IoT デバイスメーカー向けの Matter 標準の採用

AWS 規範ガイダンス

AWS 規範ガイダンス: IoT デバイスメーカー向けの Matter 標準の採用

Table of Contents

IoT デバイスメーカー向けの Matter 標準の採用

Tushar Patel、Vijay Ujjain、および David Huters、Amazon Web Services (AWS)

2024 年 2 月 (ドキュメント履歴)

Statista によると、世界中のスマートホーム世帯の数が 2028 年に 7 億 8,000 万に達すると予想されています。この急速な成長により、運用と管理に課題が生じています。コンシューマーの観点から見ると、各デバイスベンダーは、そのデバイスベンダーに固有のアプリを通じてスマートホームデバイスをホームネットワークにオンボーディングする方法が異なります。これにより、さまざまなベンダーのさまざまなタイプのデバイスの増え続ける配列を管理することが難しくなります。同様に、デバイスメーカーの観点から見ると、スマートホーム製品をさまざまなエコシステムで認証すると、ビジネスプロセスのコストと複雑さが増します。例えば、同じデバイスモデルに対して異なる SKUsが必要になる場合があります。魅力的なユーザーエクスペリエンスアプリを維持し、定期的に更新することで、より良い製品の構築と提供に重点を置いたリソースをなくすことは、追加のオーバーヘッドです。コンシューマーとデバイスメーカーの両方が、共通のスマートホーム相互運用性標準から恩恵を受けるでしょう。この標準により、複数のベンダーのデバイスは、シームレスで安全で信頼性の高い方法で相互運用できます。

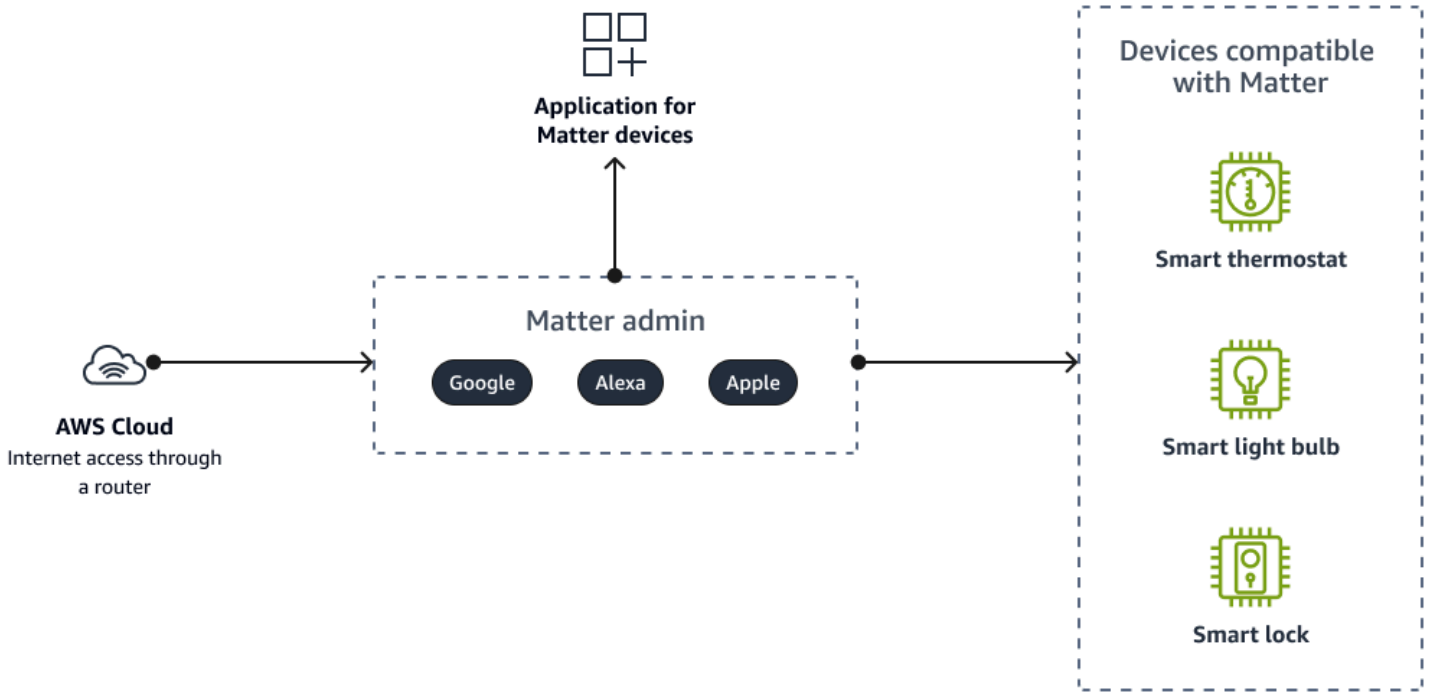
新しい Matter 標準は、スマートホーム空間におけるモノのインターネット (IoT) デバイスメーカーにとって エキサイティングな機会を提供します。この標準は、さまざまな製造元のデバイス間の互換性と相互運用性を向上させることを目的としています。Matter は、IoT デバイス、モバイルアプリ、クラウドサービス間の通信を可能にするオープンでスマートホームな接続プロトコルです。

目的

Matter 標準を製品に統合する場合、IoT デバイスメーカーは開発を開始する前にいくつかの課題に対処する必要があります。Matter は、デバイスの相互運用性、セキュリティ、シンプルさ、信頼性、将来の保証など、独自の IoT プロトコルよりも多くの利点を提供します。ただし、Matter を新規および既存の IoT デプロイの両方に統合するには、慎重な計画と戦略が必要です。メーカーは、メリットを活用しながら落とし穴を回避するために、Matter コンプライアンスプロセスに関するガイダンスを必要としています。このガイドでは、IoT デバイスメーカーに Matter の導入に関する包括的なガイダンスを提供します。これには、戦略から実装までの明確なロードマップが含まれます。このガイドは Matter への移行を容易にし、スマートホームエコシステムに定着する安全で相互運用可能で、将来に対応した製品を構築するのに役立ちます。適切な戦略的アプローチにより、組織は Matter 導入のハードルを克服し、オープンスタンダードを受け入れる革新的な IoT デバイスを開発できます。

このガイドでは、デバイスメーカーに Matter の包括的な概要と Matter に準拠するために必要な手順について説明します。Matter 導入戦略を計画するための長所と短所を概説します。このガイドでは、既存のワイヤレスプロトコルを段階的にサポートし続けながら Matter を活用するためのベストプラクティスも提案しています。このガイドは、スマートホームソリューションを検討している IoT デバイスメーカー向けに、接続戦略に関する情報を提供します。

