産業分野における IoT (IIoT) デジタルトランスフォーメーション戦略の構築

AWS 規範ガイダンス

AWS 規範ガイダンス: 産業分野における IoT (IIoT) デジタルトランスフォーメーション戦略の構築

Table of Contents

産業分野における IoT (IIoT) デジタルトランスフォーメーション戦略の構築

Salih Bakir、Vladi Salomon、Asim Kumar Sasmal (Amazon Web Services (AWS))

2022 年 6 月 (ドキュメント履歴)

産業分野における IoT (IIoT) とは、製造、エネルギー、自動車、ヘルスケア、ライフサイエンス、農業などの産業分野で、インターネットに接続されたセンサーやデバイスを使用することを指します。IIoT では、運用環境にある機器、機械、フィールドデバイスから遠隔測定データを収集できます。これらの環境は通常、産業規制、コンピューティング、ネットワーク、電力の制約、厳しい条件の影響を受けます。これらの課題のすべてが、IIoT ソリューションの設計を複雑にする要因となっています。

IIoT データやその他のエンタープライズ、IT、運用技術 (OT) データを使用して、運用の最適化、生産性の向上、可用性の向上など、さらなるビジネス価値を創出できます。「The age of analytics: Competing in a data-driven world」(McKinsey Global Institute の調査) によると、メーカーは IIoT データを活用して製品開発コストを最大 50% 削減、運用コストを最大 25% 削減、粗利益率を最大 33% 増加できるといいます。そのため、産業部門の多くの組織が、IIoT を使用してビジネス上の問題を解決するためのデジタルトランスフォーメーションジャーニーを始めています。

ターゲットを絞ったビジネス成果

このガイドは、IIoT ビジネス目標の特定からその実現まで、カスタマイズしたロードマップを作成するのに役立ちます。このガイドは、Amazon Web Services (AWS) の経験に基づくもので、Professional Services チームがお客様のパートナーとなり、IIoT デジタルトランスフォーメーションジャーニーを支援します。このドキュメントで説明する段階的アプローチを使用すると、次のことが可能になります。

- ビジネス目標、測定可能な主要業績評価指標 (KPI)、優先順位付けされたユースケースを特定できます。
- 現在のシステムやテクノロジーを評価し、チームのスキルを評価し、ギャップを特定できます。
- 反復可能で再利用可能なブループリントを実装して、大規模で迅速なデプロイを可能にします。ブループリントとは、デジタルトランスフォーメーションジャーニーで導入するエンドツーエンドの IIoT システムリファレンスアーキテクチャのことです。
- 組織を継続的なイノベーションに備えましょう。

対象者

このガイドは、IT/ビジネスエグゼクティブ、プログラム/プロジェクトマネージャー、アーキテクト、プロダクトオーナーのほか、運営責任者、プラントマネージャー、オペレーションマネージャーなど OT の意思決定者向けです。

IIoT デジタルトランスフォーメーションジャーニーを始めたばかりであっても、まだ道半ばであっても、このガイドで説明する段階的アプローチを使用して、それぞれのジャーニーに合わせてカスタマイズしたプランを作成したり、現在のプランのギャップを特定したりできます。

IIoT デジタルトランスフォーメーションジャーニーのフェーズ

AWS プロフェッショナルサービスは段階的なアプローチを使用して、IIoT デジタルトランスフォーメーションジャーニーの計画を立て、実現します。

- フェーズ 1: ビジネス目標の特定 — 対処すべきビジネスチャンスや問題を明確に特定し、優先順位を付けます。これらがプロセス全体の主要な推進要因あり、基盤でもあります。ビジネス目標は、トップダウンで組織の目標を共有し、野心的でありながら達成可能なものでなければなりません。一般的な IIoT デジタルトランスフォーメーションジャーニーは、1 つのプロジェクトだけではありません。成功のためには、大きく考え、小さなことから始めて、迅速にスケールするという、包括的なアプローチを推奨します。
- フェーズ 2: 現在の状態を評価する — 現在のエンタープライズ、ITシステム、OT システムを評価し、現在のチームのスキルセットを評価してギャップを特定します。長期的な成功が必要な分野のテクノロジー、トレーニング、またはリソースに投資します。成功するために、IT チームと OT チームが戦略的に連携していることを確認してください。
- フェーズ 3: ブループリントの定義 — ターゲットのリファレンスアーキテクチャとなるブループリントを定義します。これは産業施設全体で大規模に迅速にデプロイできるように、繰り返し可能かつ再利用可能なものでなければなりません。このブループリントがジャーニーの基盤であり、「大きく考え、小さく始めて、迅速にスケールする」というアプローチを採用することで、ビジネス目標を実現するのに役立ちます。
- フェーズ 4: 継続的なイノベーションの実現 — ブループリントが運用可能になったら、収集したデータを使用して、継続的な改善と改良の機会を特定します。既存のデータや新しいデータから得られるインサイトを最大化するソリューションを探し続けます。

[開始する前に]

IIoT デジタルトランスフォーメーションジャーニーへの長期的な投資には、経営幹部レベルのコミットメントが重要です。エグゼクティブスポンサーは、持続可能な戦略と歩調を合わせ、目標とする成果を達成するために忍耐強く取り組む必要があります。「The age of analytics: Competing in a data-driven world」(McKinsey Global Institute の調査) にはこう述べられています、「自社の変革を支援するために最高デジタル責任者を雇用したと答えたのは全回答者の 3 分の 1 未満でした。しかし、最高デジタル責任者を雇用した企業は、他の企業よりもデジタルトランスフォーメーションの成功を報告する可能性が 1.6 倍高くなっています」。そのため、ジャーニーを開始する前に、経営陣が投資戦

略、予算、スケジュールを理解し、足並みを揃えていることを確認してください。IT と OT の全体にわたり、すべてのビジネスステークホルダーがコミットしていることを確認します。

フェーズ 1: ビジネス目標の特定

The business case for the digital investment report (Econsultancy のウェブサイト) には、「明確な長期的ビジネスケースと ROI の欠如、取締役会レベルの理解と支援の欠如、デジタルマーコムが戦略的ではなく戦術的であるという認識はすべて、回答企業の少なくとも 4 分の 3 が、デジタル戦略に適したレベルの投資を確保する上での重大な課題と見ている」と記載されています。したがって、測定可能な KPI に基づいてビジネスチャンスを特定し、優先順位を付けることが重要です。

ビジネスケースは、製造、エネルギー、自動車、ヘルスケア、ライフサイエンス、農業などの産業分野によって異なる場合があることに注意してください。製造業に対するビジネス上の影響の例については、Hitachi Vantara Solution Brief の「Achieved Impact from Successful Digital Industrial Solutions」セクションを参照してください。

このフェーズでは、以下のことを行います。

1. ビジネス上の課題の特定
2. 測定可能な KPI を特定
3. ビジネス目標の特定
4. ユースケースの特定

このフェーズの成果として、すべてのステークホルダーが目標に向かって足並みを揃え、期待値を理解し、成功の測定方法を把握できるようになります。

ビジネス上の課題の特定

ビジネス目標を定義する最初のステップは、解決したい現在のビジネス上の課題と、IIoT デジタルトランスフォーメーションソリューションを環境に実装することで直面する可能性のある新しいビジネス課題のリストを作成することです。

IIoT デジタルトランスフォーメーションジャーニーの初期段階にある製造会社や工業会社でよく見られる、ビジネス上の課題を以下に示します。

- 従来の産業用機械や設備のスマート化を図ること
- 閉じ込められた生産データを抽出して新たな知見を得ること

- 無秩序な運用と根本原因分析のプロセスの遅れによる生産性の低下とダウンタイムの増加
- データサイロと資産のデジタル追跡の欠如による資産管理の課題
- プラント、ライン、機械レベルでの設備総合効率 (OEE)、スループット、サイクルタイムのモニタリングなど、さまざまな運用レベルにおけるほぼリアルタイムでのモニタリングの欠如

測定可能な KPI を特定

特定したビジネス上の課題に基づいて、この問題をうまく解決できたかどうか、どのように評価すればよいのか? と自問するところから始めます。この質問に答えることで、データ主導型のアプローチでソリューションの成功を評価できるようになります。

ジャーニーの成功を測るために使用する KPI を決定し、それが測定可能なものであることを確認します。以下は、さまざまな産業分野に適用されている KPI の例です。

- 設備総合効率 (OEE) または類似する KPI の改善率 (%)
- 運用コストの削減率 (%)
- オンプレミスと比較して、クラウドのストレージとコンピューティングのコスト削減率 (%)
- プロアクティブなモニタリングとメンテナンスによる、予定外のダウンタイムの削減率 (%)
- 需要予測と在庫管理における精度 (%)
- ビジネスユーザーがビジネスインテリジェンス (BI) レポートを作成する際に確認したレイテンシーの削減率 (%)
- 履歴データを機械学習などの高度な分析に利用できるようになるまでの時間の短縮率 (%)
- コンピューティングとストレージのスケーリングに要する時間の削減率 (%)
- システム稼働時間の増加率 (%)
- 生産性の向上率 (%)
- ダウンタイムの削減率 (%)

ビジネス目標の特定

解決したいビジネス上の課題を特定し、成功を測定する方法を決定したら、次はビジネス目標を定義できます。こうした目標を立てることで、なぜこの問題は解決する価値があるのか? この問題を解決することで利益を得るのは誰か? といった質問に答えられるようになります。現在の状態の KPI を、特定のビジネス目標に対するターゲット状態の KPI と比較するなど、成功を測定するためのデータ主導型の戦略を決定します。

使用したい各指標や KPI について、ビジネス目標を測定可能なターゲット値で言い換えます。例えば、ビジネス上の課題が、手動の検出プロセスにより製品 1 は頻繁に在庫切れになる、というもので、測定基準が、問題を検出するまでのレイテンシー短縮率であるとすると、ビジネス目標としては、製品 1 の在庫切れの可能性を特定する際のレイテンシーを 95% 削減する、というものになるかもしれません。

ビジネス目標に優先順位を付けることで、チームがリソース割り当ての優先順位を決める方法を明確に理解できるようになります。

ユースケースの特定

ビジネス目標を定義したら、次はユースケースに集中できます。ユースケースはエンドユーザーとシステムとのやりとりを正確に定義し、それに基づいて期待されるビジネス成果を自動的に生み出す方法を決定します。ブループリントを構築する際には、ユースケースが主な要件となります。

それぞれのユースケースは、次に挙げる 4 つの重要な要素で構成されている必要があります。

- システムと対話する 1 人以上のエンドユーザーペルソナ
- 各ペルソナの目標
- ペルソナが経験したとおりに、実装したいシステムアクション
- ペルソナが経験したシステムアクションの期待される結果

