ゼロトラストの導入: 安全かつ機敏なビジネス変革戦略のための戦略

AWS 規範ガイダンス

AWS 規範ガイダンス: ゼロトラストの導入: 安全かつ機敏なビジネス変革戦略のための戦略

Table of Contents

ゼロトラストの導入: 安全かつ機敏なビジネス変革戦略のための戦略

Greg Gooden (Amazon Web Services (AWS))

2023 年 12 月 (ドキュメント履歴)

今日、組織はこれまで以上にセキュリティを重要な優先事項として重視しています。これにより、顧客の信頼の維持から、従業員のモビリティの向上、新しいデジタルビジネス機会の開拓まで、幅広いメリットが得られます。その際、「システムとデータに適切なレベルのセキュリティと可用性を確保するための最適なパターンは何か？」という古くからの質問が次から次へと出てきます。ゼロトラストが、この質問に対する答えを表すのに使われる最新の用語になってきています。

ゼロトラストアーキテクチャ (ZTA) は、従来のネットワーク制御やネットワーク境界だけに依存しない、またはそれに根本的に依存しない、デジタル資産に関するセキュリティ制御を提供することに焦点を当てた概念モデルおよび、関連する一連のメカニズムです。代わりに、ID、デバイス、動作、その他の豊富なコンテキストやシグナルをネットワーク制御に追加して、よりきめ細かく、インテリジェントで、適応性が高く、継続的なアクセスに関する意思決定を行います。ZTA モデルを実装することで、サイバーセキュリティ、特に多層防御の概念が継続的に成熟する中で、次の段階において有意義な成果を上げることができます。

意思決定プロセス

ZTA 戦略を実施するには、慎重な計画と意思決定が必要です。これには、さまざまな要素を評価し、組織の目標と整合させることが含まれます。ZTA の取り組みに着手するための主な意思決定プロセスには以下が含まれます。

1. 利害関係者の関与 — 他の経営幹部、バイスプレジデント、上級管理職と連携して、組織のセキュリティ態勢に関する優先事項、懸案事項、ビジョンを理解してもらうことが重要です。主要な利害関係者を最初から関与させることで、ZTA の導入を全体的な戦略的目標に合わせることができ、必要なサポートやリソースを獲得できます。
2. リスク評価 — 包括的なリスク評価を実施することで、問題、過剰な露出、重要な資産を特定できます。これによりセキュリティ制御と投資について情報に基づいた決定を下すことができます。業界や運用環境に固有のリスク状況に基づいて、組織の既存のセキュリティ態勢を評価し、潜在的な弱点を特定し、改善すべき分野に優先順位を付けます。

3. 技術評価 — 組織の既存の技術状況を評価し、ギャップを特定することは、ZTA の原則に沿った適切なツールやソリューションを選択するのに役立ちます。この評価には、以下の項目を綿密に分析する必要があります。
   - ネットワークアーキテクチャ
   - アイデンティティとアクセス管理システム
   - 認証と認可のメカニズム
   - 統合エンドポイント管理
   - リソース所有ツールとプロセス
   - 暗号化技術
   - モニタリングとログ記録の機能
   - 堅牢な ZTA モデルを構築するには、適切なテクノロジースタックを選択することが欠かせません。
4. 変更管理 — ZTA モデルを採用することによる文化的および組織的な影響を認識することは不可欠です。変更管理のプラクティスを導入することで、組織全体での移行と承認が円滑になります。これには、ZTA の原則と利点に関する従業員の教育、新しいセキュリティ慣行に関するトレーニングの提供、アカウンタビリティと継続的な学習を奨励するセキュリティ意識の文化の促進が含まれます。

この規範的なガイダンスは、経営幹部、バイスプレジデント、上級管理職に ZTA を導入するための包括的な戦略を提供することを目的としています。以下を含む ZTA の主要な側面について掘り下げて説明します。

- 組織の準備状況
- 段階的導入アプローチ
- 利害関係者の協力
- 安全かつ機敏なビジネス変革を実現するためのベストプラクティス

このガイダンスに従うことで、組織は ZTA ランドスケープをナビゲートし、Amazon Web Services (AWS) クラウドでセキュリティジャーニーを成功させることができます。 AWS は AWS Verified Access、、 AWS Identity and Access Management (IAM)、Amazon Virtual Private Cloud (Amazon VPC)、Amazon VPC Lattice、Amazon Verified Permissions、Amazon API Gateway、Amazon GuardDuty など、ZTA の実装に使用できるさまざまなサービスを提供します。これらのサービスは、不正アクセスから AWS リソースを保護するのに役立ちます。

ターゲットを絞ったビジネス成果

このセクションでは、組織全体でのゼロトラストアーキテクチャの定義と実装に関連して期待される成果について説明します。

セキュリティ態勢の強化

ゼロトラストの原則を採用することで、組織はセキュリティ体制を強化し、セキュリティリスクを軽減し、クラウドインフラストラクチャとデータを保護することができます。知る必要性に応じてアクセス権を付与するというゼロトラストの基本原則は、厳格な管理と相まって、露出を大幅に削減し、セキュリティイベントの潜在的な影響を制限します。このプロアクティブなアプローチにより、組織は新たなセキュリティリスクに先んじて、資産の機密性、整合性、可用性を達成することができます。

シームレスなクラウドの採用

明確に定義されたゼロトラストアーキテクチャ (ZTA) 導入計画を策定することで、クラウド環境への移行を円滑に成功させることができます。ZTA の原則は、組織がクラウドコンピューティングのメリットを安全に享受するための強固な基盤を提供するという点で、クラウドセキュリティのベストプラクティスと密接に一致しています。ZTA の原則を最初から組み込むことで、組織はセキュリティを中核要素とするクラウドアーキテクチャを設計しやすくなります。

コンプライアンスと規制の調整

ZTA プラクティスを導入することで、組織は業界や規制の要件や基準を満たすことができます。ZTA は本質的に最小特権の原則を推進し、厳格なアクセス制御を実施しています。アクセス制御は、多くの場合、次のような規制によって義務付けられています。

- Federal Risk and Authorization Management Program (FedRAMP)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)。

ゼロトラストを採用することで、組織は罰則や風評被害を受ける可能性を最小限に抑えながら、データ保護、プライバシー、規制順守への取り組みを実証することができます。

データ保護の強化

組織は、データ暗号化、アクセス制御、定期的なセキュリティ評価を実施することで、クラウド導入プロセス全体を通じて機密データを保護できます。組織では次のような具体的な対策を講じることができます。

- データ暗号化 — データ暗号化 — データ暗号化は、クリアテキストデータを暗号文に暗号化するプロセスで、データを復号化して元のクリアテキスト形式に戻すには鍵が必要です。これにより、たとえ権限のない個人がデータのコピーを入手できたとしても、機密データにアクセスすることがはるかに困難になります。
- アクセス制御 — アクセス制御は、機密データにアクセスできるユーザーと、そのデータを使ってできることを制限します。これは、ユーザーの役割とアクセス許可を割り当て、多要素認証やその他の方法を使用してユーザー ID を確認することで実現できます。
- 定期的なセキュリティ評価 — 定期的なセキュリティ評価により、組織はセキュリティ問題を特定して対処し、事前に修正することができます。これらの評価は、社内のセキュリティチームまたは外部のセキュリティ会社によって実施されます。

ゼロトラストアーキテクチャは、さまざまなセキュリティ対策を実施することにより、データ保護に包括的なアプローチを取ります。これらの対策には、強力な認証、データ暗号化、きめ細かなアクセス制御が含まれます。このアプローチは、データ関連のセキュリティイベントのリスクを最小限に抑え、機密情報を不正アクセスから保護します。

効率的なインシデント対応

組織は、クラウド環境で監視とインシデント対応のフレームワークを確立することで、セキュリティイベントをより迅速かつ効果的に検出して対応できます。ゼロトラストアーキテクチャは、継続的な監視、脅威インテリジェンスの統合、ユーザーアクティビティ、ネットワークトラフィック、システム動作のリアルタイムの可視化に重点を置いています。そうすると、セキュリティチームはセキュリティイベントを事前に特定して軽減できます。このアプローチは、潜在的な問題の検出と対応にかかる時間を短縮し、事業運営への影響を最小限に抑えます。主な特徴は次のとおりです。

- テスト — 組織が採用しているインシデント対応のフレームワークや方法論にかかわらず、インシデント対応計画を定期的にテストする必要があります。テーブルトップ演習、シミュレーション、レッドチーム編成によって、現実的な設定でインシデント対応を実践し、ツールや能力のギャップを明らかにし、インシデント対応担当者の経験と自信を高めることができます。

