



のメインフレームデータレプリケーション戦略 AWS クラウド

# AWS 規範ガイド



# AWS 規範ガイド: のメインフレームデータレプリケーション戦略 AWS クラウド

Copyright © 2026 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

序章 .....	1
対象者 .....	1
ビジネス上の利点 .....	2
主な考慮事項 .....	4
戦略的アプローチ .....	6
評価 .....	6
準備 .....	7
移行とモダナイズ .....	9
最適化 .....	9
管理 .....	10
ユースケース .....	11
変更データキャプチャ .....	11
リアルタイムレポート .....	12
メッセージングプロトコル .....	13
新しいチャネル .....	14
コンプライアンスとアーカイブ .....	15
オフロード処理とバッチレプリケーション .....	16
次の手順 .....	18
リソース .....	18
ドキュメント履歴 .....	19
用語集 .....	20
# .....	20
A .....	21
B .....	23
C .....	25
D .....	28
E .....	32
F .....	35
G .....	36
H .....	37
I .....	39
L .....	41
M .....	42
O .....	46

---

P .....	49
Q .....	52
R .....	52
S .....	55
T .....	59
U .....	60
V .....	61
W .....	61
Z .....	62
.....	lxiii

# のメインフレームデータレプリケーション戦略 AWS クラウド

Vaidy Sankaran と Pablo Alonso Prieto、Amazon Web Services

2025 年 2 月 ([ドキュメント履歴](#))

企業は、レガシーメインフレームワークロードを維持しながら、イノベーションと俊敏性を開拓しようとしています。これにより、クラウドの導入が不可欠です。このガイドでは、へのメインフレームデータレプリケーションを成功させるための主要なビジネスユースケース、考慮事項、および方法論的なアプローチについて説明します AWS クラウド。

へのデータレプリケーション AWS クラウド は、エンタープライズレベルのメインフレームモダライゼーションジャーニーにおける重要なコンポーネントです。クラウドにメインフレームデータをレプリケートするという決定は、次のようないくつかの魅力的なビジネスニーズによって左右される可能性があります。

- **インサイトのロック解除** – メインフレームデータは、高度な分析、AI、機械学習イニシアチブのための貴重なリソースを提供します。データを にレプリケートすることで AWS クラウド、組織は新しいインサイトを引き出し、意思決定プロセスを強化し、AI 主導の変革戦略を推進できます。
- **俊敏性と成長の促進** – データレプリケーションは、拡張と新しいチャネルの開発を容易にします。これにより、ビジネスイニシアチブを加速し、俊敏性を高めることができます。このアプローチにより、企業は進化する市場需要に迅速に適応し、データリソースを俊敏にデプロイすることで成長の機会を得ることができます。
- **移行の促進** – データレプリケーションは、移行されたワークロードと移行されていないワークロード間で中間統合とデータ整合性をサポートします。これにより、シームレスな移行が容易になり、運用の中断が軽減され、ビジネス目標に沿った、まとまりのあるモダナイズされたインフラストラクチャの基盤が構築されます。

## 対象者

この戦略的アプローチは、メインフレームワークロードのモダナイズと の導入を検討している企業のエグゼクティブやアーキテクトに推奨されます AWS クラウド。このガイドは、データレプリケーションがモダライゼーション戦略の重要なコンポーネントとして識別される場合に強く推奨されます。

# メインフレームデータを にレプリケートするビジネス上の利点 AWS

戦略的動機によって、メインフレームデータを にレプリケートするという決定が促進されます AWS クラウド。これらの動機は、ビジネスの俊敏性、イノベーション、回復力を高めることを目的としています。これには以下のものが含まれます。

- 俊敏性とイノベーション — ペースの速いビジネス環境では、俊敏性とイノベーションは競争の先頭に立つのに役立ちます。データを にレプリケートすることで AWS クラウド、企業はイノベーションの新しい機会を開拓し、新しい製品やサービスのtime-to-marketし、変化する顧客のニーズと市場ダイナミクスに迅速に対応できます。
- スケーラビリティと柔軟性 – 従来のメインフレームシステムでは、多くの場合、スケーラビリティと柔軟性に制限があります。これは、進化するビジネス要件に適應する能力を妨げます。へのデータレプリケーション AWS クラウド は、スケーラビリティと柔軟性の点で優れています。企業は、必要に応じてリソースをスケールアップまたはスケールダウンし、変動するワークロードに対応し、新しいビジネスモデルやテクノロジーを試すことができます。
- コスト最適化 – コスト最適化は、IT 投資の価値を最大化し、運用コストを最小限に抑えることを目指す企業にとって重要な優先事項です。へのデータレプリケーション AWS クラウド により、組織はpay-as-you-goモデルを使用できます。これらのモデルは、前払いの設備投資を削減し、リソース使用率を最適化するため、時間の経過とともに大幅なコスト削減につながります。
- レジリエンスとビジネス継続性 — 自然災害、サイバー攻撃、システム障害など、中断が発生した場合のレジリエンスとビジネス継続性は、事業運営を保護し、顧客の信頼を維持する上で不可欠です。へのデータレプリケーション AWS クラウド は、組み込みの冗長性、ディザスタリカバリ機能、地理的分散を提供します。データレプリケーションは、重要なデータとアプリケーションの継続的な可用性を提供します。

へのデータレプリケーション AWS クラウド には、次のような戦略的動機に沿った利点があります。

- ビジネスの俊敏性の向上 – 新機能の迅速なデプロイ、新しいテクノロジーとのシームレスな統合、市場機会への迅速な対応を可能にします。
- スケーラビリティと柔軟性の向上 – スケーラブルなリソースへのオンデマンドアクセスを提供し、動的なリソース割り当てを可能にし、ビジネスの成長をサポートします。

- コスト削減 – インフラストラクチャコストを最適化し、設備投資を削減し、コストのかかるハードウェア更新サイクルの必要性を排除します。
- 耐障害性の向上 – 冗長データストレージ、自動フェイルオーバー、ディザスタリカバリ機能を通じて、耐障害性とビジネス継続性を強化します。
- 意思決定の強化 – 正確で実用的なインサイトへのリアルタイムのアクセスを容易にし、情報に基づいた意思決定を強化し、ビジネスイノベーションを促進します。

# メインフレームデータを にレプリケートする際の主な考慮事項 AWS

メインフレームデータを にレプリケートするジャーニーに取り組む企業は AWS クラウド、慎重な検討と戦略的計画を必要とするいくつかの重要な課題に直面します。組織は、パフォーマンスの最適化、コストの制御、レガシーメインフレームシステムと最新のクラウドサービス間のシームレスな統合を確保しながら、技術的な複雑さを乗り越える必要があります。これらの課題を理解し、効果的に対処することは、運用要件とビジネス目標の両方を満たす mainframe-to-cloud データレプリケーション戦略を成功させるために不可欠です。

