Creating an enterprise encryption strategy for data at rest

AWS 規範ガイダンス

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

AWS 規範ガイダンス: Creating an enterprise encryption strategy for data at rest

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

Amazon の商標およびトレードドレスは、Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は、Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

保存データのエンタープライズ暗号化戦略の作成

Venki Srivatsav、Andrea Di Fabio、Vikramaditya Bhatnagar、Amazon Web Services (AWS)

2022年9月 (ドキュメント履歴)

多くの企業は、データ漏えいによるサイバーセキュリティの脅威を懸念しています。データ侵害が発生すると、権限のない人がネットワークにアクセスし、企業データを盗みます。ファイアウォールとマルウェア対策サービスは、この脅威からの保護に役立ちます。実装できるもう 1 つの保護は、データ暗号化です。このガイドの「データ暗号化について」セクションでは、データ暗号化の仕組みと使用可能な種類について詳しく説明しています。

暗号化について話すとき、一般的に言って、データには 2 種類あります。転送中のデータとは、ネットワークリソース間など、ネットワーク内を活発に移動しているデータです。保存データとは、ストレージ内のデータなど、静止していて休止しているデータです。この戦略は、保管中のデータに焦点を当てています。転送中のデータの暗号化の詳細については、「転送中のデータの保護 (AWSWell-Architected フレームワーク)」を参照してください。

暗号化戦略は、順次開発する 4 つの部分で構成されます。暗号化ポリシーは、上級管理職によって決定され、暗号化に関する規制、コンプライアンス、およびビジネス要件の概要を示しています。暗号化標準は、ポリシーを実装する人がそれを理解し、遵守するのに役立ちます。標準は技術的なものでも手続き的なものでもかまいません。フレームワークは、標準の実装をサポートする標準的な運用手順、構造、およびガードレールです。最後に、アーキテクチャとは、使用する環境、サービス、ツールなど、暗号化標準を技術的に実装することです。このドキュメントの目的は、ビジネス、セキュリティ、コンプライアンスのニーズに合った暗号化戦略の作成を支援することです。これには、コンプライアンスとビジネスニーズを総合的に満たせるように、保存データのセキュリティ基準を見直して実装する方法に関する推奨事項が含まれています。

この戦略では、AWS Key Management Service (AWS KMS) を使用して、データの保護に役立つ暗号鍵の作成と管理を支援します。 AWS KMSAWSは多くのサービスと統合して、保存中のすべてのデータを暗号化します。別の暗号化サービスを選択した場合でも、このガイドの推奨事項とフェーズを採用できます。

対象者

この戦略は、以下のオーディエンスを対象としています。

- CEO、最高技術責任者（CTO）、最高情報責任者（CIO）、最高情報セキュリティ責任者（CISO）など、企業のポリシーを策定する執行役員

- 技術標準の設定を担当する技術担当者 (技術担当副社長や取締役など)
- 法定および自主的なコンプライアンス体制を含むコンプライアンスポリシーの遵守状況の監視を担当するコンプライアンスおよびガバナンス責任者

ターゲットを絞ったビジネス成果

- Data-at-rest 暗号化ポリシー — 意思決定者と政策立案者は、暗号化ポリシーを作成し、ポリシーに影響する重要な要素を理解できます。
- Data-at-rest 暗号化標準 — 技術リーダーは、暗号化ポリシーに基づいた暗号化標準を開発できます。
- 暗号化のフレームワーク — 技術リーダーと実装者は、ポリシーを決定する人と標準を作成する人の間の架け橋となるフレームワークを作成できます。この文脈におけるフレームワークとは、ポリシーの範囲内で標準を実装するのに役立つ適切なプロセスとワークフローを特定することを意味します。フレームワークは、ポリシーや標準を変更するための標準的な運用手順や変更管理プロセスに似ています。
- 技術的なアーキテクチャと実装 — 開発者やアーキテクトなどの実践的な実装者は、暗号化戦略の実装に役立つアーキテクチャのリファレンスを知っています。

制約事項

このドキュメントは、企業のニーズに最適なカスタム暗号化戦略を策定するのに役立つことを目的としています。これ自体は暗号化戦略ではなく、コンプライアンスチェックリストでもありません。次のトピックは、このドキュメントには含まれていません。

