マルチクラウド戦略を開発するための実証済みのプラクティス

AWS 規範ガイダンス

AWS 規範ガイダンス: マルチクラウド戦略を開発するための実証済みのプラクティス

Table of Contents

マルチクラウド戦略を開発するための実証済みのプラクティス

Tom Godden と Ellie Tamari、Amazon Web Services

2025 年 9 月 (ドキュメント履歴)

今日の組織は、マルチクラウド導入に関する矛盾するメッセージに直面しています。それに対して完全にアドバイスする人もいれば、誰もがマルチクラウド環境に切り替えていると主張する人もいます。現実はこれらの極端の間にあります。正当な理由は、マルチクラウド戦略のためにも対戦するためにも存在し、成功は潜在的なビジネス価値と固有の複雑さとリスクのバランスを取ることにかかっています。

相互運用性へのコミットメントは AWS、多くのお客様が当社のプラットフォームを選択する主な理由です。当社は、ワークロードがどこにあってもイノベーションを起こす自由を提供し、ニーズに最適なテクノロジーを選択できると確信しています。では AWS、あらゆる環境でアプリケーションを構築およびデプロイできるソリューションの開発の最前線にいます。この顧客中心のアプローチは AWS クラウド、世界中の何百万ものお客様から信頼されている の基本です。

既存のツールと将来のテクノロジー選択の両方とシームレスに連携するクラウドプラットフォームがお客様に必要であると理解しています。別のプロバイダーから機能を追加するときに、すべてを再構築する必要はありません。クラウドは、すべてのプラットフォームで工キスパートになることを強制することなく、環境間のワークロードの接続、保護、管理に役立ちます。 は、 のみを使用するか、選択的なマルチクラウドアプローチ AWS に従うかにかかわらず、効果的な運用に役立つ接続ポイントを直接サービスに AWS 構築します。

すべての組織には、クラウド戦略の決定を促進する固有のビジネス要件があることを認識しています。ワークロードを主に で実行しているか AWS、複数のクラウドで実行しているか、より広範なマルチクラウドアーキテクチャ AWS の一部として を使用しているかにかかわらず、当社はお客様の成功を支援することに全力を注いでいます。 は、ワークロードが存在する場所を問わず、より簡単かつ迅速に構築、移行、運用できるように、さまざまなツールと機能 AWS を提供します。 AWS ツールは、クラウド投資のパフォーマンスと価値を最大化しながら、プロバイダー間の管理を簡素化します。

このホワイトペーパーでは、マルチクラウド戦略を成功させるための実証済みの教義に焦点を当てています。これには、マルチクラウドアプローチが有効なタイミングと場所、企業がマルチクラウド戦略を成功させる AWS 方法が含まれます。これは、エグゼクティブがマルチクラウドの導入に関連す

る情報に基づいた戦略と意思決定の選択を行うのに役立つ規範的なガイダンスを提供します。このホワイトペーパーでは、マルチクラウド実装に関する技術的な詳細な説明は提供していません。技術的な実装のサポートと特定の課題のサポートについては、 AWS ソリューションアーキテクトと連携することをお勧めします。

このホワイトペーパーでは、 AWS エンタープライズのお客様の経験に基づいて、マルチクラウドを成功させるための 9 つの実証済みの原則を紹介します。各原則は、ビジネス目標の整合からセキュリティ実装まで、マルチクラウド戦略の重要な側面に対処します。これらの原則を適用することで、組織はマルチクラウドの複雑さを自信を持ってナビゲートできます。

- テネット 1。マルチクラウドの目標を戦略に合わせる
- テネット 2。マルチクラウドの誤解に注意する
- テネット 3。それをサポートする明確な戦略とガバナンスを持つ
- テネット 4。連続したワークロードをクラウドに分散させない
- テネット 5。長期的な統合戦略を持つ
- テネット 6。コンテナを戦略的に使用する
- テネット 7。1 つの CCoE があるが、その中で特化している
- テネット 8。セキュリティが常に最優先事項であることを確認する
- テネット 9。等しい分散で 80/20 アプローチを採用する

テネット 1。マルチクラウドの目標を戦略に合わせる

ガートナーによる調査と業界の傾向は、組織が特定のビジネスニーズに対応するためにマルチクラウドアプローチを採用する傾向が高まっていることを示しています。次のシナリオは、マルチクラウドインフラストラクチャが戦略的に有利な場合を示しています。

合併と買収

合併と買収 (M&A) は、クラウド戦略に関する即時の決定を作成します。複数のクラウドを運用するとコストと複雑さが増加する可能性がありますが、迅速な統合により統合価値が遅延し、事業運営が中断される可能性があります。クラウドに関する意思決定は、M&A のメリットを実現するための中心となります。

統合計画では、完全なテクノロジー環境を考慮する必要があります。各ワークロードには、統合タイムラインとビジネスの優先順位のコンテキスト内で評価が必要です。

ガイダンス:

- 即時の統合ニーズと長期的な運用効率のバランスを取るビジネス主導の統合戦略を策定します。急激な統合によって重要な事業運営が中断されたり、M&A 価値の実現が遅れたりする可能性がある状況では、最初は複数のクラウドを維持します。
- 統合タイムラインに沿った明確なワークロード配置基準を作成します。技術的な依存関係と運用要件を考慮しながら、収益を生み出すアプリケーションとコアビジネスプロセスに優先順位を付けます。

別の CSP の長期的な差別化された機能を活用したい

不足する恐れにより、一部の企業はあらゆるクラウドを少しでも望んでいます。ワークロード配置の決定は、エンジニアリングチームから財務、セキュリティオペレーションまで、組織全体に影響します。

したがって、組織は複数の雲を追求する理由を調べる必要があります。一部の は、各ワークロードがニーズに最適なクラウドサービスプロバイダー (CSP) で動作する必要があると主張しています。ただし、個々のワークロードの最適化は、より広範な組織への影響とのバランスを取る必要があります。クラウドプロバイダーを追加するたびに、運用の複雑さが増し、新しい人材要件が作成され、テクノロジー組織全体に影響を与えるセキュリティ上の考慮事項が導入されるリスクがあります。