戦略計画では、以下の重要な考慮事項に対処する必要があります。

- **データ機密性** – クラウドにデータをレプリケートして保存するときは、データプライバシー規制とセキュリティ標準に従ってください。これは、組織が個人を特定できる情報 (PII) または財務データをメインフレームデータベースに保存する場合に特に重要です。このデータをクラウドに転送する前に、機密性を評価し、一般データ保護規則 (GDPR) や Payment Card Industry Data Security Standard (PCI DSS) などの規制に準拠してください。レプリケーション中および保管中に暗号化を実装し、厳格なアクセスコントロールを適用して、不正アクセスやデータ侵害のリスクを軽減します。
- **ネットワーク帯域幅** – データレプリケーションに使用できるネットワーク帯域幅を評価して、転送がタイムリーで効率的であることを確認します。ネットワークインフラストラクチャが限られているグローバルリージョンやネットワークの輻輳が多いグローバルリージョンで事業を行っている場合、メインフレームからクラウドに大量のデータを転送するのは難しい場合があります。ネットワーク帯域幅評価を実施することで、制限を理解し、レプリケーションスケジュールを最適化できます。たとえば、帯域幅の制約を軽減するために、オフピーク時にデータレプリケーションをスケジュールしたり、データ圧縮手法を実装したりできます。レイテンシーを最小限に抑え、ネットワーク使用率を最適化するため、データの重複排除は、即時のデータ更新が重要なリアルタイムストリーミングシナリオで最も効果的です。
- **データ整合性** – データ整合性とは、クラウド内のレプリケートされたデータがメインフレームトランザクションデータベースに対して行われたリアルタイムの更新を正確に反映する状態を指します。データの一貫性を維持することは、不一致を避けるために重要です。レプリケーション中にメインフレームとクラウド間のデータ整合性を維持するメカニズムを実装します。2 フェーズコミットや変更データキャプチャ (CDC) などのトランザクション整合性プロトコルを実装して、レプリケートされたデータにメインフレームからのリアルタイム更新が反映されるようにします。これにより、両方の環境にわたってデータの整合性が維持されます。

- レイテンシー – レプリケーションがアプリケーションのレイテンシーとパフォーマンスに与える影響を評価します。クラウドへのデータレプリケーションによって生じるレイテンシーは、ユーザーエクスペリエンスとトランザクション処理時間に影響を与える可能性があります。レイテンシーの問題を軽減し、シームレスなアプリケーションパフォーマンスを確保するために、レプリケーションプロセスを最適化したり、専用ネットワーク接続[AWS Direct Connect](#)に使用したり、キャッシュメカニズムをデプロイしたりできます。
- コスト管理 – データレプリケーション、ストレージ、クラウドリソースの使用によるコストへの影響を分析します。慎重なコスト管理がない場合、大量の履歴データを高性能ストレージ階層に保存すると、不要な費用が発生する可能性があります。データライフサイクルポリシーを実装して、アクセス頻度に基づいてデータストレージを階層化できます。また、などのコスト最適化ツールを使用して[AWS Cost Explorer](#)、パフォーマンス要件を満たしながらストレージコストを最適化することもできます。
- 統合の複雑さ – メインフレームシステムとの統合の課題に対処します AWS のサービス。企業がメインフレームベースの顧客関係管理 (CRM) システムに依存しているとします。これらのシステムを AWS のサービス、顧客データを保存するための [Amazon Simple Storage Service \(Amazon S3\)](#) や分析用の [Amazon Redshift](#) などと統合するには、互換性の問題に対処し、データ交換がシームレスであることを確認する必要があります。などのミドルウェアソリューションを実装することも IBM MQ、などのデータ統合 AWS のサービスに使用することもできます [AWS Glue](#)。これらのサービスは、統合プロセスを簡素化し、メインフレーム環境とクラウド環境間のデータフローを合理化します。

これらの考慮事項に対処することで、企業は情報に基づいた意思決定を行い、データレプリケーションの複雑さをクラウドに正常にナビゲートできます。

# メインフレームデータレプリケーションの戦略的アプローチ

メインフレームからへのデータレプリケーション AWS クラウドは、オンプレミスのメインフレームシステムからクラウド環境にデータを転送するプロセスです。

このプロセスを通じて、メインフレームデータ所有者、セキュリティチーム、クラウドアーキテクトなどの関係者が積極的に参加し、移行が成功し、準備していることを確認する必要があります。さらに、ガイドンスと実装のサポートについては、メインフレームのモダナイゼーションに関する専門知識を持つ[AWS プロフェッショナルサービス](#)または[AWS パートナー](#)を採用することを検討してください。

このセクションでは、メインフレームデータレプリケーションの計画と実装に使用できる大まかな戦略的アプローチについて説明します。これには、次のフェーズが含まれます。

1. [評価](#)
2. [準備](#)
3. [移行とモダナイズ](#)
4. [最適化](#)
5. [管理](#)

## 評価

評価フェーズは、mainframe-to-cloudデータ移行戦略を成功させるための基盤となります。この初期段階では、現在のメインフレーム環境を包括的に評価し、ワークロード、データ特性、インフラストラクチャ機能を慎重に分析します。この体系的な評価は、クラウドレプリケーションの候補となるデータセットを特定するのに役立ちます。この分析を通じて、範囲と潜在的な課題を明確に理解できます。

評価フェーズでは、以下を実行します。

1. メインフレームワークロードを評価し、にレプリケートするデータセットを特定します AWS クラウド。
2. データの機密性、コンプライアンス要件、パフォーマンスに関する考慮事項を徹底的に分析します。
3. データレプリケーションの既存のネットワークインフラストラクチャと帯域幅の可用性を評価します。

## 準備

動員フェーズでは、メインフレームシステムとの統合のための技術アーキテクチャ、データの一貫性とセキュリティを維持するための AWS のサービス運用フレームワーク、明確な成功メトリクスの確立という 3 つの基本的な側面に対処する包括的なレプリケーション戦略を開発します。堅牢なセキュリティコントロールを実装するアーキテクチャを設計する際には、さまざまなレプリケーション頻度、同期方法、フェイルオーバーメカニズムを慎重に検討する必要があります。

動員フェーズで以下を実行します。

### 1. 以下を含む詳細なデータレプリケーション戦略を作成します。

- 頻度 – ビジネス要件、データの変動性、ネットワーク帯域幅の可用性に基づいて、データレプリケーションの頻度を決定します。頻度オプションには以下が含まれます。
  - リアルタイムレプリケーションは、作成後すぐにデータをクラウドにコピーするプロセスです。このオプションは、最小限のレイテンシーが必要なトランザクションデータに最適です。
  - ほぼリアルタイムのレプリケーションは、わずかな遅延でデータをクラウドにコピーするプロセスです。このオプションは、中程度のレイテンシーが許容される優先度の高いデータに適しています。
  - スケジュールされたバッチレプリケーションは、スケジュールされた時間にクラウドにデータをコピーするプロセスです。このオプションは、定期的な更新で十分である non-real-time データに適しています。
- 同期方法 – データ整合性を高め、レプリケーションのオーバーヘッドを最小限に抑える適切な同期方法を選択します。同期オプションには以下が含まれます。
  - 変更データキャプチャ (CDC) は、データソースへの変更を追跡し、変更に関するメタデータを記録するプロセスです。このアプローチでは、変更されたデータのみをキャプチャしてレプリケートします。このオプションを使用すると、レプリケーショントラフィックを減らし、効率を向上させることができます。
  - スナップショットレプリケーションは、ある時点でデータセットのコピーを作成し、そのコピーをレプリケートするプロセスです。メインフレームデータの snapshots を定期的に作成し、にレプリケートできます AWS クラウド。このオプションは、動的でないデータセットに適しています。
- フェイルオーバーメカニズム – 継続的な可用性とデータ整合性を促進するフェイルオーバーメカニズムを実装します。フェイルオーバーメカニズムのオプションは次のとおりです。