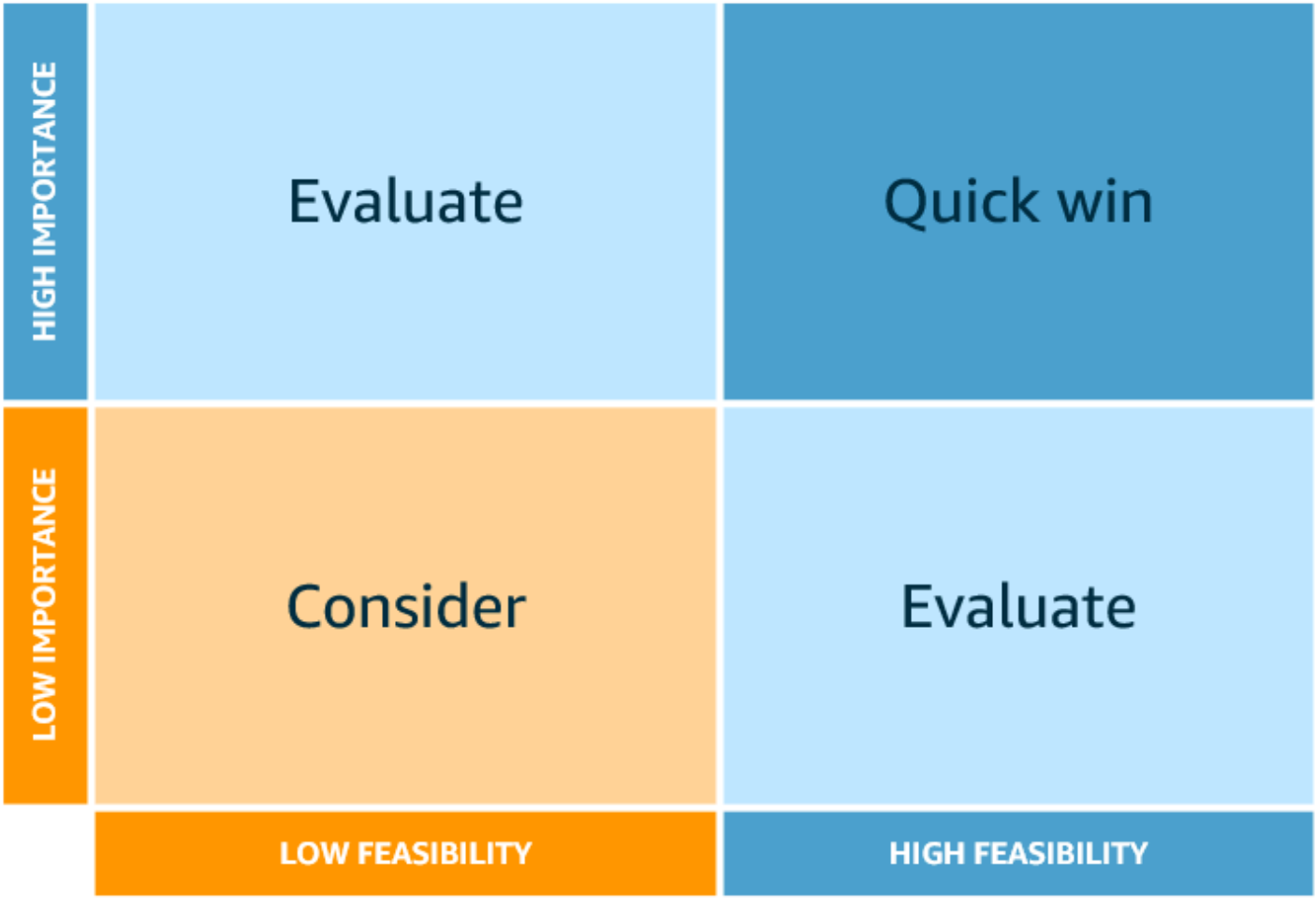
製品 1 の在庫切れの状況を特定するためのレイテンシーを 95% 削減する、というビジネス目標の例を使用すると、この目標のユースケースの例は以下のようになります。

- ペルソナ — ビジネスアナリスト
- ゴール — トレンド分析を使用して、製品 1 の在庫切れ状況を数分以内に推定します。
- アクション — BI レポートツールを使用して、傾向を示すレポートを生成します。
- 結果 — 新しいソリューションでは、以前の手動プロセスと比較して、在庫切れの状況を特定する際のレイテンシーが 95% 短縮されているはずです。

ユースケースのリストを作成したら、各ユースケースの重要性と実現可能性に基づいてステークホルダーと評価します。重要性とは、投資収益率 (ROI) など、ユースケースから得られると予想される価値のことで、実現可能性とは、実装のしやすさのことです。次のようなテーブルを作成し、各ユースケースの重要性と実現可能性についてステークホルダーに投票してもらいます。例えば、次のテーブルのユースケース 1 は、重要度が高い 4 票、重要度が低い 3 票を獲得しています。過半数の投票は、このユースケースの重要性が高いことを示しています。

	重要性		実現可能性		多数決票	
	高い	低	高い	低	重要性	実現可能性
ユースケース 1	4	3	5	2	高い	高
ユースケース 2	5	2	1	6	高	低
ユースケース 3	1	6	3	4	低	低

次に、投票結果を使用してユースケースに優先順位を付けます。2 つとも高評価を獲得したユースケースは、クイックウィンとみなされます。高評価と低評価が 1 つずつあるユースケースを評価カテゴリに、2 つとも低評価だったユースケースを検討カテゴリに分類します。次のテーブルは、この分類を視覚化するために使用できるクアドラントチャートを示しています。



クイックウィンのユースケースに優先順位を付け、依存関係を確認します。ジャーニーを完了したらクイックウィンから始め、進行するにつれて、予算とスケジュールに基づいて、評価カテゴリと検討カテゴリにユースケースを追加できます。

フェーズ 2: 現在の状態を評価する

IIoT デジタルトランスフォーメーションジャーニーの全行程には、IIoT 固有のデバイスや戦略だけでなく、それらの IIoT 資産を IT や OT インフラストラクチャ、運用ペルソナとどのように統合するかを包括的に検討する必要があります。ユーザーのインフラストラクチャはオンプレミス (ローカル)、もしくはオンプレミスとクラウドのハイブリッドインフラストラクチャである可能性があります。インフラストラクチャをクラウドに移行することで、クラウドネイティブの機能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ることができます。

このフェーズでは、以下のことを行います。

- 人と文化に焦点を当てる

- 現在のシステムとテクノロジースタックをよく調べる
- その他の重要な考慮事項を確認します。

AWS プロフェッショナルサービスは、他の のお客様にtried-and-tested一連の規範的なサービスを使用します。現在の状態を評価し、目標とする状態への段階的なロードマップを構築するお手伝いをします。

人と文化に焦点を当てる

重要な課題の 1 つは、IIoT デジタルトランスフォーメーションを実現し維持するための適切なチームスキルセットがないことです。成功に導くには、チームのスキルを高め、新しい役割を創出し、新しい人材を採用する必要があります。「Unlocking success in digital transformations」(McKinsey & Companyの調査レポート) は、「デジタル人材に適切な金額を投資したと回答した組織は、デジタルトランスフォーメーションが成功する可能性が 3 倍以上高くなる」と述べています。現在のチームのスキルを評価し、それに応じて行動を起こすために、以下のトピックを検討することを推奨します。

- クラウドテクノロジースタックの専門知識
- 以下の主要な技術スキルセット
  - IIoT
  - 機械学習 (ML)
  - データ分析ツールと手法
  - データレイク
  - SQL/NoSQL データベースやデータウェアハウスなど、オンライン分析処理 (OLAP) およびオンライントランザクション処理 (OLTP) システム
  - ビジネスインテリジェンスツール
  - リアルタイムモニタリングツール
  - フロントエンドとバックエンドを含むウェブアプリケーション開発
  - Linux などのオペレーティングシステム
  - Java、Python、JavaScript などのプログラミング言語
- ソフトウェア製品およびソリューションを構築するためのリソースには、以下が含まれます。
  - ビジネスアナリスト
  - プロダクトオーナー
  - プロジェクトマネージャー

  - UX/UI デザイナー
  - ソフトウェアアーキテクト
  - データアーキテクト
  - IoT アーキテクト
  - ソフトウェア開発者
  - ソフトウェアテストおよび自動化エンジニア
  - 開発運用 (DevOps) エンジニア
  - データサイエンティスト
  - 加工技術者、生産技術者、プラントマネージャー、ラインマネージャーなどの OT 対象分野の専門家 (SME)
- チームはアジャイルの原則とプラクティスに従って規模と組織化を行います
- 長期的および短期的なアクセラレーションとトレーニングのパートナー

もう 1 つの重要な点は、デジタルトランスフォーメーションを受け入れ、それを推進する革新的な文化を持つことです。なぜなら、正しい戦略、プロセス、ツールが整っていても、組織文化がイノベーションと導入を促さなければ、デジタルトランスフォーメーションが成功する可能性は低いからです。組織でのデジタルトランスフォーメーションの導入を促すために、以下の戦略を検討します。

- North Star のビジョン、価値観、原則を掲げる (詳細については、North Star ビジョン を参照してください)
- 上級管理職のサポートを受ける
- 業務の中断を最小限に抑えるロードマップを用意する
- 起業家精神を育み、失敗を受け入れる
- データ主導型で顧客重視の目標を掲げる
- アジャイルなプロセスとツールを導入する
- デジタルトランスフォーメーションを提唱する個人を評価し、イニシアチブの主導や参加の機会を提供する
- 従業員をイニシアチブに参加させる
- チームの自主性と柔軟性を高める
- チームワーク、コミュニケーション、透明性を促す
- 強力で迅速なフィードバックメカニズムを確立する

現在のシステムとテクノロジースタックをよく調べる

既存のシステムの技術的能力によって、将来のシステムアーキテクチャの範囲が決まります。そのため、IT と OT のインフラストラクチャを詳しく調べて、現在の技術的能力を理解する必要があります。

現在のエッジインフラストラクチャの機能を評価するには、以下の点を考慮してください。

- 現在のエッジアーキテクチャ
- 既存の IoT または IIoT システムまたはソリューションとその機能
- 記述的分析、予測分析、異常検出、予知保全と予防保全、ほぼリアルタイムのダッシュボード、BI レポートなど、現在のデータ分析と機械学習のユースケース
- 既存のソリューションの規模と将来の要件
- データを取り込むためのデータソースとその機能。これには以下が含まれます。
  - センサー、アクチュエーター、プログラマブルロジックコントローラ (PLC)、ゲートウェイ、OPC Unified Architecture (OPC UA) サーバーなどのデバイスやツール
  - これらのデバイスやツールでサポートされているプロトコル (Modbus、BACnet、MQTT、OPC UA など)
  - テレメトリの頻度、一般的なメッセージのサイズ、フォーマット、ボリュームなどのデータ仕様
- OT と IT ネットワークを明確に分離するためのネットワークインフラストラクチャ
- イーサネット、Wi-Fi、LoRaWAN、5G などのネットワーク接続
- 既存のヒストリアンとデータストレージシステム
- 既存のクラウド接続オプション

現在のクラウドインフラストラクチャの機能を評価するには、次の点を考慮してください。

- 現在のクラウドアーキテクチャ
- データレイク
- データ分析
- データ変換
- データサービスレイヤー
- データモニタリングと BI
- 機械学習
- ウェブアプリケーション

その他の重要な考慮事項を確認します。

インフラストラクチャに関する考慮事項に加えて、セキュリティ、コンプライアンス、リスク管理、ガバナンス、運用上の要素もあり、現在の状態を評価する際に考慮する必要があります。以下のトピックを詳細に評価して、これらの考慮事項の一部に対処します。

- 脅威を評価し軽減する情報セキュリティ戦略。
- システムの目標復旧時間 (RTO) や目標復旧時点 (RPO) などの高可用性要件。
- データガバナンスとアクセスコントロール。
- システムのアイデンティティとアクセス管理。
- データ保持ポリシー。
- データ分類と気密性。
- 保管中と転送中のデータ暗号化。
- 機密データの処理と保存に関するコンプライアンス要件と規制要件は重要です。これには、EU 一般データ保護規則 (GDPR)、個人を特定できる情報 (PII)、医療保険の相互運用性と説明責任に関する法律 (HIPAA) などの規制が含まれます。
- ダウンストリームのデータ消費とアプリケーションに関するサービスレベルアグリーメント (SLA)。
- ビジネスリスク管理。
- 資産とデバイスのライフサイクル管理。

