



AWS ランディングゾーンからへの移行 AWS Control Tower

# AWS 規範ガイドンス



# AWS 規範ガイド: AWS ランディングゾーンからへの移行 AWS Control Tower

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標とトレードドレスは、Amazon 以外の製品またはサービスとの関連において、顧客に混乱を招いたり、Amazon の名誉または信用を毀損するような方法で使用することはできません。Amazon が所有していない他のすべての商標は、それぞれの所有者の所有物であり、Amazon と提携、接続、または後援されている場合とされていない場合があります。

# Table of Contents

はじめに .....	1
ターゲットを絞ったビジネス成果 .....	1
概要ステップ .....	2
前提条件 .....	3
デプロイAWS Control Tower .....	5
AWSAWS Control Tower既存の組織への既存アカウントの登録 .....	6
AWS Control Towerコンソールから OUAWS Control Tower 登録機能を使用する .....	6
AWS既存の組織のアカウントを新しい組織に登録するAWS Control Tower .....	7
カスタマイズソリューション .....	8
既存または新規ベースラインの追加AWS Control Tower .....	8
AWSランディングゾーン廃止措置 .....	10
ベストプラクティス .....	12
リソース .....	13
リファレンス .....	13
追加情報 .....	13
チュートリアルとラボ .....	13
ネットワーク .....	13
セキュリティ、アイデンティティ、ログ記録 .....	14
リソースのデプロイとワークロードの管理 .....	14
既存の組織とアカウントの操作 .....	14
オートメーションと統合 .....	15
AWS Marketplace .....	15
よくある質問 .....	16
ある OU から別の OU にアカウントを移動しますか? .....	16
の導入は私の Active DirectoryAWS Control Tower セットアップにどのように影響しますか? ....	16
GuardDuty Amazonをに移動するにはどうすればいいですかAWS Control Tower? .....	16
AWS Control Towerコアアカウントをに登録できますか? .....	16
パイプラインのビルドステージステータスを Succeeded にするにはどうすればよいですか? ...	17
ドキュメント履歴 .....	18
用語集 .....	19
# .....	19
A .....	20
B .....	23
C .....	24

---

D .....	27
E .....	31
F .....	33
G .....	34
H .....	35
I .....	36
L .....	38
M .....	39
O .....	43
P .....	45
Q .....	47
R .....	47
S .....	50
T .....	53
U .....	55
V .....	55
W .....	56
Z .....	57
.....	lviii

# AWSランディングゾーンからAWS Control Tower

ガウラヴ・ グプタ、 Amazon Web Services ( AWS )

2022年2月 ([ドキュメント履歴](#))

設計の選択肢が多いため、マルチアカウント環境の設定にはかなりの時間がかかる場合があります。複数のアカウントとサービスの設定が必要になる場合があり、Amazon Web Services (AWS) に関する深い理解が必要です。AWS Landing Zone ソリューションは、AWS ベストプラクティスに基づき、安全なマルチアカウントAWS環境をより迅速に構築することを支援します。

AWS Landing Zone ソリューションの採用が時間の経過とともに拡大するにつれて、ソリューションの管理とカスタマイズに伴う複雑さも増えています。これに対処するために、AWS Control Tower 新しいサービスを開始しました。

AWS Control Towerは、新規マルチアカウントAWS環境を設定し、大規模に管理する効率的な方法を求めている、複数のアカウントとチームを持つ組織を対象としています。を使用するとAWS Control Tower、クラウド管理者は、組織のアカウントが確立されたポリシーに準拠していることを確信し、ビルダーが新しいAWSアカウントを迅速にプロビジョニングできます。

AWS Landing Zone ソリューションの開発は活発に行われていないため、AWS Landing Zone から Landing Zone への移行を検討することが重要ですAWS Control Tower。

## ターゲットを絞ったビジネス成果

- セキュリティ、運用、コンプライアンスポリシー管理が自動化された、AWSすぐに使える環境により、AWSクラウド導入を迅速化
- 確立された予防、検知、AWSおよびコンプライアンス管理を通じてワークロードを移行することにより、ビジネスリスクを軽減
- 統合ダッシュボードの使用によるセキュリティ、運用、コンプライアンスポリシー管理の効率化

## 移行の大まかなステップ

- AWS Control Tower既存の組織にデプロイする場合は、AWS OrganizationsAWSランディングゾーンがデプロイされている場所の既存のクォータを必ず確認してください。既存の組織の使用方法の詳細については、[AWSドキュメントを参照してください](#)。
- OU の登録機能を使用して組織単位 (OU)AWS Control Tower を登録することにより、AWS[既存のアカウントを登録します](#)。
- 登録後、AWS Control Tower[新しいガードレールをチェックして](#)、使用したい別のリソースがガードレールによってブロックされていないことを確認します。
- [AWS Control Towerソリューションのカスタマイズを展開して](#)、CloudFormation既存のベースラインテンプレートまたはサービスコントロールポリシー (SCP) を統合します。
- 該当する場合は、AWS Landing Zone ソリューションによってデプロイされたリソースの使用を停止します。

## 前提条件

- AWS Organizations管理アカウントで、以下のサービスのクォータを確認してください。
  - AWS CloudTrail
  - AWS Config
  - AWS CloudFormation StackSets
  - AWS Organizations管理アカウント
  - サービスコントロールポリシー
- AWS既存のランディングゾーン環境のインベントリと評価を行います。少なくとも、以下のリソースを見てください。
  - AWSmanifest.yamlランディングゾーンファイル
    - その他のベースラインを
    - その他のService Catalog
  - AWS リージョンAWS IAM Identity Centerが設定されている場所 (使用する場合)
  - AWS CloudFormationスタックセット
  - カスタマイズがデプロイされました
- 新しい組織を使用する場合は、AWS Control Tower管理アカウント用のメールアドレスを作成してください。(AWS Control Tower既存の組織をデプロイに使用している場合、これは必要ありません。)

AWSこのメールアドレスが以前に使用されたことがないことを確認してください。

- (オプション) ログアーカイブアカウントの E メールアドレスを作成します。(AWS Control Tower既存の組織をデプロイに使用している場合、これは必要ありません。)

AWSこのメールアドレスが以前に使用されたことがないことを確認してください。

- (オプション) 監査アカウントの E メールアドレスを作成します。(既存のアカウントを使用している場合は、これは必要ありません。)

AWSこのメールアドレスが以前に使用されたことがないことを確認してください。

アカウントの詳細については、の「AWS Control Tower[AWSアカウントについて](#)」を参照してくださいAWS Control Tower。

- この移行中は、AWS Landing ZoneAWS CodePipeline のパイプラインを実行していないことを確認してください。AWS管理コンソールのAWS-Control-Tower-Pipeline ページで、AWSランディングゾーンパイプラインのソースステージとビルドステージの間の移行を無効にするを選択します。



# AWSランディングゾーン組織への配備AWS Control Tower

このシナリオでは、AWS Landing ZoneAWS Control TowerAWS Organizations ソリューションを現在運用している組織への導入に必要な手順を詳しく説明します。

1. 現在のサービスクォータを超えずに2つの新しいアカウントを作成できることを確認してください。必要に応じて、[リクエストサービスのクォータを増やしてください](#)。landing zone に使用したランディングゾーンの既存のアカウントを使用している場合を除き、[AWS Control Tower新しいアカウントはデプロイの一部としてデプロイされます](#)。AWS
2. 現在を使用している場合はAWS IAM Identity Center、IAM Identity CenterAWS Control TowerAWS が設定されているのと同じリージョンにデプロイしてください。
3. AWS Organizationsコンソールで、[ AWS ConfigAWS CloudTrailおよびサービスの信頼済みアクセスを無効にする ] を選択します (有効になっている場合)。詳細については、「[AWS ドキュメント](#)」を参照してください。
4. AWS Control Tower をデプロイします。詳細については、「[AWS ドキュメント](#)」を参照してください。

既存の組織に AWS Control Tower ランディングゾーンをセットアップするときは、以下のことが想定されます。

- AWS Organizations組織ごとに1つのlanding zone をセットアップできます。
- AWS Control Towerは、その管理アカウントとして既存のAWS Organizations組織の管理アカウントを使用します。新しい管理アカウントは不要です。
- AWS Control Towerセットアップ中に既存のアカウントを使用しない限り、登録済み Security OU に2つの新しいアカウントとして、監査アカウントとログ記録アカウントを設定します。既存のアカウントを使用している場合は、AWS Control TowerAWS Control Tower展開時に作成した OU の監査アカウントとログアーカイブアカウントを移動します。
- 組織のサービスクォータがこれら2つの追加のアカウントの作成に適している必要があります。
- 起動後、AWS Control TowerガードレールはそのOUのアカウントに自動的に適用されます。
- によって管理されるOUに、既存のAWSアカウントを追加で登録するとAWS Control Tower、それらのアカウントにガードレールが適用されます。

AWSAWS Control Tower設定後に既存のアカウントまたはOUを登録する場合は、ガイドの「[AWS 既存の組織への既存のアカウントの登録](#)」セクションを参照してください。AWS Control Tower

## AWS Control Tower 既存の組織への既存アカウントの登録

既に管理されている組織単位 (OU) に登録すると、AWS Control Tower ガバナンスを個々の既存の AWS アカウントに拡張できます AWS Control Tower。OU AWS Organizations と同じ組織の一部である未登録の AWS Control Tower OU に存在するアカウントが対象となります。

OU AWS Control Tower AWS Control Tower はコンソールからに登録できます。OU AWS Control Tower を登録すると、その OU AWS Control Tower のすべてのアカウントがに登録されます。

個別のアカウントを登録するよりも、OU を登録することをお勧めします。この方法の利点は、OU ID が変更されないことです。OU ID を使用するポリシーやルールがある場合は、変更を加える必要はありません。

AWS にアカウントを登録する前に AWS Control Tower、AWS CloudFormation AWS-Landing-Zone-Baseline-EnableConfig という名前のスタックセットからスタックインスタンスを削除します。登録する各アカウント、AWS Control Tower デプロイされているすべてのリージョンで、AWS-Landing-Zone-Baseline-EnableConfig スタックインスタンスを削除する必要があります。スタックセット全体を削除するには時間がかかるため、登録しているアカウントのスタックインスタンスだけを削除することをお勧めします。理想的には、特定のアカウントのスタックインスタンスを削除すると、AWS Config レコーダーと配信チャネルも削除されるはずですが、そのアカウントで次のコマンドを実行すると、削除を確認できます。

```
aws configservice describe-configuration-records --region <region_name>
aws configservice describe-delivery-channels --region <region_name>
```

## AWS Control Tower コンソールから OU AWS Control Tower 登録機能を使用する

AWS 既存のアカウントを持つ OU 全体を登録する前に、必ず以下を実行してください。

- 前述のように、その OU AWS Config のすべてのアカウントのすべてのリージョンからレコーダーと配信チャネルを削除します。

詳細については、「[既存の組織単位をに登録する](#)」を参照してください AWS Control Tower。

アカウントを登録すると AWS Control Tower、登録したアカウントの別のプロビジョニング済み製品が Service Catalog に表示されます。プロビジョニングされた製品の名前の先頭には Enroll- が付き

ます。つまり、1つのアカウントで Service Catalog に2つの製品がプロビジョニングされたこととなります。

- AWSランディングゾーンアカウント自動販売機からプロビジョニングされた製品1つ
- への登録からプロビジョニングされた製品が1つAWS Control Tower

