の暗号化のベストプラクティスと機能 AWS のサービス

AWS 規範ガイダンス

AWS 規範ガイダンス: の暗号化のベストプラクティスと機能 AWS のサービス

Table of Contents

の暗号化のベストプラクティスと機能 AWS のサービス

Kurt Kumar、Amazon Web Services

2026 年 2 月 (ドキュメント履歴)

暗号化は、デジタル時代の機密データを保護するための基本的なサイバーセキュリティツールです。組織は生成 AI のデプロイなど、運用を推進するためにデータにますます依存しているため、堅牢な暗号化プラクティスを通じてこの貴重な情報を保護することは、包括的なデータ保護戦略の重要な要素です。このガイドは、暗号化の原則と が提供する AWS 暗号化機能を理解するのに役立ちます。

最新のサイバーセキュリティの脅威には、データ侵害のリスクが含まれます。これは、情報アセットへの不正アクセスによってデータが失われた場合です。データは、各組織に固有のビジネスアセットです。これには、顧客情報、事業計画、設計文書、コードなどが含まれます。ビジネスを保護するということは、データを保護するということです。

データ暗号化は、侵害が発生した後でもビジネスデータを保護するのに役立ちます。意図しない開示に対する防御レイヤーを提供します。 AWS クラウド内の暗号化されたデータにアクセスするには、ユーザーは、キーを使用して復号化する権限と、データが保存されているサービスを使用する権限を必要とします。この両方の権限がないと、ユーザーはデータを復号化して表示することができません。

通常、暗号化できるデータは 3 種類あります。1 つは転送中のデータで、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のことです。もう 1 つは保管中のデータで、ストレージ内のデータなど、静止していて休眠中のデータのことです。例としては、ブロックストレージ、オブジェクトストレージ、データベース、アーカイブ、モノのインターネット (IoT) デバイスなどです。使用中のデータとは、アプリケーションまたはサービスがアクティブに処理または使用しているデータを指します。組織は、使用時にデータを保護することで、意図しない開示のリスクを軽減できます。

このガイドでは、転送中のデータと保管中のデータを暗号化するための考慮事項とベストプラクティスについて説明します。また、多くの で使用できる暗号化機能とコントロールについても確認します AWS のサービス。これらの暗号化レコメンデーションは、 AWS クラウド 環境のサービスレベルで実装できます。

対象者

このガイドは、公共機関と民間企業の両方の、小規模、中規模、大規模の組織で使用できます。組織がデータ保護戦略の評価と実施の初期段階にあるか、または既存のセキュリティ管理の強化を目指しているかにかかわらず、このガイドで説明する推奨事項は次の対象者に最適です。

- 最高経営責任者 (CEO)、最高技術責任者 (CTO)、最高情報責任者 (CIO)、最高情報セキュリティ責任者 (CISO) など、企業の方針を策定する執行役員
- 技術担当副社長や取締役など、技術標準の設定を担当する技術責任者
- 以下の責任を負うビジネスステークホルダーとアプリケーションオーナー
  - リスク体制、データ分類、保護要件の評価
  - 確立された組織基準の遵守状況の監視
- 法定および任意のコンプライアンス制度を含む、コンプライアンスポリシーの遵守状況の監視を担当するコンプライアンス、内部監査、ガバナンス担当者

AWS 暗号化へのアプローチ

暗号化アルゴリズムは、機密性 (暗号化) 、信頼性 (メッセージ認証コードとデジタル署名) 、否認防止 (デジタル署名) などのセキュリティサービスを提供するように設計された数学的な構造です。暗号化、暗号化、および関連する用語を初めて使用する場合は、このガイドに進む前に「データ暗号化について」を読むことをお勧めします。

AWS 暗号化基盤

暗号化は、転送中 AWS、保管中、またはメモリ内のデータの暗号化 AWS のサービス をサポートする のセキュリティに不可欠な部分です。 イノベーションへの AWS コミットメントと、主権と暗号化機能の追加コントロールへの投資の詳細については、AWS デジタル主権の約束を発表するブログ記事を参照してください。

AWS は、 責任共有モデルに従ってデータを保護します。 は、業界標準を満たし、相互運用性を促進する信頼できる暗号化アルゴリズム AWS のサービス を使用します。これらのアルゴリズムは、公的標準機関と学術研究によって審査されます。関連する標準は、政府、業界、学界によって広く受け入れられています。

AWS はデフォルトで高保証の暗号化実装であり、効率的なハードウェア最適化ソリューションが推奨されます。当社の暗号化コアライブラリである AWS-LC は、透明性と業界全体の再利用のためのオープンソースとして利用できます。 AWS LC 内の多くの暗号化アルゴリズム実装は、いくつかの異なるプラットフォームでの実装の正確性とセキュリティを保証するために正式に検証されています。ライブラリは NIST の FIPS-140 プログラムでも検証されます。

暗号アルゴリズム

次の 3 種類の暗号化アルゴリズムを定義します。

- 非対称暗号化では、暗号化 (または検証) 用のパブリックキーと復号 (または署名) 用のプライベートキーのペアを使用します。パブリックキーは復号化には使用されないため共有できますが、プライベートキーへのアクセスは厳しく制限する必要があります。 は、ML-KEM や ML-DSA などのポスト量子アルゴリズム AWS のサービス をサポートまたはサポートする計画です。 は、RSA や楕円曲線暗号 (ECC) などの従来の暗号化アルゴリズム AWS のサービス もサポートしています。
- 対称暗号化では、同じキーを使用して暗号化と復号化、またはデータの認証と検証を行います。AWS のサービス は一般的に、AES-256 のモードを使用する保管中のデータの暗号化のために AWS Key Management Service (AWS KMS) と統合されます。

- 他の暗号化関数は、非対称暗号化と対称暗号化と組み合わせて使用され、機密性、完全性、認証、否認防止アプリケーションのための安全で実用的なプロトコルを構築します。例としては、ハッシュ関数やキー取得関数などがあります。

での推奨暗号化アルゴリズム AWS

次の表は、 がデータを保護するためにサービス全体のデプロイに適している AWS と考える暗号化アルゴリズム、モード、およびキーサイズをまとめたものです。このガイダンスは、暗号化標準が進化するにつれて、時間の経過とともに進化します。

サービス内で利用できるアルゴリズムはさまざまであり、各サービスのドキュメントで説明されています。承認されたアルゴリズムにソフトウェアライブラリの実装が必要な場合は、最新バージョンの AWS-LC ライブラリに含まれているかどうかを確認してください。

アルゴリズムは、次の 2 つのカテゴリのいずれか AWS で での使用が承認されています。

- 推奨されるアルゴリズムは、 AWS セキュリティとパフォーマンスの基準を満たしています。
- 許容アルゴリズムは、一部のアプリケーションの互換性の目的で使用できますが、優先されません。

非対称暗号化

次の表に、暗号化、キーアグリーメント、デジタル署名 AWS のために での使用に適していると考えられる非対称アルゴリズムを示します。

タイプ	アルゴリズム	ステータス
暗号化	RSA-OAEP (≥2048 ビットモジュラス)	Acceptable
暗号化	HPKE (P-256 または P-384、HKDF、AES-GCM)	Acceptable
キーアグリーメント	ML-KEM-768 または ML-KEM-1024	優先 (量子耐性)
キーアグリーメント	P-256, P-384, P-521または X25519 を使用した ECDH(E)	Acceptable

キーアグリーメント	ECDH(E) と brainpool P256r1、brainpoolP384r1、または brainpoolP512r1	Acceptable
[署名]	ML-DSA-65 または ML-DSA-87	優先 (量子耐性)
[署名]	SLH-DSA	許容 (量子耐性)
[署名]	P-256, P-384, P-521または Ed25519 を使用した ECDSA	Acceptable
[署名]	RSA (≥2048 ビットモジュラス)	Acceptable

対称暗号化

次の表は、暗号化、認証された暗号化、およびキーラッピング AWS のために での使用に適していると考えられる対称アルゴリズムの一覧です。

タイプ	アルゴリズム	ステータス
認証された暗号化	AES-GCM-256	推奨値
認証された暗号化	AES-GCM-128	Acceptable
認証された暗号化	ChaCha20/Poly1305	Acceptable
暗号化モード	AES-XTS-256 (ブロックストレージ用)	推奨値
暗号化モード	AES-CBC/CTR (非認証モード)	Acceptable
キーラッピング	AES-GCM-256	推奨値
キーラッピング	256 ビットキーを含む AES-KW または AES-KWP	Acceptable

その他の暗号化関数

次の表は、ハッシュ、キー取得、およびメッセージ認証 AWS のために での使用に適していると考えられるアルゴリズムの一覧です。

タイプ	アルゴリズム	ステータス
ハッシュ	SHA-384	推奨値
ハッシュ	SHA-256	Acceptable
ハッシュ	SHA3	Acceptable
キー取得	SHA-256 を使用した HKDF_Expand または HKDF	推奨値
キー取得	HMAC-SHA-256 を使用したカウンターモード KDF	Acceptable
メッセージ認証コード	HMAC-SHA-384	推奨値
メッセージ認証コード	HMAC-SHA-256	Acceptable
メッセージ認証コード	KMAC	Acceptable
パスワードハッシュ	SHA384 による暗号化	推奨値
パスワードハッシュ	PBKDF2	Acceptable

で使用される暗号化 AWS のサービス

AWS のサービス は、検証済みのアルゴリズムの安全なオープンソース実装に依存してデータを保護します。アルゴリズムの具体的な選択と設定は、サービスによって異なります。一部の AWS ツールやサービスは、特定のアルゴリズムを使用します。それ以外の場合は、サポートされているアルゴリズムとキーの長さから選択することも、推奨されるデフォルトを使用することもできます。

AWS 暗号化サービスは、さまざまな暗号化セキュリティ標準に準拠しているため、政府または業界の規制に準拠できます。 AWS のサービス が準拠するデータセキュリティ標準の完全なリストについては、AWS 「 コンプライアンスプログラム」を参照してください。