- 転送中のデータの暗号化
- トークン分割
- ハッシュ
- コンプライアンスとデータガバナンス
- 暗号化プログラムの予算編成

これらの各トピックの詳細については、リソースを参照してください。

データの暗号化について

このセクションでは、暗号化の概念と専門用語の高レベルの概要を示します。詳細については、「暗号化の概念 (AWS暗号化サービスおよびツールガイド)」を参照してください。データの暗号化は、データの機密保持を強化するのに役立ちます。暗号化とアクセス制御を実装することで、企業内のデータを保護できます。

暗号化キーについて

暗号化サービスは暗号化キーを使用してデータを暗号化します。暗号化キーは、暗号化アルゴリズムによって生成されるランダム化されたビットの暗号化文字列です。キーの長さはさまざまで、各キーは予測不能でユニークになるように設計されています。暗号化の強度は、通常、キーの長さと使用するアルゴリズムという 2 つの要素によって決まります。一般に、キーが長いほど暗号化が強化されます。

暗号化アルゴリズムについて

暗号化キーを生成するアルゴリズムには、対称型と非対称型の 2 種類があります。

対称暗号化では、データの暗号化と復号化に同じキーが使用されます。このタイプの暗号化は一般的に処理速度が速いため、大量のデータに対しては効率的です。このタイプの暗号化は広く使用されており、一般的に安全であると認められています。暗号化と復号化の両方に 1 つのキーが使用されるため、権限のない人がキーを取得できないように、キーを頻繁に変更するのがベストプラクティスです。対称暗号化が推奨される場合の詳細については、対称暗号化が必要なのはどのような場合ですか?よくある質問セクションのを参照してください。

非対称暗号化では、暗号化には公開鍵、復号には秘密鍵のペアを使用します。公開鍵は復号化には使用されないため共有できますが、秘密鍵へのアクセスは厳しく制限する必要があります。非対称暗号化は一般に対称暗号化よりも安全であると考えられていますが、使用するキーの長さが長く、暗号化計算がより複雑になるため、処理速度は遅くなります。非対称暗号化が推奨される場合の詳細については、非対称暗号化はどのような場合に必要ですか?よくある質問セクションのを参照してください。

エンベロープ暗号化について

データを暗号化すると、暗号化キーがシークレットである間のみ保護されます。データの暗号化に使用するキーは、データキーと呼ばれます。エンベロープ暗号化とは、キー暗号化キーと呼ばれる別の

暗号化キーを使用してデータキーを暗号化する方法です。そのキーを別の暗号化キーで暗号化することも可能です。最終的には、キーとデータを復号するために、1 つのキーをプレーンテキストで保持する必要があります。この最上位プレーンテキストキーの暗号化キーは、ルートキーと呼ばれます。

エンベロープ暗号化には、いくつかの利点があります。

- 利便性 — データキーは暗号化されているため、暗号化されたデータと一緒に保存できます。
- 効率性 — 暗号化オペレーションには時間がかかります (特に、データ量が大きい場合)。異なるキーで raw データを複数回にわたって再暗号化する代わりに、raw データを保護するデータキーのみを再暗号化できます。これにより、データを再暗号化しなくても、2 層以上の暗号化保護を実現できます。
- パフォーマンス — 暗号化アルゴリズムを組み合わせることができます。たとえば、未加工のデータには対称暗号化を使用し、データキーには非対称暗号化を使用できます。これは、両方の暗号化アルゴリズムの長所を組み合わせたものです。

エンベロープ暗号化の仕組みの詳細については、エンベロープ暗号化 (AWS Key Management Serviceドキュメント) を参照してください。エンベロープ暗号化が必要かどうかの判断方法について詳しくは、エンベロープ暗号化はどのような場合に必要ですか?よくある質問セクションのを参照してください。

暗号化戦略構築のフェーズ

エンタープライズレベルの暗号化戦略を構築するには、多段階的なアプローチが必要です。各フェーズでは、希望する具体的な結果を達成するのに役立つ一連のコントロールが定義されています。このドキュメントでは、これらのフェーズを順を追って説明し、暗号化戦略のカスタマイズに役立つ具体的な質問を示します。

保存中のデータの暗号化戦略の構築は、次の段階で構成されています。

1. 暗号化ポリシー— data-at-rest 企業の暗号化目標を定義するポリシーを構築します。
2. 暗号化規格：企業方針の実現に役立つ技術標準と手続き基準を定義できます。
3. 暗号化フレームワーク：すべての利害関係者が自社の暗号化標準を理解し、変更し、実装するのに役立つフレームワークを構築します。
4. 実装— 暗号化インフラストラクチャを導入。