AWS Landing Zone からアカウントのプロビジョニング済み製品を終了することもできますが、移行が完了するまで待つことをお勧めします。

AWS Landing Zone環境で販売されているアカウントのプロビジョニング済み製品を終了すると、TerminateAWS CloudFormation操作により関連するベースラインスタックセットの削除が開始されるため、残しておくよい場合があります。manifest.yamlのベースラインスタックセットを必ず評価し、スタックセットを削除した場合の影響を理解してください。スタックセットに残しておきたいリソースがある場合は、プロビジョニングされた製品を削除しないでください。部分的に削除すると、プロビジョニングされた製品は Service Catalog コンソールで汚染された状態になります。

または、アカウント自動販売機で作成したプロビジョニング済み製品をAWS Landing Zone から保持することもできます。

## AWS既存の組織のアカウントを新しい組織に登録するAWS Control Tower

AWS Control TowerAWS Organizations新しい組織に配備したいと思うかもしれません。AWS Control Tower新しい組織をセットアップするには、以下のステップを実行します。

1. [AWS新しいアカウントを作成します。](#)
2. AWS Control Tower新しく作成したアカウントにデプロイします。
3. AWSアカウントを既存の組織からデプロイした新しい組織に移行するにはAWS Control Tower、[手順を参照してください](#)。対象となるアカウントアクセス、請求、ライセンス、税金に関するすべての考慮事項を確認して理解することが重要です。
4. AWS組織間でアカウントを移行するプロセスを理解するには、「[AWS Organizations一括請求によるすべての機能へのアカウントの移行](#)」ブログ投稿を参照してください。
5. AWSアカウントの登録を開始しますAWS Control Tower。登録を行うには、「[AWS既存の組織に既存のアカウントを登録するAWS Control Tower](#)」を参照してください。

# AWS Control Towerソリューション用のカスタマイズの導入

サービスコントロールポリシー (SCP)、AWS CloudFormationカスタムテンプレート、およびベースラインテンプレートを登録済みアカウントに展開するには、[Control Tower ソリューションのカスタマイズを導入できます](#)。

テンプレートは以下を起動します。

- [AWS CodePipeline](#) パイプライン
- [AWS CodeBuild](#) プロジェクト
- [AWS Step Functions](#) ワークフロー
- [AWS Lambda](#) 関数
- [EventBridge](#) アマゾンのイベントルール
- [Amazon Simple Queue Service](#) (Amazon SQS) キュー
- サンプル設定パッケージを含む Amazon [Simple S3](#) バケット

このソリューションでは、S3 バケットを使用する代わりに、[AWS CodeCommit](#) サンプル構成パッケージを含むリポジトリを作成することもできます。

## 既存または新規ベースラインの追加AWS Control Tower

AWS Landing Zoneでは、AWS CloudFormationアカウント作成時にスタックセットを使用してリソースをデプロイできます。これらのスタックセットは、manifest.yamlファイル内ではベースラインリソースとも呼ばれます。スタックセットまたはサービスコントロールポリシー (SCP) AWS Control Tower としてデプロイされます。これらのベースラインリソースをと統合するにはAWS Control Tower、次の手順を参照してください。プロセス中にベースラインを変更することもできます。

1. AWS Control Tower AWS デプロイしたリージョンのセットアップの管理アカウントに、[AWS Control Tower AWS Control Tower ソリューションのカスタマイズをデプロイします](#)。
2. ステップ 1 でデプロイしたソリューションの一部として作成された S3 custom-control-tower-configuration.zip バケットからファイルをダウンロードして解凍します。
3. AWS CloudFormation スタックセットをベースラインとして追加するには、manifest.yaml manifest.yaml ファイルを開き、cloudformation\_resources セクションで次の操作を行います。

- ベースラインをデプロイするアカウントのアカウント名またはアカウント番号を追加します。または、組織単位 (OU) の名前を指定して、OU の下にあるすべてのアカウントにベースラインをデプロイします。
  - AWS CloudFormationテンプレートをメインフォルダーのフォルダーにアップロードし、manifest.yamlファイルに正しいパスが記載されていることを確認します。
  - パラメータがある場合は、parameters.jsonなどのパラメータファイルを parameters フォルダに追加します。
4. サービスコントロールポリシーをベースラインとして追加するには、ファイルを開き、organization\_policiesセクションで次の操作を行います。manifest.yaml
    - サービスコントロールポリシー (SCP) を適用する組織単位を追加します。
    - policies必ずメインフォルダーのフォルダーにポリシーをアップロードし、マニフェストファイルに正しいパスが記載されていることを確認してください。
  5. custom-control-tower-configurationフォルダを圧縮し、ダウンロード元の S3 バケットにアップロードします。これにより、パイプラインが開始され、指定したアカウントまたは OU にベースラインが適用されます。

# AWSランディングゾーン廃止措置

AWSランディングゾーンのリソースを使用停止にする前に、AWS Control Tower 必要なリソースをすべてランディングゾーンから環境に移行したことを確認してください。

廃止プロセスは手動で行われ、AWS Landing Zone ソリューションをデプロイした管理アカウントへの管理者アクセス権が必要です。

リソースを削除する前に、それらのリソースへの影響と依存関係を理解してください。

に正常に移行すると、AWS次のリソースをランディングゾーンから削除できますAWS Control Tower。環境から削除したいカスタムリソースがある場合もあります。

- で始まるスタックセットAWS-Landing-Zone-
  - リソースを実行している場合などPrimaryVPC、特定のスタックセットを保持する必要がある場合があります。
- Amazon GuardDuty ベースラインテンプレート
  - GuardDuty ベースラインテンプレートは自動的に削除されません。GuardDuty デテクタが監視しているすべてのアカウントについて、各リージョンのデテクタからアカウントアソシエーションを削除する必要があります。これを行う最も効率的な方法は、AWS Command Line Interface (AWS CLI) コマンドを使用することです。以下のコマンドを使用して、GuardDuty が有効になっているすべてのリージョンのリソースを削除します。

```
aws guardduty list-detectors --region  
aws guardduty disassociate-members --detector-id <detector_id> --account-ids  
<SecurityAccountID> --region  
aws guardduty delete-members --detector-id <detector_id> --account-ids  
<SecurityAccountID> --region
```

CloudFormation コンソールで、GuardDuty 管理アカウントからスタックセットを削除します。

- AWSランディングゾーン開始テンプレート
  - テンプレートを削除する前に、AWSランディングゾーン設定ファイルを含む S3 バケット内のすべてのオブジェクトを削除します。
- AWS Service Catalog
  - AWS-ランディングゾーンアカウント自動販売機プロビジョニング製品
    - この手順は、などの関連するスタックセットをすべて削除する準備ができているかどうかによって異なりますPrimaryVPC。AVM でプロビジョニングされた製品を削除するとき

は、AWS Landing Zone マニフェストファイルに基づいて AVMAWS CloudFormation に関連するすべてのスタックセットが削除されるため、特に注意してください。

# ベストプラクティス

を利用する際に役立つベストプラクティスとユースケースは以下の通りですAWS Control Tower。

- ユースケースは念頭にあってもどこから始めるべきかわからない場合は、AWS Control Towerダッシュボードで [Get guidance] (パーソナライズされたガイダンスを取得する) を選択してください。
- AWS のネットワークに対して繰り返し可能で管理可能なパターンをセットアップします。
- セキュリティ体制を拡張し、外部または既存のアイデンティティプロバイダーと統合して、ログ記録システムを一元管理します。
- を使ってワークロードの移行に役立つその他のAWSサービス (などAWS Application Migration Service) を利用する。AWS Control Tower



# リソース

## リファレンス

- [AWS Service Catalog ポートフォリオへのアクセス許可の追加](#)
- [AWS Control Tower カスタマイズソリューション](#)
- [に既存の AWS アカウントを登録する AWS Control Tower](#) (ブログ記事)
- [AWS メンバーアカウントを から に移行する AWS OrganizationsAWS Control Tower](#) (パターン)

## 追加情報

### チュートリアルとラボ

- [AWS Control Tower ワークショップ](#) – これらのラボでは、に関連する一般的なタスクの概要を説明します AWS Control Tower。
- [AWS Control Tower 動画](#) – AWS Control Tower 機能の使用方法について詳しく YouTube 説明する、に関する厳選された動画セット。

### ネットワーク

- [AWS Control Tower を使用した のセルフサービス VPCs AWS Service Catalog](#) – このブログ記事では、Account Factory を使用して、カスタマイズされた VPCs でアカウントをプロビジョニングする方法について説明します。
- [での Serverless Transit Network Orchestrator \(STNO\) の実装 AWS Control Tower](#) – このブログ記事では、アカウント間のネットワーク接続アクセスを自動化する方法について説明しています。この投稿は、AWS 環境内のネットワークを管理する AWS Control Tower 管理者および他のユーザーを対象としています。

## セキュリティ、アイデンティティ、ログ記録

### セキュリティ

- [AWS Control Tower ライフサイクルイベントによる AWS Security Hub アラートの自動化](#) — このブログ記事では、既存のアカウントと新しいアカウントで AWS Control Tower マルチアカウント環境で Security Hub の有効化と設定を自動化する方法について説明します。
- [IAM ロールでの IAM Access Analyzer クロスアカウントアクセスの検出結果の解決を自動化する](#) — このブログ記事では、IAM Access Analyzer の検出結果を有効にして一元化することで、組織のセキュリティの可視性を高める方法について説明します。

### アイデンティティ

- [の次の進化 AWS IAM Identity Center](#) — このブログ記事では、IAM Identity Center とで Azure AD を使用する方法について説明します AWS Control Tower。
- [Okta ユニバーサルディレクトリととの間のシングルサインオン AWS](#) (ブログ記事)

### ログ記録

- [集中ログ記録ソリューション](#) — この AWS ソリューションの実装により、組織は複数のアカウントと AWS でログを収集、分析、表示できます AWS リージョン。

### リソースのデプロイとワークロードの管理

- [クラウドカストディアンのへの継続的デプロイ AWS Control Tower](#) (ブログ記事)

### 既存の組織とアカウントの操作

- [組織とアカウントでを有効にする AWS Control Tower](#) — このトピックでは、既存の組織 AWS Control Tower へのデプロイについて説明します。
- [コン AWS Config フォーマンスパックを使用して AWS Control Tower ガバナンスを拡張する](#) (ブログ記事)
- [での複数のアカウントの作成を自動化する方法 AWS Control Tower](#) (ブログ記事)

## オートメーションと統合

- [ライフサイクルイベントを使用した AWS Control Tower アクションの追跡と自動ワークフローのトリガー \(ブログ記事\)](#)
- [での複数のアカウントの作成を自動化する方法 AWS Control Tower \(ブログ記事\)](#)
- [AWS Control Tower ライフサイクルイベントを使用した VPC フローログの自動化 \(ブログ記事\)](#)

## AWS Marketplace

- サードパーティソフトウェアを と統合するためのソリューション AWS Marketplace の提供 [AWS Control Tower 元である ソリューション AWS Marketplace](#) AWS Control Tower。これらのソリューションは、ID 管理、マルチアカウント環境のセキュリティ、集中型ネットワーク、運用インテリジェンス、セキュリティ情報とイベント管理 (SIEM) など、インフラストラクチャと運用の主要なユースケースを解決するのに役立ちます。

## よくある質問

アカウントを登録した後、アカウントをある組織単位 (OU)AWS Control Tower から別の組織単位に移動する方法を教えてください。

アカウントのプロビジョニング済み製品を更新し、パラメータでターゲット OU を選択します。AWS Service Catalog または、AWS Organizations アカウントをコンソールから手動で移動しないでください。移動するとドリフトが発生しますAWS Control Tower。

AWS サードパーティプロバイダのランディングゾーンに Active Directory をセットアップしています。AWS Control Tower の導入はこれにどのように影響しますか？

AWS Control Tower デプロイによって既存のセットアップが妨げられることはありません。デプロイでは、AWS Control Tower 特定の権限セットのみが作成されます。

