssec-config		
			resolver-endpoint		
			resolver-query-log-config		
			resolver-rule		
				aws:TagKeys	
UpdateFirewallConfig	ファイアウォール設定の選択した設定を更新するためのアクセス許可を付与します	Write	firewall-config*		ec2:DescribeVpcs

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateFirewallDomains	ファイアウォールドメインの一覧にファイアウォールドメインを追加、削除、または置換するためのアクセス許可を付与します	Write	firewall-domain-list*		
UpdateFirewallRule	ファイアウォールルールグループのファイアウォールルールについて選択した設定を更新するためのアクセス許可を付与します	Write	firewall-domain-list* firewall-rule-group*		
UpdateFirewallRuleGroupAssociation	ファイアウォールルールグループの関連付けについて選択した設定を更新するためのアクセス許可を付与します	書き込み	firewall-rule-group-association*		
UpdateOutpostResolver	指定された Route 53 Resolver on Outposts 用に選択された設定を更新するための許可を付与します	書き込み	outpost-resolver*		
UpdateResolverConfig	指定されたリソース内の Resolver Config ステータスを更新するアクセス許可を付与します	書き込み	resolver-config*		ec2:DescribeVpcs
UpdateResolverDnssecConfig	指定されたリソース内の DNS クエリの DNSSEC 検証サポートステータスを更新する権利を付与します。	Write	resolver-dnssec-config*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateResolverEndpoint	インバウンドまたはアウトバウンドの Resolver エンドポイントの選択した設定を更新する許可を付与	Write	resolver-endpoint*		ec2:AssignIpv6Addresses ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:ModifyNetworkInterfaceAttribute ec2:UnassignIpv6Addresses
UpdateResolverRule	指定した Resolver ルールの設定を更新する許可を付与	Write	resolver-rule*		

Amazon Route 53 Resolver で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
resolver-dnssec-config	arn:${Partition}:route53resolver:${Region}:${Account}:resolver-dnssec-config/${ResourceId}	aws:ResourceTag/${TagKey}
resolver-query-log-config	arn:${Partition}:route53resolver:${Region}:${Account}:resolver-query-log-config/${ResourceId}	aws:ResourceTag/${TagKey}
resolver-rule	arn:${Partition}:route53resolver:${Region}:${Account}:resolver-rule/${ResourceId}	aws:ResourceTag/${TagKey}
autodefined-rule	arn:${Partition}:route53resolver:${Region}:${Account}:autodefined-rule/${ResourceId}	aws:ResourceTag/${TagKey}
resolver-endpoint	arn:${Partition}:route53resolver:${Region}:${Account}:resolver-endpoint/${ResourceId}	aws:ResourceTag/${TagKey}
firewall-rule-group	arn:${Partition}:route53resolver:${Region}:${Account}:firewall-rule-group/${ResourceId}	aws:ResourceTag/${TagKey}
firewall-rule-group-association	arn:${Partition}:route53resolver:${Region}:${Account}:firewall-rule-group-association/${ResourceId}	aws:ResourceTag/${TagKey}
firewall-domain-list	arn:${Partition}:route53resolver:${Region}:${Account}:firewall-domain-list/${ResourceId}	aws:ResourceTag/${TagKey}
firewall-config	arn:${Partition}:route53resolver:${Region}:${Account}:firewall-config/${ResourceId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
resolver-config	arn:${Partition}:route53resolver:${Region}:${Account}:resolver-config/${ResourceId}	
outpost-resolver	arn:${Partition}:route53resolver:${Region}:${Account}:outpost-resolver/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon Route 53 Resolver の条件キー

Amazon Route 53 Resolver は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアによってアクセスをフィルタリングする	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

Amazon S3 Express のアクション、リソース、および条件キー

Amazon S3 Express (サービスプレフィックス: s3express) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon S3 Express で定義されるアクション
- Amazon S3 Express で定義されるリソースタイプ
- Amazon S3 Express の条件キー

Amazon S3 Express で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateAccessPoint	新しいアクセスポイントを作成するアクセス許可を付与します	Write	accesspoint*		
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3express:authType s3express:LocationName s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 aws:RequestTag/${TagKey} aws:TagKeys	
CreateBucket	新しいバケットを作成するアクセス許可を付与します	書き込み	bucket*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3express:authType s3express:LocationName s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSession	PutObject、GetObject などのオブジェクト APIs に使用されるセッショントークンを作成するアクセス許可を付与します	書き込み	bucket*		
			accesspoint	s3express:Permissions	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3express:authType s3express:ResourceAccount s3express:SessionMode s3express:signatureAge s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 s3express:x-amz-server-side-encryption	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3express:x-amz-server-side-encryption-aws-kms-key-id s3express:AllAccessRestrictedToLocalZoneGroup s3express:Permissions	
DeleteAccessPoint	URI で指定されたアクセスポイントを削除するアクセス許可を付与します	Write	accesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteAccessPointPolicy	指定したアクセスポイントでポリシーを削除するアクセス許可を付与します	権限の管理	accesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteAccessPointScope	指定されたアクセスポイントのスコープ設定を削除するアクセス許可を付与します	権限の管理	accesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteBucket	URI で指定されたバケットを削除するアクセス許可を付与します	Write	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
DeleteBucketPolicy	指定したバケットのポリシーを削除するアクセス許可を付与	権限の管理	bucket*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
GetAccessPoint	指定したアクセスポイントに関する設定情報を返すアクセス許可を付与します	読み取り	accesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetAccessPointPolicy	指定されたアクセスポイントに関連付けられたアクセスポイントポリシーを返すアクセス許可を付与します	読み取り	accesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetAccessPointScope	指定されたアクセスポイントに関連付けられたスコープ設定を返すアクセス許可を付与します	読み取り	accesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetBucketPolicy	指定したバケットのポリシーを返すアクセス許可を付与します	読み取り	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
GetEncryptionConfiguration	ディレクトリバケットにデフォルトの暗号化設定を返す許可を付与する	読み取り	bucket*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetLifecycleConfiguration	ディレクトリバケットに設定されたライフサイクル設定情報を返すアクセス許可を付与します	読み取り	bucket*	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListAccessPointsForDirectoryBuckets	アクセスポイントを一覧表示する許可を付与	リスト		s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListAllMyDirectoryBuckets	リクエストの認証された送信者が所有するすべてのディレクトリバケットを一覧表示するためのアクセス許可を付与	リスト		s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
ListTagsForResource	指定されたリソースのすべてのタグを一覧表示するアクセス許可を付与します	リスト	accesspoint		
			bucket		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
PutAccessPointPolicy	アクセスポリシーを指定されたアクセスポイントに関連付けるアクセス許可を付与します	権限の管理	accesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutAccessPointScope	アクセスポイントを指定されたアクセスポイントスコープ設定に関連付けるアクセス許可を付与します	権限の管理	accesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutBucketPolicy	バケットのバケットポリシーを追加または置き換えるアクセス許可を付与します	権限の管理	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
PutEncryptionConfiguration	ディレクトリバケットの暗号化設定を設定するアクセス許可を付与します	書き込み	bucket*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutLifecycleConfiguration	ディレクトリバケットの新しいライフサイクル設定を作成するか、既存のライフサイクル設定を置き換えるアクセス許可を付与します	書き込み	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
TagResource	新しいユーザー定義タグを作成したり、既存のタグを更新したりするアクセス許可を付与します	Tagging	accesspoint		
			bucket		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	S3 リソースから指定されたユーザー定義タグを削除するアクセス許可を付与します	Tagging	accesspoint		
			bucket		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 aws:TagKeys	

Amazon S3 Express で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
bucket	arn:${Partition}:s3express:${Region}:${Account}:bucket/${BucketName}	aws:ResourceTag/${TagKey} s3express:BucketTag/${TagKey}
accesspoint	arn:${Partition}:s3express:${Region}:${Account}:accesspoint/${AccessPointName}	aws:ResourceTag/${TagKey} s3express:AccessPointTag/${TagKey}

Amazon S3 Express の条件キー

Amazon S3 Express は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

条件キー	説明	タイプ
s3express:AccessPointNetworkOrigin	ネットワークオリジン (インターネットまたは VPC) によるアクセスをフィルタリングします	String
s3express:AccessPointTag/${TagKey}	アクセスポイントにアタッチされたタグキーと値のペアでアクセスをフィルタリングします	String
s3express:AllAccessRestrictedToLocalZoneGroup	この条件キーで指定された AWS ローカルゾーンネットワーク境界グループ (複数可) でアクセスをフィルタリングします	String
s3express:BucketTag/${TagKey}	バケットにアタッチされたタグキーと値のペアでアクセスをフィルタリングします	String
s3express:DataAccessPointAccount	アクセスポイントを所有する AWS アカウント ID でアクセスをフィルタリングします	String
s3express:DataAccessPointArn	アクセスポイント Amazon リソースネーム (ARN) でアクセスをフィルタリングします	ARN
s3express:LocationName	特定のアベイラビリティーゾーンまたはローカルゾーン ID でアクセスをフィルタリングします	String
s3express:Permissions	GetObject、PutObject などのアクセスポイントスコープ設定によってリクエストされたアクセス許可でアクセスをフィルタリングします	ArrayOfString
s3express:ResourceAccount	リソース所有者 AWS アカウント ID でアクセスをフィルタリングします	String

条件キー	説明	タイプ
s3express:SessionMode	CreateSession API でリクエストされたアクセス許可 (ReadOnly、ReadWrite など) でアクセスをフィルタリングします	String
s3express:TlsVersion	クライアントが使用する TLS バージョンでアクセスをフィルタリングします	数値
s3express:authType	認証方式でアクセスをフィルタリングします	文字列
s3express:signatureAge	リクエスト署名の経過時間 (ミリ秒単位) でアクセスをフィルタリングします	数値
s3express:signatureversion	リクエストで使用される AWS 署名バージョンでアクセスをフィルタリングします	String
s3express:x-amz-content-sha256	バケット内の署名されていないコンテンツによりアクセスをフィルタリングします	String
s3express:x-amz-server-side-encryption	サーバー側の暗号化でアクセスをフィルタリングします	String
s3express:x-amz-server-side-encryption-aws-kms-key-id	サーバー側の暗号化用に KMS AWS カスタマーマネージドキーでアクセスをフィルタリングします	ARN

Amazon S3 Glacier のアクション、リソース、および条件キー

Amazon S3 Glacier (サービスプレフィックス: `glacier`) では、IAM 許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon S3 Glacier で定義されるアクション
- Amazon S3 Glacier で定義されるリソースタイプ
- Amazon S3 Glacier の条件キー

Amazon S3 Glacier で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AbortMultipartUpload	アップロード ID によって識別されるマルチパートアップロードを中止する許可を付与する	書き込み	vault*		
AbortVaultLock	ボールトロックが Locked 状態でない場合にボールトロック処理を中止する許可を付与する	権限の管理	vault*		
AddTagsToVault	ボールトに指定したタグを追加する許可を付与する	Tagging	vault*		
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CompleteMultipartUpload	マルチパートアップロードプロセスを完了する許可を付与する	書き込み	vault*		
CompleteVaultLock	ボールトロック処理を完了する許可を付与する	権限の管理	vault*		
CreateVault	指定された名前の新しいボールトを作成する許可を付与する	書き込み	vault*		
DeleteArchive	ボールトからアーカイブを削除する許可を付与する	書き込み	vault*		
				glacier:ArchiveAgeInDays	
DeleteVault	ボールトを削除する許可を付与する	書き込み	vault*		
DeleteVaultAccessPolicy	指定されたボールトに関連付けられたアクセスポリシーを削除する許可を付与する	権限の管理	vault*		
DeleteVaultNotifications	ボールトに割り当てられている通知設定を削除する許可を付与する	書き込み	vault*		
DescribeJob	以前に開始されたジョブに関する情報を取得する許可を付与する	読み取り	vault*		
DescribeVault	ボールトに関する情報を取得する許可を付与する	読み取り	vault*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetDataRetrievalPolicy	データ取得ポリシーを取得する許可を付与する	読み取り			
GetJobOutput	指定されたジョブの出力をダウンロードする許可を付与する	読み取り	vault*		
GetVaultAccessPolicy	ボールトのアクセスポリシーのサブリソースセットを取得する許可を付与する	読み取り	vault*		
GetVaultLock	指定されたボールトのロックポリシーのサブリソースセットから属性を取得する許可を付与する	読み取り	vault*		
GetVaultNotifications	ボールトの通知設定のサブリソースセットを取得する許可を付与する	読み取り	vault*		
InitiateJob	指定されたタイプのジョブを開始する許可を付与する	書き込み	vault*		
				glacier:ArchiveAgeInDays	
InitiateMultipartUpload	マルチパートアップロードを開始する許可を付与する	書き込み	vault*		
InitiateVaultLock	ボールトロック処理を開始する許可を付与する	権限の管理	vault*		
ListJobs	進行中のボールトのジョブ、および最近終了したジョブを一覧表示する許可を付与する	リスト	vault*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListMultipartUploads	指定されたボールトに対して進行中のマルチパートアップロードを一覧表示する許可を付与する	リスト	vault*		
ListParts	特定のマルチパートアップロード用にアップロードされた部分を一覧表示する許可を付与する	リスト	vault*		
ListProvisionedCapacity	指定された のプロビジョニングされた容量を一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListTagsForVault	ボールトに添付されているすべてのタグを一覧表示する許可を付与する	リスト	vault*		
ListVaults	すべてのボールトを一覧表示する許可を付与する	リスト			
PurchaseProvisionedCapacity	のプロビジョニングされたキャパシティユニットを購入するアクセス許可を付与します AWS アカウント	書き込み			
RemoveTagsFromVault	ボールトに添付されたタグのセットから 1 つ以上のタグを削除する許可を付与する	Tagging	vault*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SetDataRetrievalPolicy	PUT リクエストで指定されたリージョンのデータ取得ポリシーを設定して有効にする許可を付与する	権限の管理			
SetVaultAccessPolicy	ボールト用のアクセスポリシーを設定し、既存のポリシーを上書きする許可を付与する	権限の管理	vault*		
SetVaultNotifications	ボールト通知を取得する許可を付与する	書き込み	vault*		
UploadArchive	ボールトにアーカイブをアップロードする許可を付与する	書き込み	vault*		
UploadMultipartPart	アーカイブの一部をアップロードする許可を付与する	書き込み	vault*		

Amazon S3 Glacier で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
vault	`arn:${Partition}:glacier:${Region}:${Account}:vaults/${VaultName}`	

Amazon S3 Glacier の条件キー

Amazon S3 Glacier は、以下の条件キーを定義しており、IAM ポリシーの Condition 要素での使用が可能です。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
glacier:ArchiveAgeInDays	アーカイブがボールトに保存されている日数によってアクセスをフィルタリングする	String
glacier:ResourceTag/	お客様定義のタグでアクセスをフィルタリングする	String

Amazon S3 Object Lambda のアクション、リソース、条件キー

Amazon S3 Object Lambda (サービスプレフィックス: s3-object-lambda) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon S3 Object Lambda によって定義されたアクション

- Amazon S3 Object Lambda によって定義されたリソースタイプ
- Amazon S3 Object Lambda の条件キー

Amazon S3 Object Lambda によって定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AbortMultipartUpload	マルチパートアップロードを中止するアクセス許可を付与	Write	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
DeleteObject	オブジェクトの null バージョンを削除し、削除マーカーを挿入する許可を付与。このマーカーは、オブジェクトの現在のバージョンになります	Write	objectlambdaaccesspoint*		
				s3-object-lambda:authType	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
DeleteObjectTagging	タグ付けサブリソースを使用して、指定したオブジェクトからタグセット全体を削除するアクセス許可を付与	タグ付け	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
DeleteObjectVersion	特定のバージョンのオブジェクトを削除するアクセス許可を付与	Write	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
DeleteObjectVersionTagging	オブジェクトの特定のバージョンのタグセット全体を削除するアクセス許可を付与	タグ付け	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObject	Amazon S3 からオブジェクトを取得するためのアクセス許可を付与	Read	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectAcl	オブジェクトのアクセスコントロールリスト (ACL) を返すアクセス許可を付与	Read	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectLegalHold	オブジェクトの現在のリーガルホールドステータスを取得するアクセス許可を付与	Read	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectRetention	オブジェクトの保存設定を取得するアクセス許可を付与	Read	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectTagging	オブジェクトのタグセットを返すアクセス許可を付与	Read	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectVersion	特定のバージョンのオブジェクトを取得するためのアクセス許可を付与	Read	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObjectVersionAcl	特定のオブジェクトバージョンのアクセスコントロールリスト (ACL) を返すアクセス許可を付与	Read	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObjectVersionTagging	特定のバージョンのオブジェクトのタグセットを返すアクセス許可を付与	Read	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
ListBucket	Amazon S3 バケット内のオブジェクトの一部またはすべてを一覧表示する許可を付与 (最大 1000)	リスト	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListBucketMultipartUploads	進行中のマルチパートアップロードを一覧表示するアクセス許可を付与	リスト	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListBucketVersions	Amazon S3 バケット内のすべてのバージョンオブジェクトに関するメタデータを一覧表示するアクセス許可を付与	リスト	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListMultipartUploadParts	特定のマルチパートアップロード用にアップロードされた部分を一覧表示するアクセス許可を付与	リスト	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObject	バケットにオブジェクトを追加する許可を付与	書き込み	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectAcl	S3 バケット内の新規または既存のオブジェクトに対して、アクセスコントロールリスト (ACL) を設定するためのアクセス許可を付与する	権限の管理	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectLegalHold	指定したオブジェクトにリーガルホールド設定を適用するアクセス許可を付与	Write	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectRetention	オブジェクトにオブジェクト保持設定を配置するアクセス許可を付与	Write	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectTagging	指定されたタグセットを、バケット内に既に存在するオブジェクトに設定するアクセス許可を付与	タグ付け	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutObjectVersionAcl	acl サブリソースを使用して、バケットにすでに存在するオブジェクトのアクセスコントロールリスト (ACL) アクセス許可を設定するアクセス許可を付与	Permissions management	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
PutObjectVersionTagging	特定のバージョンのオブジェクトに対して指定されたタグセットを設定するアクセス許可を付与	タグ付け	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
RestoreObject	オブジェクトのアーカイブされたコピーを Amazon S3 に復元するアクセス許可を付与	Write	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
WriteGetObjectResponse	S3 Object Lambda に送信する GetObject リクエストのデータを提供する許可を付与	Write	objectlambdaaccesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	

Amazon S3 Object Lambda によって定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
objectlambdaaccesspoint	`arn:${Partition}:s3-object-lambda:${Region}:${Account}:accesspoint/${AccessPointName}`	

Amazon S3 Object Lambda の条件キー

Amazon S3 Object Lambda では、IAM ポリシーの Condition 要素で使用できる以下の条件キーが定義されます。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
s3-object-lambda:TlsVersion	クライアントが使用する TLS バージョンでアクセスをフィルタリングします	数値
s3-object-lambda:authType	認証方式でアクセスをフィルタリングします	文字列
s3-object-lambda:signatureAge	リクエスト署名の経過時間 (ミリ秒単位) でアクセスをフィルタリングします	数値
s3-object-lambda:versionid	特定のオブジェクトバージョンでアクセスをフィルタリングします	文字列

Amazon S3 on Outposts のアクション、リソース、条件キー

Amazon S3 on Outposts (サービスプレフィックス: s3-outposts) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon S3 on Outposts によって定義されたアクション
- Amazon S3 on Outposts によって定義されたリソースタイプ
- Amazon S3 on Outposts の条件キー

Amazon S3 on Outposts によって定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AbortMultipartUpload	マルチパートアップロードを中止するアクセス許可を付与	Write	object*		
				s3-outposts:DataAccessPointArn s3-outposts:DataAccessPointAccount s3-outposts:AccessPointNetworkOrigin s3-outposts:authType	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
CreateAccessPoint	新しいアクセスポイントを作成する許可を付与	Write	accesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3-outposts:x-amz-content-sha256	
CreateBucket	新しいバケットを作成するアクセス許可を付与します	Write	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
CreateEndpoint	新しいエンドポイントを作成する許可を付与	Write	endpoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteAccessPoint	URI で指定されたアクセスポイントを削除するアクセス許可を付与します	Write	accesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:DataAccessPointArn s3-outposts:DataAccessPointAccount s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:x-amz-content-sha256	
DeleteAccessPointPolicy	指定したアクセスポイントでポリシーを削除するアクセス許可を付与します	Permissions management	accesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:DataAccessPointArn s3-outposts:DataAccessPointAccount s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3-outposts:x-amz-content-sha256	
DeleteBucket	URI で指定されたバケットを削除するアクセス許可を付与します	Write	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteBucketPolicy	指定したバケットのポリシーを削除するアクセス許可を付与	Permissions management	bucket*	s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
DeleteEndpoint	URI で指定されたエンドポイントを削除する許可を付与	Write	endpoint*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteObject	オブジェクトの null バージョンを削除し、削除マーカーを挿入する許可を付与。このマーカーは、オブジェクトの現在のバージョンになります	Write	object*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				ureversion s3-outposts:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteObjectTagging	タグ付けサブリソースを使用して、指定したオブジェクトからタグセット全体を削除するアクセス許可を付与	タグ付け	object*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				ts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
DeleteObjectVersion	特定のバージョンのオブジェクトを削除するアクセス許可を付与	Write	object*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:versionid s3-outposts:x-amz-content-sha256	
DeleteObjectVersionTagging	オブジェクトの特定のバージョンのタグセット全体を削除するアクセス許可を付与	Tagging	object*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetAccessPoint	指定したアクセスポイントに関する設定情報を返すアクセス許可を付与します	Read		s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:x-amz-content-sha256	
GetAccessPointPolicy	指定したアクセスポイントに関連付けられたアクセスポイントポリシーを返すアクセス許可を付与します	Read	accesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3-outposts:x-amz-content-sha256	
GetBucket	Amazon S3 バケットに関連付けられたバケット設定を返すアクセス許可を付与します	Read	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetBucketPolicy	指定したバケットのポリシーを返すアクセス許可を付与します	Read	bucket*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetBucketTagging	Amazon S3 バケットに関連付けられたタグセットを返すアクセス許可を付与します	Read	bucket*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetBucketVersioning	Amazon S3 バケットのバージョニング状態を返すアクセス許可を付与します	読み取り	bucket*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetLifecycleConfiguration	Amazon S3 バケットに設定されたライフサイクル設定情報を返すアクセス許可を付与します	Read	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetObject	Amazon S3 からオブジェクトを取得するためのアクセス許可を付与します	Read	object*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetObjectTagging	オブジェクトのタグセットを返すアクセス許可を付与	Read	object*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetObjectVersion	特定のバージョンのオブジェクトを取得するためのアクセス許可を付与	読み取り	object*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetObjectVersionForReplication	暗号化されていないオブジェクトと、SSE-KMS で暗号化されたオブジェクトの両方をレプリケートするアクセス許可を付与	読み取り	object*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetObjectVersionTagging	特定のバージョンのオブジェクトのタグセットを返すアクセス許可を付与	Read	object*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetReplicationConfiguration	Amazon S3 バケットに設定されたレプリケーション設定情報を取得するアクセス許可を付与します	読み取り	bucket*	s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListAccessPoints	アクセスポイントを一覧表示する許可を付与	リスト		s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListBucket	Amazon S3 バケット内のオブジェクトの一部またはすべてを一覧表示するアクセス許可を付与します (最大 1000)	リスト	accesspoint* bucket*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:delimiter s3-outposts:max-keys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3-outposts:prefix s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListBucketMultipartUploads	進行中のマルチパートアップロードを一覧表示するアクセス許可を付与	リスト	accesspoint* bucket*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListBucketVersions	Amazon S3 バケット内のすべてのバージョンオブジェクトに関するメタデータを一覧表示するアクセス許可を付与	リスト	bucket*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:delimiter s3-outposts:max-keys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:prefix s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListEndpoints	エンドポイントを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListMultipartUploadParts	特定のマルチパートアップロード用にアップロードされた部分を一覧表示するアクセス許可を付与	リスト	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				ureversion s3-outposts:x-amz-content-sha256	
ListOutpostsWithS3	S3 キャパシティの Outpost を一覧表示するための許可を付与します	リスト			
ListRegionalBuckets	リクエストの認証された送信者が所有するすべてのバケットを一覧表示する許可を付与	リスト		s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListSharedEndpoints	共有エンドポイントを一覧表示する許可を付与	リスト			
PutAccessPointPolicy	アクセスポリシーを指定されたアクセスポイントに関連付けるアクセス許可を付与します	Permissions management	accesspoint*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3-outposts:x-amz-content-sha256	
PutBucketPolicy	バケットのバケットポリシーを追加または置き換えるアクセス許可を付与します	Permissions management	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
PutBucketTagging	既存の Amazon S3 バケットにタグのセットを追加する許可を付与	タグ付け	bucket*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutBucketVersioning	既存の Amazon S3 バケットのバージョニング状態を設定するアクセス許可を付与します	書き込み	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutLifecycleConfiguration	バケットの新しいライフサイクル設定を作成するか、既存のライフサイクル設定を置き換えるアクセス許可を付与します	Write	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
PutObject	バケットにオブジェクトを追加するアクセス許可を付与します	Write	object*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:RequestObjectTag/<key> s3-outposts:RequestObjectTagKeys s3-outposts:authType	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-acl s3-outposts:x-amz-content-sha256 s3-outposts:x-amz-copy-source s3-outposts:x-amz-metadata-directive	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:x-amz-server-side-encryption s3-outposts:x-amz-storage-class	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutObjectAcl	バケット内にすでに存在するオブジェクトのアクセスコントロールリスト (ACL) のアクセス許可を設定する許可を付与	Permissions management	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				ts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-acl s3-outposts:x-amz-content-sha256 s3-outposts:x-amz-storage-class	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutObjectTagging	指定されたタグセットを、バケット内に既に存在するオブジェクトに設定する許可を付与	Tagging	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:RequestObjectTag/<key> s3-outpos	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				ts:RequestObjectTagKeys s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutObjectVersionTagging	特定のバージョンのオブジェクトに対して指定されたタグセットを設定するアクセス許可を付与	タグ付け	object*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:RequestObjectTag/<key> s3-outpos	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ts:RequestObjectTagKeys s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	
PutReplicationConfiguration	新しいレプリケーション設定を作成するか、既存のレプリケーション設定を置き換えるアクセス許可を付与します	書き込み	bucket*		iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
Replicate Delete	削除マーカーをレプリケート先バケットにレプリケートするアクセス許可を付与します	Write	object*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
Replicate Object	オブジェクトとオブジェクトタグをレプリケート先バケットにレプリケートするアクセス許可を付与します	Write	object*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256 s3-outposts:x-amz-server-side-encryption	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
Replicate Tags	オブジェクトタグをレプリケート先バケットにレプリケートするアクセス許可を付与します	Tagging	object*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Amazon S3 on Outposts によって定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
accesspoint	arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/accesspoint/${AccessPointName}	
bucket	arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/bucket/${BucketName}	
endpoint	arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/endpoint/${EndpointId}	
object	arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/bucket/${BucketName}/object/${ObjectName}	

Amazon S3 on Outposts の条件キー

Amazon S3 on Outposts では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
s3-outposts:AccessPointNetworkOrigin	ネットワークオリジン (インターネットまたは VPC) によるアクセスをフィルタリングします	String
s3-outposts:DataAc	アクセスポイントを所有する AWS アカウント ID でアクセスをフィルタリングします	String

条件キー	説明	タイプ
cessPoint Account		
s3-outpos ts:DataAc cessPointArn	アクセスポイント Amazon リソースネーム (ARN) でアクセスをフィルタリングします	ARN
s3-outpos ts:Existi ngObjectTag/ <key>	既存のオブジェクトタグに特定のタグのキーと値があるように要求することで、アクセスをフィルタリングします	文字列
s3-outpos ts:Reques tObjectTag/ <key>	オブジェクトで許可されているタグのキーと値を制限してアクセスをフィルタリングします	文字列
s3-outpos ts:Reques tObjectTagKeys	オブジェクトで許可されているタグキーを制限してアクセスをフィルタリングします	文字列
s3-outpos ts:authType	受信リクエストを特定の認証方式に制限してアクセスをフィルタリングします	文字列
s3-outpos ts:delimiter	区切り記号パラメータを要求してアクセスをフィルタリングします	文字列
s3-outpos ts:max-keys	ListBucket リクエストで返されるキーの最大数を制限してアクセスをフィルタリングします	数値
s3-outpos ts:prefix	キー名のプレフィックスでアクセスをフィルタリングします	文字列
s3-outpos ts:signatureAge	署名が認証された要求で有効である時間 (ミリ秒単位) を識別してアクセスをフィルタリングします	数値

条件キー	説明	タイプ
s3-outposts:signatureversion	認証されたリクエストでサポートされている AWS Signature のバージョンを特定してアクセスをフィルタリングします	String
s3-outposts:versionid	特定のオブジェクトバージョンでアクセスをフィルタリングします	String
s3-outposts:x-amz-acl	リクエスト内で特定の既定 ACL を持つ x-amz-acl ヘッダーを要求することでアクセスをフィルタリングします	文字列
s3-outposts:x-amz-content-sha256	バケット内の署名されていないコンテンツを許可しないことによってアクセスをフィルタリングします	文字列
s3-outposts:x-amz-copy-source	コピーソースを特定のバケット、プレフィックス、またはオブジェクトに制限してアクセスをフィルタリングします	文字列
s3-outposts:x-amz-metadata-directive	オブジェクトのコピー時にオブジェクトメタデータの動作 (COPY または REPLACE) を適用できるようにしてアクセスをフィルタリングします	文字列
s3-outposts:x-amz-server-side-encryption	サーバー側の暗号化を要求してアクセスをフィルタリングします	文字列
s3-outposts:x-amz-storage-class	ストレージクラスでアクセスをフィルタリングします	String

Amazon S3 Tables のアクション、リソース、および条件キー

Amazon S3 Tables (サービスプレフィックス: `s3tables`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon S3 Tables で定義されるアクション
- Amazon S3 Tables で定義されるリソースタイプ
- Amazon S3 Tables の条件キー

Amazon S3 Tables で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateNamespace	名前空間を作成するアクセス許可を付与します	書き込み	TableBucket*		
CreateTable	テーブルを作成する許可を付与。	書き込み	TableBucket*		
				s3tables:namespace s3tables:SSEAlgorithm s3tables:KMSKeyAr	
CreateTableBucket	テーブルバケットを作成するアクセス許可を付与します	書き込み	TableBucket*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3tables:SSEAlgorithm s3tables:KMSKeyAr	
DeleteNamespace	名前空間を削除するアクセス許可を付与します	書き込み	TableBucket*		
				s3tables:namespace	
DeleteTable	テーブルを削除する許可を付与。	書き込み	Table*		
				s3tables:namespace s3tables:tableName	
DeleteTableBucket	テーブルバケットを削除するアクセス許可を付与します	書き込み	TableBucket*		
DeleteTableBucketEncryption	テーブルバケットの暗号化設定を削除するアクセス許可を付与します	書き込み	TableBucket*		
DeleteTableBucketPolicy	テーブルバケットのポリシーを削除するアクセス許可を付与します	権限の管理	TableBucket*		
DeleteTablePolicy	テーブルのポリシーを削除するアクセス許可を付与します	権限の管理	Table*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3tables:namespace s3tables:tableName	
GetNamespace	名前空間を取得するアクセス許可を付与します	読み取り	TableBucket*		
				s3tables:namespace	
GetTable	テーブルを取得する許可を付与。	読み取り	Table*		
				s3tables:namespace s3tables:tableName	
GetTableBucket	テーブルバケットを取得するアクセス許可を付与します	読み取り	TableBucket*		
GetTableBucketEncryption	テーブルバケットの暗号化設定を取得するアクセス許可を付与します	読み取り	TableBucket*		
GetTableBucketMaintenanceConfiguration	テーブルバケットのメンテナンス設定を取得するアクセス許可を付与します	読み取り	TableBucket*		
GetTableBucketPolicy	テーブルバケットのポリシーを取得するアクセス許可を付与します	読み取り	TableBucket*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetTableData [許可のみ]	S3 APIs	読み取り	Table*		
				s3tables:namespace s3tables:tableName	
GetTableEncryption	テーブルの暗号化設定を取得する許可を付与	読み取り	Table*		
				s3tables:namespace s3tables:tableName	
GetTableMaintenanceConfiguration	テーブルのメンテナンス設定を取得するアクセス許可を付与します	読み取り	Table*		
				s3tables:namespace s3tables:tableName	
GetTableMaintenanceJobStatus	テーブルのメンテナンスジョブのステータスを取得するアクセス許可を付与します	読み取り	Table*		
				s3tables:namespace s3tables:tableName	
GetTableMetadataLocation	テーブルのメタデータの場所を取得するアクセス許可を付与します	読み取り	Table*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3tables:namespace s3tables:tableName	
GetTablePolicy	テーブルのポリシーを取得するアクセス許可を付与します	読み取り	Table*		
				s3tables:namespace s3tables:tableName	
ListNamespaces	名前空間を一覧表示するアクセス許可を付与します	リスト	TableBucket*		
ListTableBuckets	テーブルバケットを一覧表示するアクセス許可を付与します	リスト			
ListTables	テーブルを一覧表示するアクセス許可を付与します	リスト	TableBucket*		
				s3tables:namespace	
PutTableBucketEncryption	テーブルバケットに暗号化設定を配置または上書きするアクセス許可を付与します	書き込み	TableBucket*		
				s3tables:KMSKeyArn s3tables:SSEAlgorithm	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutTableBucketMaintenanceConfiguration	テーブルバケットにメンテナンス設定を配置するアクセス許可を付与します	書き込み	TableBucket*		
PutTableBucketPolicy	テーブルバケットでポリシーを作成または上書きするアクセス許可を付与します	権限の管理	TableBucket*		
PutTableData [許可のみ]	S3 APIs	書き込み	Table*		
				s3tables:namespace s3tables:tableName	
PutTableEncryption [アクセス許可のみ]	テーブルに暗号化設定を配置するアクセス許可を付与します	書き込み	Table*		
				s3tables:namespace s3tables:SSEAlgorithm s3tables:KMSKeyAr	
PutTableMaintenanceConfiguration	テーブルにメンテナンス設定を配置するアクセス許可を付与します	書き込み	Table*		
				s3tables:namespace s3tables:tableName	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutTablePolicy	テーブルでポリシーを作成または上書きするアクセス許可を付与します	権限の管理	Table*		
				s3tables:namespace s3tables:tableName	
RenameTable	テーブルの名前を変更したり、名前空間間でテーブルを移動したりするアクセス許可を付与します	書き込み	Table*		
				s3tables:namespace s3tables:tableName	
UpdateTableMetadataLocation	テーブルのメタデータの場所を更新するアクセス許可を付与します	書き込み	Table*		
				s3tables:namespace s3tables:tableName	

Amazon S3 Tables で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
TableBucket	arn:${Partition}:s3tables:${Region}:${Account}:bucket/${TableBucketName}	
Table	arn:${Partition}:s3tables:${Region}:${Account}:bucket/${TableBucketName}/table/${TableID}	s3tables:namespace s3tables:tableName

Amazon S3 Tables の条件キー

Amazon S3 Tables では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
s3tables:KMSKeyArn	テーブルの暗号化に使用されるキーの AWS KMS キー ARN でアクセスをフィルタリングします	ARN
s3tables:SSEAlgorithm	テーブルの暗号化に使用されるサーバー側の暗号化アルゴリズムでアクセスをフィルタリングします	String
s3tables:namespace	テーブルバケットで作成された名前空間でアクセスをフィルタリングします	String
s3tables:tableName	テーブルバケット内のテーブルの名前でアクセスをフィルタリングします	String

Amazon S3 Vectors のアクション、リソース、および条件キー

Amazon S3 Vectors (サービスプレフィックス: `s3vectors`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon S3 Vectors で定義されるアクション
- Amazon S3 Vectors で定義されるリソースタイプ
- Amazon S3 Vectors の条件キー

Amazon S3 Vectors で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateIndex	指定されたベクトルバケット内に新しいベクトルインデックスを作成するアクセス許可を付与します	書き込み	Index*		
CreateVectorBucket	新しいベクトルバケットを作成するアクセス許可を付与します	書き込み	VectorBucket*		
				s3vectors:sseType	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				s3vectors:kmsKeyArn	
DeleteIndex	指定されたベクトルインデックスを削除するアクセス許可を付与します	書き込み	Index*		
DeleteVectorBucket	指定されたベクトルバケットを削除するアクセス許可を付与します	書き込み	VectorBucket*		
DeleteVectorBucketPolicy	指定されたベクトルバケットから IAM リソースポリシーを削除するアクセス許可を付与します	権限の管理	VectorBucket*		
DeleteVectors	指定されたベクトルインデックスからベクトルのバッチを削除するアクセス許可を付与します	書き込み	Index*		
GetIndex	指定されたベクトルインデックスの属性を取得するアクセス許可を付与します	読み取り	Index*		
GetVectorBucket	指定されたベクトルバケットの属性を取得するアクセス許可を付与します	読み取り	VectorBucket*		
GetVectorBucketPolicy	特定のベクトルバケットの IAM リソースポリシーを取得する許可を付与	読み取り	VectorBucket*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetVectors	ベクトルキーによってベクトルのバッチを取得するアクセス許可を付与します	読み取り	Index*		
ListIndexes	指定されたベクトルバケット内のすべてのインデックスのページ分割されたリストを取得するアクセス許可を付与します	リスト	VectorBucket*		
ListVectorBuckets	アカウント内のすべてのベクトルバケットのページ分割されたリストを取得するアクセス許可を付与します	リスト			
ListVectors	指定されたベクトルインデックス内のすべてのベクトルのページ分割されたリストを取得するアクセス許可を付与します	リスト	Index*		s3vectors:GetVectors
PutVectorBucketPolicy	指定されたベクトルバケットに IAM リソースポリシーを追加するアクセス許可を付与します	権限の管理	VectorBucket*		
PutVectors	指定されたベクトルインデックスにベクトルのバッチを追加する許可を付与	書き込み	Index*		
QueryVectors	特定のクエリベクトルの指定された検索ベクトルインデックス内で近似近傍を検索するアクセス許可を付与します	読み取り	Index*		s3vectors:GetVectors

Amazon S3 Vectors で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Index	`arn:${Partition}:s3vectors:${Region}:${Account}:bucket/${BucketName}/index/${IndexName}`	
VectorBucket	`arn:${Partition}:s3vectors:${Region}:${Account}:bucket/${BucketName}`	

Amazon S3 Vectors の条件キー

Amazon S3 Vectors では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
s3vectors:kmsKeyArn	ベクトルバケットの暗号化に使用されるキーの AWS KMS キー ARN でアクセスをフィルタリングします	ARN
s3vectors:sseType	サーバー側の暗号化タイプでアクセスをフィルタリングします	String

Amazon SageMaker データサイエンスアシスタントのアクション、リソース、および条件キー

Amazon SageMaker データサイエンスアシスタント (サービスプレフィックス: `sagemaker-data-science-assistant`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon SageMaker データサイエンスアシスタントで定義されるアクション
- Amazon SageMaker データサイエンスアシスタントで定義されるリソースタイプ
- Amazon SageMaker データサイエンスアシスタントの条件キー

Amazon SageMaker データサイエンスアシスタントで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイ

プが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SendConversation [アクセス許可のみ]	SageMaker データサイエンスアシスタントとの会話を開始するアクセス許可を付与します	書き込み			

Amazon SageMaker データサイエンスアシスタントで定義されるリソースタイプ

Amazon SageMaker データサイエンスアシスタントは、IAM ポリシーステートメントの Resource要素でのリソース ARN の指定をサポートしていません。Amazon SageMaker データサイエンスアシスタントへのアクセスを許可するには、ポリシー"Resource": "*"で を指定します。

Amazon SageMaker データサイエンスアシスタントの条件キー

SageMakerDataScienceAssistant には、ポリシーステートメントの Condition要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon SageMaker 地理空間機能のアクション、リソース、および条件キー

Amazon SageMaker 地理空間機能 (サービスプレフィックス: sagemaker-geospatial) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon SageMaker 地理空間機能で定義されるアクション
- Amazon SageMaker 地理空間機能で定義されるリソースタイプ
- Amazon SageMaker 地理空間機能の条件キー

Amazon SageMaker 地理空間機能で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にア

クションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteEarthObservationJob	既存の地球観測ジョブを削除する DeleteEarthObservationJob オペレーションに許可を付与	書き込み	EarthObservationJob*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
DeleteVectorEnrichmentJob	既存のベクターエンリッチメントジョブを削除する DeleteVectorEnrichmentJob オペレーションに許可を付与	書き込み	VectorEnrichmentJob*		
				aws:ResourceTag/${TagKey}	
ExportEarthObservationJob	地球観測ジョブの結果を S3 ロケーションにコピーする許可を付与	書き込み	EarthObservationJob*		iam:PassRole
				aws:ResourceTag/${TagKey}	
ExportVectorEnrichmentJob	VectorEnrichmentJob の結果を S3 ロケーションにコピーする許可を付与	書き込み	VectorEnrichmentJob*		iam:PassRole
				aws:ResourceTag/${TagKey}	
GetEarthObservationJob	地球観測ジョブに関する詳細を返す許可を付与	読み取り	EarthObservationJob*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetRasterDataCollection	ラスターデータコレクションに関する詳細を返す許可を付与	読み取り	RasterDataCollection*		
				aws:ResourceTag/${TagKey}	
GetTile	地球観測ジョブのタイルを取得する許可を付与	読み取り	EarthObservationJob*		iam:PassRole
GetVectorEnrichmentJob	ベクターエンリッチメントジョブに関する詳細を返す許可を付与	読み取り	VectorEnrichmentJob*		
				aws:ResourceTag/${TagKey}	
ListEarthObservationJobs	現在のアカウントに関連付けられた地球観測ジョブの配列を返す許可を付与	リスト			
ListRasterDataCollections	指定されたモデル名に関連付けられたラスターデータコレクションの配列を返す許可を付与	リスト			
ListTagsForResource	SageMaker 地理空間リソースのタグを一覧表示する許可を付与	リスト	EarthObservationJob		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			RasterDataCollection		
			VectorEnrichmentJob		
				aws:ResourceTag/${TagKey}	
ListVectorEnrichmentJobs	現在のアカウントに関連付けられたベクターエンリッチメントジョブの配列を返す許可を付与	リスト			
SearchRasterDataCollection	ラスターデータコレクションをクエリする許可を付与	読み取り			
StartEarthObservationJob	アカウントで新しい地球観測ジョブを開始する StartEarthObservationJob オペレーションに許可を付与	書き込み	EarthObservationJob*		iam:PassRole sagemaker-geospatial:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartVectorEnrichmentJob	アカウントで新しいベクターエンリッチメントジョブを開始する StartVectorEnrichmentJob オペレーションに許可を付与	書き込み	VectorEnrichmentJob*		iam:PassRole sagemaker-geospatial:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StopEarthObservationJob	既存の地球観測ジョブを停止する StopEarthObservationJob オペレーションに許可を付与	書き込み	EarthObservationJob*		
				aws:ResourceTag/${TagKey}	
StopVectorEnrichmentJob	既存のベクターエンリッチメントジョブを停止する StopVectorEnrichmentJob オペレーションに許可を付与	書き込み	VectorEnrichmentJob*		
				aws:ResourceTag/${TagKey}	
TagResource	SageMaker 地理空間リソースをタグ付けする許可を付与	Tagging	EarthObservationJob		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			RasterDataCollection		
			VectorEnrichmentJob		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	SageMaker 地理空間リソースからタグを解除する許可を付与	Tagging	EarthObservationJob		
			RasterDataCollection		
			VectorEnrichmentJob		
				aws:TagKeys	

Amazon SageMaker 地理空間機能で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
EarthObservationJob	arn:${Partition}:sagemaker-geospatial:${Region}:${Account}:earth-observation-job/${JobID}	aws:ResourceTag/${TagKey}
RasterDataCollection	arn:${Partition}:sagemaker-geospatial:${Region}:${Account}:raster-data-collection/${CollectionID}	aws:ResourceTag/${TagKey}
VectorEnrichmentJob	arn:${Partition}:sagemaker-geospatial:${Region}:${Account}:vector-enrichment-job/${JobID}	aws:ResourceTag/${TagKey}

Amazon SageMaker 地理空間機能の条件キー

Amazon SageMaker 地理空間機能は、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

MLflow を使用した Amazon SageMaker のアクション、リソース、および条件キー

MLflow を使用して Amazon SageMaker (サービスプレフィックス: `sagemaker-mlflow`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- MLflow を使用して Amazon SageMaker で定義されるアクション
- MLflow を使用した Amazon SageMaker で定義されるリソースタイプ
- MLflow を使用した Amazon SageMaker の条件キー

MLflow を使用して Amazon SageMaker で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーショ

ンへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AccessUI	MLflow UI にアクセスする許可を付与する	読み取り			
CreateExperiment	MLflow 実験を作成する許可を付与する	書き込み	mlflow-tracking-server*		
CreateModelVersion	新しいモデルバージョンをを作成する許可を付与する	書き込み	mlflow-tracking-server*		
CreateRegisteredModel	登録モデルを作成する許可を付与する	書き込み	mlflow-tracking-server*		
CreateRun	実験内で新しい実行を作成する許可を付与する	書き込み	mlflow-tracking-server*		
DeleteExperiment	MLflow 実験を削除対象としてマークする許可を付与する	書き込み	mlflow-tracking-server*		
DeleteLoggedModel	MLflow でログに記録されたモデルを削除するアクセス許可を付与します	書き込み	mlflow-tracking-server*		
DeleteLoggedModelTag	MLflow でログに記録されたモデルのタグを削除するアクセス許可を付与します	書き込み	mlflow-tracking-server*		
DeleteModelVersion	モデルのバージョンを削除する許可を付与する	書き込み	mlflow-tracking-server*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteModelVersionTag	モデルのバージョンタグを削除する許可を付与する	書き込み	mlflow-tracking-server*		
DeleteRegisteredModel	登録済みモデルを削除する許可を付与する	書き込み	mlflow-tracking-server*		
DeleteRegisteredModelAlias	登録済みのモデルエイリアスを削除する許可を付与する	書き込み	mlflow-tracking-server*		
DeleteRegisteredModelTag	登録済みモデルタグを削除する許可を付与する	書き込み	mlflow-tracking-server*		
DeleteRun	実行を削除対象としてマークする許可を付与する	書き込み	mlflow-tracking-server*		
DeleteTag	実行中にタグを削除する許可を付与する	書き込み	mlflow-tracking-server*		
DeleteTraceTag	MLflow でトレースタグを削除するアクセス許可を付与します	書き込み	mlflow-tracking-server*		
DeleteTraces	MLflow でトレースを削除するアクセス許可を付与します	書き込み	mlflow-tracking-server*		
EndTrace	MLflow でトレースを終了する許可を付与	書き込み	mlflow-tracking-server*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
FinalizeLoggedModel	MLflow でログに記録されたモデルのステータスを設定するアクセス許可を付与します	書き込み	mlflow-tracking-server*		
GetDownloadURIForModelVersionArtifacts	特定のモデルバージョンのモデルアーティファクトをダウンロードする URI を取得する許可を付与する	読み取り	mlflow-tracking-server*		
GetExperiment	MLflow 実験のメタデータを取得する許可を付与する	読み取り	mlflow-tracking-server*		
GetExperimentByName	MLflow 実験のメタデータを名前で取得する許可を付与する	読み取り	mlflow-tracking-server*		
GetLatestModelVersions	最新のモデルバージョンを取得する許可を付与する	リスト	mlflow-tracking-server*		
GetLoggedModel	MLflow でログに記録されたモデルを取得するアクセス許可を付与します	読み取り	mlflow-tracking-server*		
GetMetricHistory	特定の実行に対して指定されたメトリクスのすべての値のリストを取得する許可を付与する	読み取り	mlflow-tracking-server*		
GetModelVersion	モデル名とバージョン別にモデルバージョンを取得する許可を付与する	読み取り	mlflow-tracking-server*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetModelVersionByAlias	MLflow のエイリアスによってモデルバージョンを取得する許可を付与する	読み取り	mlflow-tracking-server*		
GetRegisteredModel	登録済みモデルを取得する許可を付与する	読み取り	mlflow-tracking-server*		
GetRun	実行のメタデータ、メトリクス、パラメータ、タグを取得する許可を付与する	読み取り	mlflow-tracking-server*		
GetTraceInfo	MLflow のトレースに関する情報を取得する許可を付与	読み取り	mlflow-tracking-server*		
ListArtifacts	実行のアーティファクトを一覧表示する許可を付与する	リスト	mlflow-tracking-server*		
ListLoggedModelArtifacts	MLflow でログに記録されたモデルのアーティファクトを一覧表示するアクセス許可を付与します	リスト	mlflow-tracking-server*		
LogBatch	実行のメトリクス、パラメータ、タグのバッチをログに記録する許可を付与する	書き込み	mlflow-tracking-server*		
LogInputs	実行の入力をログに記録する許可を付与する	書き込み	mlflow-tracking-server*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
LogLoggedModelParams	MLflow でログに記録されたモデルのパラメータをログに記録するアクセス許可を付与します	書き込み	mlflow-tracking-server*		
LogMetric	実行のメトリクスをログに記録する許可を付与する	書き込み	mlflow-tracking-server*		
LogModel	実行に関連付けられたモデルをログに記録する許可を付与する	書き込み	mlflow-tracking-server*		
LogOutputs	MLflow での実行のモデルなどの出力をログに記録するアクセス許可を付与します	書き込み	mlflow-tracking-server*		
LogParam	実行中に追跡されたパラメータをログに記録する許可を付与する	書き込み	mlflow-tracking-server*		
RenameRegisteredModel	登録済みモデルの名前を変更する許可を付与する	書き込み	mlflow-tracking-server*		
RestoreExperiment	削除対象としてマークされた実験を復元する許可を付与する	書き込み	mlflow-tracking-server*		
RestoreRun	削除した実行を復元する許可を付与する	書き込み	mlflow-tracking-server*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SearchExperiments	MLflow 実験を検索する許可を付与する	読み取り	mlflow-tracking-server*		
SearchLoggedModels	MLflow でログに記録されたモデルを検索するアクセス許可を付与します	読み取り	mlflow-tracking-server*		
SearchModelVersions	モデルバージョンを検索する許可を付与する	読み取り	mlflow-tracking-server*		
SearchRegisteredModels	MLflow で登録済みモデルを検索する許可を付与する	読み取り	mlflow-tracking-server*		
SearchRuns	式を満たす実行を検索する許可を付与する	読み取り	mlflow-tracking-server*		
SearchTraces	MLflow でトレースを検索するアクセス許可を付与します	読み取り	mlflow-tracking-server*		
SetExperimentTag	実験にタグを設定する許可を付与する	書き込み	mlflow-tracking-server*		
SetLoggedModelTags	MLflow でログに記録されたモデルのタグを設定するアクセス許可を付与します	書き込み	mlflow-tracking-server*		
SetModelVersionTag	モデルバージョンのタグを設定する許可を付与する	書き込み	mlflow-tracking-server*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SetRegisteredModelAlias	登録されたモデルエイリアスを設定する許可を付与する	書き込み	mlflow-tracking-server*		
SetRegisteredModelTag	登録済みモデルのタグを設定する許可を付与する	書き込み	mlflow-tracking-server*		
SetTag	実行にタグを設定する許可を付与する	書き込み	mlflow-tracking-server*		
SetTraceTag	MLflow でトレースタグを設定するアクセス許可を付与します	書き込み	mlflow-tracking-server*		
StartTrace	MLflow でトレースを開始する許可を付与	書き込み	mlflow-tracking-server*		
TransitionModelVersionStage	モデルバージョンを特定のステージに移行する許可を付与する	書き込み	mlflow-tracking-server*		
UpdateExperiment	MLflow 実験のメタデータを更新する許可を付与する	書き込み	mlflow-tracking-server*		
UpdateModelVersion	モデルバージョンを更新する許可を付与する	書き込み	mlflow-tracking-server*		
UpdateRegisteredModel	登録されたモデルを更新する許可を付与する	書き込み	mlflow-tracking-server*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateRun	実行メタデータを更新する許可を付与する	書き込み	mlflow-tracking-server*		

MLflow を使用した Amazon SageMaker で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
mlflow-tracking-server	`arn:${Partition}:sagemaker:${Region}:${Account}:mlflow-tracking-server/${MlflowTrackingServerName}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

MLflow を使用した Amazon SageMaker の条件キー

Amazon SageMaker with MLflow では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:ResourceTag/${TagKey}	タグキーおよび値のペアでアクセスをフィルタリングします。	String
sagemaker:ResourceTag/${TagKey}	タグキーおよび値のペアでアクセスをフィルタリングします。	String

AWS Savings Plans のアクション、リソース、および条件キー

AWS Savings Plans (サービスプレフィックス: savingsplans) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Savings Plans で定義されるアクション
- AWS Savings Plans で定義されるリソースタイプ
- AWS Savings Plans の条件キー

AWS Savings Plans で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーショ

ンへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateSavingsPlan	Savings Plan を作成する許可を付与。	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteQueuedSavingsPlan	顧客アカウントに関連付けられた、キューに入れられた Savings Plan を削除する許可を付与。	Write	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlanRates	顧客の Savings Plan に関連する料金を説明する許可を付与。	Read	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlans	顧客アカウントに関連付けられた Savings Plans を説明する許可を付与。	Read	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlansOfferingRates	Savings Plans のサービスに関連する料金を説明する許可を付与。	Read			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeSavingsPlansOfferings	顧客が購入できる Savings Plans のサービスを説明する許可を付与。	Read			
ListTagsForResource	Savings Plan のタグを一覧表示する許可を付与。	リスト	savingsplan*		
ReturnSavingsPlan	Savings Plan を作成する許可を付与する	書き込み	savingsplan*		
				aws:ResourceTag/${TagKey}	
TagResource	Savings Plan にタグを付けるアクセス許可を付与	タグ付け	savingsplan*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Savings Plan のタグを解除する許可を付与。	タグ付け	savingsplan*		
				aws:TagKeys	

AWS Savings Plans で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
savingsplan	`arn:${Partition}:savingsplans::${Account}:savingsplan/${ResourceId}`	aws:ResourceTag/${TagKey}

AWS Savings Plans の条件キー

AWS Savings Plans では、IAM ポリシーの `Condition`要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	各タグの許可された値のセットでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値でアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内の必須タグの存在でアクセスをフィルタリングします	ArrayOfString

AWS Secrets Manager のアクション、リソース、および条件キー

AWS Secrets Manager (サービスプレフィックス: `secretsmanager`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Secrets Manager で定義されるアクション
- AWS Secrets Manager で定義されるリソースタイプ
- AWS Secrets Manager の条件キー

AWS Secrets Manager で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchGetSecretValue	シークレットのリストを取得および復号化するためのアクセス許可を付与	リスト			
CancelRotateSecret	進行中のシークレットのローテーションをキャンセルするアクセス許可を付与します。	書き込み	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:Res	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
CreateSecret	クエリおよびローテーションが可能な暗号化されたデータを保存するシークレットを作成する許可を付与します。	書き込み	Secret*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				secretsmanager:Name secretsmanager:Description secretsmanager:KmsKeyArn secretsmanager:KmsKeyId aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys secretsmanager:ResourceTag/tag-key secretsmanager:Add	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ReplicaRegions secretsmanager:ForceOverwriteReplicaSecret	
DeleteResourcePolicy	シークレットに取り付けられたリソースポリシーを削除する許可を付与します。	経営へのアクセス権	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteSecret	シークレットを削除するアクセス権限を付与します。	書き込み	Secret*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:RecoveryWindowInDays secretsmanager:ForceDeleteWithoutRecovery secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:Sec	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				retPrimaryRegion	
DescribeSecret	シークレットに関するメタデータを取得するアクセス許可を付与します。暗号化されたデータは取得できません	読み込み	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
GetRandomPassword	パスワードの作成に使用するランダムな文字列を生成するアクセス許可を付与します。	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetResourcePolicy	シークレットに取り付けられているリソースポリシーを取得するアクセス許可を付与します。	読み込み	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaAr n secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
GetSecretValue	暗号化されたデータを取得および復号化するアクセス許可を付与します。	読み込み	Secret*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				secretsmanager:SecretId secretsmanager:VersionId secretsmanager:VersionStage secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
ListSecretVersionIds		読み込み	Secret*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	利用可能なシークレットのバージョンを一覧表示する許可を付与します。			secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
ListSecrets	利用可能なシークレットを一覧表示するためのアクセス許可を付与します。	リスト			
PutResourcePolicy	リソースポリシーをシークレットに取り付ける許可を付与します。	経営へのアクセス権	Secret*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:BlockPublicPolicy secretsmanager:SecretPrimaryRegion	
PutSecretValue	新しい暗号化されたデータで新しいバージョンのシークレットを作成するアクセス許可を付与します。	書き込み	Secret*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
RemoveRegionsFromReplication	レプリケーションからリージョンを削除するアクセス許可を付与します。	書き込み	Secret*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ReplicateSecretToRegions	既存のシークレットをマルチリージョンシークレットに変換し、新しいリージョンのリストへのシークレットのレプリケートを開始する許可を付与します。	書き込み	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:AddReplicaRegions secretsmanager:ForceOverwri	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				teReplicaSecret	
RestoreSecret	シークレットの削除をキャンセルするアクセス許可を付与します。	書き込み	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
RotateSecret	シークレットのローテーションを開始するアクセス許可を付与します。	書き込み	Secret*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				secretsmanager:SecretId secretsmanager:RotationLambdaARN secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:ModifyRotationRules	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				secretsmanager:RotateImmediately	
StopReplicationToReplica	レプリケーションからシークレットを削除し、レプリカリージョンのリージョンシークレットにシークレットを昇格する許可を付与します。	書き込み	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
TagResource	シークレットにタグを追加する許可を付与します。	Tagging	Secret*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				secretsmanager:SecretId aws:RequestTag/${TagKey} aws:TagKeys secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
UntagResource	シークレットからタグを削除する許可を付与します。	Tagging	Secret*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				secretsmanager:SecretId aws:TagKeys secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
UpdateSecret	新しいメタデータもしくは新しいバージョンの暗号化データを使用してシークレットを更新する許可を付与します。	書き込み	Secret*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				secretsmanager:SecretId secretsmanager:Description secretsmanager:KmsKeyArn secretsmanager:KmsKeyId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:Sec	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				retPrimaryRegion	
UpdateSecretVersionStage	あるシークレットから別のシークレットにステージを移動するアクセス許可を付与します。	書き込み	Secret*	secretsmanager:SecretId secretsmanager:VersionStage secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ValidateResourcePolicy	ポリシーをアタッチする前にリソースポリシーを検証するアクセス許可を付与します。	権限の管理	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

AWS Secrets Manager で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Secret	arn:${Partition}:secretsmanager:${Region}:${Account}:secret:${SecretId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys secretsmanager:ResourceTag/tag-key secretsmanager:resource/AllowRotationLambdaArn

AWS Secrets Manager の条件キー

AWS Secrets Manager は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	ユーザーが Secrets Manager サービスに対して行うリクエストに含まれるキーによってアクセスをフィルタリングします。	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
aws:TagKeys	ユーザーが Secrets Manager サービスに行うリクエストに存在するすべてのタグキー名のリストに基づいて、アクセスをフィルタリングします。	ArrayOfString
secretsmanager:AddReplicaRegions	シークレットをレプリケートするリージョンのリストでアクセスをフィルタリングします。	ArrayOfString
secretsmanager:BlockPublicPolicy	リソースポリシーが広範なアクセスをブロックするかどうかで AWS アカウント アクセスをフィルタリングします	Bool
secretsmanager:Description	リクエスト内の記述テキストによるアクセスをフィルタリングします。	String
secretsmanager:ForceDeleteWithoutRecovery	シークレットがリカバリウィンドウなしですぐに削除されるかどうかによりアクセスをフィルタリングします。	Bool
secretsmanager:ForceOverwriteReplicaSecret	宛先リージョンで同じ名前のシークレットを上書きするかどうかでアクセスをフィルタリングします。	Bool
secretsmanager:KmsKeyArn	リクエスト内の KMS キーのキー ARN でアクセスをフィルタリングします	ARN
secretsmanager:KmsKeyId	リクエスト内の KMS キーのキー識別子でアクセスをフィルタリングします。非推奨: secretsmanager:KmsKeyArn を使用する	String
secretsmanager:ModifyRotationRules	シークレットのローテーションルールを変更するかどうかに基づいて、アクセスをフィルタリングします。	Bool

条件キー	説明	[Type] (タイプ)
secretsmanager:Name	リクエスト内のシークレットのフレンドリー名によるアクセスをフィルタリングします。	String
secretsmanager:RecoveryWindowInDays	Secrets Manager がシークレットを削除するまで待機する日数でアクセスをフィルタリングします。	数値
secretsmanager:ResourceTag/tag-key	タグキーおよび値のペアでアクセスをフィルタリングします。	String
secretsmanager:RotateImmediately	シークレットを直ちにローテーションするかどうかに基づいて、アクセスをフィルタリングします。	Bool
secretsmanager:RotationLambdaARN	リクエスト内のローテーション Lambda 関数の ARN によるアクセスをフィルタリングします。	ARN
secretsmanager:SecretId	リクエスト内の SecretID 値によるアクセスをフィルタリングします。	ARN
secretsmanager:SecretPrimaryRegion	シークレットがマルチリージョンシークレットである場合にシークレットが作成されるプライマリリージョンでアクセスをフィルタリングします	String
secretsmanager:VersionId	リクエスト内のシークレットのバージョンの唯一の識別子でアクセスをフィルタリングします。	String
secretsmanager:VersionStage	リクエスト内のバージョンステージのリストでアクセスをフィルタリングします。	String

条件キー	説明	[Type] (タイプ)
secretsmanager:resource/AllowRotationLambdaArn	シークレットに関連するローテーション Lambda 関数の ARN によるアクセスをフィルタリングします。	ARN

AWS Security Hub のアクション、リソース、および条件キー

AWS Security Hub (サービスプレフィックス: `securityhub`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Security Hub で定義されるアクション
- AWS Security Hub で定義されるリソースタイプ
- AWS Security Hub の条件キー

AWS Security Hub で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にア

クションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptAdministratorInvitation	メンバーアカウントになるための Security Hub の招待を受け入れるアクセス許可を付与	書き込み	hub		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptInvitation	メンバーアカウントになるための Security Hub の招待を受け入れるアクセス許可を付与	書き込み	hub		
BatchDeleteAutomationRules	Security Hub で 1 つ以上の自動化ルールを削除する許可を付与	書き込み	automation-rule*		
BatchDisableStandards	Security Hub で標準を無効にする許可を付与	書き込み	hub		
BatchEnableStandards	Security Hub で標準を有効にする許可を付与	書き込み	hub		
BatchGetAutomationRules	Amazon リソースネーム (ARN) のルールに基づいて、Security Hub から自動化ルールに関する詳細のリストを取得する許可を付与	読み取り	automation-rule*		
BatchGetConfigurationPolicyAssociations	呼び出し元アカウントの組織のメンバーアカウントと組織単位の特定のリストに関連する設定ポリシーに関する情報を取得する許可を付与	読み取り			
BatchGetControlEvaluations [許可のみ]	Security Hub コンソールで、コントロールの有効化およびコンプライアンスステータス、コントロールの検出結果の数、ならびにコントロールの全体的なセキュリティスコアを取得する許可を付与	読み取り	hub		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchGetSecurityControls	ID または ARN で識別される特定のセキュリティコントロールに関する詳細を取得する許可を付与	読み取り			securityhub:DescribeStandardsControls
BatchGetStandardsControlAssociations	標準のセキュリティコントロールのバッチの有効化ステータスを取得する許可を付与	読み取り			securityhub:DescribeStandardsControls
BatchImportFindings	統合製品から Security Hub に結果をインポートする許可を付与	書き込み	product*		
				securityhub:TargetAccount	
BatchUpdateAutomationRules	Amazon リソースネーム (ARN) のルールと入力パラメータに基づいて、Security Hub の 1 つ以上の自動化ルールを更新する許可を付与	書き込み	automation-rule*		
BatchUpdateFindings	Security Hub の結果の選択したセットについて、お客様の制御によるフィールドを更新する許可を付与	書き込み	hub		
			hubv2		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				securityhub:ASFFSyntaxPath/${ASFFSyntaxPath} securityhub:OCSFSyntaxPath/${OCSFSyntaxPath}	
BatchUpdateStandardsControlAssociations	標準のセキュリティコントロールのバッチの有効化ステータスを更新する許可を付与	書き込み			securityhub:UpdateStandardsControl
ConnectorRegistrationsV2	入力パラメータに基づいて OAuth 2.0 認可コードフローを完了する許可を付与	書き込み			
CreateActionTarget	Security Hub でカスタムアクションを作成する許可を付与	書き込み	hub		
CreateAggregatorV2	リージョン間でのデータ集約を設定する aggregatorV2 を作成するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateAutomationRule	入力パラメータに基づいて自動化ルールを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAutomationRuleV2	入力パラメータに基づいて自動化ルール V2 を作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationPolicy	セキュリティハブの組織メンバー設定を管理するための設定ポリシーを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectorV2	入力パラメータに基づいてコネクタ V2 を作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingAggregator	クロスリージョン検索集計構成を含む、検索アグリゲータを作成するアクセス許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateInsight	Security Hub でインサイトを作成する許可を付与 インサイトは、関連する結果のコレクションです	書き込み	hub		
CreateMembers	Security Hub でメンバーアカウントを作成する許可を付与	書き込み	hub		
CreateTicketV2	選択した OCSF 検出結果のチケットを作成するアクセス許可を付与します	書き込み	connectorv2		
DeclineInvitations	メンバーアカウントになるための Security Hub の招待を却下する許可を付与	書き込み	hub		
DeleteActionTarget	Security Hub でカスタムアクションを削除する許可を付与	書き込み	hub		
DeleteAggregatorV2	リージョン間でのデータ集約を設定するアaggregatorV2 を削除するアクセス許可を付与します	書き込み	aggregatorv2*		
DeleteAutomationRuleV2	Security Hub で自動化ルール V2 を削除する許可を付与	書き込み	automation-rulev2*		
DeleteConfigurationPolicy	既存の設定ポリシーを削除する許可を付与	書き込み	configuration-policy*		
DeleteConnectorV2	Security Hub でコネクタ V2 を削除する許可を付与	書き込み	connectorv2*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteFindingAggregator	検索アグリゲータを削除するアクセス許可を付与これにより、リージョン間の集約の検索が無効になります。	書き込み	finding-aggregator*		
DeleteInsight	Security Hub からインサイトを削除する許可を付与	書き込み	hub		
DeleteInvitations	メンバーアカウントになるための Security Hub の招待を削除する許可を付与	書き込み	hub		
DeleteMembers	Security Hub のメンバーアカウントを削除する許可を付与	書き込み	hub		
DescribeActionTargets	API を使用してカスタムアクションのリストを取得する許可を付与	読み込み	hub		
DescribeHub	アカウントのハブリソースに関する情報を取得する許可を付与	読み込み	hub		
DescribeOrganizationConfiguration	Security Hub の組織設定を説明する許可を付与	読み込み	hub		
DescribeProducts	利用可能な Security Hub 製品統合に関する情報を取得する許可を付与	読み取り	hub		
DescribeProductsV2	利用可能な Security Hub V2 製品統合に関する情報を取得する許可を付与	読み取り	hubv2		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeSecurityHubV2	アカウントのハブ V2 リソースに関する情報を取得するアクセス許可を付与します	読み取り			
DescribeStandards	Security Hub 標準に関する情報を取得する許可を付与	読み込み	hub		
DescribeStandardsControls	Security Hub 標準コントロールに関する情報を取得する許可を付与	読み込み	hub		
DisableImportFindingsForProduct	Security Hub 統合製品の結果のインポートを無効にする許可を付与	書き込み	hub		
DisableOrganizationAdminAccount	組織の Security Hub 管理者アカウントを削除する許可を付与	書き込み	hub		organizations:DeregisterDelegatedAdministrator organizations:DescribeOrganization organizations:ListDelegatedAdministrators