暗号化ポリシー

暗号化ポリシーの目的は、組織が満たす必要のあるビジネスとコンプライアンスの期待を上級管理職レベルで確立することです。このポリシーは、適切な暗号化戦略を定義するための出発点となります。ポリシーは、実施に自由と柔軟性を提供できるほど抽象的でなければなりません。同時に、組織目標を満たす受け入れ可能な実装の範囲を十分に具体的に定義する必要があります。一般に、ポリシーは企業の暗号化戦略の基本的な特性を定義するため、テクノロジーに依存せず、変更されることもほとんどありません。

通常、暗号化ポリシーには以下が含まれますが、これらに限定されません。

- 企業が満たさなければならないあらゆる規制またはコンプライアンス制度
- データ暗号化に関するビジネス上の義務または期待
- 暗号化する必要があるデータのタイプ
- ハッシュやトークン化など、暗号化以外のデータ保護手法をいつ使用するかの基準

通常、CIO、CTO、CISOなどの組織の最高管理レベルが暗号化ポリシーを定義して承認します。

暗号化ポリシーを作成する際は、次の点を考慮します。

- 遵守すべきコンプライアンスおよび規制体制は、事業部門によって決まります。これらの体制により、データ暗号化の要件が決まります。新しい地域への事業拡大や製品提供の拡大に関する経営幹部レベルの決定は、データに適用される規制に影響する可能性があります。たとえば、銀行が顧客にクレジットカードを提供する場合、おそらくデータの暗号化が義務付けられている決済カード業界のデータセキュリティ基準（PCI-DSS）に準拠する必要があります。
- ポリシーでは、どのタイプのデータを暗号化する必要があるかを指定する必要があります。これは、コンプライアンス要件と企業のデータ処理目標によって異なります。たとえば、ポリシーによっては、企業が取得または所有するデータはすべて保存時に暗号化する必要があると定められている場合があります。
- 暗号化ポリシーは、内部のデータ分類基準と一致している必要があります。効果的な暗号化ポリシーを策定するには、メタデータレベルでデータカテゴリを決定する必要があります。たとえば、カテゴリには公開データ、内部データ、機密データ、秘密データ、顧客データが含まれる場合があります。
- どのデータを暗号化するか、どのデータをトークン化やハッシュなどの別の手法で保護すべきかを判断する方法の基準を含めてください。たとえば、ポリシーに、監査、トレース、またはアプリケーションログに送られる個人を特定できる情報（PII）はすべてトークン化する必要があると記載されている場合があります。

暗号化規格

標準はポリシーに基づいて作成されます。これらは対象範囲が狭く、実装のフレームワークとアーキテクチャを定義するのに役立ちます。たとえば、保管中のデータを暗号化することが組織のポリシーである場合、標準では必要な暗号化の種類が定義され、ポリシーの遵守方法に関する一般的な指示が示されます。

暗号化標準では一般的に以下が規定されています。

- 使用すべき暗号化の種類
- 暗号化キーの最小仕様
- 暗号化キーにアクセスできるのは誰か
- 暗号化キーを保存する場所
- 暗号化またはハッシュ技術を選択する際に適切な鍵強度を選択するための基準
- キーのローテーションの頻度

暗号化ポリシーを更新する必要はほとんどありませんが、暗号化標準は変更される場合があります。サイバーセキュリティ業界は、絶えず変化する脅威の状況に対応するために絶えず進化しています。そのため、企業データを可能な限り保護するためには、最新のテクノロジーとベストプラクティスを採用するように基準を変更する必要があります。

企業組織では、通常、副社長、取締役、またはデータスチュワードが暗号化標準を定義し、コンプライアンス責任者がそれらを確認して承認します。

組織で暗号化標準を定義および維持する際には、次のカテゴリの要素を考慮してください。

- コストとパフォーマンスに関する考慮事項
- キーアクセスコントロール
- 暗号化タイプ
- 暗号化キーの仕様
- キー保管場所

コストとパフォーマンスに関する考慮事項

保存データの暗号化標準を決定する際には、以下の運用上の要素を考慮してください。

- 利用可能なハードウェアリソースは、お客様の標準を大規模にサポートできる必要があります。
- 暗号化のコストは、キーの長さ、データ量、および暗号化の実行に必要な時間によって異なります。たとえば、対称暗号化と比較すると、非対称暗号化では使用するキーが長く、時間がかかります。
- エンタープライズアプリケーションのパフォーマンス要件を考慮してください。アプリケーションで低レイテンシーと高スループットが必要な場合は、対称暗号化を使用するとよいでしょう。