- アクティブ/パッシブフェイルオーバーは、プライマリリソースとセカンダリリソースを使用する設定です。セカンダリリソースは、プライマリリソースが失敗した場合にのみアクティブ化されます。このアプローチでは、スタンバイレプリカを維持し AWS クラウド、メインフレームが失敗すると自動的にアクティブ化されます。
  - アクティブ/アクティブレプリケーションは、複数のサーバーが読み取りおよび書き込みオペレーションを同時に処理できるようにするデータレプリケーションの方法です。このアプローチでは、メインフレームデータをクラウド AWS リージョン 内の複数の に同時にレプリケートします。このアプローチは、高可用性とディザスタリカバリが必要な場合に適しています。
2. メインフレームシステムを と統合するためのアーキテクチャを設計し AWS のサービス、データの一貫性とセキュリティを設計します。アーキテクチャは、以下に対処する必要があります。
- との統合 AWS のサービス – 設計では以下を考慮することをお勧めします。
    - レプリケーションツール – [AWS Database Migration Service \(AWS DMS\)](#) またはサードパーティーのレプリケーションツールを使用します。
    - ストレージ – レプリケートされたデータは、スケーラビリティと耐久性を提供するため、[Amazon Simple Storage Service \(Amazon S3\)](#) に保存します。
    - データウェアハウス – データウェアハウスと分析に [Amazon Redshift](#) を使用します。このサービスは、レプリケートされたメインフレームデータからインサイトを抽出するのに役立ちます。
    - コンピューティング – [AWS Lambda](#) 関数または [Amazon Elastic Compute Cloud \(Amazon EC2\)](#) インスタンスをデプロイして、レプリケートされたデータを処理し、データ変換を実行します。
  - データの一貫性とセキュリティ – 設計では以下を考慮することをお勧めします。
    - 暗号化 – [AWS Key Management Service \(AWS KMS\)](#) を使用して、転送中と保管中の両方のデータを暗号化します。
    - アクセスコントロール – レプリケートされたデータへのアクセスを制御する [AWS Identity and Access Management \(IAM\)](#) ロールとポリシーを実装します。ユーザーの役割と責任に基づいてアクセス許可を制限します。
    - データ検証 – レプリケーション中にチェックを実行して、メインフレーム環境とクラウド環境間のデータ整合性と整合性を検証します。
    - モニタリングと監査 – [AWS CloudTrail](#) と [Amazon CloudWatch](#) を使用してレプリケーションプロセスをモニタリングし、レプリケートされたデータへのアクセスを監査します。
3. レプリケーションプロセスの成功とアプリケーションのパフォーマンスへの影響を測定するための明確なメトリクスを確立します。メトリクスには以下が含まれます。

- データの完全性 – レプリケートされたデータの完全性をソースと比較してモニタリングし、欠落または不完全なレコードを検出できるようにします。
- アプリケーションパフォーマンス – データレプリケーションの実装前後のアプリケーションの応答時間とスループットを追跡して、パフォーマンスへの影響を特定できます。
- コスト効率 – データレプリケーションと AWS クラウド 使用状況のコスト効率を評価し、オンプレミスインフラストラクチャのコストと比較できるようにします。

## 移行とモダナイズ

移行およびモダナイズフェーズでは、メインフレームからクラウドにデータをレプリケートし、レプリケーションを検証します。この重要なフェーズでは、適切なレプリケーション方法の実装、重要なツールのデプロイ、メインフレーム環境とクラウド環境間の安全なデータパスの確立を行います。従来のメインフレームシステムと最新のクラウドサービスの統合を慎重に調整しながら、堅牢なセキュリティ対策を維持し、移行プロセス全体でデータの整合性を確保する必要があります。このフェーズを成功させるには、技術的な実装、セキュリティコンプライアンス、レプリケーションプロセスの徹底的な検証に対するバランスの取れたアプローチが必要です。

移行とモダナイズのフェーズでは、以下を実行します。

1. レプリケーション方法を選択します。メインフレームデータをレプリケートするには AWS、CDC やスケジュールされたバッチレプリケーションなど、いくつかのアプローチがあります。
2. データレプリケーションツールをデプロイし、メインフレームとクラウドの間でレプリケーションワークフローを設定します。、[Amazon MQApache Kafka](#)、Amazon [Redshift](#)、[Amazon Amazon Relational Database Service RDS](#)) などのサービスやツールを使用できます。
3. 転送中または保管中のデータを保護するために、暗号化やアクセスコントロールなどの必要なセキュリティ対策を実装します。
4. レプリケーションプロセスを徹底的にテストして、データの整合性と信頼性を検証します。

## 最適化

最適化フェーズは、レプリケーションプロセスを微調整してピーク効率を実現するのに役立ちます。このフェーズでは、スケーリングの柔軟性を維持しながら、最適なパフォーマンス、コスト効率、運用レジリエンスを確保するバランスの取れたフレームワークの確立に焦点を当てます。

最適化フェーズで以下を実行します。

1. データレプリケーションプロセスのパフォーマンスを継続的にモニタリングし、必要に応じて設定パラメータを調整します。
2. AWS リソースを最適化して、パフォーマンス要件を満たしながらコストを最小限に抑えます。
3. 問題を迅速に検出して対処するのに役立つ堅牢なモニタリングおよびアラートメカニズムを実装します。
4. データボリュームや追加のデータソースの将来の増加に対応するためのスケーラビリティを計画します。

## 管理

管理フェーズでは、データ管理オペレーションにおける制御、コンプライアンス、説明責任を維持するための重要なフレームワークを確立します。このフェーズでは、データアセットを保護し、規制要件と業界標準の遵守に役立つ重要なポリシーと手順を実装します。構造化されたガバナンスメカニズムを通じて、機密情報の保護に役立つ安全で準拠した環境を作成できます。

管理フェーズで以下を実行します。

1. データレプリケーションのプロセスと AWS クラウド 使用状況を管理するためのガバナンスポリシーと手順を確立します。
2. 一般データ保護規則 (GDPR) や医療保険の相互運用性と説明責任に関する法律 (HIPAA) などの規制要件と業界標準への準拠を検証します。
3. ガバナンスとコンプライアンスのガイドラインへの準拠を検証するために、定期的な監査とレビューを実施します。

# メインフレームデータを にレプリケートするためのユースケース AWS クラウド

このセクションでは、へのメインフレームデータレプリケーションの主要な候補として浮上したいいくつかの一般的なユースケースについて説明します AWS クラウド。これらのユースケースは、さまざまな業界や運用要件にまたがり、それぞれに固有の課題と機会があります。これらのシナリオでは、データレプリケーションはビジネスのイノベーション、俊敏性、回復性を促進する上で重要な役割を果たします。

このセクションでは、以下のユースケースについて説明します。

- [ユースケース 1: データキャプチャを変更する](#)
- [ユースケース 2: リアルタイムレポートとダッシュボード](#)
- [ユースケース 3: メッセージングプロトコル](#)
- [ユースケース 4: 新しいチャネルとインターフェイス](#)
- [ユースケース 5: 規制コンプライアンスとデータアーカイブ](#)
- [ユースケース 6: オフロード処理とバッチレプリケーション](#)

## ユースケース 1: データキャプチャを変更する

変更データキャプチャ (CDC) は、ほぼリアルタイムのデータレプリケーションが必要なシナリオに最適です。変更されたデータのみをメインフレームから にキャプチャしてレプリケートします AWS クラウド。これにより、レプリケーションのオーバーヘッドとレイテンシーが最小限に抑えられます。

### 選択基準

- リアルタイムまたはほぼリアルタイムのデータレプリケーション要件
- レイテンシーに対する耐性が低い高頻度のデータ更新
- ネットワーク帯域幅とリソースを効率的に活用する必要がある