ガイダンス:

- 80/20 アプローチに従う: ほとんどのワークロードにプライマリプロバイダーを選択し、特定の価値の高いユースケースにのみ追加のプロバイダーを検討します。この戦略は、複雑さを軽減しながら、効率と人材の定着率を最大化します。
- クラウド間の運用の総コストを考慮してください。セキュリティツール、ガバナンス製品、財務管理システム、運用オーバーヘッドを分析に含めます。
- 各ワークロードの依存関係とインタラクションを評価します。ワークロードが単独で動作することはほとんどなく、データ、セキュリティコントロール、運用プロセスを共有します。
- プロバイダー全体で徹底的な価格パフォーマンス分析を実施します。直接コストだけでなく、複数の環境を管理するオーバーヘッドも比較します。

持株会社のマルチクラウドと事業会社または事業部門のプライマリクラウド

プライベート株式会社と持株会社は、独自のクラウド戦略に関する考慮事項に直面しています。ポートフォリオ企業は、多くの場合、過去の M&A 活動から生じる独立したクラウド戦略を維持しています。この構造により、各ビジネスユニットが独立して動作するため、通常はマルチクラウド運用に関連する複雑さが軽減されます。ただし、この独立性により、企業全体のボリューム割引と購入インセンティブを利用する機会が制限される可能性があります。

持株会社レベルでのクラウド戦略の有効性は、ポートフォリオ企業の自律性と個々のテクノロジーニーズによって異なります。統合により購入レバレッジが生じる可能性がありますが、持株会社やプライベート株式ポートフォリオに典型的な独立した運用モデルと競合する可能性があります。

ガイダンス:

- CSP ボリューム割引構造について説明します。各プロバイダーは、企業契約に子会社を追加または削除し、ビジネスユニットを別々のエンティティにスピンオフするメカニズムを提供します。これらは双方向のドアの決定を表します。
- クラウド購入コミットメントを慎重に計画します。CSP のアカウントチームを早期に関与させるか、 AWS クラウド運用コンピテンシー AWS Partner の にお問い合わせください。
- 独立性と効率のバランスを取ります。運用を制約することなく、ポートフォリオ企業に利益をもたらす共有サービスまたは購入契約を検討してください。
- まずビジネス目標に焦点を当てます。独自のマルチクラウド戦略を追求するのではなく、運用モデルをサポートするテクノロジー戦略を策定します。

- ポートフォリオ管理の観点からクラウド戦略を評価します。クラウドの選択が潜在的な売却や将来の買収にどのように影響するかを検討してください。

テネット 2。マルチクラウドの誤解に注意する

マルチクラウド戦略を開発するときは、以下のセクションで説明する一般的な誤解を避けてください。

全員がマルチクラウド戦略を採用している

アドバイザリー会社やメディア企業は、マルチクラウド導入の複雑なイメージを描いています。調査では、マルチクラウドアプローチに幅広い関心を示していますが、使用パターンは多くの場合、別のストーリーを語ります。実際には、多くの企業は単一のクラウド環境または明確なプライマリ/セカンダリ CSP 関係を維持しています。この切断は、見出しを超えて、組織の特定のニーズに焦点を当てることの重要性を強調しています。

当社のガイダンス:

- 業界の傾向に従うのではなく、特定のビジネス要件に基づいてクラウドに関する意思決定を行います。組織の測定可能なコストとリスクに焦点を当てます。
- 業界コンテキスト内のマルチクラウドのユースケースを調べます。コンシューマーテクノロジー企業向けのクラウド戦略は、金融サービス、製造、ゲーム環境に変換されない場合があります。
- ワークロード配置の決定の主な要因として、データ重力を考慮します。データの場所と移動によって、多くの場合、最も効果的なクラウドアーキテクチャが決まります。
- 導入統計を超えて、支出パターンを理解します。レポートされるマルチクラウド導入率が高いと、多くの場合、実際の支出パターンがマスクされます。
- マルチクラウド環境にコミットする前に、技術的な制約を評価します。一部のワークロードは、コンポーネントが 1 つのクラウド環境にとどまる場合に最適です。

マルチクラウドによりベンダーロックインのリスクが軽減

ベンダーの柔軟性は、クラウド戦略開発における正当な考慮事項です。組織は、ビジネスニーズの進化に応じてテクノロジーの選択を適応させる能力を重視しています。この懸念は、バインディングと長期的なコミットメントを生み出した従来の IT 投資の過去の経験を反映しています。 クラウドサービスは、プロバイダーの柔軟性に関するさまざまなダイナミクスを提供します。 は、オープンソースと互換性のあるサービスとデータポータビリティオプション AWS を提供し、移行への技術的な障壁を軽減します。ただし、柔軟性と運用効率のトレードオフは依然として重要です。組織は、プロバイダーオプションを維持することのビジネス価値と、プライマリプロバイダーの専門サービスと深く統合することの技術的な利点を比較検討する必要があります。

一部のお客様は、コンテナを使用するクラウドに依存しないソリューションをエンジニアリングすることで、ロックインを回避しようとしています。このアプローチでは、多くの場合、基本的なコンピューティングおよびストレージサービスに制限され、高度なクラウド機能の利点を回避します。当社の経験では、ネイティブサービスの使用と比較して、開発時間と必要なリソースが増加するため、この戦略はかなり複雑になることを示しています。

当社のガイダンス:

- クラウドに依存しないアーキテクチャの全コストを考慮してください。追加のエンジニアリングオーバーヘッドは、移植性の利点を正当化しない可能性があります。
- 最大値にはクラウドネイティブ機能を使用します。基本的なコンピューティングおよびストレージサービス単独では、セキュリティ、スケーラビリティ、イノベーションにおける大きな利点を犠牲にすることがよくあります。
- ビジネス要件に基づいてクラウド戦略を計画します。マルチクラウド実装が、複数のプラットフォームでユーザーに提供する機能など、明確な価値を追加すると、追加のエンジニアリング投資は価値があります。
- 現実的な終了シナリオとコストを評価します。プロバイダーを変更する可能性とコストを、 の完全なセットを使用する利点と比較します AWS のサービス。
- Amazon Relational Database Service (Amazon RDS) などの AWS. AWS managed サービスのオープンソース基盤に基づいて構築することで、柔軟性と運用上の優秀性の両方が得られ、現在使用しているデータベースエンジンがサポートされます。
- が提供する包括的な移行ツールを活用します AWS。ワークロードを任意の方向に移動し、他のプロバイダーの使用を離れる場合 AWS は無料のデータ出力を提供します。詳細については、 AWS ブログ記事「Free data transfer out to internet when move out AWS」を参照してください。

