AWS プライバシーリファレンスアーキテクチャ (AWS PRA)

AWS 規範ガイダンス

AWS 規範ガイダンス: AWS プライバシーリファレンスアーキテクチャ (AWS PRA)

Table of Contents

AWS プライバシーリファレンスアーキテクチャ (AWS PRA)

Amazon Web Services (寄稿者)

2024 年 3 月 (ドキュメント履歴)

ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

注意

このガイドは、情報提供のみを目的として提供されています。これは法的助言ではなく、法的助言として頼るべきではありません。 は、プライバシーおよびデータ保護環境の実装、より一般的にはビジネスに関連する適用法に関する適切な助言を顧客に求める AWS よう促します。

お客様は、本書に記載されている情報を独自に評価する責任を負うものとします。本書は、(a) 情報提供のみを目的としており、(b) 通知なしに変更される可能性がある現在の AWS 製品提供および慣行を表し、(c) AWS およびその関連会社、サプライヤー、または許諾者からのコミットメントまたは保証を作成しません。 AWS 製品またはサービスは、明示または黙示を問わず、保証、表明、または条件なしに現状のまま提供されます。

顧客 AWS に対する の責任と責任は契約によって AWS 管理され、本書は AWS とその顧客間の契約の一部でも変更もしません。

序章

AWS プライバシーリファレンスアーキテクチャ (PRA) は、 のプライバシーサポートコントロールの設計と設定に固有の一連のガイドラインを提供します AWS のサービス。このガイドは、 のプライバシーをサポートする人、プロセス、テクノロジーに関する意思決定に役立ちます AWS クラウド。

責任 AWS 共有モデルとプライバシー

では AWS クラウド、 のセキュリティとコンプライアンスに関する責任を共有します AWS。 AWS はクラウドのセキュリティを担当します。つまり、 AWS は で提供されるすべてのサービスを実行

するインフラストラクチャを保護する責任を担います AWS クラウド。クラウドのセキュリティはお客様の責任となります。つまり、セキュリティとプライバシーの要件 AWS のサービス に従って設定および管理を行う責任はお客様にあります。詳細については、AWS 「 責任共有モデル」を参照してください。

AWS のサービス は、プライバシー要件をサポートするために、クラウドに独自のプライバシーコントロールを実装できる機能を提供します。プライバシー責任は、選択した AWS のサービス および AWS リージョン 、それらのサービスの IT 環境への統合、組織やワークロードに適用される法律や規制など、さまざまな要因によって異なります。

を使用する場合 AWS のサービス、コンテンツに対する制御は維持されます。具体的には、コンテンツは、ユーザーまたはエンドユーザーがアカウント AWS のサービス に関連して によって処理、保存、またはホスティングするために当社に移管するソフトウェア (マシンイメージを含む) 、データ、テキスト、オーディオ、ビデオ、またはイメージとして定義されます。また、ユーザーまたはエンドユーザーが を使用して導き出す計算結果も含まれます AWS のサービス。お客様には、お客様の管理下にある以下の決定を管理する責任があります。

- で収集、保存、または処理するために選択したデータ AWS
- データ AWS のサービス で使用する
- データを収集、保存、または処理 AWS リージョン する 。
- データの形式と構造、およびデータのマスキング、匿名化、暗号化のいずれを行うか
- 暗号化用の暗号化キーを定義、保存、ローテーション、運用する方法
- 誰がデータにアクセスできるか、いつデータにアクセスできるか、それらのアクセス権が付与、管理、および取り消される方法

責任 AWS 共有モデルと、それがクラウドでの運用にどのように一般的に適用されるかを理解したら、ユースケースにどのように適用されるかを決定する必要があります。 AWS のサービス 使用する は、組織のプライバシー責任の一部として実行する必要がある設定の量を決定します。例えば、Amazon Elastic Compute Cloud (Amazon EC2) などのサービスは、Infrastructure as a Service (IaaS) に分類されます。そのため、Amazon EC2 を使用する場合は、ゲストオペレーティングシステムと EC2 インスタンスにインストールするアプリケーションソフトウェアまたはユーティリティに必要なすべてのプライバシー設定を実行する必要があります。Amazon Simple Storage Service (Amazon S3) や Amazon DynamoDB などの抽象化されたサービスを使用する場合、 AWS 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、プラットフォームを担当します。ユーザーの責任は、データを管理および分類し、データを保存および取得するためにエンドポイントへのアクセ

スに使用されるポリシーを設定することです。がデータとプライバシーを保護する方法 AWS の詳細については、「」の「データ保護とプライバシー AWS」を参照してください。

AWS PRA について

ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

このセクションでは、 AWS プライバシーリファレンスアーキテクチャ (AWS PRA) とその他の AWS ガイダンスの関係について説明します。このセクションでは、 AWS PRA の AWS マルチアカウント環境の例の一般的なレイアウトと構造も確認します。

このセクションは、以下のトピックで構成されます。

- AWS PRA と AWS SRA の使用
- AWS Organizations と専用アカウント構造
- AWS プライバシーサービスの運用

AWS PRA と AWS SRA の使用

ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

AWS PRA は、お客様が のインフラストラクチャとワークロードの基盤およびアプリケーションレベルのプライバシーコントロールを計画する際に役立つパターンを提供します AWS。AWS セキュリティリファレンスアーキテクチャ (AWS SRA) は、 AWS ランディングゾーンとアプリケーション全体で適切なセキュリティコントロールを実装およびサポートするアーキテクチャを構築するための一連のガイドラインを提供します。このガイドで詳しく説明されているプライバシーコントロールを確立するために、 AWS PRA は AWS SRA で説明されているのと同じ基本的なガイドラインとアカウント構造の多くを引き受けます。 AWS PRA と AWS SRA は、同じキー の多くを詳細に示します AWS のサービス。このガイドには、これらのサービスの簡単な説明のみが記載されています。これらのサービスの詳細と、 AWS SRA のセキュリティコンテキストでの使用方法について説明します。

AWS SRA は、 AWS セキュリティサービスを設計、実装、管理し、 AWS 推奨プラクティスに合わせるのに役立ちます。 AWS SRA はスタンドアロンガイドとして使用することも、 AWS SRA と

AWS PRA をコンパニオンガイドとして使用することもできます。 AWS SRA に詳述されているセキュリティガイドラインの多くは、 AWS PRA に詳述されているプライバシーコントロールと連動して従うことができます。セキュリティと同様に、 AWS クラウド ジャーニーの早い段階で行うと組織のアカウント構造の設計に影響を与える可能性があるため、プライバシーに関する基本的な考慮事項があります。例えば、次のような質問が考えられます。

- 組織は個人データをどのように定義していますか？
- 組織は個人データを処理するアプリケーションをサポートしていますか？
- 他のタイプの規制対象データを処理するアプリケーションについてはどうですか？
- デベロッパーやクラウドエンジニアを個人データからできるだけ遠ざけるために、どのような組織レベルのコントロールを実装できますか？
- 個人データを他のタイプのデータから分離するにはどうすればよいですか？
- 組織のクロスボーダーデータ転送要件は何ですか？

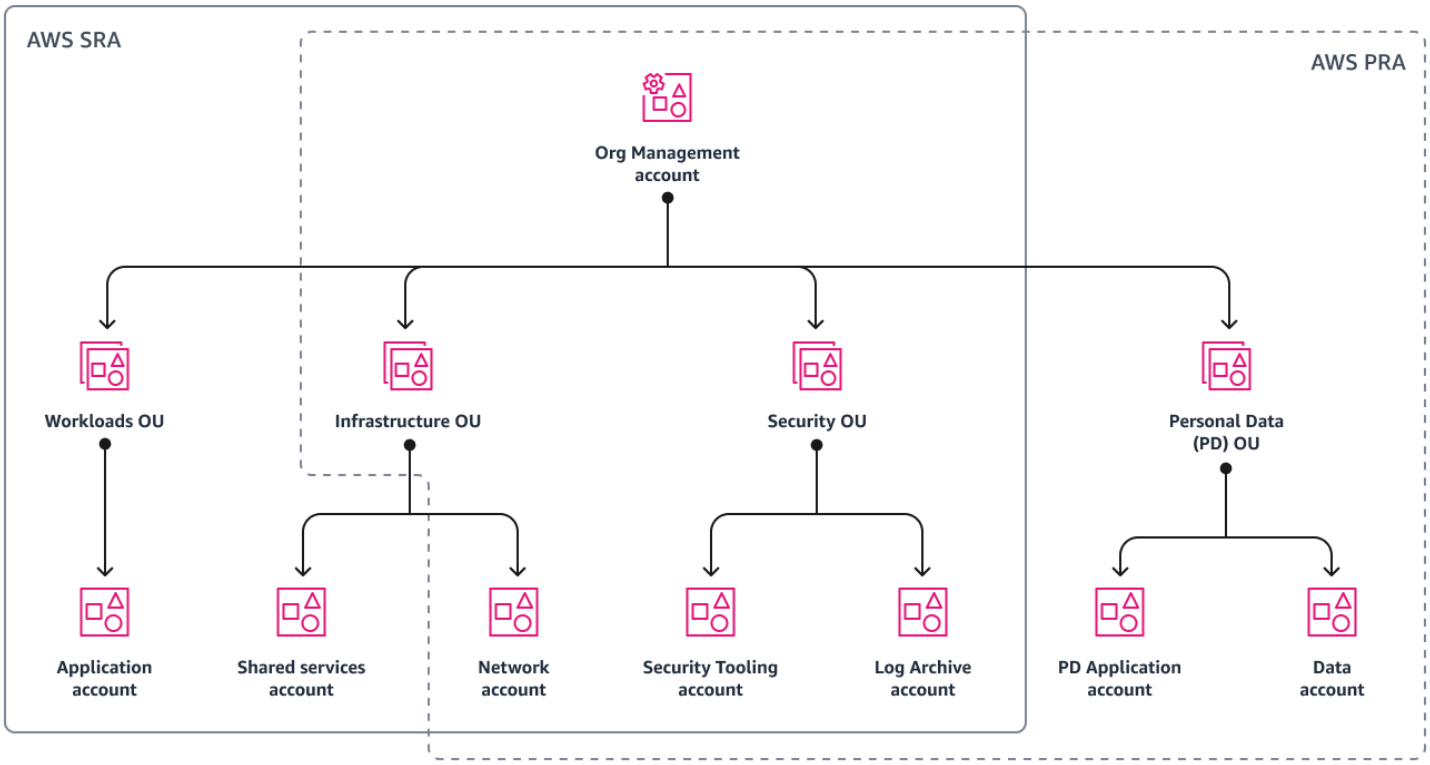
これらの質問の多くに対する回答は、 AWS アカウント 構造、サービスコントロールポリシー、AWS Identity and Access Management (IAM) ロールなど、クラウド環境の設計に影響を与える可能性があります。

AWS Organizations と専用アカウント構造

> ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

AWS Organizations は、複数の を一元的に管理および管理するのに役立つアカウント管理サービスです AWS アカウント。の使用は、適切に設計されたマルチアカウント AWS 環境の基礎 AWS Organizations です。詳細については、「ベストプラクティス AWS 環境の確立」を参照してください。

次の図は、 AWS PRA の大まかなアカウントと組織単位 (OU) 構造を示しています。ほとんどの場合、PRA の AWS 組織構造は AWS SRA の組織構造と一致します。



AWS SRA 組織からの逸脱には以下が含まれます。

- AWS PRA は、個人データの収集、保存、処理専用の個人データ (PD) OU を追加します。この構造的な分離により柔軟性が得られ、意図しない開示から個人データを保護するのに役立つ特定のきめ細かなコントロールを定義できます。
- インフラストラクチャ OU では、現在 AWS PRA には、 AWS SRA で説明されている共有サービスアカウントに関する追加のガイダンスは含まれていません。
- AWS PRA には、現在、 AWS SRA で説明されているワークロード OU に関する追加のガイダンスは含まれていません。個人データを収集または処理するアプリケーションは、PD OU の専用アカウントにあります。

は、組織全体のセキュリティとプライバシーのコントロールの全体的な基礎ガバナンスと自動デプロイAWS Control Towerに使用できます。 AWS Control Tower が組織で現在使用されていない場合でも、サービスコントロールポリシーや AWS Config ルールなど AWS Control Tower、セキュリティとプライバシーのコントロールの多くをそれぞれのサービスにデプロイできます。

アカウントとアカウントセグメンテーション戦略を含む OU 構造を計画するときに、個人データの処理を検討すると役立つ場合があります。処理するデータのタイプを、固有のユースケースや適用可能な法律や規制について考慮する必要がある場合があります。例えば、カード所有者データは

Payment Card Industry Data Security Standard (PCI DSS) で保護されており、保護対象の医療情報は医療保険の相互運用性と説明責任に関する法律 (HIPAA) の対象となる場合があります。個人データが含まれている環境を確認し、それに関するセグメンテーション戦略を綿密に計画したい場合があります。一般的なアカウントセグメンテーション戦略には、開発、ステージング、品質保証 (QA)、本番稼働専用のアカウントなど、ソフトウェア開発ライフサイクル (SDLC) AWS アカウント に合わせた専用の を含めることができます。このようなセグメンテーション戦略は、全体的な設計上の議論において重要な要素となる可能性があり、OUs は特定の規制要件に合わせる必要がある場合があります。

AWS プライバシーサービスの運用

ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

多くの人にとって、プライバシーはクロスカットです。規制チーム、コンプライアンスチーム、エンジニアリングチームなど、さまざまなチームが果たすべき役割があります。組織がプライバシープログラムの主要人物とポリシーコンポーネントの定義を開始したら、プライバシーコンプライアンスフレームワークに対してコントロールをマッピングして、一貫した運用を実現できます。フレームワークは、 AWS 環境内の個人データの基盤となるアプリケーション固有のプライバシーコントロールを実装するためのルーブリックとして機能します。

顧客がプライバシー要件の分類に使用するフレームワークにかかわらず、プライバシーコンプライアンス、プライバシーエンジニアリング、アプリケーションチームは、多くの場合、実装目標を達成するために協力する必要があります。例えば、規制チームとコンプライアンスチームが高レベルの要件を提供し、エンジニアリングチームとアプリケーションチームがこれらの要件に合わせて AWS のサービス と 機能を設定する場合があります。コントロールフレームワークから始めると、より規範的な組織的および技術的なコントロールを定義するのに役立ちます。