フェーズ 3: ブループリントの定義

前のフェーズで行った現状の評価に基づいて、ブループリントの作成を開始できます。ブループリントとは、デジタルトランスフォーメーションジャーニーで導入するエンドツーエンドの IIoT システムリファレンスアーキテクチャのことです。IIoT デジタル化のジャーニーの基盤となり、ビジネス目標の実現を後押しします。ブループリント:

- North Star ビジョン によって導かれます
- 成功するソリューションフレームワークの核となる基本理念に従います
- 繰り返し可能で再利用可能なビルディングブロックから構成されています

ブループリントの特定の部分の価値と実現可能性を実証するために、簡単な概念実証が必要な場合もあります。

North Star ビジョン

ブループリントは North Star ビジョンに基づいて作成する必要があります。North Star ビジョンとは、ビジネス上の意思決定の方向性を示す、明確で簡潔かつ長期的な目標です。North Star ビジョンがない場合は、大きく考えて作成してください。このビジョンの実現には、通常 3～5 年かかります。このビジョンを達成するには、小規模から始めて迅速にスケールすることが成功の鍵です。

ソリューションフレームワークを成功に導くための基本理念

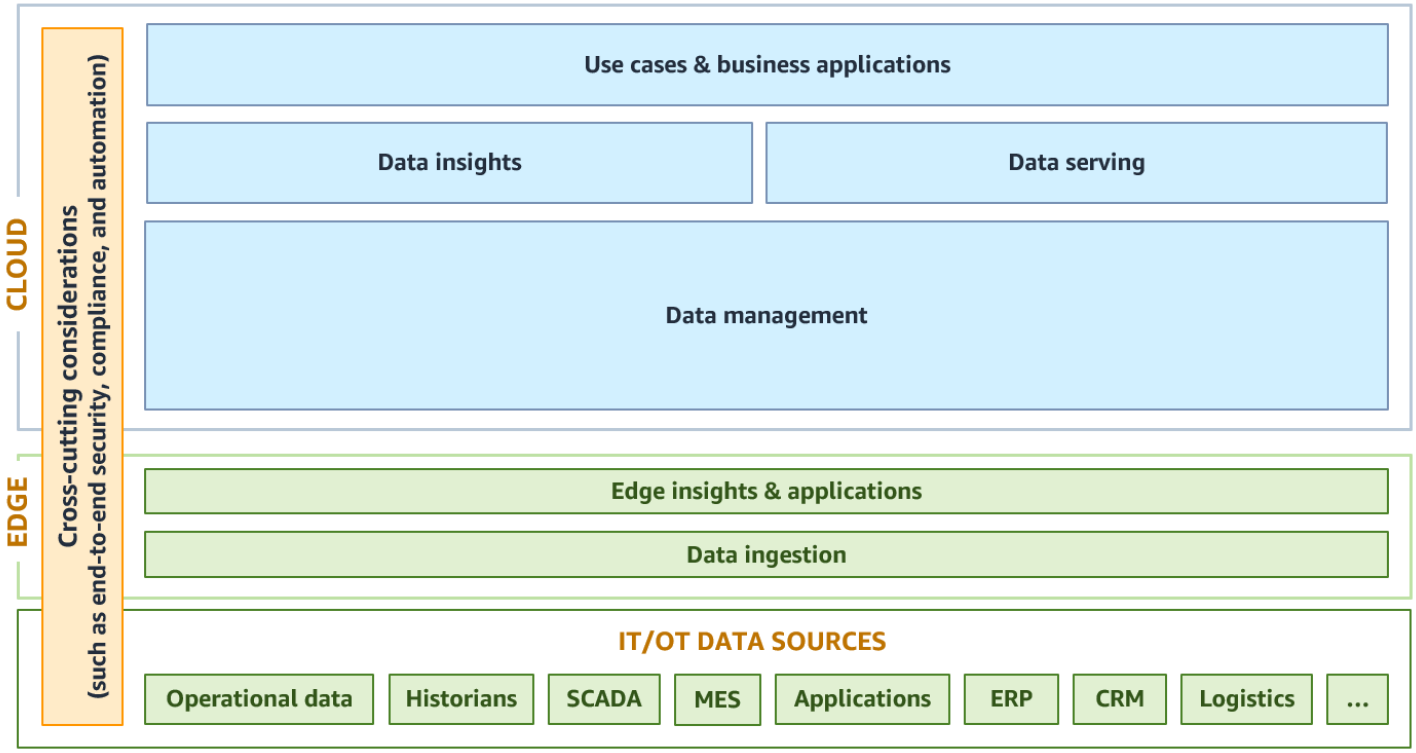
ブループリントに IT と OT の統合データバックボーンを構築するには、機能的なアーキテクチャが必要です。これまでの経験をもとに、ソリューションフレームワークの基本理念として次の 3 つを特定しました。

- インサイトを最大化する
  - データへのアクセスを民主化することで多様なインサイトが得られ、SKU マージンの最適化などビジネス価値が高まります。
  - リアルタイムまたは過去の運用データに対して記述的分析を行うことで、KPI のモニタリング、傾向の特定、改善の余地のある分野の特定ができ、対策を講じることができます。
  - データに対して診断分析を行うことで、運用上のイベントの根本原因を特定できます。
  - データに対して予測分析を行うことで、ビジネスや運用における将来の出来事を予測できます。
  - データに対して処方的分析を行うと、記述的分析と予測分析の結果に基づいて、特定の問題を解決するための複数のソリューションが提案されます。
- 技術的負債を最小限に抑える
  - 既存の主要な IT/OT システムとシームレスに統合できるため、一時的なソリューションが不要になります。
  - デプロイパイプラインを自動化することで、運用から手動プロセスを排除できます。
  - ツールを標準化することで、ツールや特注アプリケーションの拡散を防ぐことができます。
  - 一元管理サービスを使用して、標準化された設定を環境全体にデプロイすることで、ローカルサイトで非標準的かつ潜在的に問題となる設定が使用されるのを防ぎます。
  - インフラストラクチャを自動で、または反復可能なタスクのために最小限の介入で更新およびデプロイするためのパターンを作成します。例としては、オペレーティングシステムの更新、デバイス証明書の定期的な更新、パッチのインストール、データストレージの拡張などがあります。
  - 複数のサイトにまたがる大規模な本番稼働環境への迅速なデプロイを可能にする、反復可能で再利用可能なパターンの設計と実装を行います。
- モジュール式で将来への対応性を確保するブループリント

- 既存の IT/OT システムやインフラストラクチャとの相互運用性を考慮した設計。
- モジュール性を考慮した設計により、小規模から始めて迅速にスケールし、新しいコンポーネントを繰り返し追加し、ユースケースに最適なオプションを選択することができます。
- 既存の (ブラウンフィールド) と新規 (グリーンフィールド) インフラストラクチャを使用した柔軟性のある設計。

繰り返し可能で再利用可能なビルディングブロック

IIoT デジタルトランスフォーメーションジャーニーのビルディングブロックには、ブループリントを構成するさまざまな機能層、考慮事項、ユースケースがあります。以下の図は、ブループリントの大まかな構成要素である、高レベルで繰り返し可能かつ再利用可能な機能的ビルディングブロックを示しています。



ブループリントのレイヤーには次のようなものがあります。

- データインジェスト — このエッジレイヤーは、オンプレミスインフラストラクチャまたはクラウド環境のさまざまなソースからデータを収集します。一般的な IT/OT データソースには、監視制御およびデータ収集 (SCADA) システム、分散制御システム (DCS)、PLC、二次センサー、製造実行システム (MES)、Software as a Service (SaaS)、レガシーアプリケーション、エンタープライ

ズリソースプランニング (ERP) システム、顧客関係管理 (CRM) システム、さまざまなサプライチェーンシステム、およびデータヒストリアンからの遠隔測定データが含まれます。

- エッジインサイトとアプリケーション — ユースケースによっては、このエッジレイヤーのデプロイが必要になる場合があります。このレイヤーは、アーキテクチャの低レイテンシー要件やデータレジデンシー要件への対応、クラウドから切り離された状態での生産継続のサポート、エッジでのイノベーションの実現に使用されます。
- データ管理 — このレイヤーは、次のような一般的なデータ管理機能のさまざまな側面を担当します。
  - ガバナンスのために IT/OT リソースのセマンティックデータモデル (SDM) を構築および管理します。セマンティックデータモデルを使用してマシンデータにコンテキストを追加すると、プロセスやマシンモデリングのダウンストリーム分析に役立ちます。
  - 収集したデータをデータインジェストレイヤーに保存します。このレイヤーに保存されたデータは、処理やローカルインサイトの提供、およびクラウドから切断された状態でのストアアンドフォワード機能の提供に使用します。
  - データ統合、データ正規化、データ強化、データ品質、データ検出、データカタログ、検索など、エンドユーザーのさまざまな消費ニーズを満たすようにクラウドでデータを処理します。
  - 外部の消費者にビジネスインサイトを提供する柔軟なデータ消費サービスを可能にします。
- データインサイト — このクラウドレイヤーは、ほぼリアルタイムの KPI ダッシュボードなどの単純なものから、予知保全、需要予測、データ管理レイヤーの柔軟なデータ消費サービスを利用した在庫管理などの高度なものまで、さまざまなビジネスインサイトに使用されます。
- データ提供 — このクラウドレイヤーは、OT ペルソナ、データサイエンティスト、データエンジニア、データアナリストなど、さまざまなエンドユーザーのデータへのアクセスを民主化するために使用されます。このレイヤーは、データを他のエンタープライズのシステムやサードパーティのソリューションにシームレスに提供し、ユースケースやビジネスアプリケーションを実現します。
- ユースケースとビジネスアプリケーション — これはアーキテクチャの最上位層です。このクラウドレイヤーには、ビジネスユースケースに対応するビジネスアプリケーションとツールが含まれています。必要に応じて、このレイヤーのアプリケーションとツールは、サポートレイヤーのデータとインサイトにアクセスします。
- 分野横断的な考慮事項 — このレイヤーには、データソース、エッジ、クラウドに適用される機能以外の重要な要件が含まれています。このレイヤーには、エンドツーエンドのセキュリティ、設定管理、ログ記録、コンプライアンス、規制要件など、必須の要素が含まれます。このレイヤーは、アーキテクチャを安全かつ効率的に運用するのに役立つもので、パフォーマンスの向上、コストの削減、サイト間での大規模で迅速なデプロイを可能にする自動化機能の利用を可能にします。

この統合データソリューションを構築するには、ここで説明したものと同様の統合機能アーキテクチャを使用することを推奨します。この包括的なアプローチが、大きく考え、小規模から始めて、迅速にスケールするのを後押しします。デジタルトランスフォーメーションジャーニー全体を一度に行い、その道のりをありえないほど困難にするよりも、ビジネス成果の達成に役立つ小規模な成果物を繰り返し作り続けるほうが賢明です。こうしたビルディングブロックの一部を、現在すでに導入しているかもしれません。その場合は、それらを再利用することができます。

AWS IDP ソリューションの提供

AWS プロフェッショナルサービスは、tried-and-testedアプローチである産業データプラットフォーム (IDP) を使用して、Industry AWS 4.0 (スマートマニュファクチャリング、スマートファクトリー、スマート産業とも呼ばれます) の成功のための柔軟で拡張可能な統合データソリューションを検出、設計、実装します。 AWS IDP は、次のような一般的なユースケースのカタログに対処します。