暗号化のベストプラクティスの概略

このセクションでは、 でデータを暗号化するときに適用される推奨事項を示します AWS クラウド。これらの一般的な暗号化のベストプラクティスは、 に固有のものではありません AWS のサービス。このセクションでは、次のトピックについて説明します。

- データ分類
- 転送中のデータの暗号化
- 保管中のデータの暗号化

データ分類

データ分類とは、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、分類するプロセスのことです。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、 Well-Architected フレームワークのセキュリティの柱 AWS のコンポーネントです。カテゴリには、極秘データ、機密データ、非機密データ、公開データなどがありますが、分類階層とその名前は組織によって異なる場合があります。データ分類プロセス、考慮事項、モデルの詳細については、「データ分類 (ホワイトペーパー)AWS 」を参照してください。

データを分類したら、各カテゴリに必要な保護レベルに基づいて、組織の暗号化戦略を作成することができます。例えば、極秘データには非対称暗号化を使用し、公開データには暗号化は必要ないと組織で判断する場合があります。暗号化戦略の設計の詳細については、「Creating an enterprise encryption strategy for data at rest」を参照してください。このガイドに記載されている技術的な考慮事項と推奨事項は保管中のデータに限られていますが、段階的なアプローチを使用して転送中のデータの暗号化戦略を作成することもできます。

転送中のデータの暗号化

AWS グローバルネットワーク AWS リージョン 経由で 間で送信されるすべてのデータは、 AWS 保護された施設を離れる前に、物理レイヤー AWS で によって自動的に暗号化されます。 は、アベイラビリティーゾーン間のすべてのトラフィックを AWS 暗号化します。

ワークロードを通過するデータの場合、 で転送中のデータを暗号化する際の一般的なベストプラクティスは次のとおりです AWS クラウド。

- データ分類、組織の要件、該当する規制やコンプライアンス基準に基づいて、転送中のデータに関する組織の暗号化ポリシーを定義します。極秘データ、または機密データに分類される転送中のデータを暗号化することを強くお勧めします。ポリシーによっては、必要に応じて、非機密データや公開データなど、他のカテゴリの暗号化を指定する場合もあります。
- 転送中のデータを暗号化する場合は、暗号化ポリシーで定義されている承認済みの暗号化アルゴリズム、ブロック暗号モード、キーの長さを使用することをお勧めします。さらに、Application Load Balancer、Amazon API Gateway リソース、Amazon CloudFront リソース、Amazon Virtual Private Cloud (Amazon VPC) リソースに関連付けられた TLS ポリシーを定期的に確認し、それらが現在の暗号化ポリシーと一致していることを確認することをお勧めします。
- 次のいずれかを使用して、企業ネットワークおよび AWS クラウド インフラストラクチャ内の情報アセットとシステム間のトラフィックを暗号化します。
  - AWS Site-to-Site VPN 接続
  - IPsec で暗号化されたプライベートAWS Direct Connect接続を提供する AWS Site-to-Site VPN と 接続の組み合わせ
  - Direct Connect MAC セキュリティ (MACsec) をサポートして企業ネットワークから Direct Connect ロケーションにデータを暗号化する 接続
- 最小特権の原則に基づいて、マネージド証明書と TLS ポリシー設定のアクセスコントロールポリシーを特定します。最小特権とは、ユーザーに職務を遂行するために必要最小限のアクセス権を付与するという、セキュリティのベストプラクティスです。最小特権の適用について、詳しくは、「IAM でのセキュリティベストプラクティス」と「IAM ポリシーのベストプラクティス」を参照してください。

保管中のデータの暗号化

Amazon Simple Storage Service (Amazon S3) や Amazon Elastic File System (Amazon EFS) などのすべての AWS データストレージサービスには、保管中のデータを暗号化するオプションが用意されています。暗号化は、 () や などの AWS Key Management Service 256 ビット Advanced Encryption Standard (AES-256 AWS KMS) ブロック暗号および AWS 暗号化サービスを使用して実行されますAWS CloudHSM。

データ分類、エンドツーエンドの暗号化の必要性、エンドツーエンドの暗号化を使用できない技術的制限などの要因に基づき、クライアント側の暗号化またはサーバー側の暗号化を使用してデータを暗号化できます。

- クライアント側の暗号化とは、対象となるアプリケーションまたはサービスがデータを受信する前に、データをローカルで暗号化する行為のことです。 AWS のサービス は暗号化されたデータを

受け取るだけで、データの暗号化または復号化には関与しません。クライアント側の暗号化には、AWS KMS、AWS Encryption SDK、その他のサードパーティの暗号化ツールまたはサービスを使用する場合があります。

- サーバー側の暗号化とは、データの送信先でデータを暗号化することです。データを受信するアプリケーションまたはサービスが行います。サーバー側の暗号化では、ストレージブロック全体の暗号化 AWS KMS に を使用できます。また、Linux ファイルシステムをオペレーティングシステム (OS) レベルで暗号化する LUKS など、サードパーティ製の暗号化ツールやサービスを使用することもできます。

以下は、 AWS クラウドに保管中のデータを暗号化するときの一般的なベストプラクティスです。

- データ分類、組織の要件、および該当する規制やコンプライアンス基準に基づいて、保管中のデータに関する組織の暗号化ポリシーを定義します。詳細については、「Creating an enterprise encryption strategy for data at rest」を参照してください。極秘データ、または機密データに分類される保管中のデータは暗号化することを強くお勧めします。ポリシーによっては、必要に応じて、非機密データや公開データなど、他のカテゴリの暗号化を指定する場合もあります。
- 保管中のデータを暗号化する場合は、承認された暗号化アルゴリズム、ブロック暗号モード、キーの長さを使用することをお勧めします。
- 最小特権の原則に基づいて、暗号化キーのアクセス制御ポリシーを特定します。

の暗号化のベストプラクティス AWS のサービス

このセクションでは、以下の のベストプラクティスと推奨事項について説明します AWS のサービス。

- AWS CloudTrail
- Amazon DynamoDB
- Amazon Elastic Compute Cloud (Amazon EC2) および Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon Elastic File System (Amazon EFS)
- Amazon Elastic Kubernetes Service (Amazon EKS)
- AWS Encryption SDK
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- Amazon Relational Database Service (Amazon RDS)
- AWS Secrets Manager
- Amazon Simple Storage Service(Amazon S3)
- Amazon Virtual Private Cloud (Amazon VPC)

の暗号化のベストプラクティス AWS CloudTrail

AWS CloudTrail は、 AWS アカウントのガバナンス、コンプライアンス、および運用とリスクの監査を行えるように支援します。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- CloudTrail ログはカスタマーマネージドの AWS KMS keyを使用して暗号化する必要があります。ログファイルを受け取る S3 バケットと同じリージョンにある KMS キーを選択します。詳細については、「証跡を更新して KMS キーを使用する」を参照してください。
- 追加のセキュリティレイヤーとして、証跡のログファイル検証を有効にします。ログファイル検証は、CloudTrail がログファイルを配信した後に変更されたか、削除されたか、変更されていないかを判断するのに役立ちます。説明については、「CloudTrail のログファイルの整合性検証を有効にする」を参照してください。

- インターフェイス VPC エンドポイントを使用して、CloudTrail がパブリックインターネットを経由せずに他の VPC のリソースと通信できるようにします。詳細については、「VPC エンドポイントでの AWS CloudTrail の使用」を参照してください。
- `aws:SourceArn` 条件キーを KMS キーポリシーに追加して、CloudTrail が特定の 1 つまたは複数の証跡に対してのみ KMS キーを使用できるようにします。詳細については、CloudTrail の AWS KMS key ポリシーを設定する」を参照してください。
- で AWS Config、cloud-trail-encryption-enabled AWS マネージドルールを実装して、ログファイルの暗号化を検証して適用します。
- CloudTrail が Amazon Simple Notification Service (Amazon SNS) トピックで通知を送信するように設定されている場合は、`aws:SourceArn` (またはオプションの `aws:SourceAccount`) 条件キーを CloudTrail ポリシーステートメントに追加して、SNS トピックへの不正なアカウントアクセスを防止します。詳細については、「CloudTrail の Amazon SNS トピックポリシー」を参照してください。
- を使用している場合は AWS Organizations、その組織の のすべてのイベントをログ AWS アカウント に記録する組織の証跡を作成します。これには、組織内の管理アカウントおよびすべてのメンバーアカウントが含まれます。詳細については、「組織の証跡の作成」を参照してください。
- 企業データを保存するすべての に適用される AWS リージョン証跡を作成し、それらのリージョンの AWS アカウント アクティビティを記録します。が新しいリージョン AWS を起動すると、CloudTrail は新しいリージョンを自動的に含め、そのリージョンのイベントをログに記録します。

Amazon DynamoDB の暗号化のベストプラクティス

Amazon DynamoDB は、フルマネージド NoSQL データベースサービスです。高速かつ予測可能でスケーラブルなパフォーマンスを提供します。DynamoDB の保管時の暗号化では、データを堅牢なメディアに保存する際に、プライマリキー、ローカルおよびグローバルのセカンダリインデックス、ストリーム、グローバルテーブル、バックアップ、DynamoDB Accelerator (DAX) クラスターなどを暗号化テーブルで保護します。

データ分類の要件に従い、サーバー側またはクライアント側の暗号化を実装することで、データの機密性と整合性を維持できます。

サーバー側の暗号化では、新しいテーブルの作成時に AWS KMS keys を使用してテーブルを暗号化できます。 AWS 所有キー、 AWS マネージドキー、またはカスタマーマネージドキーを使用できます。キーにはカスタマーマネージドキーを使用することをお勧めします。これは、組織でキーを完全に制御できるためです。また、このキータイプを使用すると、テーブルレベルの暗号化

キー、DynamoDB テーブル、ローカルおよびグローバルのセカンダリインデックス、ストリームがすべて同じキーで暗号化されます。これらのキータイプの詳細については、「カスタマーキーと AWS キー」を参照してください。

