aws

でのセキュリティコントロールの実装 AWS

AWS 規範ガイダンス

AWS 規範ガイダンス: でのセキュリティコントロールの実装 AWS

Table of Contents

AWS でのセキュリティコントロールの実装

Iqbal Umair、Gurpreet Kaur Cheema、Wasim Hossain、Joseph Nguyen、San Brar、Lucia Vanta (Amazon Web Services (AWS)

2023 年 12 月 (ドキュメント履歴)

セキュリティはあらゆる企業にとってきわめて重要であり、AWS Well-Architected フレームワークの主要な柱の 1 つです。しかし、セキュリティ上の考慮事項に対処する方法や、包括的な、自動化されたセキュリティテストと修復戦略を、自社のクラウド環境に合わせて作成する方法について、理解している人は多くありません。AWS Config、Amazon GuardDuty、AWS CloudFormation といった AWS のサービス とツールを使用すると、セキュリティテスト戦略を作成し、それを自社の AWS クラウド 環境に組み込むことができます。

会社のセキュリティポリシーと基準を満たすため、セキュリティコントロールは、脅威アクターがセキュリティ上の脆弱性を悪用することを阻止、検出、軽減する、技術上または管理上のガードレールとして機能します。これらは、リソースとデータの機密性、完全性、可用性を保護するように設計されています。以下は、セキュリティコントロールの一例です。

- アプリケーションにサインインする必要があるユーザー向けに、多要素認証を実装する。
- アカウントアクティビティをリアルタイムで監査するため、ログ記録、モニタリング、クエリの各アクションを行う。
- 機密データを確実に暗号化する。
- 会社の保持ポリシーに従って確実にログを保存する。

セキュリティコントロールには、予防、プロアクティブ、検出、レスポンシブの 4 種類があります。本ガイドでは、それぞれのタイプについて詳しく説明し、これらのコントロールを AWS クラウド に実装し自動化する方法について重点的に解説します。本ガイドは、継続的かつプロアクティブに、セキュリティコントロールの使用を検討する際の指針となります。

対象者

本ガイドの対象読者は、AWS クラウド にセキュリティコントロールを実装する作業を担当している、アーキテクトやセキュリティエンジニアです。ガバナンスフレームワークにおけるセキュリティコントロール で規定しているセキュリティポリシー、コントロール対象、コントロール基準を自社で策定していない場合は、これらのガバナンスタスクを完了してから本ガイドの内容に進むことが推奨されます。

目標とするビジネス成果

企業は、自社のITシステムのリスクを軽減するため、またはリスクへの対抗手段として利用するために、セキュリティコントロールを使用します。セキュリティコントロールは、IT プログラムとそのセキュリティ戦略の主要なセキュリティ目標を満たすための、要件の基準線を規定します。セキュリティコントロールを実装すると、データや IT 資産の機密性、一貫性、可用性が保護され、企業のセキュリティ体制は向上します。コントロールが実装されていなければ、セキュリティの基準線を設定する際にどこに専念し労力を投じればよいかを判断することが難しくなります。

セキュリティコントロールを使用すれば、さまざまなシナリオに対処できます。例えば、リスク評価から生じる要件への適合、業界標準の達成、規制への準拠などです。セキュリティコントロールの要件が満たされているということは、システムのリスクが評価され、必要とされる保護レベルが判定され、ソリューションが事前対処的に実装されていることを意味します。ビジネス、業界、地域など、その他の要因はすべて、必要なセキュリティコントロールを決める判断材料になり得ます。

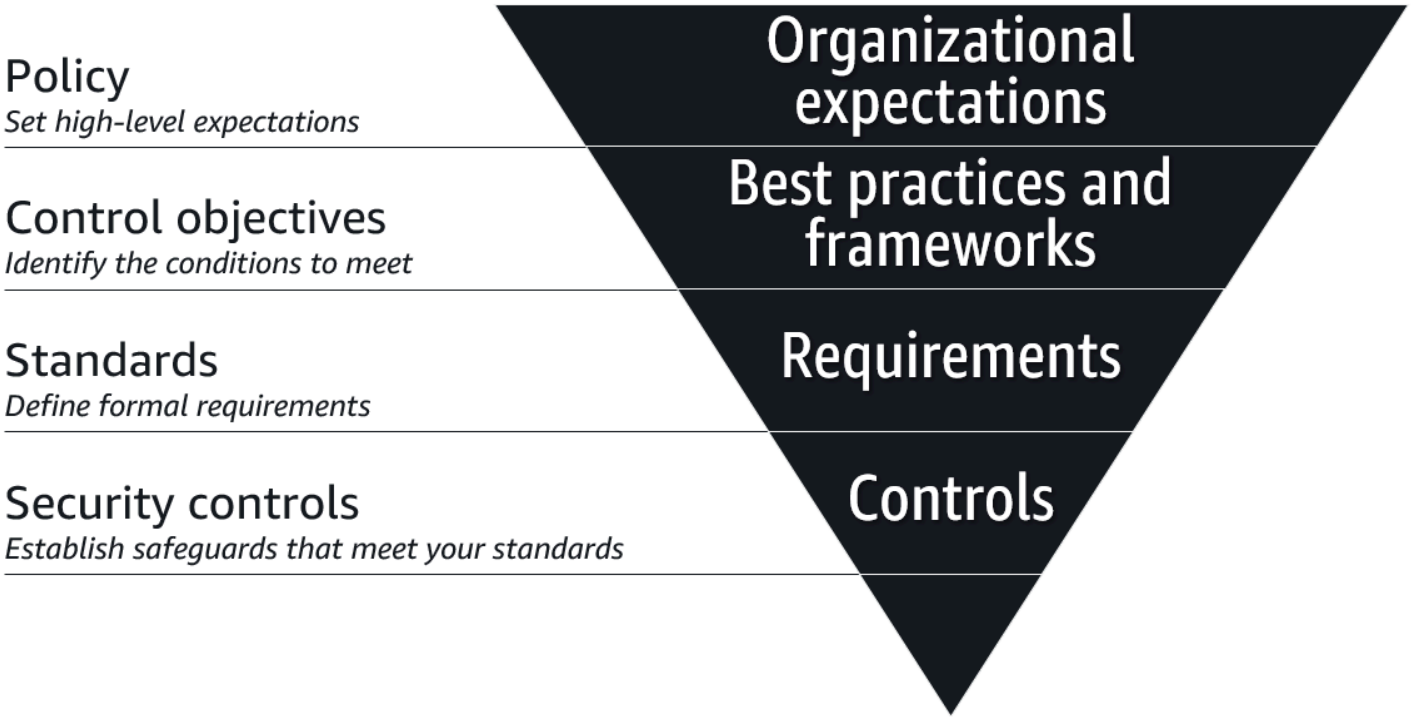
セキュリティコントロールの実装を必要とする一般的なユースケースは次のとおりです。