キーアクセスコントロール

最小権限の原則に基づいて、暗号化キーのアクセスコントロールポリシーを識別します。最小権限は、ユーザーが職務を遂行するために必要な最小限のアクセス権を付与するセキュリティ上のベストプラクティスです。標準では、次のようなアクセス制御ポリシーを定義してください。

- キー暗号化キーとデータキーを管理するロールを識別します。
- 主要な権限を定義し、役割にマッピングします。たとえば、誰が主要な管理者権限を持ち、誰が主要なユーザー権限を持っているかを定義します。キー管理者はキー暗号化キーを作成または変更でき、キーユーザーはデータを暗号化および復号化してデータキーを生成できます。

暗号化タイプ

標準で、どの暗号化タイプと機能が組織に適しているかを定義してください。

- 対称および非対称暗号化アルゴリズムの使用を記述します。詳細については、「よくある質問」セクションの「」対称暗号化が必要なのはどのような場合ですか？と非対称暗号化はどのような場合に必要ですか？「」を参照してください。
- エンベロープ暗号化を使用するかどうかを決定し、状況を定義します。詳細については、「よくある質問」エンベロープ暗号化はどのような場合に必要ですか？セクションのを参照してください。
- トークン化やハッシュなどの暗号化代替手段をいつ使用するかの基準を定義します。

暗号化キーの仕様

キーの強度やアルゴリズムなど、暗号化キーに必要な仕様を定義します。これらの仕様は、ポリシーで定義されている規制およびコンプライアンス体制に準拠している必要があります。次の仕様を定義することを検討してください。

- 対称暗号化タイプと非対称暗号化タイプの両方の最小キー強度とアルゴリズムを定義します。重要な強さの要因には、長さ、ランダム性、独自性などがあります。
- 新しいバージョンの暗号化アルゴリズムをいつ実装するかを定義します。たとえば、規格によっては、「リリースから 30 日以内にアルゴリズムの最新バージョンを実装する」、「常に最新リリースより 1 つ古いバージョンを使用する」と記載されている場合があります。
- 暗号化キーをローテーションする間隔を定義します。

キー保管場所

暗号化キーの保存場所を決定する際は、各自の基準で次の点を考慮してください。

- コンプライアンスや規制の要件によって、暗号化キーの保存場所が決まる場合があります。
- キーを一元的に保存するか、対応するデータと一緒に保存するかを決定します。詳細については、「よくある質問」暗号化キーを一元管理する必要があるのはなぜですか？セクションのを参照してください。
- 集中型ストレージを選択する場合は、キーをハードウェアセキュリティモジュール (HSM) などのエンタープライズ管理インフラストラクチャに保存するか、AWS Key Management Serviceなどのマネージドサービスプロバイダーに保存するかを決定してください。詳細については、「よくある

質問」ハードウェアセキュリティモジュール (HSM) は、どのような場合に使用すればよいですか? セクションのを参照してください。

暗号化フレームワーク

ここでいうフレームワークとは、暗号化標準やポリシーを変更するときに従う必要のある一連の標準的な操作手順を指します。フレームワークは、標準の実装に役立つ足場です。言葉を行動に変換するのに役立ちます。このフレームワークは、標準を定義する人々とそれを実装する人々を結び付けます。

フレームワークには通常、次のトピックが含まれます。

- データ分類
- 環境分類
- イベントとプロセスの変更

データ分類

データ分類は、暗号化戦略を作成する上で重要な役割を果たします。データ分類は、データの機密性に基づいてデータをカテゴリに割り当てるプロセスです。一般的なデータ分類カテゴリは、機密性の高い順に、公開、非公開、内部、機密、制限付きです。

暗号化フレームワークには、データ分類に関する次の情報が含まれている必要があります。

- 企業のデータ分類カテゴリ。
- データを適切なカテゴリに分類するために使用される分類基準。たとえば、会社の取引レシピは制限付きとして分類され、従業員の個人情報は機密情報として分類され、公式チャネルを介した従業員間の内部コミュニケーションは社内で行われる場合があります。
- カテゴリ間でデータを昇格および降格させるために使用されるプロセスです。
- 各データ分類カテゴリのアクセス基準。
- 各カテゴリに必要な暗号化キーの種類。