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisableSecurityHub	Security Hub を無効にする許可を付与	書き込み	hub		
DisableSecurityHubV2	Security Hub V2 を無効にするアクセス許可を付与します	書き込み			
DisassociateFromAdministratorAccount	Security Hub メンバーアカウントに、関連付けられた管理者アカウントとの関連付けを解除する許可を付与	書き込み	hub		
DisassociateFromMasterAccount	Security Hub メンバーアカウントに、関連付けられたマスターアカウントとの関連付けを解除する許可を付与	書き込み	hub		
DisassociateMembers	関連付けられた管理者アカウントから、Security Hub メンバーアカウントの関連付けを解除する許可を付与	書き込み	hub		
EnableImportFindingsForProduct	Security Hub 統合製品の結果のインポートを有効にする許可を付与	書き込み	hub		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
EnableOrganizationAdminAccount	組織の Security Hub 管理者アカウントを指定する許可を付与	書き込み	hub		organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:ListAWSServiceAccessForOrganization organizations:ListDelegatedAdministrators organizations:RegisterDelegatedAdministrator
EnableSecurityHub	Security Hub を有効にする許可を付与	書き込み	hub		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
EnableSecurityHubV2	Security Hub V2 を有効にするアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
GetAdhocInsightResults [アクセス許可のみ]	検出結果に関する集計された統計データを取得するアクセス許可を付与します	読み取り	hub hubv2		
GetAdministratorAccount	Security Hub 管理者アカウントに関する詳細を取得する許可を付与	読み取り	hub		
GetAggregatorV2	リージョン間でのデータ集約を設定する aggregatorV2 の詳細を取得するアクセス許可を付与します	読み取り	aggregatorv2*		
GetAutomationRuleV2	ルール Amazon リソースネーム (ARN) に基づいて Security Hub から自動化ルール V2 の詳細を取得するアクセス許可を付与します	読み取り	automation-rulev2*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetConfigurationPolicy	呼び出し元アカウントが作成した 1 つの設定ポリシーの概要を把握する許可を付与	読み取り	configuration-policy*		
GetConfigurationPolicyAssociation	呼び出し元アカウントの組織のメンバーアカウントまたは組織単位に関連する設定ポリシーに関する情報を取得する許可を付与	読み取り			
GetConnectorV2	コネクタ ID に基づいて Security Hub からコネクタ V2 の詳細を取得する許可を付与	読み取り	connectorv2*		
GetControlFindingSummary [許可のみ]	セキュリティ標準に対する、セキュリティスコアと検出数および制御ステータスのカウントを取得する許可を付与	読み込み	hub		
GetEnabledStandards	Security Hub で有効になっている標準のリストを取得する許可を付与	リスト	hub		
GetFindingAggregator	リージョン間の集計の検索を構成する、検索アグリゲータの詳細を取得するアクセス許可を付与	読み取り	finding-aggregator*		
GetFindingHistory	Security Hub から検出結果履歴のリストを取得する許可を付与	読み取り	hub		
GetFindings	Security Hub から結果のリストを取得する許可を付与	読み込み	hub		
			hubv2		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetFreeTrialEndDate [許可のみ]	アカウントで Security Hub 無料トライアルの終了日を確定する許可を付与	読み込み	hub		
GetFreeTrialUsage [許可のみ]	無料試用期間中の Security Hub の使用状況に関する情報を取得する許可を付与	読み込み	hub		
GetInsightFindingTrend [許可のみ]	グラフを生成するために Security Hub からインサイト検索傾向を取得する許可を付与	読み込み	hub		
GetInsightResults	Security Hub からインサイト結果を取得する許可を付与	読み込み	hub		
GetInsights	Security Hub のインサイトを取得する許可を付与	リスト	hub		
GetInvitationsCount	アカウントに送信されたすべての Security Hub メンバーシップの招待の数を取得する許可を付与	読み込み	hub		
GetMasterAccount	Security Hub マスターアカウントに関する詳細を取得する許可を付与	読み込み	hub		
GetMembers	Security Hub メンバーアカウントの詳細を取得する許可を付与	読み取り	hub		
GetResourcesStatisticsV2	リソースに関する集計統計を取得するアクセス許可を付与します	読み取り	hubv2		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetResourcesV2	リソースのリストを取得するアクセス許可を付与します	読み取り	hubv2		
GetSecurityControlDefinition	ID で識別される特定のセキュリティコントロールに関する詳細を取得する許可を付与	読み取り			securityhub:DescribeStandardsControls
GetUsage [許可のみ]	アカウント別の Security Hub の使用に関する情報を取得する許可を付与	読み取り	hub		
InviteMembers	Security Hub メンバー AWS アカウントに他のアカウントを招待するアクセス許可を付与します	書き込み	hub		
ListAggregatorsV2	リージョン間でのデータ集約を設定するaggregatorsV2 のリストを取得するアクセス許可を付与します	リスト			
ListAutomationRules	Security Hub から、呼び出し元アカウントの自動化ルールとメタデータのリストを取得する許可を付与	リスト			
ListAutomationRulesV2	Security Hub から呼び出し元のアカウントの自動化ルール V2 とそのメタデータのリストを取得するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListConfigurationPolicies	呼び出し元アカウントによって作成されたすべての設定ポリシーの概要を一覧表示する許可を付与	リスト			
ListConfigurationPolicyAssociations	呼び出し元アカウントの組織のすべてのメンバーアカウントと組織単位に関連付けられているすべての設定ポリシーに関する情報を取得する許可を付与	リスト			
ListConnectorsV2	Security Hub から呼び出し元のアカウントのコネクタ V2 とそのメタデータのリストを取得するアクセス許可を付与します	リスト			
ListControlEvaluationSummaries [許可のみ]	コントロール ID、ステータス、検索回数など、標準のコントロールの一覧を取得する許可を付与	読み込み	hub		
ListEnabledProductsForImport	現在有効になっている Security Hub 統合製品を取得する許可を付与	リスト	hub		
ListFindingAggregators	クロスリージョン検索集計設定を含む検索アグリゲータのリストを取得するアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListInvitations	アカウントに送信された Security Hub の招待を取得する許可を付与	リスト	hub		
ListMembers	管理者アカウントに関連付けられている Security Hub メンバーアカウントに関する詳細を取得する許可を付与	リスト	hub		
ListOrganizationAdminAccounts	組織の Security Hub 管理者アカウントを一覧表示する許可を付与	リスト	hub		organizations:DescribeOrganization organizations:ListDelegatedAdministrators
ListSecurityControlDefinitions	セキュリティコントロール定義のリストを取得する許可を付与これには、現在のリージョンにおけるセキュリティコントロールの詳細が含まれます	リスト			
ListStandardsControlAssociations	標準のセキュリティコントロールの有効化ステータスを一覧表示する許可を付与	リスト			securityhub:DescribeStandardsControls

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTagsForResource	リソースに関連付けられているタグのリストにアクセス許可を付与	読み込み	automation-rule		
			configuration-policy		
			hub		
SendFindingEvents [許可のみ]	カスタムアクションを使用して、Security Hub の結果を Amazon EventBridge に送信する許可を付与	読み込み	hub		
SendInsightEvents [許可のみ]	カスタムアクションを使用して、Amazon EventBridge に Security Hub のインサイトを送信する許可を付与	読み取り	hub		
StartConfigurationPolicyAssociation	設定ポリシーを、呼び出し元アカウントの組織内のメンバーアカウントまたは組織単位に関連付ける許可を付与	書き込み	configuration-policy		
StartConfigurationPolicyDisassociation	呼び出し元アカウントの組織内のメンバーアカウントまたは組織単位から設定ポリシーの関連付けを削除する許可を付与	書き込み	configuration-policy		
TagResource	Security Hub リソースにタグを追加する許可を付与	タグ付け	aggregatorv2		
			automation-rule		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			automation-rulev2		
			configuration-policy		
			connectorv2		
			hub		
			hubv2		
UntagResource	Security Hub リソースからタグを削除する許可を付与	タグ付け	aggregatorv2		
			automation-rule		
			automation-rulev2		
			configuration-policy		
			connectorv2		
			hub		
			hubv2		
UpdateActionTarget	Security Hub でカスタムアクションを更新する許可を付与	書き込み	hub		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateAggregatorV2	リージョン間でのデータ集約を設定するアaggregatorV2 を更新するアクセス許可を付与します	書き込み	aggregatorv2*		
UpdateAutomationRuleV2	ルール Amazon リソースネーム (ARN) と入力パラメータに基づいて Security Hub の自動化ルール V2 を更新する許可を付与	書き込み	automation-rulev2*		
UpdateConfigurationPolicy	既存の設定ポリシーを更新する許可を付与	書き込み	configuration-policy*		
UpdateConnectorV2	コネクタ ID と入力パラメータに基づいて Security Hub のコネクタ V2 を更新する許可を付与	書き込み	connectorv2*		
UpdateFindingAggregator	クロスリージョン検索集計構成を含む、検索アグリゲータを更新するアクセス許可を付与	書き込み	finding-aggregator*		
UpdateFindings	Security Hub の結果を更新する許可を付与	書き込み	hub		
UpdateInsight	Security Hub でインサイトを更新する許可を付与	書き込み	hub		
UpdateOrganizationConfiguration	Security Hub の組織設定を更新する許可を付与	書き込み	hub		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateSecurityControl	ID または ARN で識別される特定のセキュリティコントロールのプロパティを更新する許可を付与	書き込み			securityhub:UpdateStandardsControl
UpdateSecurityHubConfiguration	Security Hub の設定を更新する許可を付与	書き込み	hub		
UpdateStandardsControl	Security Hub 標準コントロールを更新する許可を付与	書き込み	hub		

AWS Security Hub で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
hub	arn:${Partition}:securityhub:${Region}:${Account}:hub/default	aws:ResourceTag/${TagKey}
hubv2	arn:${Partition}:securityhub:${Region}:${Account}:hubv2/${HubV2Id}	aws:ResourceTag/${TagKey}
product	arn:${Partition}:securityhub:${Region}:${Account}:product/${Company}/${ProductId}	

リソースタイプ	ARN	条件キー
finding-aggregator	arn:${Partition}:securityhub:${Region}:${Account}:finding-aggregator/${FindingAggregatorId}	
aggregatorv2	arn:${Partition}:securityhub:${Region}:${Account}:aggregatorv2/${AggregatorV2Id}	aws:ResourceTag/${TagKey}
automation-rule	arn:${Partition}:securityhub:${Region}:${Account}:automation-rule/${AutomationRuleId}	aws:ResourceTag/${TagKey}
automation-rulev2	arn:${Partition}:securityhub:${Region}:${Account}:automation-rulev2/${AutomationRuleV2Id}	aws:ResourceTag/${TagKey}
configuration-policy	arn:${Partition}:securityhub:${Region}:${Account}:configuration-policy/${ConfigurationPolicyId}	aws:ResourceTag/${TagKey}
connectorv2	arn:${Partition}:securityhub:${Region}:${Account}:connectorv2/${ConnectorV2Id}	aws:ResourceTag/${TagKey}

AWS Security Hub の条件キー

AWS Security Hub では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーおよび値のペアのプレゼンスに基づいてアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアに基づいてアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいたアクションでアクセスをフィルタリングします	ArrayOfString
securityhub:ASFFSyntaxPath/${ASFFSyntaxPath}	リクエスト内の特定のフィールドおよび値の存在に基づいてアクセスをフィルタリングします	String
securityhub:OCSFSyntaxPath/${OCSFSyntaxPath}	リクエスト内の特定のフィールドおよび値の存在に基づいてアクセスをフィルタリングします。	String
securityhub:TargetAccount	リクエストで指定された AwsAccountId フィールドによってアクセスをフィルタリングします	String

AWS セキュリティインシデント対応のアクション、リソース、および条件キー

AWS セキュリティインシデント対応 (サービスプレフィックス: `security-ir`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS セキュリティインシデント対応で定義されるアクション
- AWS Security Incident Response で定義されるリソースタイプ
- AWS セキュリティインシデント対応の条件キー

AWS セキュリティインシデント対応で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchGetMemberAccountDetails	メンバーアカウントの詳細をバッチで取得するアクセス許可を付与します	読み取り	membership*		
CancelMembership	メンバーシップをキャンセルするアクセス許可を付与します	書き込み	membership*		
CloseCase	ケースをクローズするアクセス許可を付与します	書き込み	case*		
CreateCase	ケースを作成するアクセス許可を付与します	書き込み	case*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateCaseComment	ケースコメントを作成するアクセス許可を付与します	書き込み	case*		
CreateMembership	メンバーシップを作成するアクセス許可を付与します	書き込み	membership*		iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:ListDelegatedAdministrators
				aws:RequestTag/${TagKey} aws:TagKeys	
GetCase	ケースを取得するアクセス許可を付与します	読み取り	case*		
GetCaseAttachmentDownloadUrl	ケースアタッチメントのダウンロード URL を取得するアクセス許可を付与します	読み取り	case*		
GetCaseAttachmentUploadUrl	ケース添付ファイルのアップロード URL を取得するアクセス許可を付与します	書き込み	case*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetMembership	メンバーシップを取得するアクセス許可を付与します	読み取り	membership*		
ListCaseEdits	ケース編集を一覧表示するアクセス許可を付与します	読み取り	case*		
ListCases	ケースを一覧表示するアクセス許可を付与します	リスト			
ListComments	ケースコメントを一覧表示するアクセス許可を付与します	読み取り	case*		
ListMemberships	メンバーシップを一覧表示するアクセス許可を付与します	リスト			
ListTagsForResource	指定されたリソースにアタッチされているタグを一覧表示する許可を付与	読み取り	case		
			membership		
				aws:ResourceTag/${TagKey} aws:TagKeys	
TagResource	指定されたリソースにタグを追加するための許可を付与します	Tagging	case		
			membership		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	指定されたリソースからタグを削除するための許可を付与します	Tagging	case		
			membership		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCase	ケースを更新するアクセス許可を付与します	書き込み	case*		
UpdateCaseComment	ケースコメントを更新するアクセス許可を付与します	書き込み	case*		
UpdateCaseStatus	ケースステータスを更新するアクセス許可を付与します	書き込み	case*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateMembership	メンバーシップを更新するアクセス許可を付与します	書き込み	membership*		iam:CreateServiceLinkedRole organizations:DescribeOrganizationalUnit
UpdateResolverType	ケースリゾルバータイプを更新する許可を付与	書き込み	case*		

AWS Security Incident Response で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
case	arn:${Partition}:security-ir:${Region}:${Account}:case/${CaseId}	aws:ResourceTag/${TagKey}
membership	arn:${Partition}:security-ir:${Region}:${Account}:membership/${MembershipId}	aws:ResourceTag/${TagKey}

AWS セキュリティインシデント対応の条件キー

AWS セキュリティインシデント対応では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon Security Lake のアクション、リソース、および条件キー

Amazon Security Lake (サービスプレフィックス: securitylake) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Security Lake で定義されるアクション

- Amazon Security Lake で定義されるリソースタイプ
- Amazon Security Lake の条件キー

Amazon Security Lake で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateAwsLogSource	信頼できる組織に属するアカウントまたはスタンドアロンアカウントに、あらゆる地域のあらゆるソースタイプを有効にする許可を付与	書き込み	data-lake*		glue:CreateDatabase glue:CreateTable glue:GetDatabase glue:GetTable iam:CreateServiceLinkedRole kms:CreateGrant kms:DescribeKey
CreateCustomLogSource	カスタムソースを追加する許可を付与	書き込み	data-lake*		glue:CreateCrawler glue:CreateDatabase

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					glue:CreateTable glue:StartCrawlerSchedule iam:DeleteRolePolicy iam:GetRole iam:PassRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey kms:GenerateDataKey lakeformation:GrantPermissions

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					lakeformation:RegisterResource s3:ListBucket s3:PutObject

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateDataLake	新しいセキュリティデータレイクを作成する許可を付与	書き込み	data-lake*		events:PutRule events:PutTargets iam:CreateServiceLinkedRole iam:DeleteRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:PassRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey lakeformation:GetD

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					ataLakeSettings lakeformation:PutDataLakeSettings lambda:AddPermission lambda:CreateEventSourceMapping lambda:CreateFunction organizations:DescribeOrganization organizations:ListAccounts organizations:ListDelegatedServicesForAccount

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					s3:CreateBucket s3:GetObject s3:GetObjectVersion s3:ListBucket s3:PutBucketPolicy s3:PutBucketPublicAccessBlock s3:PutBucketVersioning sqs:CreateQueue sqs:GetQueueAttributes sqs:SetQueueAttributes

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataLakeExceptionSubscription	例外に関する即時通知を取得する許可を付与。例外通知用の SNS トピックをサブスクライブします	書き込み			
CreateDataLakeOrganizationConfiguration	組織内の新しいメンバーアカウントのために Amazon Security Lake を自動的に有効にする許可を付与	書き込み	data-lake*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateSubscriber	サブスクライバーを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:CreateRole iam:DeleteRolePolicy iam:GetRole iam:PutRolePolicy lakeformation:GrantPermissions lakeformation:ListPermissions lakeformation:RegisterResource lakeformation:RevokePermissions ram:GetResourceSha

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					reAssociations ram:GetResourceShares ram:UpdateResourceShare s3:PutObject

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSubscriberNotification	データレイクに新しいデータがあるときにクライアントに通知するウェブフック呼び出しを作成する許可を付与	書き込み	subscriber*		events:CreateApiDestination events:CreateConnection events:DescribeRule events:ListApiDestinations events:ListConnections events:PutRule events:PutTargets iam:DeleteRolePolicy iam:GetRole iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					s3:GetBucketNotification s3:PutBucketNotification sqs:CreateQueue sqs:DeleteQueue sqs:GetQueueAttributes sqs:GetQueueUrl sqs:SetQueueAttributes
DeleteAwsLogSource	信頼できる組織に属するアカウントまたはスタンドアロンアカウントに、あらゆる地域のあらゆるソースタイプを無効にする許可を付与	書き込み	data-lake*		
DeleteCustomLogSource	カスタムソースを削除する許可を付与	書き込み	data-lake*		glue:StopCrawlerSchedule

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteDataLake	すべてのセキュリティデータレイクを削除する許可を付与	書き込み	data-lake*		organizations:DescribeOrganization organizations:ListDelegatedAdministrators organizations:ListDelegatedServicesForAccount
DeleteDataLakeExceptionSubscription	例外通知用の SNS トピックの購読を解除する許可を付与 SNS トピックの例外通知を削除します	書き込み			
DeleteDataLakeOrganizationConfiguration	新しい組織アカウントのために Amazon Security Lake アクセスの自動有効化を削除する許可を付与	書き込み	data-lake*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteSubscriber	指定されたサブスクライバーを削除する許可を付与	書き込み	subscriber*		events:DeleteApiDestination events:DeleteConnection events:DeleteRule events:DescribeRule events:ListApiDestinations events:ListTargetsByRule events:RemoveTargets iam:DeleteRole iam:DeleteRolePolicy

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					iam:GetRole iam:ListRolePolicies lakeformation:ListPermissions lakeformation:RevokePermissions sqs:DeleteQueue sqs:GetQueueUrl

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteSubscriberNotification	データレイクに新しいデータがあるときにクライアントに通知するウェブフック呼び出しを削除する許可を付与	書き込み	subscriber*		events:DeleteApiDestination events:DeleteConnection events:DeleteRule events:DescribeRule events:ListApiDestinations events:ListTargetsByRule events:RemoveTargets iam:DeleteRole iam:DeleteRolePolicy

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					iam:GetRole iam:ListRolePolicies lakeformation:RevokePermissions sqs:DeleteQueue sqs:GetQueueUrl
DeregisterDataLakeDelegatedAdministrator	委任管理者アカウントを削除し、この組織のサービスとしての Amazon Security Lake を無効にする許可を付与	書き込み			organizations:DeregisterDelegatedAdministrator organizations:DescribeOrganization organizations:ListDelegatedServicesForAccount

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetDataLakeExceptionSubscription	例外通知の SNS トピックをサブスクライブしたときに提供されたプロトコルとエンドポイントをクエリする許可を付与	読み取り			
GetDataLakeOrganizationConfiguration	新しい組織アカウント用に Amazon Security Lake アクセスを自動的に有効にするための組織の構成設定を取得する許可を付与する	読み取り	data-lake*		organizations:DescribeOrganization
GetDataLakeSources	現在のリージョンのセキュリティデータレイクの静的スナップショットを取得する許可を付与 スナップショットには有効なアカウントとログソースが含まれます	読み取り	data-lake*		
GetSubscriber	既に作成されているサブスクライバーに関する情報を取得する許可を付与	読み取り	subscriber*		
ListDataLakeExceptions	再試行できないすべてのエラーのリストを取得する許可を付与	リスト			
ListDataLakes	セキュリティデータレイクに関する情報を一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListLogSources	有効なアカウントを表示する許可を付与。有効なリージョンで有効なソースを表示できます	リスト			
ListSubscribers	すべてのサブスクライバーを一覧表示する許可を付与	リスト			
ListTagsForResource	リソースのすべてのタグを一覧表示するための許可を付与します	リスト	data-lake		
			subscriber		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RegisterDataLakeDelegatedAdministrator	あるアカウントを、組織の Amazon Security Lake 管理者アカウントとして指定する許可を付与	書き込み			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators organizations:ListDelegatedServicesForAccount organizations:RegisterDelegatedAdministrator
TagResource	リソースにタグを追加するための許可を付与します	Tagging	data-lake		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			subscriber		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除するための許可を付与します	Tagging	data-lake		
			subscriber		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateDataLake	セキュリティデータレイクを更新する許可を付与	書き込み	data-lake*		events:PutRule events:PutTargets iam:CreateServiceLinkedRole iam:DeleteRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:PutRolePolicy kms:CreateGrant kms:DescribeKey lakeformation:GetDataLakeSettings

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					lakeformation:PutDataLakeSettings lambda:AddPermission lambda:CreateEventSourceMapping lambda:CreateFunction organizations:DescribeOrganization organizations:ListDelegatedServicesForAccount s3:CreateBucket s3:GetObject

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					s3:GetObjectVersion s3:ListBucket s3:PutBucketPolicy s3:PutBucketPublicAccessBlock s3:PutBucketVersioning sqs:CreateQueue sqs:GetQueueAttributes sqs:SetQueueAttributes
UpdateDataLakeExceptionSubscription	例外通知用の SNS トピックのサブスクリプションを更新する許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateSubscriber	サブスクライバーを更新する許可を付与	書き込み	subscriber*		events:CreateApiDestination events:CreateConnection events:DescribeRule events:ListApiDestinations events:ListConnections events:PutRule events:PutTargets iam:DeleteRolePolicy iam:GetRole iam:PutRolePolicy

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateSubscriberNotification	データレイクに新しいデータがあるときにクライアントに通知するウェブフック呼び出しを更新する許可を付与	書き込み	subscriber*		events:CreateApiDestination events:CreateConnection events:DescribeRule events:ListApiDestinations events:ListConnections events:PutRule events:PutTargets iam:CreateServiceLinkedRole iam:DeleteRolePolicy

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					iam:GetRole iam:PassRole iam:PutRolePolicy s3:CreateBucket s3:GetBucketNotification s3:ListBucket s3:PutBucketNotification s3:PutBucketPolicy s3:PutBucketPublicAccessBlock s3:PutBucketVersioning

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					s3:PutLifecycleConfiguration sqs:CreateQueue sqs:DeleteQueue sqs:GetQueueAttributes sqs:GetQueueUrl sqs:SetQueueAttributes

Amazon Security Lake で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
data-lake	arn:${Partition}:securitylake:${Region}:${Account}:data-lake/default	aws:RequestTag/${TagKey}

リソースタイプ	ARN	条件キー
		aws:ResourceTag/${TagKey}
subscriber	arn:${Partition}:securitylake:${Region}:${Account}:subscriber/${SubscriberId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}

Amazon Security Lake の条件キー

Amazon Security Lake は、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストで渡されたタグによりアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーによりアクセスをフィルタリングします	ArrayOfString

AWS Server Migration Service のアクション、リソース、および条件キー

AWS Server Migration Service (サービスプレフィックス: sms) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Server Migration Service で定義されるアクション
- AWS Server Migration Service で定義されるリソースタイプ
- AWS Server Migration Service の条件キー

AWS Server Migration Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateApp	オンプレミスアプリケーションを に移行するアプリケーション設定を作成するアクセス許可を付与します AWS	書き込み			
CreateReplicationJob	オンプレミスサーバーを に移行するジョブを作成するアクセス許可を付与します AWS	書き込み			
DeleteApp	既存のアプリケーション設定を削除する許可を付与	Write			
DeleteAppLaunchConfiguration	既存のアプリケーションの起動設定を削除する許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteAppReplicationConfiguration	既存のアプリケーションのレプリケーション設定を削除する許可を付与	Write			
DeleteAppValidationConfiguration	既存のアプリケーションの検証設定を削除する許可を付与	書き込み			
DeleteReplicationJob	オンプレミスサーバーを に移行する既存のジョブを削除するアクセス許可を付与しますAWS	書き込み			
DeleteServerCatalog	に収集されたオンプレミスサーバーの完全なリストを削除するアクセス許可を付与します AWS	書き込み			
DisassociateConnector	関連付けられているコネクタの関連付けを解除する許可を付与	Write			
GenerateChangeSet	アプリケーションのCloudFormation スタックのchangeSet を生成する許可を付与	Write			
GenerateTemplate	既存のアプリケーションのCloudFormation テンプレートを生成する許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetApp	既存のアプリケーションの設定とステータスを取得する許可を付与	Read			
GetAppLaunchConfiguration	既存のアプリケーションの起動設定を取得する許可を付与	Read			
GetAppReplicationConfiguration	既存のアプリケーションのレプリケーション設定を取得する許可を付与	Read			
GetAppValidationConfiguration	既存のアプリケーションの検証設定を取得する許可を付与	Read			
GetAppValidationOutput	アプリケーション検証スクリプトから送信された通知を取得する許可を付与	Read			
GetConnectors	関連付けられているすべてのコネクタを取得する許可を付与	Read			
GetMessages [許可のみ]	AWS Server Migration Service から Server Migration Connector にメッセージを取得するアクセス許可を付与します	読み取り			
GetReplicationJobs	オンプレミスサーバーを移行する既存のすべてのジョブを取得するアクセス許可を付与します AWS	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetReplicationRuns	既存のジョブのすべての実行を取得する許可を付与	Read			
GetServers	インポートされたすべてのサーバーを取得する許可を付与	読み取り			
ImportAppCatalog	AWS Application Discovery Service からアプリケーションカタログをインポートする許可を付与	書き込み			
ImportServerCatalog	オンプレミスサーバーの完全なリストを収集する許可を付与	Write			
LaunchApp	既存のアプリケーションの CloudFormation スタックを作成して起動する許可を付与	Write			
ListApps	既存のアプリケーションのサマリーの一覧を取得する許可を付与	リスト			
NotifyAppValidationOutput	アプリケーション検証スクリプトの通知を送信する許可を付与	Write			
PutAppLaunchConfiguration	既存のアプリケーションの起動設定を作成または更新する許可を付与	Write			
PutAppReplicationConfiguration	既存のアプリケーションのレプリケーション設定を作成または更新する許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutAppValidationConfiguration	既存のアプリケーションの検証設定を配置する許可を付与	Write			
SendMessage [アクセス許可のみ]	Server Migration Connector から AWS Server Migration Service にメッセージを送信する許可を付与	書き込み			
StartAppReplication	既存のアプリケーションのレプリケーションジョブを作成および開始する許可を付与	Write			
StartOnDemandAppReplication	既存のアプリケーションのレプリケーション実行を開始する許可を付与	Write			
StartOnDemandReplicationRun	既存のレプリケーションジョブに対するレプリケーションの実行を開始する許可を付与	Write			
StopAppReplication	既存のアプリケーションのレプリケーションジョブを停止して削除する許可を付与	Write			
TerminateApp	既存のアプリケーションの CloudFormation スタックを終了する許可を付与	Write			
UpdateApp	既存のアプリケーション設定を更新する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateReplicationJob	オンプレミスサーバーを に移行する既存のジョブを更新するアクセス許可を付与します AWS	書き込み			

AWS Server Migration Service で定義されるリソースタイプ

AWS Server Migration Service は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Server Migration サービスへのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Server Migration Service の条件キー

ServerMigrationService には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Serverless Application Repository のアクション、リソース、および条件キー

AWS Serverless Application Repository (サービスプレフィックス: `serverlessrepo`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Serverless Application Repository で定義されるアクション

- AWS Serverless Application Repository で定義されるリソースタイプ
- AWS Serverless Application Repository の条件キー

AWS Serverless Application Repository で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateApplication	アプリケーションを作成するアクセス許可を付与します AWS 。オプションで SAM ファイルを含めて、同じ呼び出しで最初のアプリケーションバージョンを作成します。	書き込み			
CreateApplicationVersion	アプリケーションのバージョンを作成するアクセス許可を付与	書き込み	applications*		
CreateCloudFormationChangeSet	特定のアプリケーションの AWS CloudFormation ChangeSet を作成するアクセス許可を付与します	書き込み	applications*		
				serverlessrepo:applicationType	
CreateCloudFormationTemplate	AWS CloudFormation テンプレートを作成する許可を付与	書き込み	applications*		
				serverlessrepo:applicationType	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteApplication	指定されたアプリケーションを削除する許可を付与	書き込み	applications*		
GetApplication	指定されたアプリケーションを取得するアクセス許可を付与	読み取り	applications*		
				serverlessrepo:applicationType	
GetApplicationPolicy	指定されたアプリケーションのポリシーを取得するアクセス許可を付与	読み取り	applications*		
GetCloudFormationTemplate	指定された AWS CloudFormation テンプレートを取得するアクセス許可を付与します	読み取り	applications*		
ListApplicationDependencies	包含するアプリケーション内にネストされているアプリケーションのリストを取得するアクセス許可を付与	リスト	applications*		
				serverlessrepo:applicationType	
ListApplicationVersions	リクエスタが所有している、指定されたアプリケーションのバージョンを一覧表示するアクセス許可を付与	リスト	applications*		
				serverlessrepo:applicationType	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListApplications	リクエスタが所有しているアプリケーションを一覧表示するアクセス許可を付与	リスト			
PutApplicationPolicy	指定されたアプリケーションのポリシーを配置するアクセス許可を付与	書き込み	applications*		
SearchApplications	このユーザー向けに認証されたすべてのアプリケーションを取得するアクセス許可を付与	読み取り		serverlessrepo:applicationType	
UnshareApplication	指定されたアプリケーションの共有を解除するアクセス許可を付与	書き込み	applications*		
UpdateApplication	アプリケーションのメタデータを更新するアクセス許可を付与	書き込み	applications*		

AWS Serverless Application Repository で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
applications	arn:${Partition}:serverlessrepo:${Region}:${Account}:applications/${ResourceId}	

AWS Serverless Application Repository の条件キー

AWS サーバーレスアプリケーションリポジトリは、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
serverlessrepo:applicationType	アプリケーションタイプでアクセスをフィルタリングします	String

AWS サービス - Oracle Database@ のアクション、リソース、および条件キーAWS

AWS サービス - Oracle Database@AWS （ サービスプレフィックス: odb) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Service - Oracle Database@ で定義されるアクションAWS
- AWS サービスで定義されるリソースタイプ - Oracle Database@AWS
- AWS サービスの条件キー - Oracle Database@AWS

AWS Service - Oracle Database@ で定義されるアクションAWS

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptMarketplaceRegistration	Amazon Web Services アカウントの Amazon Web Services Marketplace トークンを登録して Oracle Database@Amazon Web Services サブスクリプションをアクティブ化するアクセス許可を付与します	書き込み			
CreateCloudAutonomousVmCluster	指定された Exadata インフラストラクチャに新しい Autonomous VM クラスターを作成するアクセス許可を付与します	書き込み	cloud-exadata-infrastructure*		
			odb-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateCloudExadataInfrastructure	Exadata インフラストラクチャを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudVmCluster	指定された Exadata インフラストラクチャに VM クラスターを作成するアクセス許可を付与します	書き込み	cloud-exadata-infrastructure*		
			odb-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDbNode [アクセス許可のみ]	DB ノードを作成するアクセス許可を付与します	書き込み	db-node*		
CreateOdbNetwork	ODB ネットワークを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateOdbPeeringConnection	ODB ピアリング接続を作成するアクセス許可を付与します	書き込み	odb-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOutboundIntegration [アクセス許可のみ]	アウトバウンド統合を作成するアクセス許可を付与します	書き込み	cloud-autonomous-vm-cluster*		
			cloud-vm-cluster*		
DeleteCloudAutonomousVmCluster	自律 VM クラスターを削除するアクセス許可を付与します	書き込み	cloud-autonomous-vm-cluster*		
DeleteCloudExadataInfrastructure	指定された Exadata インフラストラクチャを削除するアクセス許可を付与します。このオペレーションを使用する前に、この Exadata インフラストラクチャでホストされているすべての VM クラスターを削除してください。	書き込み	cloud-exadata-infrastructure*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteCloudVmCluster	指定された VM クラスターを削除するアクセス許可を付与します	書き込み	cloud-vm-cluster*		
DeleteDbNode [アクセス許可のみ]	DB ノードを削除するアクセス許可を付与します	書き込み	db-node*		
DeleteOdbNetwork	指定された ODB ネットワークを削除するアクセス許可を付与します	書き込み	odb-network*		
DeleteOdbPeeringConnection	指定された ODB ピア接続を削除するアクセス許可を付与します。ODB ピアリング接続を削除すると、基盤となる VPC ピアリング接続も削除されます。	書き込み	odb-peering-connection*		
DeleteResourcePolicy [アクセス許可のみ]	リソースポリシーを削除する許可を付与。	書き込み	cloud-exadata-infrastructure*		
			odb-network*		
GetCloudAutonomousVmCluster	特定の自律 VM クラスターに関する情報を取得するアクセス許可を付与します	読み取り	cloud-autonomous-vm-cluster*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetCloudExadataInfrastructure	指定された Exadata インフラストラクチャに関する情報を取得するアクセス許可を付与します	読み取り	cloud-exadata-infrastructure*		
GetCloudExadataInfrastructureUnallocatedResources	指定された Cloud Exadata インフラストラクチャ内の未割り当てリソースに関する情報を取得するアクセス許可を付与します	読み取り	cloud-exadata-infrastructure*		
GetCloudVmCluster	指定された VM クラスターに関する情報を取得するアクセス許可を付与します	読み取り	cloud-vm-cluster*		
GetDbNode	指定された DB ノードに関する情報を取得するアクセス許可を付与します	読み取り	cloud-vm-cluster*		
			db-node*		
GetDbServer	指定されたデータベースサーバーに関する情報を取得するアクセス許可を付与します	読み取り	cloud-exadata-infrastructure*		
GetOciOnboardingStatus	Amazon Web Services アカウントのテナンシーアクティベーションリンクとオンボーディングステータスを取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetOdbNetwork	指定された ODB ネットワークに関する情報を取得するアクセス許可を付与します	読み取り	odb-network*		
GetOdbPeeringConnection	指定された ODB ピアリング接続に関する情報を取得するアクセス許可を付与します	読み取り	odb-peering-connection*		
GetResourcePolicy [許可のみ]	リソースポリシーを取得する許可の付与	読み取り	cloud-exadata-infrastructure*		
			odb-network*		
InitializeService	アカウントで初めて ODB サービスを初期化するアクセス許可を付与します	書き込み			
ListAutonomousVirtualMachines	Autonomous VMs クラスター内のすべての Autonomous VM を一覧表示する許可を付与	読み取り	cloud-autonomous-vm-cluster		
ListCloudAutonomousVmClusters	指定された Cloud Exadata インフラストラクチャ内のすべての自律 VM クラスターを一覧表示する許可を付与	リスト	cloud-exadata-infrastructure		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListCloudExadataInfrastructures	Amazon Web Services アカウントが所有する Exadata インフラストラクチャに関する情報を一覧表示する許可を付与	リスト			
ListCloudVmClusters	Amazon Web Services アカウントが所有する VM クラスター、または指定された Exadata インフラストラクチャ上の VM クラスターのみに関する情報を一覧表示するアクセス許可を付与します	リスト	cloud-exadata-infrastructure		
ListDbNodes	指定された VM クラスターの DB ノードに関する情報を一覧表示するアクセス許可を付与します	リスト	cloud-vm-cluster*		
ListDbServers	指定された Exadata インフラストラクチャに属するデータベースサーバーに関する情報を一覧表示するアクセス許可を付与します	読み取り	cloud-exadata-infrastructure*		
ListDbSystemShapes	Exadata インフラストラクチャで使用できるシェイプに関する情報を一覧表示するアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListGiVersions	指定されたシェイプの VM クラスターで使用できる Oracle Grid Infrastructure (GI) ソフトウェアバージョンに関する情報を一覧表示するアクセス許可を付与します	読み取り			
ListOdbNetworks	Amazon Web Services アカウントが所有する ODB ネットワークに関する情報を一覧表示するアクセス許可を付与します	リスト			
ListOdbPeeringConnections	すべての ODB ピアリング接続または特定の ODB ネットワークに関連付けられている接続を一覧表示するアクセス許可を付与します	リスト	odb-network		
ListSystemVersions	指定された giVersion とシェイプの VM クラスターで使用できるシステムバージョンに関する情報を一覧表示するアクセス許可を付与します	読み取り			
ListTagsForResource	このリソースに適用されたタグに関する情報を一覧表示するアクセス許可を付与します	読み取り	cloud-autonomous-vm-cluster		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			cloud-exadata-infrastructure		
			cloud-vm-cluster		
			db-node		
			odb-network		
			odb-peering-connection		
				aws:ResourceTag/${TagKey}	
PutResourcePolicy [許可のみ]	リソースポリシーを更新する許可を付与。	書き込み	cloud-exadata-infrastructure*		
			odb-network*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RebootDbNode	VM クラスター内の指定された DB ノードを再起動するアクセス許可を付与します	書き込み	cloud-vm-cluster*		
			db-node*		
StartDbNode	VM クラスターで指定された DB ノードを起動するアクセス許可を付与します	書き込み	cloud-vm-cluster*		
			db-node*		
StopDbNode	VM クラスター内の指定された DB ノードを停止する許可を付与	書き込み	cloud-vm-cluster*		
TagResource	指定されたリソースにタグを適用するアクセス許可を付与します	Tagging	cloud-autonomous-vm-cluster		
			cloud-exadata-infrastructure		
			cloud-vm-cluster		
			db-node		
			odb-network		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			odb-peering-connection		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	指定されたリソースからタグを削除するための許可を付与します	Tagging	cloud-autonomous-vm-cluster		
			cloud-exadata-infrastructure		
			cloud-vm-cluster		
			db-node		
			odb-network		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			odb-peering-connection		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCloudExadataInfrastructure	Exadata インフラストラクチャリソースのプロパティを更新する許可を付与	書き込み	cloud-exadata-infrastructure*		
UpdateOdbNetwork	指定された ODB ネットワークのプロパティを更新する許可を付与	書き込み	odb-network*		

AWS サービスで定義されるリソースタイプ - Oracle Database@AWS

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
cloud-autonomous-vm-cluster	arn:${Partition}:odb:${Region}:${Account}:cloud-autonomous-vm-cluster/${CloudAutonomousVmClusterId}	aws:ResourceTag/${TagKey}
cloud-exadata-infrastructure	arn:${Partition}:odb:${Region}:${Account}:cloud-exadata-infrastructure/${CloudExadataInfrastructureId}	aws:ResourceTag/${TagKey}
cloud-vm-cluster	arn:${Partition}:odb:${Region}:${Account}:cloud-vm-cluster/${CloudVmClusterId}	aws:ResourceTag/${TagKey}
db-node	arn:${Partition}:odb:${Region}:${Account}:db-node/${DbNodeId}	aws:ResourceTag/${TagKey}
odb-network	arn:${Partition}:odb:${Region}:${Account}:odb-network/${OdbNetworkId}	aws:ResourceTag/${TagKey}
odb-peering-connection	arn:${Partition}:odb:${Region}:${Account}:odb-peering-connection/${OdbPeeringConnectionId}	aws:ResourceTag/${TagKey}

AWS サービスの条件キー - Oracle Database@AWS

AWS サービス - Oracle Database@ は、IAM ポリシーの Condition要素で使用できる以下の条件キーAWS を定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString

AWS Service Catalog のアクション、リソース、および条件キー

AWS Service Catalog (サービスプレフィックス: `servicecatalog`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Service Catalog で定義されるアクション
- AWS Service Catalog で定義されるリソースタイプ
- AWS Service Catalog の条件キー

AWS Service Catalog で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AcceptPortfolioShare	既に共有しているポートフォリオを受け入れるアクセス許可を付与	書き込み	Portfolio*		
AssociateAttributeGroup	属性グループをアプリケーションに関連付けるためのアクセス権限を付与	書き込み	Application*		
			AttributeGroup*		
AssociateBudgetWithResource	予算をリソースに関連付けるアクセス許可を付与	書き込み			
AssociatePrincipalWithPortfolio	IAM プリンシパルをポートフォリオに関連付けるアクセス許可を付与し、指定されたポートフォリオに関連付けられたすべての製品へのアクセスを指定されたプリンシパルに付与	書き込み	Portfolio*		
AssociateProductWithPortfolio	製品をポートフォリオに関連付けるアクセス許可を付与	書き込み			
AssociateResource	リソースをアプリケーションに関連付けるためのアクセス権限を付与	書き込み	Application*		cloudformation:DescribeStacks resource-groups:CreateGroup

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					resource-groups:GetGroup resource-groups:Tag
				servicecatalog:ResourceType servicecatalog:Resource	
AssociateServiceActionWithProvisioningArtifact	アクションをプロビジョニングアーティファクトに関連付けるアクセス許可を付与	書き込み	Product*		
AssociateTagOptionWithResource	指定された TagOption を指定されたポートフォリオまたは製品に関連付けるアクセス許可を付与	書き込み	Portfolio Product		
BatchAssociateServiceActionWithProvisioningArtifact	複数のセルフサービスアクションをプロビジョニングアーティファクトに関連付けるアクセス許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchDisassociateServiceActionFromProvisioningArtifact	セルフサービスアクションのバッチを指定されたプロビジョニングアーティファクトから関連付けを解除する許可を付与	書き込み			
CopyProduct	指定されたソース製品を、指定されたターゲット製品または新しい製品にコピーする許可を付与	書き込み			
CreateApplication	アプリケーションを作成する許可を付与	書き込み	Application*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAttributeGroup	属性グループを作成する許可を付与	書き込み	AttributeGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateConstraint	関連する製品およびポートフォリオに制約を作成する許可を付与	書き込み	Product*		
CreatePortfolio	ポートフォリオを作成する許可を付与	書き込み	Portfolio*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePortfolioShare	所有しているポートフォリオを別の と共有するためのアクセス許可を付与します AWS アカウント	権限の管理	Portfolio*		
CreateProduct	製品とその製品の最初のプロビジョニングアーティファクトを作成する許可を付与	書き込み	Product*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateProvisionedProductPlan	プロビジョニングされた新しい製品プランを追加する許可を付与	書き込み		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
CreateProvisioningArtifact	既存の製品に新しいプロビジョニングアーティファクトを追加する許可を付与	書き込み	Product*		
CreateServiceAction	セルフサービスアクションを作成する許可を付与	書き込み			
CreateTagOption	TagOption を作成する許可を付与	書き込み			
DeleteApplication	アプリケーションからすべての関連付けが削除された場合、アプリケーションを削除する許可を付与	書き込み	Application*		
DeleteAttributeGroup	すべての関連付けが属性グループから削除された場合、属性グループを削除する許可を付与	書き込み	AttributeGroup*		
DeleteConstraint	関連する製品およびポートフォリオから既存の制約を削除する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeletePortfolio	すべての関連付けや共有がポートフォリオから削除されている場合は、ポートフォリオを削除する許可を付与	書き込み	Portfolio*		
DeletePortfolioShare	AWS アカウント 以前にポートフォリオを共有した から所有しているポートフォリオの共有を解除するアクセス許可を付与します	権限の管理	Portfolio*		
DeleteProduct	すべての関連付けが製品から削除された場合は、製品を削除する許可を付与	書き込み	Product*		
DeleteProvisionedProductPlan	プロビジョニング済み製品プランを削除する許可を付与	書き込み		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DeleteProvisioningArtifact	製品からプロビジョニングアーティファクトを削除する許可を付与	書き込み	Product*		
DeleteResourcePolicy [アクセス許可のみ]	指定されたリソースのリソースベースのポリシーを削除する許可を付与する	書き込み	Application		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			Attribute Group		
DeleteServiceAction	セルフサービスアクションを削除する許可を付与	書き込み			
DeleteTagOption	指定された TagOption を削除する許可を付与。	書き込み			
DescribeConstraint	制約を記述する許可を付与	読み込み			
DescribeCopyProductStatus	指定されたコピー製品オペレーションのステータスを取得する許可を付与	読み込み			
DescribePortfolio	ポートフォリオを記述する許可を付与	読み込み	Portfolio*		
DescribePortfolioShareStatus	指定されたポートフォリオ共有オペレーションのステータスを取得する許可を付与	読み込み			
DescribePortfolioShares	指定されたポートフォリオのために作成された各ポートフォリオ共有の概要を表示する許可を付与	リスト	Portfolio*		
DescribeProduct	製品をエンドユーザーとして記述する許可を付与	読み込み	Product*		
DescribeProductAsAdmin	製品を管理者として記述する許可を付与	読み込み	Product*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeProductView	製品をエンドユーザーとして記述する許可を付与	読み込み			
DescribeProvisionedProduct	プロビジョニング済み製品を記述する許可を付与	読み込み		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeProvisionedProductPlan	プロビジョニング済み製品プランを記述する許可を付与	読み込み		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeProvisioningArtifact	プロビジョニングアーティファクトを記述する許可を付与	読み込み	Product*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeProvisioningParameters	指定されたプロビジョニングアーティファクトを正常にプロビジョニングするために指定する必要があるパラメータを説明する許可を付与	読み込み	Product*		
DescribeRecord	レコードを記述するアクセス許可を付与し、出力を一覧表示	読み込み		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeServiceAction	セルフサービスアクションを記述する許可を付与	読み込み			
DescribeServiceActionExecutionParameters	指定されたプロビジョニング済み製品に対して指定されたサービスアクションを実行した場合、デフォルトのパラメータを取得する許可を付与	読み込み		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeTagOption	指定された TagOption に関する情報を取得する許可を付与。	読み取り			
DisableAWSOrganizationsAccess	AWS Organizations 機能を使用してポートフォリオ共有を無効にするアクセス許可を付与します	書き込み			
DisassociateAttributeGroup	アプリケーションから属性グループの関連付けを解除する許可を付与	書き込み	Application*		
			AttributeGroup*		
DisassociateBudgetFromResource	リソースから予算の関連付けを解除する許可を付与	書き込み			
DisassociatePrincipalFromPortfolio	ポートフォリオから IAM プリンシパルの関連付けを解除する許可を付与	書き込み	Portfolio*		
DisassociateProductFromPortfolio	ポートフォリオから製品の関連付けを解除する許可を付与	書き込み			
DisassociateResource	リソースとアプリケーションとの関連付けを解除する許可を付与	書き込み	Application*		resource-groups:DeleteGroup

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				servicecatalog:ResourceType servicecatalog:Resource	
DisassociateServiceActionFromProvisioningArtifact	指定されたプロビジョニングアーティファクトから、指定されたセルフサービスアクションの関連付けを解除する許可を付与	書き込み	Product*		
DisassociateTagOptionFromResource	指定されたリソースから指定された TagOption の関連付けを解除する許可を付与	書き込み	Portfolio Product		
EnableAWSOrganizationsAccess	AWS Organizations を通じてポートフォリオ共有機能を有効にする許可を付与	書き込み			
ExecuteProvisionedProductPlan	プロビジョニング済み製品プランを実行する許可を付与	書き込み		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ExecuteProvisionedProductServiceAction	プロビジョニング済み製品プランを実行する許可を付与	書き込み		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
GetAWSOrganizationsAccessStatus	AWS Organization ポートフォリオ共有機能のアクセスステータスを取得する許可を付与	読み取り			
GetApplication	アプリケーションを取得する許可を付与	読み込み	Application*		
GetAssociatedResource	アプリケーションに関連付けられたリソースに関する情報を取得する許可を付与	読み込み	Application*		
				servicecatalog:ResourceType servicecatalog:Resource	
GetAttributeGroup	属性グループを取得する許可を付与	読み取り	AttributeGroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetConfiguration	AppRegistry 設定を読み取る許可を付与	読み取り			
GetProvisionedProductOutputs	プロビジョニングされた製品 ID または名前のいずれかを使用して、プロビジョニングされた製品の出力を取得する許可を付与	読み取り			
GetResourcePolicy [許可のみ]	指定されたリソースのリソースベースのポリシーを取得する許可を付与する	読み取り	Application		
			Attribute Group		
ImportAsProvisionedProduct	プロビジョニングされた製品にリソースをインポートする許可を付与	書き込み	Product*		
ListAcceptedPortfolioShares	既に共有されており、お客様が承認したポートフォリオを一覧表示する許可を付与	リスト			
ListApplications	アプリケーションを一覧表示する許可を付与	リスト			
ListAssociatedAttributeGroups	アプリケーションに関連付けられた属性グループを一覧表示する許可を付与	リスト	Application*		
ListAssociatedResources	アプリケーションに関連付けられたリソースを一覧表示する許可を付与	リスト	Application*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListAttributeGroups	属性グループを一覧表示する許可を付与	リスト			
ListAttributeGroupsForApplication	特定アプリケーションに関連付けられた属性グループを一覧表示する許可を付与	リスト	Application*		
ListBudgetsForResource	リソースに関連付けられているすべての予算を一覧表示する許可を付与	リスト			
ListConstraintsForPortfolio	特定のポートフォリオに関連付けられた制約を一覧表示する許可を付与	リスト			
ListLaunchPaths	特定の製品をエンドユーザーとして起動するさまざまな方法を一覧表示する許可を付与	リスト	Product*		
ListOrganizationPortfolioAccess	指定されたポートフォリオにアクセスできる組織のノードを一覧表示する許可を付与	リスト			
ListPortfolioAccess	特定のポートフォリオを共有した AWS アカウントを一覧表示するアクセス許可を付与します	リスト	Portfolio*		
ListPortfolios	アカウント内のポートフォリオを一覧表示する許可を付与	リスト			
ListPortfoliosForProduct	特定の製品に関連付けられたポートフォリオを一覧表示する許可を付与	リスト	Product*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListPrincipalsForPortfolio	特定のポートフォリオに関連付けられている IAM プリンシパルを一覧表示する許可を付与	リスト	Portfolio*		
ListProvisionedProductPlans	プロビジョニング済み製品プランを一覧表示する許可を付与	リスト		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListProvisioningArtifacts	特定の製品に関連付けられたプロビジョニングアーティファクトを一覧表示する許可を付与	リスト	Product*		
ListProvisioningArtifactsForServiceAction	指定されたセルフサービスアクションのすべてのプロビジョニングアーティファクトを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListRecordHistory	アカウントのすべてのレコード、またはプロビジョニングされた特定の製品に関連するすべてのレコードを一覧表示する許可を付与	リスト		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListResourcesForTagOption	指定された TagOption に関連付けられたリソースを一覧表示する許可を付与	リスト			
ListServiceActions	すべてのセルフサービスアクションを一覧表示する許可を付与	リスト			
ListServiceActionsForProvisioningArtifact	アカウント内の指定されたプロビジョニングアーティファクトに関連付けられているすべてのサービスアクションを一覧表示する許可を付与	リスト	Product*		
				servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListStackInstancesForProvisionedProduct	CFN_STACKSET タイプのプロビジョニング済み製品に関連付けられている各スタックインスタンスのアカウント、リージョン、およびステータスを一覧表示する許可を付与	リスト		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListTagOptions	指定された TagOptions またはすべての TagOptions を一覧表示する許可を付与	リスト			
ListTagsForResource	サービスカタログ appregistry リソースのタグを一覧表示する許可を付与	読み取り	Application		
			AttributeGroup		
NotifyProvisionProductEngineWorkflowResult	プロビジョニングエンジンの実行結果を通知する許可を付与	書き込み			
NotifyTerminateProvisionedProductEngineWorkflowResult	終了エンジンの実行結果を通知する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
NotifyUpdateProvisionedProductEngineWorkflowResult	更新エンジンの実行結果を通知する許可を付与	書き込み			
ProvisionProduct	指定されたプロビジョニングアーティファクトと起動パラメータを使用して製品をプロビジョニングする許可を付与	書き込み	Product*		
PutConfiguration	AppRegistry 設定を割り当てる許可を付与	書き込み			
PutResourcePolicy [アクセス許可のみ]	指定されたリソースにリソースベースのポリシーを追加する許可を付与する	書き込み	Application		
			AttributeGroup		
RejectPortfolioShare	以前に承諾した、既に共有しているポートフォリオを拒否する許可を付与	書き込み	Portfolio*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ScanProvisionedProducts	アカウント内のすべてのプロビジョニング済み製品を一覧表示する許可を付与	リスト		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
SearchProducts	エンドユーザーとして利用可能な製品を一覧表示する許可を付与	リスト			
SearchProductsAsAdmin	アカウント内のすべての製品、または特定のポートフォリオに関連付けられているすべての製品を一覧表示する許可を付与	リスト			
SearchProvisionedProducts	アカウント内のすべてのプロビジョニング済み製品を一覧表示する許可を付与	リスト		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SyncResource	AppRegistry の現在の状態とリソースを同期する許可を付与	書き込み			cloudformation:UpdateStack
TagResource	サービスカタログ AppRegistry リソースをタグ付けする許可を付与	タグ付け	Application		
			Attribute Group		
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateProvisionedProduct	既存のプロビジョニング済み製品を終了する許可を付与	書き込み		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
UntagResource	サービスカタログ appregistry リソースからタグを削除する許可を付与	タグ付け	Application		
			Attribute Group		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
UpdateApplication	既存のアプリケーションの属性を更新する許可を付与	書き込み	Application*		iam:CreateServiceLinkedRole
UpdateAttributeGroup	既存の属性グループの属性を更新する許可を付与	書き込み	AttributeGroup*		
UpdateConstraint	既存の制約のメタデータフィールドを更新する許可を付与	書き込み			
UpdatePortfolio	既存のポートフォリオのメタデータフィールドまたはタグを更新する許可を付与	書き込み	Portfolio*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdatePortfolioShare	既存のポートフォリオ共有のためにリソース共有を有効または無効にする許可を付与	Permissions management	Portfolio*		
UpdateProduct	既存の製品のメタデータフィールドまたはタグを更新する許可を付与。	書き込み	Product*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateProvisionedProduct	既存のプロビジョニング済み製品を更新する許可を付与	書き込み		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
UpdateProvisionedProductProperties	既存のプロビジョニング済み製品のプロパティを更新する許可を付与。	書き込み			
UpdateProvisioningArtifact	既存のプロビジョニングアーティファクトのメタデータフィールドを更新する許可を付与	書き込み	Product*		
UpdateServiceAction	セルフサービスアクションを更新する許可を付与	書き込み			
UpdateTagOption	指定された TagOption を更新する許可を付与	書き込み			

AWS Service Catalog で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Application	`arn:${Partition}:servicecatalog:${Region}:${Account}:/applications/${ApplicationId}`	aws:ResourceTag/${TagKey}
Attribute Group	`arn:${Partition}:servicecatalog:${Region}:${Account}:/attribute-groups/${AttributeGroupId}`	aws:ResourceTag/${TagKey}
Portfolio	`arn:${Partition}:catalog:${Region}:${Account}:portfolio/${PortfolioId}`	aws:ResourceTag/${TagKey}
Product	`arn:${Partition}:catalog:${Region}:${Account}:product/${ProductId}`	aws:ResourceTag/${TagKey}

AWS Service Catalog の条件キー

AWS Service Catalog では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

> **Note**
>
> IAM ポリシーでのこれらの条件キーの使用方法を示すポリシーの例については、「Service Catalog 管理者ガイド」の「プロビジョニング済み製品を管理するためのアクセスポリシーの例」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString
servicecatalog:Resource	AppRegistry アソシエイトリソース API の Resource パラメータとして指定できる値を制御することによりアクセスをフィルタリング	String
servicecatalog:ResourceType	AppRegistry アソシエイトリソース API の ResourceType パラメータとして指定できる値を制御することによりアクセスをフィルタリング	String
servicecatalog:accountLevel	アカウントで誰かが作成したリソースに対してアクションを表示し、実行することでアクセスをフィルタリングします。	String
servicecatalog:roleLevel	彼ら、または彼らと同じロールに連携するユーザーによって作成されたリソースに対して、アクションを表示し、実行することでアクセスをフィルタリング	String
servicecatalog:userLevel	ユーザーが作成したリソースに対してのみ、アクションを表示し実行することでアクセスをフィルタリング	String

AWS Management Console ユーザーエクスペリエンス機能を管理するための AWS Service のアクション、リソース、および条件キー。

AWS AWS Management Console ユーザーエクスペリエンス機能を管理するサービス。 (サービスプレフィックス: uxc) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Management Console ユーザーエクスペリエンス機能を管理するために AWS Service で定義されるアクション。
- AWS Management Console ユーザーエクスペリエンス機能を管理するために AWS Service で定義されるリソースタイプ。
- AWS Management Console ユーザーエクスペリエンス機能を管理するための AWS Service の条件キー。

AWS Management Console ユーザーエクスペリエンス機能を管理するために AWS Service で定義されるアクション。

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteAccountColor	アカウントに関連付けられた色を削除するアクセス許可を付与します	書き込み			
GetAccountColor	アカウントに関連付けられた色を取得するアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutAccountColor	アカウントに関連付けられた色を設定するアクセス許可を付与します	書き込み			

AWS Management Console ユーザーエクスペリエンス機能を管理するために AWS Service で定義されるリソースタイプ。

AWS AWS Management Console ユーザーエクスペリエンス機能を管理するサービス。 では、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定はサポートされていません。AWS Management Console ユーザーエクスペリエンス機能を管理するために AWS サービスへのアクセスを許可するには、ポリシー`"Resource": "*"`で を指定します。

AWS Management Console ユーザーエクスペリエンス機能を管理するための AWS Service の条件キー。

User Experience Customization (UXC) には、ポリシーステートメントの `Condition`要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS のサービスが提供するマネージドプライベートネットワークのアクション、リソース、および条件キー

AWS マネージドプライベートネットワークを提供する サービス (サービスプレフィックス: `private-networks`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS のサービスが提供するマネージドプライベートネットワークで定義されるアクション
- AWS のサービスが提供するマネージドプライベートネットワークで定義されるリソースタイプ
- AWS のサービスが提供するマネージドプライベートネットワークの条件キー

AWS のサービスが提供するマネージドプライベートネットワークで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcknowledgeOrderReceipt	オーダーが受領されたことを承認するアクセス許可を付与	書き込み	order*		
ActivateDeviceIdentifier	デバイス識別子をアクティブ化するアクセス許可を付与	書き込み	device-identifier*		
				aws:ResourceTag/${TagKey}	
ActivateNetworkSite	ネットワークサイトをアクティブ化するアクセス許可を付与	書き込み	network-site*		
			order*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ConfigureAccessPoint	アクセスポイントを設定するアクセス許可を付与	書き込み	network-resource*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateNetwork	ネットワークを作成するアクセス許可を付与	書き込み	network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNetworkSite	ネットワークサイトを作成するアクセス許可を付与	書き込み	network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeactivateDeviceIdentifier	デバイス識別子を非アクティブ化するアクセス許可を付与	書き込み	device-identifier*		
DeleteNetwork	ネットワークを削除するアクセス許可を付与	書き込み	network*		
DeleteNetworkSite	ネットワークサイトを削除するアクセス許可を付与	書き込み	network-site*		
GetDeviceIdentifier	デバイス識別子を取得するアクセス許可を付与	読み取り	device-identifier*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetNetwork	ネットワークを取得するアクセス許可を付与	読み取り	network*		
				aws:ResourceTag/${TagKey}	
GetNetworkResource	ネットワークリソースを取得するアクセス許可を付与	読み取り	network-resource*		
				aws:ResourceTag/${TagKey}	
GetNetworkSite	ネットワークサイトを取得するアクセス許可を付与	読み取り	network-site*		
				aws:ResourceTag/${TagKey}	
GetOrder	ネットワークオーダーを取得するアクセス許可を付与	読み取り	order*		
				aws:ResourceTag/${TagKey}	
ListDeviceIdentifiers	デバイス識別子を一覧表示するアクセス許可を付与	リスト	network*		
ListNetworkResources	ネットワークリソースを一覧表示するアクセス許可を付与	リスト	network*		
ListNetworkSites	ネットワークサイトを一覧表示するアクセス許可を付与	リスト	network*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListNetworks	ネットワークを一覧表示するアクセス許可を付与	リスト			
ListOrders	ネットワークオーダーを一覧表示するアクセス許可を付与	リスト	network*		
ListTagsForResource	リソースのタグのリストを返す許可を付与	リスト			
Ping	サービスの状態を確認する許可を付与	読み取り			
StartNetworkResourceUpdate	指定されたネットワークリソースの更新を開始するための許可を付与します	書き込み	network-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	指定されたリソースにタグを追加する許可を付与	Tagging	device-identifier		
			network		
			network-resource		
			network-site		
			order		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	指定されたリソースからタグを削除する許可を付与	Tagging	device-identifier		
			network		
			network-resource		
			network-site		
			order		
				aws:TagKeys	
UpdateNetworkSite	ネットワークサイトを更新するアクセス許可を付与	書き込み	network-site*		
UpdateNetworkSitePlan	ネットワークサイトでプランを更新するアクセス許可を付与	書き込み	network-site*		

AWS のサービスが提供するマネージドプライベートネットワークで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアク

ションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
network	arn:${Partition}:private-networks:${Region}:${Account}:network/${NetworkName}	aws:ResourceTag/${TagKey}
network-site	arn:${Partition}:private-networks:${Region}:${Account}:network-site/${NetworkName}/${NetworkSiteName}	aws:ResourceTag/${TagKey}
network-resource	arn:${Partition}:private-networks:${Region}:${Account}:network-resource/${NetworkName}/${ResourceId}	aws:ResourceTag/${TagKey}
order	arn:${Partition}:private-networks:${Region}:${Account}:order/${NetworkName}/${OrderId}	aws:ResourceTag/${TagKey}
device-identifier	arn:${Partition}:private-networks:${Region}:${Account}:device-identifier/${NetworkName}/${DeviceId}	aws:ResourceTag/${TagKey}

AWS のサービスが提供するマネージドプライベートネットワークの条件キー

AWS マネージドプライベートネットワークを提供する サービスでは、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアの存在有無を確認することによりアクセスをフィルタリング	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアを確認することによりアクセスをフィルタリング	String
aws:TagKeys	リクエスト内のタグキーのプレゼンスによってアクセスをフィルタリング	ArrayOfString

Service Quotas のアクション、リソース、および条件キー

Service Quotas (サービスプレフィックス: `servicequotas`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Service Quotas で定義されているアクション
- Service Quotas で定義されているリソースタイプ
- Service Quotas の条件キー

Service Quotas で定義されているアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateServiceQuotaTemplate	Service Quotas テンプレートをユーザーの組織と関連付けるアクセス許可を付与します	書き込み			organizations:DescribeOrganization organizations:EnableAWSServiceAccess
CreateSupportCase	既存のクォータ引き上げリクエストのサポートケースを作成するリクエストを送信するアクセス許可を付与します	書き込み			
DeleteServiceQuotaIncreaseRequestFromTemplate	サービスクォータテンプレートから指定されたサービスクォータを削除する許可を付与	書き込み			organizations:DescribeOrganization
DisassociateServiceQuotaTemplate	ユーザーの組織から Service Quotas テンプレートとの関連付けを削除する許可を付与	書き込み			organizations:DescribeOrganization
GetAWSDefaultServiceQuota	AWS デフォルト値を含む、指定されたサービスクォータの詳細を返すアクセス許可を付与します	読み取り			
GetAssociationForS	Service Quotas テンプレートが組織に関連付けられているかどうかが判断で	読み込み			organizations:Desc

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
erviceQuotaTemplate	きる、ServiceQuotaTemplateAssociationStatus 値を取得する許可を付与。				ribeOrganization
GetRequestedServiceQuotaChange	特定のサービスクォータ引き上げリクエストの詳細を取得する許可を付与	読み込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetServiceQuota	適用された値を含め、指定されたサービスクォータの詳細を取得する許可を付与	読み込み			autoscaling:DescribeAccountLimits cloudformation:DescribeAccountLimits dynamodb:DescribeLimits elasticloadbalancing:DescribeAccountLimits iam:GetAccountSummary kinesis:DescribeLimits rds:DescribeAccountAttributes