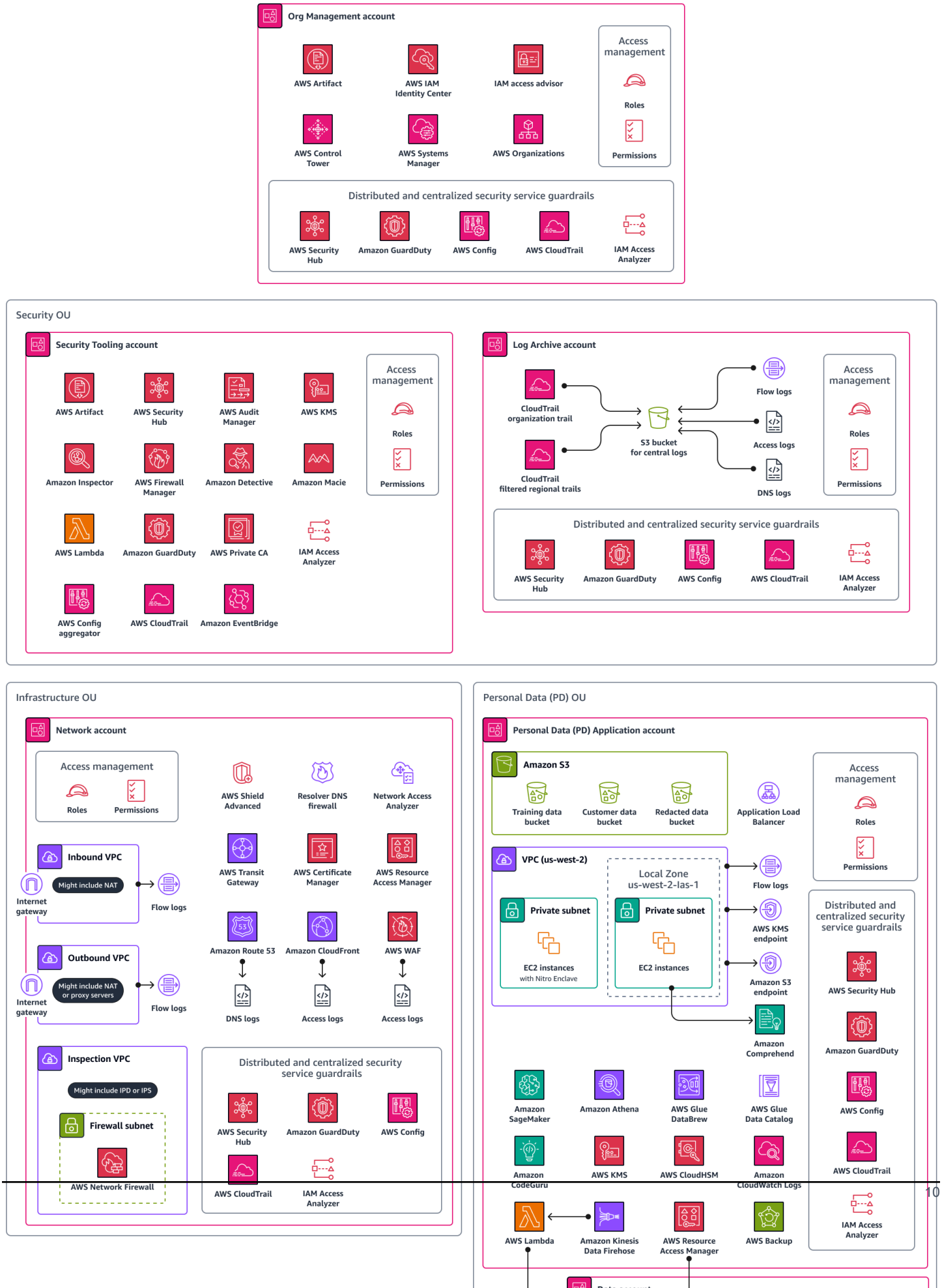
AWS のサービス および 機能の技術的コントロールを定義する際のもう 1 つの重要な決定は、コントロールを組織全体、OU、アカウント、または特定のリソースに適用するかどうかです。一部のサービスと機能は、 AWS 組織全体にコントロールを実装するのに最適です。例えば、Amazon S3 バケットへのパブリックアクセスをブロックすることは、アカウントごとに個別に設定するのではなく、組織のルートで設定するのが望ましい特定のコントロールです。ただし、保持ポリシーはアプリケーションによって異なる場合があります。つまり、リソースレベルでコントロールを適用できます。

組織内のプライバシーの運用を加速するために、 AWS は AWS ワークロードに監査およびコンプライアンスのアドバイザリサービスを提供しています。詳細については、AWS SAS にお問い合わせください。

AWS プライバシーリファレンスアーキテクチャ

ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

次の図は、 AWS プライバシーリファレンスアーキテクチャ (AWS PRA) を示しています。これは、多くのプライバシー関連の AWS のサービス および 機能を接続するアーキテクチャの例です。このアーキテクチャは、 によって管理されるランディングゾーン上に構築されています AWS Control Tower。


Org Management account
AWS Artifact
AWS IAM Identity Center
IAM access advisor
AWS Control Tower
AWS Systems Manager
AWS Organizations
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Security OU
Security Tooling account
AWS Artifact
AWS Security Hub
AWS Audit Manager
AWS KMS
Amazon Inspector
AWS Firewall Manager
Amazon Detective
Amazon Macie
AWS Lambda
Amazon GuardDuty
AWS Private CA
IAM Access Analyzer
AWS Config aggregator
AWS CloudTrail
Amazon EventBridge
Access management
Roles
Permissions
Log Archive account
CloudTrail organization trail
CloudTrail filtered regional trails
S3 bucket for central logs
Flow logs
Access logs
DNS logs
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Infrastructure OU
Network account
Access management
Roles
Permissions
Inbound VPC
Might include NAT
Internet gateway
Flow logs
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
Inspection VPC
Might include IPD or IPS
Firewall subnet
AWS Network Firewall
AWS Shield Advanced
Resolver DNS firewall
Network Access Analyzer
AWS Transit Gateway
AWS Certificate Manager
AWS Resource Access Manager
Amazon Route 53
Amazon CloudFront
AWS WAF
DNS logs
Access logs
Access logs
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Personal Data (PD) OU
Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application Load Balancer
VPC (us-west-2)
Local Zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Amazon Comprehend
Amazon SageMaker
Amazon Athena
AWS Glue DataBrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer

AWS PRA には、個人データ (PD) アプリケーションアカウントでホストされるサーバーレスウェブアーキテクチャが含まれています。このアカウントのアーキテクチャは、コンシューマーから直接個人データを収集するワークロードの例です。このワークロードでは、ユーザーはウェブ層を介して接続します。ウェブ層はアプリケーション層とやり取りします。この階層は、ウェブ階層から入力を受け取り、データを処理して保存し、承認された内部チームや第三者がデータにアクセスすることを許可し、不要になったデータは最終的にアーカイブおよび削除されます。このアーキテクチャは、データレイク、コンテナ、コンピューティング、モノのインターネット (IoT) などの特定のユースケースを掘り下げることなく、基本的なプライバシーエンジニアリング手法の多くを実証するために、意図的にモジュール化され、イベント駆動型です。

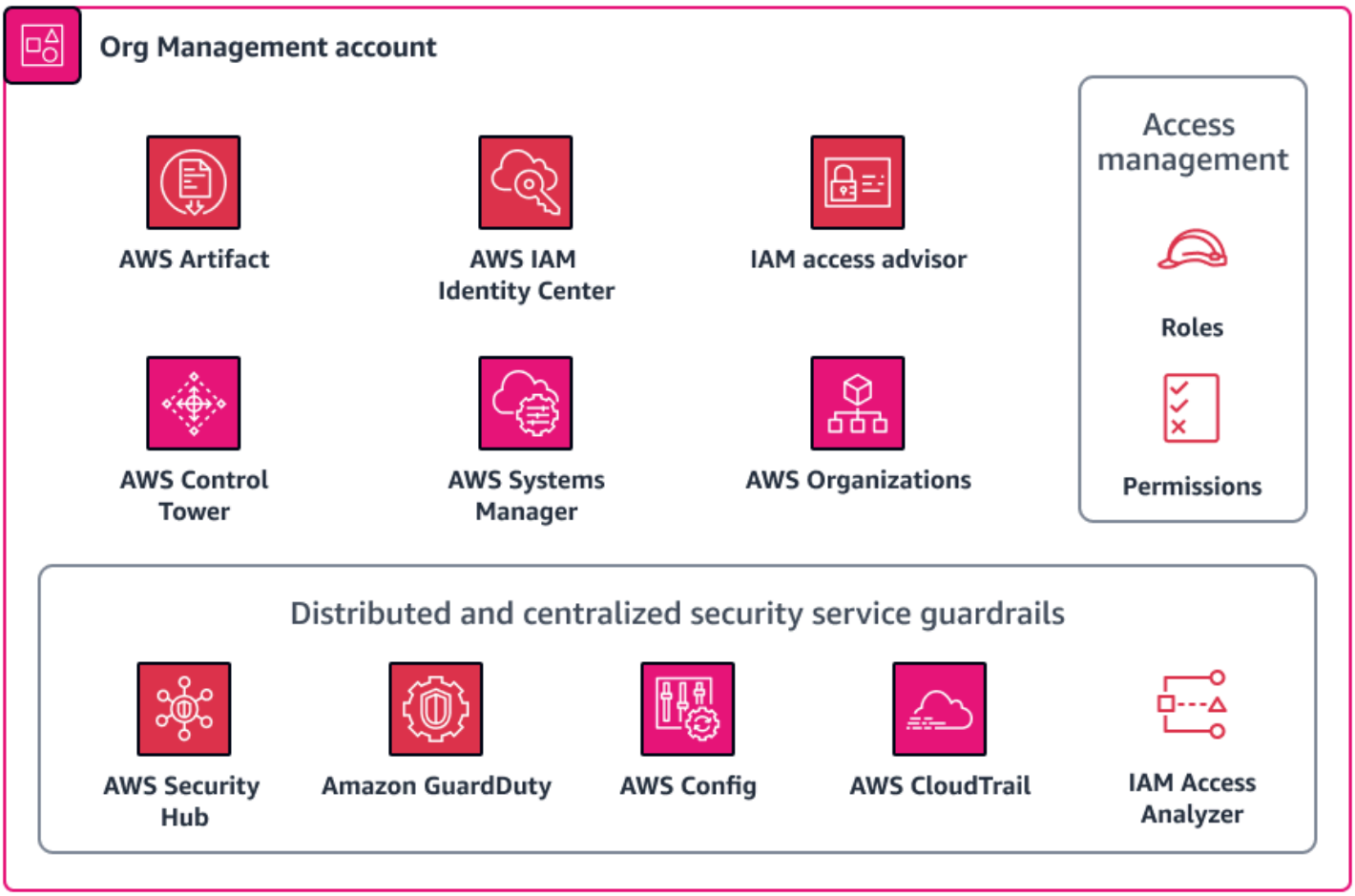
次に、このガイドでは、組織内の各アカウントについて詳しく説明します。以下の各アカウントのプライバシー関連のサービスと機能、考慮事項と推奨事項、および図について説明します。

- 組織管理アカウント
- セキュリティ OU - Security Tooling アカウント
- セキュリティ OU — ログアーカイブアカウント
- インフラストラクチャ OU — ネットワークアカウント
- 個人データ OU – PD アプリケーションアカウント

組織管理アカウント

ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

組織管理アカウントは主に、 によって管理される組織内のすべてのアカウントにおける基本的なプライバシーコントロールのリソース設定ドリフトを管理するために使用されます AWS Organizations。このアカウントは、同じセキュリティとプライバシーのコントロールの多くを使用して、新しいメンバーアカウントを一貫してデプロイできる場所でもあります。このアカウントの詳細については、AWS 「セキュリティリファレンスアーキテクチャ (AWS SRA)」を参照してください。次の図は、組織管理アカウントで設定されている AWS セキュリティおよびプライバシーサービスを示しています。



このセクションでは、このアカウントで使用される以下 AWS のサービス に関する詳細情報を提供します。

- AWS Artifact
- AWS Control Tower
- AWS Organizations

AWS Artifact

AWS Artifact は、 AWS セキュリティおよびコンプライアンスドキュメントのオンデマンドダウンロードを提供することで、監査に役立ちます。このサービスがセキュリティコンテキストでどのように使用されるかの詳細については、AWS 「セキュリティリファレンスアーキテクチャ」を参照してください。

これにより AWS のサービス 、 から AWS 継承するコントロールを理解し、 環境で実装するために残っている可能性のあるコントロールを特定できます。 は、システムおよび組織管理 (SOC) レポー

トや支払いカード業界 (PCI) レポートなどの AWS セキュリティおよびコンプライアンスレポートへのアクセス AWS Artifact を提供します。また、 AWS コントロールの実装と運用の有効性を検証する、地域やコンプライアンスの業種にわたる認定機関からの認定へのアクセスも提供します。を使用すると AWS Artifact、 AWS セキュリティコントロールの証拠として AWS 監査アーティファクトを監査人または規制当局に提供できます。以下のレポートは、 AWS プライバシーコントロールの有効性を示すのに役立ちます。

- SOC 2 タイプ 2 プライバシーレポート – このレポートは、個人データの収集、使用、保持、開示、および廃棄方法に対する AWS コントロールの有効性を示しています。詳細については、「SOC に関するよくある質問」を参照してください。
- SOC 3 プライバシーレポート – SOC 3 プライバシーレポートは、一般的な配布に関する SOC プライバシーコントロールのより詳細な説明です。
- ISO/IEC 27701:2019 認定レポート –ISO/IEC 27701:2019 では、プライバシー情報管理システム (PIMS) を確立し、継続的に改善するための要件とガイドラインについて説明しています。このレポートは、この証明書の範囲を詳しく説明し、 AWS 証明書の証明として役立ちます。この標準の詳細については、ISO/IEC 27701:2019 (ISO ウェブサイト) を参照してください。

AWS Control Tower

AWS Control Tower は、規範的なセキュリティのベストプラクティスに従う AWS マルチアカウント環境をセットアップして管理するのに役立ちます。このサービスがセキュリティコンテキストでどのように使用されるかの詳細については、AWS 「セキュリティリファレンスアーキテクチャ」を参照してください。

では AWS Control Tower、データレジデンシーとデータ保護の要件に合った、ガードレール とも呼ばれる、多数のプロアクティブ、予防的、検出的なコントロールのデプロイを自動化することもできます。例えば、データの転送を承認された のみに制限するガードレールを指定できます AWS リージョン。さらにきめ細かな制御のために、Amazon Virtual Private Network (VPN) 接続の禁止、Amazon VPC インスタンスのインターネットアクセスの禁止、リクエストされた に基づく へのアクセスの拒否など、データレジデンシーを制御するように設計された 17 を超えるガードレールから選択できます。 AWS AWS リージョンこれらのガードレールは、組織全体に均一にデプロイできる多数の AWS CloudFormation フック、サービスコントロールポリシー、および AWS Config ルールで構成されます。詳細については、 AWS Control Tower ドキュメントの「データレジデンシー保護を強化するコントロール」を参照してください。