- 監視 — クラウド環境に異常なアクティビティの兆候がないか継続的に監視します。これには、ログ分析、ネットワーク監視、脆弱性スキャンなど、さまざまなツールや手法を利用します。
- 脅威インテリジェンスの統合 — 脅威インテリジェンスを、監視およびインシデント対応のフレームワークに統合します。これにより、組織は脅威をより迅速かつ効果的に特定して対応できるようになります。
- リアルタイムの可視性 — セキュリティインシデントを迅速に特定して対応するには、ユーザーのアクティビティ、ネットワークトラフィック、システム動作をリアルタイムで可視化する必要があります。
- 事前の特定と軽減 — セキュリティイベントを事前に特定して軽減することで、潜在的な脅威の検出と対応にかかる時間を短縮し、事業運営への影響を最小限に抑えることができます。

従業員の生産性向上

現代の従業員には、ますます多様化する場所、デバイス、時間帯から仕事をこなせる柔軟性が求められます。ZTA を導入することで、組織のセキュリティ態勢を維持または改善しながら、これらの要件に対応し、従業員のモビリティ、生産性、満足度を向上させることができます。

デジタルトランスフォーメーションの活用

組織にとって、デジタルトランスフォーメーションの一環として、従来のネットワーク境界の外にあるデバイス、マシン、施設、インフラストラクチャ、プロセスの相互接続の必要性が増しています。モノのインターネット (IoT) やオペレーショナルテクノロジー (OT、産業用モノのインターネット (IIoT) とも呼ばれる) デバイスは、遠隔測定情報や予知保全情報をクラウドに直接送信することがよくあります。ワークロードを保護するには、従来の境界アプローチを超えるセキュリティ制御を適用する必要があります。

セクション概要

こうしたターゲットを絞ったビジネス成果に焦点を当てることで、組織は ZTA の可能性を最大限に引き出し、クラウドにおけるセキュリティ態勢を強化することができます。これらの成果を特定の組織の目標と整合させ、独自のビジネス要件に合わせて調整し、その有効性を定期的に評価して継続的な改善を推進することが重要です。

ゼロトラストの原則を理解する

ゼロトラストアーキテクチャ (ZTA) は、セキュリティモデルの基礎となる一連の中核となる原則に基づいています。これらの原則を理解することは、ZTA 戦略を効果的に採用しようとしている組織にとって不可欠です。このセクションでは、ZTA の中核的原則について説明します。

検証と認証

検証と認証の原則は、ユーザー、マシン、デバイスを含むあらゆるタイプのプリンシパルの強力な識別と認証の重要性を強調しています。ZTA では、セッション中、ID と認証ステータスを継続的に検証する必要があります。理想的には、リクエストごとに行われることが期待されます。それは、従来のネットワークの位置や制御だけに頼るものではありません。これには、最新の強力な多要素認証 (MFA) の実装や、認証プロセス中の追加の環境信号やコンテキスト信号の評価が含まれます。この原則を採用することで、組織はリソース承認の決定に可能な限り最高の ID インプットが反映されるようにすることができます。

最小特権アクセス

最小特権の原則では、プリンシパルにタスクの実行に必要な最低限のアクセスを付与します。最小特権アクセスの原則を採用することで、組織はきめ細かなアクセス制御を実施し、プリンシパルがそれぞれの役割と責任を果たすために必要なリソースにのみアクセスできるようにすることができます。これには、ジャストインタイムのアクセスプロビジョニング、ロールベースのアクセス制御 (RBAC)、定期的なアクセスレビューを実施して、露出と不正アクセスのリスクを最小限に抑えることが含まれます。

マイクロセグメンテーション

マイクロセグメンテーションは、特定のトラフィックフローを許可するために、ネットワークをより小さな独立したセグメントに分割するネットワークセキュリティ戦略です。ワークロードの境界を作り、異なるセグメント間で厳格なアクセス制御を実施することで、マイクロセグメンテーションを実現できます。

マイクロセグメンテーションは、ネットワーク仮想化、ソフトウェア定義ネットワーク (SDN)、ホストベースのファイアウォール、ネットワークアクセスコントロールリスト (NACLs)、Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループや などの AWS 特定の機能を通じて実

装できます AWS PrivateLink。セグメンテーションゲートウェイは、セグメント間のトラフィックを制御してアクセスを明示的に許可します。マイクロセグメンテーションとセグメンテーションゲートウェイは、組織がネットワークを経由する不要な経路、特に重要なシステムやデータにつながる経路を制限するのに役立ちます。

継続的なモニタリングと分析

継続的なモニタリングと分析には、組織の環境全体にわたるセキュリティ関連のイベントとデータの収集、分析、相関関係が含まれます。堅牢なモニタリングツールと分析ツールを導入することで、組織はセキュリティデータとテレメトリを一元的に評価できます。

この原則は、異常や潜在的なセキュリティイベントを特定するために、ユーザーの行動、ネットワークトラフィック、システムアクティビティを可視化することの重要性を強調しています。セキュリティ情報およびイベント管理 (SIEM)、ユーザーおよびエンティティ行動分析 (UEBA)、脅威インテリジェンスプラットフォームなどの高度なテクノロジーは、継続的なモニタリグと予防的な脅威検出を実現する上で重要な役割を果たします。

自動化とオーケストレーション

自動化とオーケストレーションは、組織がセキュリティプロセスを合理化し、手作業による介入を減らし、応答時間を短縮するのに役立ちます。日常的なセキュリティタスクを自動化し、オーケストレーション機能を使用することで、組織は一貫したセキュリティポリシーを実施し、セキュリティイベントに迅速に対応できます。この原則には、ユーザー権限を適時かつ正確に管理できるように、アクセスのプロビジョニングとプロビジョニング解除のプロセスを自動化することも含まれます。自動化とオーケストレーションを取り入れることで、組織は業務効率を高め、人的ミスを減らし、より戦略的なセキュリティイニシアチブにリソースを集中させることができます。

Authorization

ZTA では、リソースへのアクセスを求める各リクエストは、ゲーティング適用ポイントによって明示的に承認される必要があります。認証された ID に加えて、認可ポリシーでは、デバイスの状態と態勢、動作パターン、リソース分類、ネットワーク要因などの追加のコンテキストを考慮する必要があります。承認プロセスでは、この集中型コンテキストを、アクセスされているリソースに関連する対応するアクセスポリシーと照らし合わせて評価する必要があります。機械学習モデルで宣言型ポリシーを動的に補完できることが望ましいです。これらのモデルを使用する場合は、追加の制限のみに重点を置いてください。明示的に指定されていないアクセス権を付与すべきではありません。

セクション概要

ZTA のこれらの中核的原則を順守することで、組織は現代の企業環境の多様性に対応する強固なセキュリティモデルを確立できます。これらの原則を実装するには、テクノロジー、プロセス、人材を組み合わせた包括的なアプローチでゼロトラストの考え方を実現し、レジリエントなセキュリティ態勢を構築する必要があります。

ゼロトラストアーキテクチャの主要コンポーネント

ゼロトラストアーキテクチャ (ZTA) 戦略を効果的に実装するには、組織が ZTA を構成する主要なコンポーネントを理解する必要があります。これらのコンポーネントは連携して、ゼロトラストの原則に沿った包括的なセキュリティモデルを確立します。このセクションでは、ZTA の主要コンポーネントについて説明します。

Identity and Access Management

アイデンティティとアクセス管理は、強固なユーザー認証と大まかなアクセス制御メカニズムを提供することで ZTA の基盤を形成します。これには、シングルサインオン (SSO)、多要素認証 (MFA)、および ID ガバナンスと管理ソリューションなどのテクノロジーが含まれます。アイデンティティとアクセス管理は、ゼロトラストの認可決定を行うために不可欠な、高いレベルの認証保証と重要なコンテキストを提供します。同時に、ZTA は、ユーザーごと、デバイスごと、セッションごとにアプリケーションやリソースへのアクセスが許可されるセキュリティモデルでもあります。これにより、ユーザーの認証情報が漏えいした場合でも、組織を不正アクセスから守ることができます。

セキュアアクセスサービスエッジ

セキュアアクセスサービスエッジ (SASE) は、ネットワークとセキュリティの機能を仮想化、結合、分散して、単一のクラウドベースのサービスにする、ネットワークセキュリティへの新しいアプローチです。SASE は、ユーザーの場所に関係なく、アプリケーションやリソースへの安全なアクセスを提供します。

SASE には、セキュアウェブゲートウェイ、サービスとしてのファイアウォール、ゼロトラストネットワークアクセス (ZTNA) など、さまざまなセキュリティ機能が含まれています。これらの機能が連携して、マルウェア、フィッシング、ランサムウェアなどのさまざまな脅威から組織を保護します。

データ損失防止

データ損失防止 (DLP) テクノロジーは、組織が機密データを不正開示から保護するのに役立ちます。DLP ソリューションは、移動中および保管中のデータをモニタリングおよび制御します。これにより、組織はデータ関連のセキュリティイベントを防止するポリシーを定義して適用できるようになり、機密情報をネットワーク全体で確実に保護できるようになります。

Security Information and Event Management

Security Information and Event Management (SIEM) ソリューションは、組織のインフラストラクチャ全体のさまざまなソースからセキュリティイベントログを収集、集約、分析します。このデータを使用して、セキュリティインシデントの検出、インシデント対応の促進、潜在的な脅威や脆弱性に関するインサイトの提供を行うことができます。