- 設備総合効率 (OEE)、スループット、生産量、サイクルタイムなど、生産と資産の最適化に関する運用上および実行可能な KPI
- 予測品質を実現する品質管理と欠陥管理の自動化ソリューション
- ダウンタイムや壊滅的な設備故障を低減する予知保全
- エネルギーの最適化と二酸化炭素排出量の削減により、持続可能な製造を実現
- 在庫管理、需要予測、追跡を含むサプライチェーンの最適化

ブループリントアーキテクチャは、ユースケース、現在の状態の評価、特定したギャップによって異なる場合があります。ブループリントで使用できる関連 AWS サービスの詳細については、AWS「産業データプラットフォーム (IDP) リファレンスアーキテクチャ」を参照してください。

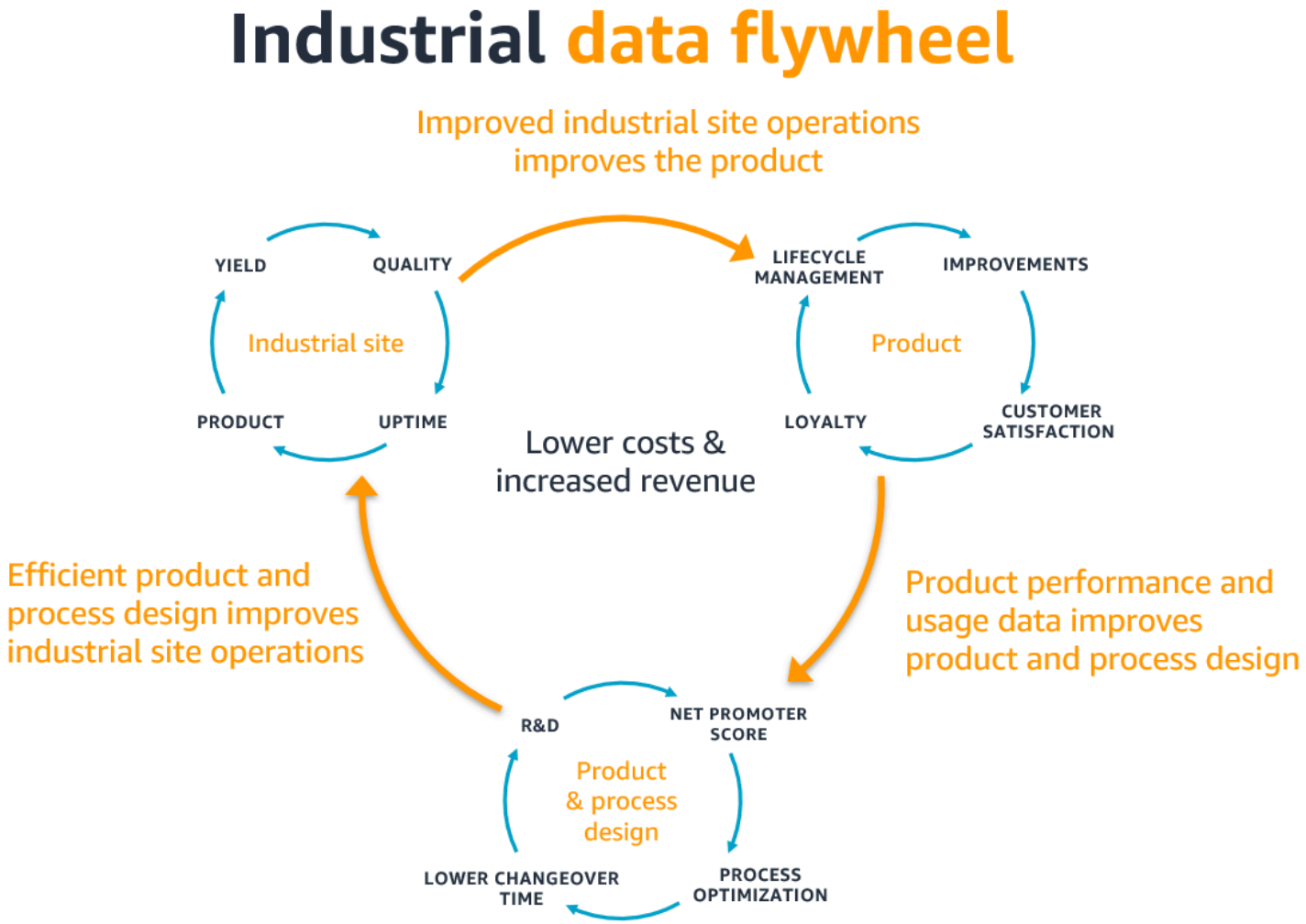
フェーズ 4: 継続的なイノベーションの実現

IIoT デジタルトランスフォーメーションの取り組みは、単一のプロジェクトではなく、ジャーニーとして考えることを推奨します。ビジネス KPI を定義し、組織を支援し、必要なスキルセットを確立し、ブループリントを構築したら、イノベーションのペースを速め、ビジネス全体で構築と拡大の機会をさらに探ります。ブループリントが実行されれば、より透明性が高く、データ主導型のビジネスになり、広範囲にわたるモニタリングと追跡が可能になります。

IIoT データを使用して、課題や機会を特定できます。さらに、イノベーションを推進するためには、常に測定可能なビジネス目標から始めることが不可欠です。そうすれば、ブループリントを拡張し、それをユースケースで裏付けることができるようになります。また、現在のビジネスモデルを評価

し、それを進化させて新しいビジネスチャンスを開拓し、競争力を高めることも重要です。例えば、製品の販売から付加価値サービスの販売にシフトできます。IIoT 機能では製品を広範囲に制御できるため、顧客の要求に基づいて製品の機能を拡張または制限し、より競争力のある価格で実現できます。

最後に、 AWS Professional Services は、Amazon フライホイール (YouTube ビデオ) と同様に、イノベーションの好循環を可能にする主要な要素を定義することで、独自のデータフライホイールを構築するのに役立ちます。 YouTube 次の画像はフライホイールの例です。



結論と次のステップ

最新の産業革命である IIoT デジタルトランスフォーメーションは、あらゆる規模のあらゆる業界のビジネスに新たな可能性を切り開いています。IIoT データを活用することで、ビジネス上の問題を解決し、新しい機会を創出できます。この IIoT ジャーニーを取り入れるビジネスでは、インサイトと生産性の向上によるメリットをすぐに実感することになります。

しかし、IIoT デジタルトランスフォーメーションにおける最大の課題は、どこから始めればよいのかわからないことと、確固たるビジネス目標を定義していないことです。ビジネス目標、成功の測定に使用する KPI、North Star ビジョンのブループリントを定義することで、ジャーニーに体系的なアプローチを導入できます。現在の状況を評価してギャップを把握し、そのギャップを埋めるためのブループリントを構築してから、継続的なイノベーションに注力できます。

このガイドでは、IIoT の段階的なデジタルトランスフォーメーションジャーニーについて説明しています。 AWS プロフェッショナルサービスの経験上、この段階的なアプローチは効果的で成功しています。 AWS プロフェッショナルサービスの支援を受けてジャーニーを加速したい場合は、お問い合わせフォームに記入してください。

お客様の成功のために必要な場合、 AWS Professional Services は当社の幅広い とも連携します AWS Partner Network。詳細については、AWS IoT Competency Partners および AWS Marketplace を参照してください。

AWS が運用目標の達成にどのように役立つかの詳細については、「」を参照してくださいリソース。

リソース

顧客事例

- Yara と AWS が、Crop™ 本番稼働システムをデジタル化
- の Volkswagen グループ AWS
- Coca-Cola İçecek が運用パフォーマンスを向上
- How Genie (a Terex brand) improved paint quality

AWS リソース

- AWS 産業モノのインターネット
- AWS 産業用データプラットフォーム (IDP)
- AWS 業界向け
- AWS 移行促進プログラム (MAP)
- AWS クラウド導入フレームワーク (AWS CAF)
- デジタルツインによる産業オペレーションの最適化 (AWS オンライン Tech Talks ビデオ)
- 産業 IoT ソリューションの 10 のセキュリティゴールデンルール (AWS ブログ記事)

ホワイトペーパー

- 「製造トランスフォーメーション: クラウドへのジャーニー」(AWS ホワイトペーパー)
- Enabling Manufacturing Innovation Through the Use of Cloud (IDC ホワイトペーパー)
- Mastering the Industrial Internet of Things (IIoT) (Roland Berger ホワイトペーパー)

ドキュメント履歴

以下の表は、本ガイドの重要な変更点について説明したものです。今後の更新に関する通知を受け取る場合は、RSS フィード をサブスクライブできます。

変更	説明	日付
初版発行	—	2022 年 6 月 20 日

AWS 規範ガイダンスの用語集

以下は、 AWS 規範ガイダンスによって提供される戦略、ガイド、パターンで一般的に使用される用語です。エントリを提案するには、用語集の最後のフィードバックの提供リンクを使用します。

数字

7 Rs

アプリケーションをクラウドに移行するための 7 つの一般的な移行戦略。これらの戦略は、ガートナーが 2011 年に特定した 5 Rs に基づいて構築され、以下で構成されています。

- リファクタリング/アーキテクチャの再設計 — クラウドネイティブ特徴を最大限に活用して、俊敏性、パフォーマンス、スケーラビリティを向上させ、アプリケーションを移動させ、アーキテクチャを変更します。これには、通常、オペレーティングシステムとデータベースの移植が含まれます。例: オンプレミスの Oracle データベースを Amazon Aurora PostgreSQL 互換エディションに移行します。
- リプラットフォーム (リフトアンドリシェイプ) — アプリケーションをクラウドに移行し、クラウド機能を活用するための最適化レベルを導入します。例: 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: カスタマーリレーションシップ管理 (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。オンプレミスプラットフォームから同じプラットフォームのクラウドサービスにサーバーを移行します。例: Microsoft Hyper-Vアプリケーションを に移行します AWS。
- 保持 (再アクセス) — アプリケーションをお客様のソース環境で保持します。これには、主要なリファクタリングを必要とするアプリケーションや、お客様がその作業を後日まで延期したいアプリケーション、およびそれらを移行するためのビジネス上の正当性がないため、お客様が保持するレガシーアプリケーションなどがあります。

- 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

アトミック性、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。より柔軟ですが、アクティブ/パッシブ移行よりも多くの作業が必要です。

アクティブ - パッシブ移行

ソースデータベースとターゲットデータベースが同期されるデータベース移行方法。ただし、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、ソースデータベースのみ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します。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

行のグループで動作し、グループの単一の戻り値を計算する SQL 関数。集計関数の例としては、 SUMや などがありますMAX。

AI

「人工知能」を参照してください。

AIOps

「人工知能オペレーション」を参照してください。

匿名化

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

アンチパターン

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

アプリケーションコントロール

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

アプリケーションポートフォリオ

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

人工知能 (AI)

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

AI オペレーション (AIOps)

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

非対称暗号化

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

原子性、一貫性、分離性、耐久性 (ACID)

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

属性ベースのアクセス制御 (ABAC)

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

信頼できるデータソース

最も信頼性のある情報源とされるデータのプライマリーバージョンを保存する場所。匿名化、編集、仮名化など、データを処理または変更する目的で、信頼できるデータソースから他の場所にデータをコピーすることができます。

アベイラビリティーゾーン

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

AWS クラウド導入フレームワーク (AWS CAF)