- アプリケーションのセキュリティ評価により、処理中のデータの機密性に基づき、アクセス制御の必要性が確認された場合。
- Payment Card Industry Data Security Standard (PCI DSS)、HIPAA (Health Insurance Portability and Accountability Act)、アメリカ国立標準技術研究所 (NIST) などのセキュリティ基準を順守しなければならない場合。
- ビジネス取引の機密情報を保護する必要がある場合。
- 一般データ保護規則 (GDPR) の順守が義務付けられている地域など、セキュリティコントロールを必要とする地域に会社の事業を拡大した場合。

本ガイドを読むことで、4 種類のセキュリティコントロールについて理解し、それらがセキュリティガバナンスのフレームワークにどのように含まれているかを理解することができます。また、AWS クラウド でセキュリティコントロールの実装と自動化を開始する準備が整います。

ガバナンスフレームワークにおけるセキュリティコントロール

基礎的なレベルから計画を立てることが重要です。どのように始めればよいのでしょうか? 次の図は、ポリシー、統制目標、標準、セキュリティコントロールに基づいてセキュリティガバナンス戦略を構築する方法を示しています。



セキュリティガバナンス戦略の階層を構成する要素は次のとおりです。

- ポリシー — ポリシーは、あらゆるサイバーセキュリティガバナンス戦略の基盤です。法定、規制、契約上の義務など、会社が果たすべき目標事項を記載した文書です。ポリシーは、業界や地域によって異なる場合があります。
- 統制目標 — 統制目標は、ポリシーの意図を満たすのに役立つ、業界で認められたベストプラクティスなどの目標です。クラウドコンピューティングについては、多くの企業がクラウドコントロールマトリックス (CCM) (クラウドセキュリティアライアンスのウェブサイト) を採用しています。これはサイバーセキュリティ統制目標のフレームワークです。
- 標準 — 標準は、統制目標を満たす正式に定められた要件です。標準にはプロセス、アクション、構成が含まれる場合があり、標準に照らしてパフォーマンスを測定できるように量で表すことができます。

- セキュリティコントロール — セキュリティコントロールは、標準を実装するために導入する技術的または管理的なメカニズムです。すべてのセキュリティコントロールが標準に対応していますが、すべての標準がセキュリティコントロールに対応しているわけではありません。セキュリティコントロールのテストは、定義された基準を効果的に満たしているかどうかを監視および測定することを目的としています。

このガイドでは、AWS クラウド に一般的なセキュリティコントロールを設計して実装する方法に焦点を当てています。

セキュリティコントロールのタイプ

セキュリティコントロールには主に 4 つのタイプがあります。

- 予防的コントロール — イベントの発生を予防するように設計されたコントロールです。
- プロアクティブコントロール — 規制に準拠していないリソースが作成されるのを防止するように設計されたコントロールです。
- 検出的コントロール - 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コントロールです。
- レスポンシブコントロール - 有害事象や、セキュリティ上の基準線からの逸脱の、修復を早めるように設計されたコントロールです。

効果的なセキュリティ戦略には、これら 4 つのタイプのセキュリティコントロールがすべて含まれています。予防的コントロールは第一の防御手段であり、ネットワークへの不正アクセスや好ましくない変更を予防します。検出的コントロールと応答的コントロールは、イベントが発生したときにこれを把握し、ただちに適切な措置を講じて修復できるようにするため、あらかじめ設定しておくことが重要になります。プロアクティブなコントロールを使用することで、一般的により厳格となる予防的コントロールが補完され、セキュリティが強化されます。

以下のセクションでは、各コントロールについてさらに詳しく説明します。各コントロールタイプの目的、実装のプロセス、ユースケース、技術的な考慮事項、目標とする成果について解説します。

予防的コントロール

予防的コントロールは、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です。このガードレールは、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、第一の防御手段です。予防的コントロールの例としては、許可されていないユーザーからの意図しない書き込みアクションを防ぐのに役立つ読み取り専用アクセス権を持つ AWS Identity and Access Management (IAM) ロールがあります。

このタイプのコントロールについては、以下の点を確認してください。

- 目的
- プロセス
- ユースケース

- テクノロジー
- ビジネス上の成果

目的

予防的コントロールの主な目的は、脅威イベントが発生する可能性をできる限り抑える、また回避することにあります。このコントロールは、システムへの不正アクセスを防ぎ、意図しない変更がシステムに影響を及ぼすことを防ぐのに役立ちます。予防的コントロールの目的は次のとおりです。

- 職務分離 — 予防的コントロールを使用すると、権限を制限する論理的境界を設定して、指定したアカウントまたは環境で特定のタスクのみを実行するように、アクセスを許可することができます。その例を以下に示します。
  - ワークロードを、特定のサービスの異なるアカウントに分割する。
  - アカウントを、本番環境、開発環境、テスト環境にそれぞれ分離する。
  - IAM ロールや引き受けられたロールを使って、特定のアクションを実行するための特定のジョブ機能のみを許可するといったように、特定の機能の実行に必要なアクセス権限と責任を複数のエンティティに委任する。
- アクセスの制御 — 予防的コントロールを使うと、環境内のリソースやデータへのアクセスを、一貫性をもって許可または拒否することができます。その例を以下に示します。
  - ユーザーが、意図されたアクセス許可を越えること (権限昇格) がないようにする。
  - アプリケーションとデータへのアクセスを、承認されたユーザーとサービスのみに制限する。
  - 管理者グループの規模を小さく抑える
  - ルートユーザーの認証情報の使用を避ける
- 実行 — 予防的コントロールを使うと、企業に自社のポリシー、ガイドライン、基準を順守させることができます。その例を以下に示します。
  - セキュリティ上の必要最低限の基準線として機能する設定を固定する。
  - 多要素認証など、追加のセキュリティ対策を実装する。
  - 未承認のロールによって実行される非標準のタスクやアクションを回避する。

プロセス

予防的コントロールのマッピングとは、各コントロールを要件に対応付け、ポリシーを使って、制限、無効化、ブロックによってこれらのコントロールを実装するプロセスのことです。コントロールをマッピングするときは、それらが環境、リソース、ユーザーに対してどのような予防的効果をもた

らすことができるかを検討します。コントロールのマッピングのベストプラクティスは、次のとおりです。

- 特定のアクティビティを禁止する厳格なコントロールは、アクションに検証、承認、変更のプロセスが必要になる本番環境にマッピングする。
- 開発環境や規制された環境では、構築とテストの俊敏性を維持するために予防的コントロールの数が少なくなる場合がある。
- データの区分、アセットのリスクレベル、リスク管理ポリシーは、予防的コントロールに影響を与える。
- 標準や規制に準拠している証拠として、既存のフレームワークにマッピングする。
- 予防的コントロールは、地理的な位置、環境、アカウント、ネットワーク、ユーザー、ロール、リソースごとに実装する。