> **Note**
>
> AWS 所有キー、 AWS マネージドキー、カスタマーマネージドキーはいつでも切り替えることができます。

データのクライアント側の暗号化とエンドツーエンドの保護には、保存中と転送中の両方で Amazon DynamoDB Encryption Client を使用できます。DynamoDB Encryption Client は、項目の属性値の機密性を保護する暗号化に加えて、項目に署名します。こうすることで、属性の追加や削除、暗号化された値の別の値への置換など、項目全体への不正な変更を検出し、整合性の保護を提供します。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- キーの無効化や削除のスケジュール設定の権限を、これらのタスクを実行する必要のあるユーザーのみに制限してください。キーの状態を無効に設定するか、削除のスケジュールを設定すると、すべてのユーザーと DynamoDB サービスは、データの暗号化と復号化、およびテーブルに対する読み取り/書き込み操作を実行できなくなります。
- DynamoDB はデフォルトで HTTPS を使用して転送中のデータを暗号化しますが、追加のセキュリティ制御が推奨されます。以下のいずれかのオプションを使用できます。
  - AWS Site-to-Site VPN 暗号化に IPsec を使用する 接続。
  - AWS Direct Connect プライベート接続を確立するための 接続。
  - AWS Direct Connect IPsec で暗号化されたプライベート AWS Site-to-Site VPN 接続の接続との接続。
  - 仮想プライベートクラウド (VPC) 内からのみ DynamoDB にアクセスする必要がある場合は、VPC ゲートウェイエンドポイントを使用して、アクセスを VPC 内リソースのみに許可することができます。これにより、トラフィックがパブリックインターネットを経由することを防ぎます。
- VPC エンドポイントを使用している場合は、エンドポイントに関連付けられているエンドポイントポリシーと IAM ポリシーを、承認されたユーザー、リソース、サービスのみに限定してください。詳細については、「IAM ポリシーを使用して DynamoDB エンドポイントへのアクセスを制御する」と「エンドポイントポリシーを使用してサービスへのアクセスを制御する」を参照してください。

- 暗号化ポリシーに従って、暗号化が必要なデータに対し、列レベルのデータ暗号化をアプリケーションレベルで実装できます。
- クラスターの設定時に、キャッシュ内のデータ、構成データ、ログファイルなどの保管中のデータを暗号化するように DAX クラスターを構成します。既存のクラスターでは保存時の暗号化を有効にすることはできません。このサーバー側の暗号化は、基盤となるストレージを経由する不正アクセスからデータを保護するのに役立ちます。保管時の DAX 暗号化は AWS KMS と自動的に統合され、クラスターの暗号化に使用される単一サービスのデフォルトキーを管理します。暗号化された DAX クラスターの作成時にサービスのデフォルトキーが存在しない場合、 AWS KMS は自動的に新しい AWS マネージドキーを作成します。詳細については、「保管時の DAX 暗号化」を参照してください。

  > **Note**
  >
  > カスタマーマネージドキーは DAX クラスターでは使用できません。

- クラスターのセットアップ時に転送中のデータを暗号化するように DAX クラスターを設定します。既存のクラスターでは転送中の暗号化を有効にすることはできません。DAX は TLS を使用してアプリケーションとクラスター間のリクエストおよびレスポンスを暗号化し、クラスターの x509 証明書を使用してクラスターの ID を認証します。詳細については、「転送中の DAX 暗号化」を参照してください。
- で AWS Config、dax-encryption-enabled AWS マネージドルールを実装して、DAX クラスターの暗号化を検証して維持します。

Amazon EC2 と Amazon EBS の暗号化のベストプラクティス

Amazon Elastic Compute Cloud (Amazon EC2) は、 AWS クラウドでスケーラブルなコンピューティング容量を提供します。仮想サーバーを必要な数だけ起動して、迅速にスケールアップまたはスケールダウンができます。Amazon Elastic Block Store (Amazon EBS) は、EC2 インスタンスで使用するためのブロックレベルのストレージボリュームを提供します。

これらのサービスでは、以下の暗号化のベストプラクティスを検討してください。

- すべての EBS ボリュームに適切なデータ分類キーと値をタグ付けします。これにより、ポリシーに従って、適切なセキュリティと暗号化の要件を決定して実装できます。
- 暗号化ポリシーと技術的実現可能性に応じて、EC2 インスタンス間、または EC2 インスタンスとオンプレミスネットワーク間で転送中のデータの暗号化を設定します。

- EC2 インスタンスのブートボリュームとデータ EBS ボリュームの両方を暗号化します。暗号化された EBS ボリュームは次のデータを保護します。
  - ボリューム内で保管中のデータ
  - ボリュームとインスタンスの間で移動されるすべてのデータ
  - ボリュームから作成されたすべてのスナップショット
  - それらのスナップショットから作成されたすべてのボリューム

  詳細については、「EBS 暗号化のしくみ」を参照してください。
- 現在の のアカウントの EBS ボリュームに対して、デフォルトで暗号化を有効にします AWS リージョン。こうすることで、新しい EBS ボリュームとスナップショットコピーはすべて強制的に暗号化されます。これは既存の EBS ボリュームまたはスナップショットには影響しません。詳細については、「デフォルトで暗号化を有効にする」を参照してください。
- Amazon EC2 インスタンスのインスタンスストアルートボリュームを暗号化します。こうすることで、オペレーティングシステムで保存されている設定ファイルやデータの保護に役立ちます。詳細については、Amazon EC2 インスタンスストア暗号化を使用して保管中のデータを保護する方法」(AWS ブログ記事) を参照してください。
- で AWS Config、暗号化ボリュームルールを実装して、適切な暗号化設定を検証して適用する自動チェックを実行します。

Amazon ECR の暗号化のベストプラクティス

Amazon Elastic Container Registry (Amazon ECR) は、セキュリティ、スケーラビリティ、信頼性を備えたマネージドコンテナイメージレジストリサービスです。

Amazon ECR は、Amazon ECR が管理する Amazon S3 バケットにイメージを保存します。各 Amazon ECR リポジトリには、リポジトリの作成時に設定される暗号化設定があります。デフォルトでは、Amazon ECR は Amazon S3 が管理する (SSE-S3) 暗号化キーによるサーバー側の暗号化を使用します。詳細については、「保管時の暗号化」(Amazon ECR ドキュメント) を参照してください。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- Amazon S3 が管理する (SSE-S3) 暗号化キーによるサーバー側暗号化 (デフォルト) を使用する代わりに、 AWS KMSに保存されているカスタマーマネージド KMS キーを使用します。このキータイプは最もきめ細かい管理オプションを提供します。

> **Note**
>
> KMS キーは、リポジトリ AWS リージョン と同じ に存在する必要があります。

- リポジトリのプロビジョニング時に Amazon ECR がデフォルトで作成する権限を取り消さないでください。取り消した場合、データへのアクセス、リポジトリにプッシュされた新しいイメージの暗号化、イメージがプルされた時の復号化などの機能に影響する可能性があります。
- を使用して AWS CloudTrail 、Amazon ECR が送信するリクエストを記録します AWS KMS。ログエントリには、より簡単に識別できるように暗号化コンテキストキーが含まれています。
- 特定の Amazon VPC エンドポイントまたは特定の VPC からのアクセスを制御するように Amazon ECR ポリシーを設定します。これにより、実質的に特定の Amazon ECR リソースへのネットワークアクセスが分離され、特定の VPC からのアクセスのみが許可されます。Amazon VPC エンドポイントとの仮想プライベートネットワーク (VPN) 接続を確立すると、転送中のデータを暗号化できます。
- Amazon ECR はリソースベースのポリシーをサポートしています。これらのポリシーを使用して、送信元 IP アドレスまたは特定の IP アドレスに基づいてアクセスを制限できます AWS のサービス。

Amazon ECS の暗号化のベストプラクティス

Amazon Elastic Container Service (Amazon ECS) は、クラスターでコンテナの実行、停止、管理を支援する、高速でスケーラブルなコンテナ管理サービスです。

Amazon ECS では、以下のいずれかの方法で転送中のデータを暗号化できます。

- サービスメッシュの作成 を使用して AWS App Mesh、デプロイされた Envoy プロキシと、仮想ノードや仮想ゲートウェイなどのメッシュエンドポイント間の TLS 接続を設定します。 AWS Private Certificate Authority またはお客様が用意した証明書から TLS 証明書を使用できます。詳細とチュートリアルについては、「(ACM) またはお客様が用意した証明書 AWS App Mesh を使用して AWS Certificate Manager のサービス間でトラフィック暗号化を有効にする」(AWS ブログ記事) を参照してください。
- サポートされている場合は、AWS Nitro Enclaves を使用します。 AWS Nitro Enclaves は、Amazon EC2 インスタンスから enclaves と呼ばれる分離された実行環境を作成できる Amazon EC2 機能です。これは、機密性の非常に高いデータの保護に役立つように設計されています。また、Nitro Enclaves 向けの ACM により、パブリックおよびプライベートの SSL/TLS 証明書を、ウェブアプリケーションおよびウェブサーバー (AWS Nitro Enclaves のある Amazon

EC2 インスタンスで稼働しているサーバー) で使用できます。詳細については、AWS 「Nitro Enclaves – Isolated EC2 Environments to Process Confidential Data」(AWS ブログ記事) を参照してください。

- Application Load Balancer で Server Name Indication (SNI) プロトコルを使用します。Application Load Balancer の単一の HTTPS リスナーの背後に複数のアプリケーションをデプロイできます。各リスナーには独自の TLS 証明書があります。ACM が提供する証明書か、自己署名証明書を使用できます。Application Load Balancer と Network Load Balancer は、いずれも SNI をサポートします。詳細については、「Application Load Balancer が SNI を使用したスマート選択で複数の TLS 証明書をサポートするようになりました (ブログ記事)」を参照してください。AWS
- セキュリティと柔軟性を向上させるには、 AWS Private Certificate Authority を使用して Amazon ECS タスクで TLS 証明書をデプロイします。詳細については、「Retaining TLS all to your container part 2: Using AWS Private CA」(AWS ブログ記事) を参照してください。
- Secret discovery service (Envoy) または ACM にホストされた証明書 (GitHub) を使用して、App Mesh に 相互 TLS (mTLS) を実装します。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- 技術的に可能であれば、セキュリティ強化のため、 AWS PrivateLinkに Amazon ECS インターフェイス VPC エンドポイントを設定します。VPN 接続を介してこれらのエンドポイントにアクセスすると、転送中のデータが暗号化されます。
- API キーやデータベース認証情報などの機密情報を安全に保管します。これらを暗号化したパラメータとしてパラメータストアに保存できます。これは AWS Systems Managerの機能です。ただし、 AWS Secrets Manager このサービスではシークレットを自動的にローテーションし、ランダムなシークレットを生成して、シークレットを共有できるため、 を使用することをお勧めします AWS アカウント。
- データセンター内のユーザーまたはアプリケーション、またはウェブ上の外部のサードパーティーが直接 HTTPS API リクエストを行っている場合は AWS のサービス、 AWS Security Token Service () から取得した一時的なセキュリティ認証情報を使用してそれらのリクエストに署名しますAWS STS。