### 利点

- レプリケーションのオーバーヘッドとネットワーク帯域幅使用率の削減

- レイテンシーを最小限に抑えることで、更新されたデータをより早く利用可能に
- 変更されたデータの選択的レプリケーションによるリソースの効率的な使用

### 欠点

- CDC メカニズムの実装と管理の複雑さ
- 変更のキャプチャによるメインフレームシステムのリソース使用率の向上の可能性
- CDC ツールとプロセスの信頼性とパフォーマンスへの依存

### 方針

- メインフレームデータベースおよび互換性のある CDC ツールを選択する AWS のサービス
- 関連するデータ変更のみをキャプチャしてレプリケートするように CDC ツールを設定する
- モニタリングと検証のメカニズムを実装して、データの一貫性と信頼性を維持する
- 継続的な可用性とデータ整合性を促進するフェイルオーバーメカニズムの実装を検討する

## ユースケース 2: リアルタイムレポートとダッシュボード

即時の可視化と分析のために、リアルタイムのレポートとダッシュボードには、メインフレームシステムからへの継続的なデータレプリケーションが必要です AWS クラウド。このユースケースは、銀行、保険、小売、医療、製造などの意思決定にリアルタイムのインサイトが重要な業界で一般的です。

### 選択基準

- 分析と視覚化のために更新されたデータにすぐにアクセスする必要がある
- ビジネスメトリクスと主要業績評価指標 (KPIs) のリアルタイムモニタリングの要件
- 意思決定プロセスにおける俊敏性と応答性に対する高い需要

### 利点

- リアルタイムの分析と意思決定のために、更新されたデータへの即時アクセスを提供します
- ビジネスパフォーマンスとタイムリーな介入のプロアクティブモニタリングを可能にします
- ステークホルダーのデータの動的でインタラクティブな視覚化を促進します

## 欠点

- リアルタイムの更新を実現するためのデータレプリケーションと処理の複雑さの増大
- 継続的なレプリケーションによるリソース消費量とインフラストラクチャコストの増加
- データの鮮度と信頼性を検証するための堅牢なモニタリングとアラートメカニズムへの依存

## 方針

- リアルタイムデータレプリケーション用の CDC またはメッセージングプロトコルを実装する
- [Amazon Kinesis Data Streams](#) AWS のサービスなどの を使用したリアルタイムのデータストリーミングと処理
- データのリアルタイムレポートおよびダッシュボードソリューションを設計してデプロイ AWS クラウドし、更新されたデータにすぐにアクセスできるようにします。
- モニタリングとアラートのメカニズムを実装して、データレプリケーションの問題を迅速に検出して対処する

## ユースケース 3: メッセージングプロトコル

Apache Kafka や などのメッセージングプロトコルとシステムは IBM MQ、メインフレームと 間の非同期通信とデータ転送を容易にします AWS クラウド。分離されたスケーラブルなデータ統合を必要とするシナリオに適しています。

### 選択基準

- 非同期データ転送要件
- スケーラブルで分離されたデータ統合アーキテクチャの必要性
- 低レイテンシーでのリアルタイムまたはほぼリアルタイムのデータレプリケーションのサポート

### 利点

- 柔軟なデータ統合を可能にする、分離されたスケーラブルなアーキテクチャ
- 低レイテンシーでのリアルタイムまたはほぼリアルタイムのデータレプリケーションのサポート
- 信頼性、メッセージキューイング、耐障害性のための組み込み機能

## 欠点

- メッセージングインフラストラクチャの設定と管理の複雑さ
- リソースの消費量と運用オーバーヘッドが増加する可能性
- メッセージングプラットフォームの信頼性とパフォーマンスへの依存

## 方針

- メインフレームと の両方と互換性のあるIBM MQ、 Apache Kafkaや などのメッセージングシステムを選択します。 AWS クラウド
- データ転送とレプリケーションを容易にするメッセージングトピックまたはキューを設計する
- メインフレームとクラウドにメッセージプロデューサーとコンシューマーを実装してデータを交換する
- モニタリングとアラートのメカニズムを設定して、メッセージ処理とレプリケーションの信頼性を検証する

## ユースケース 4: 新しいチャネルとインターフェイス

メインフレームチャネルは、メインフレームコンピュータとの間でデータを移動する接続です。チャネルはチャネルサブシステムの一部です。すぐに公開して消費するには、新しいチャネルとインターフェイスにメインフレームシステムからクラウドへの継続的なデータレプリケーションが必要です。

### 選択基準

- 新しいチャネルの更新データにすぐにアクセスする必要がある
- 新しいインターフェイスを使用したメインフレームデータへのアクセス
- 新しいチャネルの需要が高い
- さまざまなシステム、プラットフォーム、またはクラウド環境との統合

### 利点

- 新しいチャネルがメインフレームデータを消費できるようにしてメインフレームデータアクセスをロック解除する
- さまざまなシステム、プラットフォーム、またはクラウド環境との統合を容易にする
- さまざまなインフラストラクチャ間でより柔軟で効率的なデータ移動を可能にする

## 欠点

- データレプリケーション用の新しいインターフェイスまたはチャンネルを導入するには、データを保護し、規制に準拠するための追加のセキュリティ対策が必要になる場合があります。
- 新しいインターフェイスを既存のシステムやワークフローと統合するのは、特に複雑な環境やレガシー環境では難しい場合があります。

## 方針

- リアルタイムデータレプリケーション用の CDC またはメッセージングプロトコルを実装する
- Kinesis Data Streams AWS のサービスなどの を使用してリアルタイムのデータストリーミングと処理を行う
- モニタリングとアラートのメカニズムを実装して、データレプリケーションの問題を迅速に検出して対処する

## ユースケース 5: 規制コンプライアンスとデータアーカイブ

規制コンプライアンスとデータアーカイブには、メインフレームデータをクラウドにレプリケートして長期保存することが含まれます。データ保持ポリシーと規制を遵守することが重要です。このユースケースは、銀行、医療、医薬品などの規制対象業界で一般的です。

### 選択基準

- 規制コンプライアンスまたは法的要件のために履歴データの長期保存が必要
- アーカイブされたデータに対する安全でスケーラブルなストレージソリューションの要件
- データプライバシー規制と、データ保持とアーカイブに関する業界固有の義務の遵守

### 利点

- データ保持に関する規制要件と業界固有の義務の遵守
- 履歴データの長期アーカイブのためのスケーラブルで費用対効果の高いストレージソリューション
- 監査または法的目的でのアーカイブデータへの効率的な取得とアクセス

### 欠点

- アーカイブされたデータの効率的な取得とアクセスのための管理と整理の複雑さ

- 大量のデータの長期保持に関連するストレージコストの増加の可能性
- アーカイブされたデータを不正アクセスから保護するための堅牢なデータ暗号化とアクセスコントロールへの依存

## 方針

- データライフサイクルポリシーを実装して、履歴データのアーカイブと保持を自動化する
- Amazon Glacier AWS ストレージクラスなどのストレージサービスを使用して、コスト効率の高い長期ストレージを実現する [Amazon Glacier](#)
- 保管中のアーカイブデータを暗号化し、不正アクセスの防止に役立つアクセスコントロールを実装する
- アーカイブされたデータへのアクセスを追跡し、規制要件に準拠する監査証跡とログ記録メカニズムを確立する

## ユースケース 6: オフロード処理とバッチレプリケーション

オフロード処理とバッチレプリケーションでは、メインフレームからデータを抽出してにロードする定期的なバッチジョブをスケジュールします AWS クラウド。リアルタイムレプリケーションが不要で、バッチ処理が許容されるシナリオに適しています。