環境分類

企業には、開発、テスト、サンドボックス、プリプロダクション、本稼働などの複数の環境がある場合があります。環境ごとに異なる種類のデータが格納され、暗号化要件も異なります。

暗号化フレームワークには、環境に関する次の情報が含まれている必要があります。

- エンタープライズ環境を定義してください。
- 各環境の暗号化要件を定義します。たとえば、開発環境ではすべてのデータカテゴリに単一の暗号化キーを使用し、運用環境ではビジネスアプリケーションまたはデータ分類カテゴリごとに異なる暗号化キーを使用する場合があります。

イベントとプロセスの変更

暗号化標準は、最新のテクノロジー、ベストプラクティス、イノベーションに遅れずについていくことができるように、頻繁に変更される可能性があります。暗号化標準の改訂のきっかけとなる可能性のある一般的な変更イベントは次のとおりです。

- 暗号化キーの最小長の変更
- 暗号化アルゴリズムの強度の変化
- 暗号化キーにアクセスできるユーザーまたはアクセス方法の変更
- キーのローテーション間隔の変更
- キーの削除プロセスの変更
- キーストレージの場所またはポリシーの変更
- キーのバックアップと復元プロセスの変更

組織が暗号化標準またはポリシーの変更を管理、実装、伝達する準備を整えるために、暗号化フレームワークには次のものを含める必要があります。

- 変更管理プロセス — このプロセスの目的は、今後の変更を計画して準備することです。暗号化の標準やポリシーを変更する必要がある場合、この繰り返し可能でスケーラブルなプロセスにより、以下が定義されます。
  - 組織が変更の影響を評価する方法
  - 誰が変更を開始できるか
  - 変更を実施する責任者
  - 変更を承認する責任者
  - 必要に応じて組織がどのように変更をロールバックするか

- 変更の監査可能性とトレーサビリティプロセス — このプロセスは、メタデータレベルとデータレベルの両方で、組織がどのように変更を監査および追跡するかを定義します。以下の記録の保存方法とアクセス方法を定義する必要があります。
  - 何が変わったか
  - いつ変更されたか
  - 変更の開始、承認、および実施者

  たとえば、組織が暗号化キーの最小強度を変更した場合、元の要件と新しい要件、変更が有効になった時期、変更プロセスに誰が関与したかを判断できるはずです。
- 変更ロールアウトプロセス — このプロセスの目的は、変更を行うことを決定した後に、組織がどのように変更を実施するかを定義することです。このプロセスでは以下が定義されます。
  - 利害関係者は誰か
  - パイロットを完了すべきか、概念実証を完了すべきか
  - 変更の状況をいつどのように伝えるべきか
  - 必要に応じて変更をロールバックする方法。
  - 変更を実施した後の観察期間はどのくらいですか。
  - 変更に関するフィードバックの収集方法や有効性の評価方法など、変更の影響を監視するための観察プロセスの概要
- 廃棄プロセス — このプロセスの目的は、暗号化関連のリソースと情報の廃棄を組織がどのように処理するかを定義することです。実際の退職に関する指示と、退職に関するコミュニケーションプロセスが含まれています。

実装

この戦略では、アーキテクチャとは暗号化標準を技術的に実装することを指します。このセクションにはAWS のサービス、AWS Key Management Service(AWS KMS) やなどがAWS CloudHSM、data-at-rest ポリシーや標準に従って暗号化戦略を実装するのにどのように役立つかについての情報が含まれています。

AWS KMSは、ユーザーのデータを保護するために使用される、暗号化キーの作成と制御を容易にするマネージドサービスです。KMS キーは、サービスを暗号化しないままにしません。KMS キーを使用または管理するには、ユーザーが操作しAWS KMS、AWS のサービスその多くがと統合されていますAWS KMS。

AWS CloudHSMは、AWS環境内のハードウェアセキュリティモジュール (HSM) を作成および管理するための暗号化サービスです。HSM は、暗号化操作を処理し、暗号化キーを安全に保管するコンピューティングデバイスです。標準で FIPS 140-2 レベル 3 検証済みハードウェアを使用する必要がある場合、または標準で PKCS #11、Java 暗号化拡張 (JCE)、Microsoft Cryptong (CNG) などの業界標準の API の使用が規定されている場合は、を使用することを検討してくださいAWS CloudHSM。