組織がクラウドへの移行を成功させるための効率的で効果的な計画を立て AWS るための、 のガイドラインとベストプラクティスのフレームワークです。 AWS CAF は、ビジネス、人材、ガバナンス、プラットフォーム、セキュリティ、運用という 6 つの重点分野にガイダンスを整理しています。ビジネス、人材、ガバナンスの観点では、ビジネススキルとプロセスに重点を置き、プラットフォーム、セキュリティ、オペレーションの視点は技術的なスキルとプロセスに焦点を当てています。例えば、人材の観点では、人事 (HR)、人材派遣機能、および人材管理を扱うステークホルダーを対象としています。この観点から、 AWS CAF は、クラウド導入を成功させるための組織の準備に役立つ人材開発、トレーニング、コミュニケーションのためのガイダンスを提供します。詳細については、AWS CAF ウェブサイト と AWS CAF のホワイトペーパー を参照してください。

AWS ワークロード認定フレームワーク (AWS WQF)

データベース移行ワークロードを評価し、移行戦略を推奨し、作業見積もりを提供するツール。AWS WQF は AWS Schema Conversion Tool （ AWS SCT) に含まれています。データベーススキーマとコードオブジェクト、アプリケーションコード、依存関係、およびパフォーマンス特性を分析し、評価レポートを提供します。

B

不正なボット

個人や組織を混乱させたり、損害を与えたりすることを意図したボット。

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 の動作グラフを使用すると、失敗したログオンの試行、不審な API 呼び出し、その他同様のアクションを調べることができます。詳細については、Detective ドキュメントのData in a behavior graphを参照してください。

ビッグエンディアンシステム

最上位バイトを最初に格納するシステム。エンディアン性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 (青) で実行し、新しいアプリケーションバージョンを別の環境 (緑) で実行します。この戦略は、最小限の影響で迅速にロールバックするのに役立ちます。

ボット

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

ボットネット

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

ブランチ

コードリポジトリに含まれる領域。リポジトリに最初に作成するブランチは、メインブランチといいます。既存のブランチから新しいブランチを作成し、その新しいブランチで機能を開発したり、バグを修正したりできます。機能を構築するために作成するブランチは、通常、機能ブランチと呼ばれます。機能をリリースする準備ができたら、機能ブランチをメインブランチに統合します。詳細については、「ブランチの概要」(GitHub ドキュメント) を参照してください。

ブレークグラスアクセス

例外的な状況では、承認されたプロセスを通じて、ユーザーが AWS アカウント 通常アクセス許可を持たない にすばやくアクセスできるようにします。詳細については、 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。

ビジネス継続性計画 (BCP)

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

C

CAF

AWS 「クラウド導入フレームワーク」を参照してください。

Canary デプロイ

エンドユーザーへのバージョンのスローリリースと増分リリース。確信できたら、新しいバージョンをデプロイし、現在のバージョン全体を置き換えます。

CCoE

「Cloud Center of Excellence」を参照してください。

CDC

「データキャプチャの変更」を参照してください。

変更データキャプチャ (CDC)

データソース (データベーステーブルなど) の変更を追跡し、その変更に関するメタデータを記録するプロセス。CDC は、ターゲットシステムでの変更を監査またはレプリケートして同期を維持するなど、さまざまな目的に使用できます。

カオスエンジニアリング

障害や破壊的なイベントを意図的に導入して、システムの耐障害性をテストします。AWS Fault Injection Service （ AWS FIS ） を使用して、 AWS ワークロードにストレスを与え、その応答を評価する実験を実行できます。

CI/CD

「継続的インテグレーションと継続的デリバリー」を参照してください。

分類

予測を生成するのに役立つ分類プロセス。分類問題の機械学習モデルは、離散値を予測します。離散値は、常に互いに区別されます。例えば、モデルがイメージ内に車があるかどうかを評価する必要がある場合があります。

クライアント側の暗号化

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

Cloud Center of Excellence (CCoE)

クラウドのベストプラクティスの作成、リソースの移動、移行のタイムラインの確立、大規模変革を通じて組織をリードするなど、組織全体のクラウド導入の取り組みを推進する学際的なチーム。詳細については、 AWS クラウド エンタープライズ戦略ブログの CCoE 投稿を参照してください。

クラウドコンピューティング

リモートデータストレージと IoT デバイス管理に通常使用されるクラウドテクノロジー。クラウドコンピューティングは、一般的にエッジコンピューティングテクノロジーに接続されています。

クラウド運用モデル

IT 組織において、1 つ以上のクラウド環境を構築、成熟、最適化するために使用される運用モデル。詳細については、「クラウド運用モデルの構築」 を参照してください。

導入のクラウドステージ

組織が に移行するときに通常実行する 4 つのフェーズ AWS クラウド :

- プロジェクト — 概念実証と学習を目的として、クラウド関連のプロジェクトをいくつか実行する
- 基礎固め — お客様のクラウドの導入を拡大するための基礎的な投資 (ランディングゾーンの作成、CCoE の定義、運用モデルの確立など)
- 移行 — 個々のアプリケーションの移行
- 再発明 — 製品とサービスの最適化、クラウドでのイノベーション

これらのステージは、 AWS クラウド エンタープライズ戦略ブログのブログ記事「クラウドファーストへのジャーニー」と「導入のステージ」で Stephen Orban によって定義されました。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、 GitHubまたは が含まれますBitbucket Cloud。コードの各バージョンはブランチと呼ばれます。マイクロサービス

の構造では、各リポジトリは 1 つの機能専用です。1 つの CI/CD パイプラインで複数のリポジトリを使用できます。

コールドキャッシュ

空である、または、かなり空きがある、もしくは、古いデータや無関係なデータが含まれているバッファキャッシュ。データベースインスタンスはメインメモリまたはディスクから読み取る必要があり、バッファキャッシュから読み取るよりも時間がかかるため、パフォーマンスに影響します。

コールドデータ

めったにアクセスされず、通常は過去のデータです。この種類のデータをクエリする場合、通常は低速なクエリでも問題ありません。このデータを低パフォーマンスで安価なストレージ階層またはクラスに移動すると、コストを削減することができます。

コンピュータビジョン (CV)

機械学習を使用してデジタルイメージやビデオなどのビジュアル形式から情報を分析および抽出する AI の分野。例えば、Amazon SageMaker AI は CV 用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、設定が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。

構成管理データベース (CMDB)

データベースとその IT 環境 (ハードウェアとソフトウェアの両方のコンポーネントとその設定を含む) に関する情報を保存、管理するリポジトリ。通常、CMDB のデータは、移行のポートフォリオの検出と分析の段階で使用します。

コンフォーマンスパック

コンプライアンスチェックとセキュリティチェックをカスタマイズするためにアセンブルできる AWS Config ルールと修復アクションのコレクション。YAML テンプレートを使用して、コンフォーマンスパックを AWS アカウント および リージョンの単一のエンティティとしてデプロイすることも、組織全体にデプロイすることもできます。詳細については、 AWS Config ドキュメントの「コンフォーマンスパック」を参照してください。

継続的インテグレーションと継続的デリバリー (CI/CD)

ソフトウェアリリースプロセスのソース、ビルド、テスト、ステージング、本番の各ステージを自動化するプロセス。CI/CD は一般的にパイプラインと呼ばれます。プロセスの自動化、生産性

の向上、コード品質の向上、配信の加速化を可能にします。詳細については、「継続的デリバリーの利点」を参照してください。CD は継続的デプロイ (Continuous Deployment) の略語でもあります。詳細については「継続的デリバリーと継続的なデプロイ」を参照してください。

CV

「コンピュータビジョン」を参照してください。

D

保管中のデータ

ストレージ内にあるデータなど、常に自社のネットワーク内にあるデータ。

データ分類

ネットワーク内のデータを重要度と機密性に基づいて識別、分類するプロセス。データに適した保護および保持のコントロールを判断する際に役立つため、あらゆるサイバーセキュリティのリスク管理戦略において重要な要素です。データ分類は、 AWS Well-Architected フレームワークのセキュリティの柱のコンポーネントです。詳細については、データ分類を参照してください。

データドリフト

実稼働データと ML モデルのトレーニングに使用されたデータとの間に有意な差異が生じたり、入力データが時間の経過と共に有意に変化したりすることです。データドリフトは、ML モデル予測の全体的な品質、精度、公平性を低下させる可能性があります。

転送中のデータ

ネットワーク内 (ネットワークリソース間など) を活発に移動するデータ。

データメッシュ

一元管理とガバナンスを備えた分散型の分散型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。信頼された ID のみが、予想されるネットワークから信頼されたリソースにアクセスできるようにします。詳細については、「 でのデータ境界の構築 AWS」を参照してください。

データの前処理

raw データをお客様の機械学習モデルで簡単に解析できる形式に変換すること。データの前処理とは、特定の列または行を削除して、欠落している、矛盾している、または重複する値に対処することを意味します。

データ出所

データの生成、送信、保存の方法など、データのライフサイクル全体を通じてデータの出所と履歴を追跡するプロセス。

データ件名

データを収集、処理している個人。

データウェアハウス

分析などのビジネスインテリジェンスをサポートするデータ管理システム。データウェアハウスには通常、大量の履歴データが含まれており、通常はクエリや分析に使用されます。

データベース定義言語 (DDL)

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

データベース操作言語 (DML)

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

DDL

「データベース定義言語」を参照してください。

ディープアンサンブル

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

ディープラーニング

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

多層防御

一連のセキュリティメカニズムとコントロールをコンピュータネットワーク全体に層状に重ねて、ネットワークとその内部にあるデータの機密性、整合性、可用性を保護する情報セキュリティの手法。この戦略を採用するときは AWS、 AWS Organizations 構造の異なるレイヤーに複数のコントロールを追加して、リソースの安全性を確保します。たとえば、多層防御アプローチでは、多要素認証、ネットワークセグメンテーション、暗号化を組み合わせることができます。

委任管理者

では AWS Organizations、互換性のあるサービスが AWS メンバーアカウントを登録して組織のアカウントを管理し、そのサービスのアクセス許可を管理できます。このアカウントを、そのサービスの委任管理者と呼びます。詳細、および互換性のあるサービスの一覧は、 AWS Organizations ドキュメントのAWS Organizationsで使用できるサービスを参照してください。

デプロイ

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

開発環境

「環境」を参照してください。

検出管理

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

開発バリューストリームマッピング (DVSM)

ソフトウェア開発ライフサイクルのスピードと品質に悪影響を及ぼす制約を特定し、優先順位を付けるために使用されるプロセス。DVSM は、もともとリーンマニュファクチャリング・プラクティスのために設計されたバリューストリームマッピング・プロセスを拡張したものです。ソフトウェア開発プロセスを通じて価値を創造し、動かすために必要なステップとチームに焦点を当てています。

デジタルツイン

建物、工場、産業機器、生産ラインなど、現実世界のシステムを仮想的に表現したものです。デジタルツインは、予知保全、リモートモニタリング、生産最適化をサポートします。

ディメンションテーブル

スタースキーマでは、ファクトテーブル内の量的データに関するデータ属性を含む小さなテーブル。ディメンションテーブル属性は通常、テキストフィールドまたはテキストのように動作する離散数値です。これらの属性は、クエリの制約、フィルタリング、結果セットのラベル付けに一般的に使用されます。

ディザスタ

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

ディザスタリカバリ (DR)

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の詳細については、コンテナと Amazon API Gateway を使用して、従来の Microsoft ASP.NET (ASMX) ウェブサービスを段階的にモダナイズ を参照してください。

DR

「ディザスタリカバリ」を参照してください。

ドリフト検出

ベースライン設定からの偏差を追跡します。たとえば、 AWS CloudFormation を使用してシステムリソースのドリフトを検出したり、 を使用して AWS Control Tower 、ガバナンス要件への準拠に影響するランディングゾーンの変更を検出したりできます。

DVSM

「開発値ストリームマッピング」を参照してください。

E

EDA

「探索的データ分析」を参照してください。

EDI

「電子データ交換」を参照してください。

エッジコンピューティング

IoT ネットワークのエッジにあるスマートデバイスの計算能力を高めるテクノロジー。クラウドコンピューティングと比較すると、エッジコンピューティングは通信レイテンシーを短縮し、応答時間を短縮できます。