Amazon GuardDuty AWS はランディングゾーンのセキュリティアカウントで有効化されています。それをに移動するにはどうすればいいですか？AWS Control Tower

AWS Control Tower 新しく作成した監査アカウントを使用して、GuardDuty AWS Organizations 組織用にアクティブ化できます。

AWS AWS Control Tower ランディングゾーンのコアアカウントをに登録できますか？

はい。共有サービス、ロギング、セキュリティなどのコアアカウントは、セキュリティ OU AWS Control Tower を除くすべての OU に登録できます。

AWSランディングゾーンのパイプライン構築ステージのステータスは「失敗」です。「成功」ステータスにするにはどうしたらいいですか？

ビルドステージまたは Launch AVM ステージが失敗した場合は、24 行目の `buildspecpip install --upgrade awscli` に追加してみてください。

## ドキュメント履歴

以下の表は、この戦略の大きな変更点をまとめたものです。今後の更新に関する通知を受け取る場合は、[RSS フィード](#)をサブスクライブできます。

変更	説明	日付
二	<a href="https://docs.aws.amazon.com/prescriptive-guidance/latest/aws-control-tower/prerequisites.html">「https://docs.aws.amazon.com/prescriptive-guidance/latest/aws-control-tower/prerequisites.html</a> 前提条件」と「 <a href="#">AWS ランディングゾーンへの配備</a> 」AWS Control Tower の組織セクションにわかりやすい情報を追加しました。	2022 年 6 月 6 日
二	初版発行	2022 年 2 月 24 日

# AWS 規範的ガイドの用語集

以下は、AWS 規範的ガイドによって提供される戦略、ガイド、パターンで一般的に使用される用語です エントリを提案するには、用語集の最後のフィードバックの提供リンクを使用します。

## 数字

### 7 Rs

アプリケーションをクラウドに移行するための 7 つの一般的な移行戦略。これらの戦略は、ガートナーが 2011 年に特定した 5 Rs に基づいて構築され、以下で構成されています。

- リファクタリング/アーキテクチャの再設計 — クラウドネイティブ特徴を最大限に活用して、俊敏性、パフォーマンス、スケーラビリティを向上させ、アプリケーションを移動させ、アーキテクチャを変更します。これには、通常、オペレーティングシステムとデータベースの移植が含まれます。例: オンプレミスの Oracle データベースを Amazon Aurora PostgreSQL 互換エディションに移行する。
- リプラットフォーム (リフトアンドリシェイプ) — アプリケーションをクラウドに移行し、クラウド機能を活用するための最適化レベルを導入します。例: お客様のオンプレミスの Oracle データベースを AWS クラウドの Oracle 用の Amazon Relational Database Service (Amazon RDS) に移行する。
- 再購入 (ドロップアンドショップ) — 通常、従来のライセンスから SaaS モデルに移行して、別の製品に切り替えます。例: 顧客関係管理 (CRM) システムを Salesforce.com に移行する。
- リホスト (リフトアンドシフト) — クラウド機能を活用するための変更を加えずに、アプリケーションをクラウドに移行します。例: お客様のオンプレミスの Oracle データベースを AWS クラウドの EC2 インスタンス上の Oracle に移行する。
- 再配置 (ハイパーバイザーレベルのリフトアンドシフト) — 新しいハードウェアの購入、アプリケーションの書き換え、お客様の既存のオペレーションの変更を行うことなく、インフラストラクチャをクラウドに移行できます。この移行シナリオは AWS の VMware Cloud に固有のもので、お客様のオンプレミス環境と、および AWS の間の仮想マシン (VM) 互換性とワークロードの移植性をサポートします。インフラストラクチャを AWS の VMware Cloud に移行するときに、お客様のオンプレミスのデータセンターから VMware Cloud Foundation テクノロジーを使用できます。例: AWS の Oracle データベースをホストしているハイパーバイザーを VMware Cloud 上に再配置する。
- 保持 (再アクセス) — アプリケーションをお客様のソース環境で保持します。これには、主要なリファクタリングを必要とするアプリケーションや、お客様がその作業を後日まで延期したい

アプリケーション、およびそれらを移行するためのビジネス上の正当性がないため、お客様が保持するレガシーアプリケーションなどがあります。

- 使用停止 — お客様のソース環境で不要になったアプリケーションを停止または削除します。

## A

### ABAC

[「属性ベースのアクセスコントロール」](#)を参照してください。

### 抽象化されたサービス

[「マネージドサービス」](#)を参照してください。

### ACID

[「不可分性、一貫性、分離性、耐久性」](#)を参照してください。

### アクティブ - アクティブ移行

(双方向レプリケーションツールまたは二重書き込み操作を使用して) ソースデータベースとターゲットデータベースを同期させ、移行中に両方のデータベースが接続アプリケーションからのトランザクションを処理するデータベース移行方法。この方法では、1 回限りのカットオーバーの必要がなく、管理された小規模なバッチで移行できます。アクティブ [パッシブ移行](#) よりも柔軟性がありますが、より多くの作業が必要です。

### アクティブ - パッシブ移行

ソースデータベースとターゲットデータベースを同期させながら、データがターゲットデータベースにレプリケートされている間、接続しているアプリケーションからのトランザクションをソースデータベースのみで処理するデータベース移行の方法。移行中、ターゲットデータベースはトランザクションを受け付けません。

### 集計関数

行のグループを操作し、グループの単一の戻り値を計算するための SQL 関数。集計関数の例には、SUM や MAX があります。

### AI

[「人工知能」](#)を参照してください。

### AIOps

[「人工知能オペレーション」](#)を参照してください。



## 匿名化

データセット内の個人情報を完全に削除するプロセス。匿名化は個人のプライバシー保護に役立ちます。匿名化されたデータは、もはや個人データとは見なされません。

## アンチパターン

繰り返し発生する問題に対して、そのソリューションが逆効果であったり、効果がなかったり、代替ソリューションよりも効果が低かったりする場合によく使用されるソリューション。

## アプリケーションコントロール

マルウェアからシステムを保護するために、承認されたアプリケーションのみを使用できるようにするセキュリティアプローチ。

## アプリケーションポートフォリオ

アプリケーションの構築と維持にかかるコスト、およびそのビジネス価値を含む、組織が使用する各アプリケーションに関する詳細情報の集まり。この情報は、[ポートフォリオの検出と分析プロセス](#)の需要要素であり、移行、モダナイズ、最適化するアプリケーションを特定し、優先順位を付けるのに役立ちます。

## 人工知能 (AI)

コンピューティングテクノロジーを使用し、学習、問題の解決、パターンの認識など、通常は人間に関連づけられる認知機能の実行に特化したコンピュータサイエンスの分野。詳細については、「[人工知能 \(AI\) とは何ですか?](#)」を参照してください。

## AI オペレーション (AIOps)

機械学習技術を使用して運用上の問題を解決し、運用上のインシデントと人の介入を減らし、サービス品質を向上させるプロセス。AWS 移行戦略での AIOps の使用方法については、[オペレーション統合ガイド](#)を参照してください。

## 非対称暗号化

暗号化用のパブリックキーと復号用のプライベートキーから成る 1 組のキーを使用した、暗号化のアルゴリズム。パブリックキーは復号には使用されないため共有しても問題ありませんが、プライベートキーの利用は厳しく制限する必要があります。

## 原子性、一貫性、分離性、耐久性 (ACID)

エラー、停電、その他の問題が発生した場合でも、データベースのデータ有効性と運用上の信頼性を保証する一連のソフトウェアプロパティ。

## 属性ベースのアクセス制御 (ABAC)

部署、役職、チーム名など、ユーザーの属性に基づいてアクセス許可をきめ細かく設定する方法。詳細については、AWS Identity and Access Management (IAM) ドキュメントの[AWS の ABAC とは](#)を参照してください。

## 信頼できるデータソース

最も信頼性のある情報源とされるデータのプライマリバージョンを保存する場所。匿名化、編集、仮名化など、データを処理または変更する目的で、信頼できるデータソースから他の場所にデータをコピーすることができます。

## アベイラビリティゾーン

AWS リージョン 内の仕切られた場所は、他のアベイラビリティゾーンに障害が発生してもその影響を受けず、低コスト、低レイテンシーで同一リージョン内の他のアベイラビリティゾーンに接続できます。

## AWS クラウド導入フレームワーク (AWS CAF)

組織がクラウドに正常に移行するための効率的で効果的な計画を立てるのを支援する AWS からのガイドラインとベストプラクティスのフレームワーク。AWSCAF は、ビジネス、人材、ガバナンス、プラットフォーム、セキュリティ、運用の観点と呼ばれる 6 つの重点を置く分野にガイドランスを編成しています。ビジネス、人材、ガバナンスの観点では、ビジネススキルとプロセスに重点を置き、プラットフォーム、セキュリティ、オペレーションの視点は技術的なスキルとプロセスに焦点を当てています。例えば、人材の観点では、人事 (HR)、人材派遣機能、および人材管理を扱うステークホルダーを対象としています。この観点から、AWS CAF は、クラウドの導入を成功させるための組織の準備を支援するために、人材開発、トレーニング、コミュニケーションに関するガイドランスを提供します。詳細については、[AWS CAF ウェブサイト](#)と[AWS CAF のホワイトペーパー](#)を参照してください。

## AWS ワークロード資格フレームワーク (AWS WQF)

データベース移行ワークロードを評価し、移行戦略を推奨し、作業の見積もりを提供するツール。AWSWQF は AWS Schema Conversion Tool (AWS SCT) と共に含まれます。データベーススキーマとコードオブジェクト、アプリケーションコード、依存関係、およびパフォーマンス特性を分析し、評価レポートを提供します。

## B

### BCP

[「ビジネス継続性計画」](#)を参照してください。

### 動作グラフ

リソースの動作とインタラクションを経時的に示した、一元的なインタラクティブビュー。Amazon Detective の動作グラフを使用すると、失敗したログオンの試行、不審な API 呼び出し、その他同様のアクションを調べることができます。詳細については、Detective ドキュメントの[Data in a behavior graph](#)を参照してください。

### ビッグエンディアンシステム

最上位バイトを最初に格納するシステム。[エンディアン性](#)も参照してください。

### 二項分類

バイナリ結果 (2 つの可能なクラスのうちの一つ) を予測するプロセス。例えば、お客様の機械学習モデルで「この E メールはスパムですか、それともスパムではありませんか」などの問題を予測する必要があるかもしれません。または「この製品は書籍ですか、車ですか」などの問題を予測する必要があるかもしれません。

### ブルームフィルター

要素がセットのメンバーであるかどうかをテストするために使用される、確率的でメモリ効率の高いデータ構造。

### ブランチ

コードリポジトリに含まれる領域。リポジトリに最初に作成するブランチは、メインブランチといます。既存のブランチから新しいブランチを作成し、その新しいブランチで機能を開発したり、バグを修正したりできます。機能を構築するために作成するブランチは、通常、機能ブランチと呼ばれます。機能をリリースする準備ができたなら、機能ブランチをメインブランチに統合します。詳細については、[「ブランチについて \(GitHub ドキュメント\)」](#)を参照してください。

### ブレイククロスアクセス

例外的な状況や承認されたプロセスでは、ユーザーが通常アクセス許可AWS アカウントを持たないにすばやくアクセスできるようになります。詳細については、AWS Well-Architected [ガイド](#)の「[Break Glass 手順の実装](#)」インジケータを参照してください。

## ブラウフィールド戦略

環境の既存インフラストラクチャ。システムアーキテクチャにブラウフィールド戦略を導入する場合、現在のシステムとインフラストラクチャの制約に基づいてアーキテクチャを設計します。既存のインフラストラクチャを拡張している場合は、ブラウフィールド戦略と[グリーンフィールド](#)戦略を融合させることもできます。