Matter 標準について



Matter プロトコル

Matter は、デバイス、モバイルアプリ、クラウドサービス間の通信を可能にするオープンなスマートホーム接続プロトコルです。Connectivity Standards Alliance (CSA) によって開発された Matter は、コンシューマーとメーカーの接続と相互運用性を簡素化します。Matter は、さまざまなスマートホームカテゴリをサポートしています。Matter はコンシューマー向けに、エコシステム全体でオンボーディング、統合管理、制御を提供します。メーカーにとって、Matter は単一の認定とアプリケーション開発を通じて開発コストとサポートコストを削減します。Amazon、Apple、Google などの多くの大企業が Matter の導入を推進しています。CSA は、組織の関与に応じて、主催者、参加者、アダプター、アソシエイトの 4 つのメンバーシップレベルを提供します。Matter は、強力な業界サポートにより、コンシューマーにブランド間でシームレスな接続を提供し、メーカーの開発を効率化することを目指しています。

Matter の仕組みの概要

Matter は、ベンダーエコシステム全体のスマートホームデバイス向けの IP ベースのアプリケーションレベルのプロトコルです。IPv6 を使用するデバイスで動作します。概念的には、Matter は Matter

エンドポイントであるネットワークノード のコレクションとして編成されています。Matter 用語の簡単な概要を次に示します。

- Matter デバイスは、電球、スイッチ、サーモスタット、ロックなどのスマートホーム製品です。
- Matter ファブリックは、すべてのデバイスが接続されている仮想ネットワークです。すべてのデバイスは同じ信頼されたルートを共有します。ファブリックはスターネットワークトポロジを形成します。
- Matter 管理者は、ファブリック上のすべてのデバイスのセキュリティと権限を作成、維持、管理します。管理者はハブでもアプリケーションでもかまいません。Matter にはマルチ管理者機能があり、Matter デバイスは同時に複数の軌道の一部にすることができます。例えば、1 つの Matter デバイスを Amazon Alexa デバイスと Google Home デバイスの両方で管理できます。どちらも同じ物理ネットワーク上の Matter 管理者である可能性があります。
- Matter コミッショナーは、新しい Matter デバイスをファブリックにコミッショニング (またはオンボード) するデバイスです。これは、電話のアプリ、スマートホームゲートウェイ、Matter 管理者などです。
- Matter ブリッジは、IP 以外のプロトコルデバイスを Matter ファブリックに接続します。

Matter でハードウェアとソフトウェアが引き受けることができるさまざまなロールの詳細については、「Peeking Under the of Your Matter Smart Home」(CSA ブログ記事) を参照してください。

Matter による認証の利点

Matter の導入により、スマートホームコンシューマーとそれを提供するメーカーの両方に多大な利点をもたらすことが約束されます。スマートデバイスの共通言語を確立することで、Matter は、セットアップの簡素化、プラットフォーム間の統合管理、音声制御の選択と柔軟性の拡張を通じて、今日のフラグメント化された市場を切り離すことを目指しています。

コンシューマーにとって、この統一されたエクスペリエンスは、スマートホームの構築と拡張を大幅に複雑で困難なものにする必要があります。また、デバイスメーカーは、認証の合理化、開発コストの削減、カスタマーサポートの簡素化を通じて有意義なメリットを得られます。Matter は相互運用性を高め、スマートホーム導入の障壁を減らすため、どちらのグループにもメリットがあります。全体として、Matter 標準への認定は、これまで引き継がれてきた問題を解決することで、スマートホーム市場の拡大を加速する態勢を整えています。

トピック

スマートホームコンシューマー向けの Matter 認定の利点

Matter の導入は、コンシューマーに大きなメリットをもたらすことを約束します。Matter は、スマートホームデバイスが主要なプラットフォーム間でシームレスに連携するための共通言語を提供します。Matter でデバイスを認証することで、コンシューマーはスマートホームのセットアップと管理を簡素化し、デバイスの制御方法の柔軟性と選択性を高めることを期待できます。

セットアップと統合管理の簡素化

コンシューマーが直面する最大のフラストレーションの 1 つは、さまざまなスマートホームデバイスを操作して連携させるために必要な複雑なセットアップとオンボーディングプロセスです。各デバイスには、独自のアプリと個別のアカウントが必要になる場合があります。この問題に対処するために、Matter は認定済みデバイスの plug-and-play 機能を有効にします。Matter 認定デバイスのオンボーディングは、デバイスをローカルホームネットワークに接続し、Alexa アプリなどの Matter 管理者を使用してデバイスの QR コードを読み取るだけで簡単です。

1 つのアプリでこの統一されたセットアップエクスペリエンスにより、コンシューマーは複数の別々のアプリを結合してデバイスのさまざまなブランドを管理する必要がなくなります。Matter 認

定のライト、ロック、センサーなどをすべて単一のインターフェイスから表示および制御できます。Apple HomeKit、Amazon Alexa、Google Assistant のユーザーはすべて、個別の製造元アプリケーションをダウンロードしなくても Matter デバイスを検出して制御できるという利点があります。統合システムによるスマートホームデバイスの管理を簡素化することで、コンシューマーの複雑さが軽減され、セットアップの構築と拡張の面倒さが大幅に軽減されます。

音声制御の選択と柔軟性の向上

音声制御は、コンシューマーがスマートホームデバイスとやり取りするための一般的な方法となっています。ただし、今日では、音声アシスタントの選択によって、音声で制御できるデバイスのブランドが決まります。Matter は、エコシステム間で音声制御を有効にすることで、これを変更します。

コンシューマーは、デバイスの互換性を気にすることなく、ニーズに最適な音声アシスタントエコシステムを柔軟に選択できます。Google Assistant に慣れているユーザーは、デバイスがもともと Alexa または HomeKit 市場向けに製造されていた場合でも、Matter 認定デバイスを音声で制御できます。

この音声制御の相互互換性により、よりオープンな環境が構築され、ユーザーはより多くの選択肢を得られます。単一のエコシステムとの互換性ではなく、機能と料金に基づいてデバイスを選択できます。ユーザーが将来音声アシスタントを変更したい場合は、すべてのデバイスが共通の Matter 言語を話すため、既存のスマートホーム設定を簡単に移動できます。

デバイスメーカー向けの Matter 認定の利点

Matter 認定は、コンシューマーを支援するだけでなく、スマートデバイスメーカーにも有意義なメリットをもたらします。Matter 標準を採用することで、組織はコストを削減し、顧客のリーチを拡大する利点を得ることができます。

エコシステム間での単一の認定

現在、Alexa HomeKit や Google Home などのエコシステム間で互換性を確保するために、メーカーは各組織で複数の長期で高価な認定プロセスを経る必要があります。Matter は、単一の共通証明書を確立することでこれを変更します。

デバイスメーカーは、すべての主要なスマートホームエコシステムや音声アシスタントと互換性を持つために、Matter 標準に製品を一度認証するだけで済みます。これにより、開発が効率化され、ステータスクォーと比較して認定コストが大幅に削減されます。製品が更新されるにつれて、リソースを個別の証明書の維持に費やす必要がなくなります。また、単一の Matter 認定により、将来に対応した製品が提供され、新しいエコシステムが登場しても互換性が確保されます。

開発コストの削減

Matter は、製造元の開発コストを削減するのに役立ちます。共通の接続とセキュリティ標準を採用することで、組織は Matter プロジェクト全体に寄与する共有インフラストラクチャコンポーネントからメリットを得られます。