マルチクラウドによる可用性と耐障害性の向上

停止中のクラウドプロバイダー間のシームレスなワークロード切り替えに対する考え方が、一部の組織をマルチクラウド戦略に導いています。この考え方は、基本的な技術的現実を無視するクラウドインフラストラクチャのレジリエンスを過度に単純化したものです。

マルチクラウドのお客様との長年の経験に基づいて、プロバイダー間のワークロードの完全な移植性を維持すると AWS、予想されるすべての利点を実現せずに、かなりの複雑さが生じることがよくあります。データ集約型アプリケーションは、データ重力の制約により、克服できない課題に直面します。実際、データ量の多いワークロードに対して、組織が真にシームレスなマルチクラウドフェイルオーバーを正常に実装することはほぼ不可能です。

「マルチクラウドフェイルオーバーは複雑でコストがかかるため、ほとんど常に実用的ではなく、クラウドレジリエンスリスクに対処するための特に効果的な方法ではありません」というソーシャルメディア投稿で、Lydia Leong は、この視点を強調しています。ネットワーク、ストレージ、データベース、機械学習、セキュリティにおけるプロバイダー固有の違いにより、真の移植性はほぼ不可能になります。いずれかの環境で障害が発生すると、すべての環境にわたって停止が発生する可能性があるため、プロバイダー間でワークロードを分散させるとリスクが増加する可能性があります。

当社のガイダンス:

- 複雑なマルチクラウドアーキテクチャを追求するのではなく、個々のワークロードの AWS 機能をマスターすることに焦点を当てます。
- プロバイダー間のフェイルオーバーを試みるのではなく、 AWS リージョン とアベイラビリティーゾーンを通じてレジリエンスを構築します。物理データセンター間のワークロード AWS を自動的にフェイルオーバーする方法に関する技術的な詳細については、ブログ記事「ゾーンオートシフト — 潜在的な問題を検出したときにトラフィックをアベイラビリティーゾーンから自動的に移行する」を参照してください AWS 。
- ワークロードを戦略的に移行し AWS、成功を最大化するために一度に 1 つのアプリケーションに集中します。

マルチクラウドの方が料金が高くなります

価格競争力は、マルチクラウド環境ではすべての の中で最も弱い引数である可能性があります。複数年契約に縛られる複雑で高価なソフトウェアやデータセンターの契約に関する組織の経験により、IT サービスの調達には注意が払われています。従来の調達アプローチは、pay-as-you-go購入、ボリューム割引、またはクラウドでの価格競争の現実に適応していません。(2025 年 1 月現在、AWS は開始から 151 回値下げされています) 。

コスト削減の最大の唯一の推進要因は、適切に管理され最適化されたクラウド環境です。ある企業は、主に価格パフォーマンス上の利点 (AWS Graviton などのカスタム設計チップに基づくコンピューティングインスタンスなど) を提供し、優れたクラウド財務管理ソリューションを持つプロバイダーと連携することで、コストの最適化を改善しています。1,000 を超える組織を対象とした 2022 年の Hackett Group の調査によると、IT 総支出に対するインフラストラクチャ支出の割合は、マルチクラウド組織と比較して AWS 、お客様にとって 20% 低くなっています。

当社の経験から、企業は複数のクラウドでの運用に伴う追加コストと複雑さを予測しておらず、また、このコストとhead-to-head調達エンゲージメントにおける認識された利益を適切に比較検討していないことがわかりました。

当社のガイダンス:

- AWS Well-Architected フレームワークのコスト最適化の柱でコスト最適化戦略を構築します。5 つの設計原則があります。
  - クラウド財務管理を実装する: クラウドで財務上の成功を達成し、ビジネス価値の実現を加速するには、クラウド財務管理に投資する必要があります。組織は、テクノロジーと使用量管理の新たなドメインで機能を構築するために必要な時間とリソースを投入する必要があります。セキュリティまたは運用機能と同様に、コスト効率の高い組織になるには、ナレッジ構築、プログラム、リソース、プロセスを通じて機能を拡張する必要があります。
  - 消費モデルを導入する: コンピューティングリソースの使用分のみを支払い、ビジネス要件に応じて使用量を増減することができます。例えば、開発環境とテスト環境は、通常、平日に 1 日 8 時間のみ使用されます。これらのリソースは、75% の潜在的なコスト削減のために使用されていない場合に停止できます (40 時間対 168 時間) 。
  - 全体的な効率を測定する: ワークロードのビジネス出力と、配信に関連するコストを測定します。このデータを利用すると、生産性および機能性の向上とコスト削減から得られるメリットを理解することができます。
  - 差別化されていない重労働にコストを費やすのを止める: CSPs は、サーバーのラック、積み上げ、電源供給などのデータセンターオペレーションの重労働を行います。また、マネージドサービスを使用することで、オペレーティングシステムとアプリケーションを管理する運用上の負担も軽減されます。これにより、IT インフラストラクチャではなく、顧客とビジネスプロジェクトに集中できます。
  - コストを分析し帰属関係を明らかにする: クラウドでは、ワークロードのコストと使用状況を正確に確認しやすくなり、IT コストを収益システムと個々のワークロード所有者に透過的に結び付けることができます。これによって投資収益率 (ROI) を把握できるため、ワークロードの所有者はリソースを最適化してコストを削減する機会が得られます。
- さまざまなプロバイダーにまたがる運用の財務上のオーバーヘッドを考慮すると、オートメーションとコスト最適化ツールに多額の投資をするようお客様に指示します。各 CSP には、 など、この分野の広範なネイティブツールが用意されていますAWS Cost Optimization Hub。ほとんどのネイティブツールは、クラウド環境のお客様に優れた機能を提供します。ただし、複数の CSPs にわたる支出を把握するには、ISV と Software as a Service (SaaS) 製品の豊富なセットから選択して、これらの機能を拡張し、コスト最適化のための単一のエクスペリエンスを提供できます。
- 支出配分戦略を通じて購買力を枯渇しても、ビジネス価値は生まれません。これにより、ボリューム割引の可能性が損なわれ、技術設計が損なわれる可能性があります。クラウドサービスを使用する最も効率的な方法は、オペレーションの大部分にプライマリプロバイダーを使用し、ビジネス価値を追加する場合にのみ他の CSPs を使用することです。