特に ZTA にとって、さまざまなセキュリティシステムからの関連するテレメトリを相互に関連付けて理解する SIEM ソリューションの機能は、異常パターンの検出と対応を向上するために重要です。

エンタープライズリソース所有権カタログ

エンタープライズリソースへのアクセスを適切に許可するには、組織はこれらのリソースおよび、重要なこととしては、その所有者をカタログ化する信頼できるシステムを必要とします。この信頼できる情報源は、アクセス要求、関連する承認決定、およびそれらの定期的な証明を容易にするワークフローを備えている必要があります。やがて、この信頼できる情報源には、組織内において「誰が何にアクセスできるのか」という答えが含まれることになります。その回答を、承認と監査、コンプライアンスの両方に使用できます。

統合エンドポイント管理

ZTA は、ユーザーを強力に認証するだけでなく、ユーザーのデバイスのヘルス、態勢、状態も考慮して、企業データとリソースへのアクセスが安全かどうかを評価する必要があります。統合エンドポイント管理 (UEM) プラットフォームには以下の機能があります。

- デバイスプロビジョニング
- 継続的な構成とパッチ管理
- セキュリティのベースライン
- テレメトリレポート
- デバイスのクレンジングと使用終了

ポリシーベースの適用ポイント

ZTA では、各リソースへのアクセスは、ゲーティングポリシーベースの適用ポイントによって明示的に許可される必要があります。最初は、これらの適用ポイントを、既存のネットワークや ID システム内の既存の適用ポイントに基づいて設定してもかまいません。ZTA が提供する幅広いコンテキ

ストとシグナルを考慮することで、適用ポイントの機能を段階的に高めることができます。長期的には、統合コンテキストに基づいて運用され、シグナルプロバイダーを一貫して統合し、包括的なポリシーセットを維持し、テレメトリを組み合わせて収集した情報で強化される、ZTA 固有の適用ポイントを組織に導入する必要があります。

セクション概要

これらの主要要素を理解することは、ZTA の採用を計画している組織にとって不可欠です。これらのコンポーネントを実装し、まとまりのあるセキュリティモデルに統合することで、組織はゼロトラストの原則に基づいた強力なセキュリティ態勢を確立できます。以下のセクションでは、組織内での ZTA の導入を成功させるのに役立つ、組織の準備状況、段階的導入アプローチ、ベストプラクティスについて説明します。

ゼロトラスト導入に向けた組織の準備状況の評価

新しいアーキテクチャ戦略を採用することは、慎重な計画と組織の要因の検討を必要とする重要な作業です。このセクションでは、全社でゼロトラストを採用するための組織の準備状況に関する重要な考慮事項に焦点を当てます。これらの考慮事項に取り組むことで、組織はより強力で効果的なセキュリティ対策への道を開くことができます。

リーダーシップの連携とコミュニケーション

ゼロトラストをうまく実施するには、リーダーシップの連携とコミュニケーションが不可欠です。リーダーは、ゼロトラストの利点と必要なリソースを理解する必要があります。また、リーダーは組織の文化やプロセスを積極的に変えていかなければなりません。信頼を築き、賛同してもらうには、従業員とのコミュニケーションが不可欠です。従業員は、なぜ組織がゼロトラストを導入しているのか、それが彼らにとって何を意味するのか、どのように協力できるのかを理解する必要があります。コミュニケーションはオープンで、透明性があり、継続的である必要があります。

リーダーシップの支援と賛同

ゼロトラストアーキテクチャ (ZTA) の導入を成功させるには、アーキテクチャの目標、メリット、成功の尺度について、主要な利害関係者と経営陣の足並みを揃えることが重要です。従来の境界ベースのセキュリティから、よりきめ細かなユーザー中心のアプローチに移行することで、セキュリティを強化し、ビジネスの俊敏性を実現する上で、ゼロトラスト原則の重要性を共有します。このアプローチに切り替えることで、組織は変化や脅威により迅速に適応できます。経営陣が連携することで、組織の雰囲気を整え、変化に対する潜在的な抵抗を克服することができます。

透明性の高いコミュニケーション

ゼロトラストの導入プロセス全体を通じて、従業員とのオープンで透明なコミュニケーションを維持します。導入の根拠、利点、期待される結果を説明し、懸念事項に迅速に対処します。実施の進捗状況を定期的に更新します。これにより、賛同が増え、抵抗が減り、信頼が築かれます。

スキル開発とトレーニング

リーダーが足並みを揃え、コミュニケーションがオープンになったら、ゼロトラストを導入する従業員がスキルと知識を身に付けることが重要です。これには、ゼロトラストの原則の理解、業務への実装方法、セキュリティイベントへの対応方法などが含まれます。従業員がこれらのスキルを習得できるように、トレーニングと能力開発の機会を提供してください。

クラウドに関する知識とスキル

クラウドテクノロジーとゼロトラストの原則に関する組織のスキルと知識のギャップを評価します。従業員のスキルを向上させ、クラウド中心のゼロトラスト環境で効果的に働くために必要な専門知識を身に付けるためのトレーニングと能力開発プログラムを提供します。進化するテクノロジーやセキュリティ慣行に遅れずについていくために、継続的な学習の文化を育んでください。

セキュリティ文化と意識

組織のセキュリティ文化を評価します。従業員のセキュリティ意識のレベル、セキュリティのベストプラクティスに対する理解、ポリシーと手順の順守状況を評価します。セキュリティに関する知識のギャップを特定します。ゼロトラストの重要性と安全な環境を維持する上での役割について従業員を教育するために、セキュリティ意識向上トレーニングプログラムの実施を検討してください。

組織構造と役割

ゼロトラストの実装を成功させるために、効果的な組織構造と役割を確立します。これには、Cloud Center of Excellence (CCoE) の設立、セキュリティ運用のレビューと変更、脆弱性管理、インシデント対応、セキュリティモニタリングの役割と責任の割り当てが含まれます。

Cloud Center of Excellence

CCoE を確立して、クラウド運用のガイダンス、ベストプラクティス、監督を行います。CCoE は、クラウド関連のベストプラクティス、ガイドライン、ガバナンスポリシーの作成と実施を担当するチームまたは個人のグループです。CCoE にさまざまな事業部門や IT チームの代表者が参加して、コラボレーションと連携を確保します。CCoE は、クラウドホスト型のワークロードへのゼロトラストの原則の導入を促進する上で重要な役割を果たします。組織全体での知識共有を促進するのも、CCoE の役割です。

セキュリティオペレーション

ゼロトラスト環境のニーズを満たすには、現在のセキュリティ運用組織を見直し、修正します。モニタリング、インシデント対応、脅威インテリジェンス機能を向上させるには、セキュリティオペレーションセンター (SOC) またはマネージドセキュリティサービスプロバイダー (MSSP) の導入を検討してください。脆弱性管理、インシデント対応、セキュリティモニタリングの役割と責任を確立してください。軽微なセキュリティイベントを迅速に検出して修正し、一連のイベントを中断させるには、インシデント対応プロセスを適切に機能させることが不可欠です。これにより、軽微なイベントがより影響の大きいイベントに発展するのを防ぐことができます。

IT インフラストラクチャとアーキテクチャ

自社の IT アーキテクチャとインフラストラクチャを調べて、ゼロトラストアプローチの導入に影響する可能性のある制約や依存関係がないか調べます。現在のアプリケーションやシステムが、必要なゼロトラストアーキテクチャコンポーネントと互換性があるかどうかを判断します。ゼロトラスト原則の導入を成功させるためには、インフラストラクチャの改善や調整が必要かどうかを分析します。アプリケーションまたはシステムごとに、ゼロトラストを現場で実装するのが最適なのか、それとも大規模なモダナイズ努力によって実装するのが最善なのかを検討してください。

リスク管理、ガバナンス、変更管理

ゼロトラストの実装を成功させるために、効果的なリスク管理、ガバナンス、変更管理のプロセスを確立します。これには、リスク管理とゼロトラスト原則との連携、インシデント対応計画の策定、法務部門やコンプライアンス部門との協力、変更管理プロセスの確立などが含まれます。

リスク管理

自社で実施されているリスク管理戦略を調べ、それがゼロトラストの原則にどの程度準拠しているかを判断してください。現在のインシデント対応システム、セキュリティ対策、リスク評価手順の効率性を分析します。ゼロトラスト戦略に準拠するために改善が必要な分野を特定します。解決までの時間を短縮するために、自動インシデント対応システムまたは継続的なモニタリングと分析のフレームワークの開発に取りかかってください。

変更管理プロセス

クラウド関連のすべての変更がセキュリティとコンプライアンスの要件を満たすようにするために、効果的な変更管理方法を確立します。セキュリティ構成分析、リスク評価、承認、文書化を含む体系的な変更管理手順を確立します。ゼロトラストアーキテクチャの完全性を維持するために、更新を頻繁に確認して監査してください。