例えば、製造元は独自の Thread ボーダールーターを製品に含める必要がなくなり、この責任をハブ製造元に任せることができます。共有オープンソースドライバーとライブラリは、冗長エンジニアリング作業をさらに削減します。一般的なサービス検出とデバイスセットアップのメカニズムは、アプリケーション開発のカスタマイズの必要性が少ないことを意味します。これらのインフラストラクチャとアプリケーションの開発コストの削減は、より手頃な価格のスマートホームデバイスの形でコンシューマーに渡すことができます。

カスタマーサポートの簡素化

スマートホーム市場での現在の断片化は、メーカーのカスタマーサポートの負担が大きくなります。コンシューマーは、接続、セットアップ、互換性に問題が発生し、トラブルシューティングが必要になることがよくあります。Matter は、コア関数を標準化することで、これらの問題を削減することを目指しています。

問題が発生すると、基盤となる一般的な Matter プロトコルにより、企業は複数のエコシステムを考慮することなく、より簡単に接続の問題を診断して解決できます。これにより、サポートプロセスが効率化されます。単一のアプリケーションと一般的な音声互換性により、お客様はデバイスの使用について簡単に学習できるため、多くの場合、サポートの必要性が軽減されます。Matter によって簡素化されたカスタマーエクスペリエンスとトラブルシューティングにより、メーカーの長期サポートコストを削減できます。

Matter 認定戦略に関する考慮事項

Matter は、さまざまなスマートホームデバイスとプラットフォーム間の相互運用を可能にします。ただし、Matter による認証は、デバイスメーカーにとって必ずしも最適な選択肢とは限らない場合があります。実装と認定のコストは、デバイスのタイプとユースケースによっては、実用的または財務的な意味をなさない場合があります。このセクションでは、メーカーが特定のデバイスを Matter で認証しないことを選択する主な理由をいくつか説明します。

Matter 標準は開発を簡素化し、ユニバーサルな互換性を可能にすることを目的としていますが、特定のタイプのスマートホームデバイスは、利点を上回る認定の実践的な障壁に直面する可能性があります。Matter で制約が厳しい製品、IP 以外のプロトコル、対象者が限られている製品、またはデバイスタイプが定義されていない製品の場合、Matter 認定の取得は最初は最適な戦略ではない可能性があります。メーカーが Matter の導入を避ける理由は、これらである可能性があります。ただし、Matter では、IP 対応ゲートウェイデバイスが IP 以外のエンドポイントをプロキシすることを許可しています。特定のレガシーデバイスの場合、ゲートウェイアプローチは、完全なデバイス再設計を回避しながら、Matter の互換性の実現可能なパスとなる可能性があります。

Matter 標準が進化し、その範囲が拡大してより多くのユースケースをカバーするにつれて、これらの製品カテゴリであっても、認定ケースは時間の経過とともに強化される可能性があります。デバイスメーカーは、Matter コンプライアンスに関する最適なアプローチを決定するために、特定の状況とロードマップを評価する必要があります。多くの場合、少なくとも一時的に認定をオプトアウトする技術的な理由やビジネス上の理由がある可能性があります。

IP 以外の接続プロトコル

Matter 標準を採用するには、デバイスは Wi-Fi、イーサネット、スレッドなどの IP ネットワークで動作する必要があります。Zigbee、Z-Wave、Bluetooth LE などの非 IP ワイヤレスプロトコルは、一般的に低帯域幅デバイスで使用されます。これらのプロトコルは、Matter と互換性を持つために、IP から IP へのプロトコル変換機能を追加する必要があります。通常、通信モジュールをアップグレードしたり、翻訳ゲートウェイを導入したりすると、デバイスのハードウェアコストが増加します。

IP スタックのサポートを追加すると、ネットワーク処理により多くのメモリと処理能力を割り当てることができます。これは、非常に低コストで低電力のデバイスの機能を超える可能性があります。IP をサポートするためにメモリやフラッシュを追加すると、製造コストが増加し、バッテリーの寿命も短縮されます。電源またはセンサーデータのオンとオフがすべて必要なユースケースでは、非 IP プロトコルが効率的なソリューションを提供します。

Matter は基本的に、IP 以外の独自のワイヤレス規格に依存するデバイスの認証を除外します。これにより、ローエンド製品の代替接続方法を使用したいメーカーが制限される可能性があります。Wi-Fi やイーサネットなどの IP ベースのプロトコルは、さまざまなエコシステムをインターフェイスするために必要ですが、IP 以外の標準は、一部のアプリケーションでのセンサーやスイッチの基本的な接続に価値があります。

ハードウェアの制限事項

もう 1 つの課題は、Matter が必要なソフトウェアスタックをサポートするために最低限のレベルのデバイス上の処理能力とメモリを必要とすることです。ただし、最も基本的なスマートホームデバイスでは、コストとサイズの制約により、組み込みチップ機能が非常に限られていることがよくあります。

例えば、シンプルなドアまたはウィンドウセンサーには、フラッシュメモリが 100 KB 未満で RAM が 10 KB 未満のマイクロコントローラーのみが含まれている場合があります。これにより、Matter を完全に実装するための十分なストレージと処理ヘッドルームが提供されません。より強力で高価なシリコンを追加すると、部品表が大幅に増加します。

コストとサイズが最優先事項である場合、メーカーは Matter 要件がハードウェア予算と一致していないと判断することがあります。Matter を使用して非常に基本的なセンサー、スイッチ、またはコントローラーを認証すると、手頃な価格に影響する不要なハードウェアのアップグレードを強制する可能性があります。

カスタマーエコシステム

考慮すべきもう 1 つの要因は、メーカーのターゲット顧客ベースが Matter と互換性のあるスマートホームプラットフォームを使用しているかどうかです。そのセグメントのほとんどのコンシューマーがMatterコントローラーやMatter対応ハブやアプリを使用していない場合、製品を認証するインセンティブはほとんどない可能性があります。

例えば、資格のあるユーザーのニーズへの対応に注力している企業は、Matter 管理者なしで顧客が簡単なセットアップをしていることに気付くかもしれません。または do-it-yourself 、 (DIY) ホームオートメーションの愛好家はカスタムソリューションを好み、ブランド間でMatter plug-and-play の経験を必要としないかもしれません。

ターゲット属性が Matter インフラストラクチャと連携しないシナリオでは、認証によって明確なメリットなしに複雑さが増します。Matter コンプライアンスに労力を振り向けるのではなく、関連プ

ラットフォーム内のユーザーエクスペリエンスの最適化にリソースを費やす方がよいかもしれません。

まだ定義されていないデバイスタイプ

Matter は現在、照明、HVAC、ロック、死角、エンターテイメントなど、一般的なスマートホームカテゴリのデバイスプロファイルと仕様のみを定義します。これらの定義された領域外のニッチな製品タイプは、デバイスタイプが標準化されるまでカスタムプロファイルを使用する必要があります。灌漑コントローラー、プール機器、ニッチアプライアンスなど、リストされている垂直以外のデバイスカテゴリは、まだ Matter を使用できません。