電子データ交換 (EDI)

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

暗号化

人間が読み取り可能なプレーンテキストデータを暗号文に変換するコンピューティングプロセス。

暗号化キー

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

エンディアン

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

エンドポイント

「サービスエンドポイント」を参照してください。

エンドポイントサービス

仮想プライベートクラウド (VPC) 内でホストして、他のユーザーと共有できるサービス。を使用してエンドポイントサービスを作成し AWS PrivateLink 、他の AWS アカウント または AWS Identity and Access Management (IAM) プリンシパルにアクセス許可を付与できます。これら

のアカウントまたはプリンシパルは、インターフェイス VPC エンドポイントを作成することで、エンドポイントサービスにプライベートに接続できます。詳細については、Amazon Virtual Private Cloud (Amazon VPC) ドキュメントの「エンドポイントサービスを作成する」を参照してください。

エンタープライズリソースプランニング (ERP)

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

エンベロープ暗号化

暗号化キーを、別の暗号化キーを使用して暗号化するプロセス。詳細については、 AWS Key Management Service （ AWS KMS) ドキュメントの「エンベロープ暗号化」を参照してください。

環境

実行中のアプリケーションのインスタンス。クラウドコンピューティングにおける一般的な環境の種類は以下のとおりです。

- 開発環境 — アプリケーションのメンテナンスを担当するコアチームのみが使用できる、実行中のアプリケーションのインスタンス。開発環境は、上位の環境に昇格させる変更をテストするときに使用します。このタイプの環境は、テスト環境と呼ばれることもあります。
- 下位環境 — 初期ビルドやテストに使用される環境など、アプリケーションのすべての開発環境。
- 本番環境 — エンドユーザーがアクセスできる、実行中のアプリケーションのインスタンス。CI/CD パイプラインでは、本番環境が最後のデプロイ環境になります。
- 上位環境 — コア開発チーム以外のユーザーがアクセスできるすべての環境。これには、本番環境、本番前環境、ユーザー承認テスト環境などが含まれます。

エピック

アジャイル方法論で、お客様の作業の整理と優先順位付けに役立つ機能カテゴリ。エピックでは、要件と実装タスクの概要についてハイレベルな説明を提供します。たとえば、 AWS CAF セキュリティエピックには、ID とアクセスの管理、検出コントロール、インフラストラクチャセキュリティ、データ保護、インシデント対応が含まれます。 AWS 移行戦略のエピックの詳細については、プログラム実装ガイド を参照してください。

ERP

「エンタープライズリソース計画」を参照してください。

探索的データ分析 (EDA)

データセットを分析してその主な特性を理解するプロセス。お客様は、データを収集または集計してから、パターンの検出、異常の検出、および前提条件のチェックのための初期調査を実行します。EDA は、統計の概要を計算し、データの可視化を作成することによって実行されます。

F

ファクトテーブル

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

フェイルファスト

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

障害分離の境界

では AWS クラウド、障害の影響を制限し、ワークロードの耐障害性を高めるのに役立つアベイラビリティーゾーン AWS リージョン、コントロールプレーン、データプレーンなどの境界。詳細については、AWS 「障害分離境界」を参照してください。

機能ブランチ

「ブランチ」を参照してください。

特徴量

お客様が予測に使用する入力データ。例えば、製造コンテキストでは、特徴量は製造ラインから定期的にキャプチャされるイメージの可能性もあります。

特徴量重要度

モデルの予測に対する特徴量の重要性。これは通常、Shapley Additive Deskonations (SHAP) や積分勾配など、さまざまな手法で計算できる数値スコアで表されます。詳細については、「 を使用した機械学習モデルの解釈可能性 AWS」を参照してください。

機能変換

追加のソースによるデータのエンリッチ化、値のスケーリング、単一のデータフィールドからの複数の情報セットの抽出など、機械学習プロセスのデータを最適化すること。これにより、機械

学習モデルはデータの恩恵を受けることができます。例えば、「2021-05-27 00:15:37」の日付を「2021 年」、「5 月」、「木」、「15」に分解すると、学習アルゴリズムがさまざまなデータコンポーネントに関連する微妙に異なるパターンを学習するのに役立ちます。

数ショットプロンプト

同様のタスクの実行を求める前に、タスクと必要な出力を示す少数の例を 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、またはドメインの知識を必要とするタスクに効果的です。「ゼロショットプロンプト」も参照してください。

FGAC

「きめ細かなアクセスコントロール」を参照してください。

きめ細かなアクセス制御 (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

フラッシュカット移行

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

FM

「基盤モデル」を参照してください。

基盤モデル (FM)

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

G

生成 AI

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

ジオブロッキング

地理的制限を参照してください。

地理的制限 (ジオブロッキング)

特定の国のユーザーがコンテンツ配信にアクセスできないようにするための、Amazon CloudFront のオプション。アクセスを許可する国と禁止する国は、許可リストまたは禁止リストを使って指定します。詳細については、CloudFront ドキュメントのコンテンツの地理的ディストリビューションの制限を参照してください。

Gitflow ワークフロー

下位環境と上位環境が、ソースコードリポジトリでそれぞれ異なるブランチを使用する方法。Gitflow ワークフローはレガシーと見なされ、トランクベースのワークフローはモダンで推奨されるアプローチです。

ゴールデンイメージ

その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。たとえば、製造では、ゴールデンイメージを使用して複数のデバイスにソフトウェアをプロビジョニングし、デバイス製造オペレーションの速度、スケーラビリティ、生産性を向上させることができます。

グリーンフィールド戦略

新しい環境に既存のインフラストラクチャが存在しないこと。システムアーキテクチャにグリーンフィールド戦略を導入する場合、既存のインフラストラクチャ (別名ブラウンフィールド) との互換性の制約を受けることなく、あらゆる新しいテクノロジーを選択できます。既存のインフラストラクチャを拡張している場合は、ブラウンフィールド戦略とグリーンフィールド戦略を融合させることもできます。

ガードレール

組織単位 (OU) 全般のリソース、ポリシー、コンプライアンスを管理するのに役立つ概略的なルール。予防ガードレールは、コンプライアンス基準に一致するようにポリシーを実施します。これらは、サービスコントロールポリシーと IAM アクセス許可の境界を使用して実装されます。検出ガードレールは、ポリシー違反やコンプライアンス上の問題を検出し、修復のためのアラートを発信します。これらは AWS Config、、Amazon GuardDuty AWS Security Hub、、 AWS Trusted Advisor Amazon Inspector、およびカスタム AWS Lambda チェックを使用して実装されます。

H

HA

「高可用性」を参照してください。

異種混在データベースの移行

別のデータベースエンジンを使用するターゲットデータベースへお客様の出典データベースの移行 (例えば、Oracle から Amazon Aurora)。異種間移行は通常、アーキテクチャの再設計作業の一部であり、スキーマの変換は複雑なタスクになる可能性があります。AWS は、スキーマの変換に役立つ AWS SCTを提供します。

ハイアベイラビリティ (HA)

課題や災害が発生した場合に、介入なしにワークロードを継続的に運用できること。HA システムは、自動的にフェイルオーバーし、一貫して高品質のパフォーマンスを提供し、パフォーマンスへの影響を最小限に抑えながらさまざまな負荷や障害を処理するように設計されています。

ヒストリアンのモダナイゼーション

製造業のニーズによりよく応えるために、オペレーションテクノロジー (OT) システムをモダナイズし、アップグレードするためのアプローチ。ヒストリアンは、工場内のさまざまなソースからデータを収集して保存するために使用されるデータベースの一種です。

ホールドアウトデータ

機械学習モデルのトレーニングに使用されるデータセットから保留される、ラベル付きの履歴データの一部。モデル予測をホールドアウトデータと比較することで、ホールドアウトデータを使用してモデルのパフォーマンスを評価できます。

同種データベースの移行

お客様の出典データベースを、同じデータベースエンジンを共有するターゲットデータベース (Microsoft SQL Server から Amazon RDS for SQL Server など) に移行する。同種間移行は、通常、リホストまたはリプラットフォーム化の作業の一部です。ネイティブデータベースユーティリティを使用して、スキーマを移行できます。

ホットデータ

リアルタイムデータや最近の翻訳データなど、頻繁にアクセスされるデータ。通常、このデータには高速なクエリ応答を提供する高性能なストレージ階層またはクラスが必要です。

ホットフィックス

本番環境の重大な問題を修正するために緊急で配布されるプログラム。緊急性が高いため、通常の DevOps のリリースワークフローからは外れた形で実施されます。

ハイパーケア期間

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

I

IaC

「Infrastructure as Code」を参照してください。

ID ベースのポリシー

AWS クラウド 環境内のアクセス許可を定義する 1 つ以上の IAM プリンシパルにアタッチされたポリシー。

アイドル状態のアプリケーション

90 日間の平均的な CPU およびメモリ使用率が 5～20% のアプリケーション。移行プロジェクトでは、これらのアプリケーションを廃止するか、オンプレミスに保持するのが一般的です。

IIoT

「産業用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、または変更する代わりに、本番環境のワークロード用に新しいインフラストラクチャをデプロイするモデル。イミュータブルインフラストラクチャは、本質的にミュータブルインフラストラクチャよりも一貫性、信頼性、予測性が高くなります。詳細については、 AWS Well-Architected フレームワークの「変更不可能なインフラストラクチャを使用したデプロイ」のベストプラクティスを参照してください。

インバウンド (受信) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーションの外部からネットワーク接続を受け入れ、検査し、ルーティングする VPC。AWS Security Reference Architecture では、アプリ

ケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

増分移行

アプリケーションを 1 回ですべてカットオーバーするのではなく、小さい要素に分けて移行するカットオーバー戦略。例えば、最初は少数のマイクロサービスまたはユーザーのみを新しいシステムに移行する場合があります。すべてが正常に機能することを確認できたら、残りのマイクロサービスやユーザーを段階的に移行し、レガシーシステムを廃止できるようにします。この戦略により、大規模な移行に伴うリスクが軽減されます。

インダストリー 4.0

2016 年に Klaus Schwab によって導入された用語で、接続、リアルタイムデータ、自動化、分析、AI/ML の進歩によるビジネスプロセスのモダナイゼーションを指します。

インフラストラクチャ

アプリケーションの環境に含まれるすべてのリソースとアセット。

Infrastructure as Code (IaC)

アプリケーションのインフラストラクチャを一連の設定ファイルを使用してプロビジョニングし、管理するプロセス。IaC は、新しい環境を再現可能で信頼性が高く、一貫性のあるものにするため、インフラストラクチャを一元的に管理し、リソースを標準化し、スケールを迅速に行えるように設計されています。

産業分野における IoT (IIoT)

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

インスペクション VPC

AWS マルチアカウントアーキテクチャでは、VPC (同一または異なる 内 AWS リージョン)、インターネット、オンプレミスネットワーク間のネットワークトラフィックの検査を管理する一元化された VPCs。AWS Security Reference Architecture では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

IoT

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

解釈可能性

機械学習モデルの特性で、モデルの予測がその入力にどのように依存するかを人間が理解できる度合いを表します。詳細については、「 を使用した機械学習モデルの解釈可能性 AWS」を参照してください。

IoT

「モノのインターネット」を参照してください。

IT 情報ライブラリ (ITIL)

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

IT サービス管理 (ITSM)

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

ITIL

「IT 情報ライブラリ」を参照してください。

ITSM

「IT サービス管理」を参照してください。

L

ラベルベースアクセス制御 (LBAC)