### 選択基準

- リアルタイムのデータレプリケーションは不要
- バッチ処理はデータ更新で許容されます
- レイテンシーに対する耐性が中程度のデータ更新の頻度が低い

### 利点

- データ変換、圧縮、暗号化などのコンピューティング負荷の高いオペレーションをプライマリメインフレームシステムからオフロードすると、システム全体のパフォーマンスが向上し、ボトルネックが軽減されます。
- 予測可能なリソース使用率とメインフレームシステムへの影響の軽減
- ビジネス要件に基づくレプリケーションジョブのスケジュールの柔軟性

## 欠点

- リアルタイムまたはほぼリアルタイムのレプリケーションと比較して、データ可用性のレイテンシーが長くなる
- 定期的な更新によるメインフレームとクラウド間のデータ不整合の可能性
- 更新されたデータへのタイムリーなアクセスを必要とするシナリオへの適合性が限られている

## 方針

- メインフレームからデータを抽出してロードするバッチレプリケーションジョブを開発する AWS クラウド
- ビジネス要件とデータ更新頻度に基づいてレプリケーションジョブをスケジュールする
- チェックを実装してデータの整合性と整合性を検証する
- レイテンシーとリソースの消費を減らすためにバッチレプリケーションプロセスを最適化することを検討する

## 次のステップとリソース

このガイドの「[メインフレームデータレプリケーションの戦略的アプローチ](#)」で説明されているように、最初のステップはメインフレームデータレプリケーションジャーニーの評価と計画を開始することです。このガイドは、執行役、IT 担当者、インフラストラクチャチーム、データリーダーシップなど、組織内の関係者と共有することをお勧めします。

詳細な評価および計画サービスについては、[AWS プロフェッショナルサービス](#)にお問い合わせください。これらのエキスパートは、組織がメインフレーム移行とモダナイゼーションのニーズを満たすのに役立ちます。

また、次のリソースとを確認することをお勧めします AWS のサービス。

## リソース

### AWS ドキュメント

- [Amazon Kinesis Data Streams](#) (Amazon Kinesis ドキュメント)
- [Amazon Redshift Serverless データウェアハウス](#) (Amazon Redshift ドキュメント)
- [Connect from を使用して VSAM ファイルを Amazon RDS または Amazon MSK に移行およびレプリケートする Precisely](#) (AWS 規範ガイド)
- [組織を動員して大規模な移行を加速する](#) (AWS 規範ガイド)
- [を使用してメインフレームデータベースを AWS にレプリケートPrecisely Connectする](#) (AWS 規範ガイド)

### その他の AWS リソース

- [AWS クラウド導入フレームワーク \(AWS CAF\)](#)
- [AWS Well-Architected フレームワーク](#)

### その他のツールとサービス

- [Apache Kafka](#)
- [IBM MQ](#)

## ドキュメント履歴

以下の表は、本ガイドの重要な変更点について説明したものです。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
<a href="#">初版発行</a>	—	2025 年 2 月 17 日

# AWS 規範ガイドの用語集

以下は、AWS 規範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を購入したり、アプリケーションを書き換えたり、既存の運用を変更したりすることなく、インフラストラクチャをクラウドに移行できます。オンプレミスプラットフォームから同じプラットフォームのクラウドサービスにサーバーを移行します。例: Microsoft Hyper-V アプリケーションをに移行します AWS。
- 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。
- 廃止 — 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制御](#)」をご覧ください。

### 抽象化されたサービス

「[マネージドユーザー](#)」をご覧ください。

### ACID

「[原子性、一貫性、分離性、耐久性 \(ACID\)](#)」をご覧ください。

### 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](#)よりも柔軟な方法ですが、さらに多くの作業が必要となります。

### 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

複数行に処理を行い、グループ全体を対象に単一の戻り値を計算する SQL 関数。集計関数の例としては、SUM や MAX などがあります。

### AI

「[人工知能](#)」をご覧ください。

### AIOps

「[AI オペレーション](#)」をご覧ください。

### 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

繰り返し起こる問題に対して頻繁に用いられる解決策で、その解決策が逆効果であったり、効果がなかったり、代替案よりも効果が低かったりするもの。

### アプリケーション制御

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](#)の重要な要素であり、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?](#)」をご覧ください。

### 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「[の ABAC AWS](#)」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ー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 (AZ)

他のアベイラビリティゾーンの障害から AWS リージョン 隔離され、同じリージョン内の他のアベイラビリティゾーンへの低コストで低レイテンシーのネットワーク接続を提供する 内の別の場所。

## AWS クラウド導入フレームワーク (AWS CAF)

組織がクラウドへの移行を成功させるための効率的で効果的な計画を立て AWS するための、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です。AWS CAF 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、運用という 6 つの重点分野にガイドランスを整理しています。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、組織がクラウド導入を成功させるための準備を支援します。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 ワークロード認定フレームワーク (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、作業見積もりを提供するツール。AWS WQF は AWS Schema Conversion Tool (AWS SCT) に含まれています。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

## 不正なボット

個人や組織に混乱や損害を与えることを目的とした [ボット](#)。

## BCP

「[ビジネス継続性計画 \(BCP\)](#)」をご覧ください。

## 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「[動作グラフのデータ](#)」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](#)」もご覧ください。

## 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。

## ブルー/グリーンデプロイ

それぞれが独立しているが、同一の環境を 2 つ作成するデプロイ戦略。現在のアプリケーションバージョンを 1 つの環境 (ブルー) で実行し、新しいアプリケーションバージョンを別の環境 (グリーン) で実行します。この戦略は、最小限の影響で迅速にロールバックするのに役立ちます。

## ボット

インターネット経由で自動タスクを実行し、人間のアクティビティややり取りをシミュレートするソフトウェアアプリケーション。インターネット上の情報のインデックスを作成するウェブクローラーなど、一部のボットは有用または有益です。悪質なボットと呼ばれる他のボットの中には、個人や組織を混乱させたり、損害を与えたりすることを意図したものもあります。

## ボットネット

[マルウェア](#)に感染しており、ボットハーダーまたはボットオペレーターと呼ばれる単一の当事者によって制御されている[ボット](#)のネットワーク。ボットネットは、ボットとその影響力を拡大する仕組みとして、非常によく知られています。

## 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、「[ブランチの概要](#)」(GitHub ドキュメント)を参照してください。

## ブレイクグラスアクセス

例外的な状況では、承認されたプロセスを通じて、ユーザーが AWS アカウント 通常アクセス許可を持たないにすばやくアクセスできるようにします。詳細については、AWS Well-Architected ガイドの「[ブレイクグラス手順の実装](#)」インジケータを参照してください。

## ブラウн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н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н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、[AWSでのコンテナ化されたマイクロサービスの実行](#)ホワイトペーパーの「[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

## カナリアデプロイ

エンドユーザーへのバージョンリリースを、時間をかけて段階的に行うこと。確信が持てたら新規バージョンをデプロイして、現在のバージョン全体を置き換えます。

## 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

障害や破壊的なイベントを意図的に導入して、システムの耐障害性をテストすること。[AWS Fault Injection Service \(AWS FIS\)](#) を使用して、AWS ワークロードにストレスを与え、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

ターゲットがデータ AWS のサービスを受信する前のローカルでのデータの暗号化。

## 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 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、一般的に、[エッジコンピューティング](#)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、AWS クラウド エンタープライズ戦略ブログのブログ記事「[クラウドファーストへのジャーニー](#)」と「[導入のステージ](#)」で Stephen Orban によって定義されました。AWS 移行戦略との関連性については、「[移行準備ガイド](#)」を参照してください。

### CMDB

「[構成管理データベース \(CMDB\)](#)」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 や Bitbucket Cloud があります。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 (CV)