企業が既存の Matter プロファイルの対象ではない一意のデバイスタイプを開発した場合、新しいプロファイルがドラフトされるまで認定はできません。これにより、Matter がその範囲を拡大するのを待っている間に、新製品の発売が遅れる可能性があります。

イノベーションのリリースを止めるのではなく、一部のメーカーは独自の手段でニッチなソリューションを市場に早く投入することを好むかもしれません。後で認証することは、関連するプロファイルが成熟した後も引き続きオプションです。ファーストマバーの利点として、Matter direct-to-consumer を使用しない方が望ましい場合があります。

代替方法: ゲートウェイでのプロキシ

エンドポイントデバイスに Matter の直接認証を妨げる制限がある場合、代替アプローチとして、ゲートウェイでデバイスの Matter 機能をプロキシする方法があります。ゲートウェイは、エンドポイントのローカルワイヤレスプロトコルと IP ベースの Matter プロトコルを変換するブリッジとして機能します。

例えば、独自の無線規格を介して通信する基本的な温度センサーは、Matter 管理者にMatterデバイスとして表示される可能性があります。ゲートウェイは、非 IP インターフェイスでセンサーデータを受信しますが、そのデータを表す仮想 Matter エンティティを IP 経由でコントローラーに公開します。これにより、既存のハードウェアを使用し、ゲートウェイを通じて相互運用性のメリットを得ることができます。

もちろん、これによりデベロッパーの複雑さが増し、必要な翻訳レイヤーをサポートするゲートウェイが必要になります。ただし、デバイス自体にとって直接認証が難しすぎる場合は、実行可能な侵害である可能性があります。プロキシは、ハードウェアを完全にオーバーホールすることなく、低電力またはニッチなソリューションが Matter エコシステムに参加するのに役立ちます。

Matter とのクラウド接続

Matter は基本的なローカルデバイスの相互運用性を可能にしますが、堅牢な over-the-air 更新、テレメトリデータ、リモート管理、および独自のベンダーサービスとの統合を提供するには、追加のクラウド接続が必要です。デバイスメーカーには、Matter ゲートウェイハブの配送、世帯のMatter認定ハブの使用、エンドポイントへの直接クラウド接続の統合などのオプションがあります。M atter-to-cloud 接続の標準が登場しましたが、メーカーは引き続き追加の接続ソフトウェアスタックを Matter デバイスに統合する必要があります。診断や新機能の更新などの領域でスマートホームデバイスのフルバリューを実現するには、Matter メーカーは基本的なローカルオペレーションだけでなく、クラウド統合を検討する必要があります。

重要エンドポイントのクラウド接続による高度なデバイス機能の有効化

Matter 標準は、共通のプロトコルを通じてさまざまなベンダーの IoT デバイスを統合することを約束します。イーサネット、Wi-Fi、スレッドなどの IP ベースのネットワークテクノロジーを使用して、スマートホームデバイスがローカルネットワーク上で相互に検出、通信、相互運用する方法を指定します。このローカル相互運用性により、さまざまなベンダーの Matter 認定デバイスが、自動化されたシーンや音声制御などのアクティビティでシームレスに連携できるようになります。ただし、Matter はクラウドインターフェイスを定義せず、デバイスエンドポイントにインターネット接続を必要としません。

現在、多くのスマートデバイスは、 over-the-air (OTA) 更新、リモートアクセス、製造元プラットフォームとの統合など、主要な機能のために追加のクラウド接続に依存しています。高度な機能を維持しながら Matter 準拠製品を構築しようとしているデバイスメーカーは、Matter をクラウド接続で補完することに関する設計上の考慮事項に直面しています。基本的なローカルコントロールと音声アシスタントの統合はシンプルな Matter デバイスでは機能しますが、より高度な機能を有効にするには追加のクラウド接続が必要です。

クラウド接続を必要とするユースケース

Matter はローカルデバイスの相互運用性を処理しますが、クラウド接続を追加すると、いくつかの重要なスマートホームデバイス機能が可能になります。

- O ver-the-air (OTA) 更新 – インターネット経由でファームウェアとソフトウェアの更新を配信することで、ベンダーはデプロイ済みのデバイスを簡単に強化できます。OTA を使用しない場合、更

新は手動で処理されます。Matter 標準では、OTA 更新の処理方法と Matter 認定エンドポイントへの配信方法が説明されていますが、エンドポイントが接続されている Matter ハブでサポートされている機能によって異なります。さらに、エンドポイントに提供される更新には制限があります。例えば、エンドポイントが更新をリクエストすると、利用可能な最新の更新のみが提供されます。同じタイプのすべてのデバイスには、1 回の更新で提供されます。シーケンシャル更新や、更新の OTA ロールバックや削除を行うオプションはありません。エンドポイントでクラウド接続を有効にすると、OTA 更新のきめ細かな管理の欠如を軽減できます。

- リモートアクセスと制御 — ホームネットワークの外部からリモートでデバイスにアクセスして制御するには、クラウドエンドポイントが必要です。Matter は、現在定義されているように、ローカルアクセスのみをサポートします。Matter エンドポイントはローカルネットワーク内のユーザーアプリで制御できますが、リモートコントロールは Matter ハブでサポートされている場合にのみ使用できます。それでも、通常は基本的なリモートコントロールのみを使用できます。
- テレメトリと診断 — エラーログやセンサーストリームなどのフィールドデータをクラウドに集約することで、ベンダーはデバイスのヘルスをモニタリングし、問題を特定できます。Matter は一般的な診断クラスターを通じて無線およびプロトコル関連の診断をサポートしていますが、デバイスに固有の詳細な診断には、製造元がデバイスからデータを取得できるようにクラウド接続が必要です。
- ベンダー固有の統合 — Matter 仕様で定義されていないカスタム機能やデータ型には、ベンダーのクラウドプラットフォームへの接続が必要です。
- 外部統合 – Matter エコシステムやサードパーティー支払いゲートウェイ (ユースケースに応じて必要) にない音声アシスタントなどのサードパーティーサービスにリンクするには、Matter 管理者以外のインターネット接続が必要です。

これらの重要な機能はクラウド接続に依存しているため、Matter エンドポイントにはインターネットアクセスの追加オプションが必要になることがよくあります。

クラウド接続を有効にするアーキテクチャ

Matter デバイスの場合、ローカルオペレーションの仕様を満たしながら必要なクラウド接続を提供するには、3 つの一般的なアプローチがあります。

ゲートウェイが組み込まれたスマートホームハブ

一部のデバイスメーカーは、Matter 管理者とクラウドサービスへのゲートウェイの両方を組み込んだ独自のホームハブを出荷することを選択する場合があります。このホームハブは、アタッチされた Matter エンドポイントを標準に従ってローカルに管理し、高度な機能のクラウド接続も円滑化し