テネット 3。それをサポートする明確な戦略とガバナンスを持つ

マルチクラウド戦略の策定は不十分です。どのワークロードがどこへ、なぜ向かうのかを明確にガバナンスするなど、目標を達成するための戦略を確立する必要があります。ワークロードとその依存関係を最適化するには、評価基準を使用する必要があります。評価を個人に任せると、CSPs 間で調整されていないスプロールにより、マルチクラウド戦略の価値が損なわれる可能性があります。CSP ワークロードのパフォーマンスを定期的に評価し、評価を CSP の選択、基準、将来の使用状況への重要な入力として使用することをお勧めします。

効果的なガバナンス戦略では、企業全体で使用されているサービス、アプリケーション、コンポーネントの総数を可視化する必要があります。これは、CSPs にまたがる堅牢なタグ付け戦略であり、デプロイされたすべてのリソースの所有権、使用状況、環境 (開発、QA、ステージング、本番稼働など) を明確に確立します。すべて所有者にタグ付けする必要があります。タグ付けされていない場合や所有者を特定できない場合は、削除する必要があります。タグ付けされていないリソースを自動的に検索して削除する主要な金融サービス組織と密接に連携し、開発チームにとっての不便さに関係なく、これをベストプラクティスと見なします。このタグ付けアプローチは、進行するブロックを作成するのではなく (ゲートではなくガードレールを実装する) 、ガバナンスルールを体系化し、適用を自動化します。コスト、運用、セキュリティは、CSPs 全体で同じ深さのデータと透明性で、同じ方法で追跡、モニタリング、対処する必要があります。

マルチクラウド戦略を実装する場合、運用管理とセキュリティを維持するには、クラウドプロバイダー間で明確で一貫したアカウント構造を確立することが重要です。ハブhub-and-spokeモデルを採用することをお勧めします。ここでは、ビジネスユニット AWS アカウント ごとに個別に作成します。これらは、統合コンプライアンスとセキュリティモニタリング用のセキュリティ/監査アカウントと、相互接続を管理するための中央ネットワークアカウントの 2 つの重要な中央アカウントによって固定されます。(このアプローチは の設計で規定されていますAWS Control Tower。 ただし、最小特権の原則と職務分離の原則は、他の雲にも同様に適用されます。 AWS Well-Architected フレームワークでは、これらの概念を詳しく説明しており、技術的な視聴者に強くお勧めします。) この基本的なアプローチは、ガバナンスと運用の一貫性を維持するために、クラウドプロバイダー全体にミラーリングする必要があります。ワークロードアカウントは環境 (開発、ステージング、本番稼働) または機能別に整理し、アカウントの作成と削除のための明確なプロセスを確立する必要があります。

ガイダンス:

- 包括的なタグ付け戦略を実装して、すべてのクラウドリソースにわたって明確な所有権と使用パターンを維持します。一貫したタグ付けポリシーを通じて、環境、コストセンター、アプリケーション、ビジネスユニットを追跡します。ガバナンス標準を適用し、環境の明確性を維持するために、適切なタグがないリソースを削除します。
- マルチクラウド環境全体の規制要件をマッピングする統合コンプライアンスフレームワークを確立します。各クラウドプロバイダーのコントロールと証明書がコンプライアンス義務をどのようにサポートしているかを明確に文書化します。
- 手動の承認プロセスを使用する代わりに、自動化を通じてガバナンスの適用を自動化します。ポリシー違反が発生する前に防止する自動システムにガバナンスルールをコーディングします。これにより、開発速度を維持しながらヒューマンエラーが排除されます。
- 一元化されたセキュリティとネットワーク制御を使用して、hub-and-spokeモデルでアカウントを構築します。セキュリティ監査とネットワーク管理専用のアカウントを作成して、重要な機能を一元化します。この基盤により、組織全体で一貫したセキュリティポリシーとネットワーク接続が可能になります。
- 運用の境界を維持するには、さまざまな環境と機能に対して個別のアカウント、サブスクリプション、またはプロジェクト (CSP の命名規則によって異なります) を作成します。開発環境、ステージング環境、本番環境でワークロードを分割します。この分離により、セキュリティインシデントが拡散するのを防ぎ、明確な運用ドメインを維持します。
- 環境全体で一貫したメトリクスを使用して、コスト、運用、セキュリティをモニタリングします。リソース使用率、セキュリティイベント、支出パターンの統合モニタリングを実装します。このデータを使用して、ワークロードの配置とリソース割り当ての決定を最適化します。
- 組織のポリシーと自動コントロールを通じて、不正なクラウドの使用を防止します。アカウント作成とリソースプロビジョニングの明確なプロセスを定義します。サービスコントロールポリシー (SCPs) を実装して、すべてのアカウントで組織標準への準拠を適用します。
- 検出コントロールと予防コントロールを確立して、権限のないプロバイダーアカウントを通じてシャドウ IT が出現するのを防ぎます。経費レポートとネットワークトラフィックを通じて、不正なクラウド使用状況をモニタリングします。承認されたイノベーションパスを維持しながら、不正なプロバイダーアクセスをブロックします。

テネット 4。連続したワークロードをクラウドに分散させない

連続したワークロードを複数のクラウドプロバイダーに分散すると、不要な複雑さ、リスク、コストが発生します。データをまとめて処理および分析するワークロードが複数のプロバイダーにまたがる場合、組織はデータの移動、同期、一貫性の課題に直面します。チームは、プロバイダーごとに異なる APIs、管理インターフェイス、セキュリティモデル、運用プロセスをナビゲートする必要があります。これにより、エラーの可能性が高まり、運用オーバーヘッドが増大します。この複雑さにより、エラーや運用上のオーバーヘッドが発生する可能性が高くなり、俊敏性とスケーラビリティが妨げられる可能性があります。