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					route53:GetAccountLimit
GetServiceQuotaIncreaseRequestFromTemplate	サービスクォータテンプレートからクォータ引き上げリクエストの詳細を取得する許可を付与	読み取り			organizations:DescribeOrganization
ListAWSDefaultServiceQuotas	指定されたサービスのすべてのデフォルトの AWS サービスクォータを一覧表示するアクセス許可を付与します	読み取り			
ListRequestedServiceQuotaChangeHistory	サービスのクォータに対する変更のリストをリクエストする許可を付与	読み込み			
ListRequestedServiceQuotaChangeHistoryByQuota	特定のサービスクォータに対する変更のリストをリクエストする許可を付与	読み込み			
ListServiceQuotaIncreaseRequestsInTemplate	サービスクォータテンプレートからクォータ引き上げリクエストのリストを返すアクセス許可を付与します	読み取り			organizations:DescribeOrganization

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListServiceQuotas	そのアカウントのそのリージョンで、指定された AWS サービスのすべてのサービスクォータを一覧表示するアクセス許可を付与します	読み取り			autoscaling:DescribeAccountLimits cloudformation:DescribeAccountLimits dynamodb:DescribeLimits elasticloadbalancing:DescribeAccountLimits iam:GetAccountSummary kinesis:DescribeLimits rds:DescribeAccountAttributes

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					route53:GetAccountLimit
ListServices	Service Quotas で利用可能な AWS サービスを一覧表示するアクセス許可を付与します	読み取り			
ListTagsForResource	SQ リソース上の既存のタグを表示する許可を付与	読み込み			
PutServiceQuotaIncreaseRequestIntoTemplate	クォータを定義してサービスクォータテンプレートに追加する許可を付与	書き込み	quota		organizations:DescribeOrganization
				servicequotas:service	
RequestServiceQuotaIncrease	サービスクォータの引き上げのリクエストを送信する許可を付与	書き込み	quota		
				servicequotas:service	
TagResource	タグセットを既存の SQ リソースに関連付けるアクセス許可を付与します	タグ付け		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UntagResource	SQ リソースからタグセットを削除する権限を付与します。削除されるタグは、カスタマー提供のタグキーのセットと一致します	タグ付け		aws:TagKeys	

Service Quotas で定義されているリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
quota	`arn:${Partition}:servicequotas:${Region}:${Account}:${ServiceCode}/${QuotaCode}`	

Service Quotas の条件キー

Service Quotas では、Condition ポリシーの IAM 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
servicequotas:service	指定された AWS サービスでアクセスをフィルタリングします	String

Amazon SES のアクション、リソース、および条件キー

Amazon SES (サービスプレフィックス: ses) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon SES で定義されるアクション
- Amazon SES で定義されるリソースタイプ
- Amazon SES の条件キー

Amazon SES で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CloneReceiptRuleSet	既存のルールを複製して、受信ルールセットを作成する許可を付与。	Write		ses:ApiVersion	
CreateConfigurationSet	新しい設定セットを作成する許可を付与	書き込み		ses:ApiVersion	
CreateConfigurationSetEventDestination	設定セットイベントの宛先を作成する許可を付与	Write		ses:ApiVersion	
CreateConfigurationSetTrackingOptions	設定セットとオープン状態用カスタムドメイン間の関連付けを作成し、イベント追跡をクリックする許可を付与。	Write		ses:ApiVersion	
CreateCustomVerificationEmailTemplate	新しいカスタム検証 E メールテンプレートを作成する許可を付与	Write		ses:ApiVersion	
CreateReceiptFilter	新しい IP アドレスのフィルターを作成する許可を付与。	Write		ses:ApiVersion	
CreateReceiptRule	受信ルールを作成する許可を付与。	Write		ses:ApiVersion	
CreateReceiptRuleSet	空の受信ルールセットを作成する許可を付与。	Write		ses:ApiVersion	
CreateTemplate	E メールテンプレートを作成する許可を付与。	Write		ses:ApiVersion	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteConfigurationSet	既存の設定セットを削除する許可を付与	書き込み		ses:ApiVersion	
DeleteConfigurationSetEventDestination	イベントの送信先を削除するアクセス権限を付与します	Write		ses:ApiVersion	
DeleteConfigurationSetTrackingOptions	設定セットとオープン状態用カスタムドメイン間の関連付けを削除し、イベント追跡をクリックする許可を付与。	Write		ses:ApiVersion	
DeleteCustomVerificationEmailTemplate	既存のカスタム検証 E メールテンプレートを削除する許可を付与	Write		ses:ApiVersion	
DeleteIdentity	指定した ID を削除する許可を付与。	Write		ses:ApiVersion	
DeleteIdentityPolicy	指定された ID (E メールアドレスまたはドメイン) に対して、指定された送信承認ポリシーを削除する許可を付与	Permissions management		ses:ApiVersion	
DeleteReceiptFilter	指定した IP アドレスのフィルターを削除する許可を付与。	Write		ses:ApiVersion	
DeleteReceiptRule	指定した受信ルールを削除する許可を付与。	Write		ses:ApiVersion	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteReceiptRuleSet	指定した受信ルールセットとそのセットに含まれるすべての受信ルールを削除する許可を付与。	Write		ses:ApiVersion	
DeleteTemplate	E メールテンプレートを削除する許可を付与	Write		ses:ApiVersion	
DeleteVerifiedEmailAddress	指定された E メールアドレスを検証済みアドレスの一覧から削除する許可を付与。	Write		ses:ApiVersion	
DescribeActiveReceiptRuleSet	現在有効な受信ルールセットのメタデータと受信ルールを返すアクセス許可を付与します。	Read		ses:ApiVersion	
DescribeConfigurationSet	指定された構成セットの詳細を返すアクセス許可を付与します。	Read		ses:ApiVersion	
DescribeReceiptRule	指定された受信ルールの詳細を返すアクセス許可を付与します。	Read		ses:ApiVersion	
DescribeReceiptRuleSet	指定された受信ルールセットの詳細を返すアクセス許可を付与します。	Read		ses:ApiVersion	
GetAccountSendingEnabled	アカウントの E メール送信ステータスを返すアクセス許可を付与します。	Read		ses:ApiVersion	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetCustomVerificationEmailTemplate	指定したテンプレート名のカスタム E メール検証テンプレートを返すアクセス許可を付与します	Read		ses:ApiVersion	
GetIdentityDkimAttributes	エンティティの Easy DKIM 署名の現在のステータスを返すアクセス許可を付与します。	Read		ses:ApiVersion	
GetIdentityMailFromDomainAttributes	ID (E メールアドレスおよび/またはドメイン) のリストのカスタム MAIL FROM 属性を返すアクセス許可を付与します。	Read		ses:ApiVersion	
GetIdentityNotificationAttributes	検証済み ID (E メールアドレスやドメイン) のリストが与えられると、ID 通知属性を記述する構造を返すアクセス許可を付与します。	Read		ses:ApiVersion	
GetIdentityPolicies	指定された ID (E メールアドレスまたはドメイン) に対して要求された送信承認ポリシーを返すアクセス許可を付与します	Read		ses:ApiVersion	
GetIdentityVerificationAttributes	検証ステータスと (ドメイン ID の場合) ID リストの検証トークンを返すアクセス許可を付与します。	Read		ses:ApiVersion	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetSendQuota	ユーザーの現在の送信制限を返すアクセス許可を付与します。	Read		ses:ApiVersion	
GetSendStatistics	ユーザーの送信統計を返すアクセス許可を付与します。	Read		ses:ApiVersion	
GetTemplate	指定したテンプレートのテンプレートオブジェクト (件名、HTML 部分、およびテキスト部分など) を返すアクセス許可を付与します。	Read		ses:ApiVersion	
ListConfigurationSets	アカウントのすべての設定セットを一覧表示する許可を付与	リスト		ses:ApiVersion	
ListCustomVerificationEmailTemplates	アカウントの既存のカスタム検証 E メールテンプレートをすべて一覧表示する許可を付与	リスト		ses:ApiVersion	
ListIdentities	アカウントの E メール ID を一覧表示する許可を付与	リスト		ses:ApiVersion	
ListIdentityPolicies	アカウントのすべての E メールテンプレートを一覧表示する許可を付与	リスト		ses:ApiVersion	
ListReceiptFilters	アカウントに関連付けられている IP アドレスのフィルターを一覧表示する許可を付与。	Read		ses:ApiVersion	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListReceiptRuleSets	アカウントに存在する受信ルールセットを一覧表示する許可を付与。	Read		ses:ApiVersion	
ListTemplates	アカウントに存在する E メールテンプレートを一覧表示する許可を付与。	リスト		ses:ApiVersion	
ListVerifiedEmailAddresses	アカウントで検証済みのすべての E メールアドレスを一覧表示する許可を付与。	Read		ses:ApiVersion	
PutConfigurationSetDeliveryOptions	構成セットの配信オプションを追加または更新する許可を付与。	Write		ses:ApiVersion	
PutIdentityPolicy	指定された ID (E メールアドレスまたはドメイン) に対して、送信承認ポリシーを追加または更新する許可を付与。	Permissions management		ses:ApiVersion	
ReorderReceiptRuleSet	受信ルールセット内の受信ルールの順序を変更する許可を付与。	Write		ses:ApiVersion	
SendBounce	Amazon SES を通じて受信した E メールの送信者にバウンスメッセージを生成し、送信する許可を付与。	Write	identity*	ses:ApiVersion ses:FromAddress	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SendBulkTemplatedEmail	複数の送信先に E メールメッセージを作成する許可を付与	Write	identity*		
			template*		
			configuration-set		
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SendCustomVerificationEmail	ID の一覧に E メールアドレスを追加して、アカウントの検証を試みるアクセス許可を付与します。	Write	identity*		
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendEmail	E メールメッセージを送信する許可を付与	Write	identity*		
			configuration-set		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendRawEmail	クライアントによって指定されたヘッダーとコンテンツで、E メールメッセージを送信する許可を付与。	Write	identity* configuration-set		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendTemplatedEmail	E メールテンプレートを使用して E メールメッセージを作成する許可を付与。	Write	identity*		
			template*		
			configuration-set		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SetActiveReceiptRuleSet	指定された受信ルールセットをアクティブな受信ルールセットとして設定する許可を付与。	Write		ses:ApiVersion	
SetIdentityDkimEnabled	ID から送信された E メールの Easy DKIM 署名を有効または無効にする許可を付与。	Write		ses:ApiVersion	
SetIdentityFeedbackForwardingEnabled	Amazon SES が ID (E メールアドレスまたはドメイン) のバウンス通知と苦情通知を転送するかどうかを有効または無効にする許可を付与。	Write		ses:ApiVersion	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SetIdentityHeadersInNotificationsEnabled	指定された ID (E メールアドレスまたはドメイン) を指定すると、Amazon SES に、Amazon Simple Notification Service (Amazon SNS) の元の E メールヘッダーが指定されたタイプの通知を含むかどうかを設定する許可を付与。	Write		ses:ApiVersion	
SetIdentityMailFromDomain	検証された ID のカスタム MAIL FROM ドメイン設定を有効または無効にする許可を付与。	Write		ses:ApiVersion	
SetIdentityNotificationTopic	確認された ID の通知を配信するときに使用する Amazon Simple Notification Service (Amazon SNS) トピックを設定する許可を付与。	Write		ses:ApiVersion	
SetReceiptRulePosition	受信ルールセット内の指定された受信ルールの位置を設定する許可を付与。	Write		ses:ApiVersion	
TestRenderTemplate	テンプレートと一連の置換データが提供されている場合、E メール の MIME コンテンツのプレビューを作成する許可を付与	Write		ses:ApiVersion	
UpdateAccountSendingEnabled	アカウントの E メール送信を有効または無効にする許可を付与。	Write		ses:ApiVersion	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateConfigurationSetEventDestination	構成セットのイベント送信先を更新する許可を付与。	Write		ses:ApiVersion	
UpdateConfigurationSetReputationMetricsEnabled	指定された構成セットを使用して送信された E メールの評価メトリックの公開を有効または無効にする許可を付与。	Write		ses:ApiVersion	
UpdateConfigurationSetSendingEnabled	指定された構成セットを使用して送信されたメッセージの E メール送信を有効または無効にする許可を付与。	Write		ses:ApiVersion	
UpdateConfigurationSetTrackingOptions	設定セットとオープン状態用カスタムドメイン間の関連付けを変更し、イベント追跡をクリックする許可を付与。	Write		ses:ApiVersion	
UpdateCustomVerificationEmailTemplate	既存のカスタム検証 E メールテンプレートを更新する許可を付与	Write		ses:ApiVersion	
UpdateReceiptRule	受信ルールを更新する許可を付与。	Write		ses:ApiVersion	
UpdateTemplate	E メールテンプレートを更新する許可を付与	Write		ses:ApiVersion	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
VerifyDomainDkim	ドメインに対して一連の DKIM トークンを返すアクセス許可を付与します。	書き込み		ses:ApiVersion	
VerifyDomainIdentity	ドメインを確認するためのアクセス許可を付与します。	書き込み		ses:ApiVersion	
VerifyEmailAddress	E メールアドレスを検証する許可を付与。	書き込み		ses:ApiVersion	
VerifyEmailIdentity	E メール ID を検証する許可を付与。	書き込み		ses:ApiVersion	

Amazon SES で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
configuration-set	`arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	
custom-verification-email-template	`arn:${Partition}:ses:${Region}:${Account}:custom-verification-email-template/${TemplateName}`	

リソースタイプ	ARN	条件キー
identity	arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}	
template	arn:${Partition}:ses:${Region}:${Account}:template/${TemplateName}	

Amazon SES の条件キー

Amazon SES では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
ses:ApiVersion	SES API バージョンに基づいてアクションをフィルタリング	String
ses:FeedbackAddress	E メールフィードバック転送によって送信されたバウンスおよび苦情の場所を指定する「リターンパス」アドレスに基づくアクションをフィルタリングします	文字列
ses:FromAddress	メッセージの「From」アドレスに基づいてアクションをフィルタリングします	文字列
ses:FromDisplayName	メッセージの表示名として使用される「From」アドレスに基づいてアクションをフィルタリングします	文字列
ses:Recipients	「To」、「CC」、「BCC」アドレスを含むメッセージの受取人アドレスに基づくアクションをフィルタリングします	ArrayOfString

AWS Shield のアクション、リソース、および条件キー

AWS Shield (サービスプレフィックス: shield) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Shield で定義されるアクション
- AWS Shield で定義されるリソースタイプ
- AWS Shield の条件キー

AWS Shield で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateDRTLogBucket	DDoS レスポンスチームが、フローログを含む指定された Amazon S3 バケットにアクセスすることを承認する許可を付与。	書き込み			s3:GetBucketPolicy s3:PutBucketPolicy
AssociateDRTRole	指定されたロールを使用して DDoS Response チームにアクセスを許可し、潜在的な攻撃中の DDoS 攻撃の軽減 AWS アカウント を支援するアクセス許可を付与します	書き込み			iam:GetRole iam:ListAttachedRolePolicies

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					iam:PassRole
AssociateHealthCheck	リソースの Shield アドバンスト保護にヘルスベースの検出を追加する許可を付与。	Write	protection*		route53:GetHealthCheck
				aws:ResourceTag/${TagKey}	
AssociateProactiveEngagementDetails	プロアクティブな関与を初期化し、DDoS レスポンスチーム (DRT) が使用する連絡先の一覧を設定する許可を付与。	Write			
CreateProtection	指定されたリソース ARN の DDoS 保護サービスをアクティブ化する許可を付与。	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProtectionGroup	保護されたリソースのグループを作成するアクセス許可を付与して、それらを集合として処理できるようにします。	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscription	サブスクリプションをアクティブ化するためのアクセス許可を付与します。	Write			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteProtection	既存の保護を削除する許可を付与。	Write	protection*		
				aws:ResourceTag/${TagKey}	
DeleteProtectionGroup	指定された保護グループを削除する許可を付与。	Write	protection-group*		
				aws:ResourceTag/${TagKey}	
DeleteSubscription	サブスクリプションを無効にする許可を付与。	Write			
DescribeAttack	攻撃の詳細を取得する許可を付与。	読み取り	attack*		
DescribeAttackContributors [許可のみ]	特定の DDoS 攻撃の寄与要因に関する詳細情報を取得する許可を付与	読み取り	attack*		
			protection-group		
DescribeAttackStatistics	AWS Shield が昨年検出した攻撃の数とタイプに関する情報を記述する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeDRTAccess	DDoS DDoS Response チームが攻撃の軽減を支援 AWS アカウント しながら にアクセスするために使用する現在のロールと Amazon S3 ログバケットのリストを記述するアクセス許可を付与します	読み取り			
DescribeEmergencyContactSettings	疑わしい攻撃中に ユーザーに連絡するために DRT が使用できる E メールアドレスをリストする許可を付与。	Read			
DescribeProtection	保護の詳細を取得する許可を付与。	Read	protection*		
				aws:ResourceTag/${TagKey}	
DescribeProtectionGroup	指定された保護グループの仕様を説明する許可を付与。	Read	protection-group*		
				aws:ResourceTag/${TagKey}	
DescribeSubscription	開始時刻など、サブスクリプションの詳細を取得するためのアクセス許可を付与します。	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DisableApplicationLayerAutomaticResponse	リソースの Shield Advanced 保護のアプリケーションレイヤー自動応答を無効にする許可を付与	書き込み			
DisableProactiveEngagement	DDoS レスポンスチーム (DRT) から承認を削除するアクセス許可を付与し、エスカレーションについて連絡先に通知します。	Write			
DisassociateDRTLogBucket	ユーザーのフローログを含む指定された Amazon S3 バケットへの DDoS レスポンスチームのアクセスを削除する許可を付与。	書き込み			s3:DeleteBucketPolicy s3:GetBucketPolicy s3:PutBucketPolicy
DisassociateDRTRole	DDoS Response チームの へのアクセスを削除するアクセス許可を付与します AWS アカウント	書き込み			
DisassociateHealthCheck	リソースの Shield アドバンスト保護からヘルスベースの検出を削除する許可を付与	書き込み	protection*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
EnableApplicationLayerAutomaticResponse	リソースの Shield Advanced 保護のアプリケーションレイヤー自動応答を有効にする許可を付与	書き込み			apprunner:DescribeWebAclForService cloudfront:GetDistribution cognito-idp:GetWebACLForResource ec2:GetVerifiedAccessInstanceWebAcl iam:CreateServiceLinkedRole iam:GetRole wafv2:GetWebACL wafv2:GetWebACLForResource

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
EnableProactiveEngagement	DDoS レスポンスチーム (DRT) に E メールと電話を使用して、エスカレーションについて連絡先への通知を許可する許可を付与。	書き込み			
GetGlobalThreatData [アクセス許可のみ]	Shield AWS の脅威モニタリングシステムからグローバルな脅威インテリジェンスデータと傾向を取得する許可を付与	読み取り			
GetSubscriptionState	サブスクリプションの状態を取得するためのアクセス許可を付与します。	Read			
ListAttacks	既存のすべての攻撃を一覧表示する許可を付与。	リスト			
ListMitigations [許可のみ]	DDoS 攻撃中に適用された緩和アクションのリストを取得するアクセス許可を付与します	リスト	attack*		
ListProtectionGroups	アカウントの保護グループを取得する許可を付与。	リスト			
ListProtections	既存の保護をすべて一覧表示する許可を付与。	リスト			
ListResourcesInProtectionGroup	保護グループに含まれるリソースを取得するためのアクセス許可を付与します。	リスト	protection-group*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTagsForResource	Shield で指定された Amazon リソースネーム (ARN) AWS の AWS タグに関する情報を取得する許可を付与	読み取り	protection		
			protection-group		
TagResource	Shield AWS でリソースのタグを追加または更新するアクセス許可を付与します	Tagging	protection		
			protection-group		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Shield AWS のリソースからタグを削除するアクセス許可を付与します	Tagging	protection		
			protection-group		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateApplicationLayerAutomaticResponse	リソースの Shield Advanced 保護のアプリケーションレイヤー自動応答を更新する許可を付与	書き込み			apprunner:DescribeWebAclForService cognito-idp:GetWebACLForResource ec2:GetVerifiedAccessInstanceWebAcl wafv2:GetWebACL wafv2:GetWebACLForResource
UpdateEmergencyContactSettings	疑わしい攻撃中に ユーザーに連絡するために DRT が使用できる E メールアドレスのリストの詳細を更新する許可を付与。	Write			
UpdateProtectionGroup	既存の保護グループを更新する許可を付与。	Write	protection-group*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateSubscription	既存のサブスクリプションの詳細を更新する許可を付与。	Write			

AWS Shield で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
attack	`arn:${Partition}:shield::${Account}:attack/${Id}`	
protection	`arn:${Partition}:shield::${Account}:protection/${Id}`	aws:ResourceTag/${TagKey}
protection-group	`arn:${Partition}:shield::${Account}:protection-group/${Id}`	aws:ResourceTag/${TagKey}

AWS Shield の条件キー

AWS Shield では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアのプレゼンスに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいてアクションをフィルタリングします	ArrayOfString

AWS Shield ネットワークセキュリティディレクターのアクション、リソース、および条件キー

AWS Shield Network Security Director (サービスプレフィックス: `network-security-director`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Shield ネットワークセキュリティディレクターによって定義されるアクション
- AWS Shield Network Security Director で定義されるリソースタイプ
- AWS Shield Network Security Director の条件キー

AWS Shield ネットワークセキュリティディレクターによって定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetFinding	検出結果を取得するアクセス許可を付与します	読み取り			
GetNetworkSecurityScan	ネットワークセキュリティスキャンのステータスを取得するアクセス許可を付与します	読み取り			
GetResource	リソースを取得するアクセス許可を付与します	読み取り			
ListFindings	検出結果を一覧表示するアクセス許可を付与します	リスト			
ListInsights	最新のネットワークセキュリティスキャンに関するインサイトを一覧表示するアクセス許可を付与します	リスト			
ListRemediations	検出結果の修復を一覧表示するアクセス許可を付与します	リスト			
ListResources	リソースを一覧表示するアクセス許可を付与します	リスト			
StartNetworkSecurityScan	ネットワークセキュリティスキャンを開始するアクセス許可を付与します	書き込み			
UpdateFinding	検出結果のステータスを更新するアクセス許可を付与します	書き込み			

AWS Shield Network Security Director で定義されるリソースタイプ

AWS Shield Network Security Director は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Shield ネットワークセキュリティディレクターへのアクセスを許可するには、ポリシー`"Resource": "*"`で を指定します。

AWS Shield Network Security Director の条件キー

Network Security Director には、ポリシーステートメントの `Condition`要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Signer のアクション、リソース、および条件キー

AWS Signer (サービスプレフィックス: `signer`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Signer で定義されるアクション
- AWS Signer によって定義されるリソースタイプ
- AWS Signer の条件キー

AWS Signer で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddProfilePermission	署名プロファイルにクロスアカウント権限を追加する許可を付与	Permissions	signing-profile*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
		management			
CancelSigningProfile	署名プロファイルの状態を [キャンセル] に変更する許可を付与	Write	signing-profile*		
				signer:ProfileVersion	
DescribeSigningJob	特定の署名ジョブについての情報を返すアクセス許可を付与します	読み取り	signing-job*		
GetRevocationStatus	署名リソースの失効情報をクエリする許可を付与	読み取り	signing-job*		
			signing-profile*		
GetSigningPlatform	特定の署名プラットフォームについての情報を返すアクセス許可を付与します	Read			
GetSigningProfile	特定の署名プロファイルについての情報を返すアクセス許可を付与します	Read	signing-profile*		
				signer:ProfileVersion	
ListProfilePermissions	署名プロファイルに関連付けられたクロスアカウントの権限を一覧表示する許可を付与	Read	signing-profile*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListSigningJobs	アカウント内のすべての署名ジョブを一覧表示する許可を付与	リスト			
ListSigningPlatforms	使用可能なすべての署名プラットフォームを一覧表示する許可を付与	リスト			
ListSigningProfiles	アカウント内のすべての署名プロファイルを一覧表示する権限を付与します	リスト			
ListTagsForResource	署名プロファイルに関連付けられているタグを一覧表示する許可を付与	Read	signing-profile*		
PutSigningProfile	新しい署名プロファイルを作成する許可を付与	Write		aws:RequestTag/${TagKey} aws:TagKeys	
RemoveProfilePermission	署名プロファイルからクロスアカウント権限を削除する許可を付与	Permissions management	signing-profile*		
RevokeSignature	署名ジョブの状態を REVOCTED に変更する許可を付与	Write	signing-job*		
				signer:ProfileVersion	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RevokeSigningProfile	署名プロファイルの状態を REVOCTED に変更する許可を付与	書き込み	signing-profile*		
				signer:ProfileVersion	
SignPayload	提供されたペイロードで署名ジョブを開始する許可を付与	書き込み	signing-profile*		
				signer:ProfileVersion	
StartSigningJob	提供されたコードで署名ジョブを開始する許可を付与	Write	signing-profile*		
				signer:ProfileVersion	
TagResource	署名プロファイルに 1 つ以上のタグを追加する許可を付与	タグ付け	signing-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	署名プロファイルから 1 つ以上のタグを削除する許可を付与	タグ付け	signing-profile*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	

AWS Signer によって定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
signing-profile	`arn:${Partition}:signer:${Region}:${Account}:/signing-profiles/${ProfileName}`	aws:ResourceTag/${TagKey}
signing-job	`arn:${Partition}:signer:${Region}:${Account}:/signing-jobs/${JobId}`	

AWS Signer の条件キー

AWS Signer は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	各タグの許可された値のセットでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値でアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内の必須タグが存在するかどうかでアクセスをフィルタリングします	ArrayOfString
signer:ProfileVersion	署名プロファイルのバージョンでアクセスをフィルタリング	String

AWS Signin のアクション、リソース、および条件キー

AWS Signin (サービスプレフィックス: `signin`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Signin によって定義されるアクション
- AWS Signin によって定義されるリソースタイプ
- AWS Signin の条件キー

AWS Signin によって定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateTrustedIdentityPropagationApplicationForConsole	Identity Center 組織インスタンス AWS Management Console の を表す Identity Center アプリケーションを作成する許可を付与	書き込み			sso:CreateApplication sso:GetSharedSsoConfiguration sso:ListApplications sso:PutApplicationAccessScope sso:PutApplicationAssignmentConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTrustedIdentityPropagationApplicationsForConsole	を表すすべての Identity Center アプリケーションを一覧表示するアクセス許可を付与します AWS Management Console	リスト			sso:GetSharedSsoConfiguration sso:ListApplications

AWS Signin によって定義されるリソースタイプ

AWS Signin は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Signin へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Signin の条件キー

Signin には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Simple Email Service – Mail Manager のアクション、リソース、および条件キー

Amazon Simple Email Service – Mail Manager (サービスプレフィックス: `ses`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Simple Email Service – Mail Manager で定義されたアクション
- Amazon Simple Email Service – Mail Manager で定義されるリソースタイプ
- Amazon Simple Email Service – Mail Manager の条件キー

Amazon Simple Email Service – Mail Manager で定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AllowVendedLogDeliveryForResource [アクセス許可のみ]	Mail Manager リソースの販売ログ配信を設定するアクセス許可を付与します	権限の管理	mailmanager-ingress-point		
			mailmanager-rule-set		
CreateAddonInstance	アドオンインスタンスを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys ses:AddonSubscriptionArn	
CreateAddonSubscription	アドオンサブスクリプションを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:TagKeys	
CreateAddressList	アドレスリストを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAddressListImportJob	アドレスリストにインポートジョブを作成するアクセス許可を付与します	書き込み	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
CreateArchive	アーカイブを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateIngressPoint	イングレスポイントを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys ses:MailManagerRuleSetArn ses:MailManagerTrafficPolicyArn	ec2:DescribeVpcEndpoints iam:CreateServiceLinkedRole
CreateRelay	SMTP リレーを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleSet	ルールセットを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateTrafficPolicy	トラフィックポリシーを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAddonInstance	アドオンインスタンスを削除する許可を付与する	書き込み	addon-instance*		
				aws:RequestTag/${TagKey}	
DeleteAddonSubscription	アドオンサブスクリプションを削除する許可を付与する	書き込み	addon-subscription*		
				aws:RequestTag/${TagKey}	
DeleteAddressList	アドレスリストを削除するアクセス許可を付与します	書き込み	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
DeleteArchive	アーカイブを削除するアクセス許可を付与	書き込み	mailmanager-archive*		
				aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteIngressPoint	イングレスポイントを削除する許可を付与する	書き込み	mailmanager-ingress-point*		
				aws:RequestTag/${TagKey}	
DeleteRelay	SMTP リレーを削除する許可を付与する	書き込み	mailmanager-smtp-relay*		
				aws:RequestTag/${TagKey}	
DeleteRuleSet	ルールセットを削除する許可を付与する	書き込み	mailmanager-rule-set*		
				aws:RequestTag/${TagKey}	
DeleteTrafficPolicy	トラフィックポイントを削除する許可を付与する	書き込み	mailmanager-traffic-policy*		
				aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeregisterMemberFromAddressList	アドレスリストからメンバーを削除するアクセス許可を付与します	書き込み	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetAddonInstance	アドオンインスタンスに関する情報を取得する許可を付与する	読み取り	addon-instance*		
				aws:RequestTag/${TagKey}	
GetAddonSubscription	アドオンサブスクリプションに関する情報を取得する許可を付与する	読み取り	addon-subscription*		
				aws:RequestTag/${TagKey}	
GetAddressList	アドレスリストに関する情報を取得するアクセス許可を付与します	読み取り	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetAddressListImportJob	アドレスリストのインポートジョブに関する情報を取得する許可を付与	読み取り	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetArchive	アーカイブに関する情報を取得する許可を付与する	読み取り	mailmanager-archive*		
				aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetArchiveExport	アーカイブエクスポートに関する情報を取得するための許可を付与する	読み取り	mailmanager-archive*		
GetArchiveMessage	アーカイブされたメッセージを取得する許可を付与する	読み取り	mailmanager-archive*		
GetArchiveMessageContent	アーカイブされたメッセージの内容を取得する許可を付与する	読み取り	mailmanager-archive*		
GetArchiveSearch	サービスに関する情報を取得する許可を付与する	読み取り	mailmanager-archive*		
GetArchiveSearchResults	検索結果に関する情報を取得するための許可を付与する	読み取り	mailmanager-archive*		
GetIngressPoint	イングレスポイントに関する情報を取得する許可を付与する	読み取り	mailmanager-ingress-point*		
				aws:RequestTag/${TagKey}	
GetMemberOfAddressList	アドレスリストのメンバーに関する情報を取得するアクセス許可を付与します	読み取り	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetRelay	SMTP リレーに関する情報を取得する許可を付与する	読み取り	mailmanager-smtp-relay*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey}	
GetRuleSet	ルールセットに関する情報を取得する許可を付与する	読み取り	mailmanager-rule-set*		
				aws:RequestTag/${TagKey}	
GetTrafficPolicy	トラフィックポリシーに関する情報を取得する許可を付与する	読み取り	mailmanager-traffic-policy*		
				aws:RequestTag/${TagKey}	
ListAddonInstances	アカウントに関連付けられているすべてのアドオンインスタンスを一覧表示する許可を付与する	リスト			
ListAddonSubscriptions	アカウントに関連付けられているすべてのアドオンサブスクリプションを一覧表示する許可を付与する	リスト			
ListAddressListImportJobs	アドレスリストに関連付けられているすべてのインポートジョブを一覧表示するアクセス許可を付与します	リスト	mailmanager-address-list*	aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListAddressLists	アカウントに関連付けられているすべてのアドレスリストを一覧表示するアクセス許可を付与します	リスト			
ListArchiveExports	アカウントに関連付けられているすべてのアーカイブエクスポートを一覧表示する許可を付与する	リスト			
ListArchiveSearches	アカウントに関連付けられているすべてのアーカイブ検索を一覧表示する許可を付与する	リスト			
ListArchives	アカウントに関連付けられているすべてのアーカイブを一覧表示する許可を付与する	リスト			
ListIngressPoints	アカウントに関連付けられているすべてのイングレスポイントを一覧表示する許可を付与する	リスト			
ListMembersOfAddressList	アドレスリストに関連付けられているすべてのメンバーを一覧表示するアクセス許可を付与します	リスト	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
ListRelays	アカウントに関連付けられているすべての SMTP リレーを一覧表示する許可を付与する	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListRuleSets	アカウントに関連付けられているすべてのルールセットを一覧表示する許可を付与する	リスト			
ListTagsForResource	リソースに関連付けられたすべてのタグを一覧表示する許可を付与する	読み取り	addon-instance		
			addon-subscription		
			mailmanager-archive		
			mailmanager-ingress-point		
			mailmanager-rule-set		
			mailmanager-smtp-relay		
			mailmanager-traffic-policy		
ListTrafficPolicies	アカウントに関連付けられているすべてのトラフィックポリシーを一覧表示する許可を付与する	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RegisterMemberToAddressList	アドレスリストにメンバーを追加するアクセス許可を付与します	書き込み	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
StartAddressListImportJob	アドレスリストでインポートジョブを開始する許可を付与	書き込み	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
StartArchiveExport	アーカイブのエクスポートを開始する許可を付与する	書き込み	mailmanager-archive*		
StartArchiveSearch	アーカイブの検索を開始する許可を付与する	書き込み	mailmanager-archive*		
StopAddressListImportJob	アドレスリストで進行中のインポートジョブを停止するアクセス許可を付与します	書き込み	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
StopArchiveExport	アーカイブのエクスポートを停止する許可を付与する	書き込み	mailmanager-archive*		
StopArchiveSearch	アーカイブ検索を停止する許可を付与する	書き込み	mailmanager-archive*		
TagResource	指定したリソースに 1 つ以上のタグ (キーと値) を追加する許可を付与	タグ付け	addon-instance		
			addon-subscription		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			mailmanager-address-list		
			mailmanager-archive		
			mailmanager-ingress-point		
			mailmanager-rule-set		
			mailmanager-smtp-relay		
			mailmanager-traffic-policy		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	指定したリソースから 1 つ以上のタグ (キーと値) を削除する許可を付与	Tagging	addon-instance		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			addon-subscription		
			mailmanager-address-list		
			mailmanager-archive		
			mailmanager-ingress-point		
			mailmanager-rule-set		
			mailmanager-smtp-relay		
			mailmanager-traffic-policy		
				aws:TagKeys	
UpdateArchive	アーカイブを更新するアクセス許可を付与	書き込み	mailmanager-archive*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey}	
UpdateIngressPoint	イングレスポイントを更新する許可を付与する	書き込み	mailmanager-ingress-point*		
				aws:RequestTag/${TagKey} ses:MailManagerTrafficPolicyArn ses:MailManagerRuleSetArn	
UpdateRelay	SMTP リレーを更新する許可を付与する		mailmanager-smtp-relay*		
				aws:RequestTag/${TagKey}	
UpdateRuleSet	ルールセットを更新する許可を付与する	書き込み	mailmanager-rule-set*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey}	
UpdateTrafficPolicy	トラフィックポリシーを更新する許可を付与する	書き込み	mailmanager-traffic-policy*		
				aws:RequestTag/${TagKey}	

Amazon Simple Email Service – Mail Manager で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
addon-instance	arn:${Partition}:ses:${Region}:${Account}:addon-instance/${AddonInstanceId}	aws:ResourceTag/${TagKey}
addon-subscription	arn:${Partition}:ses:${Region}:${Account}:addon-subscription/${AddonSubscriptionId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
mailmanager-archive	arn:${Partition}:ses:${Region}:${Account}:mailmanager-archive/${ArchiveId}	aws:ResourceTag/${TagKey}
mailmanager-ingress-point	arn:${Partition}:ses:${Region}:${Account}:mailmanager-ingress-point/${IngressPointId}	aws:ResourceTag/${TagKey} ses:MailManagerIngressPointType
mailmanager-smtp-relay	arn:${Partition}:ses:${Region}:${Account}:mailmanager-smtp-relay/${RelayId}	aws:ResourceTag/${TagKey}
mailmanager-rule-set	arn:${Partition}:ses:${Region}:${Account}:mailmanager-rule-set/${RuleSetId}	aws:ResourceTag/${TagKey}
mailmanager-traffic-policy	arn:${Partition}:ses:${Region}:${Account}:mailmanager-traffic-policy/${TrafficPolicyId}	aws:ResourceTag/${TagKey}
mailmanager-address-list	arn:${Partition}:ses:${Region}:${Account}:mailmanager-address-list/${AddressListId}	aws:ResourceTag/${TagKey}

Amazon Simple Email Service – Mail Manager の条件キー

Amazon Simple Email Service – Mail Manager では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString
ses:AddonSubscriptionArn	SES アドオンサブスクリプション ARN でアクセスをフィルタリングする	ARN
ses:MailManagerIngressPointType	OPEN や AUTH などの SES Mail Manager イングレスポイントタイプでアクセスをフィルタリングする	String
ses:MailManagerRuleSetArn	SES Mail Manager ルールセット ARN でアクセスをフィルタリングする	ARN
ses:MailManagerTrafficPolicyArn	SES Mail Manager トラフィックポリシー ARN でアクセスをフィルタリングする	ARN

Amazon Simple Email Service v2 のアクション、リソース、および条件キー

Amazon Simple Email Service v2 (サービスプレフィックス: ses) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Simple Email Service v2 で定義されたアクション
- Amazon Simple Email Service v2 で定義されるリソースタイプ
- Amazon Simple Email Service v2 の条件キー

Amazon Simple Email Service v2 で定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchGetMetricData	アクティビティのメトリクスデータを取得する許可を付与	読み取り	configuration-set		
			identity		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CancelExportJob	エクスポートジョブをキャンセルするアクセス許可を付与します	書き込み	export-job*		
				ses:ApiVersion ses:ExportSourceType	
CreateConfigurationSet	新しい設定セットを作成する許可を付与	書き込み	configuration-set*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			dedicated-ip-pool		
			mailmanager-archive		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateConfigurationSetEventDestination	設定セットイベントの宛先を作成する許可を付与	書き込み	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateContact	連絡先を作成する許可を付与	書き込み	contact-list*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateContactList	連絡先リストを作成する許可を付与	書き込み	contact-list*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateCustomVerificationEmailTemplate	新しいカスタム検証 E メールテンプレートを作成する許可を付与	書き込み	custom-verification-email-template*		
				ses:ApiVersion	
CreateDedicatedIpPool	専用 IP アドレスの新しいプールを作成する許可を付与	書き込み	dedicated-ip-pool*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateDeliverabilityTestReport	新しい予測受信箱配置テストを作成する許可を付与	書き込み	identity*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateEmailIdentity	E メール ID の検証プロセスを開始する許可を付与	書き込み	identity*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateEmailIdentityPolicy	指定された ID に対して、指定された送信承認ポリシーを作成する許可を付与	Permissions management	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateEmailTemplate	E メールテンプレートを作成する許可を付与	書き込み	template*		
				ses:ApiVersion	
CreateExportJob	エクスポートジョブを作成するアクセス許可を付与します	書き込み		ses:ApiVersion ses:ExportSourceType	
CreateImportJob	データ送信先のインポートジョブを作成する許可を付与	書き込み		ses:ApiVersion	
CreateMultiRegionEndpoint	新しいマルチリージョンエンドポイントを作成するアクセス許可を付与します	書き込み		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateTenant	新しいテナントを作成するアクセス許可を付与します	書き込み	tenant*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateTenantResourceAssociation	SES リソースをテナントに関連付けるアクセス許可を付与します	書き込み	configuration-set*		
			identity*		
			template*		
			tenant*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
DeleteConfigurationSet	既存の設定セットを削除する許可を付与	書き込み	configuration-set*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteConfigurationSetEventDestination	イベントの送信先を削除するアクセス権限を付与します	書き込み	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteContact	連絡先リストから連絡先を削除する許可を付与	書き込み	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteContactList	すべての連絡先とともに連絡先リストを削除する許可を付与	書き込み	contact-list*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteCustomVerificationEmailTemplate	既存のカスタム検証 E メールテンプレートを削除する許可を付与	書き込み	custom-verification-email-template*		
				ses:ApiVersion	
DeleteDedicatedIpPool	専用 IP プールを削除する許可を付与	書き込み	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailIdentity	E メール ID を削除する許可を付与	書き込み	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteEmailIdentityPolicy	指定された ID (E メールアドレスまたはドメイン) に対して、指定された送信承認ポリシーを削除する許可を付与	Permissions management	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailTemplate	E メールテンプレートを削除する許可を付与	書き込み	template*		
				ses:ApiVersion	
DeleteMultiRegionEndpoint	マルチリージョンエンドポイントを削除するアクセス許可を付与します	書き込み	multi-region-endpoint*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteSuppressedDestination	アカウントのサプレッションリストから E メールアドレスを削除する許可を付与	書き込み		ses:ApiVersion	
DeleteTenant	テナントを削除するアクセス許可を付与します	書き込み	tenant*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteTenantResourceAssociation	テナントから関連付けられた SES リソースを削除するアクセス許可を付与します	書き込み	configuration-set*		
			identity*		
			template*		
			tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetAccount	アカウントの E メール送信ステータスおよび機能に関する情報を取得するためのアクセス許可を付与します	読み込み		ses:ApiVersion	
GetBlacklistReports	専用 IP アドレスまたは追跡対象ドメインが表示される拒否リストの一覧を取得するためのアクセス許可を付与します	読み込み		ses:ApiVersion	
GetConfigurationSet	既存の設定セットに関する情報を取得するためのアクセス許可を付与します	読み込み	configuration-set*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetConfigurationSetEventDestinations	設定セットに関連付けられているイベント送信先のリストを取得する許可を付与	読み込み	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetContact	連絡先リストから連絡先を返すアクセス許可を付与します	読み込み	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetContactList	連絡先リストのメタデータを返すアクセス許可を付与します	読み込み	contact-list*		
				ses:ApiVersion	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetCustomVerificationEmailTemplate	指定したテンプレート名のカスタム E メール検証テンプレートを返すアクセス許可を付与します	読み込み	custom-verification-email-template*		
				ses:ApiVersion	
GetDedicatedIp	専用 IP アドレスに関する情報を取得するためのアクセス許可を付与します	読み取り		ses:ApiVersion	
GetDedicatedIpPool	専用 IP プールに関する情報を取得するアクセス権限を付与する	読み取り	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDedicatedIps	専用 IP アドレスを専用の IP プールに一覧表示する許可を付与	読み込み	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetDeliverabilityDashboardOptions	配信性能ダッシュボードのステータスを取得するためのアクセス許可を付与します	読み込み		ses:ApiVersion	
GetDeliverabilityTestReport	受信箱配置の予測テストの結果を取得するためのアクセス許可を付与します	読み込み	deliverability-test-report*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDomainDeliverabilityCampaign	特定のキャンペーンのすべての配信性能データを取得するためのアクセス許可を付与します	読み込み		ses:ApiVersion	
GetDomainStatisticsReport	E メールの送信に使用するドメインの受信箱配置とエンゲージメント率を取得する許可を付与	読み込み	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailIdentity	特定の ID に関する情報を取得するためのアクセス許可を付与します	読み込み	identity*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailIdentityPolicies	指定された ID (E メールアドレスまたはドメイン) に対して要求された送信承認ポリシーを返すアクセス許可を付与します	読み込み	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailTemplate	指定したテンプレートのテンプレートオブジェクト (件名、HTML 部分、およびテキスト部分など) を返すアクセス許可を付与します	読み取り	template*		
				ses:ApiVersion	
GetExportJob	エクスポートジョブに関する情報を取得するためのアクセス許可を付与します	読み取り	export-job*		
				ses:ApiVersion ses:ExportSourceType	
GetImportJob	インポートジョブに関する情報を提供する許可を付与	読み取り	import-job*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ses:ApiVersion	
GetMessageInsights	メッセージに関する洞察を提供するアクセス許可を付与します	読み取り		ses:ApiVersion	
GetMultiRegionEndpoint	マルチリージョンエンドポイントに関する情報を取得する許可を付与	読み取り	multi-region-endpoint*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetReputationEntity	評価エンティティのステータスに関する情報を取得するアクセス許可を付与します	読み取り	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetSuppressedDestination	アカウントのサプレッションリストに登録されている特定の E メールアドレスに関する情報を取得するためのアクセス許可を付与します	読み取り		ses:ApiVersion	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetTenant	テナントに関する情報を取得するアクセス許可を付与します	読み取り	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListConfigurationSets	アカウントのすべての設定セットを一覧表示する許可を付与	リスト		ses:ApiVersion	
ListContactLists	アカウントで利用可能なすべての連絡先リストを一覧表示する許可を付与	リスト		ses:ApiVersion	
ListContacts	特定の連絡先リストに存在する連絡先の一覧を表示する許可を付与	リスト	contact-list*		
				ses:ApiVersion	
ListCustomVerificationEmailTemplates	アカウントの既存のカスタム検証 E メールテンプレートをすべて一覧表示する許可を付与	リスト		ses:ApiVersion	
ListDedicatedIpPools	アカウントのすべての専用 IP プールを一覧表示する許可を付与	リスト		ses:ApiVersion	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListDeliverabilityTestReports	ステータスに関係なく、アカウントで実行した受信箱配置の予測テストのリストを取得する許可を付与	リスト		ses:ApiVersion	
ListDomainDeliverabilityCampaigns	指定した期間内に特定のドメインを使用して E メールを送信したキャンペーンの配信性能データを一覧表示する許可を付与	読み込み		ses:ApiVersion	
ListEmailIdentities	アカウントの E メール ID を一覧表示する許可を付与	リスト		ses:ApiVersion	
ListEmailTemplates	アカウントのすべての E メールテンプレートを一覧表示する許可を付与	リスト		ses:ApiVersion	
ListExportJobs	アカウントのすべてのエクスポートジョブを一覧表示するアクセス許可を付与します	リスト		ses:ApiVersion ses:ExportSourceType	
ListImportJobs	アカウントのすべてのインポートジョブを一覧表示する許可を付与	リスト		ses:ApiVersion	
ListMultiRegionEndpoints	アカウントのすべてのマルチリージョンエンドポイントを一覧表示するアクセス許可を付与します	リスト		ses:ApiVersion	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListRecommendations	アカウントの推奨事項を一覧表示する許可を付与	読み取り	identity		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListReputationEntities	評価エンティティのリストを取得するアクセス許可を付与します	リスト	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListResourceTenants	SES リソースに関連付けられているすべてのテナントを一覧表示するアクセス許可を付与します	リスト	configuration-set*		
			identity*		
			template*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListSuppressedDestinations	アカウントのサプレッションリストに登録されている E メールアドレスを一覧表示する許可を付与	読み込み		ses:ApiVersion	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTagsForResource	アカウントの特定のリソースに関連付けられているタグ (キーと値) のリストを取得する許可を付与	読み取り	configuration-set		
			contact-list		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
			tenant		
				ses:ApiVersion	
ListTenantResources	テナントに関連付けられているすべてのリソースを一覧表示するアクセス許可を付与します	リスト	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListTenants	アカウントのすべてのテナントを一覧表示するアクセス許可を付与します	リスト		ses:ApiVersion	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutAccountDedicatedIpWarmupAttributes	専用 IP アドレスの自動ウォームアップ機能を有効または無効にする許可を付与	書き込み		ses:ApiVersion	
PutAccountDetails	アカウントの詳細を更新する許可を付与	書き込み		ses:ApiVersion	
PutAccountSendingAttributes	アカウントの E メール送信機能を有効または無効にする許可を付与	書き込み		ses:ApiVersion	
PutAccountSuppressionAttributes	アカウントレベルのサプレッションリストの設定を変更する許可を付与	書き込み		ses:ApiVersion	
PutAccountVdmAttributes	アカウントの VDM 設定を変更する許可を付与	書き込み		ses:ApiVersion	
PutConfigurationSetArchivingOptions	設定セットを Mail Manager アーカイブに関連付けるアクセス許可を付与します	書き込み	configuration-set*		
			mailmanager-archive		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutConfigurationSetDeliveryOptions	設定セットを専用 IP プールに関連付けるアクセス許可を付与します	書き込み	configuration-set*		
			dedicated-ip-pool		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetReputationOptions	特定の設定セットを使用して送信する E メールの評価メトリクスの収集を有効または無効にする許可を付与	書き込み	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetSendingOptions	特定の設定セットを使用するメッセージの E メール送信を有効または無効にする許可を付与	書き込み	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutConfigurationSetSuppressionOptions	特定の設定セットのアカウントサプレッションリストの設定を指定する許可を付与	書き込み	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetTrackingOptions	特定の設定セットに関して送信する E メールの開封とクリックの追跡要素に使用するカスタムドメインを指定する許可を付与	書き込み	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetVdmOptions	特定の設定セットのアカウントレベルの VDM 設定を上書きする許可を付与	書き込み	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpInPool	専用 IP アドレスを既存の専用 IP プールに移動する許可を付与	書き込み	dedicated-ip-pool*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpPoolScalingAttributes	専用 IP プールを標準からマネージドに移行する許可を付与	書き込み	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpWarmupAttributes	専用 IP ウォームアップ属性を設定するためのアクセス許可を付与します	書き込み		ses:ApiVersion	
PutDeliverabilityDashboardOption	配信性能ダッシュボードを有効または無効にする許可を付与	書き込み		ses:ApiVersion	
PutEmailIdentityConfigurationSetAttributes	設定セットを E メール ID に関連付けるアクセス許可を付与します	書き込み	identity*		
			configuration-set		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityDkimAttributes	E メール ID の DKIM 認証を有効または無効にする許可を付与	書き込み	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityDkimSigningAttributes	E メールドメイン ID の DKIM 認証設定を構成または変更する許可を付与	書き込み	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityFeedbackAttributes	E メール ID のフィードバック転送を有効または無効にする許可を付与	書き込み	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutEmailIdentityMailFromAttributes	E メール ID のカスタム MAIL FROM ドメイン設定を有効または無効にする許可を付与	書き込み	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutSuppressedDestination	サプレッションリストに E メールアドレスを追加する許可を付与	書き込み		ses:ApiVersion	
ReplicateEmailIdentityDkimSigningKey [アクセス許可のみ]	E メール ID DKIM 署名キーをレプリケートするアクセス許可を付与します	権限の管理	identity*		
				ses:ReplicaRegion	
SendBulkEmail	複数の送信先に E メールメッセージを作成する許可を付与	書き込み	identity*		
			template*		
			configuration-set		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ses:ApiVersion ses:MultiRegionEndpointId ses:TenantName	
SendCustomVerificationEmail	ID の一覧に E メールアドレスを追加して検証を試みるアクセス許可を付与します	書き込み	custom-verification-email-template*		
				ses:ApiVersion	
SendEmail	E メールメッセージを送信する許可を付与	書き込み	identity*		
			configuration-set		
			template		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients ses:MultiRegionEndpointId ses:TenantName	
TagResource	指定したリソースに 1 つ以上のタグ (キーと値) を追加する許可を付与	タグ付け	configuration-set		
			contact-list		
			dedicated-ip-pool		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			deliverability-test-report		
			identity		
			tenant		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
TestRenderEmailTemplate	テンプレートと一連の置換データが提供されている場合、E メール の MIME コンテンツのプレビューを作成する許可を付与	書き込み	template*		
				ses:ApiVersion	
UntagResource	指定したリソースから 1 つ以上のタグ (キーと値) を削除する許可を付与	タグ付け	configuration-set		
			contact-list		
			dedicated-ip-pool		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			deliverability-test-report		
			identity		
			tenant		
				ses:ApiVersion aws:TagKeys	
UpdateConfigurationSetEventDestination	設定セットのイベント送信先の設定を更新する許可を付与	書き込み	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateContact	リストの連絡先の設定を更新する許可を付与	書き込み	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateContactList	連絡先リストのメタデータを更新する許可を付与	書き込み	contact-list*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateCustomVerificationEmailTemplate	既存のカスタム検証 E メールテンプレートを更新する許可を付与	書き込み	custom-verification-email-template*		
				ses:ApiVersion	
UpdateEmailIdentityPolicy	指定された ID (E メールアドレスまたはドメイン) に対して、指定された送信承認ポリシーを更新する許可を付与	Permissions management	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateEmailTemplate	E メールテンプレートを更新する許可を付与	書き込み	template*		
				ses:ApiVersion	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateReputationEntityCustomerManagedStatus	カスタマー管理の送信ステータスを更新する許可を付与	書き込み	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateReputationEntityPolicy	評価ポリシーを割り当てるアクセス許可を付与します	書き込み	reputation-policy*		
			tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Amazon Simple Email Service v2 で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
reputation-policy	arn:${Partition}:ses:${Region}:aws:reputation-policy/${ReputationPolicyName}	
configuration-set	arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}	aws:ResourceTag/${TagKey}
contact-list	arn:${Partition}:ses:${Region}:${Account}:contact-list/${ContactListName}	aws:ResourceTag/${TagKey}
custom-verification-email-template	arn:${Partition}:ses:${Region}:${Account}:custom-verification-email-template/${TemplateName}	
dedicated-ip-pool	arn:${Partition}:ses:${Region}:${Account}:dedicated-ip-pool/${DedicatedIPPool}	aws:ResourceTag/${TagKey}
deliverability-test-report	arn:${Partition}:ses:${Region}:${Account}:deliverability-test-report/${ReportId}	aws:ResourceTag/${TagKey}
export-job	arn:${Partition}:ses:${Region}:${Account}:export-job/${ExportJobId}	
identity	arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}	aws:ResourceTag/${TagKey}
import-job	arn:${Partition}:ses:${Region}:${Account}:import-job/${ImportJobId}	

リソースタイプ	ARN	条件キー
template	arn:${Partition}:ses:${Region}:${Account}:template/${TemplateName}	
multi-region-endpoint	arn:${Partition}:ses:${Region}:${Account}:multi-region-endpoint/${EndpointName}	
mailmanager-archive	arn:${Partition}:ses:${Region}:${Account}:mailmanager-archive/${ArchiveId}	aws:ResourceTag/${TagKey}
tenant	arn:${Partition}:ses:${Region}:${Account}:tenant/${TenantName}/${TenantId}	aws:ResourceTag/${TagKey}

Amazon Simple Email Service v2 の条件キー

Amazon Simple Email Service v2 では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString
ses:ApiVersion	SES API バージョンでアクセスをフィルタリングします	String
ses:ExportSourceType	エクスポートソースタイプによるアクセスをフィルタリングします	String
ses:FeedbackAddress	E メールフィードバック転送によって送信されたバウンスおよび苦情の場所を指定する「リターンパス」アドレスによるアクセスをフィルタリングします	String
ses:FromAddress	メッセージの「From」アドレスによるアクセスをフィルタリングします	String
ses:FromDisplayName	メッセージの表示名として使用される「From」アドレスによるアクセスをフィルタリングします	String
ses:MultiRegionEndpointId	E メールの送信に使用されるマルチリージョンエンドポイント ID でアクセスをフィルタリングします	String
ses:Recipients	「To」、「CC」、「BCC」アドレスを含むメッセージの受取人アドレスによるアクセスをフィルタリングします	ArrayOfString
ses:ReplicaRegion	ドメイン DKIM 署名キーをレプリケートするためのレプリカリージョンでアクセスをフィルタリングします	ArrayOfString
ses:TenantName	E メールの送信に使用されるテナント名でアクセスをフィルタリングします	String

Amazon Simple Workflow Service のアクション、リソース、および条件キー

Amazon Simple Workflow Service (サービスプレフィックス: swf) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Simple Workflow Service で定義されるアクション
- Amazon Simple Workflow Service で定義されるリソースタイプ
- Amazon Simple Workflow Service の条件キー

Amazon Simple Workflow Service で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイ

プが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelTimer [アクセス許可のみ]	以前にスタートしたタイマーをキャンセルし、履歴に TimerCanceled イベントを記録するアクセス許可を付与します	書き込み	domain*		
CancelWorkflowExecution [アクセス許可のみ]	ワークフローの実行を閉じて WorkflowExecutionCanceled イベントを履歴に記録するアクセス許可を付与します	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CompleteWorkflowExecution [アクセス許可のみ]	ワークフローの実行を閉じて WorkflowExecutionCompleted イベントを履歴に記録するアクセス許可を付与します	書き込み	domain*		
ContinueAsNewWorkflowExecution [アクセス許可のみ]	ワークフローの実行を閉じて、同じワークフロー ID と一意の runId を使用し、同じタイプの新しいワークフロー実行をスタートするアクセス許可を付与します	書き込み	domain*		
CountClosedWorkflowExecutions	指定されたフィルタリング条件を満たす特定のドメイン内で、クローズ状態のワークフロー実行数を返すアクセス許可を付与します	読み込み	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CountOpenWorkflowExecutions	指定されたフィルタリング条件を満たす特定のドメイン内で、オープン状態のワークフロー実行数を返すアクセス許可を付与します	読み込み	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
CountPendingActivityTasks	指定されたタスクリストのアクティビティタスクの推定数を返すアクセス許可を付与します	読み込み	domain*		
				swf:taskList.name	
CountPendingDecisionTasks	指定されたタスクリストの決定タスクの推定数を返すアクセス許可を付与します	読み取り	domain*		
				swf:taskList.name	
DeleteActivityType	指定されたアクティビティタイプを削除する許可を付与する	書き込み	domain*		
				swf:activityType.name swf:activityType.version	
DeleteWorkflowType	指定されたワークフロータイプを削除する許可を付与する	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				swf:workflowType.name swf:workflowType.version	
DeprecateActivityType	指定されたアクティビティタイプを非推奨にするアクセス許可を付与します	書き込み	domain*		
				swf:activityType.name swf:activityType.version	
DeprecateDomain	指定されたドメインを非推奨にするアクセス許可を付与します	書き込み	domain*		
DeprecateWorkflowType	指定されたワークフロータイプを非推奨にするアクセス許可を付与します	書き込み	domain*		
				swf:workflowType.name swf:workflowType.version	
DescribeActivityType	指定されたアクティビティタイプに関する情報を返すアクセス許可を付与します	読み込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				swf:activityType.name swf:activityType.version	
DescribeDomain	説明とステータスを含む、指定されたドメインに関する情報を返すアクセス許可を付与します	読み込み	domain*		
DescribeWorkflowExecution	指定されたワークフローの実行に関する情報(ワークフローのタイプと一部の統計を含む) を返すアクセス許可を付与します	読み込み	domain*		
DescribeWorkflowType	指定されたワークフロータイプに関する情報を返すアクセス許可を付与します	読み取り	domain*		
				swf:workflowType.name swf:workflowType.version	
FailWorkflowExecution [許可のみ]	ワークフローの実行を閉じて WorkflowExecutionFailed イベントを履歴に記録するアクセス許可を付与します	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetWorkflowExecutionHistory	指定されたワークフローの実行履歴を返すアクセス許可を付与します	読み込み	domain*		
ListActivityTypes	指定された名前と登録ステータスと一致する指定されたドメインで、すべての登録されたアクティビティに関する情報を返すアクセス許可を付与します	リスト	domain*		
ListClosedWorkflowExecutions	フィルタリング条件を満たす指定されたドメイン内の、クローズ状態のワークフロー実行数のリストを返すアクセス許可を付与します	リスト	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
ListDomains	アカウントに登録されているドメインのリストを返すアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListOpenWorkflowExecutions	フィルタリング条件を満たす指定されたドメイン内の、オープン状態のワークフロー実行数のリストを返すアクセス許可を付与します	リスト	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
ListTagsForResource	SWF AWS リソースのタグを一覧表示するアクセス許可を付与します	リスト	domain		
ListWorkflowTypes	指定されたドメインのワークフロータイプに関する情報を返すアクセス許可を付与します	リスト	domain*		
PollForActivityTask	指定されたアクティビティ taskList から ActivityTask を取得するために、ワーカーにアクセス許可を付与します	書き込み	domain*		
				swf:taskList.name	
PollForDecisionTask	指定された決定 taskList から DecisionTask を取得するために、ディサイダーにアクセス許可を付与します	書き込み	domain*		
				swf:taskList.name	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RecordActivityTaskHeartbeat	指定された taskToken によって表される ActivityTask がまだ進行中であることをサービスに報告するために、ワーカーにアクセス許可を付与します	書き込み	domain*		
RecordMarker [アクセス許可のみ]	履歴に MarkerRecorded イベントを記録するアクセス許可を付与します	書き込み	domain*		
RegisterActivityType	指定されたドメインに新しいアクティビティタイプとその構成設定を登録するアクセス許可を付与します	書き込み	domain*		
				swf:defaultTaskList.name swf:name swf:version	
RegisterDomain	新しいドメインを登録するアクセス許可を付与します	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
RegisterWorkflowType	指定されたドメインに新しいワークフロータイプとその構成設定を登録するアクセス許可を付与します	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				swf:defaultTaskList.name swf:name swf:version	
RequestCancelActivityTask [アクセス許可のみ]	以前にスケジュールされたアクティビティタスクをキャンセルするアクセス許可を付与します	書き込み	domain*		
RequestCancelExternalWorkflowExecution [アクセス許可のみ]	指定された外部ワークフローの実行をキャンセルするリクエストを要求するアクセス許可を付与します	書き込み	domain*		
RequestCancelWorkflowExecution	特定のドメイン、workflowId、runId によって識別される現在実行中のワークフロー実行に WorkflowExecutionCancelRequested イベントを記録するアクセス許可を付与します	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RespondActivityTaskCanceled	taskToken によって識別された ActivityTask が正常にキャンセルされたことをサービスに伝えるために、ワーカーにアクセス許可を付与します	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RespondActivityTaskCompleted	taskToken によって識別された ActivityTask が正常に完了したことを、その結果 (提供されている場合) とともにサービスに伝えるために、ワーカーにアクセス許可を付与します	書き込み	domain*		
				swf:activityType.name swf:activityType.version swf:tagList.member.0 swf:tagList.member.1 swf:tagList.member.2 swf:tagList.member.3 swf:tagList.member.4 swf:taskList.name	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				swf:workflowType.name swf:workflowType.version	
RespondActivityTaskFailed	taskToken によって識別された ActivityTask が失敗したことをその理由 (指定されている場合) とともにサービスに伝えるために、ワーカーにアクセス許可を付与します	書き込み	domain*		
RespondDecisionTaskCompleted	taskToken によって識別された DecisionTask が正常に完了したことをサービスに伝えるために、ディサイダーにアクセス許可を付与します	書き込み	domain*		
ScheduleActivityTask [アクセス許可のみ]	アクティビティタスクをスケジューリングするアクセス許可を付与します	書き込み	domain*		
SignalExternalWorkflowExecution [アクセス許可のみ]	指定された外部ワークフローの実行および記録を配信するシグナルをリクエストするアクセス許可を付与します	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SignalWorkflowExecution	ワークフロー実行履歴に WorkflowExecutionSignaled イベントを記録し、特定のドメイン、workflowId および runId によって識別されるワークフロー実行の決定タスクを作成するアクセス許可を付与します	書き込み	domain*		
StartChildWorkflowExecution [アクセス許可のみ]	子ワークフローの実行開始をリクエストするアクセス許可を付与します	書き込み	domain*		
StartTimer [アクセス許可のみ]	ワークフロー実行のタイマーをスタートするアクセス許可を付与します	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartWorkflowExecution	指定された workflowId と入力データを使用して、指定されたドメインでワークフロータイプの実行をスタートするアクセス許可を付与します	書き込み	domain*	swf:tagList.member.0 swf:tagList.member.1 swf:tagList.member.2 swf:tagList.member.3 swf:tagList.member.4 swf:taskList.name swf:workflowType.name swf:workflowType.version	
TagResource		Tagging	domain		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	SWF AWS リソースにタグを付けるアクセス許可を付与します			aws:TagKeys aws:RequestTag/${TagKey}	
TerminateWorkflowExecution	WorkflowExecutionTerminated イベントを記録し、特定のドメイン、runId、workflowId によって識別されるワークフロー実行を強制的に終了するアクセス許可を付与します	書き込み	domain*		
UndeprecateActivityType	以前に非推奨とされたアクティビティタイプの非推奨状態を解除するアクセス許可を付与します	書き込み	domain*		
				swf:activityType.name swf:activityType.version	
UndeprecateDomain	以前に非推奨とされたドメインの非推奨状態を解除するアクセス許可を付与します	書き込み	domain*		
UndeprecateWorkflowType	以前に非推奨とされたワークフロータイプの非推奨状態を解除するアクセス許可を付与します	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				swf:workflowType.name swf:workflowType.version	
UntagResource	SWF AWS リソースからタグを削除するアクセス許可を付与します	Tagging	domain		
				aws:TagKeys	

Amazon Simple Workflow Service で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
domain	`arn:${Partition}:swf::${Account}:/domain/${DomainName}`	aws:ResourceTag/${TagKey}

Amazon Simple Workflow Service の条件キー

Amazon Simple Workflow Service は、IAM ポリシーの `Condition` 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストのタグでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースのタグでアクセスをフィルタリングします	String
aws:TagKeys	キーのタグでアクセスをフィルタリングします	ArrayOfString
swf:activityType.name	アクティビティタイプ名でアクセスをフィルタリングします	String
swf:activityType.version	アクティビティタイプのバージョンでアクセスをフィルタリングします	String
swf:defaultTaskList.name	デフォルトのタスクリスト名でアクセスをフィルタリングします	String
swf:name	アクティビティ名またはワークフロー名でアクセスをフィルタリングします	String
swf:tagFilter.tag	tagFilter.tag 値でアクセスをフィルタリングします	String
swf:tagList.member.0	指定されたタグでアクセスをフィルタリングします	String
swf:tagList.member.1	指定されたタグでアクセスをフィルタリングします	String
swf:tagList.member.2	指定されたタグでアクセスをフィルタリングします	String
swf:tagList.member.3	指定されたタグでアクセスをフィルタリングします	String

条件キー	説明	[Type] (タイプ)
swf:tagList.member.4	指定されたタグでアクセスをフィルタリングします	String
swf:taskList.name	tasklist 名でアクセスをフィルタリングします	String
swf:typeFilter.name	タイプフィルター名でアクセスをフィルタリングします	String
swf:typeFilter.version	タイプフィルターのバージョンでアクセスをフィルタリングします	String
swf:version	アクティビティまたはワークフローのバージョンでアクセスをフィルタリングします	String
swf:workflowType.name	ワークフロータイプ名でアクセスをフィルタリングします	String
swf:workflowType.version	ワークフロータイプのバージョンでアクセスをフィルタリングします	String

Amazon SimpleDB のアクション、リソース、および条件キー

Amazon SimpleDB (サービスプレフィックス: sdb) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon SimpleDB で定義されるアクション