機械学習を使用してデジタルイメージやビデオといった、ビジュアル形式の情報を分析および抽出する [AI](#) の分野。例えば、Amazon SageMaker AI では、CV 用の画像処理アルゴリズムを利用できます。

## 設定ドリフト

ワークロードにおいて、設定が想定した状態から変化すること。これによって、ワークロードが非準拠になる可能性があります。この状態は、徐々に生じ、意図的なものではありません。

## 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。

## コンフォーマンスパック

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するためにアセンブルできる AWS Config ルールと修復アクションのコレクション。YAML テンプレートを使用して、コンフォーマンスパックを AWS アカウント および リージョンの単一のエンティティとしてデプロイすることも、組織全体にデプロイすることもできます。詳細については、AWS Config ドキュメントの「[コン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。

## CV

[「コンピュータビジョン」](#) 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コンポーネントです。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。

## データメッシュ

非一元的で分散型のデータ所有権を持つとともに、一元的な管理およびガバナンスを行えるアーキテクチャフレームワーク。

## 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。でデータ最小化を実践 AWS クラウドすることで、プライバシーリスク、コスト、分析のカーボンフットプリントを削減できます。

## データ境界

AWS 環境内の一連の予防ガードレール。信頼できる ID のみが、期待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します。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。データウェアハウスには、一般的に、大量の履歴データが含まれており、多くの場合、それらはクエリや分析に使用されます。

## 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ます。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。

## 深層学習

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。

## 多層防御

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。この戦略を採用するときは AWS、リソースの保護に役立つように、AWS Organizations 構造の異なるレイヤーに複数のコントロールを追加します。たとえば、多層防御アプローチでは、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

では AWS Organizations、互換性のあるサービスが AWS メンバーアカウントを登録して組織のアカウントを管理し、そのサービスのアクセス許可を管理できます。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で利用できるサービス](#)」を参照してください。

## トラブルシューティング

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、「AWSでのセキュリティコントロールの実装」の「[検出的コントロール](#)」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](#)において、ファクトテーブルの定量データに関するデータ属性が含まれる小さいテーブル。ディメンションテーブルの属性は、通常、テキストフィールド、またはテキストのように扱える個別の数値で示されます。これらの属性は、一般的に、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使用されます。

## デザスタ

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。

## ディザスタリカバリ (DR)

[ディザスタ](#)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の戦略とプロセス。詳細については、AWS Well-Architected フレームワークの「[でのワークロードのディザスタリカバリ](#)」[AWS: クラウドでのリカバリ](#)」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偏差を追跡します。たとえば、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、を使用して AWS Control Tower、ガバナンス要件のコンプライアンス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

「[開発バリューSTREAMマッピング](#)」を参照してください。

## E

### EDA

「[探索的データ分析](#)」を参照してください。

### EDI

「[電子データ交換](#)」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、応答時間を改善できます。

## 電子データ交換 (EDI)

組織間で行う、ビジネスドキュメントの自動交換。詳細については、[「電子データ交換とは」](#)を参照してください。

## 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処理。

## 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す。

## 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。を使用してエンドポイントサービスを作成し AWS PrivateLink、他の AWS アカウント または AWS Identity and Access Management (IAM) プリンシパルにアクセス許可を付与できます。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。

## エンタープライズリソースプランニング (ERP)

エンタープライズの主要なビジネスプロセス (会計、[MES](#)、プロジェクト管理など) を自動化および管理するシステム。

## 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、ID とアクセスの管理、検出コントロール、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。

### ERP

「[エンタープライズリソース計画](#)」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

[スタースキーマ](#)の中央にあるテーブル。ビジネスオペレーションに関する定量的データが保存されます。一般的に、ファクトテーブルは、2種類の列で構成されます。1つは測定値が含まれる列、もう1つはディメンションテーブルへの外部キーが含まれる列です。

### フェイルファスト

開発ライフサイクルを短縮するために、頻繁かつ段階的にテストを行う哲学であり、アジャイルアプローチでは、この考え方がきわめて重要です。

### 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高めるのに役立つ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、「[を使用した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。

### 数ショットプロンプト

[LLM](#) に、タスクと望ましい出力を示す例を少数提示した後に、類似のタスクを実行させること。この手法は、プロンプトに記述された例(ショット)からモデルが学習する「インコンテキスト学

習」の一種です。数ショットプロンプトは、特定のフォーマット、推論、専門知識が必要なタスクに効果的です。「[ゼロショットプロンプト](#)」も参照してください。

## FGAC

「[きめ細かなアクセス制御](#)」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

[変更データのキャプチャ](#)による継続的なデータ複製を利用して、段階的なアプローチではなく、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。

## FM

「[基盤モデル](#)」を参照してください。

### 基盤モデル (FM)

大規模な深層学習ニューラルネットワークであり、一般化およびラベル付けされていないデータからなる大規模データセットでトレーニングされています。FMにより、言語理解、テキストおよび画像生成、自然言語での会話といった、一般的な各種タスクを実行できます。詳細については、「[基盤モデルとは何ですか?](#)」を参照してください。

## G

### 生成 AI

[AI](#) モデルのサブセット。大量のデータでトレーニングされており、シンプルなテキストプロンプトを使用して、画像、動画、テキスト、オーディオなどの新しいコンテンツやアーティファクトを作成できます。詳細については、「[生成 AI とは何ですか?](#)」を参照してください。

### ジオブロッキング

「[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)

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ための、Amazon CloudFront のオプション。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 ワークフローは古いと見なされている方法であり、[トランクベースのワークフロー](#)は推奨されている新しい方法です。

## ゴールデンイメージ

システムまたはソフトウェアのスナップショットであり、システムまたはソフトウェアの新規インスタンスをデプロイするテンプレートとして使用されます。製造の例で言えば、ゴールデンイメージを使用すると、複数のデバイスにソフトウェアをプロビジョニングして、デバイス製造オペレーションの速度、スケーラビリティ、生産性を向上させることができます。

## 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、AWS Security Hub CSPM、Amazon GuardDuty、AWS Trusted Advisor Amazon Inspector、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 (HA)

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。

## ヒストリアンの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) システムをモダナイズし、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。

## ホールドアウトデータ

[機械学習](#)モデルのトレーニング用データセットから保留される、ラベル付き履歴データの一部。ホールドアウトデータを使用すると、モデル予測をホールドアウトデータと比較して、モデルのパフォーマンスを評価できます。

## 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。緊急性が高いため、通常の DevOps のリリースワークフローからは外れた形で実施されます。

## 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

### IaC

「[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する 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

「[インダストリアル IoT](#)」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

既存インフラストラクチャの更新、パッチ適用、変更などを行わずに、本番環境ワークロードに使用する新規インフラストラクチャをデプロイするモデル。本質的に、イミュータブルインフラストラクチャは、[ミュータブルインフラストラクチャ](#)よりも一貫性、信頼性、予測性に優れています。詳細については、AWS Well-Architected フレームワークにある「[イミュータブルインフラストラクチャを使用してデプロイする](#)」のベストプラクティス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では、アプリケーションの外部から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。

## インダストリー 4.0

2016 年に [Klaus Schwab](#) 氏が提唱した用語で、接続、リアルタイムデータ、オートメーション、分析、AI/ML の進歩による、ビジネスプロセスのモダナイズを意味します。

## 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。

## インダストリアル 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、「[インダストリアル IoT \(IIoT\) デジタルトランスフォーメーション戦略の構築](#)」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では、VPC (同一または異なる 内 AWS リージョン)、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 VPCs。 [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、[「を使用した機械学習モデルの解釈可能性 AWS」](#)を参照してください。