Amazon EFS の暗号化のベストプラクティス

Amazon Elastic File System (Amazon EFS) は、 AWS クラウドでの共有ファイルシステムの作成と設定に役立ちます。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- で AWS Config、efs-encrypted-check AWS マネージドルールを実装します。このルールは、Amazon EFS が を使用してファイルデータを暗号化するように設定されているかどうかを確認します AWS KMS。
- Amazon CloudWatch アラームを作成して Amazon EFS ファイルシステムの暗号化を強制します。ここでは CloudTrail ログで `CreateFileSystem` イベントを監視し、暗号化されていないファイルシステムが作成されるとアラームをトリガーします。詳細については、「チュートリアル: 保管時に Amazon EFS ファイルシステムの暗号化を強制する」を参照してください。。
- EFS マウントヘルパーを使用してファイルシステムをマウントする こうすることで、クライアントと Amazon EFS サービス間の TLS 1.2 トンネルが設定および維持され、すべてのネットワークファイルシステム (NFS) トラフィックがこの暗号化されたトンネルを介してルーティングされます。次のコマンドは、転送中の暗号化に TLS を使用する機能を実装します。

  ```
  sudo mount -t efs  -o tls file-system-id:/ /mnt/efs
  ```

  詳細については、「EFS マウントヘルパーを使用して EFS ファイルシステムをマウントする」を参照してください。
- を使用して AWS PrivateLink、インターフェイス VPC エンドポイントを実装し、VPCs と Amazon EFS API 間のプライベート接続を確立します。VPN 接続を介してエンドポイントへ、またはエンドポイントから転送されるデータが暗号化されます。詳細については、「インターフェイス VPC エンドポイントを使用して AWS のサービス にアクセスする」を参照してください。
- IAM ID ベースのポリシーの `elasticfilesystem:Encrypted` 条件キーを使用して、暗号化されていない EFS ファイルシステムをユーザーが作成できないようにします。詳細については、「IAM を使用して暗号化されたファイルシステムの作成を強制する」を参照してください。
- EFS 暗号化に使用する KMS キーは、リソースベースのキーポリシーを使用して最小特権アクセスに設定する必要があります。
- EFS ファイルシステムポリシーの `aws:SecureTransport` 条件キーを使用して、EFS ファイルシステムへの接続時に、NFS クライアントに TLS を強制的に使用します。詳細については、「Amazon Elastic File System によるファイルデータの暗号化https://docs.aws.amazon.com/whitepapers/latest/efs-encrypted-file-systems/encryption-of-data-in-transit.html」(AWS ホワイトペーパー) を参照してください。 Amazon Elastic File System

Amazon EKS の暗号化のベストプラクティス

Amazon Elastic Kubernetes Service (Amazon EKS) を使用すると、独自の Kubernetes コントロールプレーンやノードをインストールまたは維持 AWS することなく、 で Kubernetes を実行でき

ます。Kubernetes では、ユーザー証明書、パスワード、API キーなどの機密情報の管理にシークレットが役立ちます。デフォルトでは、これらのシークレットは API サーバーの基盤となるデータストアに暗号化されずに保存されます。このデータストアは etcd と呼ばれます。Amazon EKS では、etcdノードの Amazon Elastic Block Store (Amazon EBS) ボリュームは Amazon EBS 暗号化で暗号化されます。API アクセスまたは etcd のアクセス権を持つすべてのユーザーは、シークレットを取得または変更できます。さらに、名前空間にポッドを作成する権限を持つユーザーは誰でも、そのアクセス権を使ってその名前空間のシークレットを読み取ることができます。マネージドキーまたはカスタマー AWS マネージドキーを使用して AWS KMS keys、Amazon EKS で保管中のこれらのシークレットを暗号化できます。etcd を使用する代替の方法として、AWS Secrets and Config Provider (ASCP) (GitHub リポジトリ) を使用することもできます。ASCP は IAM およびリソースベースのポリシーと統合して、アクセス先をクラスター内の特定の Kubernetes ポッド内のシークレットのみに制限および限定します。

Kubernetes では、次の AWS ストレージサービスを使用できます。

- Amazon EBS では、ツリー内ストレージドライバーまたは Amazon EBS CSI ドライバーを使用できます。どちらにも、ボリュームの暗号化やカスタマーマネージドキーの提供のためのパラメータが含まれています。
- Amazon Elastic File System (Amazon EFS) には、Amazon EFS CSI ドライバーを使用できます。これは動的プロビジョニングと静的プロビジョニングの両方をサポートします。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- etcd を使用している場合、デフォルトでシークレットオブジェクトは暗号化されずに保存されますが、シークレットを保護するために以下を実行してください。
  - 「保管中のシークレットデータを暗号化する」(Kubernetes ドキュメント)。
  - Kubernetes シークレットのエンベロープ暗号化 AWS KMS に使用します。これにより、シークレットを一意のデータキーで暗号化できます。キー暗号化キーを使用して AWS KMS 、データキーを暗号化できます。キー暗号化キーは、定期的なスケジュールで自動的にローテーションできます。Kubernetes 用 AWS KMS プラグインを使用すると、すべての Kubernetes シークレットが暗号文etcdで に保存されます。これらは Kubernetes API サーバーによってのみ復号できます。詳細については、「Amazon EKS 暗号化プロバイダーによる詳細な防御のサポートの使用」および「既存のクラスター AWS KMS で で Kubernetes シークレットを暗号化する」を参照してください。
  - シークレットの読み取りおよび書き込みを制限するロールベースアクセスコントロール (RBAC) ルールで認可を有効化または設定します。新しいシークレットの作成や、既存のシークレットの

置換を行う権限を制限します。詳細については、「認可の概要」(Kubernetes ドキュメント) を参照してください。

- ポッドに複数のコンテナを定義してあり、そのうちの 1 つのコンテナのみがシークレットへのアクセスを必要とする場合は、他のコンテナがそのシークレットにアクセスできないようにボリュームマウントを定義します。`tmpfs` ボリュームとしてマウントされたシークレットはインスタンス化され、ポッドが削除されるとノードから自動的に削除されます。環境変数を使用することもできますが、環境変数の値がログに表示される可能性があるため、この方法はお勧めしません。詳細については、「シークレット」(Kubernetes ドキュメント) を参照してください。
- `watch` へのアクセスと、名前空間内のシークレットに対する `list` リクエストの許可はできるだけ避けてください。Kubernetes API では、クライアントがその名前空間のすべてのシークレットの値を調べることができるため、このようなリクエストはかなりの力を持ちます。
- 読み取り専用アクセスを含めて、クラスター管理者のみが `etcd` にアクセスできるようにしてください。
- 複数の `etcd` インスタンスがある場合、`etcd` が `etcd` ピア間の通信に TLS を使用していることを確認してください。

- ASCP を使用している場合は、シークレットを保護するために次のことを行ってください。
  - サービスアカウントの IAM ロールを使用して、シークレットアクセスを許可されたポッドのみに制限します。
  - AWS 暗号化プロバイダー (GitHub リポジトリ) を使用して Kubernetes シークレットの暗号化を有効にし、カスタマーマネージド KMS キーでエンベロープ暗号化を実装します。
- 環境変数によるデータ漏えいのリスクを低減するために、AWS Secrets Manager と Secret Store CSI Driver用設定プロバイダー (GitHub) を使用することをお勧めします。このドライバーを使用すると、Secrets Manager に保存されているシークレットと、パラメータストアに保存されているパラメータを、Kubernetes ポッドにマウントされたファイルとして表示できます。

> **Note**
>
> AWS Fargate はサポートされていません。

- Amazon CloudWatch メトリクスフィルタとアラームを作成して、シークレットの削除や削除待ち期間中のシークレットバージョンの使用など、管理者が指定する操作に関するアラートを送信します。詳細については、「異常検出に基づいてアラームを作成する」を参照してください。

の暗号化のベストプラクティス AWS Encryption SDK

AWS Encryption SDK は、オープンソースのクライアント側暗号化ライブラリです。業界標準とベストプラクティスを使用して、複数のプログラミング言語での実装と相互運用性をサポートします。は、安全で認証された対称キーアルゴリズムを使用してデータを AWS Encryption SDK 暗号化し、暗号化のベストプラクティスに準拠したデフォルトの実装を提供します。詳細については、「AWS Encryption SDKでサポートされているアルゴリズムスイート」を参照してください。

の主な機能の 1 つは、使用中のデータの暗号化のサポート AWS Encryption SDK です。encrypt-then-use アプローチを採用することで、アプリケーションロジックで処理される前に機密データを暗号化できます。これにより、アプリケーション自体がセキュリティイベントの影響を受けている場合でも、潜在的な露出や改ざんからデータを保護することができます。