## バッファキャッシュ

アクセス頻度が最も高いデータが保存されるメモリ領域。

## ビジネス能力

価値を生み出すためにビジネスが行うこと (営業、カスタマーサービス、マーケティングなど)。マイクロサービスのアーキテクチャと開発の決定は、ビジネス能力によって推進できます。詳細については、ホワイトペーパー[AWS でのコンテナ化されたマイクロサービスの実行のビジネス機能を中心に組織化](#)セクションを参照してください。

## ビジネス継続性計画 (BCP)

大規模移行など、中断を伴うイベントが運用に与える潜在的な影響に対処し、ビジネスを迅速に再開できるようにする計画。

## C

### CAF

[AWS 「クラウド導入フレームワーク」](#)を参照してください。

### CCoE

[「Cloud Center of Excellence」](#)を参照してください。

### CDC

[「変更データキャプチャ」](#)を参照してください。

## 変更データキャプチャ (CDC)

データソース (データベーステーブルなど) の変更を追跡し、その変更に関するメタデータを記録するプロセス。CDC は、ターゲットシステムでの変更を監査またはレプリケートして同期を維持するなど、さまざまな目的に使用できます。

## カオス エンジニアリング

システムの耐障害性をテストするために、意図的に障害や破壊的なイベントを導入する。[AWS Fault Injection Service \(AWS FIS\)](#) を使用して、AWS ワークロードに負荷を掛け、その応答を評価する実験を実行できます。

## CI/CD

[「継続的インテグレーションと継続的デリバリー」](#) を参照してください。

## 分類

予測を生成するのに役立つ分類プロセス。分類問題の機械学習モデルは、離散値を予測します。離散値は、常に互いに区別されます。例えば、モデルがイメージ内に車があるかどうかを評価する必要がある場合があります。

## クライアント側の暗号化

ターゲットの AWS のサービスが受け取る前に、データをローカルで暗号化すること。

## Cloud Center of Excellence (CCoE)

クラウドのベストプラクティスの作成、リソースの移動、移行のタイムラインの確立、大規模変革を通じて組織をリードするなど、組織全体のクラウド導入の取り組みを推進する学際的なチーム。詳細については、AWS クラウドエンタープライズ戦略ブログの [CCoE の投稿](#) を参照してください。

## クラウドコンピューティング

リモートデータストレージと IoT デバイス管理に通常使用されるクラウドテクノロジー。クラウドコンピューティングは、エッジ [コンピューティング](#) テクノロジーに一般的に接続されています。

## クラウド運用モデル

IT 組織において、1 つ以上のクラウド環境を構築、成熟、最適化するために使用される運用モデル。詳細については、[「クラウド運用モデルの構築」](#) を参照してください。

## 導入のクラウドステージ

組織が、AWS クラウドへの移行時に通常実行する 4 つの段階。

- プロジェクト — 概念実証と学習を目的として、クラウド関連のプロジェクトをいくつか実行する
- 基礎固め — お客様のクラウドの導入を拡大するための基礎的な投資 (ランディングゾーンの作成、CCoE の定義、運用モデルの確立など)

- 移行 — 個々のアプリケーションの移行
- 再発明 — 製品とサービスの最適化、クラウドでのイノベーション

これらのステージは Stephen Orban が AWS クラウドエンタープライズ戦略ブログの [クラウドファーストジャーニーと導入ステージ](#) というブログ記事で定義したものです。これらが、AWS 移行戦略とどのような関係があるかについては、[移行準備ガイド](#)を参照してください。

## CMDB

[「設定管理データベース」](#)を参照してください。

## コードリポジトリ

ソースコードやその他の資産 (ドキュメント、サンプル、スクリプトなど) が保存され、バージョン管理プロセスを通じて更新される場所。一般的なクラウドリポジトリには、GitHub またはが含まれますAWS CodeCommit。コードの各バージョンはブランチと呼ばれます。マイクロサービスの構造では、各リポジトリは 1 つの機能専用です。1 つの CI/CD パイプラインで複数のリポジトリを使用できます。

## コールドキャッシュ

空である、または、かなり空きがある、もしくは、古いデータや無関係なデータが含まれているバッファキャッシュ。データベースインスタンスはメインメモリまたはディスクから読み取る必要があり、バッファキャッシュから読み取るよりも時間がかかるため、パフォーマンスに影響します。

## コールドデータ

めったにアクセスされず、通常は過去のデータです。この種類のデータをクエリする場合、通常は低速なクエリでも問題ありません。このデータを低パフォーマンスで安価なストレージ階層またはクラスに移動すると、コストを削減することができます。

## コンピュータビジョン

画像内の人物、場所、物を人間と同等以上の精度で識別するために機械が使用するAIの分野です。多くの場合、深層学習モデルを使用して構築され、1 つの画像または一連の画像からの有用な情報の抽出、分析、分類、理解を自動化します。

## 構成管理データベース ( CMDB )

データベースとその IT 環境 (ハードウェアとソフトウェアの両方のコンポーネントとその設定を含む) に関する情報を保存、管理するリポジトリ。通常、CMDB のデータは、移行のポートフォリオの検出と分析の段階で使用します。

## パフォーマンスパック

組み合わせることでコンプライアンスチェックとセキュリティチェックをカスタマイズできる、AWS Config ルールと修復アクションのコレクション。パフォーマンスパックは、1つのエンティティとして AWS アカウント とリージョンに、または YAML テンプレートを使用して組織全体にデプロイできます。詳細については、AWS Config ドキュメントの[パフォーマンスパック](#)を参照してください。

## 継続的インテグレーションと継続的デリバリー (CI/CD)

ソフトウェアリリースプロセスのソース、ビルド、テスト、ステージング、本番の各ステージを自動化するプロセス。CI/CD は一般的にパイプラインと呼ばれます。プロセスの自動化、生産性の向上、コード品質の向上、配信の加速化を可能にします。詳細については、「[継続的デリバリーの利点](#)」を参照してください。CD は継続的デプロイ (Continuous Deployment) の略語でもあります。詳細については「[継続的デリバリーと継続的なデプロイ](#)」を参照してください。

# D

## 保管中のデータ

ストレージ内にあるデータなど、常に自社のネットワーク内にあるデータ。

## データ分類

ネットワーク内のデータを重要度と機密性に基づいて識別、分類するプロセス。データに適した保護および保持のコントロールを判断する際に役立つため、あらゆるサイバーセキュリティのリスク管理戦略において重要な要素です。データ分類は、AWS Well-Architected フレームワークの、セキュリティの柱の一要素です。詳細については、[データ分類](#)を参照してください。

## データドリフト

実稼働データと ML モデルのトレーニングに使用されたデータとの間に有意な差異が生じたり、入力データが時間の経過と共に有意に変化したりすることです。データドリフトは、ML モデル予測の全体的な品質、精度、公平性を低下させる可能性があります。

## 転送中のデータ

ネットワーク内 (ネットワークリソース間など) を活発に移動するデータ。

## データ最小化

厳密に必要なデータのみを収集し、処理するという原則。AWS クラウド でデータ最小化を実践することで、プライバシーリスク、コスト、分析の二酸化炭素排出量を削減することができます。

## データ境界

信頼できる ID だけが想定されるネットワークから信頼できるリソースにアクセスできるようにするAWS一連の予防ガードレール。詳細については、[「でのデータ境界の構築AWS」](#)を参照してください。

## データの前処理

raw データをお客様の機械学習モデルで簡単に解析できる形式に変換すること。データの前処理とは、特定の列または行を削除して、欠落している、矛盾している、または重複する値に対処することを意味します。

## データ出所

データの生成、送信、保存の方法など、データのライフサイクル全体を通じてデータの出所と履歴を追跡するプロセス。

## データ件名

データを収集、処理している個人。

## データウェアハウス

分析などのビジネスインテリジェンスをサポートするデータ管理システム。通常、データウェアハウスには大量の履歴データが含まれており、クエリや分析には通常使用されます。

## データベース定義言語 (DDL)

データベース内のテーブルやオブジェクトの構造を作成または変更するためのステートメントまたはコマンド。

## データベース操作言語 (DML)

データベース内の情報を変更 (挿入、更新、削除) するためのステートメントまたはコマンド。

## DDL

[「データベース定義言語」](#)を参照してください。



## ディープアンサンブル

予測のために複数の深層学習モデルを組み合わせる。ディープアンサンブルを使用して、より正確な予測を取得したり、予測の不確実性を推定したりできます。

## ディープラーニング

人工ニューラルネットワークの複数層を使用して、入力データと対象のターゲット変数の間のマッピングを識別する機械学習サブフィールド。

## defense-in-depth

一連のセキュリティメカニズムとコントロールをコンピュータネットワーク全体に層状に重ねて、ネットワークとその内部にあるデータの機密性、整合性、可用性を保護する情報セキュリティの手法。この戦略を AWS に採用すると、AWS Organizations 構造内の各層に複数のコントロールが追加され、リソースの安全を維持できます。例えば、defense-in-depth アプローチは多要素認証、ネットワークセグメンテーション、暗号化を組み合わせることができます。

## 委任管理者

AWS Organizations では、互換性のあるサービスは AWS メンバーアカウントを登録することで、組織のアカウントやそのサービスのアクセス許可を管理できるようになります。このアカウントを、そのサービスの委任管理者と呼びます。詳細、および互換性のあるサービスの一覧は、AWS Organizations ドキュメントの [AWS Organizations で使用できるサービス](#) を参照してください。

## デプロイメント

アプリケーション、新機能、コードの修正をターゲットの環境で利用できるようにするプロセス。デプロイでは、コードベースに変更を施した後、アプリケーションの環境でそのコードベースを構築して実行します。

## 開発環境

[「環境」](#) を参照してください。

## 検出管理

イベントが発生したときに、検出、ログ記録、警告を行うように設計されたセキュリティコントロール。これらのコントロールは副次的な防衛手段であり、実行中の予防的コントロールをすり抜けたセキュリティイベントをユーザーに警告します。詳細については、Implementing security controls on AWSの [Detective controls](#) を参照してください。

## 開発バリューストリームマッピング ( DVSM )

ソフトウェア開発ライフサイクルのスピードと品質に悪影響を及ぼす制約を特定し、優先順位を付けるために使用されるプロセス。DVSM は、もともとリーン・ マニファクチャリング・ プラクティスのために設計されたバリュー・ ストリーム・ マッピング・ プロセスを拡張したものです。ソフトウェア開発プロセスを通じて価値を創造し、動かすために必要なステップとチームに焦点を当てています。

## デジタルツイン

建物、工場、産業機器、生産ラインなど、現実世界のシステムを仮想的に表現したものです。デジタルツインは、予知保全、リモートモニタリング、生産最適化をサポートします。

## ディメンションテーブル

[スタースキーマ](#) では、ファクトテーブル内の量子データに関するデータ属性を含む小さなテーブル。ディメンションテーブル属性は通常、テキストフィールドまたはテキストのように動作する離散数値です。これらの属性は、クエリの制約、フィルタリング、結果セットのラベル付けによく使用されます。

## ディザスタ

ワークロードまたはシステムが、導入されている主要な場所でのビジネス目標の達成を妨げるイベント。これらのイベントは、自然災害、技術的障害、または意図しない設定ミスやマルウェア攻撃などの人間の行動の結果である場合があります。

## での災害対策

[災害](#)によるダウンタイムとデータ損失を最小限に抑えるために使用する戦略とプロセス。詳細については、Well-Architected Framework ドキュメントの「Disaster recovery options in the cloud」を参照してください。