ます。ハブは、エンドポイントの OTA 更新、リモートアクセス、テレメトリ収集をサポートできます。

クラウド接続を既存の Matter ハブにオフロードする

デバイスは、カスタムハブをバンドルするのではなく、Amazon Echo や Google Home などの Matter ハブに接続してインターネット接続できるように設計できます。この場合、既存の Matter ハブは標準に従ってローカルデバイス通信を処理し、それを必要とするエンドポイントのクラウドへのゲートウェイも提供します。これは、コンシューマーが既に持っている可能性のあるインフラストラクチャを利用します。ただし、このアプローチは、標準で Matter ハブの標準として指定されていない機能に対して Matter ハブによって提供されるサポートのレベルによって異なります。

エンドポイントでのクラウド直接接続

Wi-Fi などの直接インターネット接続を備えたデバイスは、Matter ローカルネットワークとベンダークラウドサービス用に別々の接続を統合することができます。これにより、デバイスはクラウドへの独自のゲートウェイとして機能します。ただし、Thread などのプロトコルに依存する非 Wi-Fi エンドポイントにはソリューションが必要です。これにより、デバイスはクラウドに個別に接続できますが、シンプルで低コストのバッテリー駆動デバイスでは不可能な場合があります。

Bridging Matter と製造元のクラウドプラットフォーム

Matter はローカルの相互運用性を簡素化しますが、Matter 管理システムと製造元のクラウドプラットフォームをスムーズに接続するには、追加の労力が必要です。Connectivity Standards Alliance (CSA) などの組織は、Matter デバイスがクラウドとやり取りして OTA 更新などの機能をどのように標準化するかに取り組んでいます。このクラウド接続の標準を広く採用することで、デバイスメーカーの開発が容易になります。

最適な方法は、特定の製品のユースケース、価格ポイント、ビジネスモデルによって異なります。スマートホームコンシューマーが期待するすべての機能を引き出すには、ローカルの相互運用性に焦点を当てた Matter 準拠のデバイスであっても、クラウドサービスへの堅牢なアクセスが必要であることは明らかです。デバイスメーカーは、慎重に設計されたクラウド接続を通じて高度な機能を提供しながら、相互運用性のためにMatterを使用する機会があります。

セキュリティ

設計によるセキュリティとは、デバイス設計段階でセキュリティ機能を組み込む方法であり、開発の後半段階では後述するものではありません。暗号化通信と over-the-air (OTA) 更新は、設計上のセキュリティの例です。Matter は、信頼できる安全な製造施設からセキュリティを設計によって実装することで、スマートホームデバイスの強固な基盤を提供します。Matter デバイスは、信頼できる既知の製品認証局 (PAA) 認証局 (CA) の所有者のみが製造およびプロビジョニングできます。

デバイス認証

Matter デバイスは、通信する前に相互に認証し、コントローラーに対して認証する必要があります。Matter ファブリックに接続できるのは、認可されたデバイスのみです。製造中、デバイスは一意の ID と、デバイス認証証明書 (DAC) と呼ばれる X.509 証明書でプロビジョニングされます。デバイスが Matter ファブリックに初めて接続しようとすると、コミッショナーデバイスは DAC の有効性と、それが既知の信頼できる製品認証中間 (PAI) CA によって署名されていることを確認します。コミッショナーデバイスは、ネットワークに接続しようとしているデバイスが Matter の仕様、プロトコル、およびセキュリティ標準に準拠しているかどうかも確認します。デバイスには、すべてのチェックが成功した場合にのみ Matter ファブリックへのアクセスが許可されます。

暗号化された通信

デバイスに Matter ファブリックへのアクセスが許可されると、デバイス間で渡されるすべてのデータは強力な暗号化によって保護されます。データの整合性は、多層アプローチを使用して保持されます。Matter コミッショナーは、ECC-256 secp256r1 曲線を使用してキー交換と署名の検証を実行します。キーの交換後、Matter デバイスは AES-256 を使用して転送中のデータを暗号化します。メッセージごとに、デバイスは SHA-256 アルゴリズムを使用して、送信中にデータが改ざんされていないことを確認します。

O ver-the-air 更新

Matter 標準では、デバイスは over-the-air (OTA) 更新のための堅牢なセキュリティ体制を実装する必要もあります。OTA はスマートホームエコシステムの重要な部分であり、デバイスが新しい機能とともにセキュリティアップデートを受信できるようにします。Matter デバイスの各ファームウェア更新は、製造元のプライベートキーによって署名される必要があります。デバイスは、対応する非対称パブリックキーを使用してペイロード署名を検証します。ペイロードの署名が検証されると、デバイスはイメージをブートローダーにコミットしてリセットできます。起動プロセス中に、デバイスは

イメージを再度検証して改ざんされていないことを確認する必要があり、既知の最新バージョンが実行されていることも検証します。

Matter による開発

Alexa の使用

Amazon は Matter 開発用の包括的なツールスイートを提供しています。これらのツールは、すべての主要なエコシステムと互換性があり、Amazon Alexa とシームレスに連携するMatter製品を構築するための迅速な道を提供します。

プログラム: Alexa と連携

このプログラムにより、Alexa に接続されたデバイスが優れたカスタマーエクスペリエンスを提供できるようになります。Works with Alexa (WWA) バッジは、顧客の信頼度を高め、認定済みデバイスの優先設定を促進します。詳細については、「Matter Launch の発表」および「Matter デバイス用の Alexa との連携 (WWA) の紹介」(Amazon ブログ記事) を参照してください。

SDK: Alexa で Matter を開発する

この SDK を使用すると、マネージドクラウド接続、ビジネスインテリジェンス、OTA サポートを含めながら、デバイスにローカル Matter 接続を追加できます。詳細については、「Alexa でMatterを最大限に活用する」を参照してください。

キット: Alexa アンビエントホームデベロッパーキット

このキットは、Alexa でアンビエントで統合されたスマートホームを構築するために、プロトコル間でデバイスと統合するのに役立ちます。詳細については、「Amazon Alexa」を参照してください。

エンドポイント: コミッショナブルエンドポイント

スキル接続された Matter デバイスの場合、コミッショナブルエンドポイント API は、顧客がアクセス許可を持つ必要な手順なしで、Alexa デバイスへのMatterベースのローカル接続を作成します。詳細については、「Alexa.Commissionable Interface 1.0 (Alexa Skills Kit)」を参照してください。

AWS Private CA Matter のサポート

AWS Private Certificate Authority （ AWS Private CA) は Matter 標準の使用に関するガイダンスを提供します。

Matter の DAC

Matter には、Matter パブリックキーインフラストラクチャ (PKI) 証明書ポリシー (CP) に準拠するデバイス認証 CA によって発行されるデバイス認証証明書 (DAC) が必要です。デバイスベンダーは、AWS Private CA を使用して次のことを実行できます。

- 製品認証局 (PAA) 認証局 (CA) をホストする
- 製品認証中間 (PAI) CA をホストする
- 各デバイスの DAC を発行、署名、維持する

詳細については、 AWS セキュリティブログの「 AWS Private Certificate Authority を使用して Matter のデバイス認証証明書を発行する」を参照してください。

Matter のインフラストラクチャ

AWS は、 を使用して Matter AWS Cloud Development Kit (AWS CDK)の PKI インフラストラクチャをセットアップする例を示しています。Matter PKI CP の要件を満たす AWS Private CA ために を使用します。詳細については、 の「Matter PKI CDK project」を参照してください GitHub。