データレジデンシーコントロールを超えてプライバシーガードレールをデプロイする必要がある場合、 AWS Control Tower にはいくつかの必須コントロール が含まれます。これらのコントロール

は、ランディングゾーンを設定するときに、すべての OU にデフォルトでデプロイされます。これらの多くは、ログアーカイブの削除の禁止や CloudTrail ログファイル の整合性検証の有効化など、ログを保護するように設計された予防的コントロールです。

AWS Control Tower は、検出コントロールを提供するために AWS Security Hub とも統合されています。これらのコントロールは、サービスマネージドスタンダードと呼ばれます。 AWS Control Towerこれらのコントロールを使用して、Amazon Relational Database Service (Amazon RDS) データベースインスタンスの保管時の暗号化など、プライバシーをサポートするコントロールの設定ドリフトをモニタリングできます。

AWS Organizations

AWS PRA は AWS Organizations を使用して、アーキテクチャ内のすべてのアカウントを一元管理します。詳細については、このガイドの「AWS Organizations と専用アカウント構造」を参照してください。では AWS Organizations、サービスコントロールポリシー (SCPsと管理ポリシーを使用して、個人データとプライバシーを保護することができます。

サービスコントロールポリシー (SCP)

サービスコントロールポリシー (SCPsは、組織内のアクセス許可を管理するために使用できる組織ポリシーの一種です。ターゲットアカウント、組織単位 AWS Identity and Access Management (OU)、または組織全体の (IAM) ロールとユーザーに対して、使用可能な最大アクセス許可を一元的に制御できます。組織管理アカウントから SCPs を作成して適用できます。

を使用して AWS Control Tower 、アカウント間で SCPs均一にデプロイできます。を通じて適用できるデータレジデンシーコントロールの詳細については AWS Control Tower、このガイドAWS Control TowerのSCPsの完全な補完 AWS Control Tower が含まれています。が組織で現在使用 AWS Control Tower されていない場合は、これらのコントロールを手動でデプロイすることもできます。

SCPs を使用してデータレジデンシー要件に対応する

特定の地理的リージョンにデータを保存して処理することで、個人データの居住要件を管理するのが一般的です。管轄区域固有のデータ所在地の要件が満たされていることを確認するには、規制チームと緊密に連携して要件を確認することをお勧めします。これらの要件が決定されると、サポートに役立つ AWS 基本的なプライバシーコントロールが多数存在します。例えば、SCPs を使用して、データの処理と保存 AWS リージョン に使用できる を制限できます。サンプルポリシーについては、このガイド間でのデータ転送を制限する AWS リージョンの「」を参照してください。

SCPs を使用して高リスク API コールを制限する

どのセキュリティとプライバシーのコントロール AWS に責任があり、どのセキュリティとプライバシーのコントロールに責任があるかを理解することが重要です。例えば、使用する に対して実行できる API コールの結果は、お客様の責任 AWS のサービス となります。また、どの呼び出しがセキュリティやプライバシー体制の変更につながる可能性があるかを理解する責任もあります。特定のセキュリティおよびプライバシー体制の維持について懸念がある場合は、特定の API コールを拒否する SCPsを有効にできます。これらの API コールは、個人データの意図しない開示や特定のクロスボーダーデータ転送の違反などに影響を与える可能性があります。例えば、次の API コールを禁止することができます。

- Amazon Simple Storage Service (Amazon S3) バケットへのパブリックアクセスの有効化
- Amazon を無効にする GuardDuty か、Trojan:EC2/DNSDataExfiltration 検出結果などのデータ流出検出結果の抑制ルールを作成する
- AWS WAF データ流出ルールの削除
- Amazon Elastic Block Store (Amazon EBS) スナップショットのパブリック共有
- 組織からメンバーアカウントを削除する
- リポジトリから Amazon CodeGuru Reviewer の関連付けを解除する

管理ポリシー

の管理ポリシー AWS Organizations は、 AWS のサービス とその機能を一元的に設定および管理するために役立ちます。選択した管理ポリシーのタイプによって、ポリシーが継承する OUs とアカウントにどのように影響するかが決まります。タグポリシーは、プライバシーに直接関連する の管理ポリシーの例 AWS Organizations です。

タグポリシーの使用

タグは、 AWS リソースの管理、識別、整理、検索、フィルタリングに役立つキーと値のペアです。個人データを処理する組織内のリソースを区別するタグを適用すると便利です。タグの使用は、このガイドの多くのプライバシーソリューションをサポートしています。例えば、リソース内で処理または保存されるデータの一般的なデータ分類を示すタグを適用できます。特定のタグまたはタグのセットを持つリソースへのアクセスを制限する属性ベースのアクセスコントロール (ABAC) ポリシーを記述できます。例えば、ポリシーで、SysAdminロールが `dataclassification:4` タグを持つリソースにアクセスできないように指定できます。詳細とチュートリアルについては、IAM ドキュメントの「タグに基づいて AWS リソースにアクセスするためのアクセス許可を定義する」を参照してください。さらに、組織が AWS Backupを使用して、多くのアカウントのバックアップにデータ保持ポリシーを広く適用する場合、そのリソースをそのバックアップポリシーの範囲内に配置するタグを適用できます。

タグポリシーは、組織全体で一貫したタグを維持するのに役立ちます。タグポリシーでは、リソースにタグが付けられたときに適用されるルールを指定します。例えば、 DataClassificationや などの特定のキーでリソースにタグを付けるように要求したりDataSteward、キーの有効な大文字と小文字の処理や値を指定したりできます。強制を使用して、非準拠のタグ付けリクエストが完了しないようにすることもできます。

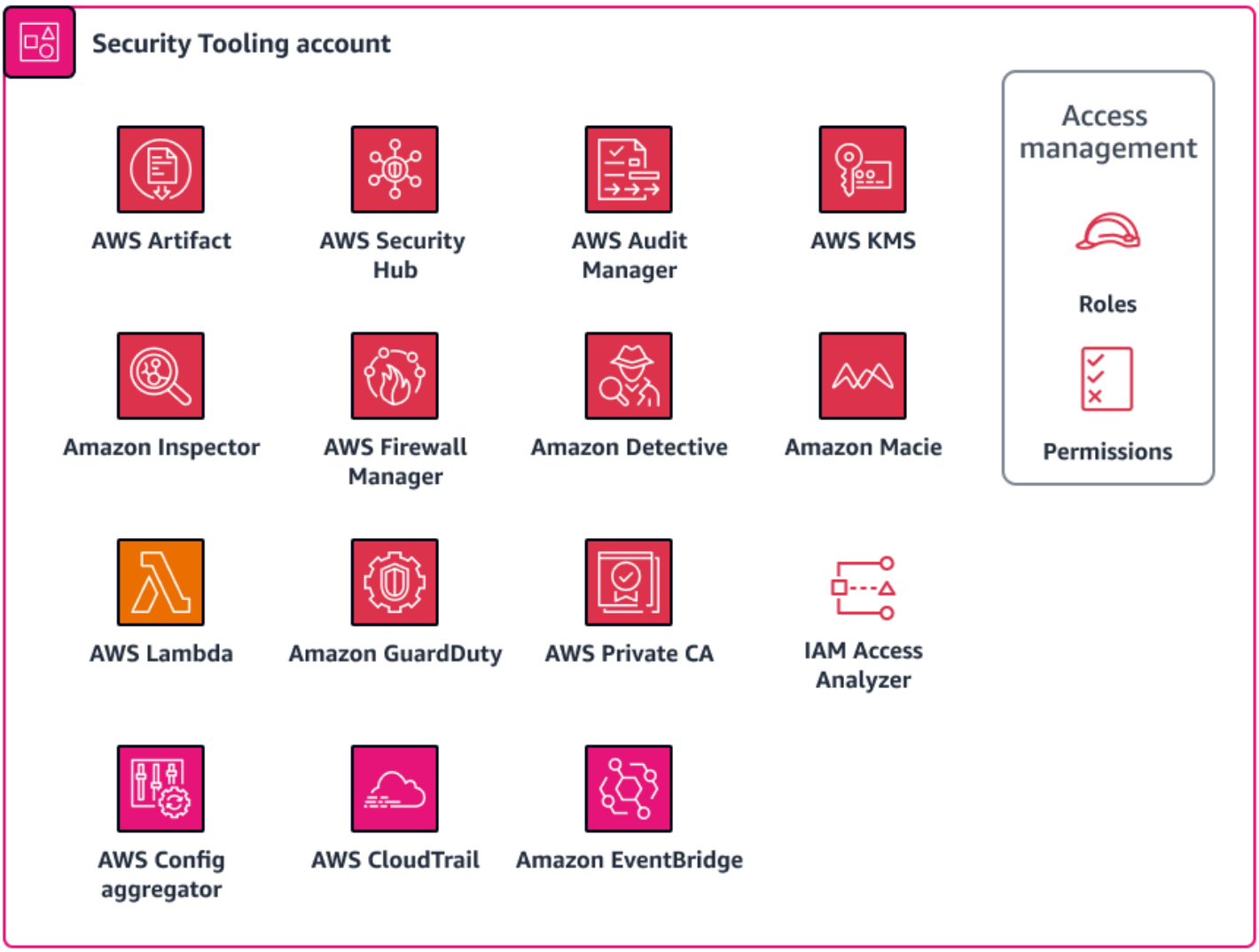
タグをプライバシーコントロール戦略のコアコンポーネントとして使用する場合は、次の点を考慮してください。

- 個人データやその他のタイプの機密データをタグキーまたは値に配置することによる影響を考慮してください。テクニカルサポート AWS が必要な場合は、 にお問い合わせいただき、タグやその他のリソース識別子 AWS を分析して問題の解決に役立ててください。この場合、タグ値を識別解除してから、IT サービス管理 (ITSM) システムなどのカスタマー管理システムを使用して再識別できます。 では、個人を特定できる情報をタグに含めない AWS ことをお勧めします。
- タグに依存する ABAC 条件など、技術的な制御の回避を防ぐために、一部のタグ値を不変 (変更不可) にする必要があることを考慮してください。

セキュリティ OU - Security Tooling アカウント

ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

Security Tooling アカウントは、セキュリティとプライバシーの基本サービスの運用、 のモニタリング AWS アカウント、セキュリティとプライバシーのアラートと対応の自動化に専念しています。このアカウントの詳細については、AWS 「セキュリティリファレンスアーキテクチャ (AWS SRA)」を参照してください。次の図は、 AWS Security Tooling アカウントで設定されているセキュリティおよびプライバシーサービスを示しています。



このセクションでは、このアカウントの以下に関する詳細情報を提供します。

- AWS CloudTrail
- AWS Config
- Amazon GuardDuty
- IAM Access Analyzer
- Amazon Macie

AWS CloudTrail

AWS CloudTrail は、 の全体的な API アクティビティを監査するのに役立ちます AWS アカウント。個人データを保存、処理、または送信 AWS リージョン するすべての AWS アカウント および

CloudTrail で を有効にすると、このデータの使用と開示を追跡するのに役立ちます。AWS セキュリティリファレンスアーキテクチャでは、組織の証跡を有効にすることをお勧めします。これは、組織内のすべてのアカウントのすべてのイベントを記録する単一の証跡です。ただし、この組織の証跡を有効にすると、マルチリージョンのログデータがログアーカイブアカウントの単一の Amazon Simple Storage Service (Amazon S3) バケットに集約されます。個人データを処理するアカウントの場合、設計上の考慮事項がいくつか追加される可能性があります。ログレコードには、個人データへの参照が含まれている場合があります。データの所在地とデータ転送要件を満たすには、S3 バケットがある 1 つのリージョンにクロスリージョンログデータを集約することを再検討する必要がある場合があります。組織は、組織の証跡に含める、または除外するリージョンのワークロードを検討できます。組織の証跡から除外するワークロードについては、個人データをマスクするリージョン固有の証跡を設定することを検討してください。個人データのマスキングの詳細については、このガイドのAmazon Data Firehose「」セクションを参照してください。最終的に、組織には、一元化されたログアーカイブアカウントに集約される組織の証跡とリージョンの証跡の組み合わせがある可能性があります。

単一リージョンの証跡の設定の詳細については、 AWS Command Line Interface （ AWS CLI ） またはコンソール を使用する手順を参照してください。組織の証跡を作成するときは、 でオプトイン設定を使用するかAWS Control Tower、CloudTrail コンソール で証跡を直接作成できます。

全体的なアプローチと、ログとデータ転送要件の一元化を管理する方法の詳細については、このガイドの一元化されたログストレージ「」セクションを参照してください。どの設定を選択しても、Security Tooling アカウントの証跡管理を AWS SRA に従ってログアーカイブアカウントのログストレージから分離できます。この設計により、ログを管理する必要があるユーザーとログデータを使用する必要があるユーザーに対して、最小特権のアクセスポリシーを作成できます。

AWS Config

AWS Config は、 内のリソース AWS アカウント とその設定方法の詳細ビューを提供します。これにより、リソースが互いにどのように関連し、時間の経過とともに設定がどのように変化したかを特定できます。このサービスがセキュリティコンテキストでどのように使用されるかの詳細については、AWS 「セキュリティリファレンスアーキテクチャ」を参照してください。

では AWS Config、 AWS Config ルールと修復アクションのセットであるコンフォーマンスパック をデプロイできます。コンフォーマンスパックは、 マネージドルールまたはカスタム AWS Config ルールを使用して、プライバシー、セキュリティ、運用、コスト最適化のガバナンスチェックを可能にするように設計された汎用フレームワークを提供します。このツールは、大規模な自動化ツールのセットの一部として使用して、 AWS リソース設定が独自のコントロールフレームワークの要件に準拠しているかどうかを追跡できます。

NIST プライバシーフレームワーク v1.0 コンフォーマンスパックの運用上のベストプラクティスは、NIST プライバシーフレームワークのプライバシー関連のさまざまなコントロールに整合しています。各 AWS Config ルールは特定の AWS リソースタイプに適用され、1 つ以上の NIST プライバシーフレームワークコントロールに関連付けられます。このコンフォーマンスパックを使用して、アカウントのリソース全体でプライバシー関連の継続的なコンプライアンスを追跡できます。このコンフォーマンスパックに含まれるルールの一部を次に示します。

- `no-unrestricted-route-to-igw` – このルールは、VPC ルートテーブルのデフォルトルート`0.0.0.0/0`またはインターネットゲートウェイへの`::/0`出力ルートを継続的にモニタリングすることで、データプレーン上のデータ流出を防ぐのに役立ちます。これにより、特に悪意のあることがわかっている CIDR 範囲がある場合に、インターネット宛てのトラフィックの送信先を制限できます。
- `encrypted-volumes` – このルールは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされている Amazon Elastic Block Store (Amazon EBS) ボリュームが暗号化されているかどうかを確認します。組織に、個人データを保護するための AWS Key Management Service （ AWS KMS) キーの使用に関する特定の制御要件がある場合は、ルールの一部として特定のキー IDs を指定して、ボリュームが特定の AWS KMS キーで暗号化されていることを確認することができます。
- `restricted-common-ports` – このルールは、Amazon EC2 セキュリティグループが指定されたポートへの無制限の TCP トラフィックを許可しているかどうかをチェックします。セキュリティグループは、 AWS リソースへの入出力ネットワークトラフィックをステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。から リソース上の TCP 3389 や TCP 21 などの共通ポート`0.0.0.0/0`への進入トラフィックをブロックすると、リモートアクセスを制限できます。