ただし、いくつかの実用的なシナリオでは、特定のビジネス要件または技術要件により、組織はクラウド全体に連続したワークロードを分散する必要がある場合があります。このような場合は、明確な基準と指針を確立してトレードオフを評価し、アプローチが組織の全体的なマルチクラウド戦略と一致していることを確認することをお勧めします。

組織が複数のクラウドにワークロードを分散することを選択した場合、メッセージングと疎結合を中心としたアーキテクチャを採用することで、関連する課題の多くを軽減できます。これは、クラウド間で懸念を分離し、プロバイダーに障害が発生した場合の影響範囲を減らす最善の方法です。財務取引など、最も期限の厳しいオペレーションは、理想的には 1 つの環境内に保持する必要があります。ある環境の停止は、別の環境のワークロードを危険にさらすことを決して許可しないでください。

当社のガイダンス :

- プロバイダー間のリアルタイムの依存関係を最小限に抑えるために、運用上の独立性を実現するクラウドワークロードを設計します。ワークロードの分散が必要な場合は、一定のクラウド間接続を維持するのではなく、効率的な一括データ転送メカニズムを実装します。
- 提案された各分散ワークロードを明確なビジネス基準に照らして評価します。ディストリビューションによってもたらされる戦略的利点と運用上の複雑さの両方を考慮してください。

テネット 5。長期的な統合戦略を持つ

異なるクラウド内のアプリケーション間で大量のデータを移動する場合、特にコンピューティングリソースとアプリケーションが 1 つの CSP にデプロイされ、データストレージリソースが別の CSP にデプロイされている場合は注意してください。このような状況では、認識される利点を相殺する可能性のある複雑さとレイテンシーが生じる可能性があります。あるクラウドにデータレイクがあるが、別の CSP のツールを使用して機械学習 (ML) または分析を実行したいと考えている多くのお客様と話します。マルチクラウド環境にワークロードを配置する場所を決定することは、組織が直面する最も重要な決定の 1 つであり、多くの場合、最も困難な決定でもあります。各ワークロード配置の決定は、技術要件、ビジネスニーズ、プロバイダーの強みという 3 つの重要な側面を通じて評価することをお勧めします。

コンピューティング能力、データオペレーション、応答時間のニーズ、成長要件など、各ワークロードの重要な特性をマッピングして、技術的な評価を開始します。アプリケーションは、データの近くにある場合、自然に最高のパフォーマンスを発揮します。アプリケーションをデータソースから遠ざけると、不要な技術的な障害が発生し、パフォーマンスが低下します。

ビジネス上の意思決定では、プロバイダーの料金、データレジデンシー要件、ベンダー契約を考慮する必要があります。各ワークロード配置は、組織全体の運用、セキュリティ、生産性に影響します。ワークロードを単独で見ると、最適ではない決定につながります。

当社のガイダンス :

- リアルタイムアクセスではなく、クラウド間で一括データ転送を実装します。クラウド間で一定の API コールを使用する代わりに、効率的な一括オペレーションを使用して定期的なデータ更新をスケジュールします。このアプローチにより、コストを削減し、信頼性を向上させ、一貫したパフォーマンスを維持します。たとえば、クラウド間で個々のトランザクションをクエリするのではなく、要約された日次売上データをエクスポートします。
- ワークロード配置を設計するときは、データ重力を考慮してください。パフォーマンスを維持し、コストを削減するために、アプリケーションをプライマリデータソースに近づけます。ML モデル、分析エンジン、トランザクション処理システムはすべて、データに直接アクセスできるという利点があります。これらのワークロードをデータから遠ざけると、不要なネットワークレイテンシーと複雑さが発生します。
- ワークロードの決定は、個別にレビューするのではなく、完全なクラウド戦略のコンテキスト内で評価します。各配置の選択が組織全体の運用プロセス、セキュリティコントロール、チーム機能にどのように影響するかを検討します。単一のワークロードに最適と思われる決定は、モニタリングを複雑にしたり、総合的に見るとセキュリティリスクを高める可能性があります。

- さまざまなタイプのデータが存在する場所を指定する明確なデータ所有権とガバナンスポリシーを定義します。クラウドプロバイダー間のデータ配置に関する一貫した意思決定を促進するデータ分類フレームワークを作成します。

テネット 6。コンテナを戦略的に使用する

コンテナはマルチクラウド戦略をサポートする上で重要な役割を果たしますが、その制限を認識することも重要です。コンテナを使用すると、さまざまな環境間で移植性と一貫性の利点が得られるため、最新のクラウドネイティブアプリケーションには一般的にお勧めします。コンテナはプラットフォームに依存しません。つまり、Kubernetes などのコンテナ化テクノロジーをサポートする任意のクラウドプラットフォームまたはインフラストラクチャで実行できます。コンテナを使用する組織は、アプリケーションを一度開発してパッケージ化し、複数のクラウドプロバイダーまたはオンプレミス環境に一貫してデプロイできます。大幅な変更は必要ありません。コンテナ内にアプリケーションコード、依存関係、ランタイム環境をカプセル化することで、高度な移植性を実現できます。これにより、クラウドプロバイダー間、またはクラウドとオンプレミスのデータセンター間でワークロードをシームレスに移動できます。

ただし、コンテナは、すべてのユースケースを解決したり、組織がマルチクラウド戦略を採用する際に直面する可能性のあるすべての課題を排除したりするとは限りません。コンテナは、最新のマイクロサービスベースのアーキテクチャに最適ですが、大規模なモノリシックアプリケーションには適していない場合があります。さらに、コンテナはアプリケーションのランタイムなど、移植性の特定の側面に対処できますが、データ管理、セキュリティポリシー、その他のクラウド間の依存関係に関する問題は自動的に解決されません。組織は、一貫したデータ管理、統一されたセキュリティコントロール、クラウドホストコンポーネントとオンプレミスコンポーネント間のシームレスな統合を確保するために、マルチクラウドソリューションを慎重に計画および設計する必要があります。