ユースケース

データの処理

ロールは、アカウント内のすべてのデータにアクセスできるように作成されています。暗号化された機密データがある場合、権限が緩すぎると、このロールを引き受けることのできるユーザーまたはグループによってはリスクにつながる可能性があります。 AWS Key Management Service（ AWS KMS) でキーポリシーを使用することで、キーにアクセスできるユーザーとデータを復号できるユーザーを制御できます。

権限昇格

管理のアクセス許可と書き込みのアクセス許可の割り当て範囲が広すぎると、ユーザーは、意図されたアクセス許可の制限をすり抜けて、追加の権限を自分で自分に付与することが可能になります。ロールを作成し管理するユーザーは、ロールに許可する権限の上限を規定する、アクセス許可の境界を割り当てることができます。

ワークロードのロックダウン

ビジネスで特定の サービスを使用する必要性が予測できない場合は、組織のメンバーアカウントで運用できるサービスを制限するか、 に基づいてサービスを制限するサービスコントロールポリシーを有効にします AWS リージョン。この予防的コントロールにより、脅威アクターがセキュリティを侵害して組織内のアカウントにアクセスした場合の影響を、抑えることができます。詳細については、このガイドの「サービスコントロールポリシー」を参照してください。

他のアプリケーションへの影響

予防的コントロールを使うと、アプリケーションのセキュリティ要件を満たすため、IAM、暗号化、ログ記録などのサービスや機能の使用を強制することができます。また、これらのコントロールを使うと、不測のエラーや設定ミスが原因で脅威アクターに悪用されるアクションを最小限に抑え、脆弱性から保護することもできます。

テクノロジー

サービスコントロールポリシー

では AWS Organizations、サービスコントロールポリシー (SCPsは、組織内のメンバーアカウントで使用可能なアクセス許可の最大数を定義します。これらのポリシーを使うことで、アカウントは、組織のアクセスコントロールのガイドラインの、範囲内にとどまることができます。組織の SCP を設定する際は、以下の点に注意します。

- SCPsは、組織のメンバーアカウントの IAM ロールとユーザーに許可されるアクセス許可の上限を定義して適用するため、予防的コントロールです。
- SCPs、組織のメンバーアカウント内の IAM ロールとユーザーのみに影響します。組織の管理アカウントのユーザーとロールには、影響を与えません。

各 AWS リージョンのアクセス許可の上限を定義すると、SCP をより細かく設定できます。

IAM アクセス許可の境界

AWS Identity and Access Management (IAM) では、アクセス許可の境界を使用して、アイデンティティベースのポリシーが IAM エンティティ (ユーザーまたはロール) に付与できるアクセス許可の上限を設定します。エンティティのアクセス許可の境界により、エンティティは、アイデンティティベースのポリシーとそのアクセス許可の境界の両方で許可されているアクションのみを、実行することができます。アクセス許可の境界を使用するときは、以下の点に注意します。

- AWS 管理ポリシーまたはカスタマー管理ポリシーを使用して、IAM エンティティの境界を設定できます。
- アクセス許可の境界自体は、アクセス許可を付与しません。アクセス許可の境界ポリシーは IAM エンティティに付与されるアクセス許可を制限します。

ビジネス上の成果

時間を節約できる

- 予防的コントロールを設定した後に自動化を追加することで、手動による介入の必要性と工ラーの発生頻度を減らすことができます。
- アクセス許可の境界を予防的コントロールとして使用すれば、セキュリティチームと IAM チームは、ガバナンスやサポートなどの重要タスクに専念することができます。

規制を確実に順守できる

- 企業では、社内や業界の規制を順守する必要が出てくる場合があります。このような規制は、リージョン、ユーザーやロール、サービスなどに制約をもたらす可能性があります。SCP を使用すると、常に規制を順守でき、違反による罰則を防ぐことができます。

リスクを軽減できる

- 会社が成長すると、新しいロールやポリシーの作成と管理を要求するリク工ストの数が増えます。それに伴って、各アプリケーションのアクセス許可を手動で作成するために何が必要なのか、そのコンテクストを理解することがますます難しくなります。設定した予防的コントロールは基準線として機能し、ユーザーに誤ってアクセス許可が付与された場合でも意図されていないアクションが実行されることを防ぐことができます。
- アクセスポリシーに予防的コントロールを適用すると、データやアセットを保護する新しいレイヤーが追加されます。

プロアクティブコントロール

プロアクティブコントロールとは、規制に準拠していないリソースの作成を防ぐように設計されたセキュリティコントロールです。これらのコントロールにより、レスポンシブコントロールと検出コントロールによって処理されるセキュリティイベントの数を減らすことができます。デプロイ前にデプロイされたリソースがコンプライアンスに準拠していることを確認できるため、対応や修復が必要な検出イベントが発生しません。

例えば、Amazon Simple Storage Service (Amazon S3) バケットが一般に公開された場合に通知する検出コントロールを設定することができます。また、それを修正するレスポンシブコントロールを設ける場合もあります。これら 2 つのコントロールがすでに設定されている場合でも、プロアクティ

ブコントロールを追加することで保護をさらに強化できます。を通じて AWS CloudFormation、プロアクティブコントロールは、パブリックアクセスが有効になっている S3 バケットの更新の作成を防ぐことができます。脅威アクターは引き続きこのコントロールをバイパスし、 の外部にリソースをデプロイまたは変更できます CloudFormation。この場合、検出コントロールとレスポンシブコントロールを使用することで、セキュリティイベントが修復されます。

このタイプのコントロールについては、以下の点を確認してください。

- 目的
- プロセス
- ユースケース
- テクノロジー
- ビジネス上の成果

目的

- プロアクティブコントロールは、セキュリティの運用プロセスと品質プロセスの改善に役立ちます。
- プロアクティブコントロールは、セキュリティポリシー、基準、規制やコンプライアンス上の義務を順守するのに役立ちます。
- プロアクティブコントロールで、コンプライアンス違反しているリソースの生成を防ぐことができます。
- プロアクティブコントロールにより、セキュリティに関する検出結果を減らすことができます。
- プロアクティブコントロールは、予防的コントロールを迂回してコンプライアンスに違反したリソースをデプロイしようと試みる脅威アクターに対する保護をさらに強化します。
- 予防的コントロール、検出的コントロール、レスポンシブコントロールを組み合わせることで、潜在的なセキュリティインシデントへの対処に役立ちます。

プロセス

プロアクティブコントロールは予防的コントロールを補完します。プロアクティブコントロールは、組織のセキュリティリスクを軽減し、コンプライアンスに準拠したリソースのデプロイを強化します。これらのコントロールは、リソースが作成または更新される前に、リソースのコンプライアンス状態を評価します。プロアクティブコントロールは通常、 CloudFormation フックを使用して実装されます。リソースがプロアクティブコントロールの検証に失敗した場合、リソースのデプロイに失敗