Java サンプル

AWS Private CA は、Matter 準拠の製品認証機関 (PAA) 証明書、製品認証中間 (PAI) 証明書、およびデバイス認証証明書 (DACs) を作成するための Java サンプルを提供します。詳細については、AWS Private Certificate Authority ドキュメントの AWS Private CA 「 API を使用して Matter 標準を実装する (Java の例) 」を参照してください。

Matter PKI コンプライアンスガイド

この Matter PKI コンプライアンスガイドでは、CSA Matter PKI CP 要件への準拠を実装し、実証する方法について説明します。を使用して Matter 準拠の認証機関 (CAs) AWS Private CA を作成および運用する方法に関する情報を提供します。

よくある質問

Matter のメンバーシップレベルはどのくらいですか？

2023 年 1 月現在、Matter には次の 4 つのレベルのメンバーシップがあります。

メンバータイプ	年間メンバーシップ料金 (USD)	説明
主催者	105,000 USD	すべての標準の最終承認で取締役会を主導し、取締役会の席を確保し、取締役会の委員会に参加する
Participant	20,000 USD	標準に貢献し、ドラフト仕様にアクセスして市場投入を迅速化する
アダプター	7,000 USD	承認された仕様を使用して製品を構築および認証する
関連付け	0 USD*	認定移管プログラムを通じて認定製品にラベルを付ける

* 製品をホワイトラベルまたはリブランドするアソシエイトメンバーの場合、製品ごとに 2,500 USD (USD) の初期料金と、製品ごとに 1 年あたり 500 USD の継続料金がかかります。

選択するメンバーシップレベルは、製品の認証 (アダプター) または標準内の製品タイプの定義 (参加者) に対する関心によって異なります。メンバーシップレベルの詳細については、CSA ウェブサイトの「Impact the Future of the IoT」を参照してください。

スマートホームコンシューマーは Matter からどのようなメリットを得られますか？

コンシューマーは、以下の点で Matter の恩恵を受けます。

- Matter デバイスの自宅へのオンボーディングを簡素化
- 1 つのアプリケーションによるすべてのスマートホームデバイスの統合管理
- 異なるエコシステムの 1 つ以上の音声アシスタントからのデバイス制御

詳細については、このガイドの「スマートホームコンシューマー向けの Matter 認定の利点」を参照してください。

デバイスメーカーは Matter からどのようにメリットを得ていますか？

デバイスメーカーは、以下の点で Matter の恩恵を受けます。

- Amazon Alexa や Google Home など、各エコシステムで複数の証明書を使用する代わりに、デバイスの単一の証明書。
- アプリの開発が不要になりました
- インフラストラクチャ要素 (スレッドボーダールーターなど) を出荷する必要がないため、マテリアルのコストを削減
- インフラストラクチャと接続の問題があるお客様をサポートするためのコストの削減

詳細については、このガイドの「デバイスメーカー向けの Matter 認定の利点」を参照してください。

Matter は Wi-Fi、Bluetooth、または Thread を置き換えますか？

いいえ、Matter は IP ネットワーク上で実行されるアプリケーションレベルのプロトコルです。接続に Wi-Fi、イーサネット、または Thread を使用するデバイスは、Matter 認定を受ける可能性があります。次の表は、Matter と Wi-Fi、Bluetooth、Thread の対比をまとめたものです。

機能	Matter	Wi-Fi	Bluetooth	Thread
目的	スマートホーム通信	インターネットアクセスとデータ転送	短距離ワイヤレス通信	低電力ワイヤレスメッシュネットワーク

機能	Matter	Wi-Fi	Bluetooth	Thread
[Range] (範囲)	基盤となるプロトコルによって異なります	最大 300 フィート	最大 30 フィート	最大 300 フィート
[帯域幅]	基盤となるプロトコルによって異なります	1 秒あたり最大 10 ギガビット	1 秒あたり最大 2 メガビット	1 秒あたり最大 250 キロビット
消費電力	基盤となるプロトコルによって異なります	比較的高い	比較的低い	非常に低い
セキュリティ	基盤となるプロトコルによって異なります	WPA2, WPA3	AES、BLE セキュア接続	AES
コスト	デバイスによって異なります	比較的安価	比較的安価	比較的高価

ベンダー ID と製品 ID とは

CSA メンバーは、サプライヤーとして識別するベンダー ID を申請できます。今後、会社の製品はこの ID に割り当てられ、そのオリジンまで遡ることができます。さらに、一意の製品 ID を受け取ります。16 桁の数値コードは、パスポート番号などの製品に付属しており、ベンダーと区別できないものとしてレンダリングされます。

Matter 認定が必要なデバイス

Matter ファブリックを認証し、その一部である必要があるデバイスは、Matter 認定を受ける必要があります。ただし、非標準 (専有) プロトコルを介してベンダー指定のハブとのみやり取りするように設計されたデバイスは、Matter 認定プロセスからメリットを得ません。例えば、スマートホームセキュリティシステムハブは Matter 苦情として認定される必要がありますが、ハブと通信するドアまたはウィンドウセンサーは Matter 準拠として認定される必要はありません。Matter の認定を受けるかどうかの選択は、主にこの考慮事項によって決まります。

私の製品タイプは現在 Matter で定義されていません。Matter 認定を受けるには、 にどのような追加タスクを予算に入れる必要がありますか？

Matter 仕様は、すべてのタイプのデバイスをサポートしているわけではありません。デバイスタイプがサポートされていない場合、最初のステップは参加者として CSA に参加することです。これには、CSA への財務と時間投資が必要です。参加者メンバーとして、デバイスタイプの定義を主導し、より迅速な go-to-market 戦略を可能にする仕様のドラフトにアクセスできます。メンバーシッププレベルの詳細については、CSA ウェブサイトの「Impact the Future of the IoT」を参照してください。

一部のデバイスは、ホーム Wi-Fi ネットワークに直接接続します。これらのデバイスは Matter 認定を受ける必要がありますか？

Matter 認定は、Matter ファブリックに接続できるため、スマートホームネットワークに直接接続するデバイスにとってメリットがあります。これにより、コンシューマーは同じ Matter ファブリック上の仮想アシスタントを通じてデバイスを制御できます。ただし、コンシューマーはベンダー固有で Matter 仕様で定義されていないオペレーションには、デバイス固有のアプリケーションを使用する必要があります。

リソース

AWS リソース

- Alexa で Matter を最大限に活用する
- Matter デバイス向けの Matter Launch and Introduction Works with Alexa (WWA) の発表 (Amazon Alexa ブログ)

IoT 用 Connectivity Standards Alliance (CSA)

- CSA ウェブサイト
- CSA 認定プロセスの概要
- CSA 認定テストプロバイダー
- Matter の仕様

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	—	2024 年 2 月 5 日

AWS 規範的ガイダンスの用語集

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

数字

7 Rs

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

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

- 使用停止 — お客様のソース環境で不要になったアプリケーションを停止または削除します。

A

ABAC

「属性ベースのアクセスコントロール」を参照してください。

抽象化されたサービス

「 マネージドサービス」を参照してください。

ACID

「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

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

AI

「人工知能」を参照してください。

AIOps

「人工知能オペレーション」を参照してください。

匿名化

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

アンチパターン

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

アプリケーションコントロール

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

アプリケーションポートフォリオ

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

人工知能 (AI)