## IoT

[「IoT」](#)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、スケーラブルで安全な、適切に設計されたマルチアカウント 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。

## 大規模言語モデル (LLM)

大量のデータで事前トレーニングされた深層学習 AI モデル。LLM では、質問への回答、ドキュメントの要約、他言語へのテキスト翻訳、文を完成させるなど、さまざまなタスクを実行できます。詳細については、「[大規模言語モデル \(LLM\) とは何ですか?](#)」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

「[ラベルベースアクセス制御](#)」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](#)」もご覧ください。

### LLM

「[大規模言語モデル](#)」を参照してください。

### 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。

## マルウェア

コンピュータのセキュリティやプライバシーを侵害するように設計されたソフトウェア。マルウェアは、コンピュータシステムの中断、機密情報の漏洩、不正アクセスを招く可能性があります。マルウェアの例には、ウイルス、ワーム、ランサムウェア、トロイの木馬、スパイウェア、キーロガーなどがあります。

## マネージドサービス

AWS のサービスは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 AWS を運用し、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します。マネージドサービスの例として、Amazon Simple Storage Service (Amazon S3) と Amazon DynamoDB が挙げられます。このサービスは、抽象化されたサービスとも呼ばれます。

## 製造実行システム (MES)

生産プロセスを追跡、モニタリング、文書化、制御するソフトウェアシステムであり、工場では、これによって、原材料から製品を完成させます。

## MAP

[「Migration Acceleration Program」](#) を参照してください。

## メカニズム

ツールを作成してその導入を推進し、導入結果を調べて調整を行うための包括的なプロセス。メカニズムとは、運用中にそれ自体を強化し改善するサイクルを意味します。詳細については、AWS 「Well-Architected フレームワーク」の [「メカニズムの構築」](#) を参照してください。

## メンバーアカウント

組織の一部である管理アカウント AWS アカウント 以外のすべて AWS Organizations。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。

## MES

[「製造実行システム」](#) を参照してください。

## Message Queuing Telemetry Transport (MQTT)

[発行/サブスクリプション](#) のパターンに基づく、軽量のマシンツーマシン (M2M) 通信プロトコルであり、リソースに限りのある [IoT](#) デバイスに使用されます。

## 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たマイクロサービスの統合」](#)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、「[でのマイクロサービスの実装 AWS](#)」を参照してください。

## Migration Acceleration Program (MAP)

組織がクラウドに移行する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、運用、ビジネスアナリストおよび所有者、移行エンジニア、デベロッパー、および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は、ターゲットサブネット、セキュリティグループ、AWS アカウントなどがあります。

## 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 への移行をリホストします。

## Migration Portfolio Assessment (MPA)

オンラインツール。これによって、AWS クラウドに移行するビジネスケースの検証に必要な情報を得られます。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 AWS コンサルタントと APN パートナー コンサルタントが無料で利用できます。

## 移行準備状況評価 (MRA)

AWS CAF を使用して、組織のクラウド準備状況に関するインサイトを取得し、長所と短所を特定し、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、「[組織を動員し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。

## 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 クラウドで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。

### MPA

「[Migration Portfolio Assessment](#)」を参照してください。

### MQTT

「[Message Queuing Telemetry Transport](#)」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。

### ミュータブルなインフラストラクチャ

本番ワークロードに使用する既存のインフラストラクチャを更新および変更するためのモデル。Well-Architected AWS フレームワークでは、一貫性、信頼性、予測可能性を向上させるために、[イミュータブルインフラストラクチャ](#)の使用をベストプラクティスとして推奨しています。

## O

### OAC

「[オリジンアクセス制御](#)」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

「[オペレーション統合](#)」を参照してください。

## Ola

「[オペレーショナルレベルアグリーメント](#)」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に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。

## OPC-UA

「[Open Process Communications - Unified Architecture](#)」を参照してください。

## Open Process Communications - Unified Architecture (OPC-UA)

産業オートメーション用のマシンツーマシン (M2M) 通信プロトコル。OPC-UA により、相互運用の際に、データ暗号化、認証、認可の各スキームを標準化できます。

## 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 (ORR)

質問と関連するベストプラクティスのチェックリスト。インシデントや起こり得る障害を理解、評価、防止したり、その範囲を縮小したりする際に役立ちます。詳細については、AWS Well-Architected フレームワークの「[Operational Readiness Reviews \(ORR\)](#)」を参照してください。

## 運用テクノロジー (OT)

産業オペレーション、機器、インフラストラクチャを制御するために物理環境と連携させるハードウェアおよびソフトウェアシステム。製造分野では、[Industry 4.0](#) への変革を進める上で、OT と情報技術 (IT) システムの統合に焦点が当てられています。

## 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

組織 AWS アカウント 内のすべてのイベント AWS CloudTrail をログに記録することによって作成された証跡 AWS Organizations。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、CloudTrail ドキュメントの「[組織の証跡の作成](#)」を参照してください。

## 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化のスピードにより、このフレームワークは人材アクセラレーションと呼ばれます。詳細については、[OCM ガイド](#)を参照してください。

## オリジンアクセス制御 (OAC)

Amazon Simple Storage Service (Amazon S3) コンテンツを保護するための、CloudFront のアクセス制限の強化オプション。OAC は AWS リージョン、すべての S3 バケット、AWS KMS (SSE-KMS) によるサーバー側の暗号化、S3 バケットへの動的 PUT および DELETE リクエストをサポートします。

## オリジンアクセスアイデンティティ (OAI)

CloudFront の、Amazon S3 コンテンツを保護するためのアクセス制限オプション。OAI を使用すると、CloudFront が、Amazon S3 に認証可能なプリンシパルを作成します。認証されたプリンシパルは、S3 バケット内のコンテンツに、特定の CloudFront ディストリビューションを介してのみアクセスできます。[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制御が可能です。

## ORR

「[運用準備状況レビュー](#)」を参照してください。

## OT

「[運用テクノロジー](#)」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は、アプリケーション内から開始され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。

## PLC

「[プログラマブルロジックコントローラー](#)」を参照してください。

## PLM

「[製品ライフサイクル管理](#)」を参照してください。

## ポリシー

次の操作を可能にするオブジェクト: アクセス許可を定義する ([ID ベースのポリシー](#)を参照)。アクセス条件を指定する ([リソースベースのポリシー](#)を参照)。AWS Organizations の組織における全アカウントにアクセス許可の上限を定義する ([サービスコントロールポリシー](#)を参照)。

## 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。

## 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、「[移行の準備状況の評価](#)」を参照してください。

## 述語

true または false を返すためのクエリ条件。一般的に、WHERE 句に記述されます。

## 述語プッシュダウン

データベースクエリを最適化する手法。これによって、転送前にクエリ内のデータをフィルタリングします。この手法を取ると、リレーショナルデータベースから取得し処理する必要のあるデータの量が減少するため、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、「AWSでのセキュリティコントロールの実装」の「[予防的コントロール](#)」を参照してください。

## プリンシパル

アクションを実行し AWS、リソースにアクセスできるのエンティティ。このエンティティは通常、IAM AWS アカウントロール、またはユーザーのルートユーザーです。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](#)」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

開発プロセス全体を通してプライバシーが考慮されている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

非準拠リソースのデプロイ防止を目的とした[セキュリティコントロール](#)。このコントロールにより、プロビジョニング前にリソースをスキャンします。コントロールに準拠していないリソースは、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「[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