## DML

[「データベース操作言語」](#)を参照してください。

## ドメイン駆動型設計

各コンポーネントが提供している変化を続けるドメイン、またはコアビジネス目標にコンポーネントを接続して、複雑なソフトウェアシステムを開発するアプローチ。この概念は、エリック・エヴァンスの著書、Domain-Driven Design: Tackling Complexity in the Heart of Software ( ドメイン駆動設計:ソフトウェアの中心における複雑さへの取り組み ) で紹介されています ( ポストン: Addison-Wesley Professional、2003 )。strangler fig パターンでドメイン駆動型設計を使

用する方法の詳細については、[コンテナと Amazon API Gateway を使用して、従来の Microsoft ASP.NET \(ASMX\) ウェブサービスを段階的にモダナイズ](#)を参照してください。

## DR

[ディザスタリカバリ](#)を参照してください。

### ドリフト検出

ベースライン設定からの逸脱の追跡。例えば、AWS CloudFormationを使用して[システムリソースのドリフトを検出](#)したり、AWS Control Towerを使用してガバナンス要件への準拠に影響を与える可能性のある[ランディングゾーンの変更を検出](#)したりできます。

## DVSM

[「開発値ストリームマッピング」](#)を参照してください。

## E

### EDA

[「調査データ分析」](#)を参照してください。

### エッジコンピューティング

IoT ネットワークのエッジにあるスマートデバイスの計算能力を高めるテクノロジー。[クラウドコンピューティング](#)と比較すると、エッジコンピューティングは通信レイテンシーを短縮し、応答時間を短縮できます。

### 暗号化

人間が読み取り可能なプレーンテキストデータを暗号文に変換するコンピューティングプロセス。

### 暗号化キー

暗号化アルゴリズムが生成した、ランダム化されたビットからなる暗号文字列。キーの長さは決まっておらず、各キーは予測できないように、一意になるように設計されています。

### エンディアン

コンピュータメモリにバイトが格納される順序。ビッグエンディアンシステムでは、最上位バイトが最初に格納されます。リトルエンディアンシステムでは、最下位バイトが最初に格納されません。

## エンドポイント

「[サービスエンドポイント](#)」を参照してください。

### エンドポイントサービス

仮想プライベートクラウド (VPC) 内でホストして、他のユーザーと共有できるサービス。エンドポイントサービスは AWS PrivateLink を使って作成でき、アクセス許可を他の AWS アカウントまたは AWS Identity and Access Management (IAM) プリンシパルに付与することができます。これらのアカウントまたはプリンシパルは、インターフェイス VPC エンドポイントを作成することで、エンドポイントサービスにプライベートに接続できます。詳細については、Amazon Virtual Private Cloud (Amazon VPC) ドキュメントの「[エンドポイントサービスを作成する](#)」を参照してください。

### エンベロープ暗号化

暗号化キーを、別の暗号化キーを使用して暗号化するプロセス。詳細については、AWS Key Management Service (AWS KMS) ドキュメントの[エンベロープ暗号化](#)を参照してください。

### 環境

実行中のアプリケーションのインスタンス。クラウドコンピューティングにおける一般的な環境の種類は以下のとおりです。

- 開発環境 — アプリケーションのメンテナンスを担当するコアチームのみが利用できる、実行中のアプリケーションのインスタンス。開発環境は、上位の環境に昇格させる変更をテストするときに使用します。このタイプの環境は、テスト環境と呼ばれることもあります。
- 下位環境 — 初期ビルドやテストに使用される環境など、アプリケーションのすべての開発環境。
- 本番環境 — エンドユーザーがアクセスできる、実行中のアプリケーションのインスタンス。CI/CD パイプラインでは、本番環境が最後のデプロイ環境になります。
- 上位環境 — コア開発チーム以外のユーザーがアクセスできるすべての環境。これには、本番環境、本番前環境、ユーザー承認テスト環境などが含まれます。

### エピック

アジャイル方法論で、お客様の作業の整理と優先順位付けに役立つ機能カテゴリ。エピックでは、要件と実装タスクの概要についてハイレベルな説明を提供します。例えば、AWS CAF セキュリティエピックには、アイデンティティとアクセスの管理、検出型制御、インフラストラクチャセキュリティ、データ保護、インシデント対応が含まれます。AWS 移行戦略のエピックの詳細については、[プログラム実装ガイド](#)を参照してください。

## 探索的データ分析 (EDA)

データセットを分析してその主な特性を理解するプロセス。お客様は、データを収集または集計してから、パターンの検出、異常の検出、および前提条件のチェックのための初期調査を実行します。EDA は、統計の概要を計算し、データの可視化を作成することによって実行されます。

## F

### ファクトテーブル

[星スキーマ](#) 内の中央テーブル。事業運営に関する量子データを保存します。通常、ファクトテーブルには、メジャーを含む列とディメンションテーブルへの外部キーを含む列の 2 種類の列が含まれます。

### フェイルファスト

頻繁で段階的なテストを使用して開発ライフサイクルを短縮する哲学。これはアジャイルアプローチの重要な部分です。

### 障害分離境界

ではAWS クラウド、障害の影響を制限し、ワークロードの耐障害性を向上させるアベイラビリティゾーンAWS リージョン、コントロールプレーン、データプレーンなどの境界。詳細については、[AWS「障害分離境界」](#)を参照してください。

### 機能ブランチ

[ブランチ](#) を参照してください。

### 特徴量

お客様が予測に使用する入力データ。例えば、製造コンテキストでは、特徴量は製造ラインから定期的にキャプチャされるイメージの可能性もあります。

### 特徴量重要度

モデルの予測に対する特徴量の重要性。これは通常、Shapley Additive Deskonations (SHAP) や積分勾配など、さまざまな手法で計算できる数値スコアで表されます。詳細については、[「による機械学習モデルの解釈可能性 : AWS」](#)を参照してください。

### 機能変換

追加のソースによるデータのエンリッチ化、値のスケーリング、単一のデータフィールドからの複数の情報セットの抽出など、機械学習プロセスのデータを最適化すること。これにより、機械

学習モデルはデータの恩恵を受けることができます。例えば、「2021-05-27 00:15:37」の日付を「2021年」、「5月」、「木」、「15」に分解すると、学習アルゴリズムがさまざまなデータコンポーネントに関連する微妙に異なるパターンを学習するのに役立ちます。

## FGAC

[「きめ細かなアクセスコントロール」](#)を参照してください。

### きめ細かなアクセス制御 (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

### フラッシュカット移行

段階的なアプローチを使用する代わりに、[変更データキャプチャ](#)による継続的なデータレプリケーションを使用して、可能な限り短時間でデータを移行するデータベース移行方法。目的はダウンタイムを最小限に抑えることです。

## G

### Geo ブロック

[「地理的制限」](#)を参照してください。

### 地理的制限 (ジオブロッキング)

Amazon では CloudFront、特定の国のユーザーがコンテンツ配信にアクセスできないようにするオプション。アクセスを許可する国と禁止する国は、許可リストまたは禁止リストを使って指定します。詳細については、CloudFront ドキュメントの[「コンテンツの地理的ディストリビューションの制限」](#)を参照してください。

### Gitflow ワークフロー

下位環境と上位環境が、ソースコードリポジトリでそれぞれ異なるブランチを使用する方法。Gitflow ワークフローはレガシーと見なされ、[トランクベースのワークフロー](#)は最新の推奨アプローチです。

### グリーンフィールド戦略

新しい環境に既存のインフラストラクチャが存在しないこと。システムアーキテクチャにグリーンフィールド戦略を導入する場合、既存のインフラストラクチャ (別名 [ブラウンフィールド](#)) との互換性の制約を受けることなく、あらゆる新しいテクノロジーを選択できます。既存のインフラ

ストラクチャを拡張している場合は、ブラウンフィールド戦略とグリーンフィールド戦略を融合させることもできます。

## ガードレール

組織単位 (OU) 全般のリソース、ポリシー、コンプライアンスを管理するのに役立つ概略的なルール。予防ガードレールは、コンプライアンス基準に一致するようにポリシーを実施します。これらは、サービスコントロールポリシーと IAM アクセス許可の境界を使用して実装されます。検出ガードレールは、ポリシー違反やコンプライアンス上の問題を検出し、修復のためのアラートを発信します。これらは、AWS Config、Amazon AWS Security Hub、GuardDuty、Amazon Inspector AWS Trusted Advisor、およびカスタムAWS Lambdaチェックを使用して実装されます。

# H

## HA

[「高可用性」](#)を参照してください。

### 異種混在データベースの移行

別のデータベースエンジンを使用するターゲットデータベースへお客様の出典データベースの移行 (例えば、Oracle から Amazon Aurora)。異種間移行は通常、アーキテクチャの再設計作業の一部であり、スキーマの変換は複雑なタスクになる可能性があります。[AWS は、スキーマの変換に役立つ AWS SCT を提供します](#)。

### 高可用性

課題や災害が発生した場合に、介入なしにワークロードを継続的に運用できること。HA システムは、自動的にフェイルオーバーし、一貫して高品質のパフォーマンスを提供し、パフォーマンスへの影響を最小限に抑えながらさまざまな負荷や障害を処理するように設計されています。

### ヒストリアンモダナイゼーション

製造業のニーズによりよく応えるために、オペレーション・テクノロジー (OT) システムを近代化し、アップグレードするためのアプローチ。ヒストリアンは、工場内のさまざまなソースからデータを収集して保存するために使用されるデータベースの一種です。

### 同種データベースの移行

お客様の出典データベースを、同じデータベースエンジンを共有するターゲットデータベース (Microsoft SQL Server から Amazon RDS for SQL Server など) に移行する。同種間移行は、通

常、リホストまたはリプラットフォーム化の作業の一部です。ネイティブデータベースユーティリティを使用して、スキーマを移行できます。

## ホットデータ

リアルタイムデータや最近の翻訳データなど、頻繁にアクセスされるデータ。通常、このデータには高速なクエリ応答を提供する高性能なストレージ階層またはクラスが必要です。

## ホットフィックス

本番環境の重大な問題を修正するために緊急で配布されるプログラム。その緊急性により、通常は一般的な DevOps リリースワークフローの外部で修正が行われます。

## ハイパーケア期間

カットオーバー直後、移行したアプリケーションを移行チームがクラウドで管理、監視して問題に対処する期間。通常、この期間は 1~4 日です。ハイパーケア期間が終了すると、アプリケーションに対する責任は一般的に移行チームからクラウドオペレーションチームに移ります。

## I

### laC

「Infrastructure [as Code](#)」を参照してください。

### ID ベースのポリシー

AWS クラウド 環境内のアクセス許可を定義している、1 つ以上の IAM プリンシパルにアタッチされたポリシー。

### アイドル状態のアプリケーション

90 日間の平均的な CPU およびメモリ使用率が 5~20% のアプリケーション。移行プロジェクトでは、これらのアプリケーションを廃止するか、オンプレミスに保持するのが一般的です。

## IIoT

「[産業分野におけるモノのインターネット](#)」を参照してください。

### イミュータブルインフラストラクチャ

既存のインフラストラクチャを更新、パッチ適用、または変更する代わりに、本番稼働用ワークロードに新しいインフラストラクチャをデプロイするモデル。イミュータブルなインフラストラ



クチャは、本質的に [ミュータブルなインフラストラクチャ](#) よりも一貫性、信頼性、予測性が高くなります。詳細については、AWS Well-Architected Framework の「[イミュータブルなインフラストラクチャのベストプラクティスを使用したデプロイ](#)」を参照してください。

## インバウンド (受信) VPC

AWS マルチアカウントアーキテクチャ内で、アプリケーション外部からのネットワーク接続を受け入れ、検査し、ルーティングする VPC。 [AWS Security Reference Architecture](#) では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

## 増分移行

アプリケーションを 1 回ですべてカットオーバーするのではなく、小さい要素に分けて移行するカットオーバー戦略。例えば、最初は少数のマイクロサービスまたはユーザーのみを新しいシステムに移行する場合があります。すべてが正常に機能することを確認できたら、残りのマイクロサービスやユーザーを段階的に移行し、レガシーシステムを廃止できるようにします。この戦略により、大規模な移行に伴うリスクが軽減されます。