- Amazon SimpleDB で定義されるリソースタイプ
- Amazon SimpleDB の条件キー

Amazon SimpleDB で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BatchDeleteAttributes	1 回の呼び出しで複数の DeleteAttributes オペレーションを実行し、ラウンドトリップとレイテンシーを減らすことができます	書き込み	domain*		
BatchPutAttributes	BatchPutAttributes オペレーションを使用すると、1 回の呼び出しで複数の PutAttribute オペレーションを実行することができます。BatchPutAttributes オペレーションを使用すると、1 回の呼び出しで複数の PutAttribute オペレーションを実行できます	書き込み	domain*		
CreateDomain	CreateDomain オペレーションでは、新しいドメインを作成できます	書き込み	domain*		
DeleteAttributes	項目に関連付けられた 1 つまたは複数の属性を削除します	書き込み	domain*		
DeleteDomain	DeleteDomain オペレーションでは、ドメインを削除できます	書き込み	domain*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DomainMetadata	ドメインの作成日時、項目と属性の数、属性の名前と値のサイズなど、ドメインに関する情報を返します	読み取り	domain*		
GetAttributes	項目に関連付けられているすべての属性を返します	読み取り	domain*		
ListDomains	ListDomains の説明	リスト			
PutAttributes	PutAttributes オペレーションでは、項目内における属性の作成または置き換えができます	書き込み	domain*		
Select	Select の説明	Read	domain*		

Amazon SimpleDB で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
domain	`arn:${Partition}:sdb:${Region}:${Account}:domain/${DomainName}`	

Amazon SimpleDB の条件キー

SimpleDB には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS SimSpace Weaver のアクション、リソース、および条件キー

AWS SimSpace Weaver (サービスプレフィックス: simspaceweaver) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS SimSpace Weaver で定義されるアクション
- AWS SimSpace Weaver で定義されるリソースタイプ
- AWS SimSpace Weaver の条件キー

AWS SimSpace Weaver で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSnapshot	スナップショットを作成する許可を付与	書き込み	Simulation*		
DeleteApp	アプリケーションを削除する許可を付与	書き込み	Simulation*		
DeleteSimulation	シミュレーションクを削除する許可の付与	書き込み	Simulation*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeApp	アプリケーションを記述する許可を付与	読み取り	Simulation*		
DescribeSimulation	シミュレーションを記述する許可の付与	読み取り	Simulation*		
ListApps	アプリケーションを一覧表示する許可を付与	読み取り	Simulation*		
ListSimulations	シミュレーションを一覧表示する許可の付与	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り			
StartApp	アプリケーションを開始する許可を付与	書き込み	Simulation*		
StartClock	シミュレーションクロックを開始する許可の付与	書き込み	Simulation*		
StartSimulation	シミュレーションを開始する許可の付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
StopApp	アプリケーションを停止する許可を付与	書き込み	Simulation*		
StopClock	シミュレーションクロックを停止する許可の付与	書き込み	Simulation*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StopSimulation	シミュレーションクを停止する許可の付与	書き込み	Simulation*		
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	Simulation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースのタグを解除する許可を付与	Tagging	Simulation*		
				aws:TagKeys	

AWS SimSpace Weaver で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Simulation	`arn:${Partition}:simspaceweaver:${Region}:${Account}:simulation/${SimulationName}`	aws:ResourceTag/${TagKey}

AWS SimSpace Weaver の条件キー

AWS SimSpace Weaver では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストで渡されたタグによりアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグによりアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーによりアクセスをフィルタリングします	ArrayOfString

AWS Snow Device Management のアクション、リソース、および条件キー

AWS Snow Device Management (サービスプレフィックス: snow-device-management) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Snow Device Management で定義されるアクション

- AWS Snow Device Management で定義されるリソースタイプ
- AWS Snow Device Management の条件キー

AWS Snow Device Management で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelTask	リモートデバイスでタスクをキャンセルする許可を付与	書き込み	task*		
CreateTask	リモートデバイスでタスクを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeDevice	リモートで管理されたデバイスを記述する許可を付与	読み取り	managed-device*		
DescribeDeviceEc2Instances	リモートで管理されたデバイスの EC2 インスタンスを記述する許可を付与	読み取り	managed-device*		
DescribeExecution	タスクの実行を記述する許可を付与	読み取り			
DescribeTask	タスクを記述する許可を付与	読み取り	task*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListDeviceResources	リモートで管理されたデバイスのリソースを一覧表示する許可を付与	リスト	managed-device*		
ListDevices	リモートで管理されたデバイスを一覧表示する許可を付与	リスト			
ListExecutions	タスクの実行を一覧表示する許可を付与	リスト			
ListTagsForResource	リソース (デバイスまたはタスク) のタグを一覧表示する許可を付与	読み取り		aws:RequestTag/${TagKey} aws:TagKeys	
ListTasks	タスクを一覧表示する許可を付与	リスト			
TagResource	リソースにタグを付けるアクセス許可を付与	タグ付け	managed-device		
			task		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースのタグを解除する許可を付与	Tagging	managed-device		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			task		
				aws:TagKeys	

AWS Snow Device Management で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
managed-device	arn:${Partition}:snow-device-management:${Region}:${Account}:managed-device/${ResourceId}	aws:ResourceTag/${TagKey}
task	arn:${Partition}:snow-device-management:${Region}:${Account}:task/${ResourceId}	aws:ResourceTag/${TagKey}

AWS Snow Device Management の条件キー

AWS Snow Device Management では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグのキーと値でアクセスをフィルター	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアによってアクセスをフィルタリングする	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

AWS Snowball のアクション、リソース、および条件キー

AWS Snowball (サービスプレフィックス: snowball) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Snowball で定義されるアクション
- AWS Snowball で定義されるリソースタイプ
- AWS Snowball の条件キー

AWS Snowball で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CancelCluster	クラスタージョブをキャンセルするための許可を付与します	書き込み			
CancelJob	指定されたジョブをキャンセルするための許可を付与しますする	書き込み			
CreateAddress	Snowball の発送先となるアドレスを作成ための許可を付与します	書き込み			
CreateCluster	空のクラスターを作成するための許可を付与します	書き込み			
CreateJob	Amazon S3 とオンプレミスデータセンターの間でデータをインポートまたはエクスポートするジョブを作成するための許可を付与します	書き込み			
CreateLongTermPricing	顧客がジョブの前払い請求契約を追加できるように LongTermPricingListEntry を作成するアクセス許可を付与	書き込み			
CreateReturnShippingLabel	Snow デバイスを に返送するために使用される配送ラベルを作成するアクセス許可を付与します AWS	書き込み			
DescribeAddress	そのアドレスに関する特定の詳細を Address オブジェクト	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	の形式で取得するための許可を付与します				
DescribeAddresses	指定された数の ADDRESS オブジェクトを記述するための許可を付与します	リスト			
DescribeCluster	出荷情報、クラスターのステータス、その他の重要なメタデータなど、特定のクラスターに関する情報を記述するための許可を付与します	読み取り			
DescribeJob	出荷情報、ジョブステータス、その他の重要なメタデータなど、特定のジョブに関する情報を記述するための許可を付与します	読み取り			
DescribeReturnShippingLabel	に返される Snow デバイスの配送ラベルに関する情報を記述するアクセス許可を付与します AWS	読み取り			
GetJobManifest	指定された JobId 値に関連付けられたマニフェストファイルの Amazon S3 署名付き URL へのリンクを取得するための許可を付与します	読み取り			
GetJobUnlockCode	指定されたジョブの UnlockCode コードの値を取得するための許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetSnowballUsage	アカウントの Snowball サービスの制限に関する情報と、アカウントが使用中の Snowball の数を取得するための許可を付与します	読み取り			
GetSoftwareUpdates	指定された JobId に関連付けられた更新ファイルの Amazon S3 署名付き URL を返すための許可を付与します	読み取り			
ListClusterJobs	指定された長さの JobListEntry オブジェクトを一覧表示するための許可を付与します	リスト			
ListClusters	指定された長さの ClusterListEntry オブジェクトを一覧表示するための許可を付与します	リスト			
ListCompatibleImages	Snow デバイスでの使用がサポートされている が所有するさまざまな Amazon EC2 Amazon マシンイメージ (AMIs) のリストを返 AWS アカウント すアクセス許可を付与します	リスト			
ListJobs	指定された長さの JobListEntry オブジェクトを一覧表示するための許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListLongTermPricing	リクエストを行っているアカウントの LongTermPricingListEntry オブジェクトを一覧表示する許可を付与	読み取り			
ListPickupLocations	指定された長さの集荷可能な Address オブジェクトを一覧表示する許可を付与	リスト			
ListServiceVersions	Snow オンデバイスサービス用にサポートされているすべてのバージョンを一覧表示するための許可を付与します	リスト			
UpdateCluster	クラスターの ClusterState 値が AwaitingQuorum 状態にある間に更新するための許可を付与します。クラスターに関連付けられた情報の一部を更新できます	書き込み			
UpdateJob	ジョブの JobState 値が [新規] のときに更新するための許可を付与します。ジョブに関連付けられた情報の一部を更新できます	書き込み			
UpdateJobShipmentState	出荷の状態が別の状態に変わったときに、状態を更新するための許可を付与します	書き込み			
UpdateLongTermPricing	ジョブの特定の前払い請求契約を更新する許可を付与	書き込み			

AWS Snowball で定義されるリソースタイプ

AWS Snowball は、IAM ポリシーステートメントの Resource要素でのリソース ARN の指定をサポートしていません。 AWS Snowball へのアクセスを許可するには、ポリシーで "Resource": "*" を指定します。

AWS Snowball の条件キー

Snowball には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon SNS のアクション、リソース、および条件キー

Amazon SNS (サービスプレフィックス: sns) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon SNS で定義されるアクション
- Amazon SNS で定義されるリソースタイプ
- Amazon SNS の条件キー

Amazon SNS で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddPermission	トピックのアクセスコントロールポリシーにステートメントを追加するアクセス許可	権限の管理	topic*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	を付与し、指定された AWS アカウントに指定されたアクションへのアクセスを付与します				
CheckIfPhoneNumberIsOptedOut	電話番号を受け入れ、電話の所有者がお客様のアカウントからの SMS メッセージの受信をオプトアウトしたかどうかを示すアクセス許可を付与	Read			
ConfirmSubscription	以前の Subscribe アクションでエンドポイントに送信したトークンを検証することによって、メッセージを受信するというエンドポイントの所有者の意思を確認する許可を付与	Write	topic*		
CreatePlatformApplication	デバイスやモバイルアプリを登録できるサポート対象のプッシュ通知サービス (APNS や GCM など) のプラットフォームアプリケーションオブジェクトを作成する許可を付与	Write			iam:PassRole
CreatePlatformEndpoint	サポートされているプッシュ通知サービス (APNS や GCM など) でデバイスおよびモバイルアプリケーションのエンドポイントを作成する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSMSSandboxPhoneNumber	送信先の電話番号を追加し、のその電話番号にワンタイムパスワード (OTP) を送信するアクセス許可を付与しますAWS アカウント	書き込み			
CreateTopic	通知を発行できるトピックを作成する許可を付与	Write	topic*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteEndpoint	Amazon SNS からデバイスとモバイルアプリのエンドポイントを削除する許可を付与	Write			
DeletePlatformApplication	サポートされているプッシュ通知サービス (APNS や GCM など) のプラットフォームアプリケーションオブジェクトを削除する許可を付与	書き込み			
DeleteSMSSandboxPhoneNumber	の検証済みまたは保留中 AWS アカウントの電話番号を削除するアクセス許可を付与します	書き込み			
DeleteTopic	トピックとそのすべてのサブスクリプションを削除する許可を付与	書き込み	topic*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetDataProtectionPolicy	トピックのデータ保護ポリシーを返すアクセス許可を付与	読み取り	topic*		
GetEndpointAttributes	サポートされているプッシュ通知サービス (APNS や GCM など) 上のデバイスのエンドポイント属性を取得する許可を付与	Read			
GetPlatformApplicationAttributes	サポートされているプッシュ通知サービス (APNS や GCM) のプラットフォームアプリケーションオブジェクトの属性を取得する許可を付与	Read			
GetSMSAttributes	アカウントから SMS メッセージを送信するための設定を返すアクセス許可を付与	Read			
GetSMSSandboxAccountStatus	ターゲットリージョンの呼び出し元アカウントのサンドボックスステータスを取得する許可を付与	Read			
GetSubscriptionAttributes	サブスクリプションのすべてのプロパティを返すアクセス許可を付与	Read			
GetTopicAttributes	トピックのすべてのプロパティを返すアクセス許可を付与	Read	topic*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListEndpointsByPlatformApplication	サポートされているプッシュ通知サービス (GCM や APNS など) のデバイスおよびモバイルアプリのエンドポイントとエンドポイント属性を一覧表示する許可を付与	リスト			
ListOriginationNumbers	すべての発信番号とそのメタデータを一覧表示する許可を付与	リスト			
ListPhoneNumbersOptedOut	オプトアウトされている電話番号のリストを返すアクセス許可を付与SMS メッセージを送信することはできません	Read			
ListPlatformApplications	サポートされているプッシュ通知サービス (APNS や GCM など) のプラットフォームアプリケーションオブジェクトを一覧表示する許可を付与	リスト			
ListSMSSandboxPhoneNumbers	発信元アカウントの現在の保留中および確認済みの宛先電話番号を一覧表示する許可を付与	リスト			
ListSubscriptions	リクエスタのサブスクリプションのリストを返すアクセス許可を付与	リスト			
ListSubscriptionsByTopic	特定のトピックのサブスクリプションのリストを返すアクセス許可を付与	リスト	topic*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTagsForResource	指定した Amazon SNS トピックに追加されたすべてのタグを一覧表示する許可を付与	Read	topic		
ListTopics	リクエスタのトピックのリストを返すアクセス許可を付与	リスト			
OptInPhoneNumber	現在オプトアウトされている電話番号をオプトインするアクセス許可を付与し、その番号への SMS メッセージの送信を再開することを許可します	Write			
Publish	トピックのサブスクライブされているエンドポイントすべてにメッセージを送信する許可を付与	書き込み	topic*		
PutDataProtectionPolicy	トピックの所有者がデータ保護ポリシーを設定できるようにするアクセス許可を付与	書き込み	topic*		
RemovePermission	トピックのアクセス制御ポリシーからステートメントを削除する許可を付与	Permissions management	topic*		
SetEndpointAttributes	サポートされているいずれかのプッシュ通知サービス (APNS や GCM など) 上のデバイスのエンドポイント属性を設定する許可を付与	Write			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SetPlatformApplicationAttributes	サポートされているプッシュ通知サービス (APNS や GCM など) にプラットフォームアプリケーションオブジェクトの属性を設定する許可を付与	Write			iam:PassRole
SetSMSAttributes	SMS メッセージの送信と毎日の SMS 使用状況レポートの受信のためのデフォルト設定を設定する許可を付与	Write			
SetSubscriptionAttributes	サブスクリプション所有者がトピックの属性を新しい値に設定することを許可する許可を付与	Write			
SetTopicAttributes	トピックの所有者がトピックの属性を新しい値に設定することを許可する許可を付与	権限の管理	topic*		iam:PassRole
Subscribe	エンドポイントに確認メッセージを送信することによってエンドポイントのサブスクライブを準備する許可を付与	Write	topic*		
				sns:Endpoint sns:Protocol	
TagResource	指定した Amazon SNS トピックにタグを追加する許可を付与	タグ付け	topic		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
Unsubscribe	サブスクリプションを削除する許可を付与	Write			
UntagResource	指定した Amazon SNS トピックからタグを削除する許可を付与	Tagging	topic		
				aws:TagKeys	
VerifySMSSandboxPhoneNumber	のワンタイムパスワード (OTP) を使用して送信先電話番号を検証するアクセス許可を付与します AWS アカウント	書き込み			

Amazon SNS で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
topic	arn:${Partition}:sns:${Region}:${Account}:${TopicName}	aws:ResourceTag/${TagKey}

Amazon SNS の条件キー

Amazon SNS では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストからのタグに基づいてアクセスをフィルタリング	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグによりアクセスをフィルタリングします	String
aws:TagKeys	リクエストからのタグキーに基づいてアクセスをフィルタリング	ArrayOfString
sns:Endpoint	URL、E メールアドレス、または Subscribe リクエストや以前に確認されたサブスクリプションの ARN に基づいてアクセスをフィルタリング	String
sns:Protocol	Subscribe リクエストまたは以前に確認されたサブスクリプションからのプロトコル値に基づいてアクセスをフィルタリング	String

AWS SQL Workbench のアクション、リソース、条件キー

AWS SQL Workbench (サービスプレフィックス: sqlworkbench) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS SQL Workbench で定義されるアクション
- AWS SQL Workbench で定義されるリソースタイプ
- AWS SQL Workbench の条件キー

AWS SQL Workbench で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateConnectionWithChart [アクセス許可のみ]	接続をチャートに関連付ける許可を付与	書き込み	chart*		
			connection*		
AssociateConnectionWithTab [アクセス許可のみ]	接続をタブに関連付ける許可を付与	書き込み	connection*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateNotebookWithTab [アクセス許可のみ]	ノートブックをタブに関連付けるアクセス許可を付与	書き込み	notebook*		
AssociateQueryWithTab [アクセス許可のみ]	クエリをタブに関連付ける許可を付与	書き込み	query*		
BatchDeleteFolder [アクセス許可のみ]	アカウントでフォルダを削除する許可を付与	書き込み			
BatchGetNotebookCell [アクセス許可のみ]	アカウントでノートブックセルの内容を取得するアクセス許可を付与	読み取り	notebook*		
CreateAccount [許可のみ]	SQLWorkbench アカウントを作成する許可を付与	書き込み			
CreateChart [アクセス許可のみ]	アカウントで新しい保存済みグラフを作成する許可を付与	書き込み	chart*		
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateConnection [アクセス許可のみ]	アカウントで新しい接続を作成する許可を付与	書き込み	connection*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateFolder [アクセス許可のみ]	アカウントでフォルダを作成する許可を付与	書き込み			
CreateNotebook [アクセス許可のみ]	アカウントで新しいノートブックを作成するアクセス許可を付与	書き込み	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNotebookCell [アクセス許可のみ]	アカウントでノートブックセルを作成するアクセス許可を付与	書き込み	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateNotebookFromVersion [アクセス許可のみ]	アカウントでノートブックバージョンから新しいノートブックを作成するアクセス許可を付与	書き込み	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNotebookVersion [アクセス許可のみ]	アカウントでノートブックバージョンを作成するアクセス許可を付与	書き込み	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateSavedQuery [アクセス許可のみ]	アカウントで新しい保存済みクエリを作成する許可を付与	書き込み	query*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChart [アクセス許可のみ]	アカウントでチャートを削除する許可を付与	書き込み	chart*		
DeleteConnection [アクセス許可のみ]	アカウントの接続を削除する許可を付与	書き込み	connection*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteNotebook [アクセス許可のみ]	アカウントでノートブックを削除するアクセス許可を付与	書き込み	notebook*		
DeleteNotebookCell [アクセス許可のみ]	アカウントでノートブックセルを削除するアクセス許可を付与	書き込み	notebook*		
DeleteNotebookVersion [アクセス許可のみ]	アカウントでノートブックセルを削除するアクセス許可を付与	書き込み	notebook*		
DeleteQCustomContext [アクセス許可のみ]	アカウント全体のカスタムコンテキストを削除する許可を付与する	書き込み			
DeleteSavedQuery [アクセス許可のみ]	アカウントで保存されたクエリを削除する許可を付与	書き込み	query*		
DeleteSqlGenerationContext [アクセス許可のみ]	SQL 生成コンテキストを削除するアクセス許可を付与します	書き込み			
DeleteTab [アクセス許可のみ]	アカウントのタブを削除する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DriverExecute [アクセス許可のみ]	Redshift クラスターでクエリを実行する許可を付与	書き込み	connection*		
DuplicateNotebook [アクセス許可のみ]	アカウントで既存のノートブックを複製して新しいノートブックを作成するアクセス許可を付与	書き込み	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ExportNotebook [アクセス許可のみ]	アカウントでノートブックをエクスポートするアクセス許可を付与	読み取り	notebook*		
GenerateSession [許可のみ]	アカウントで新しいセッションを生成する許可を付与	書き込み			
GetAccountInfo [アクセス許可のみ]	アカウント情報を取得する許可を付与	読み取り			
GetAccountSettings [許可のみ]	アカウント設定を取得する許可を付与	読み取り			
GetAutocompletionMetadata [許可のみ]	オートコンプリート用のデータベース構造のメタデータを取得するための許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetAutocompletionResource [許可のみ]	オートコンプリート用のデータベース構造に関する情報を取得するための許可を付与します	読み取り			
GetChart [許可のみ]	アカウントでチャートを取得する許可を付与	読み取り	chart*		
GetConnection [許可のみ]	アカウントで接続を取得する許可を付与	読み取り	connection*		
GetNotebook [許可のみ]	アカウントでノートブックのメタデータを取得するアクセス許可を付与	読み取り	notebook*		
GetNotebookVersion [許可のみ]	アカウントでノートブックバージョンの内容を取得するアクセス許可を付与	読み取り	notebook*		
GetQCustomContext [許可のみ]	アカウント全体のカスタムコンテキストを取得する許可を付与する	読み取り			
GetQSqlPromptQuotas [許可のみ]	Q 生成 SQL 最大プロンプトクォータを取得する許可を付与する	読み取り			
GetQSqlRecommendations [許可のみ]	SQL 推奨事項を取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetQueryExecutionHistory [許可のみ]	アカウントでクエリ実行履歴を取得する許可を付与	読み取り			
GetSavedQuery [許可のみ]	アカウントで保存されたクエリを取得する許可を付与	読み取り	query*		
GetSchemaInference [許可のみ]	ファイルから推測された列とデータ型を取得するための許可を付与します	読み取り			
GetSqlGenerationContext [許可のみ]	SQL 生成コンテキストを取得する許可を付与	読み取り			
GetSqlRecommendations [許可のみ]	SQL 推奨事項を取得する許可を付与	読み取り			
GetUserInfo [許可のみ]	ユーザー情報を取得する許可を付与	読み取り			
GetUserWorkspaceSettings [許可のみ]	アカウントでワークスペース設定を取得する許可を付与	読み取り			
ImportNotebook [許可のみ]	アカウントでノートブックをインポートするアクセス許可を付与	書き込み	notebook*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
ListConnections [アクセス許可のみ]	アカウントで接続を一覧表示する許可を付与	リスト			
ListDatabases [許可のみ]	Redshift クラスターのデータベースを一覧表示する許可を付与	リスト			
ListFiles [許可のみ]	ファイルとフォルダを一覧表示する許可を付与	リスト			
ListNotebookVersions [許可のみ]	アカウントでノートブックバージョンのメタデータを取得するアクセス許可を付与	リスト	notebook*		
ListNotebooks [許可のみ]	アカウントでノートブックを一覧表示するアクセス許可を付与	リスト			
ListQueryExecutionHistory [許可のみ]	アカウントでクエリ実行履歴を一覧表示する許可を付与	リスト			
ListRedshiftClusters [許可のみ]	アカウントで Redshift クラスターを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListSampleDatabases [許可のみ]	サンプルデータベースを一覧表示する許可を付与	読み取り			
ListSavedQueryVersions [許可のみ]	アカウントで保存されたクエリのバージョンを一覧表示する許可を付与	リスト	query*		
ListTabs [許可のみ]	アカウントのタブを一覧表示する許可を付与	リスト			
ListTaggedResources [許可のみ]	タグ付けされたリソースを一覧表示する許可を付与	読み取り			
ListTagsForResource [許可のみ]	SQLWorkbench リソースのタグを一覧表示する許可を付与	読み取り	chart		
			connection		
			notebook		
			query		
PassAccountSettings [許可のみ]	リクエストでアカウント設定を提供するアクセス許可を付与します	書き込み			
PutQCustomContext [アクセス許可のみ]	アカウント全体のカスタムコンテキストを更新する許可を付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutSqlGenerationContext [アクセス許可のみ]	SQL 生成コンテキストを更新する許可を付与	書き込み			
PutTab [アクセス許可のみ]	アカウントでタブを作成または更新する許可を付与	書き込み			
PutUserWorkspaceSettings [アクセス許可のみ]	アカウントでワークスペース設定を更新する許可を付与	書き込み			
RestoreNotebookVersion [アクセス許可のみ]	アカウントでノートブックをあるバージョンに復元するアクセス許可を付与	書き込み	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource [アクセス許可のみ]	SQLWorkbench リソースにタグ付けする許可を付与	Tagging	chart		
			connection		
			notebook		
			query		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [アクセス許可のみ]	SQLWorkbench リソースのタグ付けを解除する許可を付与	Tagging	chart		
			connection		
			notebook		
			query		
				aws:TagKeys	
UpdateAccountConnectionSettings [アクセス許可のみ]	アカウント全体での接続設定を更新する許可を付与	書き込み			
UpdateAccountExportSettings [アクセス許可のみ]	アカウント全体でのエクスポート設定を更新する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateAccountGeneralSettings [アクセス許可のみ]	アカウント全体の全般設定を更新する許可を付与	書き込み			
UpdateAccountQSqlSettings [アクセス許可のみ]	アカウント全体のテキストを SQL 設定に更新する許可を付与	書き込み			
UpdateChart [アクセス許可のみ]	アカウントでチャートを更新する許可を付与	書き込み	chart*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateConnection [アクセス許可のみ]	アカウントで接続を更新する許可を付与	書き込み	connection*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateFileFolder [アクセス許可のみ]	アカウントでファイルを移動する許可を付与	書き込み	chart		
			query		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateFolder [アクセス許可のみ]	アカウントでフォルダの名前と詳細を更新する許可を付与	書き込み			
UpdateNotebook [アクセス許可のみ]	アカウントでノートブックのメタデータを更新するアクセス許可を付与	書き込み	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateNotebookCellContent [アクセス許可のみ]	アカウントでノートブックセルの内容を更新するアクセス許可を付与	書き込み	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateNotebookCellLayout [アクセス許可のみ]	アカウントでノートブックセルのレイアウトを更新するアクセス許可を付与	書き込み	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateSavedQuery [アクセス許可のみ]	アカウントで保存されたクエリを更新する許可を付与	書き込み	query*		
				aws:TagKeys aws:RequestTag/${TagKey}	

AWS SQL Workbench で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
connection	arn:${Partition}:sqlworkbench:${Region}:${Account}:connection/${ResourceId}	aws:ResourceTag/${TagKey}
query	arn:${Partition}:sqlworkbench:${Region}:${Account}:query/${ResourceId}	aws:ResourceTag/${TagKey}
chart	arn:${Partition}:sqlworkbench:${Region}:${Account}:chart/${ResourceId}	aws:ResourceTag/${TagKey}
notebook	arn:${Partition}:sqlworkbench:${Region}:${Account}:notebook/${ResourceId}	aws:ResourceTag/${TagKey}

AWS SQL Workbench の条件キー

AWS SQL Workbench では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon SQS のアクション、リソース、および条件キー

Amazon SQS (サービスプレフィックス: sqs) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon SQS で定義されるアクション
- Amazon SQS で定義されるリソースタイプ
- Amazon SQS の条件キー

Amazon SQS で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddPermission	特定のプリンシパルのキューへの許可を付与	権限の管理	queue*		
CancelMessageMoveTask	進行中のメッセージ移動タスクをキャンセルする許可を付与	書き込み	queue*		
ChangeMessageVisibility	キュー内の指定されたメッセージの可視性タイムアウトを新しい値に変更する許可を付与	書き込み	queue*		
CreateQueue	新しいキューを作成する許可を付与するか、既存のキューの URL を返す	書き込み	queue*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMessage	指定されたキューから指定されたメッセージを削除する許可を付与	書き込み	queue*		
DeleteQueue	キューが空かどうかに関係なく、キュー URL で指定されたキューを削除する許可を付与	書き込み	queue*		
GetQueueAttributes	指定されたキューの属性を取得する許可を付与	読み取り	queue*		
GetQueueUrl	既存のキューの URL を返す許可を付与	読み取り	queue*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListDeadLetterSourceQueues	デッドレターキューを使用して設定された RedrivePolicy キュー属性を持つキューのリストを返す許可を付与	読み取り	queue*		
ListMessageMoveTasks	メッセージ移動タスクを一覧表示する許可を付与	読み取り	queue*		
ListQueueTags	SQS キューに追加されたタグを一覧表示する許可を付与	読み取り	queue*		
ListQueues	キューのリストを返す許可を付与	読み取り			
PurgeQueue	キュー URL によって指定されたメッセージを削除する許可を付与	書き込み	queue*		
ReceiveMessage	指定されたキューから最大 10 件のメッセージを取得する許可を付与	読み取り	queue*		
RemovePermission	指定されたラベルパラメータに一致するキューポリシー内のアクセス許可を取り消す許可を付与	権限の管理	queue*		
SendMessage	指定されたキューにメッセージを配信する許可を付与	書き込み	queue*		
SetQueueAttributes	1 つ以上のキュー属性の値を設定する許可を付与	書き込み	queue*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartMessageMoveTask	メッセージ移動タスクを開始する許可を付与	書き込み	queue*		
TagQueue	指定した SQS キューにタグを追加する許可を付与	Tagging	queue*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagQueue	指定した SQS キューからタグを削除する許可を付与	Tagging	queue*		
				aws:TagKeys	

Amazon SQS で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

> **Note**
>
> キューの ARN は、IAM アクセス許可ポリシーでのみ使用されます。API コールおよび CLI コールでは、代わりにキューの URL を使用します。

リソースタイプ	ARN	条件キー
queue	arn:${Partition}:sqs:${Region}:${Account}:${QueueName}	aws:ResourceTag/${TagKey}

Amazon SQS の条件キー

Amazon SQS は、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Step Functions のアクション、リソース、および条件キー

AWS Step Functions (サービスプレフィックス: states) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Step Functions で定義されるアクション
- AWS Step Functions で定義されるリソースタイプ
- AWS Step Functions の条件キー

AWS Step Functions で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateActivity	アクティビティを作成する許可を付与	Write	activity*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStateMachine	ステートマシンを作成する許可を付与	書き込み	statemachine*		iam:PassRole states:PublishStateMachineVersion
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateStateMachineAlias	ステートマシンのエイリアスを作成する許可を付与	書き込み	statemachine*		
				states:StateMachineQualifier	
DeleteActivity	アクティビティを削除する許可を付与	Write	activity*		
DeleteStateMachine	ステートマシンを削除する許可を付与	書き込み	statemachine*		
DeleteStateMachineAlias	ステートマシンのエイリアスを削除する許可を付与	書き込み	statemachine*		
				states:StateMachineQualifier	
DeleteStateMachineVersion	ステートマシンのバージョンを削除する許可を付与	書き込み	statemachine*		
				states:StateMachineQualifier	
DescribeActivity	アクティビティを記述する許可を付与	Read	activity*		
DescribeExecution	実行を記述する許可を付与	読み取り	execution*		
			express*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeMapRun	マップ実行を記述する許可を付与	読み取り	maprun*		
DescribeStateMachine	ステートマシンを記述する許可を付与	読み取り	statemachine*		
				states:StateMachineQualifier	
DescribeStateMachineAlias	ステートマシンのエイリアスを記述する許可を付与	読み取り	statemachine*		
				states:StateMachineQualifier	
DescribeStateMachineForExecution	実行のためのステートマシンを記述する許可を付与	Read	execution*		
GetActivityTask	実行中のステートマシンによって実行がスケジュールされたタスク (指定されたアクティビティ ARN を持つ) を取得するためにワーカーによって使用されます	Write	activity*		
GetExecutionHistory	指定された実行の履歴をイベントのリストとして返す許可を付与	読み取り	execution*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
InvokeHTTPEndpoint [許可のみ]	HTTP タスクステートの呼び出しする許可を付与	書き込み			
ListActivities	既存のアクティビティを一覧表示する許可を付与	リスト			
ListExecutions	ステートマシンの実行を一覧表示する許可を付与	リスト	maprun*		
			statemachine*		
				states:StateMachineQualifier	
ListMapRuns	実行中のマップ実行を一覧表示する許可を付与	リスト	execution*		
ListStateMachineAliases	ステートマシンのエイリアスを一覧表示する許可を付与	リスト	statemachine*		
				states:StateMachineQualifier	
ListStateMachineVersions	ステートマシンのバージョンを一覧表示する許可を付与	リスト	statemachine*		
ListStateMachines	既存のステートマシンを一覧表示する許可を付与	リスト			
ListTagsForResource		リスト	activity		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	AWS Step Functions リソースのタグを一覧表示するアクセス許可を付与します		statemachine		
PublishStateMachineVersion	ステートマシンのバージョンを公開する許可を付与	書き込み	statemachine*		
RedriveExecution	実行をリドライブする許可を付与	書き込み	execution*		
RevealSecrets [アクセス許可のみ]	実行時に機密データの公開をする許可を付与	読み取り			
SendTaskFailure	taskToken によって識別されたタスクが失敗したことを報告する許可を付与	Write			
SendTaskHeartbeat	指定された taskToken によって表されるタスクがまだ進行中であることを、サービスに報告する許可を付与	Write			
SendTaskSuccess	taskToken によって識別されたタスクが正常に完了したことを報告する許可を付与	Write			
StartExecution	ステートマシンの実行を開始する許可を付与	Write	statemachine*		
				states:StateMachineQualifier	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartSyncExecution	同期高速状態マシンの実行を開始する許可を付与	Write	statemachine*		
				states:StateMachineQualifier	
StopExecution	実行を停止する許可を付与	書き込み	execution*		
TagResource	AWS Step Functions リソースにタグを付けるアクセス許可を付与します	Tagging	activity		
			statemachine		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
TestState	ステートマシンを削除する許可を付与	書き込み			states:RevealSecrets
UntagResource	AWS Step Functions リソースからタグを削除するアクセス許可を付与します	Tagging	activity		
			statemachine		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateMapRun	マップ実行を更新する許可を付与	書き込み	maprun*		
UpdateStateMachine	ステートマシンを更新する許可を付与	書き込み	statemachine*		iam:PassRole states:PublishStateMachineVersion
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateStateMachineAlias	ステートマシンのエイリアスを更新する許可を付与	書き込み	statemachine*		
				states:StateMachineQualifier	
ValidateStateMachineDefinition	ステートマシン定義を検証する許可を付与する	読み取り			

AWS Step Functions で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
activity	arn:${Partition}:states:${Region}:${Account}:activity:${ActivityName}	aws:ResourceTag/${TagKey}
execution	arn:${Partition}:states:${Region}:${Account}:execution:${StateMachineName}:${ExecutionId}	aws:ResourceTag/${TagKey}
express	arn:${Partition}:states:${Region}:${Account}:express:${StateMachineName}:${ExecutionId}:${ExpressId}	
statemachine	arn:${Partition}:states:${Region}:${Account}:stateMachine:${StateMachineName}	aws:ResourceTag/${TagKey}
statemachineversion	arn:${Partition}:states:${Region}:${Account}:stateMachine:${StateMachineName}:${StateMachineVersionId}	aws:ResourceTag/${TagKey}
statemachinealias	arn:${Partition}:states:${Region}:${Account}:stateMachine:${StateMachineName}:${StateMachineAliasName}	aws:ResourceTag/${TagKey}
maprun	arn:${Partition}:states:${Region}:${Account}:mapRun:${StateMachineName}/${MapRunLabel}:${MapRunId}	
labelled execution	arn:${Partition}:states:${Region}:${Account}:execution:${StateMachineName}/${MapRunLabel}:${ExecutionId}	
labelled express	arn:${Partition}:states:${Region}:${Account}:express:${StateMachineName}	

リソースタイプ	ARN	条件キー
	/${MapRunLabel}:${ExecutionId}:${ExpressId}	

AWS Step Functions の条件キー

AWS Step Functions は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString
states:HTTPEndpoint	リクエストで HTTP タスクのステートが許可するエンドポイントでアクセスをフィルタリングします	String
states:HTTPMethod	リクエストで HTTP タスクステートが許可するメソッドでアクセスをフィルタリングします	String
states:StateMachineQualifier	ステートマシン ARN の修飾子でアクセスをフィルタリングします	ArrayOfString

AWS Storage Gateway のアクション、リソースおよび条件キー

AWS Storage Gateway (サービスプレフィックス: `storagegateway`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Storage Gateway で定義されるアクション
- AWS Storage Gateway で定義されるリソースタイプ
- AWS Storage Gateway の条件キー

AWS Storage Gateway で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ActivateGateway	以前ホストにデプロイしたゲートウェイをアクティブ化する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
AddCache	キャッシュされたボリュームゲートウェイのキャッシュとして 1 つまたは複数のゲートウェイローカルディスクを設定する許可を付与	書き込み	gateway*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddTagsToResource	指定されたリソースに 1 つ以上のタグを追加する権限を付与します	タグ付け	cache-report		
			fs-association		
			gateway		
			share		
			tape		
			tapepool		
			volume		
				aws:RequestTag/${TagKey} aws:TagKeys	
AddUploadBuffer	指定したゲートウェイのアップロードバッファとして 1 つまたは複数のゲートウェイローカルディスクを設定する許可を付与	書き込み	gateway*		
AddWorkingStorage	ゲートウェイの作業ストレージとして 1 つまたは複数のゲートウェイローカルディスクを設定する許可を付与	書き込み	gateway*		
AssignTapePool		書き込み	tape*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	指定されたターゲットプールにテープを移動する許可を付与		tapepool*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateFileSystem	Amazon FSx ファイルシステムを Amazon FSX ファイルゲートウェイに関連付けるアクセス許可を付与します。	書き込み	gateway*		ds:DescribeDirectories ec2:DescribeNetworkInterfaces fsx:DescribeFileSystems iam:CreateServiceLinkedRole logs:CreateLogDelivery logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
AttachVolume	ボリュームを iSCSI 接続に接続するアクセス許可を付与してから、ボリュームを指定されたゲートウェイにアタッチする	書き込み	gateway*		
			volume*		
BypassGovernanceRetention	プールのガバナンス保持ロックをバイパスできるようにする許可を付与	書き込み	tapepool*		
CancelArchival	アーカイブプロセスが開始された後で、仮想テープシェルフ (VTS) への仮想テープのアーカイブをキャンセルする許可を付与	書き込み	gateway*		
			tape*		
CancelCacheReport	キャッシュレポートをキャンセルするアクセス許可を付与します	書き込み	cache-report*		
CancelRetrieval	取得プロセスが開始された後で、仮想テープシェルフ (VTS) からゲートウェイへの仮想テープの取得をキャンセルする許可を付与	書き込み	gateway*		
			tape*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateCachediSCSIVolume	指定されたキャッシュゲートウェイでキャッシュボリュームを作成する許可を付与。このオペレーションは、ゲートウェイキャッシュ型ボリュームアーキテクチャでのみサポートされています	書き込み	gateway*		
			volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNFSFileShare	既存のファイルゲートウェイで NFS ファイル共有を作成する許可を付与	書き込み	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSMBFileShare	既存のファイルゲートウェイで SMB ファイル共有を作成する許可を付与	書き込み	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	ボリュームのスナップショットを開始する許可を付与	書き込み	volume*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotFromVolumeRecoveryPoint	ボリュームリカバリポイントからゲートウェイのスナップショットを開始する許可を付与	書き込み	volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorediSCSIVolume	指定されたゲートウェイでボリュームを作成する許可を付与	書き込み	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTapePool	テーププールを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTapeWithBarcode	独自のバーコードを使用して仮想テープを作成する許可を付与	書き込み	gateway*		
			tapepool*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTapes	1 つまたは複数の仮想テープを作成する許可を付与。仮想テープにデータを書き込み、テープをアーカイブします	書き込み	gateway*		
			tapepool*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAutomaticTapeCreationPolicy	ゲートウェイ VTL に設定されている自動テープ作成ポリシーを削除する許可を付与	書き込み	gateway*		
DeleteBandwidthRateLimit	ゲートウェイの帯域幅レート制限を削除する許可を付与	書き込み	gateway*		
DeleteCacheReport	キャッシュレポートに関連付けられたメタデータを削除するアクセス許可を付与します	書き込み	cache-report*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteChapCredentials	指定された iSCSI ターゲットとイニシエータペアのチャレンジハンドシェイク認証プロトコル (CHAP) 認証情報を削除する許可を付与	書き込み	target*		
DeleteFileShare	ファイルゲートウェイからファイル共有を削除する許可を付与	書き込み	share*		
DeleteGateway	ゲートウェイを削除する許可を付与	書き込み	gateway*		
DeleteSnapshotSchedule	ボリュームのスナップショットを削除する許可を付与	書き込み	volume*		
DeleteTape	指定された仮想テープを削除する許可を付与	書き込み	gateway*		
			tape*		
DeleteTapeArchive	指定した仮想テープを仮想テープシェルフ (VTS) から削除する許可を付与	書き込み			
DeleteTapePool	指定されたテーププールを削除する許可を付与	書き込み	tapepool*		
DeleteVolume	CreateCachediSCSIVolume または CreateStorediSCSIVolume API を使用して以前に作成した指定済みゲートウェイボリュームを削除する許可を付与	書き込み	volume*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeAvailabilityMonitorTest	ゲートウェイで実行された最新の高可用性モニタリングテストに関する情報を取得する許可を付与	読み込み	gateway*		
DescribeBandwidthRateLimit	ゲートウェイの帯域幅レート制限を取得する許可を付与	読み込み	gateway*		
DescribeBandwidthRateLimitSchedule	ゲートウェイの帯域幅レート制限スケジュールを取得する許可を付与	読み込み	gateway*		
DescribeCache	ゲートウェイのキャッシュに関する情報を取得する許可を付与。このオペレーションは、ゲートウェイキャッシュ型ボリュームアーキテクチャでのみサポートされています	読み取り	gateway*		
DescribeCacheReport	キャッシュレポートの説明を取得するアクセス許可を付与します	読み取り	cache-report*		
DescribeCachediSCSIVolumes	リクエストで指定されたゲートウェイボリュームの説明を取得する許可を付与。このオペレーションは、ゲートウェイキャッシュ型ボリュームアーキテクチャでのみサポートされています	読み込み	volume*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeChapCredentials	ターゲットとイニシエータのペアごとに 1 つずつ、指定した iSCSI ターゲットのチャレンジハンドシェイク認証プロトコル (CHAP) 認証情報の配列を取得する許可を付与	読み込み	target*		
DescribeFileSystemAssociations	1 つまたは複数のファイルシステムの関連付けの説明を取得するためのアクセス許可を付与します。	読み込み	fs-association*		
DescribeGatewayInformation	名前、ネットワークインターフェイス、設定したタイムゾーン、および状態 (ゲートウェイが実行中かどうか) など、ゲートウェイに関するメタデータを取得する許可を付与	読み込み	gateway*		
DescribeMaintenanceStartTime	曜日と時刻を含むゲートウェイの週次メンテナンス開始時刻を確定する許可を付与	読み込み	gateway*		
DescribeNFSFileShares	ファイルゲートウェイから 1 つまたは複数のファイル共有の説明を取得するためのアクセス許可を付与する	読み込み	share*		
DescribeSMBFileShares	ファイルゲートウェイから 1 つまたは複数のファイル共有の説明を取得するためのアクセス許可を付与する	読み込み	share*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeSMBSettings	ファイルゲートウェイからサーバーメッセージブロック (SMB) のファイル共有設定の説明を取得する許可を付与	読み込み	gateway*		
DescribeSnapshotSchedule	指定されたゲートウェイボリュームのスナップショットスケジュールを説明する許可を付与	読み込み	volume*		
DescribeStorediSCSIVolumes	リクエストで指定されたゲートウェイボリュームの説明を取得する許可を付与	読み込み	volume*		
DescribeTapeArchives	仮想テープシェルフ (VTS) 内の指定された仮想テープの説明を取得する許可を付与	読み込み			
DescribeTapeRecoveryPoints	指定したゲートウェイ VTL で使用可能な仮想テープリカバリポイントのリストを取得する許可を付与	読み込み	gateway*		
DescribeTapes	仮想テープの指定された Amazon リソースネーム (ARN) の説明を取得する許可を付与	読み込み	gateway*		
DescribeUploadBuffer	ゲートウェイのアップロードバッファに関する情報を取得する許可を付与	読み込み	gateway*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeVTLDevices	指定したゲートウェイの仮想テープライブラリ (VTL) デバイスの説明を取得する許可を付与	読み込み	gateway*		
DescribeWorkingStorage	ゲートウェイの作業ストレージに関する情報を取得する許可を付与	読み込み	gateway*		
DetachVolume	iSCSI 接続からボリュームを切断するアクセス許可を付与してから、指定されたゲートウェイからそのボリュームを切断する	書き込み	volume*		
DisableGateway	ゲートウェイが機能しなくなったときにゲートウェイを無効にする許可を付与	書き込み	gateway*		
DisassociateFileSystem	Amazon FSx ファイルゲートウェイから Amazon FSX ファイルシステムの関連付けを解除する許可を付与。	書き込み	fs-association*		
EvictFilesFailingUpload	Amazon S3 へのアップロードに失敗したファイルエントリの共有のキャッシュをクリーンアップするアクセス許可を付与します	書き込み	share*		
JoinDomain	Active Directory ドメインに参加できるようにする許可を付与	書き込み	gateway*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListAutomaticTapeCreationPolicies	指定された gateway-VTL または が所有するすべての gateway-VTLs に設定されている自動テープ作成ポリシーを一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListCacheReports	が所有するキャッシュレポートのリストを取得するアクセス許可を付与します AWS アカウント	リスト			
ListFileShares	特定のファイルゲートウェイのファイル共有のリスト、または が所有するファイル共有のリストを取得するアクセス許可を付与します AWS アカウント	リスト			
ListFileSystemAssociations	指定されたゲートウェイのファイルシステムの関連付け一覧を取得するためのアクセス許可を付与します。	リスト			
ListGateways	リクエストで指定されたリージョン AWS アカウント の が所有するゲートウェイを一覧表示するアクセス許可を付与します。返されるリストは、ゲートウェイ Amazon リソースネーム (ARN) によって順序付けられます	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListLocalDisks	ゲートウェイのローカルディスクのリストを取得する許可を付与	リスト	gateway*		
ListTagsForResource	指定されたリソースに追加されたタグを取得する許可を付与	リスト	gateway		
			share		
			tape		
			volume		
ListTapePools	が所有するテーププールを一覧表示するアクセス許可を付与します AWS アカウント	リスト			
ListTapes	仮想テープライブラリ (VTL) と仮想テープシェルフ (VTS) の仮想テープを一覧表示する許可を付与	リスト			
ListVolumeInitiators	ボリュームに接続されている iSCSI イニシエータを一覧表示する許可を付与	リスト	volume*		
ListVolumeRecoveryPoints	指定したゲートウェイのリカバリポイントを一覧表示する許可を付与	リスト	gateway*		
ListVolumes	ゲートウェイの iSCSI 保存ボリュームを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
NotifyWhenUploaded	NFS ファイル共有に書き込まれたすべてのファイルが Amazon S3 にアップロードされたときに CloudWatch Events を通じて通知を送信する許可を付与	書き込み	share*		
RefreshCache	指定したファイル共有のキャッシュを更新する許可を付与	書き込み	share*		
RemoveTagsFromResource	指定されたリソースから 1 つ以上のタグを削除する権限を付与します	タグ付け	cache-report		
			fs-association		
			gateway		
			share		
			tape		
			tapepool		
			volume		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ResetCache	エラーが発生したすべてのキャッシュディスクをリセットするアクセス許可を付与し、ディスクをキャッシュストレージとして再設定できるようにする	書き込み	gateway*		
RetrieveTapeArchive	アーカイブされた仮想テープを仮想テープシェルフ (VTS) からゲートウェイ VTL に取得する許可を付与	書き込み	gateway* tape*		
RetrieveTapeRecoveryPoint	指定した仮想テープのリカバリポイントを取得する許可を付与	書き込み	gateway* tape*		
SetLocalConsolePassword	VM ローカルコンソールのパスワードを設定する許可を付与	書き込み	gateway*		
SetSMBGuestPassword	SMB ゲストユーザーのパスワードを設定する許可を付与	書き込み	gateway*		
ShutdownGateway	ゲートウェイをシャットダウンする許可を付与	書き込み	gateway*		
StartAvailabilityMonitorTest	指定されたゲートウェイがホスト環境で高可用性モニタリング用に構成されていることを確認するテストを開始する許可を付与	書き込み	gateway*		
StartCacheReport	既存のファイル共有のキャッシュレポートを開始する許可を付与	書き込み	share*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
StartGateway	以前にシャットダウンしたゲートウェイを起動する許可を付与	書き込み	gateway*		
UpdateAutomaticTapeCreationPolicy	ゲートウェイ VTL に設定されている自動テープ作成ポリシーを更新する許可を付与	書き込み	gateway* tapepool*		
UpdateBandwidthRateLimit	ゲートウェイの帯域幅レート制限を更新する許可を付与	書き込み	gateway*		
UpdateBandwidthRateLimitSchedule	ゲートウェイの帯域幅レート制限スケジュールを更新する許可を付与	書き込み	gateway*		
UpdateChapCredentials	指定された iSCSI ターゲットのチャレンジハンドシェイク認証プロトコル (CHAP) 認証情報を更新する許可を付与	書き込み	target*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateFileSystemAssociation	ファイルシステムの関連付けを更新する許可を付与。	書き込み	fs-association*		logs:CreateLogDelivery logs:DeleteLogDelivery logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery
UpdateGatewayInformation	ゲートウェイの名前とタイムゾーンを含む、ゲートウェイのメタデータを更新する許可を付与	書き込み	gateway*		
UpdateGatewaySoftwareNow	ゲートウェイ仮想マシン (VM) ソフトウェアを更新する許可を付与	書き込み	gateway*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateMaintenanceStartTime	曜日と時刻を含むゲートウェイの週次メンテナンス開始時刻情報を更新する許可を付与。メンテナンス時間は、ゲートウェイのタイムゾーンの時間です	書き込み	gateway*		
UpdateNFSFileShare	NFS ファイル共有を更新する許可を付与	書き込み	share*		
UpdateSMBFileShare	SMB ファイル共有を更新する許可を付与	書き込み	share*		
UpdateSMBFileShareVisibility	ゲートウェイ上の共有がネットビューまたは参照リストに表示されるかどうかを更新する許可を付与	書き込み	gateway*		
UpdateSMBLocalGroups	ゲートウェイ上の SMB ファイル共有に対する特別な許可を持つアクティブディレクトリのユーザーとグループのリストを更新する許可を付与します	書き込み	gateway*		
UpdateSMBSecurityStrategy	ファイルゲートウェイで SMB セキュリティ戦略を更新する許可を付与	書き込み	gateway*		
UpdateSnapshotSchedule	ゲートウェイボリューム用に構成されたスナップショットスケジュールを更新する許可を付与	書き込み	volume*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateVTLDeviceType	ゲートウェイ VTL でメディアチェンジャーのタイプを更新する許可を付与	書き込み	device*		

AWS Storage Gateway で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
cache-report	arn:${Partition}:storagegateway:${Region}:${Account}:share/${ShareId}/cache-report/${CacheReportId}	aws:ResourceTag/${TagKey}
device	arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/device/${Vtldevice}	
fs-association	arn:${Partition}:storagegateway:${Region}:${Account}:fs-association/${FsaId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
gateway	arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}	aws:ResourceTag/${TagKey}
share	arn:${Partition}:storagegateway:${Region}:${Account}:share/${ShareId}	aws:ResourceTag/${TagKey}
tape	arn:${Partition}:storagegateway:${Region}:${Account}:tape/${TapeBarcode}	aws:ResourceTag/${TagKey}
tapepool	arn:${Partition}:storagegateway:${Region}:${Account}:tapepool/${PoolId}	aws:ResourceTag/${TagKey}
target	arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/target/${IscsiTarget}	
volume	arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/volume/${VolumeId}	aws:ResourceTag/${TagKey}

AWS Storage Gateway の条件キー

AWS Storage Gateway では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	各タグの許可された値のセットでアクセスをフィルタリングします	String

条件キー	説明	タイプ
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値でアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内の必須タグの存在でアクセスをフィルタリングします	ArrayOfString

AWS Supply Chain のアクション、リソース、および条件キー

AWS Supply Chain (サービスプレフィックス: scn) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Supply Chain によって定義されたアクション
- AWS Supply Chain によって定義されたリソースタイプ
- AWS Supply Chain の条件キー

AWS Supply Chain によって定義されたアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssignAdminPermissionsToUser	フェデレーティッドユーザーに AWS Supply Chain 管理者	書き込み	instance*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	アクセス許可を追加するアクセス許可を付与します				
CreateBillOfMaterialsImportJob	BillOfMaterials レコードの CSV ファイルをインポートする BillOfMaterialsImportJob を作成する許可を付与する	書き込み	instance*		
CreateDataIntegrationFlow	複数のソースから 1 つのターゲットに変換できる DataIntegrationFlow を作成する許可を付与する	書き込み	instance*		
CreateDataLakeDataset	データレイクデータセットを作成する許可を付与する	書き込み	instance*		
CreateDataLakeNamespace	データレイク名前空間を作成するアクセス許可を付与します	書き込み	instance*		
CreateInstance	新しい AWS Supply Chain インスタンスを作成するアクセス許可を付与します	書き込み	instance*		
CreateSSOApplication	AWS Supply Chain インスタンスの IAM Identity Center アプリケーションを作成するアクセス許可を付与します	書き込み	instance*		
DeleteDataIntegrationFlow	DataIntegrationFlow を削除する許可を付与する	書き込み	data-integration-flow*		
DeleteDataLakeDataset	データレイクデータセットを削除する許可を付与する	書き込み	dataset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteDataLakeNamespace	データレイク名前空間を削除する許可を付与	書き込み	namespace*		
DeleteInstance	AWS Supply Chain インスタンスを削除するアクセス許可を付与します	書き込み	instance*		
DeleteSSOApplication	AWS Supply Chain インスタンスの IAM Identity Center アプリケーションを削除するアクセス許可を付与します	書き込み	instance*		
DescribeInstance	AWS Supply Chain インスタンスの詳細を表示するアクセス許可を付与します	読み取り	instance*		
GetBillOfMaterialsImportJob	BillOfMaterialsImportJob のステータスと詳細を表示する許可を付与する	読み取り	bill-of-materials-import-job*		
GetDataIntegrationEvent	DataIntegrationEvent を取得する許可を付与	読み取り	instance*		
GetDataIntegrationFlow	DataIntegrationFlow の詳細を取得する許可を付与する	読み取り	data-integration-flow*		
GetDataIntegrationFlowExecution	指定された 1 つの DataIntegrationFlow の特定の実行を取得する許可を付与	読み取り	data-integration-flow*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetDataLakeDataset	データセットの詳細を取得する許可を付与する	読み取り	dataset*		
GetDataLakeNamespace	名前空間の詳細を取得するアクセス許可を付与します	読み取り	namespace*		
GetInstance	AWS Supply Chain インスタンスの詳細を表示するアクセス許可を付与します	読み取り	instance*		
ListAdminUsers	インスタンスの AWS Supply Chain 管理者を一覧表示するアクセス許可を付与します	リスト	instance*		
ListDataIntegrationEvents	インスタンス内のすべての DataIntegrationEvents を一覧表示する許可を付与	リスト	instance*		
ListDataIntegrationFlowExecutions	指定された 1 つの DataIntegrationFlow のすべての実行を一覧表示するアクセス許可を付与します	リスト	data-integration-flow*		
ListDataIntegrationFlows	ページ分割された方法ですべての DataIntegrationFlows を一覧表示する許可を付与する	リスト	instance*		
ListDataLakeDatasets	特定のインスタンスと名前空間にデータレイクデータセットを一覧表示する許可を付与する	リスト	instance*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListDataLakeNamespaces	特定のインスタンスでデータレイク名前空間を一覧表示するアクセス許可を付与します	リスト	instance*		
ListInstances	に関連付けられた AWS Supply Chain インスタンスを表示するアクセス許可を付与します AWS アカウント	リスト	instance*		
ListTagsForResource	AWS Supply Chain リソースのタグを一覧表示する許可を付与	リスト	instance*		
RemoveAdminPermissionsForUser	フェデレーティッドユーザーから AWS Supply Chain 管理者許可を削除する許可を付与	書き込み	instance*		
SendDataIntegrationEvent	データをリアルタイムで取り込む DataIntegrationEvent を作成する許可を付与する	書き込み	instance*		
TagResource	AWS Supply Chain リソースにタグを付けるアクセス許可を付与します	Tagging	instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	AWS Supply Chain リソースからタグを削除する許可を付与	Tagging	instance*		
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateDataIntegrationFlow	DataIntegrationFlow を更新する許可を付与する	書き込み	data-integration-flow*		
UpdateDataLakeDataset	データレイクデータセットを更新する許可を付与する	書き込み	dataset*		
UpdateDataLakeNamespace	データレイク名前空間を更新する許可を付与	書き込み	namespace*		
UpdateInstance	AWS Supply Chain インスタンスを更新する許可を付与	書き込み	instance*		

AWS Supply Chain によって定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
instance	arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}	
bill-of-materials-import-job	arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}/bill-of-materials-import-job/${JobId}	

リソースタイプ	ARN	条件キー
data-integration-flow	arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}/data-integration-flows/${FlowName}	
namespace	arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}/namespaces/${Namespace}	
dataset	arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}/namespaces/${Namespace}/datasets/${DatasetName}	

AWS Supply Chain の条件キー

AWS Supply Chain は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアによってアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアによってアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルター	ArrayOfString

AWS サポートのアクション、リソース、および条件キー

AWS サポート (サービスプレフィックス: support) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS サポートで定義されるアクション
- AWS サポートで定義されるリソースタイプ
- AWS サポートの条件キー

AWS サポートで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

> **Note**
>
> サポート では、ケースへのアクセス、変更、解決、Trusted Advisor アクションの使用が可能です。サポート API を使用して Trusted Advisor 関連のアクションを呼び出す場合、「trustedadvisor:*」アクションのいずれもアクセスを制限しません。「trustedadvisor:*」アクションは、 AWS Management Consoleの Trusted Advisor にのみ適用されます。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddAttachmentsToSet	1 つ以上の添付ファイルを AWS サポート ケースに追加するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AddCommunicationToCase	AWS サポート ケースに顧客通信を追加するアクセス許可を付与します	書き込み			
CreateCase	新しい AWS サポート ケースを作成するアクセス許可を付与します	書き込み			
DescribeAttachment	アタッチメントの詳細を記述するアクセス許可を付与します	読み取り			
DescribeCaseAttributes	セカンダリサービスに AWS サポート ケース属性の読み取りを許可するアクセス許可を付与します。これは内部で管理される関数です。	読み取り			
DescribeCaseOptions	1 つの AWS サポート ケースで使用可能なオプションを記述するアクセス許可を付与します。これは内部管理機能です	読み取り			
DescribeCases	指定された入力に一致する AWS サポート ケースを一覧表示するアクセス許可を付与します	読み取り			
DescribeCommunication	1 つの AWS サポート ケースに対して 1 つの通信と添付ファイルを取得するアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeCommunications	1 つ以上の AWS サポートケースの通信と添付ファイルを一覧表示するアクセス許可を付与します	読み取り			
DescribeCreateCaseOptions	サポートケースを作成する際に利用可能なオプションを説明する許可を付与します	読み取り			
DescribeIssueTypes	AWS サポート ケースの問題タイプを返すアクセス許可を付与します	読み取り			
DescribeServices	各 AWS サービスに適用されるサービスとカテゴリを一覧表示するアクセス許可を付与します	読み取り			
DescribeSeverityLevels	AWS サポート ケースに割り当てることができる重要度レベルを一覧表示するアクセス許可を付与します	読み取り			
DescribeSupportLevel	AWS アカウント識別子のサポートレベルを返すアクセス許可を付与します	読み取り			
DescribeSupportedLanguages	指定されたカテゴリコード、サービスコード、および問題タイプで利用可能なサポート言語を説明する許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeTrustedAdvisorCheckRefreshStatuses	チェック識別子のリストに基づいて Trusted Advisor の更新チェックのステータスを取得するアクセス許可を付与します。	読み取り			
DescribeTrustedAdvisorCheckResult	指定されたチェック識別子を持つ Trusted Advisor チェックの結果を取得するアクセス許可を付与します。	読み取り			
DescribeTrustedAdvisorCheckSummaries	指定されたチェック識別子を持つ Trusted Advisor チェックの結果のサマリーを取得するアクセス許可を付与します。	読み取り			
DescribeTrustedAdvisorChecks	名前、識別子、カテゴリ、説明など、使用可能なすべての Trusted Advisor チェックのリストを取得するアクセス許可を付与します	読み取り			
GetInteraction	アカウントおよび特定のインタラクションの技術的な問題に対して、パーソナライズされたトラブルシューティング支援を取得するアクセス許可を付与します	読み取り			
InitiateCallForCase	AWS サポート Center で通話を開始するアクセス許可を付与します。これは内部管理機能です	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
InitiateChatForCase	AWS サポート Center でチャットを開始するアクセス許可を付与します。これは内部で管理される関数です。	書き込み			
PutCaseAttributes	セカンダリサービスが AWS サポート ケースに属性をアタッチすることを許可するアクセス許可を付与します。これは内部管理機能です	書き込み			
RateCaseCommunication	AWS サポート ケース通信を評価するアクセス許可を付与します	書き込み			
RefreshTrustedAdvisorCheck	指定されたチェック識別子を持つ Trusted Advisor チェックの更新をリクエストするアクセス許可を付与します	書き込み			
ResolveCase	AWS サポート ケースを解決するアクセス許可を付与します	書き込み			
SearchForCases	指定された入力に一致する AWS サポート ケースのリストを返すアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartInteraction	アカウントと技術的な問題に対してパーソナライズされたトラブルシューティング支援を受けるための特定のインタラクションを開始するアクセス許可を付与します	書き込み			
UpdateCaseSeverity	1 つの AWS サポート ケースの重要度を更新するアクセス許可を付与します。これは内部管理機能です	書き込み			
UpdateInteraction	特定のインタラクションを更新して、アカウントと技術的な問題に関するパーソナライズされたトラブルシューティング支援を受けるアクセス許可を付与します	書き込み			

AWS サポートで定義されるリソースタイプ

AWS サポート では、IAM ポリシーステートメントの Resource要素でのリソース ARN の指定はサポートされていません。 AWS サポートへのアクセスを許可するには、ポリシーで "Resource": "*" を指定します。

AWS サポートの条件キー

サポートには、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS サポート App in Slack のアクション、リソース、条件キー

AWS サポート App in Slack (サービスプレフィックス: supportapp) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS サポート App in Slack で定義されたアクション
- AWS サポート App in Slack で定義されたリソースタイプ
- AWS サポート App in Slack の条件キー

AWS サポート App in Slack で定義されたアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSlackChannelConfiguration	アカウントに Slack チャネル設定を作成する権限を付与する	書き込み			
DeleteAccountAlias	アカウントからエイリアスを削除する権限を付与する	書き込み			
DeleteSlackChannelConfiguration	アカウントから Slack チャネル設定を削除する権限を付与する	書き込み			
DeleteSlackWorkspa	アカウントから Slack ワークスペース設定を削除する権限を付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ceConfiguration					
DescribeSlackChannels [アクセス許可のみ]	AWS サポート アプリを招待したワークスペース内のすべてのパブリック Slack チャネルを一覧表示するアクセス許可を付与します	読み取り			
GetAccountAlias	アカウントにエイリアスを取得する権限を付与する	読み取り			
GetSlackOauthParameters [許可のみ]	AWS サポート アプリケーションがワークスペースの認可に使用する Slack OAuth コードのパラメーターを取得する許可を付与する	読み取り			
ListSlackChannelConfigurations	アカウントのすべての Slack チャネル設定を一覧表示する権限を付与する	読み取り			
ListSlackWorkspaceConfigurations	アカウントのすべての Slack ワークスペース設定を一覧表示する権限を付与する	読み取り			
PutAccountAlias	アカウントのエイリアスを作成するまたは更新する権限を付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RedeemSlackOauthCode [アクセス許可のみ]	AWS サポート アプリケーションがワークスペースの認可に使用する Slack OAuth コードを引き換える許可を付与する	書き込み			
RegisterSlackWorkspaceForOrganization	組織の一部 AWS アカウントである の Slack ワークスペースを登録する許可を付与	書き込み			
UpdateSlackChannelConfiguration	アカウントの Slack チャネル設定を更新する権限を付与する	書き込み			

AWS サポート App in Slack で定義されたリソースタイプ

AWS サポート Slack のアプリは、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS サポート App in Slack へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS サポート App in Slack の条件キー

サポートアプリには、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS サポート コンソールのアクション、リソース、および条件キー

AWS サポート コンソール (サービスプレフィックス: `support-console`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS サポート コンソールで定義されるアクション
- AWS サポート コンソールで定義されるリソースタイプ
- AWS サポート コンソールの条件キー

AWS サポート コンソールで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CheckSubscription [アクセス許可のみ]	アカウントが特定の製品にアクセスできるかどうかを確認するアクセス許可を付与します	読み取り			
CreateCaseDraft [許可のみ]	指定されたケースタイプのケースドラフトを作成または更新するアクセス許可を付与します	書き込み			
CreateContact [アクセス許可のみ]	指定された問い合わせタイプの認証済み問い合わせを作成するアクセス許可を付与します	書き込み			
DeleteCaseDraft [アクセス許可のみ]	指定されたケースタイプのケースドラフトを削除するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeDynamicHelp [アクセス許可のみ]	特定のサービスとカテゴリの動的ヘルプリソースを取得する許可を付与	読み取り			
GetAccountGovCloudEnabled [許可のみ]	呼び出し元のアカウントがGovCloud が有効になっているかどうかを判断するアクセス許可を付与します	読み取り			
GetAccountState [許可のみ]	呼び出し元のアカウントの状態を取得するアクセス許可を付与します	読み取り			
GetBanner [許可のみ]	サポートバナー情報を取得する許可を付与	読み取り			
GetCaseDraft [許可のみ]	特定のケースタイプのケースドラフトを取得するアクセス許可を付与します	読み取り			
GetQuestionnaire [許可のみ]	フィードバックアンケートを取得する許可を付与	読み取り			
SaveFeedback [許可のみ]	アンケートのフィードバックを保存するアクセス許可を付与します	書き込み			

AWS サポート コンソールで定義されるリソースタイプ

AWS サポート コンソールは、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS サポート コンソールへのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS サポート コンソールの条件キー

サポートコンソールには、ポリシーステートメントの Condition要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS サポート Plans のアクション、リソース、および条件キー

AWS サポート プラン (サービスプレフィックス: supportplans) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS サポート Plans によって定義されたアクション
- AWS サポート Plans で定義されるリソースタイプ
- AWS サポート Plans の条件キー