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

AI オペレーション (AIOps)

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

非対称暗号化

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

原子性、一貫性、分離性、耐久性 (ACID)

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

属性ベースのアクセス制御 (ABAC)

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

信頼できるデータソース

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

アベイラビリティーゾーン

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

AWS クラウド導入フレームワーク (AWS CAF)

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

AWS ワークロード認定フレームワーク (AWS WQF)

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

B

不正なボット

個人や組織に混乱や損害を与えることを目的としたボット。

BCP

「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、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インタラクションをシミュレートするソフトウェアアプリケーション。インターネット上の情報のインデックスを作成するウェブクローラーなど、一部のボットは有用または有益です。悪質なボット と呼ばれる他のボッ

トの中には、個人や組織に混乱を与えたり、損害を与えたりすることを意図しているものがあります。

ボットネット

マルウェアに感染し、ボットのヘルダーまたはボットオペレーター と呼ばれる、単一関係者の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

例外的な状況や承認されたプロセスを通じて、ユーザーが通常アクセス許可を持たない AWS アカウント 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低速かつ増分的なリリース。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 ワークロードに負荷をかけ、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 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 の投稿」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。移行戦略とどのように関連しているかについては、 AWS 「移行準備ガイド」を参照してください。

CMDB

「設定管理データベース」を参照してください。

コードリポジトリ

ソースコードやその他の資産 (ドキュメント、サンプル、スクリプトなど) が保存され、バージョン管理プロセスを通じて更新される場所。一般的なクラウドリポジトリには、 GitHub または が含まれます AWS CodeCommit。コードの各バージョンはブランチと呼ばれます。マイクロサー

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

コールドキャッシュ

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

コールドデータ

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

コンピュータビジョン (CV)

機械学習を使用してデジタルイメージやビデオなどのビジュアル形式から情報を分析および抽出する AI の分野。例えば、 はオンプレミスのカメラネットワークに CV を追加するデバイス AWS Panorama を提供し、Amazon SageMaker 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。

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

一元化された管理とガバナンスにより、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。信頼できる ID のみが、期待されるネットワークから信頼できるリソースにアクセスしていることを確認できます。詳細については、「 でのデータ境界の構築 AWS」を参照してください。

データの前処理

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

データ出所

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

データ件名

データを収集、処理している個人。

データウェアハウス

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

データベース定義言語 (DDL)

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

データベース操作言語 (DML)

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

DDL

「データベース定義言語」を参照してください。

ディープアンサンブル

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

ディープラーニング

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

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 に採用するときは 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、 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 ガバナンス要件への準拠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。

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。

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 (アカウンティング、MES、プロジェクト管理など) を自動化および管理するシステム。

エンベロープ暗号化

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

環境

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

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

エピック

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

ERP

「エンタープライズリソース計画」を参照してください。

探索的データ分析 (EDA)

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

F

ファクトテーブル

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

フェイルファスト

開発ライフサイクルを短縮するために頻繁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。

障害分離境界

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

機能ブランチ

「ブランチ」を参照してください。

特徴量

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

特徴量重要度

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

機能変換

追加のソースによるデータのエンリッチ化、値のスケーリング、単一のデータフィールドからの複数の情報セットの抽出など、機械学習プロセスのデータを最適化すること。これにより、機械学習モデルはデータの恩恵を受けることができます。例えば、「2021-05-27 00:15:37」の日付を「2021 年」、「5 月」、「木」、「15」に分解すると、学習アルゴリズムがさまざまなデータコンポーネントに関連する微妙に異なるパターンを学習するのに役立ちます。

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。

G

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 では CloudFront、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。

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 AWS Security Hub、GuardDuty、Amazon Inspector AWS Trusted Advisor、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。

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。緊急性のため、通常、修正は一般的な DevOps リリースワークフローの外で行われます。

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

IIoT

「産業モノのインターネット」を参照してください。

イミュータブルインフラストラクチャ

既存のインフラストラクチャを更新、パッチ適用、または変更するのではなく、本番ワークロード用の新しいインフラストラクチャをデプロイするモデル。イミュータブル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 (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

接続、リアルタイムデータ、自動化、分析、AI/ML の進歩を通じて、 のビジネスプロセスのモダナイズを指すために 2016 年に Klaus Schwab によって導入された用語。

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、「AWS を使用した機械学習モデルの解釈」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 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。

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 サービス がインフラストラクチャレイヤー、オペレーティングシステム、プラットフォーム AWS を運用し、ユーザーがエンドポイントにアクセスしてデータを保存および取得します。Amazon Simple Storage Service (Amazon S3) と Amazon DynamoDB は、 マネージドサービスの例です。これらは抽象化されたサービス とも呼ばれます。

製造実行システム (MES)

生産プロセスを追跡、モニタリング、文書化、制御するためのソフトウェアシステム。これにより、加工品を現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、調整のために結果を検査する完全なプロセス。メカニズムとは、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

内の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の machine-to-machine (M2M) 通信プロトコル。

マイクロサービス

明確に定義された API を介して通信し、通常は小規模な自己完結型のチームが所有する、小規模で独立したサービスです。例えば、保険システムには、販売やマーケティングなどのビジネス機能、または購買、請求、分析などのサブドメインにマッピングするマイクロサービスが含まれる場合があります。マイクロサービスの利点には、俊敏性、柔軟なスケーリング、容易なデプロ

イ、再利用可能なコード、回復力などがあります。詳細については、AWS 「サーバーレスサービスを使用したマイクロサービスの統合」を参照してください。

マイクロサービスアーキテクチャ

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

Migration Acceleration Program (MAP)

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

大規模な移行

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

移行ファクトリー

自動化された俊敏性のあるアプローチにより、ワークロードの移行を合理化する部門横断的なチーム。移行ファクトリーチームには、通常、オペレーション、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: Application Migration Service を使用して Amazon EC2 AWS 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、組織のクラウド対応状況に関するインサイトを取得し、長所と短所を特定し、特定されたギャップを埋めるためのアクションプランを構築するプロセス。詳細については、移行準備状況ガイド を参照してください。MRA は、AWS 移行戦略の第一段階です。

移行戦略

ワークロードを に移行するために使用されるアプローチ AWS クラウド。詳細については、この用語集の「7 Rs エントリ」と「組織を動員して大規模な移行を加速する」を参照してください。

ML

「機械学習」を参照してください。

モダナイゼーション

古い (レガシーまたはモノリシック) アプリケーションとそのインフラストラクチャをクラウド内の俊敏で弾力性のある高可用性システムに変換して、コストを削減し、効率を高め、イノベーションを活用します。詳細については、「」の「アプリケーションをモダナイズするための戦略 AWS クラウド」を参照してください。