## インフラストラクチャ

アプリケーションの環境に含まれるすべてのリソースとアセット。

## Infrastructure as Code (IaC)

アプリケーションのインフラストラクチャを一連の設定ファイルを使用してプロビジョニングし、管理するプロセス。IaC は、新しい環境を再現可能で信頼性が高く、一貫性のあるものにするため、インフラストラクチャを一元的に管理し、リソースを標準化し、スケールを迅速に行えるように設計されています。

## 産業分野における IoT (IIoT)

製造、エネルギー、自動車、ヘルスケア、ライフサイエンス、農業などの産業部門におけるインターネットに接続されたセンサーやデバイスの使用。詳細については、「[Building an industrial Internet of Things \(IIoT\) digital transformation strategy](#)」を参照してください。。

## インスペクション VPC

AWS マルチアカウントアーキテクチャ内で、(同一または異なる AWS リージョンの) VPC、インターネット、オンプレミスネットワーク間のネットワークトラフィックの検査を管理する、一元化された VPC。 [AWS Security Reference Architecture](#) では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウン

ド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

## IoT

インターネットまたはローカル通信ネットワークを介して他のデバイスやシステムと通信する、センサーまたはプロセッサが組み込まれた接続済み物理オブジェクトのネットワーク。詳細については、「[IoT とは](#)」を参照してください。

### 解釈可能性

機械学習モデルの特性で、モデルの予測がその入力にどのように依存するかを人間が理解できる度合いを表します。詳細については、「[AWS を使用した機械学習モデルの解釈](#)」を参照してください。

## IoT

「[モノのインターネット](#)」を参照してください。

## IT 情報ライブラリ (ITIL)

IT サービスを提供し、これらのサービスをビジネス要件に合わせるための一連のベストプラクティス。ITIL は ITSM の基盤を提供します。

## IT サービス管理 (ITSM)

組織の IT サービスの設計、実装、管理、およびサポートに関連する活動。クラウドオペレーションと ITSM ツールの統合については、[オペレーション統合ガイド](#) を参照してください。

## ITIL

「[IT 情報ライブラリ](#)」を参照してください。

## ITSM

「[IT サービス管理](#)」を参照してください。

## L

## ラベルベースアクセス制御 (LBAC)

強制アクセス制御 (MAC) の実装で、ユーザーとデータ自体にそれぞれセキュリティラベル値が明示的に割り当てられます。ユーザーセキュリティラベルとデータセキュリティラベルが交差する部分によって、ユーザーに表示される行と列が決まります。

## ランディングゾーン

ランディングゾーンは、Well-Architected の、スケーラブルで安全なマルチアカウント AWS 環境です。これは、組織がセキュリティおよびインフラストラクチャ環境に自信を持ってワークロードとアプリケーションを迅速に起動してデプロイできる出発点です。ランディングゾーンの詳細については、[安全でスケーラブルなマルチアカウント AWS 環境のセットアップ](#) を参照してください。

### 大規模な移行

300 台以上のサーバの移行。

### LBAC

[「ラベルベースのアクセスコントロール」](#) を参照してください。

### 最小特権

タスクの実行には必要最低限の権限を付与するという、セキュリティのベストプラクティス。詳細については、IAM ドキュメントの[最小特権アクセス許可を適用する](#) を参照してください。

### リフトアンドシフト

[「7 Rs」](#) を参照してください。

### リトルエンディアンシステム

最下位バイトを最初に格納するシステム。[エンディアン性](#) も参照してください。

### 下位環境

[「環境」](#) を参照してください。

## M

### 機械学習 (ML)

パターン認識と学習にアルゴリズムと手法を使用する人工知能の一種。ML は、モノのインターネット (IoT) データなどの記録されたデータを分析して学習し、パターンに基づく統計モデルを生成します。詳細については、「[機械学習](#)」を参照してください。

### メインブランチ

[「ブランチ」](#) を参照してください。

## マネージドサービス

AWS のサービスがインフラストラクチャレイヤー、オペレーティングシステム、プラットフォームをAWS運用し、ユーザーがエンドポイントにアクセスしてデータを保存および取得する対象になります。Amazon Simple Storage Service (Amazon S3) と Amazon DynamoDB は、マネージドサービスの例です。これらは抽象化されたサービスとも呼ばれます。

## MAP

[「移行促進プログラム」](#)を参照してください。

## メカニズム

ツールを作成し、ツールの導入を推進し、結果を検査して調整を行う完全なプロセス。メカニズムとは、動作中に自身を強化および改善するサイクルです。詳細については、AWS Well-Architected フレームワークの「Building [mechanisms](#)」を参照してください。

## メンバーアカウント

AWS Organizations の組織に含まれる管理アカウント以外の、すべての AWS アカウント。アカウントが組織のメンバーになることができるのは、一度に1つのみです。

## マイクロサービス

明確に定義された API を介して通信し、通常は小規模な自己完結型のチームが所有する、小規模で独立したサービスです。例えば、保険システムには、販売やマーケティングなどのビジネス機能、または購買、請求、分析などのサブドメインにマッピングするマイクロサービスが含まれる場合があります。マイクロサービスの利点には、俊敏性、柔軟なスケーリング、容易なデプロイ、再利用可能なコード、回復力などがあります。詳細については、[AWS サーバーレスサービスを使用してマイクロサービスを統合する](#)を参照してください。

## マイクロサービスアーキテクチャ

各アプリケーションプロセスをマイクロサービスとして実行する独立したコンポーネントを使用してアプリケーションを構築するアプローチ。これらのマイクロサービスは、軽量 API を使用して、明確に定義されたインターフェイスを介して通信します。このアーキテクチャの各マイクロサービスは、アプリケーションの特定の機能に対する需要を満たすように更新、デプロイ、およびスケーリングできます。詳細については、[AWS でのマイクロサービスの実装](#)を参照してください。

## Migration Acceleration Program (MAP)

組織がクラウドへの移行のための強力な運用基盤を構築し、移行の初期コストを相殺するのに役立つコンサルティングサポート、トレーニング、サービスを提供する AWS プログラム。MAP に

は、組織的な方法でレガシー移行を実行するための移行方法論と、一般的な移行シナリオを自動化および高速化する一連のツールが含まれています。

## 大規模な移行

アプリケーションポートフォリオの大部分を次々にクラウドに移行し、各ウェーブでより多くのアプリケーションを高速に移動させるプロセス。この段階では、以前の段階から学んだベストプラクティスと教訓を使用して、移行ファクトリー チーム、ツール、プロセスのうち、オートメーションとアジャイルデリバリーによってワークロードの移行を合理化します。これは、[AWS 移行戦略](#) の第 3 段階です。

## 移行ファクトリー

自動化された俊敏性のあるアプローチにより、ワークロードの移行を合理化する部門横断的なチーム。移行ファクトリーチームには、通常、オペレーション、ビジネスアナリストと所有者、移行エンジニア、デベロッパー、スプリントで作業する DevOps プロフェッショナルが含まれます。エンタープライズアプリケーションポートフォリオの 20~50% は、ファクトリーのアプローチによって最適化できる反復パターンで構成されています。詳細については、このコンテンツセットの[移行ファクトリーに関する解説](#)と [Cloud Migration Factory ガイド](#) を参照してください。

## 移行メタデータ

移行を完了するために必要なアプリケーションおよびサーバーに関する情報。移行パターンごとに、異なる一連の移行メタデータが必要です。移行メタデータの例として、ターゲットサブネット、セキュリティグループ、AWS アカウントが挙げられます。

## 移行パターン

移行戦略、移行先、および使用する移行アプリケーションまたはサービスを詳述する、反復可能な移行タスク。例: AWS Application Migration Service を使用して Amazon EC2 への移行を再ホストする。

## Migration Portfolio Assessment (MPA)

AWS クラウドに移行するためのビジネスケースを検証するための情報を提供するオンラインツール。MPA は、詳細なポートフォリオ評価 (サーバーの適切なサイジング、価格設定、TCO 比較、移行コスト分析) および移行プラン (アプリケーションデータの分析とデータ収集、アプリケーションのグループ化、移行の優先順位付け、およびウェーブプランニング) を提供します。[MPA ツール](#) (ログインが必要) は、すべての人に無料で利用できる AWS コンサルタントと APN パートナーコンサルタントです。

## 移行準備状況評価 (MRA)

組織のクラウド対応状況に関するインサイトを獲得し、長所と短所を特定し、AWS CAF を使用して特定されたギャップを埋めるためのアクションプランを構築するプロセス。詳細については、[移行準備状況ガイド](#) を参照してください。MRA は、[AWS 移行戦略](#) の第一段階です。

## 移行戦略

ワークロードを AWS クラウドに移行するために使用するアプローチ。詳細については、この用語集の「[7 Rs エントリ](#)」と「[組織の準備を行って大規模な移行を加速する](#)」を参照してください。

## ML

「[機械学習](#)」を参照してください。

## MPA

「[移行ポートフォリオ評価](#)」を参照してください。

## モダナイゼーション

古い (レガシーまたはモノリシック) アプリケーションとそのインフラストラクチャをクラウド内の俊敏で弾力性のある高可用性システムに変換して、コストを削減し、効率を高め、イノベーションを活用します。詳細については、[AWS クラウドのアプリケーションのモダナイズ戦略](#) を参照してください。

## モダナイゼーション準備状況評価

組織のアプリケーションのモダナイゼーションの準備状況を判断し、利点、リスク、依存関係を特定し、組織がこれらのアプリケーションの将来の状態をどの程度適切にサポートできるかを決定するのに役立つ評価。評価の結果として、ターゲットアーキテクチャのブループリント、モダナイゼーションプロセスの開発段階とマイルストーンを詳述したロードマップ、特定されたギャップに対処するためのアクションプランが得られます。詳細については、[AWS クラウドでのアプリケーションのモダナイゼーションの準備状況を評価する](#) を参照してください。

## モノリシックアプリケーション (モノリス)

緊密に結合されたプロセスを持つ単一のサービスとして実行されるアプリケーション。モノリシックアプリケーションにはいくつかの欠点があります。1つのアプリケーション機能エクスペリエンスの需要が急増する場合は、アーキテクチャ全体をスケーリングする必要があります。モノリシックアプリケーションの特徴を追加または改善することは、コードベースが大きくなると複雑になります。これらの問題に対処するには、マイクロサービスアーキテクチャを使用できます。詳細については、[モノリスをマイクロサービスに分解する](#) を参照してください。

## 多クラス分類

複数のクラスの予測を生成するプロセス (2 つ以上の結果の 1 つを予測します)。例えば、機械学習モデルが、「この製品は書籍、自動車、電話のいずれですか?」または、「このお客様にとって最も関心のある商品のカテゴリはどれですか?」と聞くかもしれません。

## 変更可能なインフラストラクチャ

本番ワークロードの既存のインフラストラクチャを更新および変更するモデル。一貫性、信頼性、予測可能性を向上させるために、AWS Well-Architected フレームワークでは、[イミュータブルインフラストラクチャ](#)をベストプラクティスとして使用することをお勧めします。

## O

### OAC

[「オリジンアクセスコントロール」](#)を参照してください。

### OAI

[「オリジンアクセスアイデンティティ」](#)を参照してください。

### OCM

[「組織の変更管理」](#)を参照してください。

## オフライン移行

移行プロセス中にソースワークロードを停止させる移行方法。この方法はダウンタイムが長くなるため、通常は重要ではない小規模なワークロードに使用されます。

### OI

[「オペレーションの統合」](#)を参照してください。

### OLA

[「運用レベルの契約」](#)を参照してください。

## オンライン移行

ソースワークロードをオフラインにせずターゲットシステムにコピーする移行方法。ワークロードに接続されているアプリケーションは、移行中も動作し続けることができます。この方法はダウンタイムがゼロから最小限で済むため、通常は重要な本番稼働環境のワークロードに使用されます。