AWS CloudHSMのカスタムキーストアとして設定できますAWS KMS。このソリューションでは、の利便性とサービス統合に加えて、AWS KMSAWS CloudHSMでクラスタを使用することによる制御とコンプライアンスの利点も兼ね備えていますAWS アカウント。詳細については、「カスタムキーストア (AWS KMSドキュメント)」を参照してください。

このドキュメントでは、AWS KMS機能を大まかに説明し、AWS KMSポリシーと標準にどのように対応できるかを説明します。

コスト、利便性、管理

AWS KMSには、さまざまな種類のキーが用意されています。所有または管理されているものもあればAWS、顧客によって作成および管理されているものもあります。重要事項とコスト上の考慮事項をどの程度管理したいかに応じて、次のオプションを選択できます。

- AWS所有キー —AWS これらのキーを所有および管理し、複数で使用されますAWS アカウント。AWS のサービスAWS一部は所有キーをサポートしています。これらのキーは無料でご利用いただけます。このキータイプにより、キーのライフサイクルとそのアクセスの管理にかかるコストと管理上のオーバーヘッドが軽減されます。このタイプのキーの詳細については、「AWS所有キー (AWS KMSドキュメント)」を参照してください。
- AWS管理キー —AWS のサービスAWS KMS がと統合されている場合、サービス内のリソースを保護するために、ユーザーに代わってこのタイプのキーを作成、管理、使用できます。これらのキーはで作成されAWS アカウント、AWS のサービス使用できるのはキーだけです。AWSマネージドキーの月額料金はかかりません。これらは、無料利用枠を超える量を使用した場合は有料になりますが、AWS のサービス一部のコストがカバーされます。ID ポリシーを使用してこれらのキーの表示と監査アクセスを制御できますが、AWSキーのライフサイクルは管理します。このタイプのキーの詳細については、AWSマネージドキー (AWS KMSドキュメント) を参照してください。AWS のサービスと統合されるものの包括的なリストについてはAWS KMS、「AWS のサービス統合 (AWSマーケティング)」を参照してください。
- 顧客管理キー — このタイプのキーは自分で作成、所有、管理でき、キーのライフサイクルを完全に制御できます。役割分担については、IDベースのポリシーとリソースベースのポリシーの両方を使用してキーへのアクセスを制御できます。自動キーローテーションを設定することもできます。カスタマーマネージドキーには月額料金がかかり、無料利用枠を超えると、使用料金もかかりま

す。このタイプのキーの詳細については、「カスタマー管理キー (AWS KMSドキュメント)」を参照してください。

キーストレージと使用方法の詳細については、「AWS Key Management Service価格 (AWSマーケティング)」を参照してください。

パフォーマンスと暗号化タイプ

標準で選択した暗号化タイプに基づいて、2 種類の KMS キーを使用できます。

- 対称 —AWS KMS key すべてのタイプが対称暗号化をサポートしています。カスタマー管理キーを暗号化する場合、AES-256-GCM による暗号化と復号化に単一強度のキーを使用できます。
- 非対称 — 顧客管理キーは非対称暗号化をサポートします。用途に応じて、さまざまな主な長所とアルゴリズムを選択できます。非対称キーは RSA を使用して暗号化および復号化でき、RSA または ECC を使用して操作に署名および検証できます。非対称キーアルゴリズムは本質的に役割を分離し、キー管理を簡素化します。で非対称暗号化を使用する場合AWS KMS、キーのローテーションや外部キーマテリアルのインポートなど、一部の操作はサポートされません。

AWS KMS対称キーと非対称キーがサポートする操作の詳細については、「キータイプリファレンス (AWS KMSドキュメント)」を参照してください。

エンベロープ暗号化

AWS KMSエンベロープ暗号化が組み込まれています。ではAWS KMS、データキーはプレーンテキスト形式または暗号化形式で生成します。暗号化されたデータキーは、KMS キーで暗号化されます。KMS キーは、AWS CloudHSMクラスターのカスタムキーストアに保存できます。エンベロープ暗号化のメリットの詳細については、「」を参照してくださいエンベロープ暗号化について。