## 製品ライフサイクル管理 (PLM)

製品の設計、開発、発売から、成長、成熟、衰退、廃棄に至る、製品のライフサイクル全体を通してデータとプロセスを管理すること。

## 本番環境

「[環境](#)」を参照してください。

## プログラマブルロジックコントローラー (PLC)

製造分野で使用される、信頼性と適応性に優れたコンピュータであり、これによって、マシンをモニタリングするとともに、製造プロセスを自動化します。

## プロンプトチェイニング

1 つの [LLM](#) プロンプトによる出力を次のプロンプトの入力に使用して、より良いレスポンスを生成します。この手法を使用すると、複雑なタスクをサブタスクに分割したり、事前レスポンスを繰り返し改良または拡張したりできます。これによって、モデルのレスポンスの精度と関連性が向上し、粒度の高いパーソナライズされた結果を得られます。

## 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。

## 発行/サブスクライブ (pub/sub)

マイクロサービス間の非同期通信を可能にするパターン。これにより、スケーラビリティと応答性を向上させます。例えば、マイクロサービスベースの [MES](#) の場合、マイクロサービスは、他のマイクロサービスがサブスクライブ可能なチャンネルにイベントメッセージを発行できます。このシステムでは、発行サービスの変更なしに、新規マイクロサービスを追加できます。

## Q

### クエリプラン

手順などの一連のステップであり、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ます。

### 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

「[実行責任者、説明責任者、協業先、報告先 \(RACI\)](#)」を参照してください。

### RAG

「[検索拡張生成](#)」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

「[実行責任者、説明責任者、協業先、報告先 \(RACI\)](#)」を参照してください。

### RCAC

「[行と列のアクセス制御](#)」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。

### リアーキテクト

「[7 Rs](#)」を参照してください。

## 目標復旧時点 (RPO)

最後のデータリカバリポイントからの最大許容時間です。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)

サービスが中断から復旧までの最大許容遅延時間。

## リファクタリング

「[7 Rs](#)」を参照してください。

## リージョン

地理的エリア内の 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、耐障害性を提供するために、他のから分離され、独立しています。詳細については、「[アカウントが使用できる AWS リージョンを指定する](#)」を参照してください。

## リグレッション

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。

## リプラットフォーム

「[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。

## 回復性

中断に抵抗または中断から回復するアプリケーションの機能。AWS クラウドでの回復力を計画する際には、一般的に、[高可用性](#)と[ディザスタリカバリ](#)が考慮されます。詳細については、「[AWS クラウドの耐障害性](#)」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。サポートが含まれる場合は RASCI マトリックスと呼ばれ、含まれない場合は 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、「AWSでのセキュリティコントロールの実装」の「[レスポンスコントロール](#)」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。

## 検索拡張生成 (RAG)

[生成 AI](#) の技術。これにより、[LLM](#) では、レスポンスの生成前に、トレーニングデータソースの外部にある信頼できるデータソースが参照されます。例えば、RAG モデルによって、組織のナレッジベースまたはカスタムデータのセマンティック検索を実行できる場合があります。細については、「[RAG \(検索拡張生成\) とは何ですか?](#)」を参照してください。

## ローテーション

定期的に[シークレット情報](#)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 (IdP) が使用しているオープンスタンダード。この機能を使用すると、フェデレーテッドシングルサインオン (SSO) が有効になるため、ユーザーは組織内のすべてのユーザーを IAM で作成しなくても、AWS マネジメントコンソールにログインしたり AWS、API オペレーションを呼び出すことができます。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。

### SCADA

「[監視制御とデータ取得](#)」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

暗号化された形式で保存する AWS Secrets Manager 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付き情報。シークレット値とそのメタデータで構成されます。シークレット値には、バイナリ、1つの文字列、複数の文字列を指定できます。詳細については、Secrets Manager ドキュメントの「[Secrets Manager シークレットの概要](#)」を参照してください。

## セキュリティバイデザイン

開発プロセス全体を通してセキュリティが考慮されているシステムエンジニアリングのアプローチ。

## 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 4 つの種類があります。4 つとは、[予防](#)、[検出](#)、[レスポンス](#)、[プロアクティブ](#)です。

### 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への自動レスポンスまたは自動修復を目的として、事前定義およびプログラムされたアクション。これらの自動化は、セキュリティのベストプラクティスを実装するのに役立つ[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。自動レスポンス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、認証情報の更新などがあります。

### サーバー側の暗号化

送信先で、それ AWS のサービスを受け取る によるデータの暗号化。

### 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](#)」を参照してください。

### サービスエンドポイント

のエンドポイントの URL AWS のサービス。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、スループットといった、サービスパフォーマンス面の指標。

## サービスレベル目標 (SLO)

[サービスレベルインジケータ](#)によって測定され、サービスの状態を表すターゲットメトリクス。

## 責任共有モデル

クラウドのセキュリティとコンプライアンス AWS について と共有する責任を説明するモデル。AWS はクラウドのセキュリティを担当しますが、 はクラウドのセキュリティを担当します。詳細については、「[責任共有モデル](#)」を参照してください。

## SIEM

「[Security Information and Event Management システム](#)」を参照してください。

## 単一障害点 (SPOF)

特定のアプリケーションを構成する単一の重要なコンポーネントで発生し、システム稼働に支障をきたす可能性のある障害。

## 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。

## スプリットアンドシードモデル

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、「[AWS クラウドでのアプリケーションをモダナイズするための段階的アプローチ](#)」を参照してください。

## SPOF

「[単一障害点](#)」を参照してください。

## スタースキーマ

データベースの編成構造を意味し、1つの大きいファクトテーブルにトランザクションデータまたは測定データが保存され、1つ以上の小さいディメンションテーブルにデータ属性が保存されます。この構造は、[データウェアハウス](#)やビジネスインテリジェンスを用途とするように設計されています。

## 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。

## 監視制御とデータ取得 (SCADA)

製造分野において、ハードウェアとソフトウェアを使用して物理アセットと本番運用をモニタリングするシステム。

## 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

ユーザーとのやり取りをシミュレートして、起こり得る問題を検出したり、パフォーマンスをモニタリングしたりすることで、システムをテストします。[Amazon CloudWatch Synthetics](#) を使用すると、こうしたテストを作成できます。

## システムプロンプト

コンテキスト、指示、ガイドラインなどを提示して、[LLM](#) に動作を指示する手法。システムプロンプトは、コンテキストを設定して、ユーザーとやり取りするルールを確立するのに有用です。

# 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「[トランジットゲートウェイとは](#)」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

ユーザーに代わって AWS Organizations およびそのアカウントで組織内でタスクを実行するために指定したサービスにアクセス許可を付与します。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と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、ドキュメントの「[Using AWS Organizations with other AWS services](#) AWS Organizations」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 枚のピザを分け合えることができるくらい小さな 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

現在のレコードに何らかの形で関連している行のグループに計算を実行する SQL 関数。ウィンドウ関数は、移動平均を計算したり、現在の行の相対位置に基づいて他の行の値にアクセスするといった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 ワークロード資格フレームワーク](#)」を参照してください

## Write-Once-Read-Many (WORM)

データを 1 回のみ書き込むことで、データの削除や変更を防ぐストレージモデル。承認済みユーザーは、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](#)と見なされます。

## Z

### ゼロデイ 익스プロイト

[ゼロデイ脆弱性](#)を悪用した攻撃 (一般的にマルウェアによる)。

### 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。

### ゼロショットプロンプト

[LLM](#) にタスク実行の手順は提示するが、実行のガイドとして役立つ例 (ショット) は提示しない方法。LLM は、事前トレーニング済みの知識を使用してタスクを処理する必要があります。ゼロショットプロンプトの有効性は、タスクの複雑さとプロンプトの品質によって異なります。「[数ショットプロンプト](#)」も参照してください。

### 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。