するか、警告メッセージを表示するかを選択できます。予防的コントロールを構築するためのヒントとベストプラクティスを以下に示します。

- 予防的コントロールが組織のコンプライアンス要件に準拠していることを確認してください。
- 予防的コントロールが関連サービスのセキュリティ上のベストプラクティスに従ったものであることを確認してください。
- CloudFormation StackSets または別のソリューションを使用して、複数の AWS リージョン またはアカウントにプロアクティブコントロールをデプロイします。
- プロアクティブコントロールに関連する警告または失敗メッセージが、明示的かつ明確であることを確認してください。開発者がリソースが評価に合格しなかった理由を理解するのに役立ちます。
- 新しいプロアクティブコントロールを構築するときには、オブザーバビリティモードから始めます。つまり、リソースのデプロイを失敗させるのではなく、警告メッセージを送信します。これは、プロアクティブコントロールの影響を理解する上で役立ちます。
- プロアクティブコントロールのために Amazon CloudWatch Logs のログ記録を有効にします。
- 特定のプロアクティブコントロールの呼び出しをモニタリングする必要がある場合は、Amazon EventBridge ルールを使用し、フックの呼び出しイベントをサブスクライブします CloudFormation。

ユースケース

- 準拠していないリソースのデプロイを防ぐ
- コンプライアンス要件への準拠
- セキュリティ上の問題をデプロイ前に強制的に修正することで、コードの品質を向上させます。
- デプロイ後の、セキュリティ問題の修正に伴う運用上のダウンタイムを短縮します。

テクノロジー

CloudFormation フック

AWS CloudFormation は、 AWS リソースをセットアップし、迅速かつ一貫してプロビジョニングし、 AWS アカウント および リージョン全体でライフサイクル全体にわたってリソースを管理するのに役立ちます。CloudFormation フックは、デプロイ前に CloudFormation リソースの設定をプロアクティブに評価します。準拠していないリソースが見つかると、障害ステータスが返されます。フック障害モードに基づいて、 CloudFormation は操作を失敗させたり、ユーザーがデプロイを続行

できるようにする警告を表示したりできます。利用可能なフックを使用することも、独自のフックを開発することもできます。

AWS Control Tower

AWS Control Tower は、ランディングゾーンで有効にできる事前設定されたプロアクティブコントロール AWS Control Tower を提供する規範的なベストプラクティスに従って、 AWS マルチアカウント環境をセットアップして管理するのに役立ちます。ランディングゾーンが を使用して設定されている場合は AWS Control Tower、これらのオプションのプロアクティブコントロールを組織の出発点として使用できます。 CloudFormation 必要に応じて、 で追加のカスタムプロアクティブコントロールを構築できます。

ビジネス上の成果

人的作業とエラーが減る

プロアクティブコントロールは、コンプライアンス違反リソースのデプロイへとつながる人為的ミスのリスクを軽減します。また、開発者がデプロイ前にリソースのセキュリティを考慮するようになるため、開発サイクルの後半に発生する人的労力も削減されます。これにより、開発ライフサイクルの早い段階でコンプライアンスを義務付けることになるため、安全なリソースの構築にシフトレフトの実践を適用することになります。

コストの削減

一般的に、デプロイ後にセキュリティ問題を修正する方がコストがかかります。開発サイクルの早い段階で問題を特定して修正することで、開発コストを削減できます。

時間を節約できる

プロアクティブコントロールはコンプライアンス違反のリソースのデプロイを防ぐため、セキュリティ問題の優先順位付けと修正に費やす時間を短縮できます。また、開発サイクルの後半で発見されるセキュリティ上の検出結果の数も、検出されます。

規制を確実に順守できる

組織が内部規制や業界規制を順守する必要がある場合、予防的コントロールを使用することで、準拠した状態を保ち、違反による罰則を防ぐことができます。

リスクを軽減できる

プロアクティブコントロールにより、開発者は規制に準拠した、より安全に構築されたリソースを展開できるため、プロアクティブコントロールによって組織のセキュリティリスクが軽減されます。

検出的コントロール

検出的コントロールとは、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です。検出的コントロールはガバナンスフレームワークの基本要素です。このガードレールは、予防的コントロールをすり抜けたセキュリティ問題をユーザーに通知する、副次的な防衛手段となります。

例えば、Amazon Simple Storage Service (Amazon S3) バケットが一般に公開された場合に、検出的コントロールを適用してこれを検出し、ユーザーに通知することができます。S3 バケットへのパブリックアクセスをアカウントレベルで無効にした後に SCP 経由でアクセスを無効にする予防的コントロールを実行している場合、脅威アクターはその間、管理ユーザーとしてログインすることでこのコントロールをすり抜けることができます。このような場合、検出的コントロールを使うと、設定ミスや潜在的脅威をユーザーに警告することができます。

このタイプのコントロールについては、以下の点を確認してください。

- 目的
- プロセス
- ユースケース
- テクノロジー
- ビジネス上の成果

目的

- 検出的コントロールは、セキュリティの運用プロセスと品質プロセスの改善に役立ちます。
- 検出的コントロールは、規制、法律、コンプライアンス関連の義務の履行に役立ちます。
- 検出的コントロールを使うことで、セキュリティ運用チームは、予防的コントロールをすり抜ける高度な脅威を含む、セキュリティ問題への対応を可視化することができます。
- 検出的コントロールは、セキュリティ問題や潜在的な脅威への適切な対応方法を特定するのに役立ちます。

プロセス

検出的コントロールは 2 段階で実施されます。まず、Amazon CloudWatch Logs などの一元的な場所にイベントとリソースの状態を記録するようにシステムを設定します。一元的なログ記録を実行したら、そのログを分析して脅威となる可能性のある異常を検出します。各分析が、元の要件やポリシーに対応付けられたコントロールです。例えば、ログで特定のパターンを検索し、一致するパターンが見つかれば警告を発信するように、検出的コントロールを作成できます。検出的コントロールは、セキュリティチームが、システムに影響を及ぼす脅威やリスクの全体的な視認性を高めるのに使用します。

ユースケース

不審な動作の検出

検出的コントロールを使うと、特権ユーザーの認証情報への不正アクセス、機密データへのアクセスまたは機密データの流出など、異常なアクティビティを特定することができます。このコントロールは重要な反応因子であり、企業が異常なアクティビティの範囲を特定して理解するのに役立ちます。

不正行為の検出

このコントロールは、ポリシーをすり抜けて不正な取引を行っているユーザーなど、社内の脅威を検出し特定するのに役立ちます。

コンプライアンス

検出的コントロールは、Payment Card Industry Data Security Standard (PCI DSS) などのコンプライアンス要件を満たし、個人情報のなりすましを防ぐのに役立ちます。このコントロールを使うと、個人を特定できる情報など、規制順守の対象となる機密情報を発見して保護することができます。