このサービスでは、以下のベストプラクティスを検討してください。

- 「AWS Encryption SDKのベストプラクティス」に記載されているすべての推奨事項を順守してください。
- データキーの保護に役立つラップキーを 1 つ以上選択します。詳細については、「ラップキーの選択」を参照してください。
- `KeyId` パラメータを ReEncrypt オペレーションに渡し、信頼できない KMS キーの使用を防止します。詳細については、「クライアント側の暗号化の改善: 明示的な KeyIds とキーコミットメント (AWS ブログ記事) 」を参照してください。
- AWS Encryption SDK で を使用する場合は AWS KMS、ローカル`KeyId`フィルタリングを使用します。詳細については、「クライアント側の暗号化の改善: 明示的な KeyIds とキーコミットメント (AWS ブログ記事) 」を参照してください。
- 大量のトラフィックで暗号化または復号が必要なアプリケーション、またはアカウントが AWS KMS リクエストクォータを超えている場合は、 のデータキーキャッシュ機能を使用できます AWS Encryption SDK。データキーキャッシュに関しては、以下のベストプラクティスに注意してください。
  - キャッシュセキュリティのしきい値を設定し、各キャッシュデータキーの使用期間および各データキーで保護されるデータ量を制限します。これらのしきい値を設定する際の推奨事項については、「キャッシュセキュリティのしきい値の設定」を参照してください。
  - ローカルキャッシュは、特定のアプリケーションユースケースのパフォーマンスを向上させるため、データキーの数を必要最小限に設定してください。ローカルキャッシュの制限を設定する手順と例については、「データキーキャッシュの使用: ステップバイステップ」を参照してください。

詳細については、AWS Encryption SDK「: データキーキャッシュがアプリケーションに適しているかどうかを判断する方法」(AWS ブログ記事) を参照してください。

の暗号化のベストプラクティス AWS Key Management Service

AWS Key Management Service (AWS KMS) は、データの保護に役立つ暗号化キーの作成と制御に役立ちます。 は、データを暗号化 AWS のサービス できる他のほとんどの と AWS KMS 統合します。完全なリストについては、「 AWS のサービス と統合されている AWS KMS」を参照してください。 AWS KMS また、 とも AWS CloudTrail 統合され、監査、規制、コンプライアンスのニーズに対応するための KMS キーの使用をログに記録します。

KMS キーは のプライマリリソースであり AWS KMS、暗号化キーの論理表現です。KMS キーには主に 3 つのタイプがあります。

- カスタマーマネージドキーは、お客様が作成する KMS キーです。
- AWS マネージドキーは、ユーザーに代わって がアカウントに AWS のサービス 作成する KMS キーです。
- AWS 所有キーは、 AWS のサービス が所有および管理し、複数の で使用する KMS キーです AWS アカウント。

キーの種類の詳細については、「カスタマーキーと AWS キー」を参照してください。

では AWS クラウド、 ポリシーを使用して、リソースとサービスにアクセスできるユーザーを制御します。例えば、 AWS Identity and Access Management (IAM) では、アイデンティティベースのポリシーはユーザー、ユーザーグループ、またはロールのアクセス許可を定義し、リソースベースのポリシーは S3 バケットなどのリソースにアタッチし、アクセスを許可するプリンシパル、サポートされているアクション、および満たす必要があるその他の条件を定義します。IAM ポリシーと同様に、 はキーポリシー AWS KMS を使用して KMS キーへのアクセスを制御します。各 KMS キーにはキーポリシーが必要です。また、各キーには 1 つのキーポリシーしか指定できません。KMS キーへのアクセスを許可または拒否するポリシーを定義する場合、次の点に注意してください。

- カスタマーマネージドキーのキーポリシーは制御できますが、 AWS マネージドキーまたは AWS 所有キーのキーポリシーを直接制御することはできません。
- キーポリシーを使用すると、 内の AWS KMS API コールへのきめ細かなアクセスを許可できます AWS アカウント。キーポリシーで明示的に許可されていない限り、IAM ポリシーを使用して KMS キーへのアクセスを許可することはできません。キーポリシーからの許可がない場合、許可

を許可する IAM ポリシーは効力を持ちません。詳細については、「IAM ポリシーに KMS キーへのアクセスを許可する」を参照してください。

- IAM ポリシーを使用して、キーポリシー対応する権限がないカスタマーマネージドキーへのアクセスを拒否できます。
- マルチリージョンキーのキーポリシーと IAM ポリシーを設計する際は、次の内容を考慮します。
  - キーポリシーはマルチリージョンキーの共有プロパティではありません。また、関連するマルチリージョンキー間のキーポリシーをコピーまたは同期しません。
  - `CreateKey` と `ReplicateKey` のアクションを使用してマルチリージョンキーを作成した場合、リクエストでキーポリシーが指定されていない限り、デフォルトキーポリシーが適用されます。
  - aws:RequestedRegion などの条件キーを実装して、特定の AWS リージョンへのアクセス許可を制限できます。
  - 権限を使用して、マルチリージョンのプライマリキーまたはレプリカキーへのアクセス許可を付与できます。ただし、マルチリージョンキーが関連付けられている場合でも、単一の権限を使用して複数の KMS キーにアクセス許可を付与することはできません。

AWS KMS を使用してキーポリシーを作成するときは、次の暗号化のベストプラクティスとその他のセキュリティのベストプラクティスを考慮してください。

- AWS KMS ベストプラクティスについては、以下のリソースの推奨事項に従ってください。
  - AWS KMS 許可のベストプラクティス (AWS KMS ドキュメント)
  - IAM ポリシーのベストプラクティス (AWS KMS ドキュメント)
- 職務分掌のベストプラクティスに従い、キーを管理する人物と使用する人物の ID は個別に管理してください。
  - キーの作成および削除を行う管理者ロールは、そのキーを使用できないようにする必要があります。
  - 一部のサービスでは、データの暗号化のみを必要とするため、キーを使用して復号する権限を付与するべきではない場合があります。
- キーポリシーは、常に最小特権モデルに従う必要があります。`kms:*` は、IAM またはキーポリシーのアクションに使用しないでください。これはプリンシパルにキーの管理と使用の権限が両方付与されてしまうためです。
- キーポリシー内の kms:ViaService 条件キー AWS のサービス を使用して、カスタマーマネージドキーの使用を特定の に制限します。

- キータイプの中から選択できる場合は、カスタマーマネージドキーをお勧めします。これは、次のようなきめ細かな制御オプションが提供されるためです。
  - 認証とアクセスコントロールの管理
  - キーの有効化と無効化
  - AWS KMS keysのローテーション
  - キーのタグ付け
  - エイリアスの作成
  - AWS KMS keysの削除
- AWS KMS 管理および変更のアクセス許可は、未承認のプリンシパルに対して明示的に拒否する必要があり、 AWS KMS 変更のアクセス許可は、未承認のプリンシパルの許可ステートメントに存在してはいけません。詳細については、AWS Key Management Serviceのアクション、リソース、および条件キーを参照してください。
- KMS キーの不正使用を検出するには、 で AWS Configiam-customer-policy-blocked-kms-actions および iam-inline-policy-blocked-kms-actions ルールを実装します。これにより、プリンシパルがすべてのリソースで復 AWS KMS 号アクションを使用できなくなります。
- のサービスコントロールポリシー (SCPs に実装 AWS Organizations して、権限のないユーザーまたはロールが コマンドとして直接、またはコンソールを介して KMS キーを削除しないようにします。詳細については、「予防的コントロールとしての SCPs」(AWS ブログ記事) を参照してください。
- CloudTrail ログに AWS KMS API コールを記録します。こうすることで、実行されたリクエストの内容、リクエストの送信元 IP アドレス、リクエストを実行したユーザーなど、関連するイベント属性が記録されます。詳細については、「 を使用した API コールのログ記録 AWS KMSAWS CloudTrail」を参照してください。
- 暗号化コンテキストを使用する場合、機密情報を含めるべきではありません。CloudTrail は暗号化コンテキストをプレーンテキストの JSON ファイルに保存します。このファイルは、情報を含む S3 バケットにアクセスできるユーザーなら誰でも閲覧できます。
- カスタマーマネージドキーの使用状況をモニタリングする場合、キーの作成、カスタマーマネージドキーポリシーの更新、キーマテリアルのインポートなど、特定のアクションが検出された際に通知するようイベントを設定します。また、キーを無効化する AWS Lambda 関数や組織のポリシーで指定されているインシデント対応アクションを実行する関数などの自動応答を実装することもお勧めします。
- マルチリージョンキーは、コンプライアンス準拠、ディザスタリカバリ、バックアップなど、特定のシナリオにお勧めします。マルチリージョンキーのセキュリティプロパティは、単一リージョン

キーとは大きく異なります。マルチリージョンキーの作成、管理、使用を許可する際には、以下の推奨事項が適用されます。

- プリンシパルが、必要とする AWS リージョン のみにマルチリージョンキーをコピーできるようにします。
- マルチリージョンキーのアクセス許可を、それらを必要とするプリンシパルおよびタスクに対してのみ付与します。

の暗号化のベストプラクティス AWS Lambda

AWS Lambda は、サーバーのプロビジョニングや管理を行うことなくコードを実行できるコンピューティングサービスです。環境変数の保護する場合、サーバー側の暗号化を使用して保管中のデータを保護し、クライアント側の暗号化を使用して転送中のデータを保護することができます。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- Lambda は、 AWS KMS keyで常にサーバー側の暗号化を提供します。デフォルトでは、Lambda は AWS マネージドキーを使用します。管理、ローテーション、監査などの面でキーを完全に制御できるため、カスタマーマネージドキーを使用することをお勧めします。
- 暗号化が必要な転送中のデータについては、ヘルパーを有効にして、転送中の保護のために環境変数をクライアント側で、任意の KMS キーを使用して暗号化できます。詳細については、「環境変数の保護」の「転送中のセキュリティ」を参照してください。
- 機密データや重要なデータを保持する Lambda 関数の環境変数は、転送中に暗号化する必要があります。これにより、関数に動的に渡されるデータ (通常はアクセス情報) を不正アクセスから保護できます。
- ユーザーが環境変数を表示できないようにするには、デフォルトキー、カスタマーマネージドキー、またはすべてのキーへのアクセスを拒否するステートメントを IAM ポリシーのユーザーのアクセス権限かキーポリシーに追加します。詳細については、AWS Lambda 環境変数の使用を参照してください。