AWS サポート Plans によって定義されたアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSupportPlanSchedule [アクセス許可のみ]	このサポートプランスケジュールを作成するアクセス許可を付与します AWS アカウント	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetSupportPlan [アクセス許可のみ]	このの現在のサポートプランに関する詳細を表示するアクセス許可を付与します AWS アカウント	読み取り			
GetSupportPlanUpdateStatus [許可のみ]	サポートプランの更新リクエストのステータスに関する詳細を表示するための許可を付与します	読み取り			
ListSupportPlanModifiers [許可のみ]	こののすべてのサポートプラン修飾子のリストを表示するアクセス許可を付与します AWS アカウント	リスト			
StartSupportPlanUpdate [許可のみ]	こののサポートプランを更新するアクセス許可を付与します AWS アカウント	書き込み			

AWS サポート Plans で定義されるリソースタイプ

AWS サポート プランは、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS サポート Plans へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS サポート Plans の条件キー

Support Plans には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS サステナビリティのアクション、リソース、条件キー

AWS 持続可能性 (サービスプレフィックス: sustainability) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS サステナビリティで定義されるアクション
- AWS サステナビリティで定義されるリソースタイプ
- AWS サステナビリティの条件キー

AWS サステナビリティで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetCarbonFootprintSummary	カーボンフットプリントツールを表示するアクセス許可を付与	読み取り			

AWS サステナビリティで定義されるリソースタイプ

AWS 持続可能性は、IAM ポリシーステートメントの Resource要素でのリソース ARN の指定をサポートしていません。 AWS サステナビリティへのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS サステナビリティの条件キー

サステナビリティには、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Systems Manager のアクション、リソース、および条件キー

AWS Systems Manager (サービスプレフィックス: ssm) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Systems Manager で定義されるアクション
- AWS Systems Manager で定義されるリソースタイプ
- AWS Systems Manager の条件キー

AWS Systems Manager で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AddTagsToResource	指定された AWS リソースの 1 つ以上のタグを追加または上書きするアクセス許可を付与します	Tagging	association		
			automation-execution		
			document		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			instance		
			maintenancewindow		
			managed-instance		
			opsitem		
			opsmetadata		
			parameter		
			patchbaseline		
			task		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
AssociateOpsItemRelatedItem	OpsItem に RelatedItem を関連付けるためのアクセス許可を付与	書き込み	opsitem*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelCommand	指定した Run Command コマンドをキャンセルする許可を付与	書き込み			
CancelMaintenanceWindowExecution	進行中のメンテナンスウィンドウの実行をキャンセルする許可を付与	書き込み	maintenancewindow*		
CreateActivation	オンプレミスサーバーと仮想マシン (VM) を Systems Manager に登録するために使用するアクティベーションを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssociation	指定した Systems Manager ドキュメントを、指定したインスタンスまたは他のターゲットに関連付けるアクセス許可を付与	書き込み	association*		
			document*		
			instance		
			managed-instance		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssociationBatch	1 つのコマンドで複数の CreateAssociation オペレーションのエントリを結合する許可を付与	書き込み	document*		
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateDocument	Systems Manager SSM ドキュメントを作成する許可を付与	書き込み	document*		iam:PassRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys ssm:DocumentType	
CreateMaintenanceWindow	メンテナンスウィンドウを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOpsItem	OpsCenter で OpsItem を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOpsMetadata	AWS リソースの OpsMetadata オブジェクトを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreatePatchBaseline	パッチベースラインを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateResourceDataSync	リソースデータ同期設定を作成する許可を付与。この設定は、マネージドインスタンスからインベントリデータを定期的に収集し、Amazon S3 バケット内のデータを更新	書き込み	resourcedatasync*		
				ssm:SyncType	
DeleteActivation	マネージドインスタンスの指定されたアクティベーションを削除する許可を付与	書き込み			
DeleteAssociation	指定した SSM ドキュメントを指定したインスタンスから関連付け解除する許可を付与	書き込み	association		
			document		
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	
DeleteDocument	指定した SSM ドキュメントとそのインスタンスの関連付けを削除する許可を付与	書き込み	document*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ssm:DocumentType	
DeleteInventory	カスタムインベントリタイプまたは当該タイプに関連付けられているデータを削除する許可を付与	書き込み			
DeleteMaintenanceWindow	指定したメンテナンスウィンドウを削除する許可を付与	書き込み	maintenancewindow*		
DeleteOpsItem	OpsItem を削除する許可を付与	書き込み	opsitem*		
DeleteOpsMetadata	OpsMetadata オブジェクトを削除する許可を付与	書き込み	opsmetadata*		
DeleteParameter	指定した SSM パラメータを削除する許可を付与	書き込み	parameter*		
				aws:ResourceTag/${TagKey}	
DeleteParameters	複数の指定する SSM パラメータを削除する許可を付与	書き込み	parameter*		
				aws:ResourceTag/${TagKey}	
DeletePatchBaseline	指定したパッチベースラインを削除する許可を付与	書き込み	patchbaseline*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteResourceDataSync	指定したリソースデータ同期を削除する許可を付与	書き込み	resourcedatasync*		
				ssm:SyncType	
DeleteResourcePolicy	Systems Manager のポリシーを削除する許可を付与	権限の管理	document		
			opsitemgroup		
			parameter		
DeregisterManagedInstance	Systems Manager から指定したオンプレミスサーバーまたは仮想マシン (VM) の登録を解除する許可を付与	書き込み	managed-instance*		
				ssm:resourceTag/tag-key	
DeregisterPatchBaselineForPatchGroup	指定したパッチベースラインを、指定したパッチグループのデフォルトパッチベースラインから登録解除する許可を付与	書き込み	patchbaseline*		
DeregisterTargetFromMaintenanceWindow	指定したターゲットをメンテナンスウィンドウから登録解除する許可を付与	書き込み	maintenancewindow*		
			windowtarget*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeregisterTaskFromMaintenanceWindow	指定されたタスクをメンテナンスウィンドウから登録解除する許可を付与	書き込み	maintenancewindow*		
			windowtask*		
DescribeActivations	指定されたマネージドインスタンスのアクティベーションに関する詳細を表示する許可を付与 (作成日時、アクティベーションを使用して登録されたインスタンスの数など)	読み取り			
DescribeAssociation	指定したインスタンスまたはターゲットの指定した関連付けの詳細を表示する許可を付与	読み取り	association		
			document		
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	
DescribeAssociationExecutionTargets	指定した関連付け実行に関する情報を表示する許可を付与	読み取り	association*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeAssociationExecutions	指定した関連付けのすべての実行を表示する許可を付与	読み取り	association*		
				aws:ResourceTag/${TagKey}	
DescribeAutomationExecutions	すべてのアクティブなオートメーション実行と終了したオートメーション実行の詳細を表示する許可を付与	読み取り			
DescribeAutomationStepExecutions	オートメーションワークフローでアクティブなステップ実行と終了したステップ実行のすべてを表示する許可を付与	読み取り	automation-execution*		
DescribeAvailablePatches	パッチベースラインに含める資格のあるすべてのパッチを表示する許可を付与	読み取り			
DescribeDocument	指定した SSM ドキュメントの詳細を表示する許可を付与	読み取り	document*		
				ssm:DocumentType	
DescribeDocumentParameters	Systems Manager コンソールで SSM ドキュメントパラメータに関する情報を表示する許可を付与 (内部 Systems Manager のアクション)	読み取り	document*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeDocumentPermission	指定した SSM ドキュメントのアクセス許可を表示する許可を付与	読み取り	document*		
				ssm:DocumentType	
DescribeEffectiveInstanceAssociations	指定したインスタンスの現在の関連付けをすべて表示する許可を付与	読み取り	instance*		
			managed-instance*		
				aws:ResourceTag/${TagKey}	
DescribeEffectivePatchesForPatchBaseline	指定したパッチベースラインに現在関連付けられているパッチの詳細を表示する許可を付与 (Windows のみ)	読み取り	patchbaseline*		
DescribeInstanceAssociationsStatus	指定したインスタンスの関連付けのステータスを表示する許可を付与	読み取り	instance*		
			managed-instance*		
				aws:ResourceTag/${TagKey}	
DescribeInstanceInformation	指定したインスタンスに関する詳細を表示する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeInstancePatchStates	指定したインスタンスのパッチに関するステータスの詳細を表示する許可を付与	読み取り	instance*		
			managed-instance*		
				aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}	
DescribeInstancePatchStatesForPatchGroup	指定したパッチグループ内のインスタンスのパッチ状態の概要を記述する許可を付与	読み取り			
DescribeInstancePatches	指定したインスタンスのパッチに関する全般的な詳細を表示する許可を付与	読み取り	instance*		
			managed-instance*		
				aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeInstanceProperties	マネージドインスタンスのノードをレンダリングするアクセス許可をユーザーのAmazon EC2 コンソールに付与	読み取り			
DescribeInventoryDeletions	指定したインベントリ削除の詳細を表示する許可を付与	読み取り			
DescribeMaintenanceWindowExecutionTaskInvocations	メンテナンスウィンドウに対して指定したタスク実行の詳細を表示する許可を付与	リスト			
DescribeMaintenanceWindowExecutionTasks	指定したメンテナンスウィンドウの実行中に実行されたタスクの詳細を表示する許可を付与	リスト			
DescribeMaintenanceWindowExecutions	指定したメンテナンスウィンドウの実行を表示する許可を付与	リスト	maintenancewindow*		
DescribeMaintenanceWindowSchedule	指定したメンテナンスウィンドウの今後の実行に関する詳細を表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeMaintenanceWindowTargets	指定したメンテナンスウィンドウに関連付けられているターゲットのリストを表示する許可を付与	リスト	maintenancewindow*		
DescribeMaintenanceWindowTasks	指定したメンテナンスウィンドウに関連付けられたタスクのリストを表示する許可を付与	リスト	maintenancewindow*		
DescribeMaintenanceWindows	すべてまたは指定したメンテナンスウィンドウに関する情報を表示する許可を付与	リスト			
DescribeMaintenanceWindowsForTarget	指定したインスタンスに関連付けられたメンテナンスウィンドウのターゲットおよびタスクに関する情報を表示する許可を付与	リスト			
DescribeOpsItems	指定した OpsItems の詳細を表示する許可を付与	読み取り			
DescribeParameters	指定した SSM パラメータの詳細を表示する許可を付与	リスト			
DescribePatchBaselines	指定した条件を満たすパッチベースラインに関する情報を表示する許可を付与	リスト			
DescribePatchGroupState	指定したパッチグループのパッチの集約ステータス詳細を表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribePatchGroups	指定したパッチグループのパッチベースラインに関する情報を表示する許可を付与	リスト			
DescribePatchProperties	指定したオペレーティングシステムおよびパッチプロパティで使用可能なパッチの詳細を表示する許可を付与	リスト			
DescribeSessions	指定した検索条件を満たす最近の Session Manager セッションのリストを表示する許可を付与	リスト			
DisassociateOpsItemRelatedItem	OpsItem から RelatedItem の関連付けを解除するためのアクセス許可を付与	書き込み	opsitem*		
ExecuteAPI	Systems Manager の委任された管理者に、 の複数の AWS アカウントにわたる OpsItems に関する関連リソースの詳細を表示するアクセス許可を付与します AWS Management Console	読み取り			
GetAccessToken	just-in-timeノードアクセスで使用する認証情報セットを返す許可を付与	読み取り	opsitem*		
GetAutomationExecution	指定したオートメーション実行の詳細を表示する許可を付与	読み取り	automation-execution*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
GetCalendar [許可のみ]	特定のカレンダーの詳細を表示する許可を付与	読み取り	document*		
GetCalendarState	変更カレンダーまたは変更カレンダーの一覧のカレンダーの状態を表示する許可を付与	読み取り	document*		
GetCommandInvocation	指定した呼び出しまたはプラグインのコマンド実行に関する詳細を表示する許可を付与	読み取り			
GetConnectionStatus	指定したマネージドインスタンスの Session Manager 接続ステータスを表示する許可を付与	読み取り	instance		
			managed-instance		
			task		
				ssm:resourceTag/${TagKey} aws:ResourceTag/${TagKey}	
GetDefaultPatchBaseline	指定したオペレーティングシステムタイプの現在の既定のパッチベースラインを表示する許可を付与	読み取り	patchbaseline*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetDeployablePatchSnapshotForInstance	指定したインスタンスの現在のパッチベースラインスナップショットを取得する許可を付与	読み取り			
GetDocument	指定された SSM ドキュメントの内容を表示する許可を付与	読み取り	document*		
				ssm:DocumentCategories ssm:DocumentType	
GetExecutionPreview	指定された Automation ランブックを実行するとターゲットリソースに与える影響を示す既存のプレビューを取得するアクセス許可を付与します	読み取り			
GetInventory	指定した基準に従ってインスタンスインベントリの詳細を表示する許可を付与	読み取り			
GetInventorySchema	指定したインベントリ項目タイプのインベントリタイプまたは属性名のリストを表示する許可を付与	読み取り			
GetMaintenanceWindow	指定したメンテナンスウィンドウの詳細を表示する許可を付与	読み取り	maintenancewindow*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetMaintenanceWindowExecution	指定したメンテナンスウィンドウの実行に関する詳細を表示する許可を付与	読み取り			
GetMaintenanceWindowExecutionTask	指定したメンテナンスウィンドウの実行タスクの詳細を表示する許可を付与	読み取り			
GetMaintenanceWindowExecutionTaskInvocation	特定のターゲットで実行されている特定のメンテナンスウィンドウのタスクの詳細を表示する許可を付与	読み取り			
GetMaintenanceWindowTask	指定したメンテナンスウィンドウに登録されたタスクの詳細を表示する許可を付与	読み取り	maintenancewindow*		
GetManifest [許可のみ]	Systems Manager および SSM Agent に、インスタンスのパッケージのインストール要件を決定する許可を付与（内部 Systems Manager の呼び出し）	読み取り			
GetOpsItem	指定した OpsItem に関する情報を表示する許可を付与	読み取り	opsitem*		
GetOpsMetadata	OpsMetadata オブジェクトを取得する許可を付与	読み取り	opsmetadata*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetOpsSummary	指定したフィルターとアグリゲータに基づいて OpsItems に関する概要情報を表示する許可を付与	読み取り	resourcedatasync*		
GetParameter	指定したパラメータに関する情報を表示する許可を付与	読み取り	parameter*		
				aws:ResourceTag/${TagKey}	
GetParameterHistory	指定したパラメータの詳細と変更を表示する許可を付与	読み取り	parameter*		
				aws:ResourceTag/${TagKey}	
GetParameters	指定した複数のパラメータに関する情報を表示する許可を付与	読み取り	parameter*		
				aws:ResourceTag/${TagKey}	
GetParametersByPath	指定した階層内のパラメータに関する情報を表示する許可を付与	読み取り	parameter*		
				ssm:Recursive	
GetPatchBaseline	指定したパッチベースラインに関する情報を表示する許可を付与	読み取り	patchbaseline*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetPatchBaselineForPatchGroup	指定したパッチグループの現在のパッチベースラインの ID を表示する許可を付与	読み取り			
GetResourcePolicies	Systems Manager のリソースポリシーを一覧表示する許可を付与	リスト	document		
			opsitemgroup		
			parameter		
GetServiceSetting	AWS サービスのアカウントレベルの設定を表示するアクセス許可を付与します	読み取り	servicesetting*		
LabelParameterVersion	指定したバージョンのパラメータに識別ラベルを適用する許可を付与	書き込み	parameter*		
				aws:ResourceTag/${TagKey}	
ListAssociationVersions	指定した関連付けのバージョンを一覧表示する許可を付与	リスト	association*		
				aws:ResourceTag/${TagKey}	
ListAssociations	指定した SSM ドキュメントまたはマネージドインスタンスの関連付けを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListCommandInvocations	指定したインスタンスに送信されたコマンド呼び出しに関する情報を一覧表示する許可を付与	リスト			
ListCommands	指定したインスタンスに送信されたコマンドを一覧表示する許可を付与	リスト			
ListComplianceItems	指定したリソース上の指定したリソースタイプに対するコンプライアンスステータスを一覧表示する許可を付与	リスト			
ListComplianceSummaries	指定したコンプライアンスタイプについて、準拠リソースと非準拠リソースの集計カウントを一覧表示する許可を付与	リスト			
ListDocumentMetadataHistory	指定した SSM ドキュメントについてのメタデータ履歴を表示する許可を付与	リスト	document*		
				ssm:DocumentType	
ListDocumentVersions	指定したドキュメントのすべてのバージョンを一覧表示する許可を付与	リスト	document*		
				ssm:DocumentType	
ListDocuments	指定した SSM ドキュメントに関する情報を表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListInstanceAssociations	SSM Agent に、新しいステートマネージャーの関連付けをチェックするアクセス許可を付与 (内部 Systems Manager の呼び出し)	リスト	instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	
ListInventoryEntries	指定したインスタンスの指定したインベントリタイプのリストを表示する許可を付与	リスト			
ListNodes	指定されたフィルターに基づいてマネージドノードの詳細を表示するアクセス許可を付与します	リスト	resourcedatasync*		
ListNodesSummary	指定されたフィルターとアグリゲータに基づいてマネージドノードに関する概要情報を表示するアクセス許可を付与します	リスト	resourcedatasync*		
ListOpsItemEvents	OpsItemEvents を表示する許可を付与	リスト			
ListOpsItemRelatedItems	OpsItem RelatedItems の詳細を表示するためのアクセス許可を付与	リスト			
ListOpsMetadata	OpsMetadata オブジェクトのリストを表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListResourceComplianceSummaries	リソースレベルの集計カウントを一覧表示する許可を付与	リスト			
ListResourceDataSync	アカウントのリソースデータ同期設定に関する情報を一覧表示する許可を付与	リスト		ssm:SyncType	
ListTagsForResource	指定したリソースのリソースタグのリストを表示する許可を付与	リスト	association		
			automation-execution		
			document		
			maintenancewindow		
			managed-instance		
			opsitem		
			opsmetadata		
			parameter		
			patchbaseline		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
ModifyDocumentPermission	カスタム SSM ドキュメントを指定された AWS アカウントとパブリックまたはプライベートに共有するアクセス許可を付与します	権限の管理	document*		
				ssm:DocumentType	
PutCalendar [許可のみ]	特定のカレンダーを作成/編集する許可を付与	書き込み	document*		
PutComplianceItems	指定したリソースのコンプライアンスタイプおよびその他のコンプライアンス詳細を登録する許可を付与	書き込み	instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN	
PutConfigurePackageResult [アクセス許可のみ]	SSM Agentに、 特定のエージェントリクエスト（内部 Systems Manager の呼び出し）の結果のレポートを生成する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutInventory	指定した複数のマネージドインスタンスでインベントリ項目を追加または更新する許可を付与	書き込み		ssm:InventoryTypeName	
PutParameter	SSM パラメータを作成する許可を付与	書き込み	parameter*		
				aws:RequestTag/${TagKey} aws:TagKeys ssm:Overwrite ssm:Policies	
PutResourcePolicy	Systems Manager のリソースポリシーを作成または更新する許可を付与	権限の管理	document		
			opsitemgroup		
			parameter		
RegisterDefaultPatchBaseline	オペレーティングシステムタイプの既定のパッチベースラインを指定する許可を付与	書き込み	patchbaseline*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RegisterManagedInstance	Systems Manager Agent を登録するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
RegisterPatchBaselineForPatchGroup	指定したパッチグループのデフォルトのパッチベースラインを指定する許可を付与	書き込み	patchbaseline*		
RegisterTargetWithMaintenanceWindow	メンテナンスウィンドウでターゲットを登録する許可を付与	書き込み	maintenancewindow*		
RegisterTaskWithMaintenanceWindow	指定したメンテナンスウィンドウでタスクを登録する許可を付与	書き込み	maintenancewindow*		
RemoveTagsFromResource	指定したリソースから指定したタグキーを削除する許可を付与	Tagging	association		
			automation-execution		
			document		
			instance		
			maintenancewindow		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			managed-instance		
			opsitem		
			opsmetadata		
			parameter		
			patchbaseline		
			task		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ResetServiceSetting	のサービス設定をデフォルト値 AWS アカウント にリセットするアクセス許可を付与します	書き込み	servicesetting*		
ResumeSession	マネージドインスタンスに Session Manager のセッションを再接続する許可を付与	書き込み	session*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ssm:resourceTag/aws:ssmmessages:session-id ssm:resourceTag/aws:ssmmessages:target-id	
SendAutomationSignal	指定したオートメーション実行の現在の動作やステータスを変更するための信号を送信する許可を付与	書き込み	automation-execution*		
				aws:ResourceTag/${TagKey}	
SendCommand	指定した 1 つ以上のマネージドインスタンスでコマンドを実行する許可を付与	書き込み	document*		
			bucket		
			instance		
			managed-instance		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}	
StartAccessRequest	just-in-timeノードアクセスセッションのワークフローを開始する許可を付与	書き込み	instance		
			managed-instance		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartAssociationsOnce	指定した関連付けを手動で実行する許可を付与	書き込み	association*		
				aws:ResourceTag/${TagKey}	
StartAutomationExecution	オートメーションドキュメントの実行を開始する許可を付与	書き込み	automation-definition*		
			document*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
StartChangeRequestExecution	自動化ドキュメントの実行を開始する許可を付与	書き込み	automation-definition*		
			document*		
				aws:RequestTag/${TagKey} aws:TagKeys ssm:AutoApprove	
StartExecutionPreview	指定された Automation ランブックを実行するとターゲットリソースに与える影響を示すプレビューを作成するアクセス許可を付与します	読み取り			
StartSession	セッションマネージャーセッションの指定したターゲットへの接続を開始する許可を付与	書き込み	document		
			instance		
			managed-instance		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			task		
				ssm:SessionDocumentAccessCheck ssm:resourceTag/${TagKey} aws:ResourceTag/${TagKey} ssm:AccessRequestId	
StopAutomationExecution	既に進行中の指定したオートメーションの実行を停止する許可を付与	書き込み	automation-execution*		
				aws:ResourceTag/${TagKey}	
TerminateSession	インスタンスへの Session Manager 接続を永続的に終了するアクセス許可を付与	書き込み	session*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				ssm:resourceTag/aws:ssmmessages:session-id ssm:resourceTag/aws:ssmmessages:target-id	
UnlabelParameterVersion	指定済みバージョンのパラメータから識別ラベルを削除する許可を付与	書き込み	parameter*		
				aws:ResourceTag/${TagKey}	
UpdateAssociation	指定したターゲットで関連付けを更新し、関連付けをただちに実行する許可を付与	書き込み	association*		
			document		
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateAssociationStatus	指定したインスタンスに関連付けられている SSM ドキュメントのステータスを更新する許可を付与	書き込み	document*		
			instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN aws:ResourceTag/${TagKey}	
UpdateDocument	SSM ドキュメントの 1 つ以上の値を更新する許可を付与	書き込み	document*		
				ssm:DocumentType	
UpdateDocumentDefaultVersion	SSM ドキュメントのデフォルトバージョンを変更する許可を付与	書き込み	document*		
				ssm:DocumentType	
UpdateDocumentMetadata	SSM ドキュメントのメタデータを更新する許可を付与	書き込み	document*		
				ssm:DocumentType	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateInstanceAssociationStatus [アクセス許可のみ]	現在実行中の関連付けのステータスを更新するSSM Agentに許可を付与 (内部 Systems Manager の呼び出し)	書き込み	association*		
			instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN aws:ResourceTag/${TagKey}	
UpdateInstanceInformation	ハートビート信号をクラウド内の Systems Manager サービスに送信する SSM Agent に許可を付与	書き込み	instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateMaintenanceWindow	指定したメンテナンスウィンドウを更新する許可を付与	書き込み	maintenancewindow*		
UpdateMaintenanceWindowTarget	メンテナンスウィンドウターゲットを更新する許可を付与	書き込み	maintenancewindow*		
			windowtarget*		
UpdateMaintenanceWindowTask	メンテナンスウィンドウタスクを更新する許可を付与	書き込み	maintenancewindow*		
			windowtask*		
UpdateManagedInstanceRole	指定したマネージドインスタンスに割り当てられた IAM ロールを割り当てまたは変更する許可を付与	書き込み	iam-role*		
			managed-instance*		
				ssm:resourceTag/tag-key	
UpdateOpsItem	OpsItem を編集または変更する許可を付与	書き込み	opsitem*		
UpdateOpsMetadata	OpsMetadata オブジェクトを更新する許可を付与	書き込み	opsmetadata*		
UpdatePatchBaseline	指定したパッチベースラインを更新する許可を付与	書き込み	patchbaseline*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateResourceDataSync	リソースデータの同期を更新する許可を付与	書き込み	resourcedatasync*		
				ssm:SyncType	
UpdateServiceSetting	のサービス設定を更新するアクセス許可を付与します AWS アカウント	書き込み	servicesetting*		

AWS Systems Manager で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

> **Note**
>
> 一部の State Manager API パラメータは非推奨となりました。これは予期しない動作につながる可能性があります。詳細については、「IAM を使用した関連付けの作業」を参照してください。

リソースタイプ	ARN	条件キー
association	`arn:${Partition}:ssm:${Region}:${Account}:association/${AssociationId}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
automation-execution	arn:${Partition}:ssm:${Region}:${Account}:automation-execution/${AutomationExecutionId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
automation-definition	arn:${Partition}:ssm:${Region}:${Account}:automation-definition/${AutomationDefinitionName}:${VersionId}	
bucket	arn:${Partition}:s3:::${BucketName}	
document	arn:${Partition}:ssm:${Region}:${Account}:document/${DocumentName}	aws:ResourceTag/${TagKey} ssm:DocumentCategories ssm:DocumentType ssm:resourceTag/${TagKey}
iam-role	arn:${Partition}:iam::${Account}:role/${RoleName}	
instance	arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}
maintenancewindow	arn:${Partition}:ssm:${Region}:${Account}:maintenancewindow/${ResourceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key

リソースタイプ	ARN	条件キー
managed-instance	arn:${Partition}:ssm:${Region}:${Account}:managed-instance/${InstanceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
managed-instance-inventory	arn:${Partition}:ssm:${Region}:${Account}:managed-instance-inventory/${InstanceId}	
opsitem	arn:${Partition}:ssm:${Region}:${Account}:opsitem/${ResourceId}	aws:ResourceTag/${TagKey}
opsitemgroup	arn:${Partition}:ssm:${Region}:${Account}:opsitemgroup/default	
opsmetadata	arn:${Partition}:ssm:${Region}:${Account}:opsmetadata/${ResourceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}
parameter	arn:${Partition}:ssm:${Region}:${Account}:parameter/${ParameterNameWithoutLeadingSlash}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
patchbaseline	arn:${Partition}:ssm:${Region}:${Account}:patchbaseline/${PatchBaselineIdResourceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key

リソースタイプ	ARN	条件キー
session	arn:${Partition}:ssm:${Region}:${Account}:session/${SessionId}	ssm:resourceTag/aws:ssmmessages:session-id ssm:resourceTag/aws:ssmmessages:target-id
resourcedatasync	arn:${Partition}:ssm:${Region}:${Account}:resource-data-sync/${SyncName}	
servicesetting	arn:${Partition}:ssm:${Region}:${Account}:servicesetting/${ResourceId}	
windowtarget	arn:${Partition}:ssm:${Region}:${Account}:windowtarget/${WindowTargetId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
windowtask	arn:${Partition}:ssm:${Region}:${Account}:windowtask/${WindowTaskId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
task	arn:${Partition}:ecs:${Region}:${Account}:task/${TaskId}	aws:ResourceTag/${TagKey}

AWS Systems Manager の条件キー

AWS Systems Manager は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	指定したタグで許可されている値のセットに基づいて「作成」リクエストでアクセスをフィルタリング	String
aws:ResourceTag/${TagKey}	AWS リソースに割り当てられたタグキーと値のペアに基づいてアクセスをフィルタリングします	String
aws:TagKeys	必須タグがリクエストに含まれているかどうかに基づいて、「作成」リクエストでアクセスをフィルタリング	ArrayOfString
ec2:SourceInstanceARN	リクエストが発生したインスタンスの ARN によってアクセスをフィルタリングします	ARN
ssm:AccessRequestId	ユーザーがリクエストで指定されたアクセスリクエスト ID にアクセスできることを確認して、アクセスをフィルタリングします	String
ssm:AutoApprove	ユーザーがレビューステップなしで (変更フリーズイベントは例外) 、Change Manager ワークフローを開始するアクセス可能を持っていることを確認して、アクセスをフィルタリング	Bool
ssm:DocumentCategories	ユーザーが特定のカテゴリに属するドキュメントにアクセスする許可を持っていることを確認して、アクセスをフィルタリング	ArrayOfString
ssm:DocumentType	ユーザーが特定のドキュメントタイプに属するドキュメントにアクセスするアクセス許可を持っていることを確認して、アクセスをフィルタリングします。「aws」、「aws-cn」、「aws-us-gov」パーティションでのみ使用可能	String

条件キー	説明	[Type] (タイプ)
ssm:InventoryTypeName	ユーザーがリクエストで指定された InventoryType にもアクセスできることを確認して、アクセスをフィルタリングします	ArrayOfString
ssm:Overwrite	Systems Manager のパラメータを上書きできるかどうかの制御によって、アクセスをフィルタリング	String
ssm:Policies	IAM エンティティ (ユーザーまたはロール) がパラメータポリシーを含むパラメータを作成または更新できるかどうかを制御することでアクセスをフィルタリングする	String
ssm:Recursive	階層構造で作成された Systems Manager のパラメータによってアクセスをフィルタリング	String
ssm:SessionDocumentAccessCheck	ユーザーがデフォルトの Session Manager 設定ドキュメントまたはリクエストで指定されたカスタム設定ドキュメントにアクセスする権限を持っていることを確認して、アクセスをフィルタリング	Bool
ssm:SourceInstanceARN	リクエスト元の AWS Systems Manager マネージドインスタンスの Amazon リソースネーム (ARN) を検証してアクセスをフィルタリングします。EC2 インスタンスプロファイルに関連付けられた IAM ロールで認証されたマネージドインスタンスからリクエストが送信された場合、このキーは存在しません。	ARN
ssm:SyncType	リクエストで指定された ResourceDataSync SyncType にユーザーがアクセスできることを確認して、アクセスをフィルタリング	String
ssm:resourceTag/${TagKey}	Systems Manager リソースに割り当てられたタグのキーおよび値のペアによってアクセスをフィルタリング	String

条件キー	説明	[Type] (タイプ)
ssm:resourceTag/aws:ssmmessages:session-id	Systems Manager セッションリソースに割り当てられたタグのキーおよび値のペアに基づいてアクセスをフィルタリングします	String
ssm:resourceTag/aws:ssmmessages:target-id	Systems Manager セッションリソースに割り当てられたタグのキーおよび値のペアに基づいてアクセスをフィルタリングします	String
ssm:resourceTag/tag-key	Systems Manager リソースに割り当てられたタグのキーおよび値のペアに基づいてアクセスをフィルタリング	String

AWS Systems Manager for SAP のアクション、リソース、および条件キー

AWS Systems Manager for SAP (サービスプレフィックス: `ssm-sap`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Systems Manager for SAP で定義されるアクション
- AWS Systems Manager for SAP で定義されるリソースタイプ
- AWS Systems Manager for SAP の条件キー

AWS Systems Manager for SAP で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
BackupDatabase	指定されたデータベースでバックアップオペレーションを実行する許可を付与	書き込み			
DeleteResourcePermission	SSM for SAP のデータベースリソースに関連する SSM for SAP レベルを削除する許可を付与	書き込み			
DeregisterApplication	SAP アプリケーションを SSM for SAP から登録解除する許可を付与	書き込み	application		
GetApplication	アプリケーション ID またはアプリケーション ARN を提供し、SSM for SAP に登録されているアプリケーションに関する情報にアクセスする許可を付与	読み取り			
GetComponent	アプリケーション ID およびコンポーネント ID を提供し、SSM for SAP に登録されているコンポーネントに関する情報にアクセスする許可を付与	読み取り	component		
GetDatabase	アプリケーション ID、コンポーネント ID およびデータベース ID を提供し、SSM for SAP に登録されているデータベースに関する情報にアクセスする許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetOperation	オペレーション ID を提供し、オペレーションに関する情報にアクセスする許可を付与	読み取り			
GetResourcePermission	SSM for SAP のデータベースリソースに関連する SSM for SAP レベルを取得する許可を付与	読み取り			
ListApplications	顧客の下で SSM for SAP に登録されているすべてのアプリケーションのリストを取得するアクセス許可を付与しますAWS アカウント	リスト			
ListComponents	顧客のアカウント、または特定のアプリケーションのすべてのコンポーネントのリストを取得する許可を付与	リスト	application		
ListDatabases	顧客のアカウント、または特定のアプリケーションのすべてのデータベースのリストを取得する許可を付与	リスト			
ListOperationEvents	指定されたオペレーション内のすべてのオペレーションイベントのリストを取得する許可を付与する	リスト			
ListOperations	顧客のアカウント (追加フィルター適用可能) のすべてのオペレーションのリストを取得する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTagsForResource	指定したリソース ARN のタグを一覧表示する許可を付与	読み取り			
PutResourcePermission	SSM for SAP のデータベースリソースに関連する SSM for SAP レベルのリソース アクセス許可を追加する許可を付与	書き込み			
RegisterApplication	SSM for SAP に SAP アプリケーションを登録する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
RestoreDatabase	データベースを別のデータベースから復元する許可を付与	書き込み			
StartApplication	登録済みの SSM for SAP アプリケーションを起動する許可を付与する	書き込み	application		
StartApplicationRefresh	SAP アプリケーション用の登録済み SSM のオンデマンド検出を開始するための許可を付与します	書き込み	application		
StopApplication	登録済みの SSM for SAP アプリケーションを停止する許可を付与する	書き込み	application		
TagResource	指定されたリソース ARN にタグを付ける許可を付与	Tagging	application		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			component		
			database		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	指定されたリソース ARN からタグを削除する許可を付与	Tagging	application		
			component		
			database		
				aws:TagKeys	
UpdateApplicationSettings	登録した SSM for SAP アプリケーションの設定を更新する許可を付与	書き込み	application		
UpdateHANABackupSettings	指定されたデータベースの HANA バックアップ設定を更新する許可を付与	書き込み			

AWS Systems Manager for SAP で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
application	`arn:${Partition}:ssm-sap:${Region}:${Account}:${ApplicationType}/${ApplicationId}`	aws:ResourceTag/${TagKey}
component	`arn:${Partition}:ssm-sap:${Region}:${Account}:${ApplicationType}/${ApplicationId}/COMPONENT/${ComponentId}`	aws:ResourceTag/${TagKey}
database	`arn:${Partition}:ssm-sap:${Region}:${Account}:${ApplicationType}/${ApplicationId}/DB/${DatabaseId}`	aws:ResourceTag/${TagKey}

AWS Systems Manager for SAP の条件キー

AWS Systems Manager for SAP では、IAM ポリシーの `Condition`要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列

条件キー	説明	タイプ
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Systems Manager GUI Connectのアクション、リソース、および条件キー

AWS Systems Manager GUI Connect (サービスプレフィックス: `ssm-guiconnect`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Systems Manager GUI Connectで定義されるアクション
- AWS Systems Manager GUI Connectで定義されるリソースタイプ
- AWS Systems Manager GUI Connectの条件キー

AWS Systems Manager GUI Connectで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にア

クションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CancelConnection [アクセス許可のみ]	GUI Connect 接続を終了する許可を付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteConnectionRecordingPreferences	GUI Connect 接続記録設定を削除するアクセス許可を付与します	書き込み			
GetConnection [アクセス許可のみ]	GUI Connect 接続のメタデータを取得する許可を付与する	読み取り			
GetConnectionRecordingPreferences	GUI Connect 接続記録設定を取得する許可を付与	読み取り			
ListConnections [許可のみ]	GUI Connect 接続のメタデータを一覧表示する許可を付与する	リスト			
StartConnection [許可のみ]	GUI Connect 接続を開始する許可を付与する	書き込み			
UpdateConnectionRecordingPreferences	GUI Connect 接続の記録設定を更新するアクセス許可を付与します	書き込み			

AWS Systems Manager GUI Connectで定義されるリソースタイプ

AWS Systems Manager GUI Connect は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Systems Manager GUI Connecにアクセスするには、`"Resource": "*"`のポリシーで特定してください。

AWS Systems Manager GUI Connectの条件キー

GUI Connectには、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Systems Manager Incident Manager のアクション、リソース、および条件キー

AWS Systems Manager Incident Manager (サービスプレフィックス: ssm-incidents) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Systems Manager Incident Manager によって定義されるアクション
- AWS Systems Manager Incident Manager によって定義されたリソースタイプ
- AWS Systems Manager Incident Manager の条件キー

AWS Systems Manager Incident Manager によって定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にア

クションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchGetIncidentFindings	インシデントレコードの指定された検出結果に関する詳細を取得する許可を付与	読み取り	incident-record*		
			response-plan*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateReplicationSet	レプリケーションセットを作成するためのアクセス許可を付与します	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole ssm-incidents:TagResource
CreateResponsePlan	対応プランを作成するためのアクセス許可を付与します	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole ssm-incidents:TagResource
CreateTimelineEvent	インシデントレコードのタイムラインイベントを作成するためのアクセス許可を付与します	Write	incident-record* response-plan*		
DeleteIncidentRecord	インシデントレコードを削除するためのアクセス許可を付与します	Write	incident-record*		
DeleteReplicationSet	レプリケーションセットを削除するためのアクセス許可を付与します	Write	replication-set*		
DeleteResourcePolicy	対応プランからリソースポリシーを削除するためのアクセス許可を付与します	Permissions management	response-plan*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteResponsePlan	対応プランを削除するためのアクセス許可を付与します	Write	response-plan*		
DeleteTimelineEvent	タイムラインイベントを削除するためのアクセス許可を付与します	Write	incident-record*		
GetIncidentRecord	インシデントレコードの内容を表示するためのアクセス許可を付与します	Read	incident-record*		
			response-plan*		
GetReplicationSet	レプリケーションセットを表示するためのアクセス許可を付与します	Read	replication-set*		
GetResourcePolicies	対応プランのリソースポリシーを表示するためのアクセス許可を付与します	Read	response-plan*		
GetResponsePlan	指定された対応プランの内容を表示するためのアクセス許可を付与します	Read	response-plan*		
GetTimelineEvent	タイムラインイベントを表示するためのアクセス許可を付与します	読み取り	incident-record*		
			response-plan*		
ListIncidentFindings	インシデントレコードの検出結果を一覧表示する許可を付与	リスト	incident-record*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			response-plan*		
ListIncidentRecords	すべてのインシデントレコードの内容を一覧表示するためのアクセス許可を付与します	リスト			
ListRelatedItems	インシデントレコードの関連アイテムを一覧表示する許可を付与	リスト	incident-record*		
			response-plan*		
ListReplicationSets	すべてのレプリケーションセットを一覧表示するためのアクセス許可を付与します	リスト			
ListResponsePlans	すべての対応プランを一覧表示するためのアクセス許可を付与します	リスト			
ListTagsForResource	指定したリソースのリソースタグのリストを表示する許可を付与	Read	incident-record		
			replication-set		
			response-plan		
ListTimelineEvents	インシデントレコードのすべてのタイムラインイベントを一覧表示するためのアクセス許可を付与します。	リスト	incident-record*		
			response-plan*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutResourcePolicy	対応プランにリソースポリシーを配置するためのアクセス許可を付与します	Permissions management	response-plan*		
StartIncident	対応プランを使用して新しいインシデントを開始する許可を付与	Write	response-plan*		
TagResource	対応プランにタグを追加するためのアクセス許可を付与	タグ付け	incident-record		
			replication-set		
			response-plan		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	対応プランからタグを削除するためのアクセス許可を付与	タグ付け	incident-record		
			replication-set		
			response-plan		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
UpdateDeletionProtection	レプリケーションセットの削除保護を更新するためのアクセス許可を付与します	Write	replication-set*		
UpdateIncidentRecord	インシデントレコードの内容を更新するためのアクセス許可を付与します	Write	incident-record*		
			response-plan*		
UpdateRelatedItems	インシデントレコードの関連アイテムを更新するためのアクセス許可を付与します	Write	incident-record*		
			response-plan*		
UpdateReplicationSet	レプリケーションセットを更新するためのアクセス許可を付与します	Write	replication-set*		
UpdateResponsePlan	対応プランの内容を更新するためのアクセス許可を付与します	Write	response-plan*		iam:PassRole ssm-incidents:TagResource

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateTimelineEvent	タイムラインイベントを更新するためのアクセス許可を付与します	Write	incident-record*		
			response-plan*		

AWS Systems Manager Incident Manager によって定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
response-plan	arn:${Partition}:ssm-incidents::${Account}:response-plan/${ResponsePlan}	aws:ResourceTag/${TagKey}
incident-record	arn:${Partition}:ssm-incidents::${Account}:incident-record/${ResponsePlan}/${IncidentRecord}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
replication-set	arn:${Partition}:ssm-incidents::${Account}:replication-set/${ReplicationSet}	aws:ResourceTag/${TagKey}

AWS Systems Manager Incident Manager の条件キー

AWS Systems Manager Incident Manager は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Systems Manager Incident Manager Contacts のアクション、リソース、および条件キー

AWS Systems Manager Incident Manager Contacts (サービスプレフィックス: ssm-contacts) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Systems Manager Incident Manager Contacts で定義されるアクション
- AWS Systems Manager Incident Manager Contacts で定義されるリソースタイプ
- AWS Systems Manager Incident Manager Contacts の条件キー

AWS Systems Manager Incident Manager Contacts で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptPage	ページを受け入れるためのアクセス許可を付与	Write	page*		
ActivateContactChannel	連絡先の連絡先チャネルを有効化するためのアクセス許可を付与	Write	contactchannel*		
AssociateContact [アクセス許可のみ]	エスカレーションプランで連絡先を使用するためのアクセス許可を付与	Permissions management	contact*		
CreateContact	連絡先を作成する許可を付与	Write	contact*		ssm-contacts:AssociateContact
				aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey}	
CreateContactChannel	連絡先の連絡先チャネルを作成するためのアクセス許可を付与	書き込み	contact*		
CreateRotation	オンコールスケジュールでのローテーションを作成する許可を付与	書き込み	rotation*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRotationOverride	オンコールスケジュールでのローテーションに対する上書きを作成する許可を付与	書き込み	rotation*		
DeactivateContactChannel	連絡先の連絡先チャネルを無効化するためのアクセス許可を付与	Write	contactchannel*		
DeleteContact	連絡先を削除するためのアクセス許可を付与	Write	contact*		
DeleteContactChannel	連絡先の連絡先チャンネルを削除するためのアクセス許可を付与	書き込み	contactchannel*		
DeleteRotation	ローテーションを削除する許可を付与	書き込み	rotation*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteRotationOverride	ローテーションに対する上書きを削除する許可を付与	書き込み	rotation*		
DescribeEngagement	エンゲージメントを記述するためのアクセス許可を付与	Read	engagement*		
DescribePage	ページを記述するためのアクセス許可を付与	Read	page*		
GetContact	連絡先を取得するためのアクセス許可を付与	Read	contact*		
GetContactChannel	連絡先の連絡先チャネルを取得するためのアクセス許可を付与	読み取り	contactchannel*		
GetContactPolicy	連絡先のリソースポリシーを取得するためのアクセス許可を付与	読み取り	contact*		
GetRotation	オンコールローテーションについての情報を取得する許可を付与	読み取り	rotation*		
GetRotationOverride	オンコールローテーションでの上書きに関する情報を取得する許可を付与	読み取り	rotation*		
ListContactChannels	連絡先のすべての連絡先チャネルを一覧表示するためのアクセス許可を付与	リスト	contact*		
ListContacts	すべての連絡先を一覧表示するためのアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListEngagements	すべてのエンゲージメントを一覧表示するためのアクセス許可を付与	リスト			
ListPageReceipts	ページのすべての受領書を一覧表示するためのアクセス許可を付与	リスト	page*		
ListPageResolutions	エンゲージメントの解決パスを一覧表示するアクセス許可を付与します	リスト	page*		
ListPagesByContact	連絡先に送信されたすべてのページを一覧表示するためのアクセス許可を付与	リスト	contact*		
ListPagesByEngagement	エンゲージメントで作成されたすべてのページを一覧表示するためのアクセス許可を付与	リスト	engagement*		
ListPreviewRotationShifts	ローテーション設定パラメータに基づいたシフトのリストを取得する許可を付与	リスト			
ListRotationOverrides	オンコールローテーションに対し現在指定されている上書きのリストを取得する許可を付与	リスト	rotation*		
ListRotationShifts	オンコールスケジュールでのローテーションシフトのリストを取得する許可を付与	リスト	rotation*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListRotations	オンコールローテーションのリストを取得する許可を付与	リスト			
ListTagsForResource	指定したリソースのリソースタグのリストを表示する許可を付与	読み取り	contact		
			rotation		
PutContactPolicy	連絡先にリソースポリシーを追加するためのアクセス許可を付与	Write	contact*		
SendActivationCode	連絡先の連絡先チャネルのアクティベーションコードを送信するためのアクセス許可を付与	Write	contactchannel*		
StartEngagement	エンゲージメントを開始するためのアクセス許可を付与	Write	contact*		
StopEngagement	エンゲージメントを停止するためのアクセス許可を付与	書き込み	engagement*		
TagResource	指定されたリソースにタグを追加するための許可を付与します	Tagging	contact		
			rotation		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource		Tagging	contact		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	指定されたリソースからタグを削除するための許可を付与します		rotation		
				aws:TagKeys	
UpdateContact	連絡先を更新するためのアクセス許可を付与	Write	contact*		ssm-contacts:AssociateContact
UpdateContactChannel	連絡先の連絡先チャネルを更新するためのアクセス許可を付与	書き込み	contactchannel*		
UpdateRotation	オンコールローテーションに指定した情報を更新する許可を付与	書き込み	rotation*		

AWS Systems Manager Incident Manager Contacts で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
contact	`arn:${Partition}:ssm-contacts:${Region}:${Account}:contact/${ContactAlias}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
contactchannel	arn:${Partition}:ssm-contacts:${Region}:${Account}:contactchannel/${ContactAlias}/${ContactChannelId}	
engagement	arn:${Partition}:ssm-contacts:${Region}:${Account}:engagement/${ContactAlias}/${EngagementId}	
page	arn:${Partition}:ssm-contacts:${Region}:${Account}:page/${ContactAlias}/${PageId}	
rotation	arn:${Partition}:ssm-contacts:${Region}:${Account}:rotation/${RotationId}	aws:ResourceTag/${TagKey}

AWS Systems Manager Incident Manager Contacts の条件キー

AWS Systems Manager Incident Manager Contacts では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列

条件キー	説明	タイプ
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Systems Manager Quick Setup のアクション、リソース、および条件キー

AWS Systems Manager 高速セットアップ (サービスプレフィックス: ssm-quicksetup) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Systems Manager Quick Setup で定義されるアクション
- AWS Systems Manager Quick Setup で定義されるリソースタイプ
- AWS Systems Manager Quick Setup の条件キー

AWS Systems Manager Quick Setup で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にア

クションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateConfigurationManager	Quick Setup 設定マネージャーリソースを作成する許可を付与する	書き込み	configuration-manager*	aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteConfigurationManager	設定マネージャーを削除する許可を付与する	書き込み	configuration-manager*		
GetConfiguration	高速セットアップ設定を取得する許可を付与	読み取り	configuration-manager		
GetConfigurationManager	設定マネージャーを取得する許可を付与する	読み取り	configuration-manager*		
GetServiceSettings	リクエスト元の AWS アカウント と で高速セットアップ用に設定された設定を取得するアクセス許可を付与します AWS リージョン	読み取り			
ListConfigurationManagers	Quick Setup 設定マネージャーを一覧表示する許可を付与する	リスト			
ListConfigurations	高速セットアップ設定を一覧表示するアクセス許可を付与します	リスト	configuration-manager		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListQuickSetupTypes	利用可能な Quick Setup の種類を一覧表示する許可を付与する	読み取り			
ListTagsForResource	リソースに割り当てられたタグを一覧表示する許可を付与する	読み取り	configuration-manager*		
TagResource	AWS リソースにメタデータのキーと値のペアを割り当てるアクセス許可を付与します	Tagging	configuration-manager*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	指定されたリソースからタグを削除するための許可を付与します	Tagging	configuration-manager*		
				aws:TagKeys	
UpdateConfigurationDefinition	Quick Setup 設定定義を更新する許可を付与する	書き込み	configuration-manager*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateConfigurationManager	Quick Setup 設定マネージャーを更新する許可を付与する	書き込み	configuration-manager*		
UpdateServiceSettings	Quick Setup 用に設定された設定を更新する許可を付与する	書き込み			

AWS Systems Manager Quick Setup で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
configuration-manager	arn:${Partition}:ssm-quicksetup:${Region}:${Account}:configuration-manager/${ConfigurationManagerId}	aws:ResourceTag/${TagKey}

AWS Systems Manager Quick Setup の条件キー

AWS Systems Manager クイックセットアップでは、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

タグエディタ のアクション、リソース、および条件キー

タグエディタ (サービスプレフィックス: `resource-explorer`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- タグエディタで定義されるアクション
- タグエディタで定義されるリソースタイプ
- タグエディタの条件キー

タグエディタで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListResourceTypes [アクセス許可のみ]	タグエディターで現在サポートされているリソースタイプを取得するためのアクセス許可を付与	リスト			
ListResources [許可のみ]	内のリソースの識別子を取得するアクセス許可を付与します AWS アカウント	リスト			
ListTags [許可のみ]	指定されたリソース識別子にアタッチされたタグを取得するためのアクセス許可を付与	Read			tag:GetResources

タグエディタで定義されるリソースタイプ

タグエディタでは、IAM ポリシーステートメントの `Resource` 要素でのリソース ARN の指定はサポートされていません。タグエディタへのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

タグエディタの条件キー

タグエディターには、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Tax Settings のアクション、リソース、および条件キー

AWS Tax Settings (サービスプレフィックス: `tax`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Tax Settingsで定義されるアクション
- AWS Tax Settings で定義されるリソースタイプ
- AWS Tax Settings の条件キー

AWS Tax Settingsで定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchDeleteTaxRegistration	税登録データを一括削除する許可を付与する	書き込み			
BatchPutTaxRegistration	税登録をバッチ更新するアクセス許可を付与	書き込み			
DeleteSupplementalTaxRegistration	補足税登録データを削除する許可を付与	書き込み			
DeleteTaxRegistration	税登録データを削除するアクセス許可を付与	書き込み			
GetExemptions	免税データを表示するアクセス許可を付与	読み取り			
GetTaxInfoReportingDocument [許可のみ]	税務書類/フォームを表示/ダウンロードする許可を付与する	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetTaxInheritance	税継承ステータスを表示するアクセス許可を付与	読み取り			
GetTaxInterview [許可のみ]	Tax Interview データを取得する許可を付与	読み取り			
GetTaxRegistration	税登録データを表示する許可を付与	読み取り			
GetTaxRegistrationDocument	税登録ドキュメントをダウンロードするアクセス許可を付与	読み取り			
ListSupplementalTaxRegistrations	補助税登録を表示する許可を付与	読み取り			
ListTaxRegistrations	税登録を表示するアクセス許可を付与	読み取り			
PutSupplementalTaxRegistration	補足税登録データを更新する許可を付与	書き込み			
PutTaxInheritance	税継承を設定するアクセス許可を付与	書き込み			
PutTaxInterview [アクセス許可のみ]	Tax Interview データを更新する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutTaxRegistration	税登録データを更新する許可を付与	書き込み			
UpdateExemptions	免税データを更新するアクセス許可を付与	書き込み			

AWS Tax Settings で定義されるリソースタイプ

AWS Tax Settings は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Tax Settings へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Tax Settings の条件キー

Tax Settings には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS Telco Network Builder のアクション、リソース、条件キー

AWS Telco Network Builder (サービスプレフィックス: `tnb`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Telco Network Builder によって定義されたアクション

- AWS Telco Network Builder によって定義されたリソースタイプ
- AWS Telco Network Builder の条件キー

AWS Telco Network Builder によって定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CancelSolNetworkOperation	ネットワークオペレーションをキャンセルするための許可を付与します	書き込み	network-operation*		
CreateSolFunctionPackage	関数パッケージを作成するための許可を付与します	書き込み	function-package*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSolNetworkInstance	ネットワークインスタンスを作成するための許可を付与します	書き込み	network-instance*		
			network-package*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateSolNetworkPackage	ネットワークパッケージを作成するための許可を付与します	書き込み	network-package*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSolFunctionPackage	関数パッケージを削除するための許可を付与します	書き込み	function-package*		
DeleteSolNetworkInstance	ネットワークインスタンスを削除するための許可を付与します	書き込み	network-instance*		
DeleteSolNetworkPackage	ネットワークパッケージを削除するための許可を付与します	書き込み	network-package*		
GetSolFunctionInstance	関数インスタンスを取得するための許可を付与します	読み取り	function-instance*		
				aws:ResourceTag/${TagKey}	
GetSolFunctionPackage	関数パッケージを取得するための許可を付与します	読み取り	function-package*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetSolFunctionPackageContent	関数パッケージのコンテンツを取得するための許可を付与します	読み取り	function-package*		
				aws:ResourceTag/${TagKey}	
GetSolFunctionPackageDescriptor	関数パッケージ記述子を取得するための許可を付与します	読み取り	function-package*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkInstance	ネットワークインスタンスを取得するための許可を付与します	読み取り	network-instance*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkOperation	ネットワークオペレーションを取得するための許可を付与します	読み取り	network-operation*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkPackage	ネットワークパッケージを取得するための許可を付与します	読み取り	network-package*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetSolNetworkPackageContent	ネットワークパッケージのコンテンツを取得するための許可を付与します	読み取り	network-package*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkPackageDescriptor	ネットワークパッケージ記述子を取得するための許可を付与します	読み取り	network-package*		
				aws:ResourceTag/${TagKey}	
InstantiateSolNetworkInstance	ネットワークインスタンスをインスタンス化するための許可を付与します	書き込み	network-instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListSolFunctionInstances	関数インスタンスを一覧表示するための許可を付与します	リスト	function-instance*		
				aws:ResourceTag/${TagKey}	
ListSolFunctionPackages	関数パッケージを一覧表示するための許可を付与します	リスト	function-package*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
ListSolNetworkInstances	ネットワークインスタンスを一覧表示するための許可を付与します	リスト	network-instance*		
				aws:ResourceTag/${TagKey}	
ListSolNetworkOperations	ネットワークオペレーションを一覧表示するための許可を付与します	リスト	network-operation*		
				aws:ResourceTag/${TagKey}	
ListSolNetworkPackages	ネットワークパッケージを一覧表示するための許可を付与します	リスト	network-package*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	リソースのタグのリストを返す許可を付与	リスト			
PutSolFunctionPackageContent	関数パッケージのコンテンツをアップロードするための許可を付与します	書き込み	function-package*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutSolNetworkPackageContent	ネットワークパッケージのコンテンツをアップロードするための許可を付与します	書き込み	network-package*		
TagResource	指定されたリソースにタグを追加するための許可を付与します	Tagging	function-instance		
			function-package		
			network-instance		
			network-operation		
			network-package		
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateSolNetworkInstance	ネットワークインスタンスを終了するための許可を付与します	書き込み	network-instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	指定されたリソースからタグを削除するための許可を付与します	Tagging	function-instance		
			function-package		
			network-instance		
			network-operation		
			network-package		
				aws:TagKeys	
UpdateSolFunctionPackage	関数パッケージを更新するための許可を付与します	書き込み	function-package*		
UpdateSolNetworkInstance	ネットワークインスタンスを更新するための許可を付与します	書き込み	function-instance*		
			network-instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateSolNetworkPackage	ネットワークパッケージを更新するための許可を付与します	書き込み	network-package*		
ValidateSolFunctionPackageContent	関数パッケージのコンテンツを検証するための許可を付与します	書き込み	function-package*		
ValidateSolNetworkPackageContent	ネットワークパッケージのコンテンツを検証するための許可を付与します	書き込み	network-package*		

AWS Telco Network Builder によって定義されたリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
function-package	`arn:${Partition}:tnb:${Region}:${Account}:function-package/${FunctionPackageId}`	aws:ResourceTag/${TagKey}
network-package	`arn:${Partition}:tnb:${Region}:${Account}:network-package/${NetworkPackageId}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
network-instance	arn:${Partition}:tnb:${Region}:${Account}:network-instance/${NetworkInstanceId}	aws:ResourceTag/${TagKey}
function-instance	arn:${Partition}:tnb:${Region}:${Account}:function-instance/${FunctionInstanceId}	aws:ResourceTag/${TagKey}
network-operation	arn:${Partition}:tnb:${Region}:${Account}:network-operation/${NetworkOperationId}	aws:ResourceTag/${TagKey}

AWS Telco Network Builder の条件キー

AWS Telco Network Builder では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアの存在有無を確認することによりアクセスをフィルタリング	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアを確認することによりアクセスをフィルタリング	String
aws:TagKeys	リクエスト内のタグキーのプレゼンスによってアクセスをフィルタリング	ArrayOfString

Amazon Textract のアクション、リソース、および条件キー

Amazon Textract (サービスプレフィックス: `textract`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Textract で定義されるアクション
- Amazon Textract で定義されるリソースタイプ
- Amazon Textract の条件キー

Amazon Textract で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AnalyzeDocument	入力として提供されるイメージ内の実際のドキュメントエンティティのインスタンスを検出する許可を付与	読み取り			s3:GetObject
AnalyzeExpense	入力として提供されるイメージ内の実際のドキュメントエンティティのインスタンスを検出する許可を付与	読み取り			s3:GetObject
AnalyzeID	入力として提供されたアイデンティティドキュメントから	読み取り			s3:GetObject

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	関連情報を検出する権限を付与します。				
CreateAdapter	Amazon Textract アダプターを作成するアクセス許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAdapterVersion	Amazon Textract アダプターバージョンを作成するアクセス許可を付与	書き込み	adapter*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAdapter	Amazon Textract アダプターを削除するアクセス許可を付与	書き込み	adapter*		
DeleteAdapterVersion	Amazon Textract アダプターバージョンを削除するアクセス許可を付与	書き込み	adapterversion*		
DetectDocumentText	ドキュメントイメージ内のテキストを検出する許可を付与	読み取り			s3:GetObject
GetAdapter	Amazon Textract アダプターを取得するアクセス許可を付与	読み取り	adapter*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetAdapterVersion	Amazon Textract アダプターバージョンを取得するアクセス許可を付与	読み取り	adapterversion*		
GetDocumentAnalysis	ドキュメント分析ジョブに関する情報を返す許可を付与	読み取り			
GetDocumentTextDetection	ドキュメントテキスト検出ジョブに関する情報を返す許可を付与	読み取り			
GetExpenseAnalysis	費用分析ジョブに関する情報を返す許可を付与します。	読み取り			
GetLendingAnalysis	レンディングアナリシスジョブに関するページレベルの情報を取得する許可を付与	読み取り			
GetLendingAnalysisSummary	レンディングアナリシスジョブに関するページレベルの概要情報を取得する許可を付与	読み取り			
ListAdapterVersions	Amazon Textract アダプターバージョンを一覧表示するアクセス許可を付与	読み取り			
ListAdapters	Amazon Textract アダプターを一覧表示するアクセス許可を付与	読み取り			
ListTagsForResource	リソースに関連付けられたタグのリストを返す許可を付与します。	読み取り	adapter adapterversion		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartDocumentAnalysis	入力として提供されたイメージまたは pdf 内の実際のドキュメントエンティティのインスタンスを検出する非同期ジョブを開始する許可を付与	書き込み			s3:GetObject
StartDocumentTextDetection	ドキュメントイメージまたは pdf 内のテキストを検出する非同期ジョブを開始する許可を付与	書き込み			s3:GetObject
StartExpenseAnalysis	入力として提供されたイメージまたは pdf 内の実際のドキュメントエンティティのインスタンスを検出する非同期ジョブを開始する許可を付与	書き込み			s3:GetObject
StartLendingAnalysis	入力として提供されたイメージまたは PDF を取得し、レンディングドキュメント内のエンティティを検出する非同期ジョブを開始する許可を付与	書き込み			s3:GetObject
TagResource	リソースに 1 つ以上のタグを追加する許可を付与	タグ付け	adapter		
			adapterversion		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	リソースから 1 つ以上のタグを削除する許可を付与	Tagging	adapter		
			adapterversion		
				aws:TagKeys	
UpdateAdapter	Amazon Textract アダプターを更新するアクセス許可を付与	書き込み	adapter*		

Amazon Textract で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
adapter	`arn:${Partition}:textract:${Region}:${Account}:/adapters/${AdapterId}`	aws:ResourceTag/${TagKey}
adapterversion	`arn:${Partition}:textract:${Region}:${Account}:/adapters/${AdapterId}/versions/${AdapterVersion}`	aws:ResourceTag/${TagKey}

Amazon Textract の条件キー

Amazon Textract は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエストで渡されたタグによりアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグによりアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーによりアクセスをフィルタリングします	ArrayOfString

Amazon Timestream のアクション、リソース、および条件キー

Amazon Timestream (サービスプレフィックス: timestream) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件キーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Timestream で定義されたアクション
- Amazon Timestream で定義されるリソースタイプ

- Amazon Timestream の条件キー

Amazon Timestream で定義されたアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CancelQuery	アカウント内のクエリをキャンセルする許可を付与	書き込み			timestream:DescribeEndpoints
CreateBatchLoadTask	アカウントでバッチロードタスクを作成するための許可を付与します	書き込み	table*		timestream:DescribeEndpoints timestream:WriteRecords
CreateDatabase	アカウントでデータベースを作成する許可を付与。	書き込み	database*		timestream:DescribeEndpoints
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScheduledQuery	アカウントで新しい保存済みクエリを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole timestream:DescribeEndpoints

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateTable	アカウントでテーブルを作成する許可を付与。	書き込み	table*		timestream:DescribeEndpoints
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDatabase	アカウント内のデータベースを削除する許可を付与。	書き込み	database*		timestream:DescribeEndpoints
DeleteScheduledQuery	アカウントで バッチジョブキューを削除する許可を付与	書き込み	scheduled-query*		timestream:DescribeEndpoints
DeleteTable	アカウント内のテーブルを削除する許可を付与。	書き込み	table*		timestream:DescribeEndpoints
DescribeAccountSettings	アカウント設定を記述する許可を付与する	読み取り			timestream:DescribeEndpoints

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeBatchLoadTask	アカウントでバッチロードタスクを記述するための許可を付与します	読み取り			timestream:DescribeEndpoints
DescribeDatabase	アカウント内のデータベースを説明する許可を付与。	読み取り	database*		timestream:DescribeEndpoints
DescribeEndpoints	Timestream のエンドポイントを説明する許可を付与。	リスト			
DescribeScheduledQuery	アカウント内の 1 つ以上のスケジュールされたインスタンスを記述する許可を付与	読み取り	scheduled-query*		timestream:DescribeEndpoints
DescribeTable	アカウント内のテーブルを説明する許可を付与	読み取り	table*		timestream:DescribeEndpoints
ExecuteScheduledQuery	アカウント内でスケジュールされたクエリを実行するアクセス許可を付与します	書き込み	scheduled-query*		timestream:DescribeEndpoints
GetAwsBackupStatus	Timestream Table Backup のステータスを取得する許可を付与	読み取り			timestream:DescribeEndpoints

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetAwsRestoreStatus	Timestream Table Restore のステータスを取得する許可を付与	読み取り			timestream:DescribeEndpoints
ListBatchLoadTasks	アカウントのバッチロードタスクを一覧表示するための許可を付与します	リスト			timestream:DescribeEndpoints
ListDatabases	アカウント内のデータベースを一覧表示する許可を付与	リスト			timestream:DescribeEndpoints
ListMeasures	アカウント内のテーブルの測定を一覧表示する許可を付与	リスト	table*		timestream:DescribeEndpoints
ListScheduledQueries	アカウントのスケジュールを一覧表示する許可を付与	リスト			timestream:DescribeEndpoints
ListTables	アカウントのテーブルを一覧表示する許可を付与	リスト	database*		timestream:DescribeEndpoints
ListTagsForResource	アカウント内のリソースのタグを一覧表示する許可を付与。	読み取り	database*		timestream:DescribeEndpoints

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			scheduled-query*		
			table*		
PrepareQuery	'prepare' クエリを発行する許可を付与	読み取り	table*		timestream:DescribeEndpoints timestream:Select
ResumeBatchLoadTask	アカウントでバッチロードタスクを再開するための許可を付与します	書き込み			timestream:DescribeEndpoints timestream:WriteRecords
Select	'select from table' クエリを発行する許可を付与	読み取り	table*		timestream:DescribeEndpoints
SelectValues	'select 1' クエリを発行する許可を付与	読み取り			timestream:DescribeEndpoints

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartAwsBackupJob	Timestream Table のバックアップジョブを開始する許可を付与	書き込み	table*		timestream:DescribeEndpoints
StartAwsRestoreJob	Timestream Table のバックアップのための復元ジョブを開始する許可を付与	書き込み	table*		timestream:DescribeEndpoints
TagResource	リソースにタグを追加するアクセス許可を付与します	Tagging	database*		timestream:DescribeEndpoints
			scheduled-query*		
			table*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
Unload	UNLOAD クエリを発行する許可を付与	書き込み	table*		s3:AbortMultipartUpload s3:GetObject s3:PutObject timestream:DescribeEndpoints timestream:Select
UntagResource	リソースからタグを削除する許可を付与	Tagging	database*		timestream:DescribeEndpoints
			scheduled-query*		
			table*		
				aws:TagKeys	
UpdateAccountSettings	アカウント設定を更新する許可を付与する	書き込み			timestream:DescribeEndpoints

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateDatabase	アカウント内のデータベースを更新する許可を付与。	書き込み	database*		timestream:DescribeEndpoints
UpdateScheduledQuery	アカウントで保存されたクエリを更新する許可を付与	書き込み	scheduled-query*		timestream:DescribeEndpoints
UpdateTable	アカウント内のテーブルを更新する許可を付与。	書き込み	table*		timestream:DescribeEndpoints
WriteRecords	アカウント内のテーブルにデータを取り込むアクセス許可を付与します。	書き込み	table*		timestream:DescribeEndpoints

Amazon Timestream で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
database	arn:${Partition}:timestream:${Region}:${Account}:database/${DatabaseName}	aws:ResourceTag/${TagKey}
table	arn:${Partition}:timestream:${Region}:${Account}:database/${DatabaseName}/table/${TableName}	aws:ResourceTag/${TagKey}
scheduled-query	arn:${Partition}:timestream:${Region}:${Account}:scheduled-query/${ScheduledQueryName}	aws:ResourceTag/${TagKey}

Amazon Timestream の条件キー

Amazon Timestream では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString

Amazon Timestream InfluxDB のアクション、リソース、および条件キー

Amazon Timestream InfluxDB (サービスプレフィックス: `timestream-influxdb`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件キーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Timestream InfluxDB で定義されたアクション
- Amazon Timestream InfluxDB で定義されるリソースタイプ
- Amazon Timestream InfluxDB の条件キー