自動分析

検出的コントロールでは、ログを自動的に分析し、異常やその他不正行為の兆候を検出することができます。

AWS CloudTrail ログ、VPC フローログ、ドメインネームシステム (DNS) ログなどさまざまなソースのログを自動的に分析し、害を及ぼす恐れのある活動の兆候がないか調べることができます。組織に役立つように、複数の のセキュリティアラートや検出結果を一元 AWS のサービス 的に集約します。

テクノロジー

一般的な検出コントロールでは、1 つ以上のモニタリングサービスを実装し、ログなどのデータソースを分析してセキュリティの脅威を特定します。では AWS クラウド、 AWS CloudTrail ログ、Amazon S3 アクセスログ、Amazon Virtual Private Cloud フローログなどのソースを分析して、異常なアクティビティを検出できます。Amazon GuardDuty、Amazon Detective、Amazon Macie などの AWS セキュリティサービスには AWS Security Hub、モニタリング機能が組み込まれています。

GuardDuty および Security Hub

Amazon GuardDuty は、脅威インテリジェンス、機械学習、異常検出技術を使用して、ログソースに悪意のあるアクティビティや不正なアクティビティがないか継続的にモニタリングします。ダッシュボードは、 AWS アカウント および ワークロードのリアルタイムヘルスに関するインサイトを提供します。ベストプラクティスへの準拠をチェックしAWS Security Hub、アラートを集約し、自動修復を可能にするクラウドセキュリティ体制管理サービスである と統合 GuardDutyできます。は、情報を一元化する方法として、結果を Security Hub GuardDuty に送信します。さらに、Security Hub を、セキュリティ情報とイベント管理 (SIEM) ソリューションと統合すれば、組織のモニタリングと警告の機能を拡張できます。

Macie

Amazon Macie は、フルマネージドのデータセキュリティおよびデータプライバシーサービスであり、機械学習とパターンマッチングを使用して AWS内の機密データを検出し保護します。以下は、Macie で使用できる検出的コントロールと機能の一部です。

- Macie では、バケットインベントリと Amazon S3 に保存されているオブジェクトのすべてが検査されます。この情報はダッシュボードの単一画面に表示できるため、バケットのセキュリティを把握し、評価するのに役立ちます。
- Macie では、機密データの検出に、組み込みのマネージドデータ識別子を使用するほか、カスタムデータ識別子もサポートしています。
- Macie は他の AWS のサービス および ツールとネイティブに統合されます。例えば、Macie は検出結果を Amazon EventBridge イベントとして発行し、Security Hub に自動的に送信します。

Macie の検出的コントロールの設定に関するベストプラクティスは、次のとおりです。

- すべてのアカウントで Macie を有効にします。委任管理の機能を使用して、複数のアカウントで AWS Organizationsを使って Macie を有効にします。

- Macie を使用して、アカウント内の S3 バケットのセキュリティ体制を評価します。これにより、データの場所やアクセスが可視化され、データ損失を防ぐことができます。詳細については、「Analyzing your Amazon S3 security posture」(Macie ドキュメント) を参照してください。
- 自動処理ジョブとデータ検出ジョブを実行およびスケジュール設定して、S3 バケット内の機密データの検出を自動化します。これで、S3 バケット内に機密データがないか、定期的に検査されます。

AWS Config

AWS Config resources. AWS Config discovers existing AWS AWS resources のコンプライアンスを監査して記録し、各リソースの設定詳細とともに完全なインベントリを生成します。設定に変更があれば、その変更は記録されてユーザーに通知されます。これにより、インフラストラクチャの不正な変更を検出して元の状態に戻すことができます。 AWS マネージドルールを使用し、カスタムルールを作成できます。

AWS Configでの検出的コントロールの設定に関するベストプラクティスは、次のとおりです。

- 組織内の AWS Config 各メンバーアカウントと、保護するリソース AWS リージョン を含む各 に対して を有効にします。
- 設定が変更された場合に備えて Amazon Simple Notification Service (Amazon SNS) のアラートを設定します。
- S3 バケットに設定データを保存し、Amazon Athena を使ってそのデータを分析します。
- AWS Systems Managerの機能であるオートメーションを使って、非準拠のリソースの修復を自動化します。
- EventBridge または Amazon SNS を使用して、非準拠 AWS リソースに関する通知を設定します。

Trusted Advisor

AWS Trusted Advisor は、検出的コントロールのサービスとして使用することが可能です。一連のチェックを通じて、 は、インフラストラクチャの最適化、パフォーマンスとセキュリティの向上、コスト削減が可能な分野 Trusted Advisor を特定します。 Trusted Advisor は、 サービスとリソースの改善に役立つ AWS ベストプラクティスに基づいて推奨事項を提供します。ビジネスおよびエンタープライズサポートプランでは、 AWS Well-Architected フレームワークの柱について利用可能なすべてのチェックにアクセスできます。

Trusted Advisorでの検出的コントロールの設定に関するベストプラクティスは、次のとおりです。

- チェックレベルの概要を確認します。
- 警告とエラーの状態に関する、リソース固有の推奨事項を実装します。
- レコメンデーションを積極的に確認して実装するには、 を Trusted Advisor 頻繁にチェックしてください。

Amazon Inspector

Amazon Inspector は、有効化した後にワークロードを継続的にスキャンし、意図しないネットワークの公開やソフトウェアの脆弱性を検出する、自動化された脆弱性管理サービスです。検出結果をリスクスコアとして文脈化し、コンプライアンス状況の改善や確認など、次に行うべきステップを判断できるようにします。

Amazon Inspector での検出的コントロールの設定に関するベストプラクティスは、次のとおりです。

- すべてのアカウントで Amazon Inspector を有効にし、 EventBridge と Security Hub に統合して、セキュリティの脆弱性に関するレポートと通知を設定します。
- Amazon Inspector のリスクスコアに基づき、修復やその他のアクションに優先順位を付けます。

ビジネス上の成果

人的作業とエラーが減る

Infrastructure as Code (IaC) を使用することで自動化を実現できます。モニタリングと修復のためのサービスおよびツールの、デプロイと設定を自動化すれば、マニュアル作業によるエラーのリスクを減らし、検出的コントロールのスケールに必要な、時間と労力とを減らすことができます。自動化はセキュリティランブックの開発を後押しし、セキュリティアナリストのマニュアルでの操作を減らすことにつながります。定期的な点検により自動化ツールを調整し、検出的コントロールを継続的に反復し改善することができます。

潜在的脅威に適切に対処できる

ログやメトリクスからイベントをキャプチャし、分析することは、可視性を高めるためにきわめて重要です。それによりアナリストは、セキュリティイベントや潜在的な脅威に対処し、ワークロードを保護することができます。どのような脆弱性が存在するのかをすばやく特定できれば、アナリストはその脆弱性に対処し、修正のための適切な措置を講じることができます。