AWS Config は、 リソースの AWS プロアクティブコンプライアンスチェックとリアクティブコンプライアンスチェックの両方に使用できます。コンフォーマンスパックにあるルールを考慮するだけでなく、これらのルールを検出評価モードとプロアクティブ評価モードの両方に組み込むことができます。これにより、アプリケーションデベロッパーはデプロイ前チェックの組み込みを開始できるため、ソフトウェア開発ライフサイクルの早い段階でプライバシーチェックを実装できます。例えば、プロアクティブモードが有効になっているすべてのプライバシー関連の AWS Config ルールと照らし合わせて AWS CloudFormation 、テンプレート内の宣言されたリソースをチェックするフックをテンプレートに含めることができます。詳細については、AWS Config 「 Rules Now Support Proactive Compliance」（ AWS ブログ記事) を参照してください。

Amazon GuardDuty

AWS は、Amazon S3、Amazon Relational Database Service (Amazon RDS)、Kubernetes を使用した Amazon EC2 など、個人データの保存または処理に使用できる複数のサービスを提供します。Amazon EC2 Amazon GuardDuty は、インテリジェントな可視性と継続的なモニタリングを組み合わせて、個人データの意図しない開示に関連する可能性のある指標を検出します。このサービスがセキュリティコンテキストでどのように使用されるかの詳細については、AWS 「セキュリティリファレンスアーキテクチャ」を参照してください。

を使用すると GuardDuty、攻撃ライフサイクル全体で、悪意のある可能性のあるプライバシー関連のアクティビティを特定できます。例えば、 GuardDuty は、ブラックリストに登録されたサイトへの接続、異常なネットワークポートトラフィックまたはトラフィックボリューム、DNS の流出、予期しない EC2 インスタンスの起動、異常な ISP 発信者について警告できます。また、独自の信頼された IP リストからの信頼された IP アドレスのアラートを停止し、独自の脅威リストから既知の悪意のある IP アドレスをアラート GuardDuty するように を設定することもできます。

AWS SRA で推奨されているように、組織 AWS アカウント 内のすべての GuardDuty に対して を有効にし、Security Tooling アカウントを GuardDuty 委任管理者として設定できます。 GuardDuty は、組織全体の結果をこの 1 つのアカウントに集約します。詳細については、「 による GuardDuty アカウントの管理 AWS Organizations」を参照してください。また、検出と分析から封じ込めと根絶まで、インシデント対応プロセスにおけるプライバシー関連の利害関係者をすべて特定し、データの流出を伴う可能性のあるインシデントにそれらを含めることを検討することもできます。

IAM Access Analyzer

多くのお客様は、個人データが事前に承認され、意図されたサードパーティープロセッサと適切に共有され、他のエンティティと共有されていないという継続的な保証を望んでいます。データペリメーターは、予想されるネットワークからの信頼できる ID のみが環境内の信頼できるリソースにアクセスできるようにするように設計された予防ガードレールのセットです AWS 。個人データの意図しない意図された開示に対するコントロールを定義すると、信頼できる ID、信頼できるリソース、および期待されるネットワークを定義できます。

AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) を使用すると、組織は信頼 AWS アカウント ゾーンを定義し、その信頼ゾーンに対する違反のアラートを設定できます。IAM Access Analyzer は IAM ポリシーを分析し、機密性の高いリソースへの意図しないパブリックアクセスまたはクロスアカウントアクセスを特定して解決するのに役立ちます。IAM Access Analyzer は、数学ロジックと推論を使用して、 の外部からアクセスできるリソースの包括的な検出結果を生成します AWS アカウント。最後に、過度に制限された IAM ポリシーに応答して修正する

ために、IAM Access Analyzer を使用して IAM ベストプラクティスに照らして既存のポリシーを検証し、提案を提供できます。IAM Access Analyzer は、IAM プリンシパルの以前のアクセスアクティビティに基づく最小特権の IAM ポリシーを生成できます。 CloudTrail ログを分析し、それらのタスクを引き続き実行するために必要なアクセス許可のみを付与するポリシーを生成します。

セキュリティコンテキストでの IAM Access Analyzer の使用方法の詳細については、AWS 「セキュリティリファレンスアーキテクチャ」を参照してください。

Amazon Macie

Amazon Macie は、機械学習とパターンマッチングを使用して機密データを検出し、データセキュリティリスクを可視化し、それらのリスクに対する保護を自動化するのに役立つサービスです。Macie は、潜在的なポリシー違反や Amazon S3 バケットのセキュリティまたはプライバシーの問題を検出すると、検出結果を生成します。Macie は、組織がコンプライアンスの取り組みをサポートするために自動化を実装するために使用できるもう 1 つのツールです。このサービスがセキュリティコンテキストでどのように使用されるかの詳細については、AWS 「セキュリティリファレンスアーキテクチャ」を参照してください。

Macie は、名前、住所、その他の識別可能な属性など、個人を特定できる情報 (PII) を含む機密データタイプの大規模で増加しているリストを検出できます。組織による個人データの定義を反映する検出基準を定義するために、カスタムデータ識別子を作成することもできます。

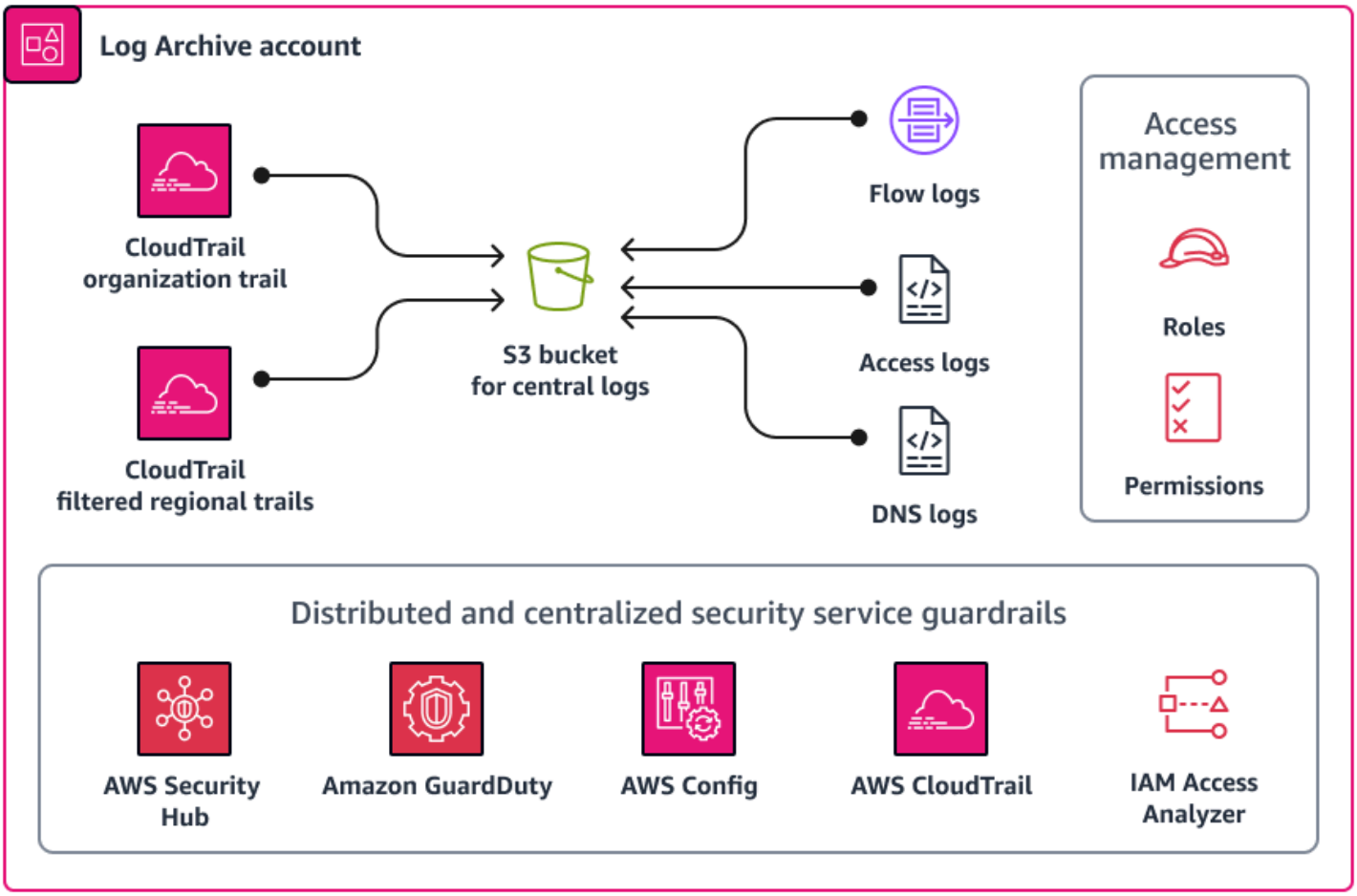
組織が個人データを含む Amazon S3 バケットの予防的コントロールを定義する際、Macie を検証メカニズムとして使用して、個人データの所在と保護方法を継続的に確認することができます。開始するには、Macie を有効にし、機密データ自動検出 を設定します。Macie は、アカウントと 全体で、すべての S3 バケット内のオブジェクトを継続的に分析します AWS リージョン。Macie は、個人データが存在する場所を示すインタラクティブなヒートマップを生成して維持します。機密データ自動検出機能は、コストを削減し、検出ジョブを手動で設定する必要性を最小限に抑えるように設計されています。自動機密データ検出機能に基づいて構築し、Macie を使用して既存のバケット内の新しいバケットまたは新しいデータを自動的に検出し、割り当てられたデータ分類タグに対してデータを検証できます。このアーキテクチャを設定して、誤って分類されたバケットや分類されていないバケットを適切な開発チームとプライバシーチームにタイムリーに通知します。

を使用して、組織内のすべてのアカウントで Macie を有効にできます AWS Organizations。詳細については、Amazon Macie での組織の統合と設定」を参照してください。

セキュリティ OU — ログアーカイブアカウント

ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

ログアーカイブアカウントは、インフラストラクチャ、サービス、アプリケーションのログタイプを一元化する場所です。このアカウントの詳細については、AWS 「セキュリティリファレンスアーキテクチャ (AWS SRA)」を参照してください。ログ専用のアカウントを使用すると、すべてのログタイプに一貫したアラートを適用し、インシデント応答者がこれらのログの集計に 1 か所からアクセスできることを確認できます。セキュリティコントロールとデータ保持ポリシーを 1 か所から設定することもできるため、プライバシー運用のオーバーヘッドが簡素化されます。次の図は、 AWS ログアーカイブアカウントで設定されているセキュリティおよびプライバシーサービスを示しています。



一元化されたログストレージ

ログファイル (AWS CloudTrail ログなど) には、個人データと見なされる可能性のある情報が含まれている場合があります。組織によっては、可視化の目的で、アカウント間 AWS リージョン およびアカウント間の CloudTrail ログを 1 つの一元的な場所に集約するために、組織の証跡を使用することを選択しています。詳細については、このガイドの「AWS CloudTrail」を参照してください。CloudTrail ログの一元化を実装する場合、通常、ログは 1 つのリージョンの Amazon Simple Storage Service (Amazon S3) バケットに保存されます。

組織における個人データの定義と適用される地域のプライバシー規制によっては、クロスボーダーデータ転送を検討する必要がある場合があります。組織が地域のプライバシー規制のデータ転送要件を満たす必要がある場合は、以下のオプションがサポートに役立ちます。

1. 組織が複数の国のデータ対象者 AWS クラウド に のサービスを提供している場合は、最も厳格なデータ所在地要件を持つ国のすべてのログを集約することを選択できます。例えば、ドイツで運用していて、最も厳しい要件がある場合は、 の S3 バケットにデータを集約`eu-central-1` AWS リージョン して、ドイツで収集されたデータがドイツの境界を離れないようにすることができます。このオプションでは、 で 1 つの組織の証跡を設定 CloudTrail して、すべてのアカウントからターゲットリージョン AWS リージョン にログを集約できます。
2. データを別のリージョンにコピーして集約 AWS リージョン する前に、 に残す必要がある個人データを編集します。例えば、ログを別のリージョンに転送する前に、アプリケーションのホストリージョンの個人データをマスクできます。個人データのマスキングの詳細については、このガイドのAmazon Data Firehose「」セクションを参照してください。