当社のガイダンス：

- 各クラウドプロバイダーのネイティブコンテナ管理機能を使用して、ビジネス価値を最大化し、配信を高速化します。このアプローチにより、最適なパフォーマンスを確保しながら、クラウドに依存しないソリューションを作成する複雑さを回避できます。これにより、意味のあるリターンはほとんど得られません。
- データ管理、セキュリティ、クラウド間の依存関係など、運用上の全体像に対応するコンテナ戦略を策定します。コンテナアーキテクチャの決定を行うときは、ビジネス成果に焦点を当てます。

テネット 7。1 つの CCoE があるが、その中で特化している

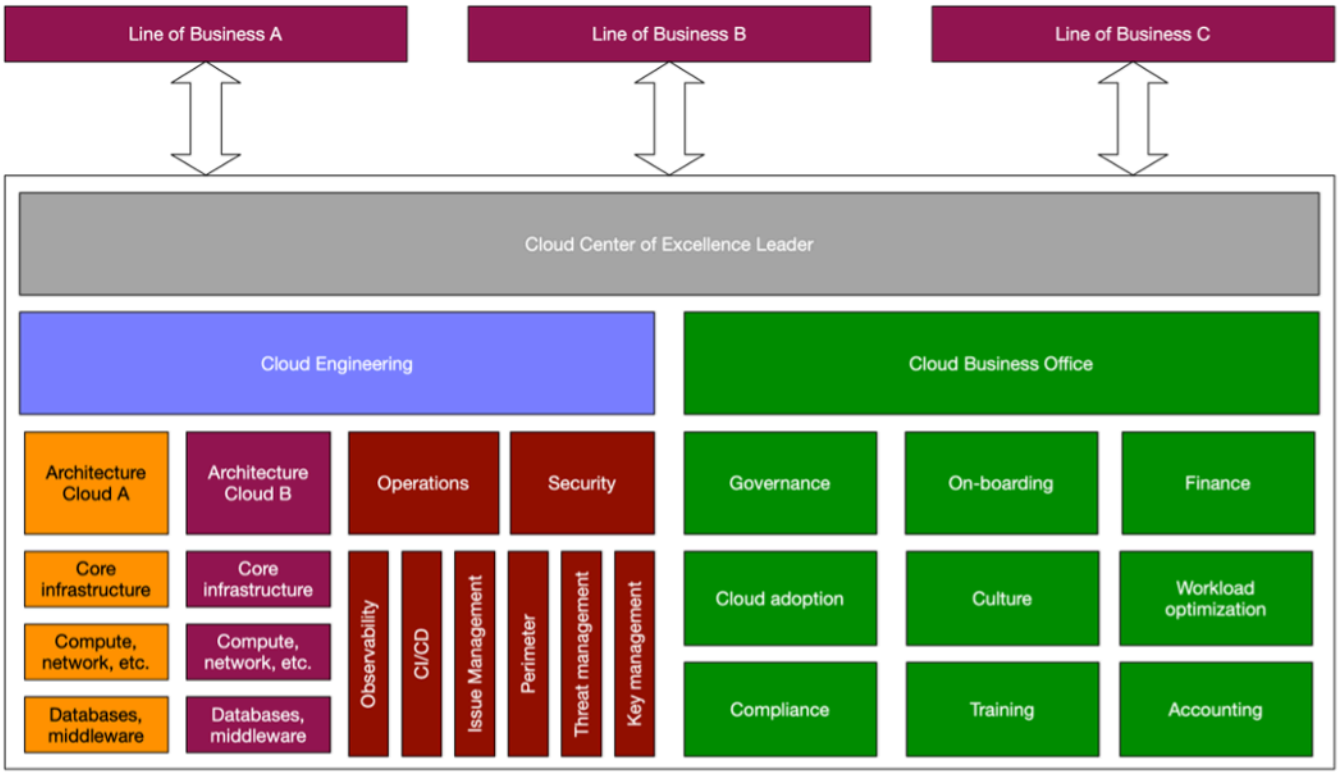
多くの AWS お客様にアドバイスしているように、組織内に Cloud Center of Excellence (CCoE) を構築し、クラウドジャーニーのリーダーシップ、標準化、加速を実現する必要があります。マルチクラウド環境に関しては、最も成功した企業は CCoE とのバランスの取れたアプローチを採用していることがわかります。

CSP ごとに個別の CCoEs を確立する代わりに、組織のマルチクラウド戦略を監督する単一の統合 CCoE を用意することをお勧めします。これにより、分散、再設計、無駄につながる可能性のあるサイロ化された作業ではなく、調整された一貫したアプローチを確保できます。単一の CCoE 内のチームに、組織が使用する各 CSP に必要な専門的なスキル、ツール、メカニズムがあることを確認します。この専門知識により、CCoE はさまざまなクラウドプラットフォームを効果的に管理、サポート、高速化できます。

例えば、CCoE には AWS クラウド、、 のサービス、ベストプラクティスを深く理解する AWS特定のエキスパートと、組織によるこれらのクラウドテクノロジーの使用をガイドできる他の CSPs の専門家が必要です。単一の CCoE 内のこの専門知識は、各クラウドプラットフォームが最適に使用されていることを確認しながら、一元化されたアプローチの調整と標準化の恩恵を受けるのに役立ちます。

単一の CCoE は、組織のマルチクラウド戦略の標準、ポリシー、ベストプラクティスを確立する一元管理機関として機能する必要があります。クラウドワークロードとプロジェクトの実際の実装は、CCOE が監視、サポート、調整を提供しながら、専門チームまたはビジネスユニットに配布できます。このバランスの取れたアプローチは、組織内で必要なレベルの柔軟性と自律性を提供しながら、まとまりのあるマルチクラウド戦略を確保するのに役立ちます。

次の図は、CCoE が複数の事業部門 (LOBs)、クラウドエンジニアリングチーム、クラウドビジネスオフィス (CBO) チームにわたって一元化されたアプローチとガバナンスを提供する方法を示しています。