インシデント対応や調査対応が改善する

検出的コントロール用ツールを自動化すれば、検出、調査、復旧のスピードを速めることができます。定義された条件に基づきアラートと通知を自動化することで、セキュリティアナリストは調査と対応を適切に行うことができます。対応因子は、異常なアクティビティの範囲を特定して理解するのに役立ちます。

レスポンシブコントロール

レスポンシブコントロールは、有害事象や、セキュリティ上の基準線からの逸脱の、修復を早めるように設計されたコントロールです。技術的なレスポンシブコントロールの例には、システムへのパッチ適用、ウイルスの隔離、プロセスのシャットダウン、システムの再起動などがあります。

このタイプのコントロールについては、以下の点を確認してください。

- 目的
- プロセス
- ユースケース
- テクノロジー
- ビジネス上の成果

目的

- レスポンシブコントロールは、フィッシングやブルートフォース攻撃など、一般的な攻撃に対処するためのランブックの作成に役立ちます。
- レスポンシブコントロールでは、潜在的なセキュリティ問題への自動対応を実装できます。
- レスポンシブコントロールは、暗号化されていない S3 バケットの削除など、 AWS リソースに対する意図しないアクションや未承認のアクションを自動的に修正できます。
- レスポンシブコントロールは、予防的コントロールや検出的コントロールと連携するようにオーケストレーションすることで、潜在的なセキュリティインシデントに対する包括的かつ事前対処的なアプローチを構築できます。

プロセス

検出的コントロールは、レスポンシブコントロールを設定するための前提条件となります。セキュリティ問題は、修復する前に、まず検出できなければなりません。セキュリティ問題に対するポリシー

や対応を設定できるのはその後です。例えば、ブルートフォース攻撃が発生した場合、修復プロセスが実行されます。修復プロセスが存在する場合、シェルスクリプトなどのプログラミング言語を使って、スクリプトとして自動化し実行することができます。

レスポンシブコントロールが、既存の本番ワークロードを中断させる可能性があるかどうか、検討します。例えば検出的コントロールにおいて、S3 バケットがパブリックにアクセス可能にしてはならず、かつ修復が Amazon S3 のパブリックアクセスをオフにするだった場合、この修復方法では、その会社と顧客に重大な影響を与える可能性があります。S3 バケットが、公開されているウェブサイトにサービスを提供している場合、パブリックアクセスをオフにすると機能が停止する可能性があります。データベースも同様です。データベースをインターネット経由でパブリックにアクセス可能にしてはならない場合、パブリックアクセスをオフにすると、アプリケーションへの接続に影響が出る可能性があります。

ユースケース

- 検出されたセキュリティイベントへの自動対応
- 検出されたセキュリティ脆弱性の自動修復
- 修復コントロールを自動化してオペレーションのダウンタイムを減らす

テクノロジー

Security Hub

AWS Security Hub は、すべての新しい検出結果と既存の検出結果のすべての更新をイベント EventBridge として に自動的に送信します。選択した結果とインサイト結果を に送信するカスタムアクションを作成することもできます EventBridge。各タイプのイベントに応答 EventBridge するように を設定できます。イベントは、修復アクションを実行する AWS Lambda 関数を開始できます。

AWS Config

AWS Config は、 ルールを使用して AWS リソースを評価し、非準拠の リソースを修復するのに役立ちます。 はAWS Systems Manager 、オートメーション を使用した修復 AWS Config を適用します。自動化ドキュメントでは、 が非準拠 AWS Config であると判断したリソースに対して実行するアクションを定義します。Automation ドキュメントを作成したら、 AWS Management Console または APIsでそれらを使用できます。非準拠のリソースの修復は、手動で行うか、自動で行うかを選択できます。

ビジネス上の成果

データ損失を最小限に抑える

サイバーセキュリティインシデントが発生した場合は、レスポンシブセキュリティコントロールを使うことで、データの損失や、システムまたはネットワークへの損害を最小限に抑えることができます。また、レスポンシブコントロールは、重要なビジネスシステムやプロセスを可能な限りすばやく復旧させるのにも役立ち、ワークロードの回復力を高めます。

コストを削減できる

自動化により、チームメンバーはインシデントに手動で対応したり、インシデントを case-by-case ベースで管理したりする必要がなくなるため、人的リソースに関連するコストを削減できます。

次のステップ

本ガイドを読むことで、4 種類のセキュリティコントロールについて理解し、それらがセキュリティガバナンスのフレームワークにどのように含まれているかを理解することができます。また、AWS クラウド でセキュリティコントロールの実装と自動化を開始する準備が整います。詳細については、リソース セクションに記載のリファレンスをを確認することをお勧めします。

また、次のステップを踏んでクラウドインフラストラクチャのセキュリティを評価し、セキュリティコントロールの実装を開始することをお勧めします。

1. AWS Security Hub を有効にして設定します。ベストプラクティスとして、利用可能な標準コントロールを有効にすることをお勧めします。詳細については、「セキュリティコントロールと標準」(Security Hub ドキュメント) を参照してください。
2. AWS Config を有効にして設定します。詳細については、「AWS Config ドキュメント」の「使用の開始」を参照してください。
3. Security Hub、Amazon Macie、AWS Config、AWS Trusted Advisor、Amazon Inspector などの AWS のサービス を使用して、お客様の組織とアカウントインフラストラクチャを評価し、改善が必要な分野を特定し、これらのサービスのレビューと推奨事項を検討します。Security Hub のセキュリティチェック機能を使用して、セキュリティ標準のセキュリティスコアを生成します。詳細については、「セキュリティスコアの決定」(Security Hub ドキュメント) を参照してください。
4. 特定された改善点に基づいて、予防、検出、応答するセキュリティコントロールを実装します。
5. フォローアップのセキュリティ評価を実施して、実施されたセキュリティコントロールの有効性を評価します。Security Hub で、セキュリティスコアが向上したかどうかを確認します。繰り返してセキュリティコントロールを改善するか、新しいセキュリティコントロールを追加します。
6. 毎年セキュリティアセスメントを実施するなど、定期的に実施するようにしてください。

よくある質問

時間とリソースが限られていて、これらすべてのコントロールタイプを実装できない場合、何に焦点を当てるべきですか?