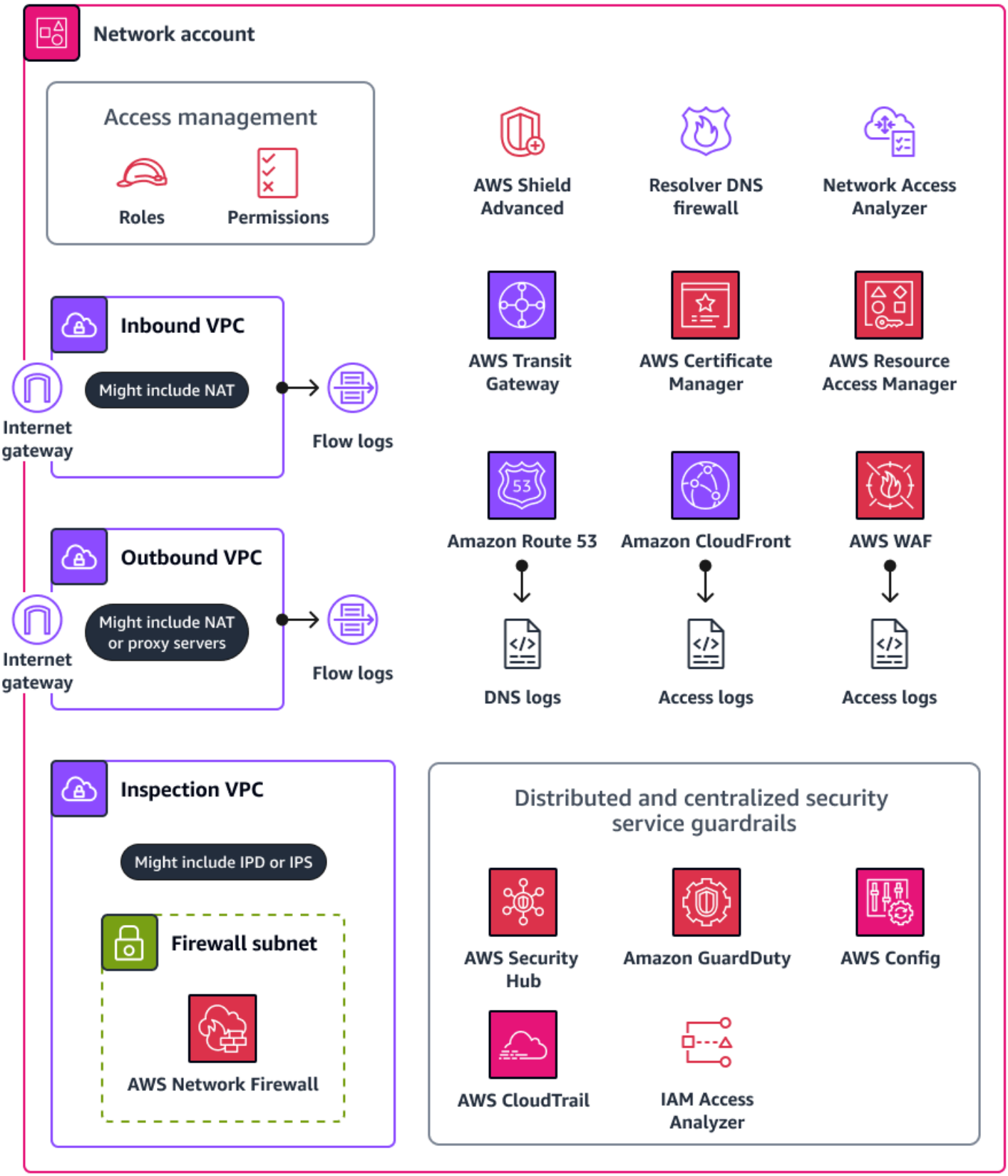
法律顧問と協力して、どの個人データが対象範囲にあり、どの AWS リージョン間転送が許可されるかを判断します。

インフラストラクチャ OU — ネットワークアカウント

ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

ネットワークアカウントでは、仮想プライベートクラウド (VPCsとより広範なインターネット間のネットワークを管理します。このアカウントでは、 を使用して広範な開示制御メカニズムを実装し AWS WAF、 AWS Resource Access Manager （ AWS RAM) を使用して VPC サブネットと AWS

Transit Gateway アタッチメントを共有し、Amazon CloudFront を使用してターゲットを絞ったサービスの使用をサポートできます。このアカウントの詳細については、AWS「セキュリティリファレンスアーキテクチャ (AWS SRA)」を参照してください。次の図は、ネットワークアカウントで設定されている AWS セキュリティおよびプライバシーサービスを示しています。


Network account
Access management
Roles
Permissions
AWS Shield Advanced
Resolver DNS firewall
Network Access Analyzer
Inbound VPC
Might include NAT
Internet gateway
Flow logs
AWS Transit Gateway
AWS Certificate Manager
AWS Resource Access Manager
Amazon Route 53
Amazon CloudFront
AWS WAF
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
DNS logs
Access logs
Access logs
Inspection VPC
Might include IPD or IPS
Firewall subnet
AWS Network Firewall
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer

このセクションでは、このアカウントで使用される以下 AWS のサービス に関する詳細情報を提供します。

- Amazon CloudFront
- 「AWS Resource Access Manager」
- AWS Transit Gateway
- AWS WAF

Amazon CloudFront

Amazon CloudFront は、フロントエンドアプリケーションとファイルホスティングの地理的制限をサポートしています。 CloudFront は、エッジロケーション と呼ばれるデータセンターのワールドワイドネットワークを通じてコンテンツを配信できます。ユーザーが で処理しているコンテンツをリクエストすると CloudFront、リクエストはレイテンシーが最も低いエッジロケーションにルーティングされます。このサービスがセキュリティコンテキストでどのように使用されるかの詳細については、AWS 「セキュリティリファレンスアーキテクチャ」を参照してください。

CloudFront 地理的制限を使用して、特定の地理的場所のユーザーがディストリビューションを通じて CloudFront配信するコンテンツにアクセスできないようにすることができます。地理的制限の詳細と設定オプションについては、 ドキュメントの「コンテンツの地理的分布の制限」を参照してください。 CloudFront

が CloudFront 受信するすべてのユーザーリクエストに関する詳細情報を含むアクセスログを生成する CloudFront ように を設定することもできます。詳細については、 CloudFront ドキュメントの「標準ログ (アクセスログ) の設定と使用」を参照してください。最後に、 CloudFront が一連のエッジロケーションでコンテンツをキャッシュするように設定されている場合、キャッシュが発生する場所を検討できます。一部の組織では、クロスリージョンキャッシュがクロスボーダーデータ転送要件の対象となる場合があります。

「AWS Resource Access Manager」

AWS Resource Access Manager (AWS RAM) は、 間でリソースを安全に共有 AWS アカウントして運用上のオーバーヘッドを削減し、可視性と監査性を提供するのに役立ちます。を使用すると AWS RAM、組織は組織 AWS アカウント 内の他の またはサードパーティアカウントと共有できる AWS リソースを制限できます。詳細については、「共有可能な AWS リソース」を参照してください。ネットワークアカウントでは、 AWS RAM を使用して VPC サブネットとトランジットゲートウェイ接続を共有できます。 AWS RAM を使用してデータプレーン接続を別の と共有する場合は

AWS アカウント、接続が事前承認された に対して行われたことを確認するプロセスを確立することを検討してください AWS リージョン。

VPCs とトランジットゲートウェイ接続の共有に加えて、 を使用して、IAM リソースベースのポリシーをサポートしていないリソースを共有 AWS RAM できます。個人データ OU でホストされているワークロードの場合、 AWS RAM を使用して、別の にある個人データにアクセスできます AWS アカウント。詳細については、AWS Resource Access Manager「Personal Data OU – PD Application account」セクションの「」を参照してください。

AWS Transit Gateway

組織のデータレジデンシー要件 AWS リージョン に沿った個人データを収集、保存、または処理する AWS リソースを にデプロイする場合、適切な技術的保護策がある場合は、コントロールプレーンとデータプレーンで未承認のクロスボーダーデータフローを防ぐためにガードレールを実装することを検討してください。コントロールプレーンでは、IAM およびサービスコントロールポリシーを使用して、リージョンの使用を制限し、その結果、リージョン間のデータフローを制限できます。

データプレーンでクロスリージョンデータフローを制御するには、複数のオプションがあります。例えば、ルートテーブル、VPC ピアリング、アタッチメント AWS Transit Gateway を使用できます。AWS Transit Gatewayは、仮想プライベートクラウド (VPCsとオンプレミスネットワークを接続する中央ハブです。大規模な AWS ランディングゾーンの一部として、データが を通過するさまざまな方法を検討できます。これには AWS リージョン、インターネットゲートウェイ、VPC 間の直接ピアリング、 とのリージョン間ピアリングが含まれます AWS Transit Gateway。例えば、 で以下を実行できます AWS Transit Gateway。

- VPCs とオンプレミス環境間の東西接続と南北接続がプライバシー要件と一致していることを確認します。
- プライバシー要件に従って VPC 設定を行います。
- AWS Organizations および IAM ポリシーでサービスコントロールポリシーを使用して、 AWS Transit Gateway および Amazon Virtual Private Cloud (Amazon VPC) の設定が変更されないようにします。サービスコントロールポリシーの例については、このガイドVPC 設定の変更を制限するの「」を参照してください。

AWS WAF

個人データの意図しない開示を防ぐために、ウェブアプリケーションに defense-in-depth アプローチをデプロイできます。アプリケーションに入力の検証とレート制限を構築できますが、別の防御

線として機能する AWS WAF ことができます。 AWS WAFは、保護されたウェブアプリケーションリソースに転送される HTTP および HTTPS リクエストをモニタリングするのに役立つウェブアプリケーションファイアウォールです。このサービスがセキュリティコンテキストでどのように使用されるかの詳細については、AWS 「セキュリティリファレンスアーキテクチャ」を参照してください。

では AWS WAF、特定の条件を検査するルールを定義してデプロイできます。以下のアクティビティは、個人データの意図しない開示に関連する可能性があります。

- 未知または悪意のある IP アドレスまたは地理的場所からのトラフィック
- Open Worldwide Application Security Project (OWASP) SQL インジェクションなどの流出関連の攻撃を含む、上位 10 件の攻撃
- リクエスト率が高い
- 一般的なボットトラフィック
- コンテンツスクレイパー

によって管理される AWS WAF ルールグループをデプロイできます AWS。のマネージドルールグループの中には、プライバシーや個人データに対する脅威を検出するために使用できるものがあります。例えば、次のとおり AWS WAF です。

- SQL データベース – このルールグループには、SQL インジェクション攻撃など、SQL データベースの悪用に関連するリクエストパターンをブロックするように設計されたルールが含まれています。アプリケーションが SQL データベースとインターフェイスする場合は、このルールグループを検討してください。
- 既知の不正な入力 – このルールグループには、無効であることがわかっており、脆弱性の悪用または検出に関連するリクエストパターンをブロックするように設計されたルールが含まれています。
- Bot Control – このルールグループには、過剰なリソースを消費し、ビジネスメトリクスを歪め、ダウンタイムを引き起こし、悪意のあるアクティビティを実行する可能性があるボットからのリクエストを管理するように設計されたルールが含まれています。
- アカウント乗っ取り防止 (ATP) – このルールグループには、悪意のあるアカウント乗っ取りの試みを防ぐように設計されたルールが含まれています。このルールグループは、アプリケーションのログインエンドポイントに送信されたログイン試行を検査します。

個人データ OU – PD アプリケーションアカウント

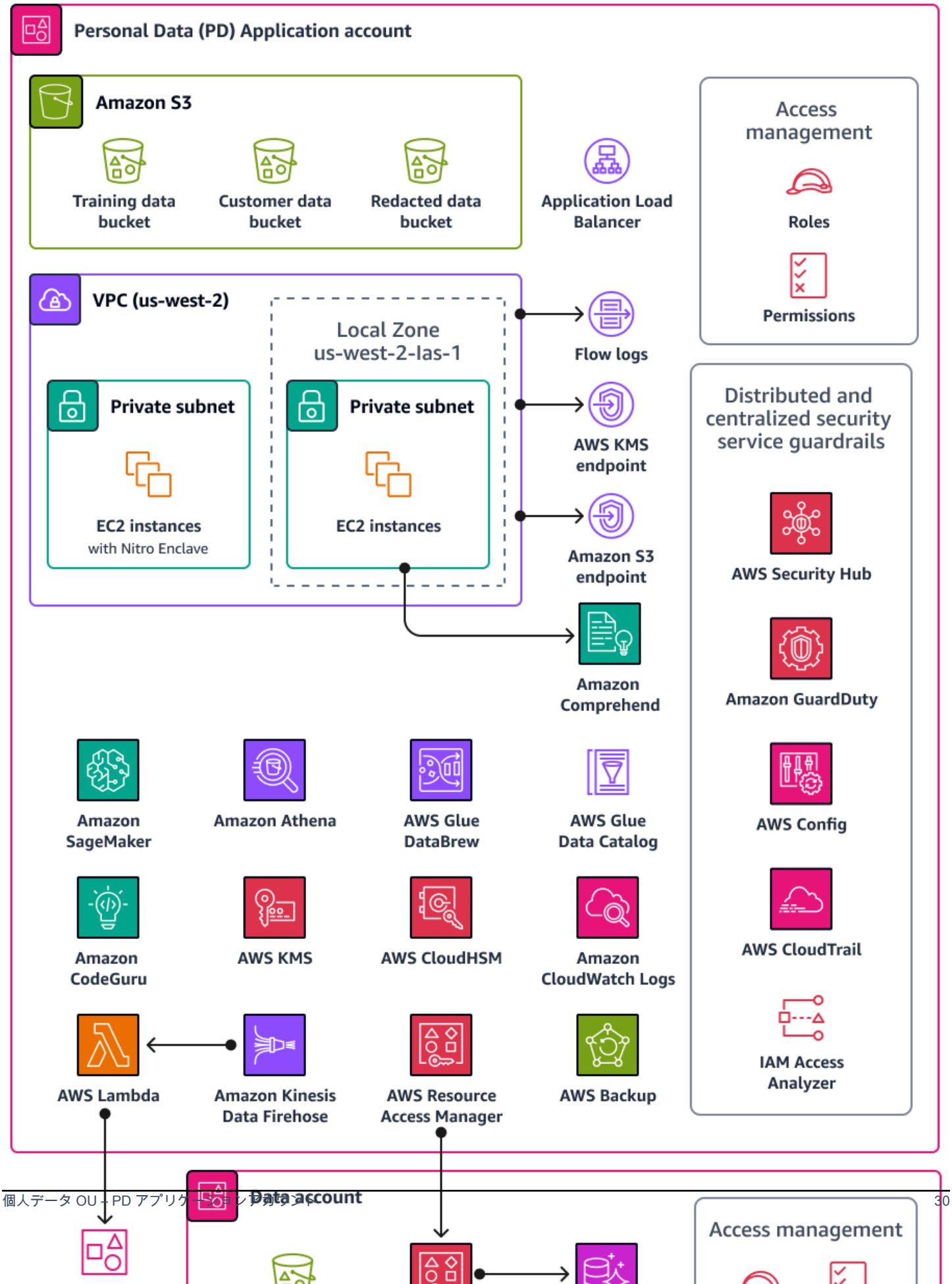
ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

個人データ (PD) アプリケーションアカウントは、組織が個人データを収集および処理するサービスをホストする場所です。具体的には、個人データとして定義したものをこのアカウントに保存できます。 AWS PRA は、多層サーバーレスウェブアーキテクチャによるプライバシー設定の例を多数示しています。 AWS ランディングゾーン全体でワークロードを運用する場合、プライバシー設定を one-size-fits-all ソリューションと見なすべきではありません。例えば、基礎となる概念、プライバシーを強化する方法、組織が特定のユースケースやアーキテクチャにソリューションをどのように適用できるかを理解することが目標かもしれません。

個人データを収集、保存、または処理する組織 AWS アカウント 内の では、 AWS Organizations とを使用して、基礎的で反復可能なガードレール AWS Control Tower をデプロイできます。これらのアカウント専用の組織単位 (OU) を確立することが重要です。例えば、データレジデンシーガードレールを、データレジデンシーが設計上の中核となるアカウントのサブセットにのみ適用できます。多くの組織では、これらは個人データを保存および処理するアカウントです。