モダナイゼーション準備状況評価

組織のアプリケーションのモダナイゼーションの準備状況を判断し、利点、リスク、依存関係を特定し、組織がこれらのアプリケーションの将来の状態をどの程度適切にサポートできるかを決定するのに役立つ評価。評価の結果として、ターゲットアーキテクチャのブループリント、モダナイゼーションプロセスの開発段階とマイルストーンを詳述したロードマップ、特定され

たギャップに対処するためのアクションプランが得られます。詳細については、「」の「アプリケーションのモダナイゼーション準備状況の評価 AWS クラウド」を参照してください。

モノリシックアプリケーション (モノリス)

緊密に結合されたプロセスを持つ単一のサービスとして実行されるアプリケーション。モノリシックアプリケーションにはいくつかの欠点があります。1 つのアプリケーション機能エクスペリエンスの需要が急増する場合は、アーキテクチャ全体をスケーリングする必要があります。モノリシックアプリケーションの特徴を追加または改善することは、コードベースが大きくなると複雑になります。これらの問題に対処するには、マイクロサービスアーキテクチャを使用できます。詳細については、モノリスをマイクロサービスに分解する を参照してください。

MPA

「移行ポートフォリオ評価」を参照してください。

MQTT

「Message Queuing Telemetry Transport」を参照してください。

多クラス分類

複数のクラスの予測を生成するプロセス (2 つ以上の結果の 1 つを予測します)。例えば、機械学習モデルが、「この製品は書籍、自動車、電話のいずれですか?」 または、「このお客様にとって最も関心のある商品のカテゴリはどれですか?」と聞くかもしれません。

変更可能な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 Framework 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

「 オペレーション統合」を参照してください。

OLA

「運用レベルの契約」を参照してください。

オンライン移行

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

OPC-UA

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

オープンプロセス通信 - 統合アーキテクチャ (OPC-UA)

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

オペレーショナルレベルアグリーメント (OLA)

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

運用準備状況レビュー (ORR)

インシデントや潜在的な障害の理解、評価、防止、または範囲の縮小に役立つ質問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「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)

産業運用、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 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

の組織 AWS アカウント 内のすべての のすべてのイベントを口グ 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、 ドキュメントの「組織の証跡の作成」を参照してください。 CloudTrail

組織変更管理 (OCM)

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

では CloudFront、Amazon Simple Storage Service (Amazon S3) コンテンツを保護するためのアクセスを制限するための拡張オプションです。OAC は、すべての 内のすべての S3 バケット AWS リージョン、 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)

では CloudFront、Amazon S3 コンテンツを保護するためのアクセスを制限するオプションです。OAI を使用する場合、 は Amazon S3 が認証できるプリンシパル CloudFront 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。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

「運用技術」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るネットワーク接続を処理する VPC。AWS Security Reference Architecture では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

P

アクセス許可の境界

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

個人を特定できる情報 (PII)

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

PII

「個人を特定できる情報」を参照してください。

プレイブック

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

PLC

「プログラム可能なロジックコントローラー」を参照してください。

PLM

「製品ライフサイクル管理」を参照してください。

ポリシー

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

多言語の永続性

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

ポートフォリオ評価

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

述語

`true` または を返すクエリ条件。`false`通常は `WHERE`句にあります。

述語のプッシュダウン

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 ロール AWS アカウント、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

エンジニアリングプロセス全体を通し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のアプローチ。

プライベートホストゾーン

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

プロアクティブコントロール

非準拠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「 での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、製品のデータとプロセスのライフサイクル全体にわたる管理、および辞退と削除。

本番環境

「環境」を参照してください。

プログラミング可能ロジックコントローラー (NAL)

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

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

Q

クエリプラン

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

クエリプランのリグレッション

データベースサービスのオプティマイザーが、データベース環境に特定の変更が加えられる前に選択されたプランよりも最適性の低いプランを選択すること。これは、統計、制限事項、環境設

定、クエリパラメータのバインディングの変更、およびデータベースエンジンの更新などが原因である可能性があります。

R

RACI マトリックス

責任、説明責任、相談、情報 (RACI) を参照してください。

ランサムウェア

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

RASCI マトリックス

責任、説明責任、相談、情報 (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。

再構築

「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 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 から分離され、独立しています。詳細については、AWS リージョン 「 を使用できるアカウントを指定する」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 Rs」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 Rs」を参照してください。

回復性

中断に耐えたり、中断から回復したりするアプリケーションの機能。で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。

ローテーション

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

行と列のアクセス制御 (RCAC)

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

RPO

「目標復旧時点」を参照してください。

RTO

「目標復旧時間」を参照してください。

ランブック

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

S

SAML 2.0

多くの ID プロバイダー (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 にログイン AWS

Management Console したり、組織内のすべてのユーザーを IAM で作成しなくても 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

では AWS Secrets Manager、暗号化された形式で保存するパスワードやユーザー認証情報などの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。

セキュリティコントロール

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

セキュリティ強化

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

Security Information and Event Management (SIEM) システム

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

セキュリティレスポンスの自動化

セキュリティイベントに自動的に応答または修正するように設計された、事前定義され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。自動レスポンスアク

ションの例としては、VPC セキュリティグループの変更、Amazon EC2 インスタンスへのパッチ適用、認証情報のローテーションなどがあります。

サーバー側の暗号化

送信先にあるデータの、それを受け取る AWS サービス 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 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 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、お客様はクラウドのセキュリティを担当します。詳細については、責任共有モデルを参照してください。

SIEM

「セキュリティ情報とイベント管理システム」を参照してください。

単一障害点 (SPOF)

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

SLA

「サービスレベルアグリーメント」を参照してください。

SLI

「サービスレベルインジケータ」を参照してください。

SLO

「サービスレベルの目標」を参照してください。

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。

監視統制とデータ収集 (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。

T

タグ

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

ターゲット変数

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

タスクリスト

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

テスト環境

「環境」を参照してください。

トレーニング

お客様の機械学習モデルに学習するデータを提供すること。トレーニングデータには正しい答えが含まれている必要があります。学習アルゴリズムは入力データ属性をターゲット (お客様が予測したい答え) にマッピングするトレーニングデータのパターンを検出します。これらのパター

ンをキャプチャする機械学習モデルを出力します。そして、お客様が機械学習モデルを使用して、ターゲットがわからない新しいデータでターゲットを予測できます。

トランジットゲートウェイ

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

トランクベースのワークフロー

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

信頼されたアクセス

ユーザーに代わって AWS Organizations およびそのアカウントで組織内でタスクを実行するために指定するサービスへの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小さな DevOps チーム。ツーピザチームの規模では、ソフトウェア開発におけるコラボレーションに最適な機会が確保されます。

U

不確実性

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

未分化なタスク

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

上位環境

「環境」を参照してください。

V

バキューミング

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

バージョンコントロール

リポジトリ内のソースコードへの変更など、変更を追跡するプロセスとツール。

VPC ピアリング

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

脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

W

ウォームキャッシュ

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

ウォームデータ

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

ウィンドウ関数

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

ワークロード

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

ワークストリーム

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

WORM

「書き込み 1 回」を参照し、多くの を読み取ります。

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な 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。

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。