Amazon RDS の暗号化のベストプラクティス

Amazon Relational Database Service (Amazon RDS) を使用して、 AWS クラウドでリレーショナルデータベース (DB) をセットアップ、運用、スケーリングできます。保管中に暗号化されるデータには、DB インスタンス、自動バックアップ、リードレプリカ、スナップショットの基本的なストレージが含まれます。

RDS DB インスタンスに保管中のデータを暗号化する方法は次のとおりです。

- Amazon RDS DB インスタンスは AWS KMS keys AWS 、 マネージドキーまたはカスタマーマネージドキーを使用して暗号化できます。詳細については、このガイドの「AWS Key Management Service」を参照してください。
- Amazon RDS for Oracle と Amazon RDS for SQL Server は、Transparent Data Encryption (TDE) による DB インスタンスの暗号化をサポートします。詳細については、「Oracle の Transparent Data Encryption」または「SQL Server の Transparent Data Encryption」のサポートを参照してください。

  TDE キーと KMS キーの両方を使用して DB インスタンスを暗号化できます。ただし、これはデータベースのパフォーマンスに若干影響する可能性があるため、これらのキーは個別に管理する必要があります。

RDS DB インスタンスに、または RDS DB インスタンスから転送中のデータを暗号化する方法は次のとおりです。

- MariaDB、Microsoft SQL Server、MySQL、Oracle、PostgreSQL を実行している Amazon RDS DB インスタンスの場合は、SSL で接続を暗号化できます。詳細については、「SSL/TLS を使用して DB インスタンスへの接続を暗号化する」を参照してください。
- また、Amazon RDS for Oracle は、Oracle ネイティブネットワーク暗号化 (NNE) をサポートしています。これを使用すると、DB インスタンスとの間でデータの移動を暗号化できます。NNE 暗号化と SSL 暗号化は同時に使用できません。詳細については、「Oracle native network encryption」を参照してください。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- 暗号化が必要なデータを処理、保存、または送信するために Amazon RDS for SQL Server または Amazon RDS for PostgreSQL DB インスタンスに接続する場合、RDS トランスポート暗号化機能を使用して接続を暗号化します。これを実装するには、パラメータグループの `rds.force_ssl` パラメータを `1` に設定します。詳細については、「パラメータグループの操作」を参照してください。Amazon RDS for Oracle は Oracle データベースのネイティブネットワーク暗号化を使用しています。
- RDS DB インスタンス暗号化用のカスタマーマネージドキーは、その目的にのみ使用し、他の AWS のサービスでは使用しないでください。

- RDS DB インスタンスを暗号化する前に、KMS キー要件を設定します。インスタンスが使用するキーは後で変更できません。たとえば、暗号化ポリシーで、ビジネス要件に基づいて、 AWS マネージドキーまたはカスタマーマネージドキーの使用および管理基準を定義します。
- カスタマーマネージド KMS キーへのアクセスを許可する場合は、IAM ポリシーで条件キーを使用して最小特権の原則に従います。例えば、Amazon RDS から送信されるリクエストにのみカスタマーマネージドキーを使用できるようにするには、 `rds.<region>.amazonaws.com`値で kms:ViaService 条件キーを使用します。さらに、Amazon RDS 暗号化コンテキストのキーまたは値を、カスタマーマネージドキーを使用する条件として使用できます。
- 暗号化された RDS DB インスタンスのバックアップを有効化することを強くお勧めします。Amazon RDS は、KMS キーが有効になっていない場合や、KMS キーへの RDS アクセスが取り消された場合などに、DB インスタンスの KMS キーにアクセスできなくなる可能性があります。この場合、暗号化された DB インスタンスは 7 日間回復可能な状態になります。DB インスタンスが 7 日経ってもキーへのアクセスを回復しない場合、最終的にデータベースにはアクセスできなくなるため、バックアップから復元する必要があります。詳細については、「DB インスタンスの暗号化」を参照してください。
- リードレプリカとその暗号化された DB インスタンスが同じ にある場合は AWS リージョン、同じ KMS キーを使用して両方を暗号化する必要があります。
- で AWS Config、rds-storage-encrypted AWS マネージドルールを実装して RDS DB インスタンスの暗号化を検証して適用し、rds-snapshots-encrypted ルールを実装して RDS データベーススナップショットの暗号化を検証して適用します。
- を使用して AWS Security Hub CSPM 、Amazon RDS リソースがセキュリティのベストプラクティスに従っているかどうかを評価します。詳細については、「Amazon RDS の Security Hub CSPM コントロール」を参照してください。

の暗号化のベストプラクティス AWS Secrets Manager

AWS Secrets Manager を使用すると、コード内のハードコードされた認証情報 (パスワードを含む) を Secrets Manager への API コールで置き換えて、プログラムでシークレットを取得することができます。Secrets Manager は と統合 AWS KMS され、 で保護された一意のデータキーを使用して、すべてのシークレット値のすべてのバージョンを暗号化します AWS KMS key。この統合により、暗号化 AWS KMS キーを使用して保存されたシークレットが保護され、暗号化されていないままになることはありません。また、KMS キーにカスタムアクセス許可を定義し、保存したシークレットを保護するデータキーを生成、暗号化、復号するオペレーションを監査することができます。詳細については、「AWS Secrets Managerのシークレットの暗号化と復号」を参照してください。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- ほとんどの場合、 `aws/secretsmanager` AWS マネージドキーを使用してシークレットを暗号化することをお勧めします。この使用には費用は発生しません。
- 別のアカウントからシークレットにアクセスしたり、暗号化キーにキーポリシーを適用したりするには、カスタマーマネージドキーを使用してシークレットを暗号化します。
  - キーポリシーで、値を `secretsmanager.<region>.amazonaws.com` kms:ViaService 条件キーに割り当てます。これにより、キーの使用が Secrets Manager からのリクエストのみに制限されます。
  - キーの使用をさらに制限して、正しいコンテキストを持つ Secrets Manager からのリクエストのみを使用するには、以下を作成して KMS キーを使用する条件として Secrets Manager 暗号化コンテキストのキーまたは値を使用します。
    - IAM ポリシーまたはキーポリシーの文字列条件演算子
    - 許可における権限の制約

Amazon S3 の暗号化のベストプラクティス

Amazon Simple Storage Service (Amazon S3) は、量にかかわらず、データを保存、保護、取得するのに役立つクラウドベースのオブジェクトストレージサービスです。

Amazon S3 でのサーバー側の暗号化には 3 つのオプションがあります。

- Amazon S3 が管理する暗号化キーによるサーバー側の暗号化 (SSE-S3)
- AWS Key Management Service (SSE-KMS) によるサーバー側の暗号化
- お客様が用意した暗号化キーを使用したサーバー側の暗号化 (SSE-C)

Amazon S3 はAmazon S3のすべてのバケットの暗号化の基本レベルとしてAmazon S3によるサーバー側の暗号化を適用します。2023 年 1 月 5 日以降、Amazon S3 にアップロードされるすべての新しいオブジェクトは、追加費用なしで、パフォーマンスに影響を与えずに自動的に暗号化されます。S3 バケットのデフォルトの暗号化設定と新しいオブジェクトのアップロードの自動暗号化ステータスは、 AWS CloudTrail ログ、S3 インベントリ、S3 ストレージレンズ、Amazon S3 コンソール、および AWS Command Line Interface (AWS CLI) と AWS SDKs の追加の Amazon S3 API レスポンスヘッダーとして使用できます。詳細については、「デフォルト暗号化に関するよくある質問」を参照してください。

アップロード時にサーバー側の暗号化を使用してオブジェクトを暗号化する場合は、リクエストに `x-amz-server-side-encryption` ヘッダーを追加して、SSE-S3、SSE-KMS、SSE-C を使用し

てオブジェクトを暗号化するよう Amazon S3 に指示します。`x-amz-server-side-encryption` ヘッダーの値としては次のようなものが考えられます。

- `AES256`。Amazon S3 が管理するキーを使用するよう、Amazon S3 に指示します。
- `aws:kms`。マネージド AWS KMS キーを使用するように Amazon S3 に指示します。
- SSE-C 用に値を `True` または `False` に設定します。

詳細については、「Defense-in-depth requirements 1: Data must be encrypted at rest and during transit」の「How to Use Bucket Policies and Apply Defense-in-Depth to Help Secure Your Amazon S3 Data」(AWS ブログ記事) を参照してください。

Amazon S3 でのクライアント側の暗号化には 2 つのオプションがあります。

- に保存されているキー AWS KMS
- アプリケーション内に保存されたキー

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- で AWS Config、s3-bucket-server-side-encryption-enabled AWS マネージドルールを実装して、S3 バケット暗号化を検証して適用します。
- アップロードされるすべてのオブジェクトが、`s3:x-amz-server-side-encryption` の条件を使用して暗号化されていることを検証する Amazon S3 バケットポリシーをデプロイします。詳細については、「SSE-S3 を使用したデータの保護」のバケットポリシーのサンプルと、「バケットポリシーの追加」を参照してください。
- S3 バケットのポリシーに `aws:SecureTransport` 条件を使用して、HTTPS (TLS) 経由での暗号化された接続のみを許可します。詳細については、S3-bucket-ssl-requests-only AWS Config 」ルールに準拠するためにどの S3 バケットポリシーを使用する必要がありますか?
- で AWS Config、s3-bucket-ssl-requests-only AWS マネージドルールを実装して、SSL を使用するリクエストを要求します。
- Amazon S3 オブジェクトにクロスアカウントアクセスを許可する必要がある場合は、カスタマーマネージドキーを使用します。他の AWS アカウントからのアクセスを許可するようにキーポリシーを設定します。