AWS Security Hub を実装することをお勧めします。Security Hub には、「AWS Foundational Security Best Practices 標準」(Security Hub ドキュメント)と呼ばれる一連の自動化されたセキュリティコントロールがあります。これは、AWS セキュリティエキスパートが管理する、厳選されたセキュリティのベストプラクティスです。これらの標準コントロールは、継続的に実行することも、関連リソースに変更があるたびに実行することもできます。定期的に実行することもできます。各コントロールには特定の重要度スコアがあり、修復作業の優先順位付けに役立ちます。詳細については、「セキュリティチェックの実行」(Security Hub ドキュメント) を参照してください。AWS Control Tower を使用している場合は、その予防、検出およびプロアクティブコントロールを確認して、有効にするかどうかを選択することもできます。

リソース

AWS ドキュメント

- AWS Security Reference Architecture (AWS SRA)
- AWS CAF セキュリティの視点
- セキュリティ、アイデンティティ、コンプライアンスのベストプラクティス
- AWS で自動化されたセキュリティ対応 (AWS ソリューション)
  - ソリューションのランディングページ
  - 実装ガイド

AWS ブログ記事

- アイデンティティガイド — AWS Identity による予防管理 — SCP
- AWS Organizations アカウントに読み取り専用のサービスコントロールポリシー (SCP) を実装する方法
- マルチアカウント環境における AWS Organizations サービスコントロールポリシーのベストプラクティス
- サービスコントロールポリシーを使用してコンプライアンスを維持し、ポリシーが常に適用されるようにする
- IAM アクセス許可の境界をいつ、どこで使用するか
- AWS CloudFormation フックを使って、プロアクティブにリソースを安全に保ちコンプライアンスを維持する

その他のリソース

- クラウドコントロールマトリックス (CCM) (クラウドセキュリティアライアンス)
- アクセス許可の境界の例 (GitHub)

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
プロアクティブコントロール	「プロアクティブコントロール」セクションなど、プロアクティブコントロールに関する情報が本ガイドに追加されました。	2023 年 12 月 4 日
初版発行	—	2022 年 12 月 12 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にある程度の最適化を導入します。例: オンプレミスの Oracle データベースを の 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: の移行 Microsoft Hyper-V アプリケーション 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

原子性、一貫性、分離性、耐久性を参照してください。

アクティブ - アクティブ移行

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

アクティブ - パッシブ移行

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

集計関数

行のグループに対して動作し、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。

人工知能オペレーション (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。AIOps が移行戦略で AWS どのように使用されるかの詳細については、「 オペレーション統合ガイド」を参照してください。

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。

アトミック性、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コントロール (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 （ ABAC) ドキュメントの「 の AWS IAM」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 内の個別の場所。

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分類します。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、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 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

個人または組織に混乱や損害を与えることを目的としたボット。

BCP

事業継続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 で動作グラフを使用して、失敗したログオン試行、不審な API 呼び出し、および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他の環境 (グリーン) 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、有益または有益なボットもあります。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 1 人の当事者による管理下にあ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、「ブランチについて」(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なります。詳細については、 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 AWS 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。

事業継続計画 (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低速かつ段階的なリリース。自信が持てたら、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

「データキャプチャの変更」を参照してください。

データキャプチャの変更 (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、同期を維持するためにターゲットシステムの変更を監査またはレプリケートするなど、さまざまな目的で使用できます。

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、システムの回復力をテストします。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
- Foundation – クラウド導入を拡大するための基本的な投資 (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。これらが AWS 移行戦略とどのように関連しているかについては、「移行準備ガイド」を参照してください。

CMDB

「設定管理データベース」を参照してください。

コードリポジトリ

ソースコードやその他の資産 (ドキュメント、サンプル、スクリプトなど) が保存され、バージョン管理プロセスを通じて更新される場所。一般的なクラウドリポジトリには、次のようなものがあります。GitHub または 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動画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 は CV の画像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、通常は段階的かつ意図的ではありません。

設定管理データベース (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、移行のポートフォリオ検出および分析段階で CMDB のデータを使用します。

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 とリージョン、または組織全体に 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 is commonly described as a pipeline. CI/CD は、プロセスの自動化、生産性の向上、コード品質の向上、より迅速な提供に役立ちます。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

一元的な管理とガバナンスにより、分散型の分散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実にします。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。

defense-in-depth

一連のセキュリティメカニズムとコントロールをコンピュータネットワーク全体に層状に重ねて、ネットワークとその内部にあるデータの機密性、整合性、可用性を保護する情報セキュリ

ティの手法。この戦略を採用するときは 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。例えば、a defense-in-depth 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。

デプロイメント

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

開発環境

「環境」を参照してください。

検出管理

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

開発値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、もともとリーンな製造プラクティス向け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ます。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に使用する戦略とプロセス。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については、「コンテナと Amazon Word API Gateway を使用してレガシー Microsoft ASP.NET (ASMX) ウェブサービスを段階的にモダナイズする」を参照してください。

DR

「ディザスタリカバリ」を参照してください。

ドリフト検出

ベースライン設定からの逸脱の追跡。例えば、 AWS CloudFormation を使用してシステムリソースのドリフトを検出したり、 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

Virtual Private Cloud (VPC) 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 Word) ドキュメントの「エンドポイントサービスの作成」を参照してください。 VPC

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、サマリー統計を計算し、データの視覚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

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

障害分離の境界

では AWS クラウド、アベイラビリティーゾーン、コントロールプレーン AWS リージョン、データプレーンなどの境界で、障害の影響を制限し、ワークロードの耐障害性の向上に役立ちます。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 Explanations (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として表されます。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

同様のタスクを実行するように求める前に、タスクと必要な出力を示す少数の例を LLM に提供します。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コントロール (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のではなく、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、可能な限り短い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)

一般化データとラベルなし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、「基礎モデルとは」を参照してください。

G

生成 AI

大量のデータに対してトレーニングされ、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)

Amazon CloudFront では、特定の国のユーザーがコンテンツディストリビューションにアクセスできないようにするオプションです。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分散の制限」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、デバイスの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 (OUs) 全体のリソース、ポリシー、コンプライアンスの管理に役立つ大まかなルール。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ている、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

ソースデータベースを、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) に移行します。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。緊急性のため、通常、ホットフィックスは一般的な DevOps リリースワークフローの外部で行われます。

ハイパーケア期間

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

I

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CPUおよびメモリ使用量が 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、本番環境のワークロードに新しいインフラストラクチャをデプロイするモデル。イミュータブルなインフラストラクチャは、本質的にミュータブルなインフラストラクチャよりも一貫性、信頼性、予測性が高くなります。詳細については、 AWS 「 Well-Architected 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 (イングレス) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーション外からのネットワーク接続を受け入れ、検査し、ルーティングする VPC。AWS セキュリティリファレンスアーキテクチャで

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VPCsを使用してネットワークアカウントを設定することをお勧めします。

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は、接続、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。

産業モノのインターネット (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、「産業モノのインターネット (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。

検査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 セキュリティリファレンスアーキテクチャでは、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VPCsを使用してネットワークアカウントを設定することをお勧めします。

IoT

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

解釈可能性

機械学習モデルの特性で、モデルの予測がその入力にどのように依存するかを人間が理解できる度合いを表します。詳細については、AWS による機械学習モデルの解釈可能性」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

ラベルベースのアクセスコントロール (LBAC)

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ている必須アクセスコントロール (MAC) の実装。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)

大量のデータに対し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 とは」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「最小特権の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 R」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や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 AWS を運用し、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。これにより、生産現場の生産物から完成した製品に加工されます。