キー保管場所

AWS KMSポリシーを使用してリソースへのアクセスを管理します。ポリシーは、誰がどのリソースにアクセスできるかを記述します。AWS Identity and Access Management(IAM) プリンシパルにアタッチされたポリシーは、アイデンティティベースのポリシーまたは IAM ポリシーと呼ばれます。他の種類のリソースにアタッチされたポリシーは、リソースポリシーと呼ばれます。 AWS KMSAWS KMS keysのリソースポリシーはキーポリシーと呼ばれます。KMS キーそれぞれに、キーポリシーがあります。

キーポリシーにより、暗号化キーを中央の場所に保存したり、データの近くに分散して保存したりする柔軟性が得られます。KMS キーをどこに保存するかを決めるときは、AWS KMS次の機能を考慮してくださいAWS アカウント。

- 単一リージョンのインフラストラクチャサポート — デフォルトでは、KMS キーはリージョン固有であり、AWS KMS暗号化されないままになることはありません。特定の地域のキーを制御するための厳しい要件が標準で定められている場合は、単一リージョンキーの使用を検討してください。
- マルチリージョンインフラストラクチャサポート —AWS KMS マルチリージョンキーと呼ばれる特殊用途のキータイプもサポートします。災害復旧では、AWS リージョンデータを複数に分けて保存するのが一般的です。マルチリージョンキーを使用すると、再暗号化せずにリージョン間でデータを転送でき、各リージョンで同じキーを使用しているかのようにデータを管理できます。この機能は、暗号化インフラストラクチャがアクティブ-アクティブ構成で複数のリージョンにまたがる必要がある標準で義務付けられている場合に非常に役立ちます。詳細については、「複数地域のキー」(AWS KMSドキュメント) を参照してください。
- 一元管理 — 標準でキーを一元的に保存する必要がある場合は、AWS KMSを使用してすべての暗号化キーを 1 つの場所に保存できますAWS アカウント。キーポリシーを使用して、同じリージョンの異なるアカウントにある他のアプリケーションへのアクセスを許可します。キー管理を一元化することで、キーライフサイクルとキーアクセス制御の管理にかかる管理費を削減できます。
- 外部キーマテリアル — 外部で生成されたキーマテリアルをにインポートできますAWS KMS。この機能は、単一リージョンおよびマルチリージョンの対称キーSupport されています。対称キーのマテリアルは外部で生成されるため、生成されたキーマテリアルを保護するのはユーザーの責任です。詳細については、インポートされたキーマテリアル (AWS KMSドキュメント) を参照してください。

アクセスコントロール

ではAWS KMS、キーポリシー、IAM ポリシー、権限というポリシーメカニズムを使用して、きめ細かなレベルのアクセス制御を実装できます。これらのコントロールを使用すると、管理者、データを暗号化できるキーユーザー、データを復号化できるキーユーザー、データを暗号化および復号化できるキーユーザーなどの役割に基づいて職務の分離を設定できます。詳細については、「認証とアクセスコントロール (AWS KMSドキュメント)」を参照してください。

監査とログ記録

AWS KMSは、AWS CloudTrail EventBridge ロギングとモニタリングを目的として Amazon と統合します。すべてのAWS KMS API CloudTrail 操作はログに記録され、監査可能です。Amazon CloudWatch、 EventBridge、を使用してカスタムモニタリングソリューションを設定し、通知と自

動修復を設定できます。AWS Lambda詳細については、「ロギングと監視 (AWS KMSドキュメント)」を参照してください。

よくある質問

このセクションでは、暗号化標準を定義するとき、または実装段階で暗号化インフラストラクチャを作成するときによく寄せられる質問に対する回答を示します。

対称暗号化が必要なのはどのような場合ですか?

対称暗号化は次の場合に使用します。

- 速度、コスト、および計算オーバーヘッドの削減が優先事項です。
- 大量のデータを暗号化する必要があります。
- 暗号化されたデータは、組織のネットワークの境界を越えることはありません。

非対称暗号化はどのような場合に必要ですか?

非対称暗号化は次のような場合に使用します。

- データを組織外で共有する必要があります。
- 規制やガバナンスにより、鍵の共有は禁止されています。
- 否認防止が必要です。(否認防止機能により、ユーザは以前の約束やアクションを拒否できなくなります)。
- 暗号化キーへのアクセスは、組織の役割に基づいて厳密に分離する必要があります。

エンベロープ暗号化はどのような場合に必要ですか?