Amazon Timestream InfluxDB で定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateDbCluster	新しい Timestream InfluxDB クラスターを作成するアクセス許可を付与します	書き込み	db-parameter-group		timestream-influxdb:CreateDbInstance
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateDbInstance	新しい Timestream InfluxDB インスタンスを作成する許可を付与する	書き込み	db-parameter-group		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDbParameterGroup	新しい Timestream InfluxDB パラメータグループを作成する許可を付与する	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDbCluster	Timestream InfluxDB クラスターを削除する許可を付与	書き込み	db-cluster*		timestream-influxdb:DeleteDbInstance
DeleteDbInstance	Timestream InfluxDB インスタンスを削除する許可を付与する	書き込み	db-instance*		
GetDbCluster	Timestream InfluxDB クラスターに関する情報を取得する許可を付与	読み取り	db-cluster*		
GetDbInstance	Timestream InfluxDB インスタンスに関する情報を取得する許可を付与する	読み取り	db-instance*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetDbParameterGroup	Timestream InfluxDB パラメータグループに関する情報を取得する許可を付与する	読み取り	db-parameter-group*		
ListDbClusters	アカウント内のすべての Timestream InfluxDB クラスターに関する情報を一覧表示するアクセス許可を付与します	リスト			
ListDbInstances	アカウント内のすべての Timestream InfluxDB インスタンスに関する情報を一覧表示する許可を付与する	リスト			
ListDbInstancesForCluster	クラスターに属するすべての Timestream InfluxDB インスタンスに関する情報を一覧表示するアクセス許可を付与します	読み取り	db-cluster*		
ListDbParameterGroups	すべての Timestream InfluxDB パラメータグループに関する情報を一覧表示する許可を付与する	リスト			
ListTagsForResource	Timestream InfluxDB リソースのタグを一覧表示する許可を付与する	読み取り	db-cluster		
			db-instance		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			db-parameter-group		
				aws:ResourceTag/${TagKey}	
TagResource	Timestream InfluxDB リソースにタグを付ける許可を付与する	Tagging	db-cluster		
			db-instance		
			db-parameter-group		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Timestream InfluxDB リソースのタグを解除する許可を付与する	Tagging	db-cluster		
			db-instance		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			db-parameter-group		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateDbCluster	Timestream InfluxDB クラスターを更新する許可を付与	書き込み	db-cluster*		timestream-influxdb:UpdateDbInstance
			db-parameter-group		
UpdateDbInstance	Timestream InfluxDB インスタンスを更新する許可を付与する	書き込み	db-instance*		
			db-parameter-group		

Amazon Timestream InfluxDB で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
db-cluster	arn:${Partition}:timestream-influxdb:${Region}:${Account}:db-cluster/${DbClusterId}	aws:ResourceTag/${TagKey}
db-instance	arn:${Partition}:timestream-influxdb:${Region}:${Account}:db-instance/${DbInstanceIdentifier}	aws:ResourceTag/${TagKey}
db-parameter-group	arn:${Partition}:timestream-influxdb:${Region}:${Account}:db-parameter-group/${DbParameterGroupIdentifier}	aws:ResourceTag/${TagKey}

Amazon Timestream InfluxDB の条件キー

Amazon Timestream InfluxDB では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString

AWS Tiros のアクション、リソース、および条件キー

AWS Tiros (サービスプレフィックス: `tiros`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Tiros で定義されるアクション
- AWS Tiros で定義されるリソースタイプ
- AWS Tiros の条件キー

AWS Tiros で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateQuery [アクセス許可のみ]	VPC 到達可能性クエリを作成する許可を付与	Write			
ExtendQuery [アクセス許可のみ]	VPC 到達可能性クエリを拡張して、呼び出し元のプリンシパルのアカウントを含めるアクセス許可を付与	書き込み			
GetQueryAnswer [アクセス許可のみ]	VPC 到達可能性クエリの回答を取得する許可を付与	Read			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetQueryExplanation [許可のみ]	VPC 到達可能性クエリの説明を取得する許可を付与	読み取り			
GetQueryExtensionAccounts [許可のみ]	新しいクエリで役立つかもしれないアカウントを一覧表示するための許可を付与します	読み取り			

AWS Tiros で定義されるリソースタイプ

AWS Tiros は、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS Tiros へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS Tiros の条件キー

Tiros には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Transcribe のアクション、リソース、および条件キー

Amazon Transcribe (サービスプレフィックス: `transcribe`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Transcribe で定義されるアクション
- Amazon Transcribe で定義されるリソースタイプ
- Amazon Transcribe の条件キー

Amazon Transcribe で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateCallAnalyticsCategory	分析カテゴリを作成する許可を付与。Amazon Transcribe は、分析カテゴリで指定された条件を、通話分析ジョブに適用	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateLanguageModel	新しいカスタム言語モデルを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject s3:ListBucket
CreateMedicalVocabulary	Amazon Transcribe Medical がオーディオファイルの文字起こしの処理方法を変更するた	書き込み		aws:RequestTag/${TagKey}	s3:GetObject

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
	めに使用できる新しいカスタム語彙を作成する許可を付与			aws:ResourceTag/${TagKey} aws:TagKeys	
CreateVocabulary	Amazon Transcribe がオーディオファイルの文字起こしの処理方法を変更するために使用できる新しいカスタム語彙を作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject
CreateVocabularyFilter	アクセス許可を付与して、新しい語彙フィルターを作成します。このフィルターを使用して、Amazon Transcribe によって生成されたオーディオファイルの文字起こしから単語をフィルタリングできます。	書き込み		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject
DeleteCallAnalyticsCategory	Amazon Transcribe からの名前を使用してコール分析カテゴリを削除する許可を付与	書き込み	callanalyticscategory*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteCallAnalyticsJob	以前に送信された文字起こしジョブを、他の生成された結果 (文字起こし、モデルなど) とともに削除する許可を付与	書き込み	callanalyticsjob*		
DeleteLanguageModel	以前に作成したカスタム言語モデルを削除する許可を付与	書き込み	languagemodel*		
DeleteMedicalScribeJob	以前に送信された Medical Scribe ジョブを削除するためのアクセス許可を付与	書き込み	medicalscribejob*		
DeleteMedicalTranscriptionJob	以前に送信された医療文字起こしジョブを削除する許可を付与	書き込み	medicaltranscriptionjob*		
DeleteMedicalVocabulary	Amazon Transcribe から医学語彙を削除する許可を付与	書き込み	medicalvocabulary*		
DeleteTranscriptionJob	以前に送信された文字起こしジョブを、他の生成された結果 (文字起こし、モデルなど) とともに削除する許可を付与	書き込み	transcriptionjob*		
DeleteVocabulary	Amazon Transcribe から語彙を削除する許可を付与	書き込み	vocabulary*		
DeleteVocabularyFilter	Amazon Transcribe から語彙フィルターを削除する許可を付与	書き込み	vocabularyfilter*		
DescribeLanguageModel	カスタム言語モデルに関する情報を返す許可を付与	読み込み	languagemodel*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetCallAnalyticsCategory	コール分析カテゴリに関する情報を取得する許可を付与	読み込み	callanalyticscategory*		
GetCallAnalyticsJob	コール分析ジョブに関する情報を返す許可を付与	読み取り	callanalyticsjob*		
GetMedicalScribeJob	Medical Scribe ジョブに関する情報を返すためのアクセス許可を付与	読み取り	medicalscribejob*		
GetMedicalScribeStream	指定された AWS HealthScribe ストリーミングセッションに関する情報を取得するアクセス許可を付与します	読み取り			
GetMedicalTranscriptionJob	医療文字起こしジョブに関する情報を返す許可を付与	読み込み	medicaltranscriptionjob*		
GetMedicalVocabulary	医学語彙に関する情報を取得する許可を付与	読み込み	medicalvocabulary*		
GetTranscriptionJob	文字起こしジョブに関する情報を返す許可を付与	読み込み	transcriptionjob*		
GetVocabulary	語彙に関する情報を取得する許可を付与	読み込み	vocabulary*		
GetVocabularyFilter	語彙フィルターに関する情報を取得する許可を付与	読み込み	vocabularyfilter*		
ListCallAnalyticsCategories	作成されたコール分析カテゴリを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListCallAnalyticsJobs	指定したステータスのコール分析ジョブを一覧表示する許可を付与	リスト			
ListLanguageModels	カスタム言語モデルを一覧表示する許可を付与	リスト			
ListMedicalScribeJobs	指定したステータスの Medical Scribe ジョブを一覧表示するためのアクセス許可を付与	リスト			
ListMedicalTranscriptionJobs	指定されたステータスの医療文字起こしジョブを一覧表示する許可を付与	リスト			
ListMedicalVocabularies	指定された条件に一致する医学語彙のリストを返すアクセス許可を付与します。条件が指定されなかった場合は、語彙のリスト全体を返す	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み込み			
ListTranscriptionJobs	指定したステータスの文字起こしジョブを一覧表示する許可を付与	リスト			
ListVocabularies	指定した条件に一致する語彙のリストを返すアクセス許可を付与します。条件が指定されなかった場合は、語彙のリスト全体を返す	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListVocabularyFilters	指定した条件に一致する語彙フィルターのリストを返すアクセス許可を付与します。条件を指定しない場合は、最大で 5 つの語彙フィルターを返す	リスト			
StartCallAnalyticsJob	発信者とエージェントの音声録音を書き起こすだけでなく、追加のインサイトを返す非同期分析ジョブを開始する許可を付与	書き込み		transcribe:OutputEncryptionKMSKeyId transcribe:OutputLocation aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
StartCallAnalyticsStreamTranscription	音声が Transcribe Call Analytics にストリーミングされ、文字起こしの結果がアプリケーションにストリーミングされるプロトコルを開始する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartCallAnalyticsStreamTranscriptionWebSocket	音声が Transcribe Call Analytics にストリーミングされ、文字起こしの結果がアプリケーションにストリーミングされる WebSocket を開始する許可を付与	書き込み			
StartMedicalScribeJob	患者と臨床医との会話を書き起こし、クリニカルノートを生成する非同期ジョブを開始するためのアクセス許可を付与	書き込み		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject
StartMedicalScribeStream	音声が AWS HealthScribe にストリーミングされ、文字起こし結果がアプリケーションにストリーミングされる双方向 HTTP2 ストリームを開始するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartMedicalStreamTranscription	音声が Transcribe Medical にストリーミングされ、文字起こしの結果がアプリケーションにストリーミングされるプロトコルを開始する許可を付与	書き込み			
StartMedicalStreamTranscriptionWebSocket	音声が Transcribe Medical にストリーミングされ、文字起こしの結果がアプリケーションにストリーミングされる WebSocket を開始する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartMedicalTranscriptionJob	医療音声をテキストに書き起こす非同期ジョブを開始する許可を付与	書き込み		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject
StartStreamTranscription	双方向の HTTP2 ストリームを開始して、音声をテキストにリアルタイムで書き起こす許可を付与	書き込み			
StartStreamTranscriptionWebSocket	Websocket ストリームを開始して、音声をテキストにリアルタイムで書き起こす許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
StartTranscriptionJob	音声をテキストに書き起こす非同期ジョブを開始する許可を付与	書き込み		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
TagResource	指定されたキーと値のペアでリソースにタグを付けるアクセス許可を付与	タグ付け		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:TagKeys	
UntagResource	指定されたキーでリソースのタグを削除する許可を付与	Tagging		aws:TagKeys	
UpdateCallAnalyticsCategory	コール分析カテゴリを新しい値で更新する許可を付与 UpdateCallAnalyticsCategory オペレーションは、リクエストで指定された値で既存のすべての情報を上書き	書き込み	callanalyticscategory*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateMedicalVocabulary	既存の医学語彙を新しい値で更新する許可を付与。UpdateMedicalVocabulary オペレーションは、リクエストで指定された値で既存のすべての情報を上書き	書き込み	medicalvocabulary*		s3:GetObject
UpdateVocabulary	既存の語彙を新しい値で更新する許可を付与。UpdateVocabulary オペレーションは、リクエストで指定された値で既存のすべての情報を上書き	書き込み	vocabulary*		s3:GetObject
UpdateVocabularyFilter	既存の語彙フィルターを新しい値で更新する許可を付与。UpdateVocabularyFilter オペレーションは、リクエストで指定された値で既存のすべての情報を上書き	書き込み	vocabularyfilter*		s3:GetObject

Amazon Transcribe で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
transcriptionjob	arn:${Partition}:transcribe:${Region}:${Account}:transcription-job/${JobName}	aws:ResourceTag/${TagKey}
vocabulary	arn:${Partition}:transcribe:${Region}:${Account}:vocabulary/${VocabularyName}	aws:ResourceTag/${TagKey}
vocabularyfilter	arn:${Partition}:transcribe:${Region}:${Account}:vocabulary-filter/${VocabularyFilterName}	aws:ResourceTag/${TagKey}
languagemodel	arn:${Partition}:transcribe:${Region}:${Account}:language-model/${ModelName}	aws:ResourceTag/${TagKey}
medicaltranscriptionjob	arn:${Partition}:transcribe:${Region}:${Account}:medical-transcription-job/${JobName}	aws:ResourceTag/${TagKey}
medicalvocabulary	arn:${Partition}:transcribe:${Region}:${Account}:medical-vocabulary/${VocabularyName}	aws:ResourceTag/${TagKey}
callanalyticsjob	arn:${Partition}:transcribe:${Region}:${Account}:analytics/${JobName}	aws:ResourceTag/${TagKey}
callanalyticscategory	arn:${Partition}:transcribe:${Region}:${Account}:analytics-category/${CategoryName}	aws:ResourceTag/${TagKey}
medicalscribejob	arn:${Partition}:transcribe:${Region}:${Account}:medical-scribe-job/${JobName}	aws:ResourceTag/${TagKey}

Amazon Transcribe の条件キー

Amazon Transcribe では、IAM ポリシーの `Condition` 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リソース作成リクエストに含まれるタグ値を要求することで、アクセスをフィルタします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値を要求することで、アクセスをフィルタリングします	String
aws:TagKeys	リクエストに必須タグの存在を要求することで、アクセスをフィルタリングします	ArrayOfString
transcribe:OutputBucketName	リクエストに含まれる出力バケット名に基づいてアクセスをフィルタリングします	文字列
transcribe:OutputEncryptionKMSKeyId	リクエストに含まれる KMS キー ID に基づいてアクセスをフィルタリングします	文字列
transcribe:OutputKey	リクエストに含まれる出力キーに基づいてアクセスをフィルタリングします	String
transcribe:OutputLocation	リクエストに含まれる出力場所に基づいてアクセスをフィルタリングします	String

AWS Transfer Family のアクション、リソース、および条件キー

AWS Transfer Family (サービスプレフィックス: `transfer`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Transfer Family で定義されるアクション
- AWS Transfer Family で定義されるリソースタイプ
- AWS Transfer Family の条件キー

AWS Transfer Family で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴

うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateAccess	サーバーに関連付けられたアクセスを追加するためのアクセス許可を付与	書き込み	server*		iam:PassRole
CreateAgreement	サーバーに関連付けられた契約を追加する許可を付与	書き込み	server*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateConnector	コネクタを作成する許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole
CreateProfile	プロファイルを作成する許可の付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateServer	サーバーを作成する許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole
CreateUser	サーバーに関連付けられたユーザーを追加する許可を付与	書き込み	server*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateWebApp	ウェブアプリケーションを作成するアクセス許可を付与します	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole
CreateWorkflow	ワークフローを作成する許可を付与。	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteAccess	アクセスを削除するための許可を付与	書き込み	server*		
DeleteAgreement	契約を削除する許可を付与	書き込み	agreement*		
DeleteCertificate	証明書を削除する許可を付与	書き込み	certificate*		
DeleteConnector	コネクタを削除する許可を付与	書き込み	connector*		
DeleteHostKey	サーバーに関連付けられたホストキーを削除するアクセス許可を付与	書き込み	host-key*		
DeleteProfile	プロファイルを削除する許可を付与	書き込み	profile*		
DeleteServer	サーバーを削除する許可を付与	書き込み	server*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteSshPublicKey	ユーザーから SSH 公開鍵を削除する許可を付与	書き込み	user*		
DeleteUser	サーバーに関連付けられたユーザーを削除する許可を付与	書き込み	user*		
DeleteWebApp	ウェブアプリを削除するアクセス許可を付与します	書き込み	webapp*		
DeleteWebAppCustomization	ウェブアプリのカスタマイズを削除するアクセス許可を付与します	書き込み	webapp*		
DeleteWorkflow	ワークフローを削除するアクセス許可を与えます。	書き込み	workflow*		
DescribeAccess	サーバに関連付けられたアクセスを詳細表示するためのアクセス許可を付与	読み取り	server*		
DescribeAgreement	サーバに関連付けられた契約を詳細表示する許可を付与	読み取り	agreement*		
DescribeCertificate	証明書を記述する許可を付与	読み取り	certificate*		
DescribeConnector	コネクタを記述する許可を付与	読み取り	connector*		
DescribeExecution	ワークフローに関連付けられた実行について詳細表示するためのアクセス許可を付与	読み取り	workflow*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeHostKey	サーバーに関連付けられたホストキーを記述するアクセス許可を付与	読み取り	host-key*		
DescribeProfile	プロファイルを記述する許可を付与	読み取り	profile*		
DescribeSecurityPolicy	セキュリティポリシーを記述する許可を付与	読み込み			
DescribeServer	サーバーを記述する許可を付与	読み込み	server*		
DescribeUser	サーバに関連付けられたユーザーを記述する許可を付与	読み取り	user*		
DescribeWebApp	ウェブアプリを記述するアクセス許可を付与します	読み取り	webapp*		
DescribeWebAppCustomization	ウェブアプリのカスタマイズを記述するアクセス許可を付与します	読み取り	webapp*		
DescribeWorkflow	ワークフローを詳細表示するためのアクセス許可を付与	読み取り	workflow*		
ImportCertificate	証明書を追加する許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
ImportHostKey	ホストキーをサーバーに追加するアクセス許可を付与	書き込み	server*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey}	
ImportSshPublicKey	SSH 公開鍵をユーザーに追加する許可を付与	書き込み	user*		
ListAccesses	アクセスを一覧表示するための許可を付与	読み取り	server*		
ListAgreements	契約を一覧表示する許可を付与	読み取り	server*		
ListCertificates	証明書を一覧表示する許可を付与	読み取り			
ListConnectors	コネクタを一覧表示する許可を付与	読み取り			
ListExecutions	ワークフローに関連付けられている実行を一覧表示するためのアクセス許可を付与	読み取り	workflow*		
ListFileTransferResults	コネクタのファイル転送ステータスを一覧表示する許可を付与する	読み取り	connector*		
ListHostKeys	サーバーに関連付けられたホストキーを一覧表示するアクセス許可を付与	読み取り	server*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListProfiles	プロファイルを一覧表示する許可の付与	読み取り			
ListSecurityPolicies	セキュリティポリシーを一覧表示する許可を付与	リスト			
ListServers	サーバーを一覧表示する許可を付与	リスト			
ListTagsForResource	AWS Transfer Family リソースのタグを一覧表示する許可を付与	読み取り	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		
			user		
			workflow		
ListUsers	サーバに関連付けられたユーザーを一覧表示する許可を付与	リスト	server*		
ListWebApps	ウェブアプリを一覧表示するアクセス許可を付与します	リスト			
ListWorkflows	ワークフローを一覧表示するためのアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
SendWorkflowStepState	非同期カスタムステップ向けにコールバックを送信するためのアクセス許可を付与	書き込み	workflow*		
StartDirectoryListing	コネクタを使用してリモートサーバーでリスト操作を開始する許可を付与する	書き込み	connector*		
StartFileTransfer	コネクタのファイル転送を開始するアクセス許可を付与	書き込み	connector*		
StartRemoteDelete	リモートサーバーでコネクタ削除オペレーションを開始するアクセス許可を付与します	書き込み	connector*		
StartRemoteMove	リモートサーバーでコネクタ移動オペレーションを開始するアクセス許可を付与します	書き込み	connector*		
StartServer	サーバーを開始する許可を付与	書き込み	server*		
StopServer	サーバーを停止する許可を付与	書き込み	server*		
TagResource	AWS Transfer Family リソースにタグを付けるアクセス許可を付与します	Tagging	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			user		
			webapp		
			workflow		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestConnection	リモートサーバーに対するコネクタの接続をテストするための許可を付与します	書き込み	connector*		
TestIdentityProvider	サーバーのカスタム ID プロバイダーをテストする許可を付与	読み取り	user*		
UntagResource	AWS Transfer Family リソースのタグを解除する許可を付与	Tagging	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		
			user		
			webapp		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			workflow		
				aws:TagKeys	
UpdateAccess	アクセスを更新するための許可を付与	書き込み			iam:PassRole
UpdateAgreement	契約を更新する許可を付与	書き込み	agreement*		iam:PassRole
UpdateCertificate	証明書を更新する許可を付与	書き込み	certificate*		
UpdateConnector	コネクタを更新する許可を付与	書き込み	connector*		iam:PassRole
UpdateHostKey	ホストキーを更新するアクセス許可を付与	書き込み	host-key*		
UpdateProfile	プロファイルを更新する許可の付与	書き込み	profile*		
UpdateServer	サーバーの構成を更新する許可を付与	書き込み	server*		iam:PassRole
UpdateUser	ユーザーの構成を更新する許可を付与	書き込み	user*		iam:PassRole
UpdateWebApp	ウェブアプリの設定を更新するアクセス許可を付与します	書き込み	webapp*		iam:PassRole
UpdateWebAppCustomization	ウェブアプリカットマイゼーションの設定を更新するアクセス許可を付与します	書き込み	webapp*		iam:PassRole

AWS Transfer Family で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
user	arn:${Partition}:transfer:${Region}:${Account}:user/${ServerId}/${UserName}	aws:ResourceTag/${TagKey}
server	arn:${Partition}:transfer:${Region}:${Account}:server/${ServerId}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:transfer:${Region}:${Account}:workflow/${WorkflowId}	aws:ResourceTag/${TagKey}
certificate	arn:${Partition}:transfer:${Region}:${Account}:certificate/${CertificateId}	aws:ResourceTag/${TagKey}
connector	arn:${Partition}:transfer:${Region}:${Account}:connector/${ConnectorId}	aws:ResourceTag/${TagKey}
profile	arn:${Partition}:transfer:${Region}:${Account}:profile/${ProfileId}	aws:ResourceTag/${TagKey}
agreement	arn:${Partition}:transfer:${Region}:${Account}:agreement/${ServerId}/${AgreementId}	aws:ResourceTag/${TagKey}
host-key	arn:${Partition}:transfer:${Region}:${Account}:host-key/${ServerId}/${HostKeyId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
webapp	arn:${Partition}:transfer:${Region}:${Account}:webapp/${WebAppId}	aws:ResourceTag/${TagKey}

AWS Transfer Family の条件キー

AWS Transfer Family は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS Transform のアクション、リソース、および条件キー

AWS Transform (サービスプレフィックス: transform) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Transform で定義されるアクション
- AWS Transform で定義されるリソースタイプ
- AWS 変換の条件キー

AWS Transform で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateConnectorResource [アクセス許可のみ]	AWS 変換時に AssociateConnectorResource を呼び出すアクセス許可を付与します	書き込み			
CreateProfile [アクセス許可のみ]	AWS 変換時に CreateProfile を呼び出すアクセス許可を付与します	書き込み	profile*		
DeleteProfile [アクセス許可のみ]	AWS 変換時に DeleteProfile を呼び出すアクセス許可を付与します	書き込み	profile*		
GetConnector [アクセス許可のみ]	AWS 変換時に GetConnector を呼び出すアクセス許可を付与します	読み取り			
ListProfiles [許可のみ]	AWS 変換時に ListProfiles を呼び出すアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RejectConnector [許可のみ]	AWS 変換時に RejectConnector を呼び出すアクセス許可を付与します	書き込み			
UpdateProfile [アクセス許可のみ]	AWS 変換時に UpdateProfile を呼び出すアクセス許可を付与します	書き込み	profile*		

AWS Transform で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
profile	`arn:${Partition}:transform:${Region}:${Account}:profile/${Identifier}`	

AWS 変換の条件キー

Transform には、ポリシーステートメントの Condition要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Translate のアクション、リソース、および条件キー

Amazon Translate (サービスプレフィックス: translate) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Translate で定義されるアクション
- Amazon Translate で定義されるリソースタイプ
- Amazon Translate の条件キー

Amazon Translate で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateParallelData	並列データを作成するアクセス許可を付与	Write	parallel-data		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteParallelData	並列データを作成する削除を付与	Write	parallel-data		
DeleteTerminology	用語を削除するアクセス許可を付与	Write	terminology		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeTextTranslationJob	非同期バッチ変換ジョブに関連付けられたプロパティを取得するアクセス許可を付与	Read			
GetParallelData	並列データを取得するアクセス許可を付与	Read	parallel-data		
GetTerminology	用語を取得する許可を付与	Read	terminology		
ImportTerminology	指定された用語名ですでに存在するかどうかに応じて、用語を作成または更新するアクセス許可を付与	書き込み	terminology		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListLanguages	サポートされている言語を一覧表示するアクセス許可を付与	リスト			
ListParallelData	アカウントに関連付けられた並列データを一覧表示するアクセス許可を付与	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り	parallel-data		
			terminology		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTerminologies	アカウントに関連付けられた用語を一覧表示するアクセス許可を付与	リスト			
ListTextTranslationJobs	送信したバッチ変換ジョブを一覧表示するアクセス許可を付与	リスト			
StartTextTranslationJob	非同期バッチ変換ジョブを開始するアクセス許可を付与 バッチ翻訳ジョブを使用すると、複数のドキュメントにまたがって大量のテキストを一度に翻訳できます	Write	parallel-data		
			terminology		
StopTextTranslationJob	進行中の非同期バッチ翻訳ジョブを停止するアクセス許可を付与	書き込み			
TagResource	指定されたキーと値のペアでリソースにタグを付けるアクセス許可を付与	Tagging	parallel-data		
			terminology		
				aws:RequestTag/${TagKey} aws:TagKeys	
TranslateDocument	ドキュメントをソース言語からターゲット言語に翻訳する許可を付与	読み取り	terminology		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TranslateText	テキストを原文言語から訳文言語に翻訳するアクセス許可を付与	読み取り	parallel-data		
			terminology		
UntagResource	指定されたキーでリソースのタグを削除する許可を付与	Tagging	parallel-data		
			terminology		
				aws:TagKeys	
UpdateParallelData	既存の並列データを更新するアクセス許可を付与	Write	parallel-data		

Amazon Translate で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
terminology	arn:${Partition}:translate:${Region}:${Account}:terminology/${ResourceName}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
parallel-data	arn:${Partition}:translate:${Region}:${Account}:parallel-data/${ResourceName}	aws:ResourceTag/${TagKey}

Amazon Translate の条件キー

Amazon Translate は、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リソース作成リクエストに含まれるタグ値を要求することで、アクセスをフィルタします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値を要求することで、アクセスをフィルタリングします	String
aws:TagKeys	リクエストに必須タグの存在を要求することで、アクセスをフィルタリングします	ArrayOfString

AWS Trusted Advisor のアクション、リソース、および条件キー

AWS Trusted Advisor (サービスプレフィックス: trustedadvisor) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Trusted Advisor で定義されるアクション
- AWS Trusted Advisor で定義されるリソースタイプ
- AWS Trusted Advisor の条件キー

AWS Trusted Advisor で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

> **Note**
>
> IAM Trusted Advisor ポリシーの説明の詳細は、Trusted Advisor コンソールにのみ適用されます。Trusted Advisor へのプログラムによるアクセスを管理する場合は、 AWS サポート API の Trusted Advisor オペレーションを使用します。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchUpdateRecommendationResourceExclusion	レコメンデーションリソースのリストの 1 つ以上の除外ステータスを更新する許可を付与する	書き込み			
CreateEngagement	エンゲージメントを作成する許可を付与	書き込み			
CreateEngagementAttachment	エンゲージメントアタッチメントを作成する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateEngagementCommunication	エンゲージメントコミュニケーションを作成する許可を付与	書き込み			
DeleteNotificationConfigurationForDelegatedAdmin	Trusted Advisor Priority の委任された管理者アカウントから E メール通知設定を削除するアクセス許可を組織管理アカウントに付与	書き込み			
DescribeAccount [アクセス許可のみ]	AWS サポート プランとさまざまな AWS Trusted Advisor の設定を表示するアクセス許可を付与します	読み取り			
DescribeAccountAccess [許可のみ]	AWS アカウント が AWS Trusted Advisor を有効または無効にしているかどうかを表示するアクセス許可を付与します	読み取り			
DescribeCheckItems	チェックアイテムの詳細を表示する許可を付与	読み取り	checks*		
DescribeCheckRefreshStatuses	AWS Trusted Advisor チェックの更新ステータスを表示するアクセス許可を付与します	読み取り	checks*		
DescribeCheckStatusHistoryChanges [許可のみ]	過去 30 日間のチェックの結果と変更されたステータスを表示する許可を付与	読み取り	checks*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeCheckSummaries	AWS Trusted Advisor チェックの概要を表示するアクセス許可を付与します	読み取り	checks*		
DescribeChecks	AWS Trusted Advisor チェックの詳細を表示するアクセス許可を付与します	読み取り			
DescribeNotificationConfigurations	Trusted Advisor Priority の E メール通知設定を取得するアクセス許可を付与	読み取り			
DescribeNotificationPreferences [許可のみ]	の通知設定を表示するアクセス許可を付与します AWS アカウント	読み取り			
DescribeOrganization [許可のみ]	が組織ビュー機能を有効にする AWS アカウント 要件を満たしているかどうかを表示するアクセス許可を付与します	読み取り			
DescribeOrganizationAccounts [許可のみ]	組織内のリンクされた AWS アカウントを表示するアクセス許可を付与します	読み取り			
DescribeReports [許可のみ]	レポート名、実行時、作成日、ステータス、形式など、組織ビューレポートの詳細を表示する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeRisk	AWS Trusted Advisor Priority でリスクの詳細を表示するアクセス許可を付与します	読み取り			
DescribeRiskResources	AWS Trusted Advisor Priority でリスクの影響を受けるリソースを表示するアクセス許可を付与します	読み取り			
DescribeRisks	AWS Trusted Advisor Priority でリスクを表示するアクセス許可を付与します	読み取り			
DescribeServiceMetadata [許可のみ]	、チェックカテゴリ、チェック名 AWS リージョン、リソースステータスなど、組織ビューレポートに関する情報を表示するアクセス許可を付与します	読み取り			
DownloadRisk	AWS Trusted Advisor Priority のリスクに関する詳細を含むファイルをダウンロードするアクセス許可を付与します	読み取り			
ExcludeCheckItems [許可のみ]	AWS Trusted Advisor チェックのレコメンデーションを除外する許可を付与	書き込み	checks*		
GenerateReport [アクセス許可のみ]	組織内の AWS Trusted Advisorチェックのレポートを作成するアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetEngagement	エンゲージメントを表示する許可を付与	読み取り			
GetEngagementAttachment	エンゲージメントのアタッチメントを表示する許可を付与	読み取り			
GetEngagementType	特定のエンゲージメントタイプを表示する許可を付与	読み取り			
GetOrganizationRecommendation	AWS 組織の組織内で特定のレコメンデーションを取得するアクセス許可を付与します。この API は、優先順位を付けた推奨事項のみをサポートします。	読み取り			
GetRecommendation	特定の推奨事項を取得する許可を付与	読み取り			
IncludeCheckItems [許可のみ]	AWS Trusted Advisor チェックのレコメンデーションを含めるアクセス許可を付与します	書き込み	checks*		
ListAccountsForParent [アクセス許可のみ]	Trusted Advisor コンソールで、ルートまたは組織単位 (OU) に含まれる AWS 組織内のすべてのアカウントを表示するアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListChecks	フィルター可能なチェックセットを一覧表示する許可を付与	リスト			
ListEngagementCommunications	エンゲージメントに対するすべてのコミュニケーションを表示する許可を付与	読み取り			
ListEngagementTypes	すべてのエンゲージメントタイプを表示する許可を付与	読み取り			
ListEngagements	すべてのエンゲージメントを表示する許可を付与	読み取り			
ListOrganizationRecommendationAccounts	AWS Organization 集計レコメンデーションのリソースを所有するアカウントを一覧表示するアクセス許可を付与します。この API は優先順位付けされた奨励事項のみをサポートします。	リスト			
ListOrganizationRecommendationResources	AWS 組織内のレコメンデーションのリソースを一覧表示するアクセス許可を付与します。この API は優先順位付けされた奨励事項のみをサポートします。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListOrganizationRecommendations	AWS 組織内のフィルタリング可能な推奨事項のセットを一覧表示するアクセス許可を付与します。この API は優先順位付けされた奨励事項のみをサポートします。	リスト			
ListOrganizationalUnitsForParent [許可のみ]	親組織単位またはルート内のすべての組織単位 (OU)Trusted Advisor コンソールで表示する許可を付与	読み取り			
ListRecommendationResources	リソースに対する推奨事項を取得する許可を付与	リスト			
ListRecommendations	フィルター可能な推奨事項を一覧表示する許可を付与	リスト			
ListRoots [許可のみ]	Trusted Advisor コンソールで、 AWS 組織で定義されているすべてのルートを表示するアクセス許可を付与します	読み取り			
RefreshCheck	AWS Trusted Advisor チェックを更新する許可を付与	書き込み	checks*		
SetAccountAccess [アクセス許可のみ]	アカウントの AWS Trusted Advisorを有効または無効にするアクセス許可を付与します	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
SetOrganizationAccess [アクセス許可のみ]	AWS Trusted Advisor の組織ビュー機能を有効にするアクセス許可を付与します	書き込み			
UpdateEngagement	エージェントの詳細を更新する許可を付与	書き込み			
UpdateEngagementStatus	エージェントのステータスを更新する許可を付与	書き込み			
UpdateNotificationConfigurations	Trusted Advisor Priority の E メール通知設定を作成または更新するアクセス許可を付与	書き込み			
UpdateNotificationPreferences [アクセス許可のみ]	AWS Trusted Advisor の通知設定を更新する許可を付与	書き込み			
UpdateOrganizationRecommendationLifecycle	AWS 組織内のレコメンデーションのライフサイクルを更新するアクセス許可を付与します。この API は優先順位付けされた奨励事項のみをサポートします。	書き込み			
UpdateRecommendationLifecycle	奨励事項のライフサイクルを更新する許可を付与 この API は優先順位付けされた奨励事項のみをサポートします。	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateRiskStatus	AWS Trusted Advisor Priority でリスクステータスを更新する許可を付与	書き込み			

AWS Trusted Advisor で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

> **Note**
>
> チェックリソースタイプの ARN にはリージョンを含めないでください。フォーマットでは、「${Region}」の代わりに「*」を使用してください。それ以外の場合、ポリシーは正しく機能しません。

リソースタイプ	ARN	条件キー
checks	`arn:${Partition}:trustedadvisor:${Region}:${Account}:checks/${CategoryCode}/${CheckId}`	

AWS Trusted Advisor の条件キー

Trusted Advisor には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS ユーザー通知のアクション、リソース、および条件キー

AWS ユーザー通知 (サービスプレフィックス: notifications) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS ユーザー通知で定義されるアクション
- AWS ユーザー通知によって定義されるリソースタイプ
- AWS ユーザー通知の条件キー

AWS ユーザー通知で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateChannel	特定の NotificationConfiguration と新しいチャネルを関連付けるためのアクセス許可を付与します	書き込み	NotificationConfiguration*		
AssociateManagedNotificationAccountContact	アカウント連絡先を特定の Managed Notification Configuration に関連付けるアクセス許可を付与します	書き込み	ManagedNotificationConfiguration*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateManagedNotificationAdditionalChannel	チャネルを特定のマネージド通知設定に関連付けるアクセス許可を付与します	書き込み	ManagedNotificationConfiguration*		
CreateEventRule	新しい EventRule を作成し、それを NotificationConfiguration に関連付けるアクセス許可を付与します	書き込み			
CreateNotificationConfiguration	NotificationConfiguration を作成するアクセス許可を付与します	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteEventRule	EventRule を削除するアクセス許可を付与します	書き込み	EventRule*		
DeleteNotificationConfiguration	NotificationConfiguration を削除するアクセス許可を付与します	書き込み	NotificationConfiguration*		
DeregisterNotificationHub	NotificationHub を登録解除するアクセス許可を付与します	書き込み			
DisableNotificationsAccessForOrganization	AWS ユーザー通知のサービス信頼を無効にするアクセス許可を付与します	書き込み			organizations:DisableAWSServiceAccess

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisassociateChannel	NotificationConfiguration からチャネルを削除するアクセス許可を付与します	書き込み	NotificationConfiguration*		
DisassociateManagedNotificationAccountContact	マネージド通知設定からアカウント連絡先を削除するアクセス許可を付与します	書き込み	ManagedNotificationConfiguration*		
DisassociateManagedNotificationAdditionalChannel	マネージド通知設定からチャネルを削除するアクセス許可を付与します	書き込み	ManagedNotificationConfiguration*		
EnableNotificationsAccessForOrganization	AWS ユーザー通知のサービストラストを有効にするアクセス許可を付与します	書き込み			iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess
GetEventRule	EventRule を取得するアクセス許可を付与します	読み取り	EventRule*		
GetFeatureOptInStatus [許可のみ]	AWS ユーザー通知サービス機能のオプトインステータスを読み取るアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetManagedNotificationChildEvent	マネージド通知の子イベントを取得するアクセス許可を付与します	読み取り	ManagedNotificationChildEvent*		
GetManagedNotificationConfiguration	マネージド通知設定を取得するアクセス許可を付与します	読み取り	ManagedNotificationConfiguration*		
GetManagedNotificationEvent	Managed NotificationEvent を取得する許可を付与	読み取り	ManagedNotificationEvent*		
GetNotificationConfiguration	NotificationConfiguration を取得するアクセス許可を付与します	読み取り	NotificationConfiguration*		
GetNotificationEvent	NotificationEvent を取得するアクセス許可を付与します	読み取り	NotificationEvent*		
GetNotificationsAccessForOrganization	AWS ユーザー通知のサービストラストを読み取るアクセス許可を付与します	読み取り			
ListChannels	NotificationConfiguration でチャネルを一覧表示するアクセス許可を付与します	リスト	NotificationConfiguration*		
ListEventRules	EventRule を一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListManagedNotificationChannelAssociations	マネージド通知設定に関連付けられたアカウントの連絡先とチャネルを一覧表示するアクセス許可を付与します	リスト	ManagedNotificationConfiguration*		
ListManagedNotificationChildEvents	マネージド通知の子イベントを一覧表示するアクセス許可を付与します	リスト			
ListManagedNotificationConfigurations	マネージド通知設定を一覧表示するアクセス許可を付与します	リスト			
ListManagedNotificationEvents	マネージド通知イベントを一覧表示するアクセス許可を付与します	リスト			
ListNotificationConfigurations	NotificationConfiguration を一覧表示するアクセス許可を付与します	リスト			
ListNotificationEvents	NotificationEvent を一覧表示するアクセス許可を付与します	リスト			
ListNotificationHubs	NotificationHub を一覧表示するアクセス許可を付与します	リスト			
ListTagsForResource	リソースのタグを取得するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
PutFeatureOptInStatus [許可のみ]	AWS ユーザー通知サービス機能のオプトインステータスを更新する許可を付与	書き込み			
RegisterNotificationHub	NotificationHub を登録するアクセス許可を付与します	書き込み			
TagResource	リソースにタグを付けるアクセス許可を付与	Tagging	NotificationConfiguration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	リソースからタグを削除する許可を付与	Tagging	NotificationConfiguration*		
				aws:TagKeys	
UpdateEventRule	EventRule を更新するアクセス許可を付与します	書き込み	EventRule*		
UpdateNotificationConfiguration	NotificationConfiguration を更新するアクセス許可を付与します	書き込み	NotificationConfiguration*		

AWS ユーザー通知によって定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
EventRule	arn:${Partition}:notifications::${Account}:configuration/${NotificationConfigurationId}/rule/${EventRuleId}	
NotificationConfiguration	arn:${Partition}:notifications::${Account}:configuration/${NotificationConfigurationId}	aws:ResourceTag/${TagKey}
NotificationEvent	arn:${Partition}:notifications:${Region}:${Account}:configuration/${NotificationConfigurationId}/event/${NotificationEventId}	
ManagedNotificationChildEvent	arn:${Partition}:notifications::${Account}:managed-notification-configuration/category/${Category}/sub-category/${Subcategory}/event/${NotificationEventId}/child-event/${NotificationChildEventId}	
ManagedNotificationConfiguration	arn:${Partition}:notifications::${Account}:managed-notification-configuration/category/${Category}/sub-category/${Subcategory}	

リソースタイプ	ARN	条件キー
ManagedNotificationEvent	arn:${Partition}:notifications::${Account}:managed-notification-configuration/category/${Category}/sub-category/${Subcategory}/event/${NotificationEventId}	

AWS ユーザー通知の条件キー

AWS ユーザー通知では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS ユーザー通知のアクション、リソース、および条件キー

AWS ユーザー通知連絡先 (サービスプレフィックス: notifications-contacts) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS ユーザー通知連絡先で定義されるアクション
- AWS ユーザー通知連絡先で定義されるリソースタイプ
- AWS ユーザー通知連絡先の条件キー

AWS ユーザー通知連絡先で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ActivateEmailContact	提供されたコードが有効であれば、指定した ARN に関連付けられた E メール連絡先を有効にするアクセス許可を付与します	書き込み	EmailContactResource*		
CreateEmailContact	E メール連絡先を作成するアクセス許可を付与します	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteEmailContact	特定のARNに関連付けられている E メール連絡先を削除するアクセス許可を付与します	書き込み	EmailContactResource*		
GetEmailContact	特定のARNに関連付けられている E メール連絡先を取得するアクセス許可を付与します	読み取り	EmailContactResource*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListEmailContacts	E メール連絡先を一覧表示するアクセス許可を付与します	リスト			
ListTagsForResource	リソースのタグを取得するアクセス許可を付与します	読み取り			
SendActivationCode	指定された ARN に関連付けられた E メールにアクティベーションリンクを送信するアクセス許可を付与します	書き込み	EmailContactResource*		
TagResource	リソースにタグを付けるアクセス許可を付与	Tagging	EmailContactResource*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	リソースからタグを削除する許可を付与	Tagging	EmailContactResource*		
				aws:TagKeys	

AWS ユーザー通知連絡先で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることがで

きる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
EmailContactResource	arn:${Partition}:notifications-contacts::${Account}:emailcontact/${EmailContactId}	aws:ResourceTag/${TagKey}

AWS ユーザー通知連絡先の条件キー

AWS ユーザー通知問い合わせでは、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS User Subscriptions のアクション、リソース、および条件キー

AWS ユーザーサブスクリプション (サービスプレフィックス: user-subscriptions) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS User Subscriptions で定義されるアクション
- AWS User Subscriptions で定義されるリソースタイプ
- AWS User Subscription の条件キー

AWS User Subscriptions で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateClaim	User Subscription クレームを作成する許可を付与する	書き込み		user-subscriptions:CreateForSelf	
DeleteClaim	User Subscription クレームを削除する許可を付与する	書き込み			
ListApplicationClaims	アプリケーションのすべての User Subscription クレームを一覧表示する許可を付与する	リスト			
ListClaims	すべての User Subscription クレームを一覧表示する許可を付与する	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListUserSubscriptions	すべての User Subscription を一覧表示する許可を付与する	リスト			
UpdateClaim	User Subscription クレームを更新する許可を付与する	書き込み			

AWS User Subscriptions で定義されるリソースタイプ

AWS ユーザーサブスクリプションは、IAM ポリシーステートメントの `Resource`要素でのリソース ARN の指定をサポートしていません。 AWS User Subscriptions へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

AWS User Subscription の条件キー

AWS ユーザーサブスクリプションでは、IAM ポリシーの `Condition`要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
user-subscriptions:CreateForSelf	発信者のユーザーサブスクリプションクレームの作成のみを許可してアクセスをフィルタリングします	Bool

AWS Verified Access のアクション、リソース、および条件キー

AWS Verified Access (サービスプレフィックス: `verified-access`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Verified Access で定義されるアクション
- AWS Verified Access で定義されるリソースタイプ
- AWS Verified Access の条件キー

AWS Verified Access で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須と

して示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AllowVerifiedAccess [アクセス許可のみ]	Verified Access インスタンスを作成する許可を付与	書き込み			

AWS Verified Access で定義されるリソースタイプ

AWS Verified Access は、IAM ポリシーステートメントの Resource要素でのリソース ARN の指定をサポートしていません。 AWS Verified Access へのアクセスを許可するには、ポリシーで "Resource": "*" を指定します。

AWS Verified Access の条件キー

Verified Access には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Verified Permissions のアクション、リソース、条件キー

Amazon Verified Permissions (サービスプレフィックス: `verifiedpermissions`) には、IAM アクセス許可ポリシーで使用できるように、次のサービス固有のリソース、アクション、および条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon Verified Permissions で定義されるアクション
- Amazon Verified Permissions によって定義されるリソースタイプ
- Amazon Verified Permissions の条件キー

Amazon Verified Permissions で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateIdentitySource	Amazon Cognito などの OpenID Connect (OIDC) 認証プロトコルと互換性のある、外部の ID プロバイダー (IdP) へのリファレンスを作成する許可を付与	書き込み	policy-store*		
CreatePolicy	Cedar ポリシーを作成し、指定されたポリシーストアに保存する許可を付与	書き込み	policy-store*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreatePolicyStore	Cedar ポリシーを作成し、指定されたポリシーストアに保存する許可を付与	書き込み		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreatePolicyTemplate	ポリシーテンプレートを作成する許可を付与	書き込み	policy-store*		
DeleteIdentitySource	Amazon Cognito などの ID プロバイダー (IdP) を参照するアイデンティティソースを削除する許可を付与	書き込み	policy-store*		
DeletePolicy	指定されたポリシーをポリシーストアから削除する許可を付与	書き込み	policy-store*		
DeletePolicyStore	指定されたポリシーストアを削除する許可を付与	書き込み	policy-store*		
DeletePolicyTemplate	指定されたポリシーテンプレートをポリシーストアから削除する許可を付与	書き込み	policy-store*		
GetIdentitySource	指定されたアイデンティティソースに関する詳細を取得する許可を付与	読み取り	policy-store*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetPolicy	指定されたポリシーに関する情報を取得する許可を付与	読み取り	policy-store*		
GetPolicyStore	ポリシーストアに関する詳細を取得する許可を付与	読み取り	policy-store*		verifiedpermissions:ListTagsForResource
GetPolicyTemplate	指定されたポリシーストアで、指定されたポリシーテンプレートの詳細を取得する許可を付与	読み取り	policy-store*		
GetSchema	指定されたポリシーストアで、指定されたスキーマの詳細を取得する許可を付与	読み取り	policy-store*		
IsAuthorized	パラメータに記述されたサービスリクエストについて承認の決定を行う許可を付与	読み取り	policy-store*		
IsAuthorizedWithToken	パラメータに記述されたサービスリクエストについて承認の決定を行う許可を付与します。このリクエストのプリンシパルは外部のアイデンティティソースから取得されます	読み取り	policy-store*		
ListIdentitySources	指定されたポリシーストアで定義されているすべての IDソースのページ分割されたリストを返す許可を付与	リスト	policy-store*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListPolicies	指定されたポリシーストアに保存されているすべてのポリシーのページ分割されたリストを返す許可を付与	リスト	policy-store*		
ListPolicyStores	呼び出し元のAmazon Web Servicesアカウントのページ分割されたリストを返す許可を付与	リスト			
ListPolicyTemplates	指定されたポリシーストアのすべてのポリシーテンプレートのページ分割されたリストを返す許可を付与	リスト	policy-store*		
ListTagsForResource	指定されたポリシーストアのリソースタグのリストを表示するアクセス許可を付与します	読み取り	policy-store*		
PutSchema	指定されたポリシーストアでポリシースキーマを作成または更新する許可を付与	書き込み	policy-store*		
TagResource	指定されたポリシーストアにタグを追加するアクセス許可を付与します	Tagging	policy-store*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UntagResource	指定されたポリシーストアからタグを削除するアクセス許可を付与します	Tagging	policy-store*		
				aws:TagKeys	
UpdateIdentitySource	指定されたアイデンティティソースを更新して新しい ID プロバイダー (IdP) ソースを使用できるようにするか、IdP から別のプリンシパルエンティティのタイプへのアイデンティティのマッピングを変更する許可を付与	書き込み	policy-store*		
UpdatePolicy	指定されたポリシーストアで、指定された Cedar の静的ポリシーを変更する許可を付与	書き込み	policy-store*		
UpdatePolicyStore	ポリシーストアの検証設定を変更する許可を付与	書き込み	policy-store*		
UpdatePolicyTemplate	指定されたポリシーテンプレートを更新する許可を付与	書き込み	policy-store*		

Amazon Verified Permissions によって定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
policy-store	arn:${Partition}:verifiedpermissions::${Account}:policy-store/${PolicyStoreId}	aws:ResourceTag/${TagKey}

Amazon Verified Permissions の条件キー

Amazon Verified Permissions では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで許可されているタグキーと値のペアによってアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	タグキーとリソースの値のペアによってアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで許可されているタグキーのリストによってアクセスをフィルタリングします	ArrayOfString

Amazon VPC Lattice のアクション、リソース、および条件キー

Amazon VPC Lattice (サービスプレフィックス: vpc-lattice) では、IAM 許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。

- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon VPC Lattice で定義されたアクション
- Amazon VPC Lattice で定義されるリソースタイプ
- Amazon VPC Lattice の条件キー

Amazon VPC Lattice で定義されたアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateViaAWSService [アクセス許可のみ]	AWS サービスマネージドネットワークを介してリソース設定を関連付ける許可を付与	権限の管理			
AssociateViaAWSService-EventsAndStates [許可のみ]	Amazon EventBridge および AWS Step Functions サービスネットワークを介してリソース設定を関連付ける許可を付与	権限の管理			
CreateAccessLogSubscription	アクセスログサブスクリプションを作成する許可を付与	書き込み	AccessLogSubscription*		logs:CreateLogDelivery logs:GetLogDelivery

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			ResourceConfiguration		
			Service		
			ServiceNetwork		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateListener	リスナーを作成する許可を付与	書き込み	Listener*		
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:Protocol vpc-lattice:TargetGroupArns	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateResourceConfiguration	リソース設定を作成するアクセス許可を付与します	書き込み	ResourceConfiguration		
			ResourceGateway		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResourceGateway	リソースゲートウェイを作成するアクセス許可を付与します	書き込み	ResourceGateway*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:VpcId	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateRule	ルールを作成する許可を付与	書き込み	Rule*		
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:TargetGroupArns	
CreateService	サービスを作成する許可を付与	書き込み	Service*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:AuthType	
CreateServiceNetwork	サービスネットワークを作成する許可を付与	書き込み	ServiceNetwork*		iam:CreateServiceLinkedRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:AuthType	
CreateServiceNetworkResourceAssociation	サービスネットワークとリソース間の関連付けを作成するアクセス許可を付与します	書き込み	ResourceConfiguration*		
			ServiceNetwork*		
			ServiceNetworkResourceAssociation*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:ResourceConfigurationArn vpc-lattice:ServiceNetworkArn	
CreateServiceNetworkServiceAssociation	サービスネットワークとサービスアソシエーションを作成する許可を付与	書き込み	Service*		
			ServiceNetwork*		
			ServiceNetworkServiceAssociation*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn	
CreateServiceNetworkVpcAssociation	サービスネットワークと VPC アソシエーションを作成する許可を付与	書き込み	ServiceNetwork*		ec2:DescribeVpcs
			ServiceNetworkVpcAssociation*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:SecurityGroupIds vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
CreateServiceNetworkVpcEndpointAssociation [アクセス許可のみ]	サービスネットワークと VPC エンドポイント間の関連付けを作成するアクセス許可を付与します	権限の管理			
CreateTargetGroup	ターゲットグループを作成する許可を付与	書き込み	TargetGroup*		iam:CreateServiceLinkedRole

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:VpcId	
DeleteAccessLogSubscription	アクセスログサブスクリプションを削除する許可を付与	書き込み	AccessLogSubscription*		logs:DeleteLogDelivery logs:GetLogDelivery
				aws:ResourceTag/${TagKey}	
DeleteAuthPolicy	認証ポリシーを削除する許可を付与	権限の管理	Service		
			ServiceNetwork		
DeleteListener	リスナーを削除するアクセス許可を付与	書き込み	Listener*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteResourceConfiguration	リソース設定を削除するアクセス許可を付与します	書き込み	ResourceConfiguration*		
				aws:ResourceTag/${TagKey}	
DeleteResourceEndpointAssociation	リソースエンドポイントの関連付けを削除するアクセス許可を付与します	書き込み	ResourceEndpointAssociation*		
				aws:ResourceTag/${TagKey}	
DeleteResourceGateway	リソースゲートウェイを削除するアクセス許可を付与します	書き込み	ResourceGateway*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	リソースポリシーを削除する許可を付与。	書き込み	ResourceConfiguration		
			Service		
			ServiceNetwork		
DeleteRule	ルールを削除する許可を付与	書き込み	Rule*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
DeleteService	サービスを削除する許可を付与	書き込み	Service*		
				aws:ResourceTag/${TagKey}	
DeleteServiceNetwork	サービスネットワークを削除する許可を付与	書き込み	ServiceNetwork*		
				aws:ResourceTag/${TagKey}	
DeleteServiceNetworkResourceAssociation	サービスネットワークとリソース間の関連付けを削除するアクセス許可を付与します	書き込み	ServiceNetworkResourceAssociation*		
				aws:ResourceTag/${TagKey}	
DeleteServiceNetworkServiceAssociation	サービスネットワークとサービスアソシエーションを削除する許可を付与	書き込み	ServiceNetworkServiceAssociation*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn	
DeleteServiceNetworkVpcAssociation	サービスネットワークと VPC アソシエーションを削除する許可を付与	書き込み	ServiceNetworkVpcAssociation*		
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
DeleteTargetGroup	ターゲットグループを削除する許可を付与	書き込み	TargetGroup*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
DeregisterTargets	ターゲットグループからターゲットの登録を削除する許可を付与	書き込み	TargetGroup*		
GetAccessLogSubscription	アクセスログサブスクリプションに関する情報を取得する許可を付与	読み取り	AccessLogSubscription*		logs:GetLogDelivery
				aws:ResourceTag/${TagKey}	
GetAuthPolicy	認証ポリシーに関する情報を取得する許可を付与	読み取り	Service		
			ServiceNetwork		
GetListener	リスナーに関する情報を取得する許可を付与	読み取り	Listener*		
				aws:ResourceTag/${TagKey}	
GetResourceConfiguration	リソース設定に関する情報を取得するアクセス許可を付与します	読み取り	ResourceConfiguration*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetResourceGateway	リソースゲートウェイに関する情報を取得するアクセス許可を付与します	読み取り	ResourceGateway*		
				aws:ResourceTag/${TagKey}	
GetResourcePolicy	リソースポリシーに関する情報を取得する許可を付与	読み取り	ResourceConfiguration		
			Service		
			ServiceNetwork		
GetRule	ルールに関する情報を取得する許可を付与	読み取り	Rule*		
				aws:ResourceTag/${TagKey}	
GetService	サービスに関する情報を取得する許可を付与	読み取り	Service*		
				aws:ResourceTag/${TagKey}	
GetServiceNetwork	サービスネットワークに関する情報を取得する許可を付与	読み取り	ServiceNetwork*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetServiceNetworkResourceAssociation	サービスネットワークとリソース設定間の関連付けに関する情報を取得するアクセス許可を付与します	読み取り	ServiceNetworkResourceAssociation*		
				aws:ResourceTag/${TagKey}	
GetServiceNetworkServiceAssociation	サービスネットワークとサービスアソシエーションに関する情報を取得する許可を付与	読み取り	ServiceNetworkServiceAssociation*		
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn	
GetServiceNetworkVpcAssociation	サービスネットワークと VPC アソシエーションに関する情報を取得する許可を付与	読み取り	ServiceNetworkVpcAssociation*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
GetTargetGroup	ターゲットグループに関する情報を取得する許可を付与	読み取り	TargetGroup*		
				aws:ResourceTag/${TagKey}	
ListAccessLogSubscriptions	サービスネットワークまたはサービスに関する一部またはすべてのアクセスログサブスクリプションを一覧表示する許可を付与	リスト			
ListListeners	一部またはすべてのリスナーを一覧表示する許可を付与	リスト			
ListResourceConfigurations	一部またはすべてのリソース設定を一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListResourceEndpointAssociations	リソース設定と VPC エンドポイント間の一部またはすべての関連付けを一覧表示するアクセス許可を付与します	リスト		vpc-lattice:ResourceConfigurationArn vpc-lattice:VpcEndpointId	
ListResourceGateways	一部またはすべてのリソースゲートウェイを一覧表示するアクセス許可を付与します	リスト			
ListRules	一部またはすべてのルールを一覧表示する許可を付与	リスト			
ListServiceNetworkResourceAssociations	サービスネットワークとリソース設定間の一部またはすべての関連付けを一覧表示するアクセス許可を付与します	リスト			
ListServiceNetworkServiceAssociations	一部またはすべてのサービスネットワークとサービスアソシエーションを一覧表示する許可を付与	リスト		vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListServiceNetworkVpcAssociations	一部またはすべてのサービスネットワークと VPC アソシエーションを一覧表示する許可を付与	リスト		vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
ListServiceNetworkVpcEndpointAssociations	サービスネットワークと VPC エンドポイント間の一部またはすべての関連付けを一覧表示するアクセス許可を付与します	リスト			
ListServiceNetworks	発信者アカウントが所有する、または発信者アカウントと共有するサービスネットワークを一覧表示する許可を付与	リスト			
ListServices	発信者アカウントが所有する、または発信者アカウントと共有するサービスを一覧表示する許可を付与	リスト			
ListTagsForResource	VPC Lattice リソースのタグ付けを一覧表示する許可を付与	読み取り			
ListTargetGroups	一部またはすべてのターゲットグループを一覧表示する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListTargets	ターゲットグループ内の一部またはすべてのターゲットを一覧表示する許可を付与	リスト	TargetGroup*		
PutAuthPolicy	サービスネットワークまたはサービスの認証ポリシーを作成または更新する許可を付与	権限の管理	Service		
			ServiceNetwork		
PutResourcePolicy	リソース設定、サービス、またはサービスネットワークのリソースポリシーを作成するアクセス許可を付与します	書き込み	ResourceConfiguration		
			Service		
			ServiceNetwork		
RegisterTargets	ターゲットグループにターゲットを登録する許可を付与	書き込み	TargetGroup*		
TagResource	VPC Lattice リソースをタグ付けする許可を付与	Tagging	AccessLogSubscription		
			Listener		
			ResourceConfiguration		
			ResourceEndpointAssociation		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			ResourceGateway		
			Rule		
			Service		
			ServiceNetwork		
			ServiceNetworkResourceAssociation		
			ServiceNetworkServiceAssociation		
			ServiceNetworkVpcAssociation		
			TargetGroup		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	VPC Lattice リソースからタグを解除する許可を付与	Tagging	AccessLogSubscription		
			Listener		
			ResourceConfiguration		
			ResourceEndpointAssociation		
			ResourceGateway		
			Rule		
			Service		
			ServiceNetwork		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			ServiceNetworkResourceAssociation		
			ServiceNetworkServiceAssociation		
			ServiceNetworkVpcAssociation		
			TargetGroup		
				aws:TagKeys	
UpdateAccessLogSubscription	アクセスログサブスクリプションを更新する許可を付与	書き込み	AccessLogSubscription*		logs:GetLogDelivery logs:UpdateLogDelivery
				aws:ResourceTag/${TagKey}	
UpdateListener	リスナーを更新する許可を付与	書き込み	Listener*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} vpc-lattice:TargetGroupArns	
UpdateResourceConfiguration	リソース設定を更新するアクセス許可を付与します	書き込み	ResourceConfiguration*		
				aws:ResourceTag/${TagKey}	
UpdateResourceGateway	リソースゲートウェイを更新するアクセス許可を付与します	書き込み	ResourceGateway*		
				aws:ResourceTag/${TagKey} vpc-lattice:SecurityGroupIds	
UpdateRule	ルールを更新する許可を付与	書き込み	Rule*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} vpc-lattice:TargetGroupArns	
UpdateService	サービスを更新する許可を付与	書き込み	Service*		
				aws:ResourceTag/${TagKey} vpc-lattice:AuthType	
UpdateServiceNetwork	サービスネットワークを更新する許可を付与	書き込み	ServiceNetwork*		
				aws:ResourceTag/${TagKey} vpc-lattice:AuthType	
UpdateServiceNetworkVpcAssociation	サービスネットワークと VPC アソシエーションを更新する許可を付与	書き込み	ServiceNetworkVpcAssociation*		ec2:DescribeSecurityGroups ec2:DescribeVpcs

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:SecurityGroupIds vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
UpdateTargetGroup	ターゲットグループを更新する許可を付与	書き込み	TargetGroup*		
				aws:ResourceTag/${TagKey}	

Amazon VPC Lattice で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
AccessLogSubscription	arn:${Partition}:vpc-lattice:${Region}:${Account}:accesslogsubscription/${AccessLogSubscriptionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
Listener	arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}/listener/${ListenerId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:Protocol vpc-lattice:TargetGroupArns
ResourceConfiguration	arn:${Partition}:vpc-lattice:${Region}:${Account}:resourceconfiguration/${ResourceConfigurationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
ResourceEndpointAssociation	arn:${Partition}:vpc-lattice:${Region}:${Account}:resourceendpointassociation/${ResourceEndpointAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

リソースタイプ	ARN	条件キー
		vpc-lattice:ResourceConfigurationArn vpc-lattice:VpcEndpointId
ResourceGateway	arn:${Partition}:vpc-lattice:${Region}:${Account}:resourcegateway/${ResourceGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:VpcId
Rule	arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}/listener/${ListenerId}/rule/${RuleId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:TargetGroupArns
Service	arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:AuthType

リソースタイプ	ARN	条件キー
ServiceNetwork	arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetwork/${ServiceNetworkId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:AuthType
ServiceNetworkResourceAssociation	arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetworkresourceassociation/${ServiceNetworkResourceAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:ResourceConfigurationArn vpc-lattice:ServiceNetworkArn
ServiceNetworkServiceAssociation	arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetworkserviceassociation/${ServiceNetworkServiceAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn

リソースタイプ	ARN	条件キー
ServiceNetworkVpcAssociation	arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetworkvpcassociation/${ServiceNetworkVpcAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:SecurityGroupIds vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId
TargetGroup	arn:${Partition}:vpc-lattice:${Region}:${Account}:targetgroup/${TargetGroupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:VpcId

Amazon VPC Lattice の条件キー

Amazon VPC Lattice では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアが存在するかどうかでアクションをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーが存在するかどうかでアクセスをフィルタリングします	ArrayOfString
vpc-lattice:AuthType	リクエストで指定された認証タイプによりアクセスをフィルタリング	String
vpc-lattice:Protocol	リクエストで指定されたプロトコルによりアクセスをフィルタリング	String
vpc-lattice:ResourceConfigurationArn	リソース設定の ARN でアクセスをフィルタリングします	ARN
vpc-lattice:SecurityGroupIds	セキュリティグループの ID によりアクセスをフィルタリング	ArrayOfString
vpc-lattice:ServiceArn	サービスの ARN によりアクセスをフィルタリング	ARN
vpc-lattice:ServiceNetworkArn	サービスネットワークの ARN によりアクセスをフィルタリング	ARN
vpc-lattice:TargetGroupArns	ターゲットグループの ARN によりアクセスをフィルタリング	ArrayOfARN

条件キー	説明	[Type] (タイプ)
vpc-lattice:VpcEndpointId	VPC エンドポイントの ID でアクセスをフィルタリングします	String
vpc-lattice:VpcId	仮想プライベートクラウド (VPC) の ID でアクセスをフィルタリングします	String

Amazon VPC Lattice Services のアクション、リソース、および条件キー

Amazon VPC Lattice Services (サービスプレフィックス: `vpc-lattice-svcs`) では、IAM 許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon VPC Lattice Services で定義されるアクション
- Amazon VPC Lattice Services で定義されるリソースタイプ
- Amazon VPC Lattice Services の条件キー

Amazon VPC Lattice Services で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
Connect	VPC Lattice サービスへの接続の許可を付与する	書き込み	TCP Service*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				vpc-lattice-svcs:Port vpc-lattice-svcs:ServiceNetworkArn vpc-lattice-svcs:ServiceArn vpc-lattice-svcs:SourceVpc vpc-lattice-svcs:SourceVpcOwnerAccount	
Invoke	VPC Lattice サービスを呼び出す許可を付与	書き込み	Service*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				vpc-lattice-svcs:Port vpc-lattice-svcs:ServiceNetworkArn vpc-lattice-svcs:ServiceArn vpc-lattice-svcs:SourceVpc vpc-lattice-svcs:SourceVpcOwnerAccount vpc-lattice-svcs:RequestHeader/${HeaderName} vpc-lattice-svcs:R	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				equestQueryString/${QueryStringKey}	

Amazon VPC Lattice Services で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
Service	arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}/${RequestPath}	
TCP Service	arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}	

Amazon VPC Lattice Services の条件キー

Amazon VPC Lattice サービスでは、 IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
vpc-lattice-svcs:Port	リクエストが行われた送信先ポートによりアクセスをフィルタリング	数値
vpc-lattice-svcs:RequestHeader/${HeaderName}	リクエストヘッダーのヘッダー名と値のペアによりアクセスをフィルタリング	String
vpc-lattice-svcs:RequestMethod	リクエスト方法によりアクセスをフィルタリング	String
vpc-lattice-svcs:RequestQueryString/${QueryStringKey}	リクエスト URL 内のクエリ文字列キーと値のペアによりアクセスをフィルタリング	ArrayOfString
vpc-lattice-svcs:ServiceArn	リクエストを受け取ったサービスの ARN によりアクセスをフィルタリング	ARN
vpc-lattice-svcs:ServiceNetworkArn	リクエストを受け取ったサービスネットワークの ARN によりアクセスをフィルタリング	ARN
vpc-lattice-svcs:SourceVpc	リクエストが行われた VPC によりアクセスをフィルタリング	String
vpc-lattice-svcs:SourceVpcOwnerAccount	リクエストが行われた所有アカウントの VPC によりアクセスをフィルタリング	String