当社のガイダンス：

- CCoE を構築して戦略的監視を維持し、各クラウドプロバイダーに専門知識を組み込みます。まれなマルチクラウドスペシャリストを探すのではなく、個々のクラウドプラットフォームでの深い専門知識の採用に集中し、組織能力を構築するための内部知識共有を促進します。
- CCoE を強化して、セキュリティやオブザーバビリティなどの懸念を横断するための企業全体の標準を確立し、クラウドネイティブのツールとサービスを使用して、個々のチームにこれらのガイドライン内で実行する自律性を与えます。
- プライマリクラウドプラットフォームの深い専門知識とより広範なアーキテクチャ知識のバランスを取る包括的な人材戦略を策定します。強力なクラウド固有のスキルとエンタープライズアーキテクチャの経験を組み合わせたチームの構築に焦点を当てます。

テネット 8。セキュリティが常に最優先事項であることを確認する

マルチクラウドアプローチでは、セキュリティ体制でより多くの攻撃対象領域を考慮する必要があるため、不正アクセスのリスクが高いため、セキュリティを確保することが困難になります。マルチクラウド戦略では、多くの場合、企業は ID 管理、ネットワークセキュリティ、アセット管理、監査ログ記録などの分野で CSPs 全体で複数のセキュリティモデルを処理する必要があります。この複雑さにより、透明性が難しくなり、セキュリティチームの負担が増大し、リスクが増大します。

マルチクラウド環境では、セキュリティの自動化が不可欠です。ID 管理は、環境間でシームレスに機能する必要があります。一貫したアクセスポリシーを維持しながら、既存の ID プロバイダーを接続する必要があります。セキュリティには、データ、ネットワーク、エンドポイントレイヤー間の統合保護が必要です。データ分類、暗号化、ライフサイクル管理が基盤となります。ネットワークセキュリティは、標準化された設計と接続パターンに基づいています。エンドポイント保護は、一貫したパッチ管理とホストベースのコントロールを通じてフレームワークを完了します。

これらの基本的な要素は、複数のクラウドプロバイダーを成功させ安全に導入するために不可欠であり、マルチクラウド戦略計画の早い段階で検討する必要があります。

当社のガイダンス：

- 標準化された分類と暗号化によるデータ保護、一貫した設計パターンによるネットワークセキュリティ、体系的な制御とパッチ管理によるエンドポイント保護の 3 つの主要要素に焦点を当てた、マルチクラウド環境全体に統合されたセキュリティフレームワークを実装します。
- 標準化されたツールとプロセスを通じて一元化された可視性と制御を維持しながら、各クラウドプロバイダーのネイティブセキュリティ機能を活用する統合セキュリティ運用モデルを確立します。
- Amazon Security Lake を使用して、セキュリティデータの収集と分析を一元化します。このプラットフォームは AWS、他のクラウドプロバイダー、SaaS アプリケーション、オンプレミスシステムからのセキュリティ情報を 1 つのビューに集約します。Open Cybersecurity Schema Framework (OCSF) をサポートし、ハイブリッドおよびマルチクラウド環境全体で標準化された分析を可能にします。この一元化されたアプローチにより、脅威の検出と対応が改善され、セキュリティ運用が簡素化されます。
- 各プロバイダーのネイティブセキュリティツールをデプロイして、保護機能を強化します。これらの専用サービスは、一元化されたセキュリティプラットフォームにデータを供給しながら、プロバイダー固有の機能に対処します。ネイティブツールと一元化された可視性を組み合わせることで、インフラストラクチャ全体で包括的なセキュリティカバレッジを提供できます。

- 運用データとセキュリティデータを含むクラウド環境全体を一から包括的に可視化する、統一されたオブザーバビリティ戦略を実装します。運用場所に関係なくビジネスサービスを一貫して追跡できる、業界をリードするモニタリングアプローチを標準化します。
- マルチクラウド環境全体で迅速な問題の特定と解決を可能にする、運用データ収集と視覚化に関するエンタープライズ全体の標準を確立します。技術的ステークホルダーとビジネスステークホルダーの両方に役立つ運用上のインサイトの信頼できる情報源を 1 つ作成することに焦点を当てます。

テネット 9。均等分散で 80/20 アプローチを採用する

プロバイダー間でワークロードを分散する方法によって、マルチクラウドの成功が根本的に決まります。多くの組織はクラウドディストリビューションで誤って平等を追求し、プロバイダー間でワークロードを均等に分散しようとします。このアプローチは、比例的な利点をもたらさずに複雑さを増します。均等な分散により、技術的な機能がフラグメント化され、購入能力が減り、不要な運用オーバーヘッドが発生します。チームは、複数のプラットフォームで同時にコンピテンシーを維持せざるを得ない場合、深い専門知識の開発に苦労します。

80/20 アプローチは、クラウド間で均等に分散するよりも明らかに優れた結果を提供します。特定の機能に他の を選択的に使用しながら、投資の 80% を 1 つのプライマリプロバイダーに集中させると、コストと複雑さの両方を軽減するバランスの取れた戦略が作成されます。この集中的なアプローチにより、チームはプライマリプラットフォームの高度なサービスに関する深い専門知識を開発できるため、イノベーションが加速します。複数の環境で表面レベルの知識を維持する代わりに、技術スタッフが 1 つのアーキテクチャのスペシャリストになることができます。エンジニアが 1 つのプラットフォームをマスターすると、より効率的に構築され、より迅速にトラブルシューティングを行い、より高度なソリューションを実装できます。

通常、80/20 アプローチを採用している企業は、チームが複数のテクノロジーにまたがって細分化されるのではなく、価値のある市場性のある専門知識を開発するため、人材保持率の向上を報告します。この集中戦略は、プロバイダー間でのさまざまなセキュリティモデルの複雑さを制限することで、セキュリティ管理を簡素化するのに役立ちます。プライマリクラウドは、セキュリティツール、モニタリングソリューション、運用プロセスへの投資のほとんどを受け取ります。これにより、均等に分割されたリソースで可能なよりも強力なセキュリティ基盤が作成されます。