モニタリングと評価

ゼロトラストの実装を成功させるには、組織はセキュリティ体制を継続的にモニタリングし、評価する必要があります。これには、重要業績評価指標 (KPI) の確立、KPI のモニタリングと評価、継続的改善の文化の促進が含まれます。これらのステップに従うことで、組織はゼロトラストの実施を成功させ、常にセキュリティの向上に取り組んでいることを確認できます。

重要業績評価指標

適切な重要業績評価指標 (KPI) を確立して、ゼロトラスト導入の成功と有効性を評価します。これらの KPI により、ユーザー満足度、設備と展開の進捗状況、コスト削減、コンプライアンス順守、セキュリティ手段の発生回数を測定する場合があります。全体的な開発状況を把握し、改善の機会を見つけるために、これらの KPI を定期的にモニタリングして評価します。

継続的な改善

ステークホルダーから意見やインサイトを引き出すシステムを確立することで、継続的な改善の文化を育むことができます。クラウド環境のセキュリティ、有効性、ユーザーエクスペリエンスを改善するための考えや提案を共有するよう、スタッフに促します。この意見を手順の効率化、セキュリティ対策の改善、イノベーションの促進に役立ててください。

セクション概要

このような組織的および文化的な考慮事項に対処することで、組織はゼロトラストのセキュリティモデルのクラウド導入を支援する環境を促進できます。次のセクションでは、段階的な導入アプローチを検討し、ゼロトラストの原則を実用的かつ管理しやすい方法で徐々に実装する方法についてのガイダンスを提供します。

ゼロトラストの考え方を育む

ゼロトラストの実装は、技術的な実装にとどまりません。組織内で文化を変化させる必要があります。ゼロトラストの考え方を育むには、以下の重要な側面を強調する必要があります。

ゼロトラストの教育とトレーニング

ゼロトラストアーキテクチャ (ZTA) の価値と利点について従業員を教育します。トレーニングセッション、ワークショップ、その他のリソースを通じて、ZTA の概念とアプローチの技術的説明と非技術的説明を提供します。ゼロトラストのセキュリティパラダイムを確立して維持する際の責任を認識するよう、スタッフに促します。

コラボレーションとコミュニケーション

ZTA の実装に関係するすべてのチームや部門でコラボレーションと透明性を促進します。全員が計画を完全に理解できるように、部門間のコミュニケーション、知識共有、情報交換を促進します。責任共有の文化を創造し、ビジネス全体のセキュリティに対する貢献の重要性を全員が認識できるようにします。

継続的な学習と改善

ゼロトラストの文脈で継続的な学習と改善を優先します。最新のセキュリティの傾向、テクノロジー、ベストプラクティスを常に把握するよう、従業員を奨励します。イノベーションと実験の文化を育むことで、従業員が組織のセキュリティ体制を強化するための新しいソリューションとアプローチを検討するよう促されます。

メトリクスと説明責任

ゼロトラスト戦略の有効性を測定するための明確なメトリクスと説明責任のメカニズムを確立します。組織のセキュリティ目標に沿った主要業績評価指標 (KPIs) を定義し、定期的に進捗状況を追跡します。ゼロトラストの原則の実装と維持への貢献について、個人とチームに説明責任を持たせます。

セクション概要

これらの側面に対処し、ゼロトラストの考え方を育むことで、組織はゼロトラストの導入と実装を成功させるための強固な基盤を構築できます。この文化シフトは、組織内のすべての人がゼロトラストの重要性を理解し、その成功に積極的に貢献するために不可欠です。

次のセクションでは、段階的な導入アプローチを検討し、ゼロトラストの原則を実用的かつ管理しやすい方法で徐々に実装する方法についてのガイダンスを提供します。

ゼロトラストへの段階的アプローチ

ゼロトラストアーキテクチャ (ZTA) を採用するには、慎重な計画と実装が必要です。移行を円滑に進め、事業運営の中断を最小限に抑えるために、段階的な導入アプローチをお勧めします。このセクションでは、ZTA の採用に関わる主な段階に関するガイダンスを提供します。

フェーズ 1: 評価と計画

ゼロトラスト導入の最初のフェーズは、評価と計画です。このフェーズは、組織の現在のセキュリティ体制におけるギャップを特定して対処する必要があるため、導入全体を成功させるために不可欠です。時間をかけて現在の状態を評価し、セキュリティ目標を定義することで、ゼロトラスト導入を成功させるための基礎を築くことができます。

同時に、完全で正確な評価が現実的ではない場合もあります。分析が停滞して次のフェーズに進めなくなることがないように、区分化の準備をするか、ある程度の不完全さを受け入れてください。

1. 現在の状態の評価 — 既存のセキュリティインフラストラクチャ、ポリシー、統制を評価してください。潜在的な脆弱性、セキュリティ上のギャップ、ゼロトラスト原則の導入によって改善が見込める分野を特定します。
2. セキュリティ目標の定義 — 現在の状況の評価結果に基づいて、ゼロトラストの原則に沿ったセキュリティ目標を定義します。これらのセキュリティ目標は、組織の全体的なセキュリティ戦略と一致するものであり、特定された脆弱性やギャップに対処できるものである必要もあります。
3. アーキテクチャの設計 — 組織のセキュリティ目標をサポートする ZTA を開発します。このアーキテクチャには、ID およびアクセス管理ソリューション、ネットワークセグメンテーションメカニズム、継続的監視システムなど、必要なコンポーネントが含まれている必要があります。また、アーキテクチャはスケーラブルで適応性があり、将来の成長や技術の進歩に対応できるものでなければなりません。このアーキテクチャは、単なる文書や図としてではなく、 AWS CloudFormation テンプレートなど、実装を担当するチームが使いやすい形式で表現されることが望ましいです。
4. 利害関係者の関与 — 事業部門、IT チーム、セキュリティチームを含むすべての利害関係者を関与させ、洞察を得て、目標を ZTA 実装計画と一致させます。ゼロトラストアプローチの利点と要件について共通の理解を確立するために、コラボレーションとコミュニケーションを奨励します。

フェーズ 2: 試験運用と実装

ゼロトラスト導入の第 2 フェーズは、試験運用と実装です。このフェーズでは、小規模で制御された環境で ZTA をテストし、組織全体に繰り返し展開します。新しいセキュリティ対策と、ゼロトラスト環境を維持する上での各自の役割について、従業員を教育することが重要です。

1. 導入の試験運用 — 小規模で制御された環境で ZTA をテストします。アーキテクチャ設計段階で定義した必要なコンポーネントとセキュリティ制御を実装します。パイロット展開を注意深く監視し、フィードバックを収集し、必要な調整を行います。ゼロトラストが架空の演習から実際の体験を構築する演習に移行する段階で、プロセスの早い段階で柔軟に対応できるように準備してください。
2. 反復的な導入 — パイロット展開から学んだ教訓に基づいて、ゼロトラストの組織全体への反復的な導入を開始してください。フライホイール効果で勢いをつけましょう。大規模なキャンペーンを行わなくても、クリティカルな大規模展開を実現できます。リーダーシップの委任やエスカレーションは、ロールアウトの長期化によって必要になる可能性がある場合に取っておきます。
3. ユーザートレーニングの提供と意識向上 — 新しいセキュリティ対策と、ゼロトラスト環境を維持する上での各自の役割について従業員を教育します。強固なパスワード、多要素認証、定期的なセキュリティアップデートなど、セキュリティ対策の重要性を強調してください。
4. 変更管理 — ゼロトラストの導入に伴う組織的および文化的な変化に対応するための包括的な変更管理計画を作成します。導入の背景にある利点と理論的根拠を従業員に伝え、懸念事項や抵抗があれば対処します。円滑な移行を促進するため、継続的なサポートとガイダンスを提供してください。

フェーズ 3: モニタリングと継続的改善

ゼロトラスト導入の最終となる第 3 フェーズは、モニタリングと継続的改善です。このフェーズでは、包括的な監視および分析プログラムの確立、包括的なインシデント対応計画の作成、ステークホルダーやユーザーからの定期的なフィードバックの募集を行います。

1. 継続的な監視 — セキュリティ状況を継続的に評価し、潜在的な異常を検出するための包括的な監視および分析プログラムを確立します。高度なセキュリティツールとテクノロジーを使用して、ユーザーの行動、ネットワークトラフィック、システムアクティビティを監視します。
2. インシデント対応と修復の計画 — ゼロトラストの原則に沿った包括的なインシデント対応計画を作成します。明確なエスカレーションパスを確立し、役割と責任を定義し、可能な場合は自動インシデント対応メカニズムを実装します。インシデント対応計画への定期的なテストと更新を行います。

3. フィードバックと評価の取得 — 利害関係者やユーザーから定期的にフィードバックを募り、ゼロトラストアーキテクチャ (ZTA) の有効性に関する洞察を集めます。定期的な評価を実施して、セキュリティ体制、運用効率、ユーザーエクスペリエンスへの影響を測定します。フィードバックと評価結果を利用して、改善すべき分野を特定します。ZTA は時間の経過とともに変化することを想定し、開発チームが最小限の労力や中断でこれらの更新を実装する方法を検討してください。

セクション概要

この段階的な導入アプローチに従うことで、組織はリスクと混乱を最小限に抑えながら、ZTA に効果的に移行できます。次のセクションでは、ゼロトラストの導入を成功させるためのベストプラクティスについて、経営幹部、バイスプレジデント、上級管理職向けの重要な考慮事項と推奨事項について説明します。

ゼロトラストで成功を収めるためのベストプラクティス

ゼロトラストアーキテクチャ (ZTA) の導入を成功させるには、戦略的アプローチとベストプラクティスの順守が必要です。このセクションでは、経営幹部、バイスプレジデント、上級管理職がゼロトラストの導入を成功に導くための一連のベストプラクティスを紹介します。以下の推奨事項に従うことで、組織は強固なセキュリティ基盤を確立し、ゼロトラストアプローチのメリットを実感できます。

- 明確な目標とビジネス成果の定義 — クラウド運用の目標と期待されるビジネス成果を明確に定義します。これらの目標をゼロトラストの原則と一致させて、強固なセキュリティ基盤を構築すると同時に、ビジネスの成長と革新を可能にします。
- 包括的な評価の実施 — 現在の IT インフラストラクチャ、アプリケーション、データ資産を総合的に評価します。依存関係、技術的負債、潜在的な互換性問題を特定します。この評価は導入計画に反映され、重要度、複雑さ、ビジネスへの影響に基づいてワークロードに優先順位を付けるのに役立ちます。
- 導入計画の策定 — ワークロード、アプリケーション、データをクラウドに移行するための段階的なアプローチを概説した詳細な導入計画を組み込みます。導入フェーズ、スケジュール、依存関係を定義します。主要な利害関係者を関与させ、それに応じてリソースを割り当てます。
- 早期に構築を始める — ゼロトラストが組織内でどのようなものになるかを真に表す能力は、(分析して話し合うよりも) ゼロトラストの構築と展開を開始した後に大幅に向上します。
- 経営幹部の後援を得る — ゼロトラストの導入に向けて、経営幹部の後援とサポートを確保しましょう。他の経営幹部の協力を得てイニシアチブを支持し、必要なリソースを割り当てます。実施を成功させるために必要な文化や組織の変革を推進するには、リーダーシップのコミットメントが不可欠です。
- ガバナンスフレームワークの実装 — ゼロトラスト導入の役割、責任、意思決定プロセスを定義するガバナンスのフレームワークを作成します。セキュリティコントロール、リスク管理、コンプライアンスに関する説明責任と所有権を明確に定義します。変化するセキュリティ要件に適応できるよう、ガバナンスのフレームワークを定期的に見直し、更新します。
- 部門間のコラボレーションのサポート — 異なる事業部門、IT チーム、セキュリティチーム間のコラボレーションとコミュニケーションを促進します。ゼロトラストの実装全体を通じて連携と調整を促進するために、責任を共有する文化を作ります。頻繁なやり取り、知識の共有、共同での問題解決を奨励します。
- データとアプリケーションの保護 — ゼロトラストとは、エンドユーザーがリソースやアプリケーションにアクセスすることだけではありません。ゼロトラストの原則は、ワークロード内および

ワークロード間にも実装する必要があります。同じ技術原則 (強固なアイデンティティ、マイクロセグメンテーション、認可) をデータセンター内でも利用できるすべてのコンテキストを活用して適用します。

- 多層防御の提供 — 複数層のセキュリティ制御を使用して、多層防御戦略を実装します。多要素認証 (MFA)、ネットワークセグメンテーション、暗号化、異常検出などのさまざまなセキュリティテクノロジーを組み合わせて、包括的な保護を提供します。各レイヤーが他のレイヤーを補完して、強力な防御システムを構築するようにしてください。
- 強力な認証を要求 — すべてのリソースにアクセスするすべてのユーザーに、MFA などの強力な認証メカニズムを適用します。理想的には、ゼロトラストに高レベルの認証を保証し、幅広いセキュリティ上の利点 (フィッシングからの保護など) をもたらす FIDO2 ハードウェアベースのセキュリティキーなどの最新の MFA を検討してください。
- 認可を一元化して改善する – すべてのアクセス試行を具体的に認可します。プロトコルの仕様によっては、接続ごとまたはリクエストごとに行う必要があります。リクエストごとが理想的です。ID、デバイス、動作、ネットワーク情報など、利用可能なすべてのコンテキストを使用して、より詳細で適応性の高い高度な承認決定を行います。
- 最小特権の原則を使用 — 最小特権の原則を実装して、職務遂行に必要な最低限のアクセス権をユーザーに付与します。職務上の役割、責任、ビジネスニーズに基づいて、アクセス許可を定期的に見直し、更新します。ジャストインタイムのアクセスプロビジョニングを実装します。
- 特権アクセス管理の使用 — 特権アクセス管理 (PAM) ソリューションを実装して、特権アカウントを保護し、重要なシステムへの不正アクセスのリスクを軽減します。PAM ソリューションには、特権アクセス制御、セッション記録、監査機能が備わっているため、組織が最も機密性の高いデータやシステムを保護しやすくなります。
- マイクロセグメンテーションの使用 — ネットワークをより小さく、より分離されたセグメントに分割します。マイクロセグメンテーションを使用して、ユーザーの役割、アプリケーション、またはデータの機密性に基づいて、セグメント間の厳格なアクセス制御を適用します。不要なネットワーク経路、特にデータにつながる経路をすべて排除するよう努めてください。
- セキュリティアラートのモニタリングと対応 — 包括的なセキュリティモニタリングとインシデント対応プログラムをクラウド環境に実装します。クラウドネイティブなセキュリティツールとサービスを使用して、脅威をリアルタイムで検出し、ログを分析し、インシデント対応を自動化します。明確なインシデント対応手順を確立し、定期的なセキュリティ評価を実施し、異常や疑わしいアクティビティを継続的にモニタリングします。
- 継続的なモニタリングの利用 — セキュリティインシデントを迅速かつ効果的に検出して対応するために、継続的なモニタンリングを実施します。高度なセキュリティ分析ツールを使用して、ユーザーの行動、ネットワークトラフィック、システムアクティビティをモニタリングします。アラートと通知を自動化して、インシデントにタイムリーに対応できるようにします。

- セキュリティとコンプライアンスの文化の促進 — セキュリティとコンプライアンスの文化を組織全体に浸透させます。セキュリティのベストプラクティス、ゼロトラストの原則を順守することの重要性、安全なクラウド環境を維持する上での従業員の役割について、従業員を教育します。定期的にセキュリティ意識向上トレーニングを実施して、従業員がソーシャルエンジニアリングに警戒し、データ保護とプライバシーに関する責任を理解するようにします。
- ソーシャルエンジニアリングシミュレーションの使用 — ソーシャルエンジニアリングシミュレーションを実施して、ソーシャルエンジニアリング攻撃に対するユーザーの感受性を評価します。シミュレーションの結果を使用して、トレーニングプログラムをユーザーの意識を高め、潜在的な脅威への対応を向上させるように調整します。
- 継続的な教育の促進 — 継続的なセキュリティトレーニングとリソースを提供することで、継続的な教育と学習の文化を確立します。進化し続けるセキュリティのベストプラクティスの情報をユーザーに提供し続けましょう。常に警戒を怠らず、疑わしいアクティビティがあれば速やかに報告するようユーザーに促してください。
- 継続的な評価と最適化 — クラウド環境の改善点を定期的に評価します。クラウドネイティブのツールを使用してリソースの使用状況とパフォーマンスをモニタリングし、脆弱性評価とペネトレーションテストを実施して弱点を特定して対処します。
- ガバナンスとコンプライアンスのフレームワークの確立 — 組織が業界標準や規制要件に準拠していることを確認するのに役立つガバナンスとコンプライアンスのフレームワークを策定します。このフレームワークでは、データやシステムを不正なアクセス、使用、開示、中断、変更、破壊から保護するためのポリシー、手順、統制を定義します。コンプライアンス指標の追跡と報告、定期的な監査の実施、コンプライアンス違反の問題への迅速な対処のためのメカニズムを実装します。
- コラボレーションと知識共有の奨励 — ZTA の採用に関わるチーム間のコラボレーションと知識共有を奨励します。これは、IT 部門、セキュリティ部門、事業部門の部門間のコミュニケーションとコラボレーションを促進することで実現できます。また、組織はフォーラム、ワークショップ、知識共有セッションを開設して、理解を促進し、課題に取り組み、導入プロセスを通じて学んだ教訓を共有することもできます。

重要なポイント

このガイドでは、ゼロトラストアーキテクチャ (ZTA) 戦略を成功させるための重要な側面について説明しました。このセクションでは、提示された規範的ガイダンスから得られた重要なポイントをまとめています。

- ゼロトラストの原則を理解する — ゼロトラストは、従来のネットワーク制御やネットワーク境界だけに依存しない、またはそれに根本的に依存しない、デジタル資産に関するセキュリティ制御を提供することに焦点を当てた概念モデルおよび、関連する一連のメカニズムです。代わりに、ID、デバイス、動作、その他の豊富なコンテキストやシグナルをネットワーク制御に追加して、よりきめ細かく、インテリジェントで、適応性が高く、継続的なアクセスに関する意思決定を行います。最小特権、マイクロセグメンテーション、継続的認証、適応型認可など、ゼロトラストの基本原則をよく理解しておいてください。
- 明確な目標の定義 — ZTA 導入の目標と期待されるビジネス成果を明確に定義します。これらの目標をゼロトラストの原則と一致させて、強固なセキュリティ基盤を確保すると同時に、ビジネスの成長と革新を可能にします。
- 包括的な評価の実施 — 既存の IT インフラストラクチャ、アプリケーション、データ資産を徹底的に評価します。依存関係、技術的負債、互換性の問題を特定して、導入戦略の参考にしてください。
- ZTA 導入計画の作成 — ワークロード、アプリケーション、データをクラウドに移行するための段階的なアプローチの概要を示す詳細な計画を作成します。コンプライアンス要件やアプリケーションのモダナイズなどの要素を検討してください。
- 強固な ZTA の実装 — きめ細かなアクセス制御、強力な認証メカニズム、継続的なモニタリングを実施する ZTA を設計して実装します。ZTA をより効率的に導入するには、 AWS Verified Access や Amazon VPC Lattice などのクラウドネイティブなゼロトラストサービスを使用します。
- データとアプリケーションのセキュリティを優先する — ゼロトラストの原則 (強固なアイデンティティ、マイクロセグメンテーション、認可) を適用して、利用可能なすべてのコンテキストを提供します。このコンテキストは、システムやリソースにアクセスするユーザーや、バックエンドコンポーネント内およびバックエンドコンポーネント間の通信とデータの流れに使用してください。
- モニタリングとインシデント対応のフレームワークの確立 — 強固なセキュリティモニタリングとインシデント対応機能をクラウド環境に実装します。クラウドネイティブのセキュリティツールを使用して、Amazon Inspector、、Amazon Amazon GuardDuty などのリアルタイムの脅威検出、ログ分析 AWS Security Hub、インシデント対応の自動化を行います。

- セキュリティとコンプライアンスの文化を育む — セキュリティ意識とコンプライアンスの文化を組織全体に浸透させます。セキュリティのベストプラクティスおよび、安全なクラウド環境を維持する上での従業員の役割について従業員を教育します。
- 継続的な評価と最適化 — クラウド環境、セキュリティコントロール、運用プロセスを定期的に評価します。インサイトを収集し、リソースの使用状況、コスト管理、パフォーマンスを最適化するには、Amazon CloudWatch や AWS Security Hubなどのクラウドネイティブな分析およびモニタリングツールを使用してください。
- ガバナンスとコンプライアンスのフレームワークの確立 — 組織が業界標準や規制要件に準拠した、ガバナンスとコンプライアンスのフレームワークを策定します。ポリシー、手順、統制を定義して、セキュリティ、プライバシー、コンプライアンス基準を確実に順守できるようにします。

次のステップ

ゼロトラストアーキテクチャ (ZTA) の導入は、組織の態勢を改善しリスクを軽減する最も安全な方法の 1 つです。この規範的なガイダンスは、原則の理解から準備状況の評価、必要なコンポーネントの実装に至るまで、ゼロトラストを導入するための包括的なロードマップを提供しています。

このワークストリームまたはドメインにおける次のステップでは、次のことを扱います。

- 採用計画実施
- ZTA の実装
- 定期的なセキュリティ評価の実施
- クラウド環境とセキュリティ制御の継続的な最適化

ZTA は継続的なプロセスであり、強固なセキュリティ基盤を確保するための継続的なモニタリング、評価、導入を必要とします。このガイダンスに記載されているベストプラクティスに従うことで、組織はセキュリティ体制を強化し、規制を確実に順守し、機密データを保護することができます。

よくある質問

このセクションでは、ゼロトラストアーキテクチャ (ZTA) の設計と実装に関するよくある質問に対して回答します。

ゼロトラストとは?

ゼロトラストは、従来のネットワーク制御やネットワーク境界だけに依存しない、またはそれに根本的に依存しない、デジタル資産に関するセキュリティ制御を提供することに焦点を当てた概念モデルおよび、関連する一連のメカニズムです。代わりに、ID、デバイス、動作、その他の豊富なコンテキストやシグナルをネットワーク制御に追加して、よりきめ細かく、インテリジェントで、適応性が高く、継続的なアクセスに関する意思決定を行います。

ゼロトラストアーキテクチャの実装には何が AWS のサービス 役立ちますか？

AWS は AWS Verified Access、ゼロトラストの実装に役立ついくつかのサービスを提供します。例えば、 AWS Identity and Access Management (IAM)、Amazon Virtual Private Cloud (Amazon VPC)、Amazon VPC Lattice、Amazon Verified Permissions、Amazon API Gateway、Amazon GuardDuty などです。

AWSでデータのセキュリティを確保するにはどうすればよいですか?

AWS は、保管中および転送中のデータ暗号化用の AWS Key Management Service （ AWS KMS ）、ネットワーク分離用の Amazon Virtual Private Cloud (Amazon VPC)、認証情報の安全な保存と取得 AWS Secrets Manager 用の などのサービスを提供します。

ゼロトラスト環境でコンプライアンス要件 AWS に対応できますか？

はい。さまざまな規制要件を満たすためのコンプライアンスプログラムとサービス AWS があります。 は AWS コンプライアンスレポートへのアクセス AWS Artifact を提供し、 AWS Config コンプライアンスの継続的なモニタリングと評価をサポートします。

ゼロトラスト環境でセキュリティを自動化するための AWS ツールやサービスはありますか？

AWS は AWS Security Hub、セキュリティ検出結果を一元化および自動化する や、セキュリティポリシーを定義および適用するための AWS Config ルールなどのサービスを提供します。

を使用してゼロトラストクラウド環境で継続的なモニタリングとインシデント対応を確保するには AWS

AWS は、Amazon CloudWatch などのサービスをリアルタイムモニタリングや口グ記録、分析 AWS CloudTrail のために提供しています。インシデント対応のベストプラクティスについては、「 AWS セキュリティインシデントレスポンスガイド」をご利用ください。

リソース

リファレンス

- Cloud Center of Excellence とは何か、なぜ組織は Cloud Center of Excellence を作成すべきなのか？ — このブログ記事では、CCoE の概要、効果的な CCoE を構築するためのベストプラクティスなどについて説明しています。
- でのゼロトラスト AWS – このページでは、ゼロトラストのセキュリティ原則と AWS 環境のベストプラクティスの概要を説明します。
- ゼロトラストアーキテクチャ: AWS パースペクティブ – このブログ記事では、ゼロトラストの実装方法の定義と指針を共有しています AWS。
- AWS Identity and Access Management (IAM) ユーザーガイド – このガイドでは、ゼロトラストアーキテクチャの重要なコンポーネントである IAM でのユーザーアクセスとアクセス許可の管理に関する包括的なドキュメントを提供します。
- AWS Security Hub – Security Hub について説明します。Security Hub は、 全体のセキュリティアラートとコンプライアンスステータスを包括的に把握できるサービスです AWS アカウント。
- AWS Well-Architected フレームワーク – AWS上の安全性、高パフォーマンス、耐障害性、効率性に優れたアーキテクチャの構築に関するガイダンスとなる、Well-Architected フレームワークについて掘り下げます。
- AWS セキュリティインシデント対応ガイド – このガイドでは、組織の AWS クラウド 環境内のセキュリティインシデントへの対応の基礎の概要を説明します。クラウドセキュリティとインシデント対応の概念の概要を示し、セキュリティ問題に対応する顧客が利用できるクラウドの機能、サービス、メカニズムを特定します。

ツール

- Amazon API Gateway
- AWS Artifact
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon GuardDuty

- AWS Identity and Access Management
- AWS Key Management Service
- AWS Secrets Manager
- AWS Security Hub
- AWS Verified Access

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
追加された更新内容	「ゼロトラストアーキテクチャの主要コンポーネント」セクションへの情報の追加、「ゼロトラスト導入に向けた組織の準備状況の評価」セクションの変更、「ベストプラクティス」セクションへの情報の追加、FAQ の変更を行いました。	2023 年 12 月 4 日
初版発行	—	2023 年 6 月 19 日

AWS 規範的ガイダンスの用語集

以下は、 AWS 規範的ガイダンスが提供する戦略、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します。
- 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: でオンプレミスの Oracle データベースを Oracle 用 Amazon Relational Database Service (Amazon RDS) に移行します AWS クラウド。
- 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 に移行します。
- 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: オンプレミスの Oracle データベースを の EC2 インスタンス上の Oracle に移行します AWS クラウド。
- 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。サーバーを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。
- 使用停止 — お客様のソース環境で不要になったアプリケーションを停止または削除します。

A

ABAC

「属性ベースのアクセスコントロール」を参照してください。

抽象化されたサービス

「 マネージドサービス」を参照してください。

ACID

不可分性、一貫性、分離性、耐久性を参照してください。

アクティブ - アクティブ移行

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

アクティブ - パッシブ移行

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

集計関数

行のグループに対して動作し、グループの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 などがありますMAX。

AI

「人工知能」を参照してください。

AIOps

「人工知能オペレーション」を参照してください。

匿名化

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

アンチパターン

繰り返し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。

アプリケーションコントロール

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

アプリケーションポートフォリオ

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

人工知能 (AI)

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

AI オペレーション (AIOps)

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

非対称暗号化

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

原子性、一貫性、分離性、耐久性 (ACID)

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

属性ベースのアクセス制御 (ABAC)

部署、役職、チーム名など、ユーザーの属性に基づいてアクセス許可をきめ細かく設定する方法。詳細については、 AWS Identity and Access Management (IAM) ドキュメントの「 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

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)

組織がクラウドに正常に移行するための効率的で効果的な計画を立て AWS るのに役立つ、 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編成します。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、組織がクラウド導入を成功させるための準備に役立つ、人材開発、トレーニング、コミュニケーションのための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、作業の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」を参照してください。

動作グラフ

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

ビッグエンディアンシステム

最上位バイトを最初に格納するシステム。エンディアンネスも参照してください。

二項分類

バイナリ結果 (2 つの可能なクラスのうちの 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

2 つの異なる同一の環境を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は 1 つの環境 (青) で実行し、新しいアプリケーションバージョンは別の環境 (緑) で実行します。この戦略は、影響を最小限に抑えながら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インタラクション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、個人や組織に混乱を与えたり、損害を与えたりすることを意図しているものがあります。

ボットネット

マルウェアに感染し、ボットのヘルダーまたはボットオペレーターとして知られる、単一の当事者によって管理されているボットのネットワーク。ボットは、ボットとその影響をスケールするための最もよく知られているメカニズムです。

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、通常はアクセス許可 AWS アカウント を持たない にユーザーがすばやくアクセスできるようにします。詳細については、 Well-Architected ガイダンスの AWS ブレークグラスプロシージャ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、ホワイトペーパー AWSでのコンテナ化されたマイクロサービスの実行 の ビジネス機能を中心に組織化 セクションを参照してください。

ビジネス継続性計画 (BCP)

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

C

CAF

AWS 「クラウド導入フレームワーク」を参照してください。

Canary デプロイ

エンドユーザーへのバージョンのスローリリースと増分リリース。確信できたら、新しいバージョンをデプロイし、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します。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 を受信する前に、ローカルでデータを暗号化します。

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テクノロジー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 に移行するときに通常実行する 4 つのフェーズ AWS クラウド :

- 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 によって定義されています。移行戦略とどのように関連しているかについては、 AWS「移行準備ガイド」を参照してください。

CMDB

「設定管理データベース」を参照してください。

コードリポジトリ

ソースコードやその他の資産 (ドキュメント、サンプル、スクリプトなど) が保存され、バージョン管理プロセスを通じて更新される場所。一般的なクラウドリポジトリには、 GitHubまたは が含まれますBitbucket Cloud。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などのビジュアル形式から情報を分析および抽出する AI の分野。例えば、 はオンプレミスのカメラネットワークに CV を追加するデバイス AWS Panorama を提供し、Amazon SageMaker AI は CV のイメージ処理アルゴリズムを提供します。

設定ドリフト

ワークロードの場合、設定は想定状態から変化します。これにより、ワークロードが非準拠になる可能性があり、通常は段階的で意図的ではありません。

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 リージョンで、または組織全体で 1 つのエンティティとしてデプロイできます。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

一元化された管理とガバナンスにより、分散された分散型のデータ所有権を提供す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していることを確認できます。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通常、大量の履歴データが含まれており、クエリや分析によく使用されます。

データベース定義言語 (DDL)

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

データベース操作言語 (DML)

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

DDL

「データベース定義言語」を参照してください。

ディープアンサンブル

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

ディープラーニング

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

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、 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て、リソースの安全性を確保します。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。

デプロイ

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

開発環境

???「環境」を参照してください。

検出管理

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

開発バリューストリームマッピング (DVSM)

ソフトウェア開発ライフサイクルのスピードと品質に悪影響を及ぼす制約を特定し、優先順位を付けるために使用されるプロセス。DVSM は、もともとリーンマニ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

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

ディザスタ

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

ディザスタリカバリ (DR)

災害によるダウンタイムとデータ損失を最小限に抑えるための戦略とプロセス。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。例えば、 AWS CloudFormation を使用してシステムリソースのドリフトを検出したり、 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

「開発値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、応答時間を短縮できます。

電子データ交換 (EDI)

組織間の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プロセス。

暗号化キー

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

エンディアン

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

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

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

フェイルファスト

開発ライフサイクルを短縮するために頻繁かつ段階的なテストを使用する哲学。これはアジャイルアプローチの重要な部分です。

障害分離の境界

では AWS クラウド、障害の影響を制限し、ワークロードの耐障害性を向上させるアベイラビリティーゾーン 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です。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 に同様のタスクの実行を求める前に、タスクと必要な出力を示す少数の例を提供します。この手法は、プロンプトに埋め込まれた例 (ショット) からモデルが学習するコンテキスト内学習の

アプリケーションです。少数ショットプロンプトは、特定のフォーマット、推論、またはドメイン知識を必要とする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コントロール」を参照してください。

きめ細かなアクセス制御 (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

フラッシュカット移行

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

FM

「基盤モデル」を参照してください。

基盤モデル (FM)

一般化およびラベル付けされていないデータの大規模なデータセットでトレーニングされている大規模な深層学習ニューラルネットワーク。FMsは、言語の理解、テキストと画像の生成、自然言語での会話など、さまざまな一般的なタスクを実行できます。詳細については、「基盤モデルとは」を参照してください。

G

生成 AI

大量のデータでトレーニングされ、シンプルなテキストプロンプトを使用してイメージ、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る AI モデルのサブセット。詳細については、「生成 AI とは」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 ワークフローはレガシーと見なされ、トランクベースのワークフローはモダンで推奨されるアプローチです。

ゴールデンイメージ

システムまたはソフトウェアの新しいインスタンスをデプロイするためのテンプレートとして使用されるシステムまたはソフトウェアのスナップショット。例えば、製造では、ゴールデンイメージを使用して複数のデバイスにソフトウェアをプロビジョニングし、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、、Amazon GuardDuty AWS Security Hub、、 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。

ハイアベイラビリティ (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に使用されるデータセットから保留される、ラベル付きの履歴データの一部。ホールドアウトデータを使用してモデル予測をホールドアウトデータと比較することで、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

「産業モノのインターネット」を参照してください。

イミュータブルインフラストラクチャ

既存のインフラストラクチャを更新、パッチ適用、または変更するのではなく、本番ワークロード用の新しいインフラストラクチャをデプロイするモデル。イミュータブルインフラストラクチャは、本質的に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、予測性が高くなります。詳細については、 AWS 「 Well-Architected フレームワーク」の「イミュータブルインフラストラクチャを使用したデプロイ」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 によって導入された用語で、接続性、リアルタイムデータ、自動化、分析、AI/ML の進歩によるビジネスプロセスのモダナイゼーションを指します。

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。

産業分野における IoT (IIoT)

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

インスペクション VPC

AWS マルチアカウントアーキテクチャでは、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

「モノのインターネット」を参照してください。

IT 情報ライブラリ (ITIL)

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

IT サービス管理 (ITSM)

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

ITIL

「IT 情報ライブラリ」を参照してください。

ITSM

「IT サービス管理」を参照してください。

L

ラベルベースアクセス制御 (LBAC)

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

ランディングゾーン

ランディングゾーンは、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)

大量のデータに基づいて事前トレーニングされた深層学習 AI モデル。LLM は、質問への回答、ドキュメントの要約、テキストの他の言語への翻訳、文の完了など、複数のタスクを実行できます。詳細については、LLMs」を参照してください。

大規模な移行

300 台以上のサーバの移行。

LBAC

「ラベルベースのアクセスコントロール」を参照してください。

最小特権

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

リフトアンドシフト

「7 Rs」を参照してください。

リトルエンディアンシステム

最下位バイトを最初に格納するシステム。エンディアンネスも参照してください。

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またはプライバシーを侵害するように設計されているソフトウェア。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、不正アクセスにつながる可能性があります。マルウェアの例としては、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 がインフラストラクチャレイヤー、オペレーティングシステム、プラットフォームを AWS 運用し、ユーザーがエンドポイントにアクセスしてデータを保存および取得します。Amazon Simple Storage Service (Amazon S3) と Amazon DynamoDB は、 マネージドサービスの例です。これらは抽象化されたサービスとも呼ばれます。

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、制御するためのソフトウェアシステム。このシステムは、加工品目を工場の完成製品に変換します。