AWS WAF のアクション、リソース、および条件キー

AWS WAF (サービスプレフィックス: waf) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS WAF で定義されるアクション
- AWS WAF で定義されるリソースタイプ
- AWS WAF の条件キー

AWS WAF で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリス

ク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateByteMatchSet	ByteMatchSet を作成する許可を付与	Write	bytematchset*		
CreateGeoMatchSet	GeoMatchSet を作成する許可を付与	Write	geomatchset*		
CreateIPSet	IPSet を作成する許可を付与	Write	ipset*		
CreateRateBasedRule	単一の IP アドレスからのリクエストの量を制限する RateBasedRule を作成する許可を付与	Write	ratebasedrule*		
				aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
CreateRegexMatchSet	RegexMatchSet を作成する許可を付与	Write	regexmatchset*		
CreateRegexPatternSet	RegexPatternSet を作成する許可を付与。	Write	regexpatternset*		
CreateRule	ウェブリクエストをフィルターするルールを作成する許可を付与	Write	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	WebACL で使用できる定義済みルールのコレクションである RuleGroup を作成する許可を付与。	Write	rulegroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSizeConstraintSet	SizeConstraintSet を作成する許可を付与	Write	sizeconstraintset*		
CreateSqlInjectionMatchSet	SqlInjectionMatchSet を作成する許可を付与	Write	sqlinjectionmatchset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateWebACL	ウェブリクエストをフィルターするルールを含む WebACL を作成する権限を付与します。	権限の管理	webacl*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebACLMigrationStack	WAF Classic から AWS WAF v2 にウェブ ACL を移行する目的で、S3 バケットに CloudFormation ウェブ ACL テンプレートを作成するアクセス許可を付与 AWS します	書き込み	webacl*		s3:PutObject
CreateXssMatchSet	クロスサイトスクリプティング攻撃を含むリクエストを検出するために使用する XssMatchSet を作成する許可を付与	Write	xssmatchset*		
DeleteByteMatchSet	ByteMatchSet を削除する許可を付与	Write	bytematchset*		
DeleteGeoMatchSet	GeoMatchSet を削除する許可を付与	Write	geomatchset*		
DeleteIPSet	IPSet を削除する許可を付与。	Write	ipset*		
DeleteLoggingConfiguration	ウェブ ACL から LoggingConfiguration を削除する許可を付与	Write	webacl*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeletePermissionPolicy	ルールグループから IAM ポリシーを削除する許可を付与	Permissions management	rulegroup*		
DeleteRateBasedRule	RateBasedRule を削除する許可を付与。	Write	ratebasedrule*		
DeleteRegexMatchSet	RegexMatchSet を削除する許可を付与	Write	regexmatchset*		
DeleteRegexPatternSet	RegexPatternSet を削除する許可を付与。	Write	regexpatternset*		
DeleteRule	ルールを削除する許可を付与。	Write	rule*		
DeleteRuleGroup	RuleGroup を削除する許可を付与	Write	rulegroup*		
DeleteSizeConstraintSet	SizeConstraintSet を削除する許可を付与	Write	sizeconstraintset*		
DeleteSqlInjectionMatchSet	SqlInjectionMatchSet を削除する許可を付与	Write	sqlinjectionmatchset*		
DeleteWebACL	WebACL を削除する許可を付与	Permissions management	webacl*		
DeleteXssMatchSet	XssMatchSet を削除する許可を付与	Write	xssmatchset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetByteMatchSet	ByteMatchSet を取得する許可を付与	Read	bytematchset*		
GetChangeToken	作成、更新、および削除リクエストで使用する変更トークンを取得する許可を付与	Read			
GetChangeTokenStatus	変更トークンのステータスを取得する許可を付与	Read			
GetGeoMatchSet	GeoMatchSet を取得する許可を付与	Read	geomatchset*		
GetIPSet	IPSet を取得する許可を付与	Read	ipset*		
GetLoggingConfiguration	ウェブ ACL の LoggingConfiguration を取得する許可を付与	Read	webacl*		
GetPermissionPolicy	ルールグループの IAM ポリシーを取得する許可を付与	Read	rulegroup*		
GetRateBasedRule	RateBasedRule を取得する許可を付与	Read	ratebasedrule*		
GetRateBasedRuleManagedKeys	RateBasedRule によって現在ブロックされている IP アドレスの配列を取得する許可を付与	Read	ratebasedrule*		
GetRegexMatchSet	RegexMatchSet を取得する許可を付与	Read	regexmatchset*		
GetRegexPatternSet	RegexPatternSet を取得する許可を付与	Read	regexpatternset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetRule	ルールを取得する許可を付与	Read	rule*		
GetRuleGroup	RuleGroup を取得する許可を付与	Read	rulegroup*		
GetSampledRequests	ウェブリクエストのサンプルセットに関する詳細情報を取得する許可を付与	Read	webacl		
GetSizeConstraintSet	SizeConstraintSet を取得するためのアクセス許可を付与します	Read	sizeconstraintset*		
GetSqlInjectionMatchSet	SqlInjectionMatchSet を取得する許可を付与	Read	sqlinjectionmatchset*		
GetWebACL	WebACL を取得する許可を付与	Read	webacl*		
GetXssMatchSet	XssMatchSet を取得する許可を付与	Read	xssmatchset*		
ListActivatedRulesInRuleGroup	ActivatedRule オブジェクトの配列を取得する許可を付与	リスト			
ListByteMatchSets	ByteMatchSetSummary オブジェクトの配列を取得する許可を付与	リスト			
ListGeoMatchSets	GeoMatchSetSummary オブジェクトの配列を取得するためのアクセス許可を付与します。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListIPSets	IPSetSummary オブジェクトの配列を取得する許可を付与	リスト			
ListLoggingConfigurations	LoggingConfiguration オブジェクトの配列を取得する許可を付与	リスト			
ListRateBasedRules	RuleSummary オブジェクトの配列を取得する権限を付与します	リスト			
ListRegexMatchSets	RegexMatchSetSummary オブジェクトの配列を取得する許可を付与	リスト			
ListRegexPatternSets	RegexPatternSetSummary オブジェクトの配列を取得する許可を付与	リスト			
ListRuleGroups	RuleGroup オブジェクトの配列を取得する許可を付与	リスト			
ListRules	RuleSummary オブジェクトの配列を取得する権限を付与します	リスト			
ListSizeConstraintSets	SizeConstraintSetSummary オブジェクトの配列を取得する許可を付与	リスト			
ListSqlInjectionMatchSets	SqlInjectionMatchSet オブジェクトの配列を取得する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListSubscribedRuleGroups	サブスクライブしている RuleGroup オブジェクトの配列を取得する許可を付与	リスト			
ListTagsForResource	リソースのタグを取得する許可を付与	Read	ratebasedrule		
			rule		
			rulegroup		
			webacl		
ListWebACLs	WebACLSummary オブジェクトの配列を取得する許可を付与	リスト			
ListXssMatchSets	XssMatchSet オブジェクトの配列を取得する許可を付与	リスト			
PutLoggingConfiguration	指定したウェブ ACL に LoggingConfiguration を関連付けるアクセス許可を付与します	Write	webacl*		iam:CreateServiceLinkedRole
PutPermissionPolicy	IAM ポリシーをルールグループにアタッチし、アカウント間でルールグループを共有する許可を付与	Permissions management	rulegroup*		
TagResource	リソースにタグを追加する許可を付与	タグ付け	ratebasedrule		
			rule		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			rulegroup		
			webacl		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	タグ付け	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:TagKeys	
UpdateByteMatchSet	ByteMatchSet に ByteMatchTuple オブジェクトを挿入または削除するアクセス許可権限を付与します	Write	bytematchset*		
UpdateGeoMatchSet	GeoMatchSet で GeoMatchConstraint オブジェクトを挿入または削除する権限を付与します	Write	geomatchset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateIPSet	IPSet 内の IPSetDescriptor オブジェクトを挿入または削除する許可を付与。	Write	ipset*		
UpdateRateBasedRule	レートベースのルールを変更する許可を付与	Write	ratebasedrule*		
UpdateRegexMatchSet	RegexMatchSet で RegexMatchTuple オブジェクトを挿入または削除する許可を付与。	Write	regexmatchset*		
UpdateRegexPatternSet	RegexPatternSet で RegexPatternStrings を挿入または削除する権限を付与します。	Write	regexpatternset*		
UpdateRule	ルールを変更する許可を付与	Write	rule*		
UpdateRuleGroup	RuleGroup で ActivatedRule オブジェクトを挿入または削除する許可を付与	Write	rulegroup*		
UpdateSizeConstraintSet	SizeConstraintSet で SizeConstraint オブジェクトを挿入または削除する許可を付与。	Write	sizeconstraintset*		
UpdateSqlInjectionMatchSet	SqlInjectionMatchSet で SqlInjectionMatchTuple オブジェクトを挿入または削除する許可を付与	Write	sqlinjectionmatchset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateWebACL	WebACL で ActivatedRule オブジェクトを挿入または削除する許可を付与	Permissions management	webacl*		
UpdateXssMatchSet	XssMatchSet で XssMatchTuple オブジェクトを挿入または削除する許可を付与	Write	xssmatchset*		

AWS WAF で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
bytematchset	`arn:${Partition}:waf::${Account}:bytematchset/${Id}`	
ipset	`arn:${Partition}:waf::${Account}:ipset/${Id}`	
ratebasedrule	`arn:${Partition}:waf::${Account}:ratebasedrule/${Id}`	aws:ResourceTag/${TagKey}
rule	`arn:${Partition}:waf::${Account}:rule/${Id}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
sizeconstraintset	arn:${Partition}:waf::${Account}:sizeconstraintset/${Id}	
sqlinjectionmatchset	arn:${Partition}:waf::${Account}:sqlinjectionset/${Id}	
webacl	arn:${Partition}:waf::${Account}:webacl/${Id}	aws:ResourceTag/${TagKey}
xssmatchset	arn:${Partition}:waf::${Account}:xssmatchset/${Id}	
regexmatchset	arn:${Partition}:waf::${Account}:regexmatch/${Id}	
regexpatternset	arn:${Partition}:waf::${Account}:regexpatternset/${Id}	
geomatchset	arn:${Partition}:waf::${Account}:geomatchset/${Id}	
rulegroup	arn:${Partition}:waf::${Account}:rulegroup/${Id}	aws:ResourceTag/${TagKey}

AWS WAF の条件キー

AWS WAF では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	各タグで許可されている値のセットに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられている tag-value に基づいてアクションをフィルタリングします。	文字列
aws:TagKeys	リクエスト内の必須タグのプレゼンスに基づいてアクションをフィルタリングします	ArrayOfString

AWS WAF Regional のアクション、リソース、および条件キー

AWS WAF Regional (サービスプレフィックス: `waf-regional`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS WAF Regional で定義されるアクション
- AWS WAF Regional で定義されるリソースタイプ
- AWS WAF Regional の条件キー

AWS WAF Regional で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセス

を許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateWebACL	ウェブ ACL をリソースに関連付けるアクセス許可を付与します	Write	loadbalancer/app/*		
			webacl*		
CreateByteMatchSet	ByteMatchSet を作成する許可を付与	Write	bytematchset*		
CreateGeoMatchSet	GeoMatchSet を作成する許可を付与	Write	geomatchset*		
CreateIPSet	IPSet を作成する許可を付与	Write	ipset*		
CreateRateBasedRule	RateBasedRule を作成する許可を付与	Write	ratebasedrule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegexMatchSet	RegexMatchSet を作成する許可を付与	Write	regexmatchset*		
CreateRegexPatternSet	RegexPatternSet を作成する許可を付与。	Write	regexpatternset*		
CreateRule	ルールを作成する許可を付与	Write	rule*		
				aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
CreateRuleGroup	RuleGroup を作成する許可を付与。	Write	rulegroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSizeConstraintSet	SizeConstraintSet を作成する許可を付与	Write	sizeconstraintset*		
CreateSqlInjectionMatchSet	SqlInjectionMatchSet を作成する許可を付与	Write	sqlinjectionmatchset*		
CreateWebACL	WebACL を作成する許可を付与	権限の管理	webacl*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateWebACLMigrationStack	WAF Classic から AWS WAF v2 にウェブ ACL を移行する目的で、S3 バケットに CloudFormation ウェブ ACL テンプレートを作成するアクセス許可を付与 AWS します	書き込み	webacl*		s3:PutObject
CreateXssMatchSet	XssMatchSet を作成する許可を付与	Write	xssmatchset*		
DeleteByteMatchSet	ByteMatchSet を削除する許可を付与	Write	bytematchset*		
DeleteGeoMatchSet	GeoMatchSet を削除する許可を付与	Write	geomatchset*		
DeleteIPSet	IPSet を削除する許可を付与。	Write	ipset*		
DeleteLoggingConfiguration	ウェブ ACL から LoggingConfiguration を削除する許可を付与	Write	webacl*		
DeletePermissionPolicy	ルールグループから IAM ポリシーを削除する許可を付与	Permissions management	rulegroup*		
DeleteRateBasedRule	RateBasedRule を削除する許可を付与。	Write	ratebasedrule*		
DeleteRegexMatchSet	RegexMatchSet を削除する許可を付与	Write	regexmatchset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteRegexPatternSet	RegexPatternSet を削除する許可を付与。	Write	regexpatternset*		
DeleteRule	ルールを削除する許可を付与。	Write	rule*		
DeleteRuleGroup	RuleGroup を削除する許可を付与	Write	rulegroup*		
DeleteSizeConstraintSet	SizeConstraintSet を削除する許可を付与	Write	sizeconstraintset*		
DeleteSqlInjectionMatchSet	SqlInjectionMatchSet を削除する許可を付与	Write	sqlinjectionmatchset*		
DeleteWebACL	WebACL を削除する許可を付与	Permissions management	webacl*		
DeleteXssMatchSet	XssMatchSet を削除する許可を付与	Write	xssmatchset*		
DisassociateWebACL	ウェブ ACL とリソース間の関連付けを削除する許可を付与	Write	loadbalancer/app/*		
GetByteMatchSet	ByteMatchSet を取得する許可を付与	Read	bytematchset*		
GetChangeToken	作成、更新、および削除リクエストで使用する変更トークンを取得する許可を付与	Read			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetChangeTokenStatus	変更トークンのステータスを取得する許可を付与	Read			
GetGeoMatchSet	GeoMatchSet を取得する許可を付与	Read	geomatchset*		
GetIPSet	IPSet を取得する許可を付与	Read	ipset*		
GetLoggingConfiguration	LoggingConfiguration を取得する許可を付与	Read	webacl*		
GetPermissionPolicy	RuleGroup にアタッチされた IAM ポリシーを取得する許可を付与	Read	rulegroup*		
GetRateBasedRule	RateBasedRule を取得する許可を付与	Read	ratebasedrule*		
GetRateBasedRuleManagedKeys	RateBasedRule によって現在ブロックされている IP アドレスの配列を取得する許可を付与	Read	ratebasedrule*		
GetRegexMatchSet	RegexMatchSet を取得する許可を付与	Read	regexmatchset*		
GetRegexPatternSet	RegexPatternSet を取得する許可を付与	Read	regexpatternset*		
GetRule	ルールを取得する許可を付与	Read	rule*		
GetRuleGroup	RuleGroup を取得する許可を付与	Read	rulegroup*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetSampledRequests	ウェブリクエストのサンプルセットの詳細情報を取得する許可を付与	Read	webacl		
GetSizeConstraintSet	SizeConstraintSet を取得するためのアクセス許可を付与します	Read	sizeconstraintset*		
GetSqlInjectionMatchSet	SqlInjectionMatchSet を取得する許可を付与	Read	sqlinjectionmatchset*		
GetWebACL	WebACL を取得する許可を付与	Read	webacl*		
GetWebACLForResource	指定したリソースに関連付けられている WebACL を取得する許可を付与	Read	loadbalancer/app/*		
GetXssMatchSet	XssMatchSet を取得する許可を付与	Read	xssmatchset*		
ListActivatedRulesInRuleGroup	ActivatedRule オブジェクトの配列を取得する許可を付与	リスト			
ListByteMatchSets	ByteMatchSetSummary オブジェクトの配列を取得する許可を付与	リスト			
ListGeoMatchSets	GeoMatchSetSummary オブジェクトの配列を取得するためのアクセス許可を付与します。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListIPSets	IPSetSummary オブジェクトの配列を取得する許可を付与	リスト			
ListLoggingConfigurations	LoggingConfiguration オブジェクトの配列を取得する許可を付与	リスト			
ListRateBasedRules	RuleSummary オブジェクトの配列を取得する権限を付与します	リスト			
ListRegexMatchSets	RegexMatchSetSummary オブジェクトの配列を取得する許可を付与	リスト			
ListRegexPatternSets	RegexPatternSetSummary オブジェクトの配列を取得する許可を付与	リスト			
ListResourcesForWebACL	指定した WebACL に関連付けられたリソースの配列を取得する許可を付与	リスト	webacl*		
ListRuleGroups	RuleGroup オブジェクトの配列を取得する許可を付与	リスト			
ListRules	RuleSummary オブジェクトの配列を取得する権限を付与します	リスト			
ListSizeConstraintSets	SizeConstraintSetSummary オブジェクトの配列を取得する許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListSqlInjectionMatchSets	SqlInjectionMatchSet オブジェクトの配列を取得する許可を付与	リスト			
ListSubscribedRuleGroups	サブスクライブしている RuleGroup オブジェクトの配列を取得する許可を付与	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	Read	ratebasedrule		
			rule		
			rulegroup		
			webacl		
ListWebACLs	WebACLSummary オブジェクトの配列を取得する許可を付与	リスト			
ListXssMatchSets	XssMatchSet オブジェクトの配列を取得する許可を付与	リスト			
PutLoggingConfiguration	LoggingConfiguration をウェブ ACL に関連付けるアクセス許可を付与します	Write	webacl*		iam:CreateServiceLinkedRole
PutPermissionPolicy	アカウント間のルールグループの共有をサポートするために、指定したルールグループに IAM ポリシーをアタッチする許可を付与	Permissions management	rulegroup*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagResource	リソースにタグを追加する許可を付与	タグ付け	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースからタグを削除する許可を付与	タグ付け	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:TagKeys	
UpdateByteMatchSet	ByteMatchSet に ByteMatchTuple オブジェクトを挿入または削除するアクセス許可権限を付与します	Write	bytematchset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateGeoMatchSet	GeoMatchSet で GeoMatchConstraint オブジェクトを挿入または削除する権限を付与します	Write	geomatchset*		
UpdateIPSet	IPSet 内の IPSetDescriptor オブジェクトを挿入または削除する許可を付与。	Write	ipset*		
UpdateRateBasedRule	レートベースのルールでの述語オブジェクトの挿入または削除、およびルール内の RateLimit の更新を行うアクセス許可を付与します	Write	ratebasedrule*		
UpdateRegexMatchSet	RegexMatchSet で RegexMatchTuple オブジェクトを挿入または削除する許可を付与。	Write	regexmatchset*		
UpdateRegexPatternSet	RegexPatternSet で RegexPatternStrings を挿入または削除する権限を付与します。	Write	regexpatternset*		
UpdateRule	ルールで述語オブジェクトを挿入または削除する許可を付与	Write	rule*		
UpdateRuleGroup	RuleGroup で ActivatedRule オブジェクトを挿入または削除する許可を付与	Write	rulegroup*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateSizeConstraintSet	SizeConstraintSet で SizeConstraint オブジェクトを挿入または削除する許可を付与。	Write	sizeconstraintset*		
UpdateSqlInjectionMatchSet	SqlInjectionMatchSet で SqlInjectionMatchTuple オブジェクトを挿入または削除する許可を付与	Write	sqlinjectionmatchset*		
UpdateWebACL	WebACL で ActivatedRule オブジェクトを挿入または削除する許可を付与	Permissions management	webacl*		
UpdateXssMatchSet	XssMatchSet で XssMatchTuple オブジェクトを挿入または削除する許可を付与	Write	xssmatchset*		

AWS WAF Regional で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
bytematchset	`arn:${Partition}:waf-regional:${Region}:${Account}:bytematchset/${Id}`	

リソースタイプ	ARN	条件キー
ipset	arn:${Partition}:waf-regional:${Region}:${Account}:ipset/${Id}	
loadbalancer/app/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}	
ratebasedrule	arn:${Partition}:waf-regional:${Region}:${Account}:ratebasedrule/${Id}	aws:ResourceTag/${TagKey}
rule	arn:${Partition}:waf-regional:${Region}:${Account}:rule/${Id}	aws:ResourceTag/${TagKey}
sizeconstraintset	arn:${Partition}:waf-regional:${Region}:${Account}:sizeconstraintset/${Id}	
sqlinjectionmatchset	arn:${Partition}:waf-regional:${Region}:${Account}:sqlinjectionset/${Id}	
webacl	arn:${Partition}:waf-regional:${Region}:${Account}:webacl/${Id}	aws:ResourceTag/${TagKey}
xssmatchset	arn:${Partition}:waf-regional:${Region}:${Account}:xssmatchset/${Id}	
regexmatchset	arn:${Partition}:waf-regional:${Region}:${Account}:regexmatch/${Id}	
regexpatternset	arn:${Partition}:waf-regional:${Region}:${Account}:regexpatternset/${Id}	
geomatchset	arn:${Partition}:waf-regional:${Region}:${Account}:geomatchset/${Id}	

リソースタイプ	ARN	条件キー
rulegroup	arn:${Partition}:waf-regional:${Region}:${Account}:rulegroup/${Id}	aws:ResourceTag/${TagKey}

AWS WAF Regional の条件キー

AWS WAF Regional では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	各タグで許可されている値のセットに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられている tag-value に基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエスト内の必須タグのプレゼンスに基づいてアクションをフィルタリングします	ArrayOfString

AWS WAF V2 のアクション、リソース、および条件キー

AWS WAF V2 (サービスプレフィックス: wafv2) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。

- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS WAF V2 で定義されるアクション
- AWS WAF V2 で定義されるリソースタイプ
- AWS WAF V2 の条件キー

AWS WAF V2 で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
Associate WebACL	WebACL をリソースに関連付けるアクセス許可を付与	Write	webacl*		amplify:AssociateWebACL apigateway:SetWebACL apprunner:AssociateWebAcl appsync:SetWebACL cognito-idp:AssociateWebACL ec2:AssociateVerifiedAccessInstanceWebAcl

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
					elasticloadbalancing:SetWebAcl wafv2:GetPermissionPolicy wafv2:PutPermissionPolicy
			amplify-app		
			apigateway		
			apprunner		
			appsync		
			loadbalancer/app/		
			userpool		
			verified-access-instance		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CheckCapacity	指定したスコープとルールのセットについて、ウェブ ACL キャパシティーユニット (WCU) 要件を計算する許可を付与	読み取り			
CreateAPIKey	JavaScript クライアントアプリケーションで CAPTCHA API での統合に使用する、API キーを作成する許可を付与	書き込み			
CreateIPSet	IPSet を作成する許可を付与	Write	ipset*		wafv2:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegexPatternSet	RegexPatternSet を作成する許可を付与。	Write	regexpatternset*		wafv2:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	RuleGroup を作成する許可を付与。	Write	rulegroup*		wafv2:TagResource
			ipset		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			regexpatternset		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebACL	WebACL を作成する許可を付与	書き込み	webacl*		wafv2:TagResource
			ipset		
			managedruleset		
			regexpatternset		
			rulegroup		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAPIKey	API キーを削除する許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeleteFirewallManagerRuleGroups	Firewall Manager によって管理されなくなった場合に WebACL から FirewallManagedRulesGroups を削除する許可を付与	Write	webacl*		
DeleteIPSet	IPSet を削除する許可を付与。	Write	ipset*		
DeleteLoggingConfiguration	WebACL から LoggingConfiguration を削除する許可を付与	Write	webacl*		
				wafv2:LogScope	
DeletePermissionPolicy	RuleGroup の PermissionPolicy を削除する許可を付与。	Permissions management	rulegroup*		
DeleteRegexPatternSet	RegexPatternSet を削除する許可を付与。	Write	regexpatternset*		
DeleteRuleGroup	RuleGroup を削除する許可を付与	Write	rulegroup*		
DeleteWebACL	WebACL を削除する許可を付与	書き込み	webacl*		
DescribeAllManagedProducts	マネージドルールグループの製品情報を取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeManagedProductsByVendor	指定されたベンダーによるマネージドルールグループの製品情報を取得する許可を付与	読み取り			
DescribeManagedRuleGroup	マネージドルールグループの高レベル情報を取得する許可を付与	読み取り			
DisassociateFirewallManager [許可のみ]	WebACL から Firewall Manager の関連付けを解除する許可を付与	書き込み	webacl*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisassociateWebACL	アプリケーションリソースから WebACL の関連付けを解除する許可を付与	書き込み	amplify-app		amplify:DisassociateWebACL apigateway:SetWebACL apprunner:DisassociateWebAcl appsync:SetWebACL cognito-idp:DisassociateWebACL ec2:DisassociateVerifiedAccessInstanceWebAcl elasticloadbalancing:SetWebAcl

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					wafv2:PutPermissionPolicy
			apigateway		
			apprunner		
			appsync		
			loadbalancer/app/		
			userpool		
			verified-access-instance		
GenerateMobileSdkReleaseUrl	モバイル SDK の指定したリリースの署名済みダウンロード URL を生成するアクセス許可を付与	読み取り			
GetDecryptedAPIKey	API キーを復号化された形式で返す許可を付与します。これは、キーのために定義したトークンドメインを確認するためにします。	読み取り			
GetIPSet	IPSet の詳細を取得するアクセス許可を付与	Read	ipset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
GetLoggingConfiguration	WebACL の LoggingConfiguration を取得する許可を付与。	読み取り	webacl*		
				aws:ResourceTag/${TagKey} wafv2:LogScope	
GetManagedRuleSet	ManagedRuleGroup の詳細を取得する許可を付与	読み取り	managedruleset*		
GetMobileSdkRelease	リリースノートやタグなど、指定したモバイル SDK リリースの情報を取得するアクセス許可を付与	読み取り			
GetPermissionPolicy	RuleGroup の PermissionPolicy を取得する許可を付与	Read	rulegroup*		
GetRateBasedStatementManagedKeys	レートベースのルールによって現在ブロックされているキーを取得する許可を付与	Read	webacl*		
				aws:ResourceTag/${TagKey}	
GetRegexPatternSet	RegexPatternSet の詳細を取得する許可を付与	Read	regexpatternset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
GetRuleGroup	RuleGroup の詳細を取得する許可を付与	Read	rulegroup*		
				aws:ResourceTag/${TagKey}	
GetSampledRequests	ウェブリクエストのサンプリングに関する詳細情報を取得する許可を付与	Read	webacl*		
GetWebACL	WebACL の詳細を取得する許可を付与	Read	webacl*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetWebACLForResource	リソースに関連付けられている WebACL を取得する許可を付与	読み取り	webacl*		amplify:GetWebACLForResource apprunner:DescribeWebAclForService cognito-idp:GetWebACLForResource ec2:GetVerifiedAccessInstanceWebAcl wafv2:GetWebACL
			amplify-app		
			apigateway		
			apprunner		
			appsync		
			loadbalancer/app/		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			userpool		
			verified-access-instance		
ListAPIKeys	指定された範囲のために定義した API キーのリストを取得する許可を付与	リスト			
ListAvailableManagedRuleGroupVersions	使用可能なマネージドルールグループのバージョンを取得する許可を付与	リスト			
ListAvailableManagedRuleGroups	使用可能なマネージドルールグループの配列を取得する許可を付与	リスト			
ListIPSets	管理する IP セットの IPSetSummary オブジェクトの配列を取得する許可を付与	リスト			
ListLoggingConfigurations	LoggingConfiguration オブジェクトの配列を取得する許可を付与	リスト		wafv2:LogScope	
ListManagedRuleSets	ManagedRuleSetオブジェクトの配列を取得するアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListMobileSdkReleases	モバイル SDK や指定したデバイスプラットフォームのリリース済みリストを取得するアクセス許可を付与	リスト			
ListRegexPatternSets	管理する正規表現パターンセットの RegexPatternSetSummary オブジェクトの配列を取得する許可を付与	リスト			
ListResourcesForWebACL	ウェブ ACL に関連付けられているリソースの Amazon リソースネーム (ARN) の配列を取得する許可を付与。	リスト	webacl*		amplify:ListResourcesForWebACL apprunner:ListAssociatedServicesForWebAcl cognito-idp:ListResourcesForWebACL ec2:DescribeVerifiedAccessInstanceWebAclAssociations

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			amplify-app		
			apprunner		
			userpool		
			verified-access-instance		
ListRuleGroups	管理するルールグループの RuleGroupSummary オブジェクトの配列を取得する許可を付与	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	Read	ipset		
			regexpatternset		
			rulegroup		
			webacl		
				aws:ResourceTag/${TagKey}	
ListWebACLs	管理するウェブ ACL の WebACLSummary オブジェクトの配列を取得する許可を付与。	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutFirewallManagerRuleGroups [許可のみ]	WebACL に FirewallManagedRulesGroups を作成する許可を付与	Write	webacl*		
PutLoggingConfiguration	LoggingConfiguration を有効にしてウェブ ACL のロギングを開始する許可を付与	書き込み	webacl*		iam:CreateServiceLinkedRole
				wafv2:LogScope wafv2:LogDestinationResource	
PutManagedRuleSetVersions	ManagedRuleSet の新しいバージョンを作成または既存のバージョンを更新するアクセス許可を付与	書き込み	managedruleset*		
			rulegroup*		
PutPermissionPolicy	アカウント間でルールグループを共有するために使用する IAM ポリシーをリソースにアタッチするアクセス許可を付与	権限の管理	rulegroup*		
TagResource	タグを AWS リソースに関連付けるアクセス許可を付与します	Tagging	ipset		
			regexpatternset		
			rulegroup		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			webacl		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
				aws:ResourceTag/${TagKey}	
UntagResource	AWS リソースからタグの関連付けを解除するアクセス許可を付与します	Tagging	ipset		
			regexpatternset		
			rulegroup		
			webacl		
				aws:TagKeys	
UpdateIPSet	IPSet を更新する許可を付与	書き込み	ipset*		
				aws:ResourceTag/${TagKey}	
UpdateManagedRuleSetVersionExpiryDate	ManagedRuleSet 内のバージョンの有効期限を更新するアクセス許可を付与	書き込み	managedruleset*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateRegexPatternSet	RegexPatternSet を更新する許可を付与	Write	regexpatternset*		
				aws:ResourceTag/${TagKey}	
UpdateRuleGroup	RuleGroup を更新する許可を付与	Write	rulegroup*		
			ipset		
			regexpatternset		
				aws:ResourceTag/${TagKey}	
UpdateWebACL	WebACL を更新する許可を付与	書き込み	webacl*		
			ipset		
			managedruleset		
			regexpatternset		
			rulegroup		
				aws:ResourceTag/${TagKey}	

AWS WAF V2 で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
webacl	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}	aws:ResourceTag/${TagKey}
ipset	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/ipset/${Name}/${Id}	aws:ResourceTag/${TagKey}
managedruleset	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/managedruleset/${Name}/${Id}	
rulegroup	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/rulegroup/${Name}/${Id}	aws:ResourceTag/${TagKey}
regexpatternset	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/regexpatternset/${Name}/${Id}	aws:ResourceTag/${TagKey}
loadbalancer/app/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}	
apigateway	arn:${Partition}:apigateway:${Region}::/restapis/${ApiId}/stages/${StageName}	

リソースタイプ	ARN	条件キー
appsync	arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}	
userpool	arn:${Partition}:cognito-idp:${Region}:${Account}:userpool/${UserPoolId}	
apprunner	arn:${Partition}:apprunner:${Region}:${Account}:service/${ServiceName}/${ServiceId}	
verified-access-instance	arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}	
amplify-app	arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}	

AWS WAF V2 の条件キー

AWS WAF V2 では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	各タグの許可された値のセットでアクセスをフィルタリングします	String
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグ値でアクセスをフィルタリングします	String

条件キー	説明	タイプ
aws:TagKeys	リクエスト内の必須タグの存在でアクセスをフィルタリングします	ArrayOfString
wafv2:LogDestinationResource	PutLoggingConfiguration API のログ送信先 ARN でアクセスをフィルタリングする	ARN
wafv2:LogScope	ログ設定 API のログスコープでアクセスをフィルタリングする	String

AWS Well-Architected Tool のアクション、リソース、および条件キー

AWS Well-Architected Tool (サービスプレフィックス: `wellarchitected`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Well-Architected Tool で定義されるアクション
- AWS Well-Architected Tool で定義されるリソースタイプ
- AWS Well-Architected Tool の条件キー

AWS Well-Architected Tool で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーショ

ンへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateLenses	指定されたワークロードにレンズを関連付けるアクセス許可を付与します	書き込み	workload*		
				aws:ResourceTag/${TagKey}	
AssociateProfiles	指定されたワークロードにプロファイルを関連付ける許可を付与	書き込み	workload*		
				aws:ResourceTag/${TagKey}	
ConfigureIntegration [アクセス許可のみ]	統合を設定する許可を付与する	書き込み			
CreateLensShare	レンズの所有者に、他の AWS アカウントや IAM ユーザーと共有するためのアクセス許可を付与します	書き込み	lens*		
				aws:ResourceTag/${TagKey}	
CreateLensVersion	新しいレンズバージョンをを作成する許可を付与します。	書き込み	lens*		
				aws:ResourceTag/${TagKey}	
CreateMilestone	指定されたワークロードの新しいマイルストーンを作成する許可を付与	書き込み	workload*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateProfile	新しいプロファイルを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfileShare	プロファイルの所有者に、他の AWS アカウントや IAM ユーザーと共有するためのアクセス許可を付与します	書き込み	profile*		
				aws:ResourceTag/${TagKey}	
CreateReviewTemplate	新しいレビューテンプレートを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTemplateShare	レビューテンプレートの所有者に、他の AWS アカウントや IAM ユーザーと共有するためのアクセス許可を付与します	書き込み	review-template*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateWorkload	新しいワークロードを作成する許可を付与	書き込み		aws:RequestTag/${TagKey} aws:TagKeys wellarchitected:JiraProjectKey	
CreateWorkloadShare	別のアカウントとワークロードを共有する許可を付与	書き込み	workload*		
				aws:ResourceTag/${TagKey}	
DeleteLens	レンズを削除するアクセス許可を付与します。	書き込み	lens*		
				aws:ResourceTag/${TagKey}	
DeleteLensShare	既存のレンズ共有を削除する許可を付与します。	書き込み	lens*		
				aws:ResourceTag/${TagKey}	
DeleteProfile	プロファイルを削除する権限を付与します	書き込み	profile*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteProfileShare	既存のプロファイル共有を削除する許可を付与	書き込み	profile*		
				aws:ResourceTag/${TagKey}	
DeleteReviewTemplate	既存のレビューテンプレートを削除する許可を付与	書き込み	review-template*		
				aws:ResourceTag/${TagKey}	
DeleteTemplateShare	既存のレビューテンプレート共有を削除する許可を付与	書き込み	review-template*		
				aws:ResourceTag/${TagKey}	
DeleteWorkload	既存の関連付けを削除する許可を付与。	書き込み	workload*		
				aws:ResourceTag/${TagKey}	
DeleteWorkloadShare	既存のワークロード共有を削除する許可を付与	書き込み	workload*		
				aws:ResourceTag/${TagKey}	
DisassociateLenses	指定されたワークロードからレンズの関連付けを解除する許可を付与	書き込み	workload*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
DisassociateProfiles	指定されたワークロードからプロファイルの関連付けを解除する許可を付与	書き込み	workload*		
				aws:ResourceTag/${TagKey}	
ExportLens	既存のレンズをエクスポートをする許可を付与します。	読み込み	lens*		
				aws:ResourceTag/${TagKey}	
GetAnswer	指定されたレンズレビューから指定された回答を取得する許可を付与	読み取り	workload*		
				aws:ResourceTag/${TagKey}	
GetConsolidatedReport	このアカウントにおいて、統合レポートのメトリクス取得、または統合レポートの PDF 生成を行う許可を付与	読み取り			
GetGlobalSettings	アカウントのすべての設定を取得する許可を付与する	読み取り			
GetLens	既存のレンズを取得する許可を付与します。	読み込み	lens*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetLensReview	指定されたワークロードの指定されたレンズレビューを取得する許可を付与	読み込み	workload*		
				aws:ResourceTag/${TagKey}	
GetLensReviewReport	指定されたレンズレビューのレポートを取得する許可を付与	読み込み	workload*		
				aws:ResourceTag/${TagKey}	
GetLensVersionDifference	指定されたレンズバージョンと利用可能な最新のレンズバージョンの違いを取得する許可を付与	読み込み	lens*		
				aws:ResourceTag/${TagKey}	
GetMilestone	指定されたワークロードの指定されたマイルストーンを取得する許可を付与	読み取り	workload*		
				aws:ResourceTag/${TagKey}	
GetProfile	指定されたプロファイルを取得する許可を付与	読み取り	profile*		
				aws:ResourceTag/${TagKey}	
GetProfileTemplate	指定されたプロファイルのテンプレートを取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetReviewTemplate	指定されたレビューテンプレートを取得する許可を付与	読み取り	review-template*		
				aws:ResourceTag/${TagKey}	
GetReviewTemplateAnswer	指定されたレビューテンプレートレンズレビューから指定された回答を取得する許可を付与	読み取り	review-template*		
				aws:ResourceTag/${TagKey}	
GetReviewTemplateLensReview	指定されたレビューテンプレートの指定されたレンズレビューを取得する許可を付与	読み取り	review-template*		
				aws:ResourceTag/${TagKey}	
GetWorkload	指定されたワークロードを取得する許可を付与	読み込み	workload*		
				aws:ResourceTag/${TagKey}	
ImportLens	新しいレンズをインポートする許可を付与します。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListAnswers	指定されたレンズレビューからの回答を一覧表示する許可を付与	リスト	workload*		
				aws:ResourceTag/${TagKey}	
ListCheckDetails	ワークロードのチェック詳細を一覧表示する許可を付与	リスト	workload*		
				aws:ResourceTag/${TagKey}	
ListCheckSummaries	ワークロードのチェック概要を一覧表示する許可を付与	リスト	workload*		
				aws:ResourceTag/${TagKey}	
ListLensReviewImprovements	指定されたレンズレビューの改善を一覧表示する許可を付与	リスト	workload*		
				aws:ResourceTag/${TagKey}	
ListLensReviews	指定されたワークロードのレンズレビューを一覧表示する許可を付与	リスト	workload*		
				aws:ResourceTag/${TagKey}	
ListLensShares	レンズ用に作成されたすべての共有を一覧表示するアクセス許可を付与します。	リスト	lens*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListLenses	このアカウントで利用可能なレンズの一覧表示を許可します	リスト			
ListMilestones	指定されたワークロードのマイルストーンを一覧表示する許可を付与	リスト	workload*		
				aws:ResourceTag/${TagKey}	
ListNotifications	アカウントまたは指定されたリソースに関連する通知を一覧表示する許可を付与	リスト			
ListProfileNotifications	指定されたリソースに関連するプロファイル通知を一覧表示する許可を付与	リスト			
ListProfileShares	プロファイル用に作成されたすべての共有を一覧表示する許可を付与	リスト	profile*		
				aws:ResourceTag/${TagKey}	
ListProfiles	このアカウントで利用可能なプロファイルを一覧表示する許可を付与	リスト			
ListReviewTemplateAnswers	指定されたレビューテンプレートレンズレビューからの回答を一覧表示する許可を付与	リスト	review-template*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListReviewTemplates	このアカウントで利用可能なレビューテンプレートを一覧表示する許可を付与	リスト			
ListShareInvitations	指定されたアカウントまたはユーザーのワークロード共有招待を一覧表示する許可を付与	リスト			
ListTagsForResource	Well-Architected リソース用のタグを一覧表示するアクセス権限を付与します	読み取り	lens		
			profile		
			review-template		
			workload		
				aws:ResourceTag/${TagKey}	
ListTemplateShares	レビューテンプレート用に作成されたすべての共有を一覧表示する許可を付与	リスト	review-template*		
				aws:ResourceTag/${TagKey}	
ListWorkloadShares	指定されたワークロードのワークロード共有を一覧表示する許可を付与	リスト	workload*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListWorkloads	このアカウント内のワークロードを一覧表示する許可を付与	リスト			
TagResource	Well-Architected リソースにタグを付けるアクセス権限を付与します	タグ付け	lens		
			profile		
			review-template		
			workload		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Well-Architected リソースのタグを解除するアクセス権限を付与します	タグ付け	lens		
			profile		
			review-template		
			workload		
				aws:TagKeys	
UpdateAnswer	指定された回答のプロパティを更新する許可を付与	書き込み	workload*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
UpdateGlobalSettings	アカウントのすべての設定を管理する許可を付与する	書き込み		wellarchitected:JiraProjectKey	
UpdateIntegration	統合のプロパティを更新する許可を付与する	書き込み	workload*		
				aws:ResourceTag/${TagKey}	
UpdateLensReview	指定されたレンズレビューのプロパティを更新する許可を付与	書き込み	workload*		
				aws:ResourceTag/${TagKey}	
UpdateProfile	指定されたプロファイルのプロパティを更新する許可を付与	書き込み	profile*		
				aws:ResourceTag/${TagKey}	
UpdateReviewTemplate	指定されたレビューテンプレートのプロパティを更新する許可を付与	書き込み	review-template*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateReviewTemplateAnswer	指定されたレビューテンプレートの回答のプロパティを更新する許可を付与	書き込み	review-template*		
				aws:ResourceTag/${TagKey}	
UpdateReviewTemplateLensReview	指定されたレビューテンプレートレンズレビューのプロパティを更新する許可を付与	書き込み	review-template*		
				aws:ResourceTag/${TagKey}	
UpdateShareInvitation	指定されたワークロード共有招待のステータスを更新する許可を付与	書き込み			
UpdateWorkload	指定されたワークロードのプロパティを更新する許可を付与	書き込み	workload*		
				aws:ResourceTag/${TagKey} wellarchitected:JiraProjectKey	
UpdateWorkloadShare	指定されたワークロード共有のプロパティを更新する許可を付与する	書き込み	workload*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpgradeLensReview	指定されたレンズレビューをアップグレードして、関連付けられているレンズの最新バージョンを使用するためのアクセス許可を付与します	書き込み	workload*		
				aws:ResourceTag/${TagKey}	
UpgradeProfileVersion	指定されたワークロードをアップグレードして、関連付けられているプロファイルの最新バージョンを使用する許可を付与	書き込み	profile*		
			workload*		
				aws:ResourceTag/${TagKey}	
UpgradeReviewTemplateLensReview	指定されたレビューテンプレートの指定されたレンズレビューを更新する許可を付与	書き込み	review-template*		
				aws:ResourceTag/${TagKey}	

AWS Well-Architected Tool で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
workload	arn:${Partition}:wellarchitected:${Region}:${Account}:workload/${ResourceId}	aws:ResourceTag/${TagKey}
lens	arn:${Partition}:wellarchitected:${Region}:${Account}:lens/${ResourceId}	aws:ResourceTag/${TagKey}
profile	arn:${Partition}:wellarchitected:${Region}:${Account}:profile/${ResourceId}	aws:ResourceTag/${TagKey}
review-template	arn:${Partition}:wellarchitected:${Region}:${Account}:review-template/${ResourceId}	aws:ResourceTag/${TagKey}

AWS Well-Architected Tool の条件キー

AWS Well-Architected Tool では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーおよび値のペアでアクセスをフィルタリングします	String

条件キー	説明	タイプ
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString
wellarchitected:JiraProjectKey	プロジェクトキーでアクセスをフィルタリングする	String

AWS Wickr のアクション、リソース、および条件キー

AWS Wickr (サービスプレフィックス: `wickr`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS Wickr で定義されるアクション
- AWS Wickr で定義されるリソースタイプ
- AWS Wickr の条件キー

AWS Wickr で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateAdminSession	Wickr ネットワークを作成および管理する許可を付与	書き込み	network*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateNetwork	新しい wickr ネットワークを作成するための許可を付与します	書き込み			
DeleteNetwork	Wickr ネットワークの作成と削除の許可を付与する	書き込み			
ListNetworks	Wickr ネットワークを表示する許可を付与	書き込み			
ListTagsForResource	Wickr リソースに適用されたタグを一覧表示するための許可を付与します	読み取り			
TagResource	指定された wickr リソースにタグを追加するための許可を付与します	Tagging	network*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	指定された wickr リソースから指定したタグを解除するための許可を付与します	Tagging	network*		
				aws:TagKeys	
UpdateNetworkDetails	Wickr ネットワークの詳細を更新するための許可を付与します	書き込み	network*		

AWS Wickr で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
network	arn:${Partition}:wickr:${Region}:${Account}:network/${NetworkId}	aws:ResourceTag/${TagKey}

AWS Wickr の条件キー

AWS Wickr は、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグのキーと値でアクセスをフィルター	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエスト内のタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon WorkDocs のアクション、リソース、および条件キー

Amazon WorkDocs (サービスプレフィックス: workdocs) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon WorkDocs で定義されるアクション
- Amazon WorkDocs で定義されるリソースタイプ
- Amazon WorkDocs の条件キー

Amazon WorkDocs で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。ア

クションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AbortDocumentVersionUpload	以前に InitiateDocumentVersionUpload によって開始された、指定されたドキュメントバージョンのアップロードを中止するアクセス権限を付与する	書き込み			
ActivateUser	指定されたユーザーを有効にする許可を付与。アクティブユーザーのみが Amazon WorkDocs にアクセスできます	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AddNotificationPermissions [アクセス許可のみ]	特定の WorkDocs サイトの通知サブスクリプション API を呼び出すことができるプリンシパルを追加する権限を付与する	書き込み			
AddResourcePermissions	指定のフォルダまたはドキュメントに対する一連のアクセス許可を作成する権限を付与する	書き込み			
AddUserToGroup [アクセス許可のみ]	ユーザーをグループに追加する権限を付与する	書き込み			
CheckAlias [アクセス許可のみ]	エイリアスを確認する権限を付与する	読み取り			
CreateComment	指定されたドキュメントバージョンに新しいコメントを追加する権限を付与する	書き込み			
CreateCustomMetadata	指定されたリソースに 1 つ以上のカスタムプロパティを追加する権限を付与する	書き込み			
CreateFolder	指定された名前と親フォルダを使用してフォルダを作成する権限を付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateInstance [アクセス許可のみ]	インスタンスを作成する権限を付与する	書き込み			
CreateLabels	指定されたリソースにラベルを追加する権限を付与する	書き込み			
CreateNotificationSubscription	Amazon SNS 通知を使用するように WorkDocs を設定する権限を付与する	書き込み			
CreateUser	Simple AD ディレクトリまたは Microsoft AD ディレクトリ内にユーザーを作成する権限を付与うする	書き込み			
DeactivateUser	指定されたユーザーを無効化する権限を付与する。これにより、Amazon WorkDocs へのユーザーのアクセス許可が取り消されます	書き込み			
DeleteComment	ドキュメントのバージョンから指定されたコメントを削除する権限を付与する	書き込み			
DeleteCustomMetadata	指定されたリソースからカスタムメタデータを削除する権限を付与する	書き込み			
DeleteDocument	指定されたドキュメントとそれに関連するメタデータを完全に削除する権限を付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteDocumentVersion	指定されたドキュメントのバージョンを削除する許可を付与	書き込み			
DeleteFolder	指定されたフォルダとそのコンテンツを完全に削除する権限を付与する	書き込み			
DeleteFolderContents	指定されたフォルダの内容を削除する権限を付与する	書き込み			
DeleteInstance [アクセス許可のみ]	インスタンスを削除する許可を付与	書き込み			
DeleteLabels	リソースから 1 つ以上のラベルを削除する権限を付与する	書き込み			
DeleteNotificationPermissions [アクセス許可のみ]	特定の WorkDocs サイトの通知サブスクリプション API を呼び出すことができるプリンシパルを削除する権限を付与する	書き込み			
DeleteNotificationSubscription	指定された組織から指定されたサブスクリプションを削除する権限を付与する	書き込み			
DeleteUser	Simple AD ディレクトリまたは Microsoft AD ディレクトリから指定されたユーザーを削除する権限を付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeregisterDirectory [アクセス許可のみ]	ディレクトリの登録を解除する権限を付与する	書き込み			
DescribeActivities	指定された期間内にユーザーアクティビティを取得する権限を付与する	リスト			
DescribeAvailableDirectories [許可のみ]	使用可能なディレクトリを記述する権限を付与する	リスト			
DescribeComments	指定されたドキュメントバージョンのすべてのコメントを一覧表示する権限を付与する	リスト			
DescribeDocumentVersions	指定されたドキュメントのドキュメントバージョンを取得する権限を付与する	リスト			
DescribeFolderContents	指定されたフォルダの内容について、ドキュメントやサブフォルダも含めて説明する権限を付与する	リスト			
DescribeGroups	ユーザーグループを記述する権限を付与する	リスト			
DescribeInstanceExports [許可のみ]	インスタンスのエクスポート履歴を記述する許可を付与する	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeInstances [許可のみ]	インスタンスを記述する権限を付与する	リスト			
DescribeNotificationPermissions [許可のみ]	特定の WorkDocs サイトの通知サブスクリプション API を呼び出すことができるプリンシパルを記述する権限を付与する	リスト			
DescribeNotificationSubscriptions	指定された通知サブスクリプションを一覧表示する権限を付与する	リスト			
DescribeResourcePermissions	指定されたリソースのアクセス許可の説明を表示する権限を付与する	リスト			
DescribeRootFolders	ルートフォルダを記述する権限を付与する	リスト			
DescribeUsers	指定されたユーザーの説明を表示する許可を付与。すべてのユーザーについて説明することも、結果をフィルタリングすることもできます (例えば、ステータスまたは組織などで)	リスト			
DownloadDocumentVersion [許可のみ]	指定されたドキュメントバージョンをダウンロードする権限を付与する	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetCurrentUser	現在のユーザーの詳細を取得する権限を付与する	読み取り			
GetDocument	指定されたドキュメントオブジェクトを取得する権限を付与する	読み取り			
GetDocumentPath	リクエストされたドキュメントのパス情報 (ルートフォルダからの階層) を取得する権限を付与する	読み取り			
GetDocumentVersion	指定されたドキュメントのバージョンメタデータを取得する権限を付与する	読み取り			
GetFolder	指定されたフォルダのメタデータを取得する権限を付与する	読み取り			
GetFolderPath	指定されたフォルダのパス情報 (ルートフォルダからの階層) を取得する権限を付与する	読み取り			
GetGroup [許可のみ]	指定したグループの詳細を取得する権限を付与する	読み取り			
GetResources	リソースのコレクションを取得する権限を付与する	読み取り			
InitiateDocumentVersionUpload	新しいドキュメントオブジェクトとバージョンオブジェクトを作成する権限を付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RegisterDirectory [アクセス許可のみ]	ディレクトリを登録する権限を付与する	書き込み			
RemoveAllResourcePermissions	指定されたリソースからすべてのアクセス許可を削除する権限を付与する	書き込み			
RemoveResourcePermission	指定されたリソースから指定されたプリンシパルのアクセス許可を削除する権限を付与する	書き込み			
RestoreDocumentVersions	指定されたドキュメントのバージョンを復元する許可を付与	書き込み			
SearchResources	リソースのメタデータとコンテンツを検索する許可を付与	リスト			
StartInstanceExport [許可のみ]	インスタンスのエクスポートを開始する許可を付与する	書き込み	organization*		
UpdateDocument	指定されたドキュメントの指定された属性を更新する権限を付与する	書き込み			
UpdateDocumentVersion	ドキュメントバージョンのステータスを有効に変更する権限を付与する	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateFolder	指定されたフォルダの指定された属性を更新する権限を付与する	書き込み			
UpdateInstanceAlias [アクセス許可のみ]	インスタンスエイリアスを更新する権限を付与する	書き込み			
UpdateUser	指定されたユーザーの指定された属性を更新するアクセス許可を付与し、Amazon WorkDocs サイトへの管理者権限を付与または取り消す	書き込み			
UpdateUserAdministrativeSettings [アクセス許可のみ]	ユーザーの管理設定を更新する許可を付与	書き込み			

Amazon WorkDocs で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
organization	arn:${Partition}:workdocs:${Region}:${Account}:organization/${ResourceId}	

Amazon WorkDocs の条件キー

WorkDocs には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon WorkLink のアクション、リソース、および条件キー

Amazon WorkLink (サービスプレフィックス: worklink) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon WorkLink で定義されるアクション
- Amazon WorkLink で定義されるリソースタイプ
- Amazon WorkLink の条件キー

Amazon WorkLink で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateDomain	ドメインを Amazon WorkLink フリートに関連付けるアクセス許可を付与	書き込み	fleet*		
AssociateWebsiteAuthorizationProvider	ウェブサイト認可プロバイダーを Amazon WorkLink フリートに関連付けるアクセス許可を付与	書き込み	fleet*		
AssociateWebsiteCertificateAuthority	ウェブサイト認証機関を Amazon WorkLink フリートに関連付けるアクセス許可を付与	書き込み	fleet*		
CreateFleet	Amazon WorkLink フリートを作成する許可を付与。	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFleet	Amazon WorkLink フリートを削除する許可を付与。	書き込み	fleet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeAuditStreamConfiguration	Amazon WorkLink フリートの監査ストリーム設定を記述する許可を付与。	読み込み	fleet*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeCompanyNetworkConfiguration	Amazon WorkLink フリートの社内ネットワーク設定を記述する許可を付与。	読み込み	fleet*		
DescribeDevice	Amazon WorkLink フリートに関連付けられたデバイスの詳細を記述する許可を付与。	読み込み	fleet*		
DescribeDevicePolicyConfiguration	Amazon WorkLink フリートのデバイスポリシー設定を記述する許可を付与。	読み込み	fleet*		
DescribeDomain	Amazon WorkLink フリートに関連付けられたドメインの詳細を記述する許可を付与。	読み込み	fleet*		
DescribeFleetMetadata	Amazon WorkLink フリートのメタデータを記述する許可を付与。	読み込み	fleet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeIdentityProviderConfiguration	Amazon WorkLink フリートの ID プロバイダー設定を記述する許可を付与。	読み込み	fleet*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeWebsiteCertificateAuthority	Amazon WorkLink フリートに関連付けられたウェブサイト認証機関を記述する許可を付与。	読み込み	fleet*		
DisassociateDomain	Amazon WorkLink フリートからドメインの関連付けを解除する許可を付与。	書き込み	fleet*		
DisassociateWebsiteAuthorizationProvider	Amazon WorkLink フリートからウェブサイト認可プロバイダーの関連付けを解除する許可を付与。	書き込み	fleet*		
DisassociateWebsiteCertificateAuthority	Amazon WorkLink フリートからウェブサイト認証機関の関連付けを解除する許可を付与。	書き込み	fleet*		
ListDevices	Amazon WorkLink フリートに関連付けられたデバイスを一覧表示する許可を付与。	リスト	fleet*		
ListDomains	Amazon WorkLink フリートの関連付けられたドメインを一覧表示する許可を付与。	リスト	fleet*		
ListFleets	アカウントに関連付けられている Amazon WorkLink フリートを一覧表示する許可を付与。	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み込み	fleet*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListWebsiteAuthorizationProviders	Amazon WorkLink フリートのウェブサイト認可プロバイダーを一覧表示する許可を付与。	リスト	fleet*		
ListWebsiteCertificateAuthorities	Amazon WorkLink フリートに関連付けられたウェブサイト認証機関を一覧表示する許可を付与。	リスト	fleet*		
RestoreDomainAccess	Amazon WorkLink フリートに関連付けられたドメインへのアクセスを復元する許可を付与。	書き込み	fleet*		
RevokeDomainAccess	Amazon WorkLink フリートに関連付けられたドメインへのアクセスを取り消すアクセス許可を付与	書き込み	fleet*		
SearchEntity [アクセス許可のみ]	Amazon WorkLink フリートのデバイスを一覧表示するアクセス許可を付与	リスト	fleet*		
SignOutUser	Amazon WorkLink フリートからユーザーをサインアウトする許可を付与。	書き込み	fleet*		
TagResource	リソースに 1 つ以上のタグを追加する許可を付与	タグ付け	fleet*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	リソースから 1 つ以上のタグを削除する許可を付与	タグ付け	fleet*		
				aws:TagKeys	
UpdateAuditStreamConfiguration	Amazon WorkLink フリートの監査ストリーム設定を更新する許可を付与。	書き込み	fleet*		
UpdateCompanyNetworkConfiguration	Amazon WorkLink フリートの社内ネットワーク設定を更新する許可を付与。	書き込み	fleet*		
UpdateDevicePolicyConfiguration	Amazon WorkLink フリートのデバイスポリシー設定を更新する許可を付与。	書き込み	fleet*		
UpdateDomainMetadata	Amazon WorkLink フリートに関連付けられたドメインのメタデータを更新する許可を付与。	書き込み	fleet*		
UpdateFleetMetadata	Amazon WorkLink フリートのメタデータを更新する許可を付与。	書き込み	fleet*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateIdentityProviderConfiguration	Amazon WorkLink フリートの ID プロバイダー設定を更新する許可を付与。	書き込み	fleet*		

Amazon WorkLink で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
fleet	`arn:${Partition}:worklink::${Account}:fleet/${FleetName}`	aws:ResourceTag/${TagKey}

Amazon WorkLink の条件キー

Amazon WorkLink では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエスト内のタグキーと値のペアのプレゼンスに基づいてアクションをフィルタリングします	文字列

条件キー	説明	タイプ
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグキーと値のペアに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエスト内のタグキーのプレゼンスに基づいてアクションをフィルタリングします	ArrayOfString

Amazon WorkMail のアクション、リソース、および条件キー

Amazon WorkMail (サービスプレフィックス: `workmail`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon WorkMail で定義されるアクション
- Amazon WorkMail で定義されるリソースタイプ
- Amazon WorkMail の条件キー