Amazon VPC の暗号化のベストプラクティス

Amazon Virtual Private Cloud (Amazon VPC) は、定義した仮想ネットワークに AWS リソースを起動するのに役立ちます。この仮想ネットワークは、お客様自身のデータセンターで運用されていた従来のネットワークに似ていますが、 AWSのスケーラブルなインフラストラクチャを使用できるというメリットがあります。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- 次のいずれかを使用して、企業ネットワークと VPC 内の情報資産とシステム間のトラフィックを暗号化します。
  - AWS Site-to-Site VPN 接続
  - IPsec で暗号化されたプライベート AWS Direct Connect 接続を提供する AWS Site-to-Site VPN と 接続の組み合わせ
  - AWS Direct Connect MAC セキュリティ (MACsec) をサポートして企業ネットワークから AWS Direct Connect ロケーションにデータを暗号化する 接続
- の VPC エンドポイントを使用して AWS PrivateLink 、インターネットゲートウェイを使用 AWS のサービス せずに、サポートされている に VPCs をプライベートに接続します。 AWS Direct Connect または Site-to-Site VPN のサービスを使用して、この接続を確立できます。VPC と他のサービス間のトラフィックは、 AWS ネットワークを離れません。詳細については、「Access AWS のサービス through AWS PrivateLink」を参照してください。
- セキュリティグループルールを設定して、TCP/443 経由の HTTPS など、安全なプロトコルと関連付けられたポートのトラフィックのみを許可します。セキュリティグループとそのルールを定期的に監査します。

リソース

- 「保管中のデータに対するエンタープライズ暗号化戦略の作成」（AWS 規範ガイダンス）
- （AWS KMS ドキュメント) のセキュリティのベストプラクティス AWS Key Management Service
- AWS のサービス の使用方法 AWS KMS (AWS KMS ドキュメント）
- セキュリティの柱: データ保護 (AWS Well-Architected Framework)

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
暗号化の更新	AWS 暗号化に関する章のアプローチを更新しました。	2026 年 2 月 19 日
アルゴリズムの更新	暗号化アルゴリズムセクションを更新しました。	2026 年 1 月 23 日
転送中のアルゴリズムと暗号化の更新	「暗号化アルゴリズムについて」セクションと「転送中のデータの暗号化」セクションを更新しました。	2025 年 10 月 28 日
アルゴリズムの更新	暗号化アルゴリズムに関する情報を暗号化アルゴリズムと AWS のサービスセクションに追加します。	2025 年 6 月 18 日
Amazon EKS の更新	Amazon Elastic Kubernetes Service (Amazon EKS) の暗号化のベストプラクティスを更新しました。	2025 年 1 月 7 日
Secrets Manager の更新	の情報と推奨事項を更新しました AWS Secrets Manager。	2024 年 9 月 9 日
AWS のサービス 更新	Amazon EKS、、Amazon Relational Database Service (Amazon RDS) AWS Encryption SDK、Amazon Simple Storage Service (Amazon S3) の情報と推奨事項を更新しました。	2024 年 9 月 4 日

初版発行	—	2022 年 12 月 2 日

AWS 規範ガイダンスの用語集

以下は、 AWS 規範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する。
- 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: お客様のオンプレミスの Oracle データベースを AWS クラウドの Oracle 用の Amazon Relational Database Service (Amazon RDS) に移行する。
- 再購入 (ドロップアンドショップ) — 通常、従来のライセンスから SaaS モデルに移行して、別の製品に切り替えます。例: 顧客関係管理 (CRM) システムを Salesforce.com に移行する。
- 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: お客様のオンプレミスの Oracle データベースを AWS クラウドの EC2 インスタンス上の Oracle に移行する。
- 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。
- 廃止 — 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制御」をご覧ください。

抽象化されたサービス

「マネージドユーザー」をご覧ください。

ACID

「原子性、一貫性、分離性、耐久性 (ACID)」をご覧ください。

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な方法ですが、さらに多くの作業が必要となります。

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

複数行に処理を行い、グループ全体を対象に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 MAX などがあります。

AI

「人工知能」をご覧ください。

AIOps

「AI オペレーション」をご覧ください。

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。

アプリケーション制御

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 の重要な要素であり、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?」をご覧ください。

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 (AZ)

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

「ビジネス継続性計画 (BCP)」をご覧ください。

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「動作グラフのデータ」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」もご覧ください。

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

それぞれが独立しているが、同一の環境を 2 つ作成するデプロイ戦略。現在のアプリケーションバージョンを 1 つの環境 (ブルー) で実行し、新しいアプリケーションバージョンを別の環境 (グリーン) 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ており、ボットハーダーまたはボットオペレーターと呼ば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。ボットネットは、ボットとその影響力を拡大する仕組みとして、非常によく知られています。

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、 AWS Well-Architected ガイダンスの「ブレークグラス手順の実装」インジケータを参照してください。

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、AWSでのコンテナ化されたマイクロサービスの実行ホワイトペーパーの「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

カナリアデプロイ

エンドユーザーへのバージョンリリースを、時間をかけて段階的に行うこと。確信が持てたら新規バージョンをデプロイして、現在のバージョン全体を置き換えます。

CCoE

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

CDC

「変更データキャプチャ」を参照してください。

変更データキャプチャ (CDC)

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

カオスエンジニアリング

障害や破壊的なイベントを意図的に導入して、システムの耐障害性をテストすること。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 AWS のサービス 受信する前に、ローカルでデータを暗号化します。

Cloud Center of Excellence (CCoE)

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

クラウドコンピューティング

リモートデータストレージと IoT デバイス管理に通常使用されるクラウドテクノロジー。クラウドコンピューティングは、一般的に、エッジコンピューティング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、 AWS クラウドへの移行時に通常実行する 4 つの段階。

- 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。移行戦略との関連性については、 AWS「移行準備ガイド」を参照してください。

CMDB

「構成管理データベース (CMDB)」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 や Bitbucket Cloud があります。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といった、ビジュアル形式の情報を分析および抽出する AI の分野。例えば、Amazon SageMaker AI では、CV 用の画像処理アルゴリズムを利用できます。

設定ドリフト

ワークロードにおいて、設定が想定した状態から変化すること。これによって、ワークロードが非準拠になる可能性がありますが、この状態は、徐々に生じ、意図的なものではありません。

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

非一元的で分散型のデータ所有権を持つとともに、一元的な管理およびガバナンスを行え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、一般的に、大量の履歴データが含まれており、多くの場合、それら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ます。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。

深層学習

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。

トラブルシューティング

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、「 AWSでのセキュリティコントロールの実装」の「検出的コントロール」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

スタースキーマにおいて、ファクトテーブルの定量データに関するデータ属性が含まれる小さいテーブル。ディメンションテーブルの属性は、通常、テキストフィールド、またはテキストのように扱える個別の数値で示されます。これらの属性は、一般的に、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)

ディザスタによるダウンタイムとデータ損失を最小限に抑えるための戦略とプロセス。詳細については、 AWS Well-Architected フレームワークの「 Disaster Recovery of Workloads on AWS: Recovery in the Cloud」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

「開発バリュー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、応答時間を改善できます。

電子データ交換 (EDI)

組織間で行う、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処理。

暗号化キー

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

エンディアン

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

エンドポイント

「サービスエンドポイント」を参照してください。

エンドポイントサービス

仮想プライベートクラウド (VPC) 内でホストして、他のユーザーと共有できるサービス。を使用してエンドポイントサービスを作成し AWS PrivateLink 、他の AWS アカウント または AWS Identity and Access Management (IAM) プリンシパルにアクセス許可を付与できます。これらのアカウントまたはプリンシパルは、インターフェイス VPC エンドポイントを作成することで、エンドポイントサービスにプライベートに接続できます。詳細については、Amazon Virtual Private Cloud (Amazon VPC) ドキュメントの「エンドポイントサービスを作成する」を参照してください。

エンタープライズリソースプランニング (ERP)

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

エンベロープ暗号化

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

環境

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

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

エピック

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

ERP

「エンタープライズリソース計画」を参照してください。

探索的データ分析 (EDA)

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

F

ファクトテーブル

スタースキーマの中央にあるテーブル。ビジネスオペレーションに関する定量的データが保存されます。一般的に、ファクトテーブルは、2 種類の列で構成されます。1 つは測定値が含まれる列、もう 1 つはディメンションテーブルへの外部キーが含まれる列です。

フェイルファスト

開発ライフサイクルを短縮するために、頻繁かつ段階的にテストを行う哲学であり、アジャイルアプローチでは、この考え方がきわめて重要です。

障害分離境界

では AWS クラウド、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、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のに役立ちます。詳細については、「AWS 障害分離境界」を参照してください。

機能ブランチ

「ブランチ」を参照してください。

特徴量

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

特徴量重要度

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

機能変換

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

数ショットプロンプト

LLM に、タスクと望ましい出力を示す例を少数提示した後に、類似のタスクを実行させること。この手法は、プロンプトに記述された例 (ショット) からモデルが学習する「インコンテキスト学

習」の一種です。数ショットプロンプトは、特定のフォーマット、推論、専門知識が必要な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制御」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

変更データのキャプチャによる継続的なデータ複製を利用して、段階的なアプローチではなく、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)

大規模な深層学習ニューラルネットワークであり、一般化およびラベル付けされていないデータからなる大規模データセットでトレーニングされています。FM により、言語理解、テキストおよび画像生成、自然言語での会話といった、一般的な各種タスクを実行できます。詳細については、「基盤モデルとは何ですか?」を参照してください。

G

生成 AI

AI モデルのサブセット。大量のデータでトレーニングされており、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ます。詳細については、「生成 AI とは何ですか?」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 ワークフローは古いと見なされている方法であり、トランクベースのワークフローは推奨されている新しい方法です。

ゴールデンイメージ

システムまたはソフトウェアのスナップショットであり、システムまたはソフトウェアの新規インスタンスをデプロイするテンプレートとして使用されます。製造の例で言えば、ゴールデンイメージを使用すると、複数のデバイスにソフトウェアをプロビジョニングして、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、、 AWS Security Hub CSPM、Amazon GuardDuty、、 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。

高可用性 (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用データセットから保留される、ラベル付き履歴データの一部。ホールドアウトデータを使用すると、モデル予測をホールドアウトデータと比較して、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

「インダストリアル IoT」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

既存インフラストラクチャの更新、パッチ適用、変更などを行わずに、本番環境ワークロードに使用する新規インフラストラクチャをデプロイするモデル。本質的に、イミュータブルインフラストラクチャは、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、予測性に優れています。詳細については、 AWS Well-Architected フレームワークにある「イミュータブルインフラストラクチャを使用してデプロイする」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 氏が提唱した用語で、接続、リアルタイムデータ、オートメーション、分析、AI/ML の進歩による、ビジネスプロセスのモダナイズを意味します。