暗号化ポリシーでキーローテーションが必要な場合は、エンベロープ暗号化をサポートして実装する必要があります。ガバナンスやコンプライアンス体制によっては、キーローテーションが必要な場合もあれば、ビジネスニーズを満たすためにポリシーによってキーローテーションが義務付けられている場合もあります。

ハードウェアセキュリティモジュール (HSM) は、どのような場合に使用すればよいですか?

ポリシーで以下への準拠が指定されている場合は、HSM が必要になることがあります。

- 連邦情報処理標準 (FIPS) 140-2 レベル 3 暗号化規格。詳細については、「FIPS 検証 (AWS CloudHSMドキュメント)」を参照してください。
- PKCS #11、Java 暗号化拡張機能 (JCE)、マイクロソフト暗号化 API: 次世代 (CNG) などの業界標準 API

暗号化キーを一元管理する必要があるのはなぜですか?

一元化されたキー管理の一般的な利点は次のとおりです。

- キーはさまざまな場所で使用および管理されるため、キーを再利用できるため、コストを削減できます。
- 暗号化キーへのアクセスをより細かく制御できます。
- キーを 1 つの場所に保存しておくと、標準が変更された場合にキーを簡単に表示、監査、更新できます。

保存中のデータには専用の暗号化インフラストラクチャを使用する必要がありますか?

次のいずれかが当てはまる場合、企業には暗号化インフラストラクチャが必要です。

- 企業は、公開データ以外のあらゆる分類のデータを処理および保存します。
- 企業は、従業員または顧客に関するデータを取得して保存します。
- 企業が PII データを処理します。
- 企業は、データの暗号化を必要とする規制やガバナンス体制に準拠している必要があります。
- 企業の経営幹部は、保存されているすべてのデータの暗号化を義務付けています。

保管中のデータの暗号化目標を達成するために、AWS KMS組織はどのように役立ちますか？

他の多くの機能に加えて、AWS Key Management Service次のことに役立ちます。

- エンベロープ暗号化を使用してください。
- キー管理とキー使用を分けるなど、暗号化キーへのアクセスを制御します。

- AWS リージョンAWS アカウント複数のおよびでキーを共有します。
- キー管理を一元化します。
- キーのローテーションの自動化と強制化

リソース

AWS のサービスドキュメント

- AWS KMS暗号の詳細
- AWS KMS デベロッパーガイド
  - AWS KMS の概念
  - 特殊用途キー
  - [Authentication and access control for AWS KMS] (の認証とアクセスコントロール)
  - のセキュリティAWS KMS
  - AWS のサービス使用方法AWS KMS
- AWS CloudHSM ユーザーガイド
- AWS暗号化サービスとツールガイド
  - 暗号化ツールまたはサービスの選択方法
  - 暗号化の概念

AWSマーケティング

- AWS KMS 料金表
- AWS KMS他との統合AWS のサービス

AWSWell-Architected フレームワーク

- 送信中のデータの保護
- 保存中のデータの保護

ハッシュとトークン化

- トークン化を使用してデータセキュリティを強化し、監査範囲を縮小する方法 (AWSブログ記事)
- 承認されたハッシュアルゴリズムを使用するアプリケーションに関する推奨事項 (NIST 出版物)

動画

- 暗号化の仕組みAWS
- 上のブロックストレージの保護AWS
- によるセキュリティ目標の達成AWS CloudHSM
- 実装のベストプラクティスAWS Key Management Service
- AWS暗号化サービスの詳細

ドキュメント履歴

このガイドは、このドキュメントの大きな変更点をまとめたものです。今後の更新に関する通知を受け取る場合は、RSS フィードをサブスクライブできます。

変更	説明	日付
初版出版	—	2022 年 9 月 15 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。集計関数の例には、 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、疑わしい 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他の環境 (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、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」インジケータを参照してください。 AWS

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

「変更データキャプチャ」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 ワークロードに負荷を与え、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
- 基盤 — 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、デジタル画像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、設定は想定した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 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 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する。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、生産現場の生産物が完成した製品に変換されます。

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、ツールの採用を推進し、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、変化の採用を加速し、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は人材アクセラレーションと呼ばれます。詳細については、 OCM ガイドを参照してください。

オリジンアクセスコントロール (OAC)

In CloudFront は、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ためのオプションです。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「 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 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」、「読み取り多数」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。承認されたユーザーは、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

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。