Amazon WorkMail で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの Resource 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの Resource 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AllowVendedLogDeliveryForRe	WorkMail 監査ログの vended log 配信を設定する許可を付与する	書き込み	organization*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
source [アクセス許可のみ]					
AssociateDelegateToResource	メンバー (ユーザーまたはグループ) をリソースの代理人のセットに追加するためのアクセス許可を付与	書き込み	organization*		
AssociateMemberToGroup	メンバー (ユーザーまたはグループ) をグループのセットに追加するためのアクセス許可を付与	書き込み	organization*		
AssumeImpersonationRole	特定の Amazon WorkMail 組織の偽装ロールを引き受ける権限を付与する	書き込み	organization*		
CancelMailboxExportJob	現在実行中のメールボックスエクスポートジョブをキャンセルするためのアクセス許可を付与	書き込み	organization*		
CreateAlias	エイリアスを WorkMail の特定のメンバー (ユーザーまたはグループ) のセットに追加するためのアクセス許可を付与	書き込み	organization*		
CreateAvailabilityConfiguration	特定の Amazon WorkMail 組織とドメインの AvailabilityConfiguration を作成するための許可を付与します	書き込み	organization*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateGroup	RegisterToWorkMail オペレーションを呼び出して WorkMail で使用できるグループを作成するためのアクセス許可を付与	書き込み	organization*		
CreateIdentityCenterApplication	WorkMail 用の Identity Center アプリケーションを作成するアクセス許可を付与します	書き込み			
CreateImpersonationRole	特定の Amazon WorkMail 組織の偽装ロールを作成する権限を付与する	書き込み	organization*		
CreateInboundMailFlowRule [アクセス許可のみ]	組織に送信されるすべての E メールに適用されるインバウンド E メールのフロールールを作成するためのアクセス許可を付与	書き込み	organization*		
CreateMailDomain [アクセス許可のみ]	メールドメインを作成するためのアクセス許可を付与	書き込み	organization*		
CreateMobileDeviceAccessRule	新しいモバイルデバイスアクセスルールを作成するためのアクセス許可を付与	書き込み	organization*		
CreateOrganization	新しい Amazon WorkMail 組織を作成するためのアクセス許可を付与	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreateOutboundMailFlowRule [アクセス許可のみ]	組織から送信されるすべての E メールに適用されるアウトバウンド E メールのフロールールを作成するためのアクセス許可を付与	書き込み	organization*		
CreateResource	新しい WorkMail リソースを作成するためのアクセス許可を付与	書き込み	organization*		
CreateSmtpGateway [アクセス許可のみ]	WorkMail 組織に SMTP ゲートウェイを登録するためのアクセス許可を付与	書き込み	organization*		
CreateUser	ユーザーを作成するためのアクセス許可を付与このアクセス許可は RegisterToWorkMail オペレーションを呼び出して後で有効にできます。	書き込み	organization*		
DeleteAccessControlRule	アクセスコントロールルールを削除するためのアクセス許可を付与	書き込み	organization*		
DeleteAlias	特定のユーザーのエイリアスのセットから 1 つ以上の指定されたエイリアスを削除するためのアクセス許可を付与	書き込み	organization*		
DeleteAvailabilityConfiguration	特定の Amazon WorkMail 組織とドメインの AvailabilityConfiguration を削除するための許可を付与します	書き込み	organization*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteEmailMonitoringConfiguration	組織の E メールモニタリング設定を削除する許可を付与	書き込み	organization*		
DeleteGroup	WorkMail からグループを削除するためのアクセス許可を付与	書き込み	organization*		
DeleteIdentityCenterApplication	WorkMail の Identity Center アプリケーションを削除する許可を付与	書き込み			
DeleteIdentityProviderConfiguration	組織の ID プロバイダー設定を削除するアクセス許可を付与します	書き込み	organization*		
DeleteImpersonationRole	特定の Amazon WorkMail 組織の偽装ロールを削除する権限を付与する	書き込み	organization*		
DeleteInboundMailFlowRule [アクセス許可のみ]	インバウンド E メールのフロールールを削除して、組織に送信された E メールに適用しないようにするためのアクセス許可を付与	書き込み	organization*		
DeleteMailDomain [アクセス許可のみ]	組織から未使用のメールドメインを削除するためのアクセス許可を付与	書き込み	organization*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteMailboxPermissions	メンバー (ユーザーまたはグループ) に付与されたアクセス許可を削除するためのアクセス許可を付与	書き込み	organization*		
DeleteMobileDevice [アクセス許可のみ]	ユーザーからモバイルデバイスを削除するためのアクセス許可を付与	書き込み	organization*		
DeleteMobileDeviceAccessOverride	モバイルデバイスアクセスルールを削除する許可を付与	書き込み	organization*		
DeleteMobileDeviceAccessRule	モバイルデバイスアクセスルールを削除する許可を付与	書き込み	organization*		
DeleteOrganization	Amazon WorkMail 組織と、組織の一部として Amazon WorkMail によって管理されるすべての基盤となる AWS リソースを削除するアクセス許可を付与します	書き込み	organization*		
DeleteOutboundMailFlowRule [アクセス許可のみ]	組織から送信された E メールには適用されないように、アウトバウンドメールのフロールールを削除するためのアクセス許可を付与	書き込み	organization*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeletePersonalAccessToken	個人用アクセストークンを削除するアクセス許可を付与します	書き込み	organization*		
DeleteResource	指定されたリソースを削除するためのアクセス許可を付与	書き込み	organization*		
DeleteRetentionPolicy	指定された組織とポリシー識別子に基づいて保持ポリシーを削除するためのアクセス許可を付与	書き込み	organization*		
DeleteSmtpGateway [アクセス許可のみ]	組織から SMTP ゲートウェイを削除するためのアクセス許可を付与	書き込み	organization*		
DeleteUser	WorkMail およびそれ以降のすべてのシステムからユーザーを削除するためのアクセス許可を付与	書き込み	organization*		
DeliverToMailbox [アクセス許可のみ]	SES MailManager DeliverToMailbox アクションを介して WorkMail 組織に E メールを送信する許可を付与する	書き込み	organization*		
DeregisterFromWorkMail	ユーザー、グループ、またはリソースを WorkMail で使用されなくなったものとしてマークするためのアクセス許可を付与	書き込み	organization*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeregisterMailDomain	組織からメールドメインを削除するためのアクセス許可を付与	書き込み	organization*		
DescribeEmailMonitoringConfiguration	組織の E メールモニタリング設定を取得する許可を付与	読み取り	organization*		
DescribeEntity	エンティティの詳細の読み取りをする許可を付与	読み取り	organization*		
DescribeGroup	グループの詳細を読み取るためのアクセス許可を付与	リスト	organization*		
DescribeIdentityProviderConfiguration	組織の ID プロバイダー設定を読み取るアクセス許可を付与します	読み取り	organization*		
DescribeInboundDmarcSettings	指定された組織について、DMARC ポリシーの設定を読み取るためのアクセス許可を付与	読み込み	organization*		
DescribeInboundMailFlowRule [許可のみ]	組織に設定されたインバウンドメールのフロールールの詳細を読み取るためのアクセス許可を付与	読み込み	organization*		
DescribeMailDomains [許可のみ]	組織に関連付けられているすべてのメールドメインの詳細を表示するためのアクセス許可を付与	リスト	organization*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeMailboxExportJob	メールボックスエクスポートジョブの詳細を取得するためのアクセス許可を付与	読み込み	organization*		
DescribeOrganization	組織の詳細を読み取るためのアクセス許可を付与	リスト	organization*		
DescribeOutboundMailFlowRule [許可のみ]	組織用に構成されたアウトバウンドメールのフロールールの詳細を読み取るためのアクセス許可を付与	読み込み	organization*		
DescribeResource	リソースの詳細を読み取るためのアクセス許可を付与	リスト	organization*		
DescribeSmtpGateway [許可のみ]	組織に登録された SMTP ゲートウェイの詳細を読み取るためのアクセス許可を付与	読み込み	organization*		
DescribeUser	ユーザーの詳細を読み取るためのアクセス許可を付与	リスト	organization*		
DisassociateDelegateFromResource	リソースの代理人のセットからメンバーを削除するためのアクセス許可を付与	書き込み	organization*		
DisassociateMemberFromGroup	グループからメンバーを削除するためのアクセス許可を付与	書き込み	organization*		
EnableMailDomain [アクセス許可のみ]	組織内のメールドメインを有効にするためのアクセス許可を付与	書き込み	organization*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetAccessControlEffect	指定された IPv4 アドレス、アクセスプロトコルアクション、またはユーザー ID に適用されるアクセスコントロールルールの効果を取得する許可を付与	読み込み	organization*		
GetDefaultRetentionPolicy	組織レベルで関連付けられている保持ポリシーを取得するためのアクセス許可を付与	読み取り	organization*		
GetImpersonationRole	特定の Amazon WorkMail 組織の偽装ロールを取得する権限を付与する	読み取り	organization*		
GetImpersonationRoleEffect	特定のユーザーに、偽装ロールに関連するルールの効果を得るための権限を付与する	読み取り	organization*		
GetJournalingRules [許可のみ]	E メールジャーナリング用に設定されたジャーナリングおよびフォールバック E メールアドレスを読み取るためのアクセス許可を付与	読み込み	organization*		
GetMailDomain	組織内の特定のメールドメインの詳細を取得するためのアクセス許可を付与	読み込み	organization*		
GetMailDomainDetails [許可のみ]	メールドメインの詳細を取得するためのアクセス許可を付与	読み取り	organization*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetMailboxDetails	ユーザーのメールボックスの詳細を読み取るためのアクセス許可を付与	読み込み	organization*		
GetMobileDeviceAccessEffect	サンプルアクセスイベントの特定の属性について、モバイルデバイスアクセスルールの効果をシミュレートするためのアクセス許可を付与	読み込み	organization*		
GetMobileDeviceAccessOverride	モバイルデバイスのアクセスオーバーライドを取得するアクセス許可を付与	読み込み	organization*		
GetMobileDeviceDetails [許可のみ]	モバイルデバイスの詳細を取得するためのアクセス許可を付与	読み込み	organization*		
GetMobileDevicesForUser [許可のみ]	ユーザーに関連付けられたモバイルデバイスのリストを取得するためのアクセス許可を付与	読み込み	organization*		
GetMobilePolicyDetails [許可のみ]	組織に関連付けられたモバイルデバイスポリシーの詳細を取得するためのアクセス許可を付与	読み取り	organization*		
GetPersonalAccessTokenMetadata	個人用アクセストークンのメタデータを読み取るアクセス許可を付与します	読み取り	organization*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListAccessControlRules	アクセスコントロールルールを一覧表示するためのアクセス許可を付与	読み込み	organization*		
ListAliases	特定のエンティティに関連付けられたエイリアスを一覧表示するためのアクセス許可を付与	リスト	organization*		
ListAvailabilityConfigurations	特定の Amazon WorkMail 組織のすべての AvailabilityConfiguration を一覧表示するための許可を付与します	読み取り	organization*		
ListGroupMembers	グループのメンバーの概要を読み取るアクセス許可を付与 ユーザーとグループは、グループのメンバーにすることができます	リスト	organization*		
ListGroups	組織のグループの概要を一覧表示するためのアクセス許可を付与	リスト	organization*		
ListGroupsForEntity	エンティティが属するグループを一覧表示する許可を付与	リスト	organization*		
ListImpersonationRoles	特定の Amazon WorkMail 組織の偽装ロールを一覧表示する権限を付与する	リスト	organization*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListInboundMailFlowRules [許可のみ]	組織用に設定されたインバウンドメールのフロールールを一覧表示するためのアクセス許可を付与	リスト	organization*		
ListMailDomains	特定の組織のメールドメインを一覧表示するアクセス許可を付与	リスト	organization*		
ListMailboxExportJobs	メールボックスエクスポートジョブの一覧を表示するためのアクセス許可を付与	リスト	organization*		
ListMailboxPermissions	ユーザー、グループ、またはリソースのメールボックスに関連付けられたメールボックスのアクセス許可を一覧表示するためのアクセス許可を付与	リスト	organization*		
ListMobileDeviceAccessOverrides	モバイルデバイスアクセスオーバーライドを一覧表示するためのアクセス許可を付与	読み込み	organization*		
ListMobileDeviceAccessRules	モバイルデバイスアクセスルールを一覧表示するためのアクセス許可を付与	読み込み	organization*		
ListOrganizations	削除されていない組織を一覧表示するためのアクセス許可を付与	リスト			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListOutboundMailFlowRules [許可のみ]	組織用に設定されたアウトバウンドメールのフロールールを一覧表示するためのアクセス許可を付与	リスト	organization*		
ListPersonalAccessTokens	個人用アクセストークンのメタデータを一覧表示する許可を付与	リスト	organization*		
ListResourceDelegates	リソースに関連付けられた代理人を一覧表示するためのアクセス許可を付与	リスト	organization*		
ListResources	組織のリソースを一覧表示する許可を付与	リスト	organization*		
ListSmtpGateways [許可のみ]	組織に登録されている SMTP ゲートウェイを一覧表示するためのアクセス許可を付与	リスト	organization*		
ListTagsForResource	Amazon WorkMail 組織リソースに適用されたタグを一覧表示する許可を付与	リスト	organization*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListUsers	組織のユーザーを一覧表示する許可を付与	リスト	organization*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
PutAccessControlRule	新しいアクセスコントロールルールを追加するためのアクセス許可を付与	書き込み	organization*		
PutEmailMonitoringConfiguration	組織の E メールモニタリング設定を追加または更新する許可を付与	書き込み	organization*		
PutIdentityProviderConfiguration	組織の ID プロバイダー設定を追加または更新するアクセス許可を付与します	書き込み	organization*		
PutInboundDmarcSettings	指定された組織について、DMARC ポリシーを有効または無効にするためのアクセス許可を付与	書き込み	organization*		
PutMailboxPermissions	ユーザー、グループ、またはリソース用にアクセス許可を設定するためのアクセス許可を付与し、既存のアクセス許可を置き換えます	書き込み	organization*		
PutMobileDeviceAccessOverride	モバイルデバイスアクセスオーバーライドを追加および更新するアクセス許可を付与	書き込み	organization*		
PutRetentionPolicy	保持ポリシーを追加または更新するためのアクセス許可を付与	書き込み	organization*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
RegisterMailDomain	組織内の新しいメールドメインを登録するアクセス許可を付与	書き込み	organization*		
RegisterToWorkMail	メールボックスおよびカレンダー機能を関連付けて、無効になっている既存のユーザー、グループ、またはリソースを登録するためのアクセス許可を付与	書き込み	organization*		
ResetPassword	管理者がユーザーのパスワードのリセットを許可するためのアクセス許可を付与	書き込み	organization*		
SearchMembers [アクセス許可のみ]	メールグループ内の特定のユーザーを検索するためのプレフィックス検索を実行するためのアクセス許可を付与	読み込み	organization*		
SetDefaultMailDomain [許可のみ]	組織のデフォルトのメールドメインを設定するためのアクセス許可を付与	書き込み	organization*		
SetJournalingRules [アクセス許可のみ]	E メールジャーナリング用のジャーナリングとフォールバックの E メールアドレスを設定するためのアクセス許可を付与	書き込み	organization*		
SetMobilePolicyDetails [アクセス許可のみ]	組織に関連付けられたモバイルポリシーの詳細を設定するためのアクセス許可を付与	書き込み	organization*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartMailboxExportJob	新しいメールボックスエクスポートジョブを開始するためのアクセス許可を付与	書き込み	organization*		
TagResource	指定された Amazon WorkMail 組織リソースにタグを付けるためのアクセス許可を付与	Tagging	organization*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestAvailabilityConfiguration	アクセスが許可されているようにするために可用性プロバイダーでテストを実行するための許可を付与します	読み取り	organization*		
TestInboundMailFlowRules [許可のみ]	特定の送信者と受信者の E メールにどのインバウンドルールが適用されるかをテストするためのアクセス許可を付与	書き込み	organization*		
TestOutboundMailFlowRules [アクセス許可のみ]	特定の送信者と受取人が指定された E メールにどのアウトバウンドルールが適用されるかをテストするためのアクセス許可を付与	書き込み	organization*		
UntagResource	指定された Amazon WorkMail 組織リソースのタグを解除する許可を付与	Tagging	organization*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys	
UpdateAvailabilityConfiguration	特定の Amazon WorkMail 組織とドメインの既存の AvailabilityConfiguration を更新するための許可を付与します	書き込み	organization*		
UpdateDefaultMailDomain	組織のデフォルトドメインであるドメインを更新するアクセス許可を付与	書き込み	organization*		
UpdateGroup	グループの詳細を更新する許可を付与	書き込み	organization*		
UpdateImpersonationRole	特定の Amazon WorkMail 組織の既存の偽装ロールを更新する権限を付与する	書き込み	organization*		
UpdateInboundMailFlowRule [アクセス許可のみ]	組織に送信されるすべての E メールに適用されるインバウンド E メールのフロールールの詳細を更新するためのアクセス許可を付与	書き込み	organization*		
UpdateMailboxQuota	ユーザーのメールボックスの最大サイズ (MB 単位) を更新するためのアクセス許可を付与	書き込み	organization*		
UpdateMobileDeviceAccessRule	モバイルデバイスアクセスルールを更新するためのアクセス許可を付与	書き込み	organization*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateOutboundMailFlowRule [アクセス許可のみ]	組織から送信されるすべてのE メールに適用されるアウトバウンド E メールのフロールールの詳細を更新するためのアクセス許可を付与	書き込み	organization*		
UpdatePrimaryEmailAddress	ユーザー、グループ、またはリソースの主要な E メールを更新するためのアクセス許可を付与	書き込み	organization*		
UpdateResource	リソースの詳細を更新するためのアクセス許可を付与	書き込み	organization*		
UpdateSmtpGateway [アクセス許可のみ]	組織に登録されている既存のSMTP ゲートウェイの詳細を更新するためのアクセス許可を付与	書き込み	organization*		
UpdateUser	ユーザーの詳細を更新する許可を付与	書き込み	organization*		
WipeMobileDevice [アクセス許可のみ]	ユーザーのアカウントに関連付けられたモバイルデバイスをリモートワイプするためのアクセス許可を付与	書き込み	organization*		

Amazon WorkMail で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの `Resource` エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
organization	arn:${Partition}:workmail:${Region}:${Account}:organization/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon WorkMail の条件キー

Amazon WorkMail では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	[Type] (タイプ)
aws:RequestTag/${TagKey}	リクエスト内のタグキーおよび値のペアでアクセスをフィルタリングします。	String
aws:ResourceTag/${TagKey}	リソースにアタッチされているタグのキーと値のペアでアクセスをフィルタリングします	String
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon WorkMail Message Flow のアクション、リソース、および条件キー

Amazon WorkMail Message Flow (サービスプレフィックス: workmailmessageflow) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon WorkMail Message Flow で定義されるアクション
- Amazon WorkMail Message Flow で定義されるリソースタイプ
- Amazon WorkMail Message Flow の条件キー

Amazon WorkMail Message Flow で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
GetRawMessageContent	指定されたメッセージ ID の E メールメッセージのコンテンツを読むアクセス許可を付与します。	読み取り	RawMessage*		
PutRawMessageContent	指定されたメッセージ ID の E メールメッセージのコンテンツを更新する許可を付与	書き込み	RawMessage*		

Amazon WorkMail Message Flow で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
RawMessage	arn:${Partition}:workmailmessageflow:${Region}:${Account}:message/${OrganizationId}/${Context}/${MessageId}	

Amazon WorkMail Message Flow の条件キー

WorkMail Message Flow には、ポリシーステートメントの Condition 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

Amazon WorkSpaces のアクション、リソース、および条件キー

Amazon WorkSpaces (サービスプレフィックス: workspaces) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon WorkSpaces で定義されるアクション
- Amazon WorkSpaces で定義されるリソースタイプ
- Amazon WorkSpaces の条件キー

Amazon WorkSpaces で定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアク

ションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AcceptAccountLinkInvitation	WorkSpaces BYOL の同じ設定を共有する他の AWS アカウントからの招待を受け入れるアクセス許可を付与します	書き込み			
AssociateConnectionAlias	接続エイリアスをディレクトリに関連付けるためのアクセス許可を付与します	書き込み	connectionalias*		
			directoryid*		
AssociateIpGroups	IP アクセスコントロールグループをディレクトリに関連付けるためのアクセス許可を付与します	書き込み	directoryid*		
			workspaceipgroup*		
AssociateWorkspaceApplication	WorkSpace とワークスペースアプリケーションを関連付けるアクセス許可を付与します	書き込み	workspaceapplication*		
			workspaceid*		
				aws:ResourceTag/${TagKey}	
AuthorizeIpRules	IP アクセスコントロールグループにルールを追加するためのアクセス許可を付与します	書き込み	workspaceipgroup*		workspaces:UpdateRulesOfIpGroup

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CopyWorkspaceImage	WorkSpace イメージをコピーするためのアクセス許可を付与します	書き込み	workspaceimage*		workspaces:DescribeWorkspaceImages
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAccountLinkInvitation	WorkSpaces BYOL の同じ設定を共有するように他の AWS アカウントを招待するアクセス許可を付与します	書き込み			
CreateConnectClientAddIn	ディレクトリ内に Amazon Connect クライアントアドインを作成する許可を付与	書き込み	directoryid*		
CreateConnectionAlias	クロスリージョンリダイレクトで使用する接続エイリアスを作成するためのアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIpGroup	IP アクセスコントロールグループを作成するためのアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateRootClientCertificate [アクセス許可のみ]	ルートクライアント証明書を作成するアクセス許可を付与します	書き込み	certificateid*		
CreateStandbyWorkspaces	1 つ以上の Standby WorkSpaces を作成する許可を付与	書き込み	directoryid*		
			workspaceid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTags	WorkSpaces リソースのタグを作成するためのアクセス許可を付与します	Tagging		aws:RequestTag/${TagKey} aws:TagKeys	
CreateUpdatedWorkspaceImage	更新された WorkSpace イメージを作成するためのアクセス許可を付与する	書き込み	workspaceimage*		
				aws:RequestTag/${TagKey} aws:TagKeys	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateWorkspaceBundle	WorkSpace バンドルを作成するためのアクセス許可を付与します	書き込み	workspacebundle*		workspaces:CreateTags
			workspaceimage*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaceImage	新しい WorkSpace イメージを作成するアクセス許可を付与	書き込み	workspaceid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaces	1 つ以上の WorkSpaces を作成するためのアクセス許可を付与します	書き込み	directoryid*		
			workspacebundle*		
			workspaceid*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspacesPool	WorkSpaces Pool を作成する許可を付与する	書き込み	directoryid*		
			workspacebundle*		
			workspacespoolid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccountLinkInvitation	WorkSpaces BYOL の同じ設定を共有するために、他の AWS アカウントへの招待を削除するアクセス許可を付与します	書き込み			
DeleteClientBranding	ディレクトリ内の AWS WorkSpaces クライアントのブランドデータを削除するアクセス許可を付与します	書き込み	directoryid*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteConnectClientAddIn	ディレクトリ内で設定された Amazon Connect クライアントアドインを削除する許可を付与	書き込み	directoryid*		
DeleteConnectionAlias	接続エイリアスを削除するためのアクセス許可を付与します	書き込み	connectionalias*		
DeleteIpGroup	IP アクセスコントロールグループを削除するためのアクセス許可を付与します	書き込み	workspaceipgroup*		
DeleteRootClientCertificate [アクセス許可のみ]	ルートクライアント証明書を削除するアクセス許可を付与します	書き込み	certificateid*		
DeleteTags	WorkSpaces リソースからタグを削除するためのアクセス許可を付与します	タグ付け		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteWorkspaceBundle	WorkSpace バンドルを削除するためのアクセス許可を付与します	書き込み	workspacebundle*		
DeleteWorkspaceImage	WorkSpace イメージを削除するためのアクセス許可を付与します	書き込み	workspaceimage*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DeployWorkspaceApplications	保留中のすべてのワークスペースアプリケーションを WorkSpace にデプロイするアクセス許可を付与します	書き込み	workspaceid*		
				aws:ResourceTag/${TagKey}	
DeregisterWorkspaceDirectory	Amazon WorkSpaces との使用からディレクトリを登録解除するためのアクセス許可を付与します	書き込み	directoryid*		
DescribeAccount	WorkSpaces アカウントの Bring-Your-Own-License (BYOL) の設定を取得するためのアクセス許可を付与します	読み込み			
DescribeAccountModifications	WorkSpaces アカウントの Bring-Your-Own-License (BYOL) の設定に対する変更を取得するためのアクセス許可を付与します	読み取り			
DescribeApplicationAssociations	WorkSpace アプリケーションに関連するリソースについての情報を取得するアクセス許可を付与します	リスト	workspaceapplication*		
				aws:ResourceTag/${TagKey}	
DescribeApplications	WorkSpace アプリケーションに関する情報を取得するためのアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeBundleAssociations	WorkSpace バンドルに関連するリソースについての情報を取得するアクセス許可を付与します	リスト	workspacebundle*		
				aws:ResourceTag/${TagKey}	
DescribeClientBranding	ディレクトリ内の AWS WorkSpaces クライアントのブランドデータを取得するアクセス許可を付与します	読み取り	directoryid*		
DescribeClientProperties	WorkSpaces クライアントに関する情報を取得するためのアクセス許可を付与します	リスト	directoryid*		
DescribeConnectClientAddIns	作成された Amazon Connect クライアントアドインのリストを取得する許可を付与	リスト	directoryid*		
DescribeConnectionAliasPermissions	接続エイリアスの所有者が接続エイリアスのために他の AWS アカウントに付与したアクセス許可を取得するアクセス許可を付与します	読み取り	connectionalias*		
DescribeConnectionAliases	クロスリージョンリダイレクトに使用される接続エイリアスを記述するリストを取得するためのアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DescribeConsent [許可のみ]	BYOL の最小要件への同意に関する情報を取得する許可を付与	読み取り			
DescribeCustomWorkspaceImageImport	WorkSpace BYOL イメージのインポートタスクに関する情報を取得する許可を付与	読み取り			
DescribeImageAssociations	WorkSpace イメージに関連するリソースについての情報を取得するアクセス許可を付与します	リスト	workspaceimage*		
				aws:ResourceTag/${TagKey}	
DescribeIpGroups	IP アクセスコントロールグループに関する情報を取得するためのアクセス許可を付与します	読み取り	workspaceipgroup*		
DescribeRootClientCertificates [許可のみ]	ルートクライアント証明書の情報を取得するアクセス許可を付与します	リスト	certificateid*		
DescribeTags	WorkSpaces リソースのタグを記述するためのアクセス許可を付与します	読み取り			
DescribeWorkspaceAssociations	WorkSpace に関連するリソースについての情報を取得するアクセス許可を付与します	リスト	workspaceid*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
DescribeWorkspaceBundles	WorkSpace バンドルに関する情報を取得するためのアクセス許可を付与します	リスト			
DescribeWorkspaceDirectories	WorkSpaces に登録されているディレクトリに関する情報を取得するためのアクセス許可を付与します	読み込み			
DescribeWorkspaceImagePermissions	WorkSpace イメージのアクセス許可に関する情報を取得するためのアクセス許可を付与します	読み込み	workspaceimage*		
DescribeWorkspaceImages	WorkSpace イメージに関する情報を取得するためのアクセス許可を付与します	リスト			
DescribeWorkspaceSnapshots	WorkSpace スナップショットに関する情報を取得するためのアクセス許可を付与します	リスト	workspaceid*		
DescribeWorkspaces	WorkSpaces に関する情報を取得するためのアクセス許可を付与します	リスト			
DescribeWorkspacesConnectionStatus	WorkSpaces の接続状態を取得するためのアクセス許可を付与します	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
DescribeWorkspacesPoolSessions	WorkSpaces Pool のセッションに関する情報を取得する許可を付与する	リスト	workspacespoolid*		
DescribeWorkspacesPools	WorkSpaces Pool に関する情報を取得するための許可を付与する	リスト			
DirectoryAccessManagement [許可のみ]	ワークスペースの管理とプロビジョニング中のディレクトリ管理アクションに対するアクセス許可を付与します	リスト	directoryid*		
DisassociateConnectionAlias	ディレクトリから接続エイリアスの関連付けを解除するためのアクセス許可を付与します	書き込み	connectionalias*		
DisassociateIpGroups	ディレクトリから IP アクセスコントロールグループの関連付けを解除するためのアクセス許可を付与します	書き込み	directoryid*		
			workspaceipgroup*		
DisassociateWorkspaceApplication	WorkSpace からワークスペースアプリケーションの関連付けを解除するアクセス許可を付与します	書き込み	workspaceapplication*		
			workspaceid*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetAccountLink	WorkSpaces BYOL の設定を共有するために、別の AWS アカウントとのリンクを取得するアクセス許可を付与します	読み取り			
ImportClientBranding	ディレクトリ内で AWS WorkSpaces クライアントのブランドデータをインポートするアクセス許可を付与します	書き込み	directoryid*		
ImportCustomWorkspaceImage	Amazon WorkSpaces に Bring-Your-Own-License (BYOL) イメージをインポートするためのアクセス許可を付与します	書き込み			
ImportWorkspaceImage	Amazon WorkSpaces に Bring-Your-Own-License (BYOL) イメージをインポートするためのアクセス許可を付与します	書き込み			ec2:DescribeImages ec2:ModifyImageAttribute
ListAccountLinks	WorkSpaces BYOL の設定を共有する AWS アカウント (複数可) とのリンクを取得するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListAvailableManagementCidrRanges	WorkSpaces アカウントで Bring-Your-Own-License (BYOL) を有効にするために使用できる CIDR 範囲を一覧表示するためのアクセス許可を付与します	リスト			
MigrateWorkspace	WorkSpaces を移行するためのアクセス許可を付与します	書き込み	workspacebundle*		
			workspaceid*		
ModifyAccount	WorkSpaces アカウントの Bring-Your-Own-License (BYOL) の設定を変更するためのアクセス許可を付与します	書き込み			
ModifyCertificateBasedAuthProperties	ディレクトリの証明書に基づいた認可プロパティを変更する許可を付与	書き込み	directoryid*		
ModifyClientProperties	WorkSpaces クライアントのプロパティを変更するためのアクセス許可を付与します	書き込み	directoryid*		
ModifyEndpointEncryptionMode	標準 TLS と FIPS 140-2 検証モードの間で指定されたディレクトリを設定するアクセス許可を付与します	書き込み	directoryid*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ModifySamlProperties	ディレクトリの SAML プロパティを変更するアクセス許可を付与	書き込み	directory id*		
ModifySelfservicePermissions	ユーザーのセルフサービス WorkSpace 管理機能を変更するためのアクセス許可を付与します	権限の管理	directory id*		
ModifyStreamingProperties	ストリーミングプロパティを変更する許可を付与する	書き込み	directory id*		
ModifyWorkspaceAccessProperties	ユーザーが WorkSpaces にアクセスするために使用できるデバイスおよびオペレーティングシステムを指定するためのアクセス許可を付与します	書き込み	directory id*		
ModifyWorkspaceCreationProperties	WorkSpaces の作成に使用するデフォルトのプロパティを変更するためのアクセス許可を付与します	書き込み	directory id*		
ModifyWorkspaceProperties	実行モードや AutoStop 期間を含む WorkSpace プロパティを変更するためのアクセス許可を付与します	書き込み	workspace id*		
ModifyWorkspaceState	WorkSpaces の状態を変更するためのアクセス許可を付与します	書き込み	workspace id*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
RebootWorkspaces	WorkSpaces を再起動するためのアクセス許可を付与します	書き込み	workspaceid*		
RebuildWorkspaces	WorkSpaces を再構築するためのアクセス許可を付与します	書き込み	workspaceid*		
RegisterWorkspaceDirectory	Amazon WorkSpaces で使用するディレクトリを登録するためのアクセス許可を付与します	書き込み	directoryid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RejectAccountLinkInvitation	WorkSpaces BYOL の同じ設定を共有する他の AWS アカウントからの招待を拒否するアクセス許可を付与します	書き込み			
RestoreWorkspace	WorkSpaces を復元するためのアクセス許可を付与します	書き込み	workspaceid*		
RevokeIpRules	IP アクセスコントロールグループからルールを削除するためのアクセス許可を付与します	書き込み	workspaceipgroup*		workspaces:UpdateRulesOfIpGroup
StartWorkspaces	AutoStop WorkSpaces を開始するためのアクセス許可を付与します	書き込み	workspaceid*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartWorkspacesPool	WorkSpaces Pool を開始する許可を付与する	書き込み	workspacespoolid*		
StopWorkspaces	AutoStop WorkSpaces を停止するためのアクセス許可を付与します	書き込み	workspaceid*		
StopWorkspacesPool	WorkSpaces Pool を停止する許可を付与する	書き込み	workspacespoolid*		
Stream	既存の認証情報を使用してサインインし、ワークスペースをストリーミングするアクセス許可をフェデレーションユーザーに付与	書き込み	directoryid*		
				workspaces:userId	
TerminateWorkspaces	WorkSpaces を終了するためのアクセス許可を付与します	書き込み	workspaceid*		
TerminateWorkspacesPool	WorkSpaces Pool を終了する許可を付与する	書き込み	workspacespoolid*		
TerminateWorkspacesPoolSession	WorkSpaces Pool セッションを終了する許可を付与する	書き込み			
UpdateConnectClientAddIn	Amazon Connect クライアントアドインを更新する許可を付与 このアクションは、Amazon Connect クライアントアドインの名前とエンドポイント URL を更新するために使用します	書き込み	directoryid*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateConnectionAliasPermission	接続エイリアスを他のアカウントと共有または共有解除するためのアクセス許可を付与します	権限の管理	connectionalias*		
UpdateConsent [許可のみ]	同意契約を BYOL の最小要件に更新する許可を付与	書き込み			
UpdateRootClientCertificate [アクセス許可のみ]	ルートクライアント証明書を更新する許可を付与	書き込み	certificateid*		
UpdateRulesOfIpGroup	IP アクセスコントロールグループのルールを置き換えるためのアクセス許可を付与します	書き込み	workspaceipgroup*		workspaces:AuthorizeIpRules workspaces:RevokeIpRules
UpdateWorkspaceBundle	WorkSpace バンドルで使用される WorkSpace イメージを更新するためのアクセス許可を付与します。	書き込み	workspacebundle*		
			workspaceimage*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateWorkspaceImagePermission	他のアカウントにイメージをコピーするアクセス許可があるかどうかを指定することにより、WorkSpace イメージを他のアカウントと共有または共有解除するためのアクセス許可を付与します	権限の管理	workspaceimage*		
UpdateWorkspacesPool	WorkSpaces Pool を更新する許可を付与する	書き込み	workspacespoolid*		

Amazon WorkSpaces で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
certificateid	`arn:${Partition}:workspaces:${Region}:${Account}:workspacecertificate/${CertificateId}`	
directoryid	`arn:${Partition}:workspaces:${Region}:${Account}:directory/${DirectoryId}`	aws:ResourceTag/${TagKey}
workspacebundle	`arn:${Partition}:workspaces:${Region}:${Account}:workspacebundle/${BundleId}`	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
workspaceid	arn:${Partition}:workspaces:${Region}:${Account}:workspace/${WorkspaceId}	aws:ResourceTag/${TagKey}
workspaceimage	arn:${Partition}:workspaces:${Region}:${Account}:workspaceimage/${ImageId}	aws:ResourceTag/${TagKey}
workspaceipgroup	arn:${Partition}:workspaces:${Region}:${Account}:workspaceipgroup/${GroupId}	aws:ResourceTag/${TagKey}
workspacespoolid	arn:${Partition}:workspaces:${Region}:${Account}:workspacespool/${PoolId}	aws:ResourceTag/${TagKey}
connectionalias	arn:${Partition}:workspaces:${Region}:${Account}:connectionalias/${ConnectionAliasId}	aws:ResourceTag/${TagKey}
workspaceapplication	arn:${Partition}:workspaces:${Region}:${Account}:workspaceapplication/${WorkSpaceApplicationId}	aws:ResourceTag/${TagKey}

Amazon WorkSpaces の条件キー

Amazon WorkSpaces では、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられているタグに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーに基づいてアクションをフィルタリングします	ArrayOfString
workspaces:userId	Workspaces ユーザーの ID によってアクセスをフィルタリング	String

Amazon WorkSpaces Application Manager のアクション、リソース、および条件キー

Amazon WorkSpaces Application Manager (サービスプレフィックス: wam) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

参照:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon WorkSpaces Application Manager で定義されるアクション
- Amazon WorkSpaces Application Manager で定義されるリソースタイプ
- Amazon WorkSpaces Application Manager の条件キー

Amazon WorkSpaces Application Manager で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AuthenticatePackager [アクセス許可のみ]	Amazon WAM パッケージインスタンスにアプリケーションパッケージカタログへのアクセスを許可します。	Write			

Amazon WorkSpaces Application Manager で定義されるリソースタイプ

Amazon WorkSpaces Application Manager では、IAM ポリシーステートメントの `Resource` 要素でのリソース ARN の指定はサポートされていません。Amazon WorkSpaces Application Manager へのアクセスを許可するには、ポリシーで `"Resource": "*"` を指定します。

Amazon WorkSpaces Application Manager の条件キー

WAM には、ポリシーステートメントの `Condition` 要素で使用できるサービス固有のコンテキストキーはありません。すべてのサービスで使用できるグローバルコンテキストキーのリストについては、AWS 「グローバル条件コンテキストキー」を参照してください。

AWS WorkSpaces マネージドインスタンスのアクション、リソース、および条件キー

AWS WorkSpaces マネージドインスタンス (サービスプレフィックス: `workspaces-instances`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS WorkSpaces マネージドインスタンスで定義されるアクション
- AWS WorkSpaces マネージドインスタンスで定義されるリソースタイプ
- AWS WorkSpaces マネージドインスタンスの条件キー

AWS WorkSpaces マネージドインスタンスで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列

にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
AssociateVolume	ワークスペースマネージドボリュームをアカウントのワークスペースマネージドインスタンスに関連付けるアクセス許可を付与します	書き込み	WorkspaceInstanceId*		ec2:AttachVolume ec2:DescribeVolumes
CreateVolume	アカウントでワークスペースマネージドボリュームを作成するアクセス許可を付与します	書き込み			ec2:CreateVolume
CreateWorkspaceInstance	アカウントにワークスペースマネージドインスタンスを作成するアクセス許可を付与します	書き込み		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeInstances ec2:RunInstances
DeleteVolume	アカウントのワークスペースマネージドボリュームを削除するアクセス許可を付与します	書き込み	VolumeId*		ec2:DeleteVolume ec2:DescribeVolumes
DeleteWorkspaceInstance	アカウント内のワークスペースマネージドインスタンスを	書き込み	WorkspaceInstanceId*		ec2:TerminateInstances

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
	削除するアクセス許可を付与します				
DisassociateVolume	アカウントのワークスペースマネージドインスタンスからワークスペースマネージドボリュームの関連付けを解除するアクセス許可を付与します	書き込み	WorkspaceInstanceId*		ec2:DescribeVolumes ec2:DetachVolume
GetWorkspaceInstance	アカウント内の特定のワークスペースマネージドインスタンスの詳細を取得するアクセス許可を付与します	読み取り	WorkspaceInstanceId*		
ListInstanceTypes	サポートされているすべてのインスタンスタイプを一覧表示するアクセス許可を付与します	リスト			
ListRegions	サポートされているすべてのAWS リージョンを一覧表示するアクセス許可を付与します	リスト			
ListTagsForResource	アカウント内のリソースのユーザータグを一覧表示するアクセス許可を付与します	リスト	WorkspaceInstanceId*		
ListWorkspaceInstances	アカウント内のワークスペースマネージドインスタンスを一覧表示するアクセス許可を付与します	リスト			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
TagResource	アカウントのリソースにユーザータグを追加するアクセス許可を付与します	Tagging	WorkspaceInstanceId*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	アカウントのリソースからユーザータグを削除するアクセス許可を付与します	Tagging	WorkspaceInstanceId*		
				aws:TagKeys	

AWS WorkSpaces マネージドインスタンスで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
WorkspaceInstanceId	arn:${Partition}:workspaces-instances:${Region}:${Account}:workspaceinstance/${WorkspaceInstanceId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
VolumeId	arn:${Partition}:ec2:${Region}:${Account}:volume/${VolumeId}	aws:ResourceTag/${TagKey}

AWS WorkSpaces マネージドインスタンスの条件キー

AWS WorkSpaces マネージドインスタンスでは、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグに基づいてアクションをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられているタグに基づいてアクションをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーに基づいてアクションをフィルタリングします	ArrayOfString

Amazon WorkSpaces Secure Browser のアクション、リソース、および条件キー

Amazon WorkSpaces Secure Browser (サービスプレフィックス: workspaces-web) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon WorkSpaces Secure Browser で定義されるアクション
- Amazon WorkSpaces Secure Browser で定義されるリソースタイプ
- Amazon WorkSpaces Secure Browser の条件キー

Amazon WorkSpaces Secure Browser で定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの Condition 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateBrowserSettings	ブラウザ設定を Web ポータルに関連付けるためのアクセス許可を付与します。	書き込み	browserSettings*		
			portal*		
AssociateDataProtectionSettings	データ保護設定をウェブポータルに関連付けるアクセス許可を付与します	書き込み	dataProtectionSettings*		
			portal*		
AssociateIpAccessSettings	ユーザーの IP アクセス設定をウェブポータルに関連付ける許可を付与	書き込み	ipAccessSettings*		
			portal*		
AssociateNetworkSettings	ネットワーク設定を Web ポータルに関連付けるためのアクセス許可を付与します。	書き込み	networkSettings*		ec2:CreateNetworkInterface

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
					ec2:CreateNetworkInterfacePermission ec2:CreateTags ec2:DeleteNetworkInterface ec2:DeleteNetworkInterfacePermission ec2:ModifyNetworkInterfaceAttribute
			portal*		
AssociateSessionLogger	セッションロガーをウェブポータルに関連付けるアクセス許可を付与します	書き込み	portal*		
			sessionLogger*		
AssociateTrustStore	トラストストアを Web ポータルに関連付けるアクセス許可を付与します。	書き込み	portal*		
			trustStore*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
AssociateUserAccessLoggingSettings	ユーザーのアクセスログ設定をウェブポータルに関連付ける権限を付与する	書き込み	portal*		kinesis:PutRecord kinesis:PutRecords
			userAccessLoggingSettings*		
AssociateUserSettings	ユーザー設定を Web ポータルに関連付ける権限を付与します。	書き込み	portal*		
			userSettings*		
CreateBrowserSettings	ブラウザー設定を作成するためのアクセス許可を付与します。	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey
CreateDataProtectionSettings	データ保護設定を作成するアクセス許可を付与します	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateIdentityProvider	IDプロバイダーを作成するアクセス権限を付与します。	書き込み	identityProvider*		
			portal*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateIpAccessSettings	IP アクセス設定を作成する許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateNetworkSettings	ネットワーク設定を作成するためのアクセス許可を付与します。	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
CreatePortal	ウエブポータルを作成する許可を付与します。	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey
CreateSessionLogger	セッションロガーを作成するアクセス許可を付与します	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateTrustStore	トラストストアを作成するアクセス許可を付与します。	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateUserAccessLoggingSettings	ユーザーのアクセスログ設定を作成する権限を付与する	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
CreateUserSettings	ユーザー設定を作成する許可を付与します。	書き込み		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteBrowserSettings	ブラウザ設定を削除するアクセス許可を付与します。	書き込み	browserSettings*		
DeleteDataProtectionSettings	データ保護設定を削除するアクセス許可を付与します	書き込み	dataProtectionSettings*		
DeleteIdentityProvider	IDプロバイダーを削除する許可を付与します。	書き込み	identityProvider*		
			portal*		
DeleteIpAccessSettings	IP アクセス設定を削除する許可を付与	書き込み	ipAccessSettings*		
DeleteNetworkSettings	ネットワーク 設定を削除する許可を付与します。	書き込み	networkSettings*		
DeletePortal	Webポータルを削除する許可を付与します。	書き込み	portal*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DeleteSessionLogger	セッションロガーを削除するアクセス許可を付与します	書き込み	sessionLogger*		
DeleteTrustStore	トラストストアを削除するアクセス許可を付与します。	書き込み	trustStore*		
DeleteUserAccessLoggingSettings	ユーザーのアクセスログ設定を削除する権限を付与する	書き込み	userAccessLoggingSettings*		
DeleteUserSettings	ユーザー設定を削除する許可を付与します。	書き込み	userSettings*		
DisassociateBrowserSettings	Web ポータルからブラウザ設定の関連付けを解除するアクセス許可を付与します。	書き込み	portal*		
DisassociateDataProtectionSettings	ウェブポータルからデータ保護ログ記録の関連付けを解除するアクセス許可を付与します	書き込み	portal*		
DisassociateIpAccessSettings	ウェブポータルからユーザーの IP アクセスログの関連付けを解除する権限を付与する	書き込み	portal*		
DisassociateNetworkSettings	Web ポータルからネットワーク設定の関連付けを解除するアクセス許可を付与します。	書き込み	portal*		
DisassociateSessionLogger	ウェブポータルからセッションロガーの関連付けを解除するアクセス許可を付与します	書き込み	portal*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
DisassociateTrustStore	Web ポータルからトラストストアの関連付けを解除するアクセス許可を付与します。	書き込み	portal*		
DisassociateUserAccessLoggingSettings	ウェブポータルからユーザーのアクセスログ設定の関連付けを解除する権限を付与する	書き込み	portal*		
DisassociateUserSettings	Web ポータルからユーザー設定の関連付けを解除するアクセス許可を付与します。	書き込み	portal*		
ExpireSession	特定のポータルからセッションを期限切れにする許可を付与する	書き込み	portal*		
GetBrowserSettings	ブラウザ設定に関する詳細を取得するアクセス許可を付与します。	読み取り	browserSettings*		
GetDataProtectionSettings	データ保護設定の詳細を取得するアクセス許可を付与します	読み取り	dataProtectionSettings*		
GetIdentityProvider	ID プロバイダーに関する詳細を取得するアクセス許可を付与します。	読み取り	identityProvider*		
GetIpAccessSettings	IP アクセス設定の詳細を取得する許可を付与	読み取り	ipAccessSettings*		
GetNetworkSettings	ネットワーク設定に関する詳細を取得するアクセス許可を付与します。	読み取り	networkSettings*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetPortal	Web ポータルに関する詳細を取得するアクセス許可を付与します。	読み取り	portal*		
GetPortalServiceProviderMetadata	Web ポータルのサービスプロバイダーのメタデータ情報を取得するアクセス許可を付与します。	読み取り	portal*		
GetSession	ポータルの特定のセッションに関する情報を取得する許可を付与する	読み取り	portal*		
GetSessionLogger	セッションロガーの詳細を取得するアクセス許可を付与します	読み取り	sessionLogger*		
GetTrustStore	トラストストアに関する詳細を取得するアクセス許可を付与します。	読み取り	trustStore*		
GetTrustStoreCertificate	トラストストアから証明書を取得するアクセス許可を付与します。	読み取り	trustStore*		
GetUserAccessLoggingSettings	ユーザーのアクセスログ設定の詳細を取得する権限を付与する	読み取り	userAccessLoggingSettings*		
GetUserSettings	ユーザー設定に関する詳細を取得するアクセス許可を付与します。	読み取り	userSettings*		
ListBrowserSettings	ブラウザ設定を一覧表示するアクセス許可を付与します。	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListDataProtectionSettings	データ保護設定を一覧表示する許可を付与	読み取り			
ListIdentityProviders	ID プロバイダを一覧表示するアクセス許可を付与します。	読み取り	identityProvider*		
ListIpAccessSettings	IP アクセス設定を一覧表示する許可を付与	読み取り			
ListNetworkSettings	ネットワーク設定を一覧表示するアクセス許可を付与します。	読み取り			
ListPortals	Webポータルを一覧表示する許可を付与します。	読み取り			
ListSessionLoggers	セッションロガーを一覧表示するアクセス許可を付与します	読み取り			
ListSessions	オプションのフィルターを使用してポータルのセッションを一覧表示する許可を付与する	読み取り	portal*		
ListTagsForResource	リソースのタグを一覧表示する許可を付与	読み取り			
ListTrustStoreCertificates	トラストストア内の証明書を一覧表示するアクセス許可を付与します。	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
ListTrustStores	トラストストアを一覧表示するアクセス許可を付与します。	読み取り			
ListUserAccessLoggingSettings	ユーザーのアクセスログ設定を一覧表示する権限を付与する	読み取り			
ListUserSettings	ユーザー設定を一覧表示するアクセス許可を付与します。	読み取り			
TagResource	リソースに 1 つ以上のタグを追加する許可を付与	タグ付け	browserSettings		
			dataProtectionSettings		
			identityProvider		
			ipAccessSettings		
			networkSettings		
			portal		
			sessionLogger		
			trustStore		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			userAccessLoggingSettings		
			userSettings		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	リソースから 1 つ以上のタグを削除する許可を付与	Tagging	browserSettings		
			dataProtectionSettings		
			identityProvider		
			ipAccessSettings		
			networkSettings		
			portal		
			sessionLogger		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
			trustStore		
			userAccessLoggingSettings		
			userSettings		
				aws:TagKeys	
UpdateBrowserSettings	ブラウザー設定を更新する許可を付与します。	書き込み	browserSettings*		
UpdateDataProtectionSettings	データ保護設定を更新する許可を付与	書き込み	dataProtectionSettings*		
UpdateIdentityProvider	ID プロバーダーを更新するアクセス権限を付与します。	書き込み	identityProvider*		
			portal*		
UpdateIpAccessSettings	IP アクセス設定を更新する許可を付与	書き込み	ipAccessSettings*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
UpdateNetworkSettings	ネットワーク設定を更新する許可を付与します。	書き込み	networkSettings*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateTags ec2:DeleteNetworkInterface ec2:DeleteNetworkInterfacePermission ec2:ModifyNetworkInterfaceAttribute
UpdatePortal	Webポータルを更新する許可を付与します。	書き込み	portal*		
UpdateSessionLogger	セッションロガーを更新するアクセス許可を付与します	書き込み	sessionLogger*		
UpdateTrustStore	トラストストアを更新するアクセス許可を付与します。	書き込み	trustStore*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateUserAccessLoggingSettings	ユーザーのアクセスログ設定を更新する権限を付与する	書き込み	userAccessLoggingSettings*		kinesis:PutRecord kinesis:PutRecords
UpdateUserSettings	ユーザー設定を更新する許可を付与します。	書き込み	userSettings*		

Amazon WorkSpaces Secure Browser で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
browserSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:browserSettings/${BrowserSettingsId}	aws:ResourceTag/${TagKey}
identityProvider	arn:${Partition}:workspaces-web:${Region}:${Account}:identityProvider/${PortalId}/${IdentityProviderId}	aws:ResourceTag/${TagKey}
networkSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:networkSettings/${NetworkSettingsId}	aws:ResourceTag/${TagKey}

リソースタイプ	ARN	条件キー
portal	arn:${Partition}:workspaces-web:${Region}:${Account}:portal/${PortalId}	aws:ResourceTag/${TagKey}
trustStore	arn:${Partition}:workspaces-web:${Region}:${Account}:trustStore/${TrustStoreId}	aws:ResourceTag/${TagKey}
userSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:userSettings/${UserSettingsId}	aws:ResourceTag/${TagKey}
userAccessLoggingSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:userAccessLoggingSettings/${UserAccessLoggingSettingsId}	aws:ResourceTag/${TagKey}
ipAccessSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:ipAccessSettings/${IpAccessSettingsId}	aws:ResourceTag/${TagKey}
dataProtectionSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:dataProtectionSettings/${DataProtectionSettingsId}	aws:ResourceTag/${TagKey}
sessionLogger	arn:${Partition}:workspaces-web:${Region}:${Account}:sessionLogger/${SessionLoggerId}	aws:ResourceTag/${TagKey}

Amazon WorkSpaces Secure Browser の条件キー

Amazon WorkSpaces Secure Browser は、IAM ポリシーの Condition 要素で使用できる次の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

Amazon WorkSpaces シンクライアントのアクション、リソース、および条件キー

Amazon WorkSpaces シンクライアント (サービスプレフィックス: `thinclient`) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソース、アクション、および条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- Amazon WorkSpaces シンクライアントで定義されるアクション
- Amazon WorkSpaces シンクライアントで定義されるリソースタイプ
- Amazon WorkSpaces シンクライアントの条件キー

Amazon WorkSpaces シンクライアントで定義されるアクション

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
CreateEnvironment	環境を作成するためのアクセス許可を付与	書き込み		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	appstream:DescribeStacks iam:CreateServiceLinkedRole workspaces-web:GetPortal workspaces-web:GetUserSettings workspaces:DescribeWorkspaceDirectories
DeleteDevice	デバイスを削除するためのアクセス許可を付与	書き込み	device*		
				aws:ResourceTag/${TagKey}	
DeleteEnvironment	環境を削除するためのアクセス許可を付与	書き込み	environment*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
DeregisterDevice	デバイスの登録を解除するためのアクセス許可を付与	書き込み	device*		
				aws:ResourceTag/${TagKey}	
GetDevice	デバイスを取得するアクセス許可を付与します	読み取り	device*		
				aws:ResourceTag/${TagKey}	
GetDeviceDetails [許可のみ]	デバイスの詳細を取得するためのアクセス許可を付与	読み取り	device*		
				aws:ResourceTag/${TagKey}	
GetEnvironment	環境の詳細を取得するためのアクセス許可を付与	読み取り	environment*		
				aws:ResourceTag/${TagKey}	
GetSoftwareSet	ソフトウェアセットの詳細を取得するためのアクセス許可を付与	読み取り	softwareset*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
ListDeviceSessions [許可のみ]	デバイスセッションを一覧表示するためのアクセス許可を付与	リスト	device*		
				aws:ResourceTag/${TagKey}	
ListDevices	デバイスを一覧表示する許可を付与	リスト			
ListEnvironments	環境を一覧表示する許可を付与	リスト			
ListSoftwareSets	ソフトウェアセットを一覧表示するためのアクセス許可を付与	リスト			
ListTagsForResource	リソースのタグを一覧表示する許可を付与。	リスト	device		
			environment		
			softwareset		
				aws:ResourceTag/${TagKey}	
TagResource	リソースに 1 つ以上のタグを追加する許可を付与	タグ付け	device		
			environment		
			softwareset		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	リソースから 1 つ以上のタグを削除する許可を付与	Tagging	device		
			environment		
			softwareset		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateDevice	デバイスを更新するためのアクセス許可を付与	書き込み	device*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateEnvironment	環境を更新するためのアクセス許可を付与	書き込み	environment*		appstream:DescribeStacks workspaces-web:GetPortal workspaces-web:GetUserSettings workspaces:DescribeWorkspaceDirectories
				aws:ResourceTag/${TagKey}	
UpdateSoftwareSet	ソフトウェアセットを更新するためのアクセス許可を付与	書き込み	softwareset*		
				aws:ResourceTag/${TagKey}	

Amazon WorkSpaces シンクライアントで定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
environment	arn:${Partition}:thinclient:${Region}:${Account}:environment/${EnvironmentId}	aws:ResourceTag/${TagKey}
device	arn:${Partition}:thinclient:${Region}:${Account}:device/${DeviceId}	aws:ResourceTag/${TagKey}
softwareset	arn:${Partition}:thinclient:${Region}:${Account}:softwareset/${SoftwareSetId}	aws:ResourceTag/${TagKey}

Amazon WorkSpaces シンクライアントの条件キー

Amazon WorkSpaces シンクライアントは、IAM ポリシーの Condition 要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列

条件キー	説明	タイプ
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString

AWS X-Ray のアクション、リソース、および条件キー

AWS X-Ray (サービスプレフィックス: xray) では、IAM アクセス許可ポリシーで使用できるように、以下のサービス固有のリソースやアクション、条件コンテキストキーが用意されています。

リファレンス:

- このサービスを設定する方法について説明します。
- このサービスで使用可能な API オペレーションのリストを表示します。
- IAM アクセス許可ポリシーを使用して、このサービスとそのリソースを保護する方法を学びます。

トピック

- AWS X-Ray によって定義されるアクション
- AWS X-Ray で定義されるリソースタイプ
- AWS X-Ray の条件キー

AWS X-Ray によって定義されるアクション

IAM ポリシーステートメントの Action エレメントでは、以下のアクションを指定できます。ポリシーを使用して、 AWSでオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、場合によっては、1 つのアクションによって複数のオペレーションへのアクセスが制御されます。あるいは、いくつかのオペレーションはいくつかの異なるアクションを必要とします。

Actions テーブルのアクセスレベル列は、アクションの分類方法 (List、Read、Permissions Management、Tagging) を示しています。このように分類することで、ポリシーで使用する際にアクションで付与するアクセスレベルを理解しやすくなります。アクセスレベルの詳細については、ポリシー概要の「アクセスレベル」を参照してください。

[アクション] テーブルの [リソースタイプ] 列は、各アクションがリソースレベルの許可をサポートしているかどうかを示します。この列に値がない場合は、ポリシーステートメントの `Resource` 要素で、ポリシーが適用されるすべてのリソース (「*」) を指定する必要があります。列にリソースタイプが含まれる場合、そのアクションを含むステートメントでそのタイプの ARN を指定できます。アクションで 1 つ以上のリソースが必須となっている場合、呼び出し元には、それらのリソースを伴うアクションを使用するための許可が付与されている必要があります。必須リソースは、アスタリスク (*) でテーブルに示されています。IAM ポリシーの `Resource` 要素でリソースアクセスを制限する場合は、必要なリソースタイプごとに ARN またはパターンを含める必要があります。一部のアクションでは、複数のリソースタイプがサポートされています。リソースタイプがオプション (必須として示されていない) の場合、オプションのリソースタイプのいずれかを使用することを選択できます。

[アクション] テーブルの [条件キー] 列には、ポリシーステートメントの `Condition` 要素で指定できるキーが含まれます。サービスのリソースに関連付けられている条件キーの詳細については、[リソースタイプ] テーブルの [条件キー] 列を参照してください。

> **Note**
>
> リソース条件キーは、リソースタイプテーブルに一覧表示されています。アクションに適用されるリソースタイプへのリンクは、[アクション] テーブルの [リソースタイプ (* 必須)] 列にあります。[リソースタイプ] テーブルのリソースタイプには、[アクション] テーブルのアクションに適用されるリソース条件キーである、[条件キー] 列が含まれています。

以下の表の列の詳細については、「アクションテーブル」を参照してください。

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
BatchGetTraceSummaryById [アク	ID で指定されたトレースリストのメタデータを取得する許可を付与	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
セス許可のみ]					
BatchGetTraces	ID で指定されたトレースのリストを取得する許可を付与。各トレースは、単一のリクエストに由来するセグメントドキュメントのコレクションです。GetTraceSummaries を使用して、トレース ID のリストを取得します。	リスト			
CancelTraceRetrieval	提供された RetrievalToken を使用して StartTraceRetrieval RetrievalToken によって開始された進行中のトレース取得ジョブをキャンセルするアクセス許可を付与します。キャンセルが成功すると、HTTP 200 レスポンスが返されます。	読み取り			
CreateGroup	名前とフィルタ式を使用してグループリソースを作成する許可を付与。	Write	group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSamplingRule	計測機能が搭載されたアプリケーションのサンプリング動作を制御するルールを作成する許可を付与。	Write	sampling-rule*		

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGroup	グループリソースを削除する許可を付与。	書き込み	group*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	リソースポリシーを削除する許可を付与	書き込み		xray:ResourcePolicyName	
DeleteSamplingRule	サンプリングルールを削除する許可を付与。	書き込み	sampling-rule*		
				aws:ResourceTag/${TagKey}	
GetDistinctTraceGraphs [アクセス許可のみ]	1 つ以上の特定のトレース ID の異なるサービスグラフを取得する許可を付与	読み取り			
GetEncryptionConfig	X-Ray データの現在の暗号化設定を取得する許可を付与。	Read			
GetGroup	グループリソースの詳細を取得する許可を付与。	Read	group*		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
				aws:ResourceTag/${TagKey}	
GetGroups	アクティブなグループの詳細をすべて取得する許可を付与。	読み取り			
GetIndexingRules	すべてのインデックス作成ルールを取得するアクセス許可を付与します。インデックス作成ルールは、CloudWatchLogs 送信先を介して取り込まれ、X-Ray によってインデックス付けされるスパンのサーバー側のサンプリングレートを決定するために使用されます。	読み取り			
GetInsight	特定のインサイトの詳細を取得する許可を付与。	Read			
GetInsightEvents	特定のインサイトのイベントを取得する許可を付与。	Read			
GetInsightImpactGraph	特定のインサイトに影響を受けるサービスグラフの一部を取得する許可を付与。	Read			
GetInsightSummaries	オプションのフィルタを使用して、グループおよび時間範囲のすべてのインサイトの概要を取得する許可を付与。	読み取り			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetRetrievedTracesGraph	トランザクション検索 CloudWatch ロググループから指定された RetrievalToken に基づいてトレースのサービスグラフを取得する許可を付与	読み取り			
GetSamplingRules	すべてのサンプリングルールを取得する許可を付与。	Read			
GetSamplingStatisticSummaries	すべてのサンプリングルールについて、最近のサンプリング結果に関する情報を取得する許可を付与。	Read			
GetSamplingTargets	サービスがリクエストのサンプリングに使用しているルールのサンプリングクォータを要求する許可を付与。	Read			
GetServiceGraph	受信リクエストを処理するサービスと、その結果として呼び出されるダウンストリームサービスを記述するドキュメントを取得する許可を付与。	Read			
GetTimeSeriesServiceStatistics	時間間隔にバケット化された特定の時間範囲によって定義されるサービス統計情報の集計を取得する許可を付与。	Read			

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
GetTraceGraph	1 つ以上の特定のトレース ID のサービスグラフを取得する許可を付与。	読み取り			
GetTraceSegmentDestination	PutTraceSegments と OpenTelemetry API に送信されるデータの現在の送信先を取得するアクセス許可を付与します	読み取り			
GetTraceSummaries	オプションのフィルタを使用して、指定したタイムフレームで使用可能なトレースの ID とメタデータを取得する許可を付与。トレース全体を取得するには、トレース ID を BatchGetTraces に渡します。	読み取り			
Link [許可のみ]	モニタリングアカウントに X-Ray リソースを共有する許可を付与	書き込み			
ListResourcePolicies	リソースポリシーを一覧表示する許可を付与	リスト			
ListRetrievedTraces	トランザクション検索 CloudWatch ロググループから特定の RetrievalToken のトレースのリストを取得する許可を付与	リスト			
ListTagsForResource	X-Ray リソースのタグを一覧表示する許可を付与	リスト	group		

アクション	説明	アクセスレベル	リソースタイプ (*必須)	条件キー	依存アクション
			sampling-rule		
PutEncryptionConfig	X-Ray データの暗号化構成を更新する許可を付与。	権限の管理			
PutResourcePolicy	リソースポリシーを作成または更新する許可を付与	書き込み		xray:ResourcePolicyName	
PutSpans	OpenTelemetry スパンを AWS X-Ray にアップロードする許可を付与	書き込み			
PutSpansForIndexing [アクセス許可のみ]	AWS X-Ray にスパンをアップロードしてインデックスを作成する許可を付与	書き込み			
PutTelemetryRecords	AWS X-Ray デーモンテレメトリをサービスに送信する許可を付与	書き込み			
PutTraceSegments	セグメントドキュメントを AWS X-Ray にアップロードするアクセス許可を付与します。X-Ray SDK はセグメントドキュメントを生成し、X-Ray デーモンに送信して、X-Ray デーモンはそれらをバッチ単位でアップロードします。	書き込み			

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
StartTraceRetrieval	指定された時間範囲とトランザクション検索 CloudWatch ロググループの指定されたトレース IDs を使用してトレース取得プロセスを開始するアクセス許可を付与します	読み取り			
TagResource	X-Ray リソースにタグを追加する許可を付与。	タグ付け	group		
			sampling-rule		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	X-Ray リソースからタグを削除する許可を付与。	タグ付け	group		
			sampling-rule		
				aws:TagKeys	
UpdateGroup	グループリソースを更新する許可を付与。	書き込み	group*		
				aws:ResourceTag/${TagKey}	

アクション	説明	アクセスレベル	リソースタイプ (* 必須)	条件キー	依存アクション
UpdateIndexingRule	インデックス作成ルールの設定を変更するアクセス許可を付与します	書き込み			
UpdateSamplingRule	サンプリングルールの構成を変更する許可を付与。	書き込み	sampling-rule*		
				aws:ResourceTag/${TagKey}	
UpdateTraceSegmentDestination	PutTraceSegments と OpenTelemetry API に送信されるデータの送信先を変更するアクセス許可を付与します	書き込み		xray:TraceSegmentDestination	

AWS X-Ray で定義されるリソースタイプ

以下のリソースタイプは、このサービスによって定義され、IAM アクセス許可ポリシーステートメントの Resource エレメントで使用できます。アクションテーブルの各アクションは、そのアクションで指定できるリソースタイプを示しています。リソースタイプは、ポリシーに含めることができる条件キーを定義することもできます。これらのキーは、[リソースタイプ] テーブルの最後の列に表示されます。以下の表の列の詳細については、「リソースタイプテーブル」を参照してください。

リソースタイプ	ARN	条件キー
group	arn:${Partition}:xray:${Region}:${Account}:group/${GroupName}/${Id}	aws:ResourceTag/${TagKey}
sampling-rule	arn:${Partition}:xray:${Region}:${Account}:sampling-rule/${SamplingRuleName}	aws:ResourceTag/${TagKey}

AWS X-Ray の条件キー

AWS X-Ray では、IAM ポリシーの Condition要素で使用できる以下の条件キーを定義します。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。以下の表の列の詳細については、「条件キーテーブル」を参照してください。

すべてのサービスで使用できるグローバル条件キーを表示するには、AWS 「グローバル条件コンテキストキー」を参照してください。

条件キー	説明	タイプ
aws:RequestTag/${TagKey}	リクエストで渡されたタグでアクセスをフィルタリングします	文字列
aws:ResourceTag/${TagKey}	リソースに関連付けられたタグでアクセスをフィルタリングします	文字列
aws:TagKeys	リクエストで渡されたタグキーでアクセスをフィルタリングします	ArrayOfString
xray:ResourcePolicyName	リクエスト内の PolicyName でアクセスをフィルタリングします	String
xray:TraceSegmentDestination	リクエスト内の TraceSegmentDestination タイプでアクセスをフィルタリングします	String

関連リソース

IAM ユーザーガイド の関連情報については、以下の関連リソースを参照してください。

- チュートリアル: はじめてのカスタマー管理ポリシーの作成とアタッチ
- AWS IAM と連携する サービス
- ポリシーの評価論理

プログラムによるアクセスの簡素化された AWS のサービス情報

AWS は、ポリシー管理ワークフローの自動化を合理化するために、JSON 形式のサービスリファレンス情報を提供します。サービスリファレンス情報を使用すると、マシンが読み取り可能なファイル AWS のサービス から で使用可能なアクション、リソース、および条件キーにアクセスできます。サービスリファレンス情報には、IAM アクションの最終アクセス時間情報や IAM Access Analyzer ポリシー生成データなど、認可の詳細以外のメタデータが含まれます。

セキュリティ管理者はガードレールを確立でき、デベロッパーはそれぞれの利用可能なアクション、リソース、および条件キーを特定することで、アプリケーションへの適切なアクセスを確保できます AWS のサービス。 は、 のサービスリファレンス情報 AWS を提供し AWS のサービス 、ポリシー管理ワークフローにメタデータを組み込むことができます。

- IAM ポリシーで使用するアクション、リソース、および条件キーのインベントリについては、 のサービス認可リファレンスページを参照してください AWS のサービス。サービスプレフィックスを共有するサービスのアクション、リソース、および条件キーは、「サービス認可リファレンス」の複数のページに分割できます。
- IAM アクションの最終アクセス時間情報が表示される AWS のサービス および アクションのリストについては、IAM ユーザーガイドの「IAM アクションの最終アクセス時間情報サービスとアクション」を参照してください。
- IAM Access Analyzer がアクションレベルの情報を含むポリシーを生成する AWS のサービス および アクションのリストについては、IAM ユーザーガイドの「IAM Access Analyzer ポリシー生成サービス」を参照してください。

「サービス認可リファレンス」に記載されているコンテンツは、異なる方法で表示されるか、異なるメタデータを含む場合があります。詳細については、「追加のフィールド定義」を参照してください。

> **Note**
>
> サービスリファレンス情報への変更は、サービスのメタデータのリストに反映されるまでに最大 24 時間かかる場合があります。

AWS のサービス リファレンス情報へのアクセス

1. サービス参照情報に移動して、参照情報が利用可能な AWS のサービス のリストにアクセスします。

   次の例は、それぞれのリファレンス情報のサービスと URL の一部リストを示しています。

```
[
    {
        "service": "s3",
        "url": "https://servicereference.us-east-1.amazonaws.com/v1/s3/s3.json"
    },
    {
        "service": "dynamodb",
        "url": "https://servicereference.us-east-1.amazonaws.com/v1/dynamodb/
dynamodb.json"
    },
    …
]
```

2. サービスを選択し、サービスの urlフィールドのサービス情報ページに移動して、サービスのアクション、リソース、および条件キーのリストを表示します。

   次の例は、Amazon S3 のサービスリファレンス情報の一部のリストを示しています。

```
{
    "Name": "s3",
    "Actions": [
        {
            "Name": "GetObject",
            "ActionConditionKeys": [
                "s3:AccessGrantsInstanceArn",
                "s3:AccessPointNetworkOrigin",
                "s3:DataAccessPointAccount",
                "s3:DataAccessPointArn",
                "s3:ExistingObjectTag/key",
                "s3:ResourceAccount",
                "s3:TlsVersion",
                "s3:authType",
                "s3:if-match",
                "s3:if-none-match",
                "s3:signatureAge",
                "s3:signatureversion",
```

```
                "s3:x-amz-content-sha256"
            ],
            "Annotations" : {
                "Properties" : {
                    "IsList" : false,
                    "IsPermissionManagement" : false,
                    "IsTaggingOnly" : false,
                    "IsWrite" : false
                }
            },
            "Resources": [
                {
                    "Name": "object"
                }
            ],
            "SupportedBy" : {
                "IAM Access Analyzer Policy Generation" : false,
                "IAM Action Last Accessed" : false
            }
        },
        {
            "Name": "ListBucket",
            "ActionConditionKeys": [
                "s3:AccessGrantsInstanceArn",
                "s3:AccessPointNetworkOrigin",
                "s3:DataAccessPointAccount",
                "s3:DataAccessPointArn",
                "s3:ResourceAccount",
                "s3:TlsVersion",
                "s3:authType",
                "s3:delimiter",
                "s3:max-keys",
                "s3:prefix",
                "s3:signatureAge",
                "s3:signatureversion",
                "s3:x-amz-content-sha256"
            ],
            "Annotations" : {
                "Properties" : {
                    "IsList" : true,
                    "IsPermissionManagement" : false,
                    "IsTaggingOnly" : false,
                    "IsWrite" : false
                }
```

```
            },
            "Resources": [
                {
                    "Name": "bucket"
                }
            ],
            "SupportedBy" : {
                "IAM Access Analyzer Policy Generation" : false,
                "IAM Action Last Accessed" : false
            }
        },
        ...
    ],
    "ConditionKeys": [
        {
            "Name": "s3:TlsVersion",
            "Types": [
                "Numeric"
            ]
        },
        {
            "Name": "s3:authType",
            "Types": [
                "String"
            ]
        },
        ...
    ],
    "Resources": [
        {
            "Name": "accesspoint",
            "ARNFormats": [
                "arn:${Partition}:s3:${Region}:${Account}:accesspoint/
${AccessPointName}"
            ]
        },
        {
            "Name": "bucket",
            "ARNFormats": [
                "arn:${Partition}:s3:::${BucketName}"
            ]
        }
        ...
    ],
```

```
    "Version": "v1.3"
}
```

3. ポリシーオーサリングワークフローで使用するサービス URL から JSON ファイルをダウンロードします。

追加のフィールド定義

アクションプロパティは、サービスアクションに関する追加のメタデータを提供し、アクセス許可の範囲に基づいて分類するのに役立ちます。これらのプロパティは、各アクションのAnnotationsフィールドにあります。メタデータは 4 つのブール値で構成されます。

- IsList – リソースコンテンツにアクセスせずに、基本的なメタデータを含むリソースを検出して一覧表示するアクセス許可を提供します。

  例 – このプロパティは Amazon S3 ListBucketアクションtrue用であり、ユーザーはオブジェクト自体にアクセスせずにバケットのリストを表示できます。

- IsPermissionManagement – IAM アクセス許可またはアクセス認証情報を変更するアクセス許可を提供します。

  例 – このプロパティは、ほとんどの IAM アクションと AWS Organizations アクション、およびPutBucketPolicyや などの Amazon S3 アクションtrue用ですDeleteBucketPolicy。

- IsTaggingOnly – タグを変更するためのアクセス許可のみを提供します。

  例 – このプロパティは IAM アクションTagRoleと true用ですがUntagRole、このプロパティはタグ付け以外の広範なアクセス許可を提供するためCreateRole、 false用です。

- IsWrite – タグの変更を含むリソースを変更するアクセス許可を提供します。

  例 – このプロパティはCreateBucket、リソースの変更を許可する Amazon S3 アクション 、DeleteBucket、および true用PutObjectです。

> **Note**
>
> これらのプロパティは相互に排他的ではありません。アクションには、複数のプロパティがに設定されている場合がありますtrue。

Amazon S3 の GetObjectアクションと同様にfalse、すべてのプロパティを にすることもできます。これは、 アクションがオブジェクトに対する読み取りアクセス許可のみを付与することを示します。

これらのプロパティを使用して、 サービスのインサイトを生成できます。次の例は、 s3プレフィックスを持つどのアクセス許可がリソースの変更を許可するかを示しています。

```
> curl https://servicereference.us-east-1.amazonaws.com/v1/s3/s3.json | \
    jq '.Actions[] | select(.Annotations.Properties.IsWrite == true) | .Name'

"AssociateAccessGrantsIdentityCenter"
"BypassGovernanceRetention"
"CreateAccessGrant"
"CreateAccessGrantsInstance"
"CreateAccessGrantsLocation"
...
```

次の例は、アクセス許可管理アクションへのアクセスを制限するために使用できるlambdaプレフィックスを持つアクション条件キーを示しています。

```
> curl https://servicereference.us-east-1.amazonaws.com/v1/lambda/lambda.json | \
    jq '.Actions[] | select(.Annotations.Properties.IsPermissionManagement == true) |
 {Name: .Name, ActionConditionKeys: (.ActionConditionKeys // [])}'

{
   "Name": "AddLayerVersionPermission",
    "ActionConditionKeys": []
}
{
    "Name": "AddPermission",
    "ActionConditionKeys": [
        "lambda:FunctionUrlAuthType",
        "lambda:Principal"
    ]
}
{
    "Name": "DisableReplication",
    "ActionConditionKeys": []
}
{
    "Name": "EnableReplication",
```

```
    "ActionConditionKeys": []
}
{
    "Name": "RemoveLayerVersionPermission",
    "ActionConditionKeys": []
}
{
    "Name": "RemovePermission",
    "ActionConditionKeys": [
        "lambda:FunctionUrlAuthType",
        "lambda:Principal"
    ]
}
```

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。