組織は、個人用データセットの信頼できるソースを保存する専用のデータアカウントをサポートしている場合があります。信頼できるデータソースは、データのプライマリバージョンを保存する場所であり、データの最も信頼性が高く正確なバージョンと見なされる場合があります。例えば、信頼できるデータソースから、トレーニングデータ、顧客データのサブセット、秘匿化されたデータの保存に使用される PD アプリケーションアカウントの Amazon Simple Storage Service (Amazon S3) バケットなどの他の場所にデータをコピーできます。このマルチアカウントアプローチを使用して、データアカウントの完全かつ決定的な個人データセットを PD アプリケーションアカウントのダウンストリームコンシューマーワークロードから分離することで、アカウントへの不正アクセスが発生した場合の影響範囲を縮小できます。

次の図は、PD アプリケーションアカウントとデータアカウントで設定されている AWS セキュリティサービスとプライバシーサービスを示しています。


Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application Load Balancer
Access management
Roles
Permissions
VPC (us-west-2)
Local Zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Amazon Comprehend
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon SageMaker
Amazon Athena
AWS Glue DataBrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup
Log Archive
Data account
Access management

このセクションでは、これらのアカウントで使用される以下 AWS のサービス に関する詳細情報を提供します。

- Amazon Athena
- Amazon CloudWatch Logs
- Amazon CodeGuru Reviewer
- Amazon Comprehend
- Amazon Data Firehose
- AWS Glue
- AWS Key Management Service
- AWS ローカルゾーン
- AWS Nitro Enclaves
- AWS PrivateLink
- AWS Resource Access Manager
- Amazon SageMaker
- AWS データライフサイクルの管理に役立つ の機能
- データのセグメント化に役立つ AWS のサービスと機能

Amazon Athena

プライバシー目標を達成するために、データクエリの制限に関するコントロールを検討することもできます。Amazon Athena は、標準 SQL を使用して Amazon S3 でデータを直接分析するのに役立つ対話型のクエリサービスです。データを Athena にロードする必要はありません。S3 バケットに保存されているデータと直接連携します。

Athena の一般的なユースケースは、データ分析チームにカスタマイズされたサニタイズされたデータセットを提供することです。データセットに個人データが含まれている場合は、データ分析チームにとってほとんど価値のない個人データの列全体をマスクすることで、データセットをサニタイズできます。詳細については、Amazon Athena AWS Lake Formation「」 (AWS ブログ記事) を参照してください。

データ変換アプローチで、Athena でサポートされている関数の外部で追加の柔軟性が必要な場合は、ユーザー定義関数 (UDF) と呼ばれるカスタム関数を定義できます。Athena に送信された SQL クエリで UDFs を呼び出すことができ、 で実行されます AWS Lambda。UDF は SELECTおよび

FILTER SQLクエリで使用でき、同じクエリで複数の UDFsを呼び出すことができます。プライバシーのために、列内のすべての値の最後の 4 文字のみを表示するなど、特定のタイプのデータマスキングを実行する UDFs を作成できます。

Amazon CloudWatch Logs

Amazon CloudWatch Logs は、すべてのシステム、アプリケーション、および からのログを一元化するのに役立ちます。 AWS のサービス これにより、ログをモニタリングして安全にアーカイブできます。 CloudWatch ログでは、新規または既存のロググループにデータ保護ポリシーを使用して、個人データの開示リスクを最小限に抑えることができます。データ保護ポリシーは、ログ内の個人データなどの機密データを検出できます。データ保護ポリシーは、ユーザーが を介してログにアクセスするときに、そのデータをマスクできます AWS Management Console。ユーザーが個人データに直接アクセスする必要がある場合は、ワークロードの全体的な目的仕様に従って、それらのユーザーにlogs:Unmask許可を割り当てることができます。アカウント全体のデータ保護ポリシーを作成し、このポリシーを組織内のすべてのアカウントに一貫して適用することもできます。これにより、 CloudWatch ログの現在および将来のすべてのロググループに対してデフォルトでマスキングが設定されます。また、監査レポートを有効にして、別のロググループ、Amazon S3 バケット、または Amazon Data Firehose に送信することをお勧めします。これらのレポートには、各ロググループ全体のデータ保護結果の詳細な記録が含まれています。

Amazon CodeGuru Reviewer

プライバシーとセキュリティの両方において、多くの組織にとって、デプロイフェーズとデプロイ後のフェーズの両方で継続的なコンプライアンスをサポートすることが重要です。PRA AWS には、個人データを処理するアプリケーションのデプロイパイプラインにプロアクティブコントロールが含まれています。Amazon CodeGuru Reviewer は、Java の個人データ JavaScript、および Python コードが公開される可能性のある潜在的な欠陥を検出できます。コードの改善に関する提案をデベロッパーに提供します。 CodeGuru レビュー担当者は、さまざまなセキュリティ、プライバシー、一般的なベストプラクティスの欠陥を特定できます。詳細については、「Amazon CodeGuru Detector Library」を参照してください。、Bitbucket、 AWS CodeCommit、Amazon S3 など GitHub、複数のソースプロバイダーで動作するように設計されています。 CodeGuru Reviewer が検出できるプライバシー関連の欠陥には、次のようなものがあります。

- SQL インジェクション
- セキュリティで保護されていない Cookie
- 認証がありません
- クライアント側の AWS KMS 再暗号化

Amazon Comprehend

Amazon Comprehend は自然言語処理 (NLP) サービスで、機械学習を使用して英語のテキストドキュメントで貴重なインサイトと接続を明らかにします。Amazon Comprehend は、構造化、半構造化、または非構造化テキストドキュメント内の個人データを検出して編集できます。詳細については、Amazon Comprehend ドキュメントの「個人を特定できる情報 (PII)」を参照してください。Amazon Comprehend

AWS SDKs と Amazon Comprehend API を使用して、Amazon Comprehend を多くのアプリケーションと統合できます。例としては、Amazon Comprehend を使用してAmazon S3 Object Lambda で個人データを検出して編集します。組織は S3 Object Lambda を使用して Amazon S3 GET リクエストにカスタムコードを追加して、アプリケーションに返されるデータを変更および処理できます。S3 Object Lambda は、行のフィルタリング、イメージの動的なサイズ変更、個人データの編集などを行うことができます。 AWS Lambda 関数を搭載したコードは、 によって完全に管理されているインフラストラクチャで実行されるため AWS、データの派生コピーを作成および保存したり、プロキシを実行したりする必要がなくなります。S3 Object Lambda でオブジェクトを変換するためにアプリケーションを変更する必要はありません。で `ComprehendPiiRedactionS3Object` Lambda 関数を使用して、個人データ AWS Serverless Application Repository を編集できます。この関数は Amazon Comprehend を使用して個人データエンティティを検出し、それらをアスタリスクに置き換えて編集します。詳細については、Amazon S3 Amazon S3ドキュメントのS3 Object Lambda と Amazon Comprehend を使用した PII データの検出と編集」を参照してください。

Amazon Comprehend には AWS SDKs を介したアプリケーション統合のための多くのオプションがあるため、Amazon Comprehend を使用して、データを収集、保存、処理するさまざまな場所で個人データを識別できます。Amazon Comprehend ML 機能を使用して、アプリケーションログ (AWS ブログ記事) 、顧客 E メール、サポートチケットなどの個人データを検出および編集できます。PD アプリケーションアカウントのアーキテクチャ図は、Amazon EC2 のアプリケーションログに対してこの関数を実行する方法を示しています。Amazon Comprehend には 2 つの秘匿化モードがあります。

- `REPLACE_WITH_PII_ENTITY_TYPE` は、各 PII エンティティをそのタイプに置き換えます。例えば、Jane Doe は NAME に置き換えられます。
- `MASK` は、PII エンティティの文字を任意の文字 (!、#、$、%、&、@) に置き換えます。例えば、Jane Doe を **** *** に置き換えることができます。

Amazon Data Firehose

Amazon Data Firehose を使用して、ストリーミングデータをキャプチャ、変換し、Amazon Managed Service for Apache Flink や Amazon S3 などのダウンストリームサービスにロードできます。Firehose は、処理パイプラインをゼロから構築することなく、アプリケーションログなどの大量のストリーミングデータを転送するためによく使用されます。

Lambda 関数を使用して、データがダウンストリームに送信される前に、カスタマイズまたは組み込みの処理を実行できます。プライバシーのために、この機能はデータ最小化とクロスボーダーデータ転送の要件をサポートします。例えば、Lambda と Firehose を使用して、マルチリージョンのログデータをログアーカイブアカウントに一元化する前に変換できます。詳細については、「: Centralized Logging Solution for Multi Accounts」 (YouTube ビデオ) を参照してください。PD アプリケーションアカウントで、Amazon CloudWatch と を設定 AWS CloudTrail して、Firehose 配信ストリームにログをプッシュします。Lambda 関数はログを変換し、ログアーカイブアカウントの中央 S3 バケットに送信します。個人データを含む特定のフィールドをマスクするように Lambda 関数を設定できます。これにより、 間での個人データの転送を防ぐことができます AWS リージョン。このアプローチを使用すると、個人データは転送前と一元化前ではなく、その後にマスクされます。クロスボーダー転送要件の対象ではない管轄区域のアプリケーションでは、通常、 の組織証跡を通じてログを集約すると、運用効率とコスト効率が向上します CloudTrail。詳細については、このガイドAWS CloudTrailの Security OU – Security Tooling アカウントセクションの「」を参照してください。

AWS Glue

個人データを含むデータセットの維持は、Privacy by Design の重要なコンポーネントです。組織のデータは、構造化、半構造化、または非構造化の形式に存在する場合があります。構造のない個人用データセットでは、データ最小化、データセットリクエストの一部として単一のデータサブジェクトに起因するデータの追跡、一貫したデータ品質の確保、データセットの全体的なセグメンテーションなど、プライバシーを強化する多くのオペレーションの実行が困難になる可能性があります。AWS Glueはフルマネージド型の抽出、変換、ロード (ETL) サービスです。データストアとデータストリーム間のデータの分類、クリーニング、強化、移動に役立ちます。 AWS Glue 機能は、分析、機械学習、アプリケーション開発用のデータセットの検出、準備、構造化、結合に役立つように設計されています。 AWS Glue を使用して、既存のデータセット上に予測可能で共通の構造を作成できます。 AWS Glue Data Catalog、、および AWS Glue Data Quality は AWS Glue DataBrew、組織のプライバシー要件をサポートするのに役立つ AWS Glue 機能です。

AWS Glue Data Catalog

AWS Glue Data Catalog は、保守可能なデータセットを確立するのに役立ちます。Data Catalog には、 の抽出、変換、ロード (ETL) ジョブのソースおよびターゲットとして使用されるデータへの参照が含まれています AWS Glue。Data Catalog 内の情報はメタデータテーブルとして保存され、各テーブルは単一のデータストアを指定します。クローラーを実行して AWS Glue 、さまざまなデータストアタイプのデータをインベントリします。組み込み分類子とカスタム分類子をクローラーに追加し、これらの分類子は個人データのデータ形式とスキーマを推測します。次に、クローラーはメタデータをデータカタログに書き込みます。一元化されたメタデータテーブルを使用すると、 AWS 環境内のさまざまな個人データのソースに構造と予測可能性が追加されるため、データセットリクエスト (消去する権利など) への対応が容易になります。Data Catalog を使用してこれらのリクエストに自動的に応答する方法の包括的な例については、Amazon S3 Find and Forget によるデータレイク内のデータ消去リクエストの処理」(AWS ブログ記事) を参照してください。最後に、組織が AWS Lake Formationを使用してデータベース、テーブル、行、セル間できめ細かなアクセスを管理および提供している場合、Data Catalog は主要なコンポーネントです。Data Catalog はクロスアカウントデータ共有を提供し、タグベースのアクセスコントロールを使用してデータレイクを大規模に管理するのに役立ちます (AWS ブログ記事) 。

AWS Glue DataBrew

AWS Glue DataBrew は、データのクリーニングと正規化に役立ちます。また、個人を特定できる情報の削除やマスキング、データパイプライン内の機密データフィールドの暗号化など、データの変換を実行できます。また、データの系統を視覚的にマッピングして、データが通過したさまざまなデータソースと変換ステップを理解することもできます。この機能は、組織が個人データの出所をよりよく理解して追跡するためにますます重要になっています。データの準備中に個人データをマスクする DataBrew のに役立ちます。データプロファイリングジョブの一部として個人データを検出し、個人データや潜在的なカテゴリを含む可能性のある列の数などの統計を収集できます。その後、置換、ハッシュ、暗号化、復号化など、組み込みの元に戻す、または元に戻せないデータ変換手法を、コードを記述せずに使用できます。その後、クリーンアップされたデータセットとマスクされたデータセットをダウンストリームで分析、レポート、機械学習タスクに使用できます。で使用できるデータマスキング手法には、 DataBrew 次のようなものがあります。

- ハッシュ — ハッシュ関数を列の値に適用します。
- 置換 — 個人データを、他の信頼できる値に置き換えます。
- Nulling out or delete – 特定のフィールドを null 値に置き換えるか、列を削除します。
- マスキング — 文字スクラブを使用するか、列内の特定の部分をマスクします。

使用可能な暗号化手法は次のとおりです。

- 決定論的暗号化 — 決定論的暗号化アルゴリズムを列値に適用します。確定的暗号化では、値に対して常に同じ暗号文が生成されます。
- 確率的暗号化 — 確率的暗号化アルゴリズムを列値に適用します。確率的暗号化は、適用されるたびに異なる暗号文を生成します。

で提供される個人データ変換レシピの完全なリストについては DataBrew、「個人を特定できる情報 (PII) レシピステップ」を参照してください。

AWS Glue データ品質

AWS Glue Data Quality は、データパイプライン間で高品質のデータがデータコンシューマーに配信される前に、プロアクティブに配信を自動化および運用するのに役立ちます。 AWS Glue Data Quality は、データパイプライン全体のデータ品質問題の統計分析を提供し、Amazon でアラートをトリガー EventBridgeし、修復のための品質ルールのレコメンデーションを作成できます。 AWS Glue Data Quality は、ドメイン固有の言語でのルール作成もサポートしているため、カスタムデータ品質ルールを作成できます。

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、ハードウェアセキュリティモジュール AWS KMS を使用して、FIPS 140-2 暗号化モジュール検証プログラム AWS KMS keys で保護と検証を行います。このサービスがセキュリティコンテキストでどのように使用されるかの詳細については、AWS 「セキュリティリファレンスアーキテクチャ」を参照してください。

AWS KMS は、暗号化 AWS のサービス を提供するほとんどの と統合されており、個人データを処理して保存するアプリケーションで KMS キーを使用できます。 AWS KMS を使用して、次のようなさまざまなプライバシー要件をサポートし、個人データを保護することができます。

- カスタマーマネージドキーを使用して、強度、ローテーション、有効期限、その他のオプションをより細かく制御できます。
- 専用のカスタマーマネージドキーを使用して、個人データへのアクセスを許可する個人データとシークレットを保護します。
- データ分類レベルを定義し、レベルごとに少なくとも 1 つの専用カスタマーマネージドキーを指定します。例えば、運用データを暗号化するキーと、個人データを暗号化するキーがあります。
- KMS キーへの意図しないクロスアカウントアクセスの防止。
- 暗号化するリソース AWS アカウント と同じ 内に KMS キーを保存します。