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。

インダストリアル 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、「インダストリアル IoT (IIoT) デジタルトランスフォーメーション戦略の構築」を参照してください。

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

「IoT」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)

大量のデータで事前トレーニングされた深層学習 AI モデル。LLM では、質問への回答、ドキュメントの要約、他言語へのテキスト翻訳、文を完成させるなど、さまざまなタスクを実行できます。詳細については、「大規模言語モデル (LLM) とは何ですか?」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

「ラベルベースアクセス制御」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」もご覧ください。

LLM

「大規模言語モデル」を参照してください。

下位環境

「環境」を参照してください。

M

機械学習 (ML)

パターン認識と学習にアルゴリズムと手法を使用する人工知能の一種。ML は、モノのインターネット (IoT) データなどの記録されたデータを分析して学習し、パターンに基づく統計モデルを生成します。詳細については、「機械学習」を参照してください。

メインブランチ

「ブランチ」を参照してください。

マルウェア

コンピュータのセキュリティやプライバシーを侵害するように設計されたソフトウェア。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、不正アクセスを招く可能性があります。マルウェアの例には、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。マネージドサービスの例として、Amazon Simple Storage Service (Amazon S3) と Amazon DynamoDB が挙げられます。このサービスは、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、制御するソフトウェアシステムであり、工場では、これによって、原材料から製品を完成させます。

MAP

「Migration Acceleration Program」を参照してください。

メカニズム

ツールを作成してその導入を推進し、導入結果を調べて調整を行うための包括的なプロセス。メカニズムとは、運用中にそれ自体を強化し改善するサイクルを意味します。詳細については、AWS 「 Well-Architected フレームワーク」の「メカニズムの構築」を参照してください。

メンバーアカウント

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

MES

「製造実行システム」を参照してください。

Message Queuing Telemetry Transport (MQTT)

発行/サブスクライブのパターンに基づく、軽量のマシンツーマシン (M2M) 通信プロトコルであり、リソースに限りのある IoT デバイスに使用されます。

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)

オンラインツール。これによって、 AWS クラウドに移行するビジネスケースの検証に必要な情報を得られます。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 AWS クラウドに移行するために使用するアプローチ。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、「AWS クラウドでのアプリケーションのモダナイズ戦略」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、「AWS クラウドで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評価する」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

「Migration Portfolio Assessment」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。

ミュータブルなインフラストラクチャ

本番ワークロードに使用する既存のインフラストラクチャを更新および変更するためのモデル。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

「オリジンアクセス制御」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

「オペレーショナルレベルアグリーメント」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。

Open Process Communications - Unified Architecture (OPC-UA)

産業オートメーション用のマシンツーマシン (M2M) 通信プロトコル。OPC-UA により、相互運用の際に、データ暗号化、認証、認可の各スキームを標準化できます。

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)

質問と関連するベストプラクティスのチェックリスト。インシデントや起こり得る障害を理解、評価、防止したり、その範囲を縮小したりする際に役立ちます。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させるハードウェアおよびソフトウェアシステム。製造分野では、Industry 4.0 への変革を進める上で、OT と情報技術 (IT) システムの統合に焦点が当てられています。

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により、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。

オリジンアクセス制御 (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制御が可能です。

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

「プログラマブル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

次の操作を可能にするオブジェクト: アクセス許可を定義する (ID ベースのポリシーを参照)。アクセス条件を指定する (リソースベースのポリシーを参照)。 AWS Organizations の組織における全アカウントにアクセス許可の上限を定義する (サービスコントロールポリシーを参照)。

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。

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、「移行の準備状況の評価」を参照してください。

述語

`true` または `false` を返すためのクエリ条件。一般的に、`WHERE` 句に記述されます。

述語プッシュダウン

データベースクエリを最適化する手法。これによって、転送前にクエリ内のデータをフィルタリングします。この手法を取ると、リレーショナルデータベースから取得し処理する必要のあるデータの量が減少するため、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、「AWSでのセキュリティコントロールの実装」の「予防的コントロール」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」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してプライバシーが考慮されている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

非準拠リソースのデプロイ防止を目的としたセキュリティコントロール。このコントロールにより、プロビジョニング前にリソースをスキャンします。コントロールに準拠していないリソースは、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)

製品の設計、開発、発売から、成長、成熟、衰退、廃棄に至る、製品のライフサイクル全体を通してデータとプロセスを管理すること。

本番環境

「環境」を参照してください。

プログラマブルロジックコントローラー (PLC)

製造分野で使用される、信頼性と適応性に優れたコンピュータであり、これによって、マシンをモニタリングするとともに、製造プロセスを自動化します。

プロンプトチェイニング

1 つの LLM プロンプトによる出力を次のプロンプトの入力に使用して、より良いレスポンスを生成します。この手法を使用すると、複雑なタスクをサブタスクに分割したり、事前レスポンスを繰り返し改良または拡張したりできます。これによって、モデルのレスポンスの精度と関連性が向上し、粒度の高いパーソナライズされた結果を得られます。

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。

発行/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。これにより、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 の場合、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可能なチャネルにイベントメッセージを発行できます。このシステムでは、発行サービスの変更なしに、新規マイクロサービスを追加できます。

Q

クエリプラン

手順などの一連のステップであり、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ます。

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

「実行責任者、説明責任者、協業先、報告先 (RACI)」を参照してください。

RAG

「検索拡張生成」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

「実行責任者、説明責任者、協業先、報告先 (RACI)」を参照してください。

RCAC

「行と列のアクセス制御」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。

リアーキテクト

「7 Rs」を参照してください。

目標復旧時点 (RPO)

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

目標復旧時間 (RTO)

サービスの中断から復旧までの最大許容遅延時間。

リファクタリング

「7 Rs」を参照してください。

リージョン

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

リグレッション

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。

リプラットフォーム

「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

中断に抵抗または中断から回復するアプリケーションの機能。 AWS クラウドでの回復力を計画する際には、一般的に、高可用性とディザスタリカバリが考慮されます。詳細については、「AWS クラウド の耐障害性」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。サポートが含まれる場合は RASCI マトリックスと呼ばれ、含まれない場合は 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、「 AWSでのセキュリティコントロールの実装」の「レスポンシブコントロール」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。

検索拡張生成 (RAG)

生成 AI の技術。これにより、LLM では、レスポンスの生成前に、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が参照されます。例えば、RAG モデルによって、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できる場合があります。細については、「RAG (検索拡張生成) とは何ですか?」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情報を更新して、攻撃者が認証情報にアクセスするのをより困難にするプロセス。

行と列のアクセス制御 (RCAC)

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

RPO

「目標復旧時点」を参照してください。

RTO

「目標復旧時間」を参照してください。

ランブック

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

S

SAML 2.0

多くの ID プロバイダー (IdP) が使用しているオープンスタンダード。この機能を使用すると、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 マネジメントコンソール 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

「監視制御とデータ取得」を参照してください。

SCP

「サービスコントロールポリシー」を参照してください。

シークレット

暗号化された形式で保存するパスワードやユーザー認証情報などの AWS Secrets Manager機密情報または制限付き情報。シークレット値とそのメタデータで構成されます。シークレット値には、バイナリ、1 つの文字列、複数の文字列を指定できます。詳細については、Secrets Manager ドキュメントの「Secrets Manager シークレットの概要」を参照してください。

セキュリティバイデザイン

開発プロセス全体を通してセキュリティが考慮されているシステムエンジニアリングのアプローチ。

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、主に 4 つの種類があります。4 つとは、予防、検出、レスポンシブ、プロアクティブです。

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への自動レスポンスまたは自動修復を目的として、事前定義および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には、VPC セキュリティグループの変更、Amazon EC2 インスタンスへのパッチ適用、認証情報の更新などがあります。

サーバー側の暗号化

送信先にあるデータの、それ AWS のサービス を受け取る による暗号化。

サービスコントロールポリシー (SCP)

AWS Organizationsの組織内の、すべてのアカウントのアクセス許可を一元的に管理するポリシー。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、スループットといった、サービスパフォーマンス面の指標。

サービスレベル目標 (SLO)

サービスレベルインジケータによって測定され、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

「Security Information and Event Management システム」を参照してください。

単一障害点 (SPOF)

特定のアプリケーションを構成する単一の重要なコンポーネントで発生し、システム稼働に支障をきたす可能性のある障害。

SLA

「サービスレベルアグリーメント」を参照してください。

SLI

「サービスレベルインジケータ」を参照してください。

SLO

「サービスレベルの目標」を参照してください。

スプリットアンドシードモデル

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

データベースの編成構造を意味し、1 つの大きいファクトテーブルにトランザクションデータまたは測定データが保存され、1 つ以上の小さいディメンションテーブルにデータ属性が保存されます。この構造は、データウェアハウスやビジネスインテリジェンスを用途と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。

監視制御とデータ取得 (SCADA)

製造分野において、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運用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、起こり得る問題を検出したり、パフォーマンスをモニタリングしたりすることで、システムをテストします。Amazon CloudWatch Synthetics を使用すると、こうしたテストを作成できます。

システムプロンプト

コンテキスト、指示、ガイドラインなどを提示して、LLM に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て、ユーザーとやり取りするルールを確立するのに有用です。

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 枚のピザを分け合える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している行のグループに計算を実行する SQL 関数。ウィンドウ関数は、移動平均を計算したり、現在の行の相対位置に基づいて他の行の値にアクセスするといった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

「Write-Once-Read-Many」を参照してください。

WQF

「AWS ワークロード資格フレームワーク」を参照してください

Write-Once-Read-Many (WORM)

データを 1 回のみ書き込むことで、データの削除や変更を防ぐストレージモデル。承認済みユーザーは、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

ゼロデイ脆弱性を悪用した攻撃 (一般的にマルウェアによる)。

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 にタスク実行の手順は提示するが、実行のガイドとして役立つ例 (ショット) は提示しない方法。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。