



セキュリティ情報

# AWS Control Catalog



# AWS Control Catalog: セキュリティ情報

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

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

# Table of Contents

|                                      |       |
|--------------------------------------|-------|
| Control Catalog とは .....             | 1     |
| オントロジーの概要 .....                      | 1     |
| Control Catalog へのアクセス .....         | 3     |
| セキュリティ .....                         | 4     |
| データ保護 .....                          | 4     |
| データ暗号化 .....                         | 5     |
| 転送中の暗号化 .....                        | 6     |
| キー管理 .....                           | 6     |
| ネットワーク間トラフィックのプライバシー .....           | 6     |
| Identity and Access Management ..... | 6     |
| 対象者 .....                            | 6     |
| アイデンティティを使用した認証 .....                | 7     |
| ポリシーを使用したアクセスの管理 .....               | 11    |
| Control Catalog と IAM の連携方法 .....    | 13    |
| アイデンティティベースのポリシーの例 .....             | 21    |
| トラブルシューティング .....                    | 24    |
| コンプライアンス検証 .....                     | 26    |
| 耐障害性 .....                           | 27    |
| インフラストラクチャセキュリティ .....               | 28    |
| 設定と脆弱性 .....                         | 28    |
| モニタリング .....                         | 29    |
| CloudTrail ログ .....                  | 29    |
| CloudTrail のコントロールカタログ情報 .....       | 29    |
| Control Catalog ログファイルエントリについて ..... | 30    |
| AWS PrivateLink .....                | 32    |
| 考慮事項 .....                           | 32    |
| インターフェイスエンドポイントの作成 .....             | 32    |
| エンドポイントポリシーを作成する .....               | 33    |
| ドキュメント履歴 .....                       | 35    |
| .....                                | xxxvi |

# Control Catalog とは

Control Catalog セキュリティ情報ガイドへようこそ。Control Catalog は の一部であり AWS Control Tower、複数の AWS サービスのコントロールを一覧表示します。これは、コントロールの統合 AWS カタログです。Control Catalog を使用する AWS Control Tower ように をセットアップする必要はありません。

Control Catalog を使用すると、セキュリティ、コスト、耐久性、オペレーションなど、一般的なユースケースに従ってコントロールを表示できます。

このドキュメントでは、Control Catalog が提供する APIs を使用するときを知っておく必要があるセキュリティおよびコンプライアンス情報を確認できます。

Control Catalog は、コントロールの標準分類システムであるコントロールオントロジーを具体化しています。

## オントロジーの概要

AWS は、コントロール間のマッピングの分類、整理、作成に役立つ標準分類システムを開発しました。このオントロジーは、コントロールを 24 のフレームワークを含む既存および新規の規制基準や、PCI、HIPAA などの規制基準にマッピングするために使用できます。また、NIST や ISO などの業界標準、および Well-Architected フレームワークを含む Amazon 固有のフレームワークにもマッピングされます。

オントロジーには 4 つの重要な側面があります。

- コントロールドメイン、コントロールの目的、一般的なコントロールによるコントロールの分類。オントロジーは、関連するコントロールを次の 3 つのレベルに整理およびグループ化するのに役立ちます。
  - L1: コントロールドメイン、
  - L2: コントロールの目標、
  - L3: 一般的なコントロール。

これらのレベルには、厳密な階層関係があります。つまり、各ドメインには複数のコントロール目標がありますが、各コントロール目標には 1 つの親ドメインが必要です。各コントロール目標には複数の共通コントロールがありますが、各共通コントロールには 1 つの親目標があります。

- 規制標準へのマッピング。オントロジーには、規制または業界標準内の特定の要件を表す標準コントロール (L4) と呼ばれる概念があります。これらの標準コントロールは、これらの特定の要件に対処するのに役立つ共通コントロールにマッピングされます。

例えば、PCI-DSS v3.2.1 などです。ID 4.1 強力な暗号化とセキュリティプロトコルを使用して、オープンなパブリックネットワークを介した送信中に機密性の高いカード所有者データを保護します。NIST 800.53.r5 ID SC-16 セキュリティおよびプライバシー属性の送信は 2 つの標準コントロールであり、どちらも転送中の暗号化データにマッピングされます。一般的なコントロール。

- コントロールの実装とコントロールの証拠。オントロジーには、コントロール実装 (L6) の概念があり、コントロール AWS、AWS Security Hub チェック、AWS Config ルールなどの特定の AWS Control Tower コントロール実装、またはプロセスガイダンス AWS などの外部の非技術的な実装を表すことができます。コントロール証拠 (L7) の別の概念は、サードパーティーのツール AWS Audit Manager、またはお客様自身によるコントロールの証拠として使用できるデータソースを表します。これらの証拠ソースは、AWS CloudTrail イベント、API コールログ、AWS Config ルール評価結果などの AWS ソースである可能性があります。または、顧客ドキュメントなどの外部ソースである場合もあります。
- Core コントロール (L5) の概念。Core コントロールは、すべてのコントロール実装 (L6)、対応する証拠ソース (L7)、関連する標準コントロール (L4)、共通コントロール (L3) を 1 つの包括的なオブジェクトに統合するマッピングレイヤーです。Core コントロールは、コントロール自体よりもマッピングドキュメントです。これは、コントロール X に関連するすべての情報を表示するという質問に答えるのに役立ちます。各コアコントロールには、複数のコントロール実装 (L6) と複数の証拠ソース (L7) を含めることができます。

要約すると、AWS コントロールカタログオントロジーには 7 つのレイヤーが含まれています。3 つは階層分類レイヤー (コントロールドメイン、コントロール目標、共通コントロール) です。もう 1 つのレイヤー (標準コントロール) では、規制または業界標準の要件について説明します。マッピングレイヤー (コアコントロール) は、特定のリソースタイプのコントロール結果を記述します。2 つのレイヤー (コントロール実装、コントロール証拠) は、特定のコントロール実装と証拠ソースを記述します。

このオントロジーは、何百人もの顧客とコンプライアンス監査を行った経験に基づいて、認定監査人の AWS チームによって設計されました。コントロールドメイン、コントロール目標、一般的なコントロール、標準コントロール (L1~L4) の概念は、業界全体で使用されています。これらは、一般的な業界パターンと NIST レコメンデーションに一致します。残りの 3 つのレイヤー (L5-L7) は、リソースタイプやマネージドコントロールなどの既存の AWS 概念に基づいて設計されました。

# Control Catalog へのアクセス

Control Catalog は、コンソールと Control Catalog アプリケーションプログラミングインターフェイス (API) から使用できます。この API は、AWS 顧客として利用可能な一般的なコントロールと関連するメタデータを特定してフィルタリングするプログラムによる方法を提供します。詳細については、「[Control Catalog API Reference](#)」を参照してください。

# Control Catalog のセキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、AWS お客様とお客様の間の責任共有です。[責任共有モデル](#)では、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ – AWS は、AWS のサービス で実行されるインフラストラクチャを保護する責任を担います AWS クラウド。は、お客様が安全に使用できるサービス AWS も提供します。サードパーティーの監査者は、[AWS コンプライアンスプログラム](#)コンプライアンスプログラムの一環として、当社のセキュリティの有効性を定期的にテストおよび検証。Control Catalog に適用されるコンプライアンスプログラムの詳細については、「コンプライアンス[AWS プログラムによる対象範囲内のサービスコンプライアンス](#)」を参照してください。
- クラウド内のセキュリティ – お客様の責任は、使用する によって決まり AWS のサービス ます。また、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、Control Catalog を使用する際の責任共有モデルの適用方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために Control Catalog を設定する方法を示します。また、Control Catalog; リソースのモニタリングと保護 AWS のサービス に役立つ他の の使用方法についても説明します。

## トピック

- [Control Catalog でのデータ保護](#)
- [Control Catalog の Identity and Access Management](#)
- [Control Catalog のコンプライアンス検証](#)
- [Control Catalog の耐障害性](#)
- [Control Catalog のインフラストラクチャセキュリティ](#)

## Control Catalog でのデータ保護

責任 AWS [共有モデル](#)、AWS Control Catalog でのデータ保護に適用されます。このモデルで説明されているように、AWS はすべての を実行するグローバルインフラストラクチャを保護する責任が

あります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「AWS のサービス」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、[データプライバシーに関するよくある質問](#)を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された [AWS 責任共有モデルおよび GDPR](#) のブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント、AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします：

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- を使用して API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「AWS CloudTrail ユーザーガイド」の[CloudTrail 証跡の使用](#)を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「[連邦情報処理規格 \(FIPS\) 140-3](#)」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、または SDK を使用して AWS Control Catalog AWS CLI または他の AWS のサービスを使用する場合も同様です。AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

## データ暗号化

AWS Control Catalog は顧客データを保存しません。

## 保管中の暗号化

AWS Control Catalog は顧客データを暗号化しません。AWS Control Catalog によって保持または保持される顧客データがないため、保管時の暗号化に関する特定のガイドラインはありません。

## 転送中の暗号化

AWS Control Catalog は顧客データを暗号化しません。AWS Control Catalog によって機密データが交換または保持されないため、転送中の暗号化に関する特定のガイドラインはありません。

## キー管理

暗号化キー管理は AWS Control Catalog には適用されません。

## ネットワーク間トラフィックのプライバシー

ネットワーク間トラフィックのプライバシーは、AWS Control Catalog には適用されません。

# Control Catalog の Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS Control Catalog リソースの使用を許可する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

### トピック

- [対象者](#)
- [アイデンティティを使用した認証](#)
- [ポリシーを使用したアクセスの管理](#)
- [Control Catalog と IAM の連携方法](#)
- [Control Catalog のアイデンティティベースのポリシーの例](#)
- [Control Catalog のアイデンティティとアクセスのトラブルシューティング](#)

## 対象者

AWS Identity and Access Management (IAM) の使用 방법은、AWS Control Catalog で行う作業によって異なります。

サービスユーザー – AWS Control Catalog サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が提供されます。さらに多くの AWS Control Catalog 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。AWS Control Catalog の機能にアクセスできない場合は、「」を参照してください[Control Catalog のアイデンティティとアクセスのトラブルシューティング](#)。

サービス管理者 – 社内の AWS Control Catalog リソースを担当している場合は、通常、AWS Control Catalog へのフルアクセスがあります。サービスユーザーがどの AWS Control Catalog 機能とリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。AWS Control Catalog で IAM を使用する方法の詳細については、「」を参照してください[Control Catalog と IAM の連携方法](#)。

IAM 管理者 – IAM 管理者は、AWS Control Catalog へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できる AWS Control Catalog アイデンティティベースのポリシーの例を表示するには、「」を参照してください[Control Catalog のアイデンティティベースのポリシーの例](#)。

## アイデンティティを使用した認証

認証は、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けることによって、認証 ( にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。AWS IAM Identity Center ( IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook 認証情報は、フェデレーション ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「AWS サインイン ユーザーガイド」の「[へのサインイン AWS アカウント](#)方法」を参照してください。

AWS プログラムで にアクセスする場合、 はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストを暗号化して署名します。AWS ツールを使用しない場合は、自分でリクエストに署名する必要があります。リクエストに自分

で署名する推奨方法の使用については、「IAM ユーザーガイド」の「[API リクエストに対するAWS Signature Version 4](#)」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。たとえば、では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用する AWS ことをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「[多要素認証](#)」および「IAM ユーザーガイド」の「[IAM のAWS 多要素認証](#)」を参照してください。

## AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「[ルートユーザー認証情報が必要なタスク](#)」を参照してください。

## フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、ID プロバイダーとのフェデレーションを使用して一時的な認証情報 AWS のサービス を使用して にアクセスすることを要求します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、アイデンティティセンターディレクトリ、または ID ソースを介して提供された認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID がアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成するか、独自の ID ソースのユーザーとグループのセットに接続して同期し、すべての AWS アカウント とアプリケーションで使用できます。IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「[What is IAM Identity Center?](#)」(IAM Identity Center とは) を参照してください。

## IAM ユーザーとグループ

[IAM ユーザー](#)は、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内の ID です。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保

有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「[長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする](#)」を参照してください。

[IAM グループ](#)は、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「[IAM ユーザーに関するユースケース](#)」を参照してください。

## IAM ロール

[IAM ロール](#)は、特定のアクセス許可 AWS アカウント を持つ 内の ID です。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。で IAM ロールを一時的に引き受けるには AWS Management Console、[ユーザーから IAM ロール \(コンソール\) に切り替える](#)ことができます。ロールを引き受けるには、または AWS API オペレーションを AWS CLI 呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「[ロールを引き受けるための各種方法](#)」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス - フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールについては、「IAM ユーザーガイド」の「[サードパーティー ID プロバイダー \(フェデレーション\) 用のロールを作成する](#)」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「[Permission sets](#)」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。

- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、(プロキシとしてロールを使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「[IAM でのクロスアカウントのリソースへのアクセス](#)」を参照してください。
- クロスサービスアクセス — 一部の は他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
- 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用してアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービスへのリクエストをリクエストする と組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「[転送アクセスセッション](#)」を参照してください。
- サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける [IAM ロール](#)です。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、「IAM ユーザーガイド」の「[AWS のサービスに許可を委任するロールを作成する](#)」を参照してください。
- サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。
- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 インスタンスに AWS ロールを割り当て、そのすべてのアプリケーションでできるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロ

ファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「[Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する](#)」を参照してください。

## ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは AWS、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「[JSON ポリシー概要](#)」を参照してください。

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースに必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、iam:GetRole アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、AWS Management Console、AWS CLI または AWS API からロール情報を取得できます。

### アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「[カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する](#)」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、AWS 管理ポリシーとカスタマー管理ポリシー

が含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「[管理ポリシーとインラインポリシーのいずれかを選択する](#)」を参照してください。

## リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、[プリンシパルを指定する](#)必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、またはを含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

## アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、および Amazon VPC は AWS WAF、ACLs。ACL の詳細については、「Amazon Simple Storage Service デベロッパーガイド」の「[アクセスコントロールリスト \(ACL\) の概要](#)」を参照してください。

## その他のポリシータイプ

AWS は、一般的でない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- **アクセス許可の境界** - アクセス許可の境界は、アイデンティティベースポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。Principal フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。

す。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「[IAM エンティティのアクセス許可の境界](#)」を参照してください。

- サービスコントロールポリシー (SCPs) – SCPsは、 の組織または組織単位 (OU) の最大アクセス許可を指定する JSON ポリシーです AWS Organizations。AWS Organizations は、ビジネスが所有する複数の AWS アカウント をグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「[サービスコントロールポリシー \(SCP\)](#)」を参照してください。
- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースのアクセス許可を制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。RCP をサポートする のリストを含む Organizations と RCP の詳細については、AWS Organizations RCPs「[リソースコントロールポリシー \(RCPs\)](#)」を参照してください。AWS のサービス
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「[セッションポリシー](#)」を参照してください。

## 複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「[ポリシー評価ロジック](#)」を参照してください。

## Control Catalog と IAM の連携方法

IAM を使用して AWS Control Catalog へのアクセスを管理する前に、AWS Control Catalog で使用できる IAM 機能を確認してください。

## Control Catalog で使用できる IAM 機能

| IAM 機能                          | AWS Control Catalog のサポート |
|---------------------------------|---------------------------|
| <a href="#">アイデンティティベースポリシー</a> | はい                        |
| <a href="#">リソースベースのポリシー</a>    | いいえ                       |
| <a href="#">ポリシーアクション</a>       | はい                        |
| <a href="#">ポリシーリソース</a>        | あり                        |
| <a href="#">ポリシー条件キー</a>        | Yes                       |
| <a href="#">ACL</a>             | いいえ                       |
| <a href="#">ABAC (ポリシー内のタグ)</a> | いいえ                       |
| <a href="#">一時的な認証情報</a>        | はい                        |
| <a href="#">プリンシパル権限</a>        | いいえ                       |
| <a href="#">サービスロール</a>         | いいえ                       |
| <a href="#">サービスリンクロール</a>      | いいえ                       |

AWS Control Catalog およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要については、「IAM ユーザーガイド」の[AWS「IAM と連携する のサービス」](#)を参照してください。

## AWS Control Catalog のアイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。ID ベースのポリシーの作成方法については、「IAM ユーザーガイド」の「[カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する](#)」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されている

ユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで利用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「[IAM JSON ポリシーの要素のリファレンス](#)」を参照してください。

## AWS Control Catalog のアイデンティティベースのポリシーの例

AWS Control Catalog のアイデンティティベースのポリシーの例については、「」を参照してください [Control Catalog のアイデンティティベースのポリシーの例](#)。

## AWS Control Catalog 内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、[プリンシパルを指定する](#) 必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、「IAM ユーザーガイド」の「[IAM でのクロスアカウントリソースアクセス](#)」を参照してください。

## AWS Control Catalog のポリシーアクション

ポリシーアクションのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの Action 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは依存アクションと呼ばれます。

このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

AWS Control Catalog アクションのリストを確認するには、「サービス認可リファレンス」の「[AWS Control Catalog で定義されるアクション](#)」を参照してください。

AWS Control Catalog のポリシーアクションは、アクションの前に次のプレフィックスを使用します。

```
controlcatalog
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [  
    "controlcatalog:ListCommonControls",  
    "controlcatalog:ListDomains"  
]
```

ワイルドカード \* を使用して複数のアクションを指定することができます。例えば、List という単語で始まるすべてのアクションを指定するには、次のアクションを含めます。

```
"Action": "controlcatalog:List*"
```

AWS Control Catalog のアイデンティティベースのポリシーの例については、「」を参照してください [Control Catalog のアイデンティティベースのポリシーの例](#)。

## AWS Control Catalog のポリシーリソース

ポリシーリソースのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Resource JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ステートメントにはResource または NotResource 要素を含める必要があります。ベストプラクティスとして、[Amazon リソースネーム \(ARN\)](#) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (\*) を使用します。

```
"Resource": "*" 
```

AWS Control Catalog リソースタイプとその ARNs [「AWS Control Catalog で定義されるリソース」](#) を参照してください。各リソースの ARN を指定できるアクションについては、[「AWS Control Catalog で定義されるアクション」](#) を参照してください。

AWS Control Catalog ドメインの Amazon リソースネーム (ARN) 形式は次のとおりです。

```
arn:${Partition}:controlcatalog:::domain/${domainId}
```

AWS Control Catalog の目標の ARN 形式は次のとおりです。

```
arn:${Partition}:controlcatalog:::objective/${objectiveId}
```

AWS Control Catalog の共通コントロールには、次の ARN 形式があります。

```
arn:${Partition}:controlcatalog:::commonControl/${commonControlId}
```

ARN の形式の詳細については、[「Amazon リソースネーム \(ARN\)」](#) を参照してください。

たとえば、ステートメントで i-1234567890abcdef0 ドメインを指定するには、次の ARN を使用します。

```
"Resource": "arn:aws:controlcatalog:::domain/i-1234567890abcdef0" 
```

特定のアカウントに属するすべてのインスタンスを指定するには、ワイルドカード \* を使用します。

```
"Resource": "arn:aws:controlcatalog:::domain/*" 
```

リソースを作成するためのアクションなど、一部の AWS Control Catalog アクションは、特定のリソースで実行できません。このような場合はワイルドカード \* を使用する必要があります。

```
"Resource": "*" 
```

一部の AWS Control Catalog API アクションは、複数のリソースをサポートしています。たとえば、は共通のコントロール、目標、ドメイン ListCommonControls にアクセスするため、プリンシパルにはこれらの各リソースにアクセスするためのアクセス許可が必要です。複数リソースを単一ステートメントで指定するには、ARN をカンマで区切ります。

```
"Resource": [
    "commonControl",
    "objective",
    "domain" ]
```

AWS Control Catalog のアイデンティティベースのポリシーの例については、「」を参照してください [Control Catalog のアイデンティティベースのポリシーの例](#)。

## AWS Control Catalog のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの [条件演算子](#) を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、AWS では AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、は論理 OR オペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「[IAM ポリシーの要素: 変数およびタグ](#)」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートしています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」の[AWS「グローバル条件コンテキストキー」](#)を参照してください。

AWS Control Catalog の条件キーのリストを確認するには、「サービス認可リファレンス」の[「AWS Control Catalog の条件キー」](#)を参照してください。条件キーを使用できるアクションとリソースについては、「[AWS Control Catalog で定義されるアクション](#)」を参照してください。

AWS Control Catalog のアイデンティティベースのポリシーの例については、「」を参照してください[Control Catalog のアイデンティティベースのポリシーの例](#)。

## AWS Control Catalog ACLs

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

## AWS Control Catalog での ABAC

ABAC (ポリシー内のタグ) のサポート: なし

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。では AWS、これらの属性はタグと呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、aws:ResourceTag/*key-name*、aws:RequestTag/*key-name*、または aws:TagKeys の条件キーを使用して、ポリシーの[条件要素](#)でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「[ABAC 認可でアクセス許可を定義する](#)」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM

ユーザーガイド」の「[属性ベースのアクセスコントロール \(ABAC\) を使用する](#)」を参照してください。

## AWS Control Catalog での一時的な認証情報の使用

一時的な認証情報のサポート: あり

一部の AWS のサービスは、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報 AWS のサービスを使用する場合などの詳細については、IAM ユーザーガイド[AWS のサービスの「IAM と連携する](#)」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法でサインインする場合、一時的な認証情報を使用します。たとえば、会社のシングルサインオン (SSO) リンク AWS を使用してアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「[ユーザーから IAM ロールに切り替える \(コンソール\)](#)」を参照してください。

一時的な認証情報は、AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用してアクセスできます AWS。長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成 AWS することをお勧めします。詳細については、「[IAM の一時的セキュリティ認証情報](#)」を参照してください。

## AWS Control Catalog のクロスサービスプリンシパルアクセス許可

転送アクセスセッション (FAS) のサポート: なし

IAM ユーザーまたはロールを使用してアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービスへのリクエストをリクエストすると組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービスまたはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「[転送アクセスセッション](#)」を参照してください。

## AWS Control Catalog のサービスロール

サービスロールのサポート: なし

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける [IAM ロール](#) です。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「[AWS のサービスに許可を委任するロールを作成する](#)」を参照してください。

#### Warning

サービスロールのアクセス許可を変更すると、AWS Control Catalog の機能が破損する可能性があります。AWS Control Catalog が指示する場合にのみ、サービスロールを編集します。

## AWS Control Catalog のサービスにリンクされたロール

サービスにリンクされたロールのサポート: なし

サービスにリンクされたロールは、にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「[IAM と提携するAWS のサービス](#)」を参照してください。表の「サービスリンクロール」列に Yes と記載されたサービスを見つけます。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

## Control Catalog のアイデンティティベースのポリシーの例

デフォルトでは、ユーザーとロールには AWS Control Catalog リソースを作成または変更するアクセス許可はありません。また、AWS Command Line Interface ( AWS CLI ) AWS Management Console、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、リソースに必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「[IAM ポリシーを作成する \(コンソール\)](#)」を参照してください。

各リソースタイプの ARNs [「AWS Control Catalog のアクション、リソース、および条件キー」](#) を参照してください。

## トピック

- [ポリシーに関するベストプラクティス](#)
- [ユーザーが自分の権限を表示できるようにする](#)
- [AWS Control Catalog からのリソースの表示をユーザーに許可する](#)

## ポリシーに関するベストプラクティス

ID ベースのポリシーは、アカウント内で誰かが AWS Control Catalog リソースを作成、アクセス、または削除できるかどうかを決定します。これらのアクションを実行すると、AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらはで使えます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「[AWS マネージドポリシー](#)」または「[ジョブ機能のAWS マネージドポリシー](#)」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「[IAM でのポリシーとアクセス許可](#)」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する – ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションがなどの特定の を通じて使用されている場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の「[IAM JSON ポリシー要素:条件](#)」を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する – IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサ

ポートします。詳細については、「IAM ユーザーガイド」の「[IAM Access Analyzer でポリシーを検証する](#)」を参照してください。

- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、MFA をオンにしてセキュリティを強化します。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「[MFA を使用した安全な API アクセス](#)」を参照してください。

IAM でのベストプラクティスの詳細については、「IAM ユーザーガイド」の「[IAM でのセキュリティベストプラクティス](#)」を参照してください。

## ユーザーが自分の権限を表示できるようにする

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",

```

```

        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

## AWS Control Catalog からのリソースの表示をユーザーに許可する

次のポリシーは、AWS Control Catalog からドメイン、目的、一般的なコントロールを一覧表示するアクセス許可を付与します。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ManageControlCatalogAccess",
      "Effect": "Allow",
      "Action": [
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives",
        "controlcatalog:ListCommonControls"
      ],
      "Resource": "*"
    }
  ]
}

```

## Control Catalog のアイデンティティとアクセスのトラブルシューティング

次の情報は、AWS Control Catalog と IAM の使用時に発生する可能性がある一般的な問題の診断と修正に役立ちます。

### トピック

- [Control Catalog でアクションを実行する権限がありません](#)
- [iam:PassRole を実行する権限がありません](#)
- [Control Catalog リソース AWS アカウント へのアクセスを自分の外部のユーザーに許可したい](#)

## Control Catalog でアクションを実行する権限がありません

アクションを実行する権限がないというエラーが表示された場合は、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要な `controlcatalog:GetWidget` アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
controlcatalog:GetWidget on resource: my-example-widget
```

この場合、`controlcatalog:GetWidget` アクションを使用して *my-example-widget* リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

## iam:PassRole を実行する権限がありません

`iam:PassRole` アクションを実行する権限がないというエラーが表示された場合は、AWS Control Catalog にロールを渡すことができるようにポリシーを更新する必要があります。

一部の AWS のサービスでは、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

次の例のエラーは、という IAM ユーザーがコンソールを使用して marymajor AWS Control Catalog でアクションを実行しようとするると発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに `iam:PassRole` アクションの実行を許可する必要があります。

サポートが必要な場合は、AWS 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

## Control Catalog リソース AWS アカウント へのアクセスを自分の外部のユーザーに許可したい

他のアカウントのユーザーや組織外の人、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- AWS Control Catalog がこれらの機能をサポートしているかどうかを確認するには、「」を参照してください [Control Catalog と IAM の連携方法](#)。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、「[IAM ユーザーガイド](#)」の「[所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する](#)」を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、IAM ユーザーガイドの「[サードパーティー AWS アカウント が所有する へのアクセスを提供する](#)」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、「IAM ユーザーガイド」の「[外部で認証されたユーザー \(ID フェデレーション\) へのアクセスの許可](#)」を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用法の違いについては、「IAM ユーザーガイド」の「[IAM でのクロスアカウントのリソースへのアクセス](#)」を参照してください。

## Control Catalog のコンプライアンス検証

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、[AWS のサービス 「コンプライアンスプログラムによる対象範囲内」](#)を参照して、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、[AWS 「コンプライアンスプログラム」](#)を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「[Downloading Reports in AWS Artifact](#)」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 は、コンプライアンスに役立つ以下のリソース AWS を提供します。

- [セキュリティのコンプライアンスとガバナンス](#) – これらのソリューション実装ガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスの機能をデプロイする手順を示します。
- [HIPAA 対応サービスのリファレンス](#) – HIPAA 対応サービスの一覧が提供されています。すべての AWS のサービス が HIPAA の対象となるわけではありません。
- [AWS コンプライアンスリソース](#) – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- [AWS カスタマーコンプライアンスガイド](#) – コンプライアンスの観点から責任共有モデルを理解します。このガイドは、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールを保護し、そのガイダンスに AWS のサービス マッピングするためのベストプラクティスをまとめたものです。
- [「デベロッパーガイド」の「ルールによるリソースの評価」](#) – この AWS Config サービスは、リソース設定が内部プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。AWS Config
- [AWS Security Hub](#) – これにより AWS のサービス、内のセキュリティ状態を包括的に把握できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールの一覧については、[Security Hub のコントロールリファレンス](#)を参照してください。
- [Amazon GuardDuty](#) – 不審なアクティビティや悪意のあるアクティビティがないか環境をモニタリングすることで AWS アカウント、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービスを検出します。GuardDuty を使用すると、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件に対応できます。
- [AWS Audit Manager](#) – これにより AWS のサービス、AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

## Control Catalog の耐障害性

AWS グローバルインフラストラクチャは、AWS リージョン およびアベイラビリティゾーンを中心に構築されています。複数の物理的に分離および分離されたアベイラビリティゾーン AWS リージョン は、低レイテンシー、高スループット、高度に冗長なネットワークで接続されています。アベイラビリティゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティゾーンは、従

来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョン およびアベイラビリティゾーンの詳細については、[AWS 「グローバルインフラストラクチャ」](#) を参照してください。

## Control Catalog のインフラストラクチャセキュリティ

マネージドサービスである Control Catalog は、ホワイトペーパー「[Amazon Web Services: セキュリティプロセスの概要](#)」に記載されている AWS グローバルネットワークセキュリティ手順で保護されています。

AWS 公開された API コールを使用して、ネットワーク経由で Control Catalog にアクセスします。クライアントで Transport Layer Security (TLS) 1.0 以降がサポートされている必要があります。TLS 1.2 以降が推奨されています。また、DHE (Ephemeral Diffie-Hellman) や ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライアントでサポートされている必要があります。これらのモードは Java 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または[AWS Security Token Service](#) (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

## Control Catalog の設定と脆弱性の分析

設定と IT コントロールは、AWS お客様と当社のお客様との間の責任共有です。詳細については、AWS [「責任共有モデル」](#) を参照してください。

# AWS Control Catalog のモニタリング

モニタリングは、AWS Control Catalog およびその他の AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。は、AWS Control Catalog をモニタリングし、問題が発生したときに報告し、必要に応じて自動アクションを実行するために以下のモニタリングツール AWS を提供します。

- AWS CloudTrail は、AWS アカウントによって、またはアカウントに代わって行われた API コールおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。詳細については、[AWS CloudTrail ユーザーガイド](#)をご参照ください。

## を使用した Control Catalog API コールのログ記録 AWS CloudTrail

AWS Control Tower Control Catalog の一部として、ユーザー AWS CloudTrail、ロール、または サービスによって実行されたアクションを記録する AWS サービスが と統合されています。CloudTrail は、Control Catalog のすべての API コールをイベントとしてキャプチャします。キャプチャされた呼び出しには、コントロールを有効または無効にするなどの AWS Control Tower コンソールから直接の呼び出しや、Control Catalog API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、Control Catalog のコントロールに関連するイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、Control Catalog に対するリクエスト (による AWS Control Tower)、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

CloudTrail の詳細については、「[AWS CloudTrail ユーザーガイド](#)」を参照してください。

## CloudTrail のコントロールカタログ情報

CloudTrail は、アカウントの作成 AWS アカウント 時に 有効になります。Control Catalog でアクティビティが発生すると、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。で最近のイベントを表示、検索、ダウンロードできます AWS アカウント。詳細については、「[CloudTrail イベント履歴でのイベントの表示](#)」を参照してください。

Control Catalog のイベントなど AWS アカウント、 のイベントの継続的な記録については、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョンに適用されます。証跡は、AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集されたイベントデータをさらに分析して処理 AWS のサービス するように他の を設定できます。詳細については、次を参照してください:

- [追跡を作成するための概要](#)
- 「[CloudTrail がサポートされているサービスと統合](#)」
- 「[CloudTrail の Amazon SNS 通知の設定](#)」
- [複数のリージョンから CloudTrail ログファイルを受け取る](#) および [複数のアカウントから CloudTrail ログファイルを受け取る](#)

すべての Control Catalog アクションは CloudTrail によってログに記録され、[Control Catalog API リファレンスに記載されています](#)。例え

ば、ListCommonControls、ListObjectives、ListDomains の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、「[CloudTrail userIdentity エlement](#)」を参照してください。

## Control Catalog ログファイルエントリについて

「トレイル」は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどの情報を含みます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

以下の例は、ListDomains アクションを示す CloudTrail ログエントリです。

```
{
  eventVersion:"1.05",
  userIdentity:{
    type:"IAMUser",
    principalId:"principalId",
    arn:"arn:aws:iam::accountId:user/userName",
    accountId:"111122223333",
    accessKeyId:"accessKeyId",
    userName:"userName",
    sessionContext:{
      sessionIssuer:{
      },
      webIdFederationData:{
      },
      attributes:{
        mfaAuthenticated:"false",
        creationDate:"2020-11-19T07:32:06Z"
      }
    }
  },
  eventTime:"2020-11-19T07:32:36Z",
  eventSource:"controlcatalog.amazonaws.com",
  eventName:"ListDomains",
  awsRegion:"us-west-2",
  sourceIPAddress:"sourceIPAddress",
  userAgent:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  requestParameters: null,
  responseElements: null,
  requestId:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
  eventId:"a782029a-959e-4549-81df-9f6596775cb0",
  readOnly:false,
  eventType:"AwsApiCall",
  recipientAccountId:"recipientAccountId"
}
```

# インターフェイスエンドポイント (AWS PrivateLink) を使用して Control Catalog にアクセスする

を使用して AWS PrivateLink、VPC と Control Catalog の間にプライベート接続を作成できます。インターネットゲートウェイ、NAT デバイス、VPN 接続、または AWS Direct Connect 接続を使用せずに、VPC 内にあるかのように AWS Control Catalog にアクセスできます。VPC 内のインスタンスは、Control Catalog にアクセスするためにパブリック IP アドレスを必要としません。

このプライベート接続を確立するには、AWS PrivateLinkを利用したインターフェイスエンドポイントを作成します。インターフェイスエンドポイントに対して有効にする各サブネットにエンドポイントネットワークインターフェイスを作成します。これらは、Control Catalog 宛てのトラフィックのエントリポイントとして機能するリクエスト管理のネットワークインターフェイスです。

詳細については、「AWS PrivateLink ガイド」の [「Access AWS のサービス through AWS PrivateLink」](#) を参照してください。

## AWS Control Catalog に関する考慮事項

Control Catalog のインターフェイスエンドポイントを設定する前に、「AWS PrivateLink ガイド」の [「考慮事項」](#) を参照してください。

Control Catalog は、インターフェイスエンドポイントを介したすべての API アクションの呼び出しをサポートしています。

## Control Catalog のインターフェイスエンドポイントを作成する

Control Catalog のインターフェイスエンドポイントは、Amazon VPC コンソールまたは AWS Command Line Interface () を使用して作成できますAWS CLI。詳細については、「AWS PrivateLink ガイド」の [「インターフェイスエンドポイントを作成」](#) を参照してください。

次のサービス名を使用して Control Catalog のインターフェイスエンドポイントを作成します。

```
com.amazonaws.region.controlcatalog
```

インターフェイスエンドポイントのプライベート DNS を有効にすると、デフォルトのリージョン DNS 名を使用して Control Catalog に API リクエストを行うことができます。例えば、service-name.us-east-1.amazonaws.com。

# インターフェイスエンドポイントのエンドポイントポリシーを作成する

エンドポイントポリシーは、インターフェイスエンドポイントにアタッチできる IAM リソースです。デフォルトのエンドポイントポリシーでは、インターフェイスエンドポイントを介して Control Catalog へのフルアクセスを許可します。VPC から Control Catalog に許可されるアクセスを制御するには、カスタムエンドポイントポリシーをインターフェイスエンドポイントにアタッチします。

エンドポイントポリシーは以下の情報を指定します。

- アクションを実行できるプリンシパル (AWS アカウント、IAM ユーザー、IAM ロール)。
- 実行可能なアクション。
- このアクションを実行できるリソース。

詳細については、AWS PrivateLink ガイドの[Control access to services using endpoint policies \(エンドポイントポリシーを使用してサービスへのアクセスをコントロールする\)](#)を参照してください。

例: Control Catalog アクションの VPC エンドポイントポリシー

以下は、カスタムエンドポイントポリシーの例です。このポリシーをインターフェイスエンドポイントにアタッチすると、すべてのリソースのすべてのプリンシパルに対して、リストされている AWS Control Catalog アクションへのアクセスが許可されます。

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives",
        "controlcatalog:ListCommonControls"
      ],
      "Resource": "*"
    }
  ]
}
```

 Note

GetControl および ListControls API オペレーションには、デフォルトのフルアクセス許可である別のアクセス許可が必要です。例については、[「デフォルトのエンドポイントポリシー」](#)を参照してください。

# Control Catalog セキュリティ情報ガイドのドキュメント履歴

次の表に、Control Catalog のドキュメントリリースを示します。

| 変更                     | 説明                                       | 日付             |
|------------------------|------------------------------------------|----------------|
| <a href="#">初回リリース</a> | Control Catalog APIsとセキュリティ情報ガイドの初回リリース。 | 2024 年 4 月 8 日 |

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。