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

ランディングゾーン

ランディングゾーンは、スケーラブルで安全な、適切に設計されたマルチアカウント AWS 環境です。これは、組織がセキュリティおよびインフラストラクチャ環境に自信を持ってワークロー

ドとアプリケーションを迅速に起動してデプロイできる出発点です。ランディングゾーンの詳細については、安全でスケーラブルなマルチアカウント AWS 環境のセットアップ を参照してください。

大規模言語モデル (LLM)

大量のデータに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」を参照してください。

大規模な移行

300 台以上のサーバの移行。

LBAC

「ラベルベースのアクセスコントロール」を参照してください。

最小特権

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

リフトアンドシフト

「7 Rs」を参照してください。

リトルエンディアンシステム

最下位バイトを最初に格納するシステム。エンディアン性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たソフトウェア。マルウェアは、コンピュータシステムの中断、機密情報の漏洩、不正アクセス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 はインフラストラクチャレイヤー、オペレーティングシステム、プラットフォーム AWS を運用し、エンドポイントにアクセスしてデータを保存および取得します。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で、原材料を工場の完成製品に変換します。

MAP

「移行促進プログラム」を参照してください。

メカニズム

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

メンバーアカウント

組織の一部である管理アカウント AWS アカウント を除くすべて AWS Organizations。アカウントが組織のメンバーになることができるのは、一度に 1 つのみです。

MES

「製造実行システム」を参照してください。

メッセージキューイングテレメトリトランスポート (MQTT)

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

マイクロサービス

明確に定義された API を介して通信し、通常は小規模な自己完結型のチームが所有する、小規模で独立したサービスです。例えば、保険システムには、販売やマーケティングなどのビジネス機能、または購買、請求、分析などのサブドメインにマッピングするマイクロサービスが含まれる場合があります。マイクロサービスの利点には、俊敏性、柔軟なスケーリング、容易なデプロイ、再利用可能なコード、回復力などがあります。詳細については、AWS「サーバーレスサービスを使用したマイクロサービスの統合」を参照してください。

マイクロサービスアーキテクチャ

各アプリケーションプロセスをマイクロサービスとして実行する独立したコンポーネントを使用してアプリケーションを構築するアプローチ。これらのマイクロサービスは、軽量 API を使用して、明確に定義されたインターフェイスを介して通信します。このアーキテクチャの各マイクロサービスは、アプリケーションの特定の機能に対する需要を満たすように更新、デプロイ、およびスケーリングできます。詳細については、「 でのマイクロサービスの実装 AWS」を参照してください。

Migration Acceleration Program (MAP)

組織がクラウドに移行するための強力な運用基盤を構築し、移行の初期コストを相殺するのに役立つコンサルティングサポート、トレーニング、サービスを提供する AWS プログラム。MAP には、組織的な方法でレガシー移行を実行するための移行方法論と、一般的な移行シナリオを自動化および高速化する一連のツールが含まれています。

大規模な移行

アプリケーションポートフォリオの大部分を次々にクラウドに移行し、各ウェーブでより多くのアプリケーションを高速に移動させるプロセス。この段階では、以前の段階から学んだベストプラクティスと教訓を使用して、移行ファクトリー チーム、ツール、プロセスのうち、オートメーションとアジャイルデリバリーによってワークロードの移行を合理化します。これは、AWS 移行戦略 の第 3 段階です。

移行ファクトリー

自動化された俊敏性のあるアプローチにより、ワークロードの移行を合理化する部門横断的なチーム。移行ファクトリーチームには、通常、運用、ビジネスアナリストおよび所有者、移行エンジニア、デベロッパー、およびスプリントで作業する DevOps プロフェッショナルが含まれます。エンタープライズアプリケーションポートフォリオの 20～50% は、ファクトリーのアプローチによって最適化できる反復パターンで構成されています。詳細については、このコンテンツセットの移行ファクトリーに関する解説とCloud Migration Factory ガイドを参照してください。

移行メタデータ

移行を完了するために必要なアプリケーションおよびサーバーに関する情報。移行パターンごとに、異なる一連の移行メタデータが必要です。移行メタデータの例としては、ターゲットサブネット、セキュリティグループ、 AWS アカウントなどがあります。

移行パターン

移行戦略、移行先、および使用する移行アプリケーションまたはサービスを詳述する、反復可能な移行タスク。例: AWS Application Migration Service を使用して Amazon EC2 への移行をリホストします。

Migration Portfolio Assessment (MPA)

に移行するためのビジネスケースを検証するための情報を提供するオンラインツール AWS クラウド。MPA は、詳細なポートフォリオ評価 (サーバーの適切なサイジング、価格設定、TCO 比較、移行コスト分析) および移行プラン (アプリケーションデータの分析とデータ収集、アプリケーションのグループ化、移行の優先順位付け、およびウェーブプランニング) を提供します。MPA ツール (ログインが必要) は、すべての AWS コンサルタントと APN パートナーコンサルタントが無料で利用できます。

移行準備状況評価 (MRA)

AWS CAF を使用して、組織のクラウド準備状況に関するインサイトを取得し、長所と短所を特定し、特定されたギャップを埋めるためのアクションプランを構築するプロセス。詳細については、移行準備状況ガイド を参照してください。MRA は、AWS 移行戦略の第一段階です。

移行戦略

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

O

OAC

「オリジンアクセスコントロール」を参照してください。

OAI

「オリジンアクセスアイデンティティ」を参照してください。

OCM

「組織変更管理」を参照してください。

オフライン移行

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

OI

「 オペレーションの統合」を参照してください。

OLA

「運用レベルの契約」を参照してください。

オンライン移行

ソースワークロードをオフラインにせずにターゲットシステムにコピーする移行方法。ワークロードに接続されているアプリケーションは、移行中も動作し続けることができます。この方法はダウンタイムがゼロから最小限で済むため、通常は重要な本番稼働環境のワークロードに使用されます。

OPC-UA

「Open Process Communications - Unified Architecture」を参照してください。

オープンプロセス通信 - 統合アーキテクチャ (OPC-UA)

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

オペレーショナルレベルアグリーメント (OLA)

サービスレベルアグリーメント (SLA) をサポートするために、どの機能的 IT グループが互いに提供することを約束するかを明確にする契約。

運用準備状況レビュー (ORR)

インシデントや潜在的な障害の理解、評価、防止、または範囲の縮小に役立つ質問とそれに関連するベストプラクティスのチェックリスト。詳細については、 AWS Well-Architected フレームワークの「Operational Readiness Reviews (ORR)」を参照してください。

運用テクノロジー (OT)

産業オペレーション、機器、インフラストラクチャを制御するために物理環境と連携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 変換の主な焦点です。

オペレーション統合 (OI)

クラウドでオペレーションをモダナイズするプロセスには、準備計画、オートメーション、統合が含まれます。詳細については、オペレーション統合ガイド を参照してください。

組織の証跡

組織 AWS アカウント 内のすべての のすべてのイベント AWS CloudTrail をログに記録する、 によって作成された証跡 AWS Organizations。証跡は、組織に含まれている各 AWS アカウント に作成され、各アカウントのアクティビティを追跡します。詳細については、CloudTrail ドキュメントの組織の証跡の作成を参照してください。

組織変更管理 (OCM)

人材、文化、リーダーシップの観点から、主要な破壊的なビジネス変革を管理するためのフレームワーク。OCM は、変化の導入を加速し、移行問題に対処し、文化や組織の変化を推進することで、組織が新しいシステムと戦略の準備と移行するのを支援します。 AWS 移行戦略では、クラウド導入プロジェクトに必要な変化のスピードのため、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)

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

オリジンアクセスアイデンティティ (OAI)

CloudFront の、Amazon S3 コンテンツを保護するためのアクセス制限オプション。OAI を使用すると、CloudFront が、Amazon S3 に認証可能なプリンシパルを作成します。認証されたプリンシパルは、S3 バケット内のコンテンツに、特定の CloudFront ディストリビューションを介してのみアクセスできます。OACも併せて参照してください。OAC では、より詳細な、強化されたアクセスコントロールが可能です。

ORR

「運用準備状況レビュー」を参照してください。

OT

「運用テクノロジー」を参照してください。

アウトバウンド (送信) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーション内から開始されたネットワーク接続を処理する VPC。AWS Security Reference Architecture では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

P

アクセス許可の境界

ユーザーまたはロールが使用できるアクセス許可の上限を設定する、IAM プリンシパルにアタッチされる IAM 管理ポリシー。詳細については、IAM ドキュメントのアクセス許可の境界を参照してください。

個人を特定できる情報 (PII)

直接閲覧した場合、または他の関連データと組み合わせた場合に、個人の身元を合理的に推測するために使用できる情報。PII の例には、氏名、住所、連絡先情報などがあります。

PII

個人を特定できる情報を参照してください。

プレイブック

クラウドでのコアオペレーション機能の提供など、移行に関連する作業を取り込む、事前定義された一連のステップ。プレイブックは、スクリプト、自動ランブック、またはお客様のモダナイズされた環境を運用するために必要なプロセスや手順の要約などの形式をとることができます。

PLC

「プログラム可能なロジックコントローラー」を参照してください。

PLM

「製品ライフサイクル管理」を参照してください。

ポリシー

アクセス許可を定義 (アイデンティティベースのポリシーを参照)、アクセス条件を指定 (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を定義 AWS Organizations （ サービスコントロールポリシーを参照) できるオブジェクト。

多言語の永続性

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

ポートフォリオ評価

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

述語

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

述語プッシュダウン

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

予防的コントロール

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

プリンシパル

アクションを実行し AWS 、リソースにアクセスできる のエンティティ。このエンティティは通常、、IAM AWS アカウントロール、またはユーザーのルートユーザーです。詳細については、IAM ドキュメントのロールに関する用語と概念内にあるプリンシパルを参照してください。

プライバシーバイデザイン

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

プライベートホストゾーン

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

プロアクティブコントロール

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

製品ライフサイクル管理 (PLM)

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

本番環境

「環境」を参照してください。

プログラム可能なロジックコントローラー (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、信頼性の高い適応可能なコンピュータです。

プロンプトの連鎖

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

仮名化

データセット内の個人識別子をプレースホルダー値に置き換えるプロセス。仮名化は個人のプライバシー保護に役立ちます。仮名化されたデータは、依然として個人データとみなされます。

パブリッシュ/サブスクライブ (pub/sub)

マイクロサービス間の非同期通信を可能にするパターン。スケーラビリティと応答性を向上させます。たとえば、マイクロサービスベースの MES では、マイクロサービスは他のマイクロサー

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

Q

クエリプラン

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

クエリプランのリグレッション

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

R

RACI マトリックス

責任、説明責任、相談、通知 (RACI) を参照してください。

RAG

「取得拡張生成」を参照してください。

ランサムウェア

決済が完了するまでコンピュータシステムまたはデータへのアクセスをブロックするように設計された、悪意のあるソフトウェア。

RASCI マトリックス

責任、説明責任、相談、通知 (RACI) を参照してください。

RCAC

「行と列のアクセスコントロール」を参照してください。

リードレプリカ

読み取り専用に使用されるデータベースのコピー。クエリをリードレプリカにルーティングして、プライマリデータベースへの負荷を軽減できます。

再設計

「7 Rs」を参照してください。

目標復旧時点 (RPO)

最後のデータリカバリポイントからの最大許容時間です。これにより、最後の回復時点からサービスが中断されるまでの間に許容できるデータ損失の程度が決まります。

目標復旧時間 (RTO)