## オペレーショナルレベルアグリーメント (OLA)

サービスレベルアグリーメント (SLA) をサポートするために、どの機能的 IT グループが互いに提供することを約束するかを明確にする契約。

## 運用準備状況レビュー (TAK)

インシデントや障害の可能性の範囲を理解、評価、防止、または縮小するのに役立つ質問と関連ベストプラクティスのチェックリスト。詳細については、AWS Well-Architected フレームワークの「[運用準備状況レビュー \(TAK\)](#)」を参照してください。

## オペレーション統合 (OI)

クラウドでオペレーションをモダナイズするプロセスには、準備計画、オートメーション、統合が含まれます。詳細については、[オペレーション統合ガイド](#)を参照してください。

## 組織の証跡

AWS Organizations 内の一組織の、すべての AWS アカウント のイベントをすべてログ記録している AWS CloudTrail が作成した証跡。証跡は、組織に含まれている各 AWS アカウント に作成され、各アカウントのアクティビティを追跡します。詳細については、ドキュメントの「[組織の証跡の作成](#)」を参照してください。CloudTrail

## 組織変更管理 (OCM)

人材、文化、リーダーシップの観点から、主要な破壊的なビジネス変革を管理するためのフレームワーク。OCM は、変化の導入を加速し、移行問題に対処し、文化や組織の変化を推進することで、組織が新しいシステムと戦略の準備と移行するのを支援します。AWS 移行戦略では、クラウド導入プロジェクトに必要な変更のスピードから、このフレームワークは人材の高速化と呼ばれます。詳細については、[OCM ガイド](#)を参照してください。

## オリジンアクセスコントロール (OAC)

では CloudFront、Amazon Simple Storage Service (Amazon S3) コンテンツを保護するためにアクセスを制限するための拡張オプションです。OAC は、すべての AWS リージョンのすべての S3 バケット、AWS KMS (SSE-KMS) を使用したサーバー側の暗号化、S3 バケットへのダイナミックな PUT および DELETE リクエストをサポートしています。

## オリジンアクセスアイデンティティ (OAI)

では CloudFront、Amazon S3 コンテンツを保護するためにアクセスを制限するオプションです。OAI を使用する場合は Amazon S3 が認証できるプリンシパル CloudFront を作成します。認証されたプリンシパルは、特定の CloudFront デイストリビューションを介してのみ S3 バケット内のコンテンツにアクセスできます。[OAC](#)も併せて参照してください。OAC では、より詳細な、強化されたアクセスコントロールが可能です。



## TAK

[「運用準備状況レビュー」](#)を参照してください。

### アウトバウンド (送信) VPC

AWS マルチアカウントアーキテクチャで、アプリケーションの内部から開始したネットワーク接続を処理する VPC。[AWS Security Reference Architecture](#) では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

## P

### アクセス許可の境界

ユーザーまたはロールが使用できるアクセス許可の上限を設定する、IAM プリンシパルにアタッチされる IAM 管理ポリシー。詳細については、IAM ドキュメントの[アクセス許可の境界](#)を参照してください。

### 個人を特定できる情報 (PII)

直接閲覧した場合、または他の関連データと組み合わせた場合に、個人の身元を合理的に推測するために使用できる情報。PII の例には、氏名、住所、連絡先情報などがあります。

## PII

[個人を特定できる情報を参照してください。](#)

### プレイブック

クラウドでのコアオペレーション機能の提供など、移行に関連する作業を取り込む、事前定義された一連のステップ。プレイブックは、スクリプト、自動ランブック、またはお客様のモダナイズされた環境を運用するために必要なプロセスや手順の要約などの形式をとることができます。

### ポリシー

アクセス許可の定義 ([アイデンティティベースのポリシー](#) を参照)、アクセス条件の指定 ([リソースベースのポリシー](#) を参照)、またはの組織内のすべてのアカウントに対する最大アクセス許可の定義 AWS Organizations ([サービスコントロールポリシー](#) を参照) が可能なオブジェクト。

### 多言語の永続性

データアクセスパターンやその他の要件に基づいて、マイクロサービスのデータストレージテクノロジーを個別に選択します。マイクロサービスが同じデータストレージテクノロジーを使用し

ている場合、実装上の問題が発生したり、パフォーマンスが低下する可能性があります。マイクロサービスは、要件に最も適合したデータストアを使用すると、より簡単に実装でき、パフォーマンスとスケーラビリティが向上します。詳細については、[マイクロサービスでのデータ永続性の有効化](#)を参照してください。

## ポートフォリオ評価

移行を計画するために、アプリケーションポートフォリオの検出、分析、優先順位付けを行うプロセス。詳細については、[移行準備状況ガイド](#)を参照してください。

## 述語

true または を返すクエリ条件。通常false、WHERE句にあります。

## 述語プッシュダウン

転送前にクエリ内のデータをフィルタリングするデータベースクエリ最適化手法。これにより、リレーショナルデータベースから取得および処理する必要があるデータの量が減少し、クエリのパフォーマンスが向上します。

## 予防的コントロール

イベントの発生を防ぐように設計されたセキュリティコントロール。このコントロールは、ネットワークへの不正アクセスや好ましくない変更を防ぐ最前線の防御です。詳細については、Implementing security controls on AWSの[Preventative controls](#)を参照してください。

## プリンシパル

アクションを実行してリソースにアクセスできる AWS 内のエンティティです。このエンティティは、通常は AWS アカウント のルートユーザー、IAM ロール、ユーザーのいずれかになります。詳細については、IAM ドキュメントの[ロールに関する用語と概念](#)内にあるプリンシパルを参照してください。

## プライバシーバイデザイン

エンジニアリングプロセス全体を通してプライバシーを考慮に入れたシステムエンジニアリングのアプローチ。

## プライベートホストゾーン

1 つ以上の VPC 内のドメインとそのサブドメインへの DNS クエリに対し、Amazon Route 53 がどのように応答するかに関する情報を保持するコンテナ。詳細については、Route 53 ドキュメントの「[プライベートホストゾーンの使用](#)」を参照してください。

## プロアクティブコントロール

非準拠のリソースのデプロイを防ぐように設計された[セキュリティコントロール](#)。これらのコントロールは、プロビジョニング前にリソースをスキャンします。リソースがコントロールに準拠していない場合、プロビジョニングされません。詳細については、AWS Control Towerドキュメントの「[コントロールリファレンスガイド](#)」および「[でのセキュリティコントロールの実装](#)」の「[プロアクティブコントロール](#)」を参照してください。 AWS

### 本番環境

[「環境」](#)を参照してください。

### 仮名化

データセット内の個人識別子をプレースホルダー値に置き換えるプロセス。仮名化は個人のプライバシー保護に役立ちます。仮名化されたデータは、依然として個人データとみなされます。

## Q

### クエリプラン

SQL リレーショナルデータベースシステムのデータにアクセスするために使用される、手順などの一連のステップ。

### クエリプランのリグレッション

データベースサービスのオプティマイザーが、データベース環境に特定の変更が加えられる前に選択されたプランよりも最適性の低いプランを選択すること。これは、統計、制限事項、環境設定、クエリパラメータのバインディングの変更、およびデータベースエンジンの更新などが原因である可能性があります。

## R

### RACI マトリックス

[「責任、説明、相談、報告 \(RACI\)」](#)を参照してください。

### ランサムウェア

決済が完了するまでコンピュータシステムまたはデータへのアクセスをブロックするように設計された、悪意のあるソフトウェア。

## RASCI マトリックス

[「責任、説明、相談、報告 \(RACI\)」](#) を参照してください。

## RCAC

[「行と列のアクセスコントロール」](#) を参照してください。

## リードレプリカ

読み取り専用で使用されるデータベースのコピー。クエリをリードレプリカにルーティングして、プライマリデータベースへの負荷を軽減できます。

## 再設計

[「7 Rs」](#) を参照してください。

## 目標復旧時点 (RPO)

RPO とは、データが最後に復旧した時点を開始とする経過時間の、許容される値のことです。これにより、最後の回復時点からサービスが中断されるまでの間に許容できるデータ損失の程度が決まります。

## 目標復旧時間 (RTO)

RTO とは、サービスが中断してから復旧するまでに経過した時間 (遅延) の、許容される値のことです。

## リファクタリング

[「7 Rs」](#) を参照してください。

## リージョン

地理的な領域内の AWS リソースのコレクション。各 AWS リージョンは、耐障害性、安定性、レジリエンスを実現するために他のリージョンと分離され、独立しています。詳細については、AWS 全般のリファレンスの [「Managing AWS リージョン」](#) を参照してください。

## 回帰

数値を予測する機械学習手法。例えば、「この家はどれくらいの値段で売れるでしょうか?」という問題を解決するために、機械学習モデルは、線形回帰モデルを使用して、この家に関する既知の事実 (平方フィートなど) に基づいて家の販売価格を予測できます。

## リホスト

[「7 Rs」](#) を参照してください。

## リリース

デプロイプロセスで、変更を本番環境に昇格させること。

## 再配置

「[7 Rs](#)」を参照してください。

## プラットフォーム変更

「[7 Rs](#)」を参照してください。

## 再購入

「[7 Rs](#)」を参照してください。

## リソースベースのポリシー

Amazon S3 バケット、エンドポイント、暗号化キーなどのリソースにアタッチされたポリシー。このタイプのポリシーは、アクセスが許可されているプリンシパル、サポートされているアクション、その他の満たすべき条件を指定します。

## 実行責任者、説明責任者、協業先、報告先 (RACI) に基づくマトリックス

移行活動とクラウド運用に関わるすべての関係者の役割と責任を定義したマトリックス。マトリックスの名前は、マトリックスで定義されている責任の種類、すなわち責任 (R)、説明責任 (A)、協議 (C)、情報提供 (I) に由来します。サポート (S) タイプはオプションです。サポートを含めると、そのマトリックスは RASCI マトリックスと呼ばれ、サポートを除外すると RACI マトリックスと呼ばれます。

## レスポンスコントロール

有害事象やセキュリティベースラインからの逸脱について、修復を促すように設計されたセキュリティコントロール。詳細については、Implementing security controls on AWSの[Responsive controls](#)を参照してください。

## 保持

「[7 Rs](#)」を参照してください。

## 廃止

「[7 Rs](#)」を参照してください。

## ローテーション

定期的に[シークレット](#)を更新して、攻撃者が認証情報にアクセスするのをより困難にするプロセス。

## 行と列のアクセス制御 (RCAC)

アクセスルールが定義された、基本的で柔軟な SQL 表現の使用。RCAC は行権限と列マスクで構成されています。

## RPO

[「目標復旧時点」](#)を参照してください。

## RTO

[「目標復旧時間」](#)を参照してください。

## ランブック

特定のタスクを実行するために必要な手動または自動化された一連の手順。これらは通常、エラー率の高い反復操作や手順を合理化するために構築されています。

# S

## SAML 2.0

多くの ID プロバイダー (IdPs) が使用するオープンスタンダード。この機能ではフェデレーティッドシングルサインオン (SSO) が有効になるため、組織内の全員に IAM のユーザーを作成しなくても、ユーザーが AWS Management Console にログインしたり AWS API オペレーションを呼び出したりできます。SAML 2.0 ベースのフェデレーションの詳細については、IAM ドキュメントの[SAML 2.0 ベースのフェデレーションについて](#)を参照してください。