- KMS キーの管理と使用の職務分離を実装します。詳細については、「KMS と IAM を使用して S3 の暗号化されたデータの独立したセキュリティコントロールを有効にする方法」(AWS ブログ記事) を参照してください。
- 予防的ガードレールと事後対応ガードレールによる自動キーローテーションの適用。

デフォルトでは、KMS キーは、作成されたリージョンでのみ保存され、使用できます。組織にデータ所在地と主権に関する特定の要件がある場合は、マルチリージョン KMS キーがユースケースに適しているかどうかを検討してください。マルチリージョンキーは、異なる の特殊用途の KMS キー AWS リージョン で、同じ意味で使用できます。マルチリージョンキーを作成するプロセスは、キーマテリアルを 内の AWS リージョン 境界を越えて移動するため AWS KMS、このリージョン分離の欠如は組織のコンプライアンス目標と互換性がない可能性があります。これを解決する 1 つの方法は、リージョン固有のカスタマーマネージドキーなど、別のタイプの KMS キーを使用することです。

AWS ローカルゾーン

データレジデンシー要件に準拠する必要がある場合は、これらの要件をサポートするために、特定の に個人データを保存および処理するリソース AWS リージョン をデプロイできます。AWS Local Zones を使用することもできます。これにより、コンピューティング、ストレージ、データベース、その他の一部の AWS リソースを大規模な人口や産業センターの近くに配置することができます。ローカルゾーンは、大都市圏に地理的に近い の拡張 AWS リージョン です。特定のタイプのリソースは、ローカルゾーンが対応するリージョンの近くにあるローカルゾーン内に配置できます。Local Zones は、同じ法的管轄区域内でリージョンが利用できない場合に、データレジデンシー要件を満たすのに役立ちます。ローカルゾーンを使用する場合は、組織内にデプロイされているデータレジデンシーコントロールを検討してください。例えば、特定のローカルゾーンから別のリージョンへのデータ転送を防ぐためのコントロールが必要になる場合があります。SCPs を使用してクロスボーダーデータ転送ガードレールを維持する方法の詳細については、「ランディングゾーンコントロールを使用して AWS ローカルゾーンのデータレジデンシーを管理するためのベストプラクティス」(AWS ブログ記事) を参照してください。

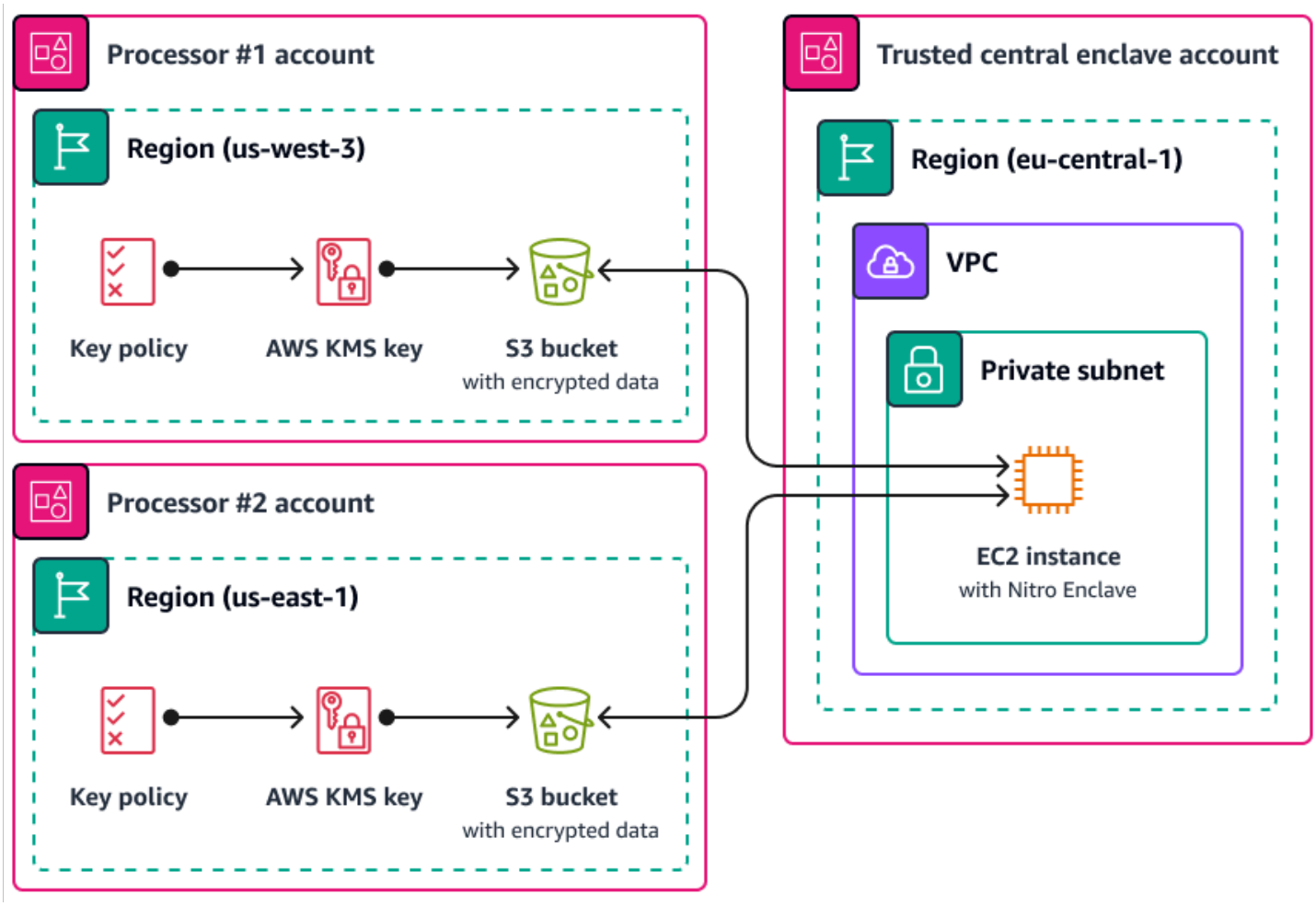
AWS Nitro Enclaves

Amazon Elastic Compute Cloud (Amazon EC2) などのコンピューティングサービスを使用して個人データを処理するなど、処理の観点からデータセグメンテーション戦略を検討します。大規模なアーキテクチャ戦略の一環としての機密コンピューティングは、分離され、保護され、信頼できる CPU エンクレーブで個人データ処理を分離するのに役立ちます。エンクレーブは、分離され、強化され、制約の厳しい仮想マシンです。AWS Nitro Enclaves は、これらの分離されたコンピューティング

環境の作成に役立つ Amazon EC2 機能です。詳細については、「The Security Design of the AWS Nitro System」(AWS ホワイトペーパー) を参照してください。

Nitro Enclaves は、親インスタンスのカーネルから分離されたカーネルをデプロイします。親インスタンスのカーネルはエンクレーブにアクセスできません。ユーザーは、エンクレーブ内のデータとアプリケーションに SSH またはリモートでアクセスすることはできません。個人データを処理するアプリケーションはエンクレーブに埋め込まれ、エンクレーブの Vsock を使用するように設定できます。これは、エンクレーブと親インスタンス間の通信を容易にするソケットです。

Nitro Enclaves が役立つユースケースの 1 つは、別々の 2 つのデータ処理装置間での共同処理 AWS リージョン であり、相互に信頼しない可能性があります。次の図は、中央処理にエンクレーブを使用する方法、エンクレーブに送信される前に個人データを暗号化するための KMS キー、および復号をリクエストするエンクレーブが認証ドキュメントで一意の測定値を持っていることを確認する AWS KMS key ポリシーを示しています。詳細と手順については、「 での暗号化認証の使用 AWS KMS」を参照してください。キーポリシーの例については、このガイドキーを使用するには AWS KMS 認証が必要ですの「」を参照してください。



この実装では、それぞれのデータ処理者と基盤となるエンクレーブのみがプレーンテキストの個人データにアクセスできます。データが公開される場所は、それぞれのデータ処理者の環境以外ではエンクレーブ自体であり、アクセスや改ざんを防ぐように設計されています。

AWS PrivateLink

多くの組織は、信頼できないネットワークへの個人データの漏洩を制限したいと考えています。例えば、アプリケーションアーキテクチャ設計全体のプライバシーを強化する場合、データの機密性に基づいてネットワークをセグメント化できます (データのセグメント化に役立つ AWS のサービスと機能セクションで説明されているデータセットの論理的および物理的な分離と同様) 。 AWS PrivateLink は、仮想プライベートクラウド (VPCs) から VPC 外のサービスへの単方向のプライベート接続を作成するのに役立ちます。を使用すると AWS PrivateLink、 環境で個人データを保存または処理するサービスへの専用プライベート接続を設定できます。パブリックエンドポイントに接続して、信頼できないパブリックネットワーク経由でこのデータを転送する必要はありません。対象範囲内 AWS PrivateLink のサービスのサービスエンドポイントを有効にすると、通信にインターネットゲートウェイ、NAT デバイス、パブリック IP アドレス、 AWS Direct Connect 接続、 AWS Site-to-Site VPN または接続は必要ありません。 AWS PrivateLink を使用して、個人データへのアクセスを提供するサービスに接続する場合、組織のデータ境界定義に従って、VPC エンドポイントポリシーとセキュリティグループを使用してアクセスを制御できます。信頼された組織の IAM 原則と AWS リソースのみがサービスエンドポイントにアクセスできるようにする VPC エンドポイントポリシーの例については、このガイド組織メンバーシップに VPC リソースへのアクセスを要求するの「」を参照してください。

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) は、 間で リソースを安全に共有 AWS アカウント して、運用上のオーバーヘッドを削減し、可視性と監査性を提供するのに役立ちます。マルチアカウントセグメンテーション戦略を計画する際は、 AWS RAM を使用して、分離された別のアカウントに保存されている個人データストアを共有することを検討してください。処理の目的で、その個人データを他の信頼できるアカウントと共有できます。では AWS RAM、共有リソースに対して実行できるアクションを定義するアクセス許可を管理できます。へのすべての API コール AWS RAM は に記録されます CloudTrail。また、リソース共有に変更が加えられたときなど AWS RAM、 の特定のイベントについて自動的に通知するように Amazon CloudWatch Events を設定できます。

Amazon S3 の IAM またはバケットポリシーでリソースベースのポリシー AWS アカウント を使用することで、他の と多くのタイプの AWS リソースを共有できますが、 AWS RAM にはプライバシーに関するいくつかの追加の利点があります。 AWS は AWS アカウント、データ所有者が 間でデータを共有する方法とユーザーについて、さらに可視化します。

- アカウント IDs のリストを手動で更新するのではなく、OU 全体とリソースを共有できる
- コンシューマーアカウントが組織の一部でない場合の共有開始の招待プロセスの実施
- 特定の IAM プリンシパルが個々のリソースにアクセスできる可視性

以前にリソースベースのポリシーを使用してリソース共有を管理し、 AWS RAM 代わりに を使用する場合は、 PromoteResourceShareCreatedFromPolicy API オペレーションを使用します。

Amazon SageMaker

Amazon SageMaker は、ML モデルを構築してトレーニングし、本番環境に対応したホスト環境にデプロイするのに役立つマネージド機械学習 (ML) サービスです。 SageMaker は、トレーニングデータの準備とモデル機能の作成を容易にするように設計されています。

Amazon SageMaker Model Monitor

多くの組織は、ML モデルのトレーニング時にデータドリフトを考慮しています。データドリフトは、本番データと ML モデルのトレーニングに使用されたデータとの間の意味のある変化、または入力データの時間の経過に伴う意味のある変化です。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。ML モデルが本番環境で受け取るデータの統計的な性質が、トレーニングされたベースラインデータの性質からずれると、予測の精度が低下する可能性があります。Amazon SageMaker Model Monitor は、本番環境の Amazon SageMaker 機械学習モデルの品質を継続的にモニタリングし、データ品質をモニタリングできます。データドリフトを早期かつプロアクティブに検出することで、モデルの再トレーニング、アップストリームシステムの監査、データ品質の問題の修正などの是正措置を実装できます。Model Monitor を使用すると、モデルを手動でモニタリングしたり、追加のツールを構築したりする必要性を軽減できます。

Amazon SageMaker Clarify

Amazon SageMaker Clarify は、モデルのバイアスと説明可能性に関するインサイトを提供します。 SageMaker Clarify は、ML モデルデータの準備中および全体的な開発段階で一般的に使用されます。開発者は性別や年齢などの関心のある属性を指定でき、 SageMaker Clarify は一連のアルゴリズムを実行して、それらの属性にバイアスが存在することを検出します。アルゴリズムが実行されると、 SageMaker Clarify は、バイアスを修復するステップを特定できるように、ソースの説明と可能性のあるバイアスの測定値を含むビジュアルレポートを提供します。例えば、ある年齢グループに対するビジネスローンの例が他の年齢グループと比較してごくわずかしか含まれていない財務データセットでは、不均衡にフラグを SageMaker 立てて、その年齢グループを嫌うモデルを回避できます。また、予測を確認し、それらの機械学習モデルにバイアスがないか継続的にモニタリング

することで、トレーニング済みのモデルにバイアスがないかを確認することもできます。最後に、SageMakerClarify は Amazon SageMaker Experiments と統合され、モデルの全体的な予測プロセスに最も寄与した特徴量を説明するグラフを提供します。この情報は、説明可能性の結果を達成するのに役立ち、特定のモデル入力がモデルの動作全体に与えるべきよりも大きな影響を与えるかどうかを判断するのに役立ちます。

Amazon SageMaker モデルカード

Amazon SageMaker Model Card は、ガバナンスとレポート作成の目的で ML モデルに関する重要な詳細を文書化するのに役立ちます。これらの詳細には、モデル所有者、汎用、意図したユースケース、行われた仮定、モデルのリスク評価、トレーニングの詳細とメトリクス、評価結果が含まれます。詳細については、AWS 「人工知能とMachine Learningソリューションによるモデルの説明可能性」(AWS ホワイトペーパー) を参照してください。

AWS データライフサイクルの管理に役立つ の機能

個人データが不要になった場合は、さまざまなデータストアのデータにライフサイクルと time-to-liveポリシーを使用できます。データ保持ポリシーを設定するときは、個人データが含まれる可能性のある以下の場所を考慮してください。

- Amazon DynamoDB や Amazon Relational Database Service (Amazon RDS) などのデータベース
- Amazon S3 バケット
- CloudWatch および からの口グ CloudTrail
- AWS Database Migration Service (AWS DMS) および AWS Glue DataBrew プロジェクトの移行からのキャッシュデータ
- バックアップとスナップショット