MAP

「移行促進プログラム」を参照してください。

メカニズム

ツールを作成し、ツールの導入を推進し、調整を行うために結果を検査する完全なプロセス。メカニズムは、動作中にそれ自体を強化および改善するサイクルです。詳細については、 AWS 「 Well-Architected フレームワーク」の「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。

メッセージキューイングテレメトリトランスポート (MQTT)

リソースに制約のある IoT デバイス用の、パブリッシュ/サブスクライブパターンに基づく軽量 machine-to-machine (M2M) 通信プロトコル。

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)

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 プログラムは、組織がクラウドへの移行のための強固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ちます。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には、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)

に移行するためのビジネスケースを検証するための情報を提供するオンラインツール AWS クラウド。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 に移行するために使用されるアプローチ AWS クラウド。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、「」の「アプリケーションをモダナイズするための戦略 AWS クラウド」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、『』の「アプリケーションのモダナイゼーション準備状況の評価 AWS クラウド」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

「移行ポートフォリオ評価」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。

ミュータブルインフラストラクチャ

本番ワークロードの既存のインフラストラクチャを更新および変更するモデル。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

「オリジンアクセスコントロール」を参照してください。

OAI

「オリジンアクセスアイデンティティ」を参照してください。

OCM

「組織変更管理」を参照してください。

オフライン移行

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

OI

「 オペレーションの統合」を参照してください。

OLA

「運用レベルの契約」を参照してください。

オンライン移行

ソースワークロードをオフラインにせず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。

オープンプロセス通信 - 統合アーキテクチャ (OPC-UA)

産業オートメーション用のmachine-to-machine (M2M) 通信プロトコル。OPC-UA は、データの暗号化、認証、認可スキームを備えた相互運用性標準を提供します。

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)

インシデントや潜在的な障害の理解、評価、防止、または範囲の縮小に役立つ質問のチェックリストと関連するベストプラクティス。詳細については、 AWS Well-Architected フレームワークの「運用準備状況レビュー (ORR)」を参照してください。

運用テクノロジー (OT)

物理環境と連携して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ハードウェアおよびソフトウェアシステム。製造では、OT と情報技術 (IT) システムの統合が、Industry 4.0 トランスフォーメーションの重要な焦点です。

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から、このフレームワークは人材の加速と呼ばれます。詳細については、OCM ガイド を参照してください。

オリジンアクセスコントロール (OAC)

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コントロールが可能です。

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

「プログラム可能な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

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

多言語の永続性

データアクセスパターンやその他の要件に基づいて、マイクロサービスのデータストレージテクノロジーを個別に選択します。マイクロサービスが同じデータストレージテクノロジーを使用している場合、実装上の問題が発生したり、パフォーマンスが低下する可能性があります。マイクロサービスは、要件に最も適合したデータストアを使用すると、より簡単に実装でき、パフォーマンスとスケーラビリティが向上します。詳細については、マイクロサービスでのデータ永続性の有効化 を参照してください。

ポートフォリオ評価

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

述語

`true` または を返すクエリ条件。一般的に `false`WHERE句にあります。

述語プッシュダウン

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

予防的コントロール

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

プリンシパル

アクションを実行し 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内にあるプリンシパルを参照してください。

プライバシーバイデザイン

開発プロセス全体を通じてプライバシーを考慮するシステムエンジニアリングアプローチ。

プライベートホストゾーン

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

プロアクティブコントロール

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

設計、開発、発売から成長と成熟まで、ライフサイクル全体を通じて製品のデータとプロセスを管理し、辞退と削除を行います。

本番環境

???「環境」を参照してください。

プログラム可能なロジックコントローラー ("")

製造では、マシンをモニタリングし、承認プロセスを自動化する、信頼性が高く、適応性の高いコンピュータです。

プロンプトの連鎖

1 つの LLM プロンプトの出力を次のプロンプトの入力として使用して、より良いレスポンスを生成します。この手法は、複雑なタスクをサブタスクに分割したり、予備応答を繰り返し改善または拡張したりするために使用されます。これにより、モデルのレスポンスの精度と関連性が向上し、より詳細でパーソナライズされた結果が得られます。

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。

パブリッシュ/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してスケーラビリティと応答性を向上させるパターン。例えば、マイクロサービスベースの MES では、マイクロサービスは他のマイクロサービス

がサブスクライブできるチャネルにイベントメッセージを発行できます。システムは、公開サービスを変更せずに新しいマイクロサービスを追加できます。

Q

クエリプラン

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

クエリプランのリグレッション

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

R

RACI マトリックス

責任、説明責任、相談、通知 (RACI) を参照してください。

RAG

「取得拡張生成」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

責任、説明責任、相談、情報提供 (RACI) を参照してください。

RCAC

「行と列のアクセスコントロール」を参照してください。

リードレプリカ

読み取り専用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。

再設計

「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、AWS リージョン 「アカウントで使用できる を指定する」を参照してください。

回帰

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

リホスト

「7 Rs」を参照してください。

リリース

デプロイプロセスで、変更を本番環境に昇格させること。

再配置

「7 Rs」を参照してください。

プラットフォーム変更

「7 Rs」を参照してください。

再購入

「7 Rs」を参照してください。

回復性

中断に耐えたり、中断から回復したりするアプリケーションの機能。で回復性を計画するときは、高可用性とディザスタリカバリが一般的な考慮事項です AWS クラウド。詳細については、AWS クラウド 「レジリエンス」を参照してください。

リソースベースのポリシー

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

実行責任者、説明責任者、協業先、報告先 (RACI) に基づくマトリックス

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

レスポンシブコントロール

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、Implementing security controls on AWSのResponsive controlsを参照してください。

保持

「7 Rs」を参照してください。

廃止

「7 Rs」を参照してください。

取得拡張生成 (RAG)

LLM がレスポンスを生成する前にトレーニングデータソースの外部にある権威データソースを参照する生成 AI テクノロジー。例えば、RAG モデルは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する場合があります。詳細については、「RAG とは」を参照してください。

ローテーション

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

行と列のアクセス制御 (RCAC)

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

RPO

「目標復旧時点」を参照してください。

RTO

目標復旧時間を参照してください。

ランブック

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

S

SAML 2.0

多くの ID プロバイダー (IdP) が使用しているオープンスタンダード。この機能により、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 にログイン AWS Management Console したり AWS 、 API オペレーションを呼び出したりできます。組織内のすべてのユーザーに対して IAM でユーザーを作成する必要はありません。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

「監視コントロールとデータ取得」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パスワードやユーザー認証情報などの AWS Secrets Manager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。シークレット値は、バイナリ、単一の文字列、または複数の文字列にすることができます。詳細については、Secrets Manager ドキュメントの「Secrets Manager シークレットの内容」を参照してください。

設計によるセキュリティ

開発プロセス全体でセキュリティを考慮するシステムエンジニアリングアプローチ。

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、予防的、検出的、応答的、プロアクティブの 4 つの主なタイプがあります。

セキュリティ強化

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

Security Information and Event Management (SIEM) システム

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

セキュリティレスポンスの自動化

セキュリティイベントに自動的に応答または修正するように設計された、事前定義されたプログラムされたアクション。これらのオートメーションは、セキュリティのベストプラクティス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としては、VPC セキュリティグループの変更、Amazon EC2 インスタンスへのパッチ適用、認証情報のローテーションなどがあります。

サーバー側の暗号化

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、スループットなど、サービスのパフォーマンス側面の測定。

サービスレベル目標 (SLO)

サービスレベルのインジケータで測定される、サービスの正常性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、お客様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

セキュリティ情報とイベント管理システムを参照してください。

単一障害点 (SPOF)

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

SLA

「サービスレベルアグリーメント」を参照してください。

SLI

「サービスレベルインジケータ」を参照してください。

SLO

「サービスレベルの目標」を参照してください。

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、『』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 AWS クラウド」を参照してください。

SPOF

単一障害点を参照してください。

star スキーマ

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

監視コントロールとデータ収集 (SCADA)

製造では、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稼働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潜在的な問題を検出したり、パフォーマンスをモニタリングしたりする方法でシステムをテストします。Amazon CloudWatch Synthetics を使用してこれらのテストを作成できます。

システムプロンプト

LLM にコンテキスト、指示、またはガイドラインを提供して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、ユーザーとのやり取りのルールを確立するのに役立ちます。

T

tags

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の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「 AWS Organizations を他の AWS のサービスで使用する 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 枚のピザで養う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

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

「書き込み 1 回」、「読み取り多数」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 回書き込み、データの削除や変更を防ぐストレージモデル。許可されたユーザーは、必要な回数だけデータを読み取ることができますが、変更することはできません。このデータストレージインフラストラクチャはイミュータブルと見なされます。

Z

ゼロデイエクスプロイト

ゼロデイ脆弱性を利用する攻撃、通常はマルウェア。

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 にタスクを実行する手順を提供するが、タスクのガイドに役立つ例 (ショット) は提供しない。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。