## SCP

[「サービスコントロールポリシー」](#)を参照してください。

## シークレット

ではAWS Secrets Manager、暗号化された形式で保存するパスワードやユーザー認証情報などの機密情報または制限された情報。シークレット値とそのメタデータで構成されます。シークレット値は、バイナリ、単一の文字列、または複数の文字列です。詳細については、[Secrets Manager](#) ドキュメントの「シークレット」を参照してください。

## セキュリティコントロール

脅威アクターによるセキュリティ脆弱性の悪用を防止、検出、軽減するための、技術上または管理上のガードレール。セキュリティコントロールには、[主に予防的](#)、[検出的](#)、[応答性](#)、[プロアクティブ](#) の 4 つのタイプがあります。

## セキュリティ強化

アタックサーフェスを狭めて攻撃への耐性を高めるプロセス。このプロセスには、不要になったリソースの削除、最小特権を付与するセキュリティのベストプラクティスの実装、設定ファイル内の不要な機能の無効化、といったアクションが含まれています。

### Security Information and Event Management (SIEM) システム

セキュリティ情報管理 (SIM) とセキュリティイベント管理 (SEM) のシステムを組み合わせたツールとサービス。SIEM システムは、サーバー、ネットワーク、デバイス、その他ソースからデータを収集、モニタリング、分析して、脅威やセキュリティ違反を検出し、アラートを発信します。

### セキュリティレスポンスの自動化

セキュリティイベントに自動的に応答または修正するように設計された、事前定義されたプログラムされたアクション。これらのオートメーションは、セキュリティのベストプラクティスの実装に役立つ検出的または応答的なAWSセキュリティコントロールとして機能します。自動応答アクションの例には、VPC セキュリティグループの変更、Amazon EC2 インスタンスへのパッチ適用、認証情報のローテーションなどがあります。

### サーバー側の暗号化

データを受信した AWS のサービスによって、送信先でデータが暗号化されること。

### サービスコントロールポリシー (SCP)

AWS Organizations の組織内の、すべてのアカウントのアクセス許可を一元的に管理するポリシー。SCP は、管理者がユーザーまたはロールに委任するアクションに、ガードレールを定義したり、アクションの制限を設定したりします。SCP は、許可リストまたは拒否リストとして、許可または禁止するサービスやアクションを指定する際に使用できます。詳細については、AWS Organizations ドキュメントの[サービスコントロールポリシー \(SCP\)](#)を参照してください。

### サービスエンドポイント

AWS のサービスのエンドポイントの URL。ターゲットサービスにプログラムで接続するには、エンドポイントを使用します。詳細については、AWS 全般のリファレンスの「[AWS のサービス エンドポイント](#)」を参照してください。

### サービスレベルアグリーメント (SLA)

サービスのアップタイムやパフォーマンスなど、IT チームがお客様に提供すると約束したものを明示した合意書。

## サービスレベルインジケータ (SLI)

エラー率、可用性、スループットなど、サービスのパフォーマンス側面の測定。

## サービスレベル目標 (SLO)

サービスレベルのインジケータによって測定される、サービスのヘルスを表すターゲットメトリクス。

## 責任共有モデル

ユーザーが、クラウドセキュリティとコンプライアンスに関する責任を AWS と共有するモデルのこと。AWS はクラウド自体のセキュリティに対して責任を負い、ユーザーはクラウド内のセキュリティに対して責任を負います。詳細については、[責任共有モデル](#)を参照してください。

## SIEM

[「セキュリティ情報とイベント管理システム」](#)を参照してください。

## 単一障害点 (SPOF)

システムを中断する可能性のある、アプリケーションの単一の重要なコンポーネントの障害。

## SLA

[「サービスレベルアグリーメント」](#)を参照してください。

## SLI

[「サービスレベルインジケータ」](#)を参照してください。

## SLO

[「サービスレベルの目標」](#)を参照してください。

## split-and-seed モデル

モダナイゼーションプロジェクトのスケーリングと加速のためのパターン。新機能と製品リリースが定義されると、コアチームは解放されて新しい製品チームを作成します。これにより、お客様の組織の能力とサービスの拡張、デベロッパーの生産性の向上、迅速なイノベーションのサポートに役立ちます。詳細については、[「」の「アプリケーションをモダナイズするための段階的なアプローチAWS クラウド」](#)を参照してください。

## SPOF

[「単一障害点」](#)を参照してください。



## star スキーマ

トランザクションデータまたは測定データを保存するために 1 つの大きなファクトテーブルを使用し、データ属性を保存するために 1 つ以上の小さなディメンションテーブルを使用するデータベースの組織構造。この構造は、[データウェアハウス](#)またはビジネスインテリジェンス目的で使用するよう設計されています。

## strangler fig パターン

レガシーシステムが廃止されるまで、システム機能を段階的に書き換えて置き換えることにより、モノリシックシステムをモダナイズするアプローチ。このパターンは、宿主の樹木から根を成長させ、最終的にその宿主を包み込み、宿主に取って代わるイチジクのつるを例えています。そのパターンは、モノリシックシステムを書き換えるときのリスクを管理する方法として [Martin Fowler](#) により提唱されました。このパターンの適用方法の例については、[コンテナと Amazon API Gateway を使用して、従来の Microsoft ASP.NET \(ASMX\) ウェブサービスを段階的にモダナイズ](#)を参照してください。

## サブネット

VPC 内の IP アドレスの範囲。サブネットは、1 つのアベイラビリティゾーンに存在する必要があります。

## 対称暗号化

データの暗号化と復号に同じキーを使用する暗号化のアルゴリズム。

## 合成テスト

潜在的な問題を検出したり、パフォーマンスを監視したりするために、ユーザーインタラクションをシミュレートする方法でシステムをテストします。[Amazon CloudWatch Synthetics](#) を使用して、これらのテストを作成できます。

# T

## タグ

AWS リソースを整理するためのメタデータとして機能するキーと値のペア。タグは、リソースの管理、識別、整理、検索、フィルタリングに役立ちます。詳細については、「[AWS リソースのタグ付け](#)」を参照してください。

## ターゲット変数

監督された機械学習でお客様が予測しようとしている値。これは、結果変数のことも指します。例えば、製造設定では、ターゲット変数が製品の欠陥である可能性があります。

## タスクリスト

ランブックの進行状況を追跡するために使用されるツール。タスクリストには、ランブックの概要と完了する必要がある一般的なタスクのリストが含まれています。各一般的なタスクには、推定所要時間、所有者、進捗状況が含まれています。

## テスト環境

[「環境」](#)を参照してください。

## トレーニング

お客様の機械学習モデルに学習するデータを提供すること。トレーニングデータには正しい答えが含まれている必要があります。学習アルゴリズムは入力データ属性をターゲット (お客様が予測したい答え) にマッピングするトレーニングデータのパターンを検出します。これらのパターンをキャプチャする機械学習モデルを出力します。そして、お客様が機械学習モデルを使用して、ターゲットがわからない新しいデータでターゲットを予測できます。

## トランジットゲートウェイ

VPC とオンプレミスネットワークを相互接続するために使用できる、ネットワークの中継ハブ。詳細については、AWS Transit Gateway ドキュメントの「[Transit Gateway とは](#)」を参照してください。

## トランクベースのワークフロー

デベロッパーが機能ブランチで機能をローカルにビルドしてテストし、その変更をメインブランチにマージするアプローチ。メインブランチはその後、開発環境、本番前環境、本番環境に合わせて順次構築されます。

## 信頼されたアクセス

AWS Organizations の組織およびそのアカウントで、ユーザーに代わって指定したサービスにタスクを実行させるためにアクセス許可を付与すること。信頼されたサービスは、サービスにリンクされたロールを必要なときに各アカウントに作成し、ユーザーに代わって管理タスクを実行します。詳細については、AWS Organizations ドキュメントの[AWS Organizations を他の AWS サービスと併用する](#)を参照してください。

## チューニング

機械学習モデルの精度を向上させるために、お客様のトレーニングプロセスの側面を変更する。例えば、お客様が機械学習モデルをトレーニングするには、ラベル付けセットを生成し、ラベルを追加します。これらのステップを、異なる設定で複数回繰り返して、モデルを最適化します。

## ツーピザチーム

2つのピザを供給できる小規模な DevOps チーム。ツーピザチームの規模では、ソフトウェア開発におけるコラボレーションに最適な機会が確保されます。

# U

## 不確実性

予測機械学習モデルの信頼性を損なう可能性がある、不正確、不完全、または未知の情報を指す概念。不確実性には、次の2つのタイプがあります。認識論的不確実性は、限られた、不完全なデータによって引き起こされ、弁論的不確実性は、データに固有のノイズとランダム性によって引き起こされます。詳細については、[深層学習システムにおける不確実性の定量化](#) ガイドを参照してください。

## 未分化なタスク

ヘビーリフティングとも呼ばれ、アプリケーションの作成と運用には必要だが、エンドユーザーに直接的な価値をもたらさなかったり、競争上の優位性をもたらしたりしない作業です。未分化なタスクの例としては、調達、メンテナンス、キャパシティプランニングなどがあります。

## 上位環境

[「環境」](#)を参照してください。

# V

## バキューミング

ストレージを再利用してパフォーマンスを向上させるために、増分更新後にクリーンアップを行うデータベースのメンテナンス操作。

## バージョンコントロール

リポジトリ内のソースコードへの変更など、変更を追跡するプロセスとツール。

## VPC ピアリング

プライベート IP アドレスを使用してトラフィックをルーティングできる、2 つの VPC 間の接続。詳細については、Amazon VPC ドキュメントの「[VPC ピア機能とは](#)」を参照してください。

## 脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

# W

## ウォームキャッシュ

頻繁にアクセスされる最新の関連データを含むバッファキャッシュ。データベースインスタンスはバッファキャッシュから、メインメモリまたはディスクからよりも短い時間で読み取りを行うことができます。

## ウォームデータ

アクセス頻度の低いデータ。この種類のデータをクエリする場合、通常は適度に遅いクエリでも問題ありません。

## ウィンドウ関数

現在のレコードに関連する行のグループに対して計算を実行する SQL 関数。ウィンドウ関数は、移動平均の計算や、現在の行の相対位置に基づく行の値へのアクセスなど、タスクの処理に役立ちます。

## ワークロード

ビジネス価値をもたらすリソースとコード (顧客向けアプリケーションやバックエンドプロセスなど) の総称。

## ワークストリーム

特定のタスクセットを担当する移行プロジェクト内の機能グループ。各ワークストリームは独立していますが、プロジェクト内の他のワークストリームをサポートしています。たとえば、ポートフォリオワークストリームは、アプリケーションの優先順位付け、ウェーブ計画、および移行メタデータの収集を担当します。ポートフォリオワークストリームは、これらの設備を移行ワークストリームで実現し、サーバーとアプリケーションを移行します。

## WORM

[「Write Once, Read Many」](#)を参照してください。

## WQF

[「AWS ワークロード認定フレームワーク」](#)を参照してください。

### Write Once, Read Many (WORM)

データを 1 回書き込み、データの削除や変更を禁止するストレージモデル。認可されたユーザーは、必要な回数だけデータを読み取ることができますが、変更することはできません。このデータストレージインフラストラクチャは、[イミュータブルな](#)と見なされます。

## Z

### ゼロデイエクスプロイト

[ゼロデイ脆弱性](#) を利用する攻撃、通常はマルウェアです。

### ゼロデイ脆弱性

実稼働システムにおける未解決の欠陥または脆弱性。脅威アクターは、このような脆弱性を利用してシステムを攻撃する可能性があります。開発者は、よく攻撃の結果で脆弱性に気付きます。

### ゾンビアプリケーション

平均 CPU およびメモリ使用率が 5% 未満のアプリケーション。移行プロジェクトでは、これらのアプリケーションを廃止するのが一般的です。

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。