サービスの中断から復旧までの最大許容遅延時間。

リファクタリング

「7 Rs」を参照してください。

リージョン

地理的エリア内の AWS リソースのコレクション。各 AWS リージョン は、耐障害性、安定性、耐障害性を提供するために、他の とは独立しています。詳細については、AWS リージョン 「アカウントで使用できる を指定する」を参照してください。

回帰

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

リホスト

「7 Rs」を参照してください。

リリース

デプロイプロセスで、変更を本番環境に昇格させること。

再配置

「7 Rs」を参照してください。

プラットフォーム変更

「7 Rs」を参照してください。

再購入

「7 Rs」を参照してください。

回復性

中断に抵抗または回復するアプリケーションの機能。高可用性とディザスタリカバリは、 で回復性を計画する際の一般的な考慮事項です AWS クラウド。詳細については、AWS クラウド「レジリエンス」を参照してください。

リソースベースのポリシー

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

実行責任者、説明責任者、協業先、報告先 (RACI) に基づくマトリックス

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

レスポンシブコントロール

有害事象やセキュリティベースラインからの逸脱について、修復を促すように設計されたセキュリティコントロール。詳細については、Implementing security controls on AWSのResponsive controlsを参照してください。

保持

「7 Rs」を参照してください。

廃止

「7 Rs」を参照してください。

取得拡張生成 (RAG)

LLM がレスポンスを生成する前にトレーニングデータソースの外部にある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またはカスタムデータのセマンティック検索を実行する場合があります。詳細については、「RAG とは」を参照してください。

ローテーション

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。

行と列のアクセス制御 (RCAC)

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

RPO

「目標復旧時点」を参照してください。

RTO

目標復旧時間を参照してください。

ランブック

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

S

SAML 2.0

多くの ID プロバイダー (IdP) が使用しているオープンスタンダード。この機能を使用すると、フェデレーティッドシングルサインオン (SSO) が有効になるため、ユーザーは組織内のすべてのユーザーを IAM で作成しなくても、 AWS Management Console にログインしたり AWS 、 API オペレーションを呼び出すことができます。SAML 2.0 ベースのフェデレーションの詳細については、IAM ドキュメントのSAML 2.0 ベースのフェデレーションについてを参照してください。

SCADA

「監視コントロールとデータ取得」を参照してください。

SCP

「サービスコントロールポリシー」を参照してください。

シークレット

暗号化された形式で保存する 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、1 つの文字列、または複数の文字列にすることができます。詳細については、Secrets Manager ドキュメントの「Secrets Manager シークレットの内容」を参照してください。

設計によるセキュリティ

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

セキュリティコントロール

脅威アクターによるセキュリティ脆弱性の悪用を防止、検出、軽減するための、技術上または管理上のガードレール。セキュリティコントロールには、予防的、検出的、応答的、プロアクティブの 4 つの主なタイプがあります。

セキュリティ強化

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

Security Information and Event Management (SIEM) システム

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

セキュリティレスポンスの自動化

セキュリティイベントに自動的に応答または修復するように設計された、事前定義されたプログラムされたアクション。これらの自動化は、セキュリティのベストプラクティスを実装するのに役立つ検出的または応答的な AWS セキュリティコントロールとして機能します。自動レスポンスアクションの例としては、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、認証情報の更新などがあります。

サーバー側の暗号化

AWS のサービス 送信先にあるデータの、それを受け取る 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。SCP は、管理者がユーザーまたはロールに委任するアクションに、ガードレールを定義したり、アクションの制限を設定したりします。SCP は、許可リストまたは拒否リストとして、許可または禁止するサービスやアクションを指定する際に使用できます。詳細については、 AWS Organizations ドキュメントの「サービスコントロールポリシー」を参照してください。

サービスエンドポイント

のエントリポイントの URL AWS のサービス。ターゲットサービスにプログラムで接続するには、エンドポイントを使用します。詳細については、AWS 全般のリファレンスの「AWS のサービス エンドポイント」を参照してください。

サービスレベルアグリーメント (SLA)

サービスのアップタイムやパフォーマンスなど、IT チームがお客様に提供すると約束したものを明示した合意書。

サービスレベルインジケータ (SLI)

エラー率、可用性、スループットなど、サービスのパフォーマンス側面の測定。

サービスレベルの目標 (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、 はクラウドのセキュリティを担当します。詳細については、責任共有モデルを参照してください。

SIEM

セキュリティ情報とイベント管理システムを参照してください。

単一障害点 (SPOF)

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

SLA

「サービスレベルの契約」を参照してください。

SLI

「サービスレベルインジケータ」を参照してください。

SLO

「サービスレベルの目標」を参照してください。

スプリットアンドシードモデル

モダナイゼーションプロジェクトのスケーリングと加速のためのパターン。新機能と製品リリースが定義されると、コアチームは解放されて新しい製品チームを作成します。これにより、お客様の組織の能力とサービスの拡張、デベロッパーの生産性の向上、迅速なイノベーションのサポートに役立ちます。詳細については、『』の「アプリケーションのモダナイズに対する段階的なアプローチ 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。

スタースキーマ

1 つの大きなファクトテーブルを使用してトランザクションデータまたは測定データを保存し、1 つ以上の小さなディメンションテーブルを使用してデータ属性を保存するデータベース組織構造。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ように設計されています。

strangler fig パターン

レガシーシステムが廃止されるまで、システム機能を段階的に書き換えて置き換えることにより、モノリシックシステムをモダナイズするアプローチ。このパターンは、宿主の樹木から根を成長させ、最終的にその宿主を包み込み、宿主に取って代わるイチジクのつるを例えています。そのパターンは、モノリシックシステムを書き換えるときのリスクを管理する方法として Martin Fowler により提唱されました。このパターンの適用方法の例については、コンテナと Amazon API Gateway を使用して、従来の Microsoft ASP.NET (ASMX) ウェブサービスを段階的にモダナイズを参照してください。

サブネット

VPC 内の IP アドレスの範囲。サブネットは、1 つのアベイラビリティーゾーンに存在する必要があります。

監視コントロールとデータ取得 (SCADA)

製造では、ハードウェアとソフトウェアを使用して物理アセットと本番稼働をモニタリングするシステム。

対称暗号化

データの暗号化と復号に同じキーを使用する暗号化のアルゴリズム。

合成テスト

ユーザーとのやり取りをシミュレートして潜在的な問題を検出したり、パフォーマンスをモニタリングしたりする方法でシステムをテストします。Amazon CloudWatch Synthetics を使用してこれらのテストを作成できます。

システムプロンプト

LLM にコンテキスト、指示、またはガイドラインを提供して動作を指示する手法。システムプロンプトは、コンテキストを設定し、ユーザーとのやり取りのルールを確立するのに役立ちます。

T

tags

AWS リソースを整理するためのメタデータとして機能するキーと値のペア。タグは、リソースの管理、識別、整理、検索、フィルタリングに役立ちます。詳細については、「AWS リソースのタグ付け」を参照してください。

ターゲット変数

監督された機械学習でお客様が予測しようとしている値。これは、結果変数 のことも指します。例えば、製造設定では、ターゲット変数が製品の欠陥である可能性があります。

タスクリスト

ランブックの進行状況を追跡するために使用されるツール。タスクリストには、ランブックの概要と完了する必要のある一般的なタスクのリストが含まれています。各一般的なタスクには、推定所要時間、所有者、進捗状況が含まれています。

テスト環境

「環境」を参照してください。

トレーニング

お客様の機械学習モデルに学習するデータを提供すること。トレーニングデータには正しい答えが含まれている必要があります。学習アルゴリズムは入力データ属性をターゲット (お客様が予測したい答え) にマッピングするトレーニングデータのパターンを検出します。これらのパターンをキャプチャする機械学習モデルを出力します。そして、お客様が機械学習モデルを使用して、ターゲットがわからない新しいデータでターゲットを予測できます。

トランジットゲートウェイ

VPC とオンプレミスネットワークを相互接続するために使用できる、ネットワークの中継ハブ。詳細については、 AWS Transit Gateway ドキュメントの「トランジットゲートウェイとは」を参照してください。

トランクベースのワークフロー

デベロッパーが機能ブランチで機能をローカルにビルドしてテストし、その変更をメインブランチにマージするアプローチ。メインブランチはその後、開発環境、本番前環境、本番環境に合わせて順次構築されます。

信頼されたアクセス

ユーザーに代わって AWS Organizations およびそのアカウントで組織内でタスクを実行するために指定したサービスにアクセス許可を付与します。信頼されたサービスは、サービスにリンクされたロールを必要なときに各アカウントに作成し、ユーザーに代わって管理タスクを実行します。詳細については、 ドキュメントの「 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 枚のピザで養うことができるくらい小さな DevOps チーム。ツーピザチームの規模では、ソフトウェア開発におけるコラボレーションに最適な機会が確保されます。

U

不確実性

予測機械学習モデルの信頼性を損なう可能性がある、不正確、不完全、または未知の情報を指す概念。不確実性には、次の 2 つのタイプがあります。認識論的不確実性は、限られた、不完全なデータによって引き起こされ、弁論的不確実性 は、データに固有のノイズとランダム性によって引き起こされます。詳細については、深層学習システムにおける不確実性の定量化 ガイドを参照してください。

未分化なタスク

ヘビーリフティングとも呼ばれ、アプリケーションの作成と運用には必要だが、エンドユーザーに直接的な価値をもたらさなかったり、競争上の優位性をもたらしたりしない作業です。未分化なタスクの例としては、調達、メンテナンス、キャパシティプランニングなどがあります。

上位環境

「環境」を参照してください。

V

バキューミング

ストレージを再利用してパフォーマンスを向上させるために、増分更新後にクリーンアップを行うデータベースのメンテナンス操作。

バージョンコントロール

リポジトリ内のソースコードへの変更など、変更を追跡するプロセスとツール。

VPC ピアリング

プライベート IP アドレスを使用してトラフィックをルーティングできる、2 つの VPC 間の接続。詳細については、Amazon VPC ドキュメントの「VPC ピア機能とは」を参照してください。

脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

W

ウォームキャッシュ

頻繁にアクセスされる最新の関連データを含むバッファキャッシュ。データベースインスタンスはバッファキャッシュから、メインメモリまたはディスクからよりも短い時間で読み取りを行うことができます。

ウォームデータ

アクセス頻度の低いデータ。この種類のデータをクエリする場合、通常は適度に遅いクエリでも問題ありません。

ウィンドウ関数

現在のレコードに何らかの形で関連する行のグループに対して計算を実行する SQL 関数。ウィンドウ関数は、移動平均の計算や、現在の行の相対位置に基づく行の値へのアクセスなどのタスクの処理に役立ちます。

ワークロード

ビジネス価値をもたらすリソースとコード (顧客向けアプリケーションやバックエンドプロセスなど) の総称。

ワークストリーム

特定のタスクセットを担当する移行プロジェクト内の機能グループ。各ワークストリームは独立していますが、プロジェクト内の他のワークストリームをサポートしています。たとえば、ポートフォリオワークストリームは、アプリケーションの優先順位付け、ウェーブ計画、および移行メタデータの収集を担当します。ポートフォリオワークストリームは、これらの設備を移行ワークストリームで実現し、サーバーとアプリケーションを移行します。

WORM

「書き込み 1 回」、「読み取り多数」を参照してください。

WQF

AWS 「ワークロード認定フレームワーク」を参照してください。

write once, read many (WORM)

データを 1 回書き込み、データの削除や変更を防ぐストレージモデル。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

LLM にタスクを実行する手順を提供しますが、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

平均 CPU およびメモリ使用率が 5% 未満のアプリケーション。移行プロジェクトでは、これらのアプリケーションを廃止するのが一般的です。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。