当社のガイダンス：

- ほとんどのビジネス要件と技術要件に合ったプライマリクラウドプロバイダーを選択します。このプロバイダーは、ワークロードの少なくとも 80% をサポートし、クラウド戦略の基盤となる必要があります。トレーニングへの投資、アーキテクチャ標準、運用プロセスは、このプライマリプラットフォームの価値を最大化することに集中します。
- セカンダリクラウドへの配置を必要とするワークロードの明確な基準を策定します。これらの基準は、プライマリプロバイダーでは達成できない特定のビジネス価値に焦点を当てる必要があります。プロバイダー間の支出の公平性や人為的なバランスを維持するために、ワークロードをセカンダリクラウドに配置しないようにします。
- 80/20 アプローチを反映するようにエンタープライズ契約を構築します。集中的な支出に基づいてプライマリプロバイダーとボリューム割引を交渉し、特定のユースケースでセカンダリプロバイ

ダーとの柔軟性を維持します。このアプローチにより、購入レバレッジが最大化され、通常、支出を均等に分割するよりも全体的な料金が高くなります。

- 人材戦略を 80/20 アプローチに合わせます。特定のワークロードをサポートするセカンダリプラットフォームに関する十分な知識を維持しながら、プライマリプロバイダーのサービスに関する深い専門知識の開発に投資します。この重点的な人材戦略により、生産性が向上し、デリバリーが加速され、重要なスキルギャップのリスクが軽減されます。
- マルチクラウド戦略のビジネス成果を定期的に測定します。各プロバイダーから取得した値を示すメトリクスを追跡し、必要に応じてディストリビューションを調整します。目標は、マルチクラウドを完全に回避することではなく、特定のワークロードが他のプロバイダーに固有の機能から本当に恩恵を受けるように戦略的に実装することです。

結論

このホワイトペーパーでは、効果的なマルチクラウド戦略を開発するための 9 つの重要な原則について説明しました。組織は、特定のビジネスニーズが必要とする追加のプロバイダーを戦略的に使用し、主要なクラウドアプローチを通じて最大の成功を達成します。これまで説明した 80/20 アプローチは、焦点と柔軟性のバランスを取り、組織は正当なマルチクラウド要件に対処しながら、より深い専門知識を開発し、より強力なプロバイダー関係を維持し、より貴重な人材を構築できます。

マルチクラウドの実装を成功させるには、業界の傾向に従うのではなく、ビジネスニーズを明確に評価する必要があります。企業は、堅牢なガバナンスを確立し、セキュリティを最優先事項として維持し、接続されたワークロードをプロバイダー間で分散させないようにし、トランザクションデータを使用してアプリケーションを維持し、コンテナの制限を認識し、統一された専門的な Cloud Center of Excellence を維持する必要があります。

クラウドへの AWS アプローチは、基本的にお客様の選択と相互運用性に基づいています。お客様のビジネスニーズが 1 つのプロバイダーにとどまらないことがよくあることを理解しているため、ツールとサービスは環境間でシームレスに機能するように設計されています。ハイブリッド接続ソリューションから、環境にまたがるコンテナオーケストレーションまで、 はテクノロジー環境全体で効果的に運用するのに役立つ機能 AWS を提供します。

は、複数のプラットフォームのエキスパートになるよう強制するのではなく、直感的なツールと一貫したインターフェイスを通じてマルチクラウド管理 AWS を簡素化します。お客様がイノベーションに集中できるように、複雑さの排除に重点を置いています。これらの機能は、 AWS のみを使用するか、他の環境 AWS のサービス と一緒に特定の を使用するかにかかわらず、独自の条件でマルチクラウド戦略を実装するのに役立ちます。

クラウドはビジネス戦略を制約するのではなく、強化する必要があります。このホワイトペーパーで説明されている原則を適用し、 AWS 相互運用性機能を活用することで、価値を最大化し、不要な複雑さを最小限に抑え、組織が今日の動的なビジネス環境で長期的に成功するためのクラウドアプローチを構築できます。

ハイブリッドおよびマルチクラウド環境全体の管理を簡素化するのに役立つ AWS ソリューションの詳細については、AWS 「マルチクラウドのソリューション」を参照してください。

リソース

リファレンス

- Cloud Center of Excellence (CCOE) を使用してエンタープライズ全体を変革する (AWS ブログ記事)
- AWS Well-Architected フレームワーク
- Cost Optimization Hub による機会の特定 (AWS Cost Management ドキュメント)
- アマゾン ウェブ サービスへの移行のビジネス価値 (ハケットグループ、2022 年 2 月)
- から移行する際のインターネットへの無料のデータ転送 AWS (AWS ブログ記事)

ツール

- ゾーンオートシフト – 潜在的な問題を検出すると、トラフィックをアベイラビリティーゾーンから自動的に移行します (AWS ブログ記事)
- AWS マルチクラウド向けの ソリューション

AWS パートナー

- AWS クラウド オペレーションのコンピテンシー

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
初版発行	—	2025 年 9 月 3 日

AWS 規範ガイダンスの用語集

以下は、 AWS 規範ガイダンス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。

アベイラビリティーゾーン (AZ)

他のアベイラビリティーゾーンの障害から 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ー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 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ダ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、クラウド導入を成功させるための組織の準備に役立つ人材開発、トレーニング、コミュニケーションに関するガイダンスを提供します。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 1 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。

ブレークグラスアクセス

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 ガイダンスの「ブレークグラス手順の実装」インジケータを参照してください。

ブラウンフィールド戦略

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ン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。

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。移行戦略との関連性については、 AWS「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が、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。信頼された ID のみが、期待されるネットワークから信頼された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 に採用するときは 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で使用できるサービス」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ュファクチャリング・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。

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 (ボストン: 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 、ガバナンス要件への準拠に影響するランディングゾーンの変更を検出したりできます。

DVSM

「開発バリューストリームマッピング」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使用できる、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ーゾーン 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/サブスクライブ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 のすべてのイベント AWS CloudTrail を ログに記録する 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

読み取り専用に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)

サービスの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。

レスポンシブコントロール

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「レスポンシブコントロール」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、フェデレーティ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、レスポンシブ、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

のエントリポイントの 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ー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の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、 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。

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

ゼロデイエクスプロイト

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。