MAP

「移行促進プログラム」を参照してください。

メカニズム

ツールを作成し、ツールの導入を推進し、調整の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して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な 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 APIs を介して通信し、通常は小規模で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。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、軽量な APIs 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。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、従来の移行を体系的に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ための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と所有者、移行エンジニア、デベロッパー、スプリントに取り組む 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 アプリケーション移行サービスを使用して Amazon EC2 への移行をリホストします。

移行ポートフォリオ評価 (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) と移行計画 (アプリケーションデータ分析とデータ収集、アプリケーショングループ化、移行の優先順位付け、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 移行戦略の最初のフェーズです。

移行戦略

ワークロードを に移行するために使用するアプローチ 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をベストプラクティスとして使用することを推奨しています。

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

「組織の変更管理」を参照してください。

オフライン移行

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

OI

「 オペレーションの統合」を参照してください。

OLA

「運用レベルの契約」を参照してください。

オンライン移行

ソースワークロードをオフラインにせず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)

産業用オートメーション用の A 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。

運用レベルの契約 (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 IT グループが相互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範囲を理解、評価、防止、または縮小するの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運用、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 と情報テクノロジー (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主要な焦点です。

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をログ AWS CloudTrail 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、移行に伴う問題に対処し、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や戦略に備え、移行するのに役立ちます。 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を人材アクセラレーションと呼びます。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)

In CloudFront。Amazon Simple Storage Service (Amazon S3) コンテンツを保護するためのアクセスを制限するための拡張オプションです。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、および 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)

In CloudFront は、Amazon S3 コンテンツを保護するためのアクセスを制限するオプションです。OAI を使用すると、 CloudFront は Amazon S3 が認証できるプリンシパルを作成します。認証されたプリンシパルは、特定の CloudFront ディストリビューションを介してのみ S3 バケット内のコンテンツにアクセスできます。Word も参照してください。OACより詳細で強化されたアクセスコントロールを提供します。

ORR

「運用準備状況レビュー」を参照してください。

OT

「運用技術」を参照してください。

アウトバウンド (出力) 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 セキュリティリファレンスアーキテクチャでは、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VPCsを使用してネットワークアカウントを設定することをお勧めします。

P

アクセス許可の境界

ユーザーまたはロールが持つことができるアクセス許可の上限を設定するための Word プリンシパルにアタッチされる IAM 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、名前、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。通常は `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「ロールの用語と概念」の「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に入れた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

Amazon Route 53 が 1 つ以上の DNS 内のドメインとそのサブドメインの VPCs クエリに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止する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、成長と成熟、辞退と削除まで、ライフサイクル全体にわたる製品のデータとプロセスの管理。

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 (PLC)

製造では、マシンをモニタリングし、製造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、事前対応を繰り返し調整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。

publish/subscribe (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。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 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内のデータにアクセスするために使用す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

「責任者」、「説明責任者」、「相談先」、「通知先」(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

「責任者」、「説明責任者」、「相談先」、「通知先」(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 R」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 R」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 とは分離され、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 R」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 R」を参照してください。

プラットフォーム変更

「7 R」を参照してください。

再購入

「7 R」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。で障害耐性を計画する場合、高可用性とディザスタリカバリがよく考慮されます 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。

責任、説明責任、相談、情報提供 (RACI) 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、マトリックスは RASCI マトリックスと呼ばれ、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 R」を参照してください。

廃止

「7 R」を参照してください。

取得拡張生成 (RAG)

レスポンスを生成する前に、LLM が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や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

攻撃者が認証情報にアクセスすることをより困難にするために、シークレットを定期的に更新するプロセス。

行と列のアクセスコントロール (RCAC)

アクセスルールが定義されている基本的で柔軟な SQL 式の使用。RCACは、行のアクセス許可と列マスクで構成されます。

RPO

「目標復旧時点」を参照してください。

RTO

目標復旧時間を参照してください。

ランブック

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

S

SAML 2.0

多くの ID プロバイダー (IdPs) が使用するオープンスタンダード。この機能により、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、ユーザーは組織内のすべてのユーザーをAWS API で作成しなくても、 AWS Management Console にログインしたりIAM オペレーションを呼び出したりできます。SAML 2.0 ベースのフェデレーションの詳細については、Word 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収集」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

開発プロセス全体を通じてセキュリティを考慮した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。

セキュリティ情報とイベント管理 (SIEM) システム

セキュリティ情報管理 (SIM) システムとセキュリティイベント管理 (SEM) 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、その他のソースからデータを収集、監視、分析して、脅威やセキュリティ違反を検出し、アラートを生成します。

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対応または修正するように設計された、事前定義され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の実装に役立つ検出的または応答的な AWS セキュリティコントロールとして機能します。自動応答アクションの例には、VPC セキュリティグループの変更、Amazon EC2 インスタンスへのパッチ適用、認証情報のローテーションなどがあります。

サーバー側の暗号化

送信先にあるデータの、それ AWS のサービス を受け取る による暗号化。

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。SCPsは、管理者がユーザーまたはロールに委任できるアクションのガードレールを定義するか、制限を設定します。SCPs を許可リストまたは拒否リストとして使用して、許可または禁止されるサービスまたはアクションを指定できます。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。

サービスレベルの目標 (SLO)

サービスレベルのインジケータによって測定される、サービスの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、ユーザー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)

システムを中断させる可能性のあるアプリケーションの 1 つの重要なコンポーネントの障害。

SLA

「サービスレベルアグリーメント」を参照してください。

SLI

「サービスレベルインジケータ」を参照してください。

SLO

「サービスレベルの目標」を参照してください。

split-and-seed モデル

モダナイゼーションプロジェクトのスケーリングと加速のためのパターン。新機能と製品リリースが定義されると、コアチームは解放されて新しい製品チームを作成します。これにより、お客様の組織の能力とサービスの拡張、デベロッパーの生産性の向上、迅速なイノベーションのサポートに役立ちます。詳細については、「」の「アプリケーションをモダナイズするための段階的アプローチ 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。このパターンを適用する方法の例については、「コンテナと Amazon ASP API Gateway を使用してレガシー Microsoft Word.NET (ASMX) ウェブサービスを段階的にモダナイズする」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生産オペレーション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

ユーザーインタラクション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

動作を指示するために、コンテキスト、指示、またはガイドラインを LLM に提供するための手法。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

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

VPCs ネットワーク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トランジットハブ。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「 を他の AWS のサービス AWS Organizations 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 つのピザを食べることができる small 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 VPCs 間の接続。詳細については、Amazon VPC ドキュメントの「Word ピアリングとは」を参照してください。 VPC

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」、「読み取り数」を参照してください。

WQF

AWS 「Word Workload Qualification Framework」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

タスクを実行するための指示を LLM に提供しますが、タスクのガイドに役立つ例 (ショット) はありません。LLM は、事前にトレーニングされた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

CPU とメモリの平均使用量が 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。