以下の AWS のサービス および 機能は、 AWS 環境でのデータ保持ポリシーの設定に役立ちます。

- Amazon S3 ライフサイクル – Amazon S3 がオブジェクトのグループに適用するアクションを定義する一連のルール。Amazon S3 ライフサイクル設定では、Amazon S3 がユーザーに代わって期限切れのオブジェクトを削除するタイミングを定義する有効期限アクションを作成できます。詳細については、「Managing your storage lifecycle」を参照してください。
- Amazon Data Lifecycle Manager – Amazon EC2 で、Amazon Elastic Block Store (Amazon EBS) スナップショットと EBS-backed Amazon マシンイメージ (AMIs) の作成、保持、削除を自動化するポリシーを作成します。

- DynamoDB Time to Live (TTL) – 項目ごとのタイムスタンプを定義して、項目が不要になったタイミングを決定します。指定されたタイムスタンプの日時の直後に、DynamoDB はテーブルから項目を削除します。
- ログの CloudWatch ログ保持設定 – 各ロググループの保持ポリシーを 1 日から 10 年の値に調整できます。
- AWS Backup – データ保護ポリシーを一元的にデプロイして、S3 バケット、RDS データベースインスタンス、DynamoDB テーブル、EBS ボリュームなど、さまざまな AWS リソースでバックアップアクティビティを設定、管理、管理します。 AWS リソースタイプを指定してバックアップポリシーをリソースに適用するか、既存のリソースタグに基づいて を適用して追加の詳細度を提供します。一元化されたコンソールからバックアップアクティビティを監査してレポートし、バックアップコンプライアンス要件を満たすのに役立ちます。

データのセグメント化に役立つ AWS のサービスと機能

データセグメンテーションは、データを別々のコンテナに保存するためのプロセスです。これにより、各データセットに差別化されたセキュリティと認証の対策を提供し、データセット全体の露出の影響範囲を減らすことができます。例えば、すべての顧客データを 1 つの大規模なデータベースに保存する代わりに、このデータをより小さく管理しやすいグループにセグメント化できます。

物理的および論理的な分離を使用して、個人データをセグメント化できます。

- 物理的な分離 — データを別々のデータストアに保存したり、データを別々の AWS リソースに分散したりする行為。データは物理的に分離されていますが、両方のリソースに同じプリンシパルがアクセスできる可能性があります。そのため、物理的な分離と論理的な分離を組み合わせることをお勧めします。
- 論理的な分離 — アクセスコントロールを使用してデータを分離する行為。職務機能ごとに、個人データのサブセットへのアクセスレベルが異なります。論理的な分離を実装するサンプルポリシーについては、このガイド特定の Amazon DynamoDB 属性へのアクセスを許可するの「」を参照してください。

論理的な分離と物理的な分離を組み合わせることで、アイデンティティベースとリソースベースのポリシーを記述する際に柔軟性、シンプルさ、粒度を提供し、職務機能間の差別化されたアクセスをサポートします。例えば、1 つの S3 バケットで異なるデータ分類を論理的に分離するポリシーを作成するのは、運用上複雑な場合があります。各データ分類に専用の S3 バケットを使用すると、ポリシーの設定と管理が簡単になります。

プライバシー関連のポリシーの例

ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

機密データを処理する多くの組織では、検出コントロールと事後対応型コントロールのレイヤーが全体に実装され、予防的なアプローチを採用しています。このセクションでは、 AWS Identity and Access Management (IAM)、 () のプライバシー関連のポリシーの例を示します AWS Organizations AWS Key Management Service AWS KMS。これらのポリシーは、予防的アプローチを使用することで、組織がさまざまな使用、開示の制限、およびクロスボーダーデータ転送のプライバシー目標を達成するために役立ちます。これらのポリシーの多くは、このガイドの前のセクションで参照されています。

このセクションには、以下のサンプルポリシーが含まれています。

- 特定の IP アドレスからのアクセスを要求する
- 組織メンバーシップに VPC リソースへのアクセスを要求する
- 間でのデータ転送を制限する AWS リージョン
- 特定の Amazon DynamoDB 属性へのアクセスを許可する
- VPC 設定の変更を制限する
- キーを使用するには AWS KMS 認証が必要です

特定の IP アドレスからのアクセスを要求する

ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

このポリシーでは、通話が 192.0.2.0/24または の範囲内の IP アドレスから発信されている場合にのみ、john_stilesIAM ロールを引き受けることができます203.0.113.0/24。このポリシーは、個人データの意図しない開示や不要なクロスボーダーデータ転送を防ぐのに役立ちます。例えば、組織に個人データへのアクセスを必要とするカスタマーサポートスタッフがある場合は、そのサポートスタッフに特定の のサブセットにあるオフィスからのみそのデータにアクセスさせたい場合があります AWS リージョン。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:user/john_stiles"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:user/john_stiles"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24",
            "203.0.113.0/24"
          ]
        }
      }
    }
  ]
}
```

組織メンバーシップに VPC リソースへのアクセスを要求する

ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

この VPC エンドポイントポリシーは、o-1abcde123組織の AWS Identity and Access Management (IAM) プリンシパルとリソースのみが Amazon Personalize (Amazon S3) エンドポイントにアクセスすることを許可します。この予防的コントロールは、信頼ゾーンを確立し、個人データの境界を定義するのに役立ちます。このポリシーが組織内のプライバシーと個人データを保護する方法の詳細については、このガイドAWS PrivateLinkの「」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyIntendedResourcesAndPrincipals",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-1abcde123",
                    "aws:ResourceOrgID": "o-1abcde123"
                }
            }
        }
    ]
}
```

間でのデータ転送を制限する AWS リージョン

ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

2 つの AWS Identity and Access Management (IAM) ロールを除いて、このサービスコントロールポリシーは、 eu-west-1と AWS リージョン 以外の のリージョン AWS のサービス への API コールを拒否しますeu-central-1。この SCP は、未承認のリージョンでの AWS ストレージおよび処理サービスの作成を防ぐのに役立ちます。これにより、これらのリージョン AWS のサービス で が個人データを完全に処理するのを防ぐことができます。このポリシーは、IAM などのグローバル AWS サービス、および AWS Key Management Service （ AWS KMS) や Amazon などのグローバルサービスと統合されるサービスを考慮するため、 NotActionパラメータを使用します CloudFront。パラメータ値では、これらのグローバルサービスやその他の適用できないサービスを例外として指定できます。このポリシーが組織内のプライバシーと個人データを保護する方法の詳細については、このガイドAWS Organizationsの「」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "chime:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
                "mobileanalytics:*",
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints",
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
                "support:*",
                "trustedadvisor:*",
                "waf-regional:*",
                "waf:*",
```

```
                "wafv2:*",
                "wellarchitected:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

特定の Amazon DynamoDB 属性へのアクセスを許可する

ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

組織が個人データを物理的および論理的に分離する戦略について議論するときは、 AWS Identity and Access Management (IAM) できめ細かなアクセスコントロールポリシーをサポートする AWS ストレージサービスを検討してください。次のアイデンティティベースのポリシーでは`UserID`、、`SignUpTime`、および 属性のみを という名前の Amazon DynamoDB テーブル`LastLoggedIn`から取得できます`Users`。例えば、このロールに完全な個人用データセットへのアクセスを許可する代わりに、このポリシーをカスタマーサポートロールにアタッチできます。このポリシーが組織内のプライバシーと個人データを保護する方法の詳細については、このガイドデータのセグメント化に役立つ AWS のサービスと機能の「」を参照してください。

```
{
   "Version":"2012-10-17",
   "Statement":[
```

```
      {
         "Effect":"Allow",
         "Action":[
            "dynamodb:GetItem",
            "dynamodb:BatchGetItem",
            "dynamodb:Query",
            "dynamodb:Scan",
            "dynamodb:TransactGetItems"
         ],
         "Resource":[
            "arn:aws:dynamodb:us-west-2:123456789012:dynamodb:table/Users"
         ],
         "Condition":{
            "ForAllValues:StringEquals":{
               "dynamodb:Attributes":[
                  "UserID",
                  "SignUpTime",
                  "LastLoggedIn"
               ]
            },
            "StringEquals":{
               "dynanamodb:Select":[
                  "SPECIFIC_ATTRIBUTES"
               ]
            }
         }
      }
   ]
}
```

VPC 設定の変更を制限する

ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

ネットワークデータフローを含むクロスボーダーデータ転送要件をサポートする AWS インフラストラクチャを設計してデプロイしたら、変更を防ぐことができます。次のサービスコントロールポリシーは、VPC 設定のドリフトや意図しない変更を防ぐのに役立ちます。新しいインターネットゲートウェイアタッチメント、VPC ピアリング接続、トランジットゲートウェイアタッチメント、およ

び新しい VPN 接続を拒否します。このポリシーが組織内のプライバシーと個人データを保護する方法の詳細については、このガイドAWS Transit Gatewayの「」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachInternetGateway",
                "ec2:CreateInternetGateway",
                "ec2:AttachEgressOnlyInternetGateway",
                "ec2:CreateVpcPeeringConnection",
                "ec2:AcceptVpcPeeringConnection",
                "ec2:CreateVpc",
                "ec2:CreateSubnet",
                "ec2:CreateRouteTable",
                "ec2:CreateRoute",
                "ec2:AssociateRouteTable",
                "ec2:ModifyVpcAttribute",
                "ec2:*TransitGateway",
                "ec2:*TransitGateway*",
                "globalaccelerator:Create*",
                "globalaccelerator:Update*"

            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

キーを使用するには AWS KMS 認証が必要です

ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

次の AWS Key Management Service （ AWS KMS) キーポリシーは、リクエスト内のエンクレーブのアテステーションドキュメントが条件ステートメントの測定値と一致する場合にのみ、 AWS Nitro Enclave インスタンスが KMS キーを使用することを許可します。このポリシーでは、信頼できるエンクレーブのみがデータを復号できます。このポリシーが組織内のプライバシーと個人データを保護する方法の詳細については、このガイドAWS Nitro Enclavesの「」を参照してください。キーポリシーおよび AWS Identity and Access Management (IAM) ポリシーで使用できる条件キーの完全なリスト AWS KMS については、「 の条件キー AWS KMS」を参照してください。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Enable enclave data processing",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:role/data-processing"
         },
         "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey",
            "kms:GenerateRandom"
         ],
         "Resource": "*",
         "Condition": {
            "StringEqualsIgnoreCase": {
               "kms:RecipientAttestation:ImageSha384":
"EXAMPLE8abcdef7abcdef6abcdef5abcdef4abcdef3abcdef2abcdef1abcdef1abcdef0abcdef1abcdEXAMPLE",
               "kms:RecipientAttestation:PCR0":
"EXAMPLEbc2ecbb68ed99a13d7122abfc0666b926a79d5379bc58b9445c84217f59cfdd36c08b2c79552928702EXAM
               "kms:RecipientAttestation:PCR1":
"EXAMPLE050abf6b993c915505f3220e2d82b51aff830ad14cbecc2eec1bf0b4ae749d311c663f464cde9f718aEXAM
               "kms:RecipientAttestation:PCR2":
"EXAMPLEc300289e872e6ac4d19b0b5ac4a9b020c98295643ff3978610750ce6a86f7edff24e3c0a4a445f2ff8EXAM
               "kms:RecipientAttestation:PCR3":
"EXAMPLE11de9baee597508183477f097ae385d4a2c885aa655432365b53b812694e230bbe8e1bb1b8de748fe1EXAM
```

```
                "kms:RecipientAttestation:PCR4":
 "EXAMPLE6b9b3d89a53b13f5dfd14a1049ec0b80a9ae4b159adde479e9f7f512f33e835a0b9023ca51ada02160EXAM
                "kms:RecipientAttestation:PCR8":
 "EXAMPLE34a884328944cd806127c7784677ab60a154249fd21546a217299ccfa1ebfe4fa96a163bf41d3bcfaeEXAM
            }
         }
      }
   ]
}
```

リソース

ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

AWS 規範ガイダンス

- AWS セキュリティリファレンスアーキテクチャ (AWS SRA)

AWS ドキュメント

- データ保護 (AWS Well-Architected Framework)
- データ分類 (AWS ホワイトペーパー)
- アマゾン ウェブ サービス: リスクとコンプライアンス (AWS ホワイトペーパー)
- 個人データ処理要件に対応するハイブリッドアーキテクチャ (AWS ホワイトペーパー)
- での GDPR コンプライアンスのナビゲート AWS (AWS ホワイトペーパー)
- でのデータ境界の構築 AWS (AWS ホワイトペーパー)
- AWS セキュリティドキュメント

その他の AWS リソース

- AWS コンプライアンスプログラム
- AWS 責任共有モデル
- データプライバシーに関するよくある質問
- AWS セキュリティ保証サービス
- AWS デジタル主権の約束: 侵害のない制御 (ブログ記事) AWS
- AWS セキュリティ学習

寄稿者

ご意見をお寄せください。簡単なアンケートに回答して、 AWS PRA に関するフィードバックを提供してください。

このガイドは Security AWS Assurance Services チームによって作成されました。このガイドの推奨事項の実装とワークロードの運用については、AWS セキュリティ保証サービスチームにお問い合わせください。

主要著者

- Daniel Nieters、 AWS プリンシパルプライバシーコンサルタント
- Amber Welch、 AWS 上級プライバシーコンサルタント
- ロバート・カーター、 AWS テクニカルプログラムマネージャー

寄稿者

- Avik Mukherjee、 AWS 上級セキュリティコンサルタント
- David Bounds、 AWS シニアソリューションアーキテクト
- Jeff Lombardo、 AWS シニアセキュリティソリューションアーキテクト
- Ram Ramani、 AWS プリンシパルセキュリティソリューションアーキテクト
- Vanessa Jacobs、 AWS シニアセキュリティコンサルタント

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
署名付き更新	全体で大幅な更新を行いました。	2024 年 3 月 26 日
初版発行	—	2023 年 10 月 2 日

AWS 規範的ガイダンスの用語集

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

数字

7 Rs

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

- リファクタリング/アーキテクチャの再設計 — クラウドネイティブ特徴を最大限に活用して、俊敏性、パフォーマンス、スケーラビリティを向上させ、アプリケーションを移動させ、アーキテクチャを変更します。これには、通常、オペレーティングシステムとデータベースの移植が含まれます。例: オンプレミスの Oracle データベースを Amazon Aurora PostgreSQL 互換エディションに移行します。
- リプラットフォーム (リフトアンドリシェイプ) – アプリケーションをクラウドに移行し、クラウド機能を活用するためにある程度の最適化を導入します。例: オンプレミスの Oracle データベースを の Oracle 用 Amazon Relational Database Service (Amazon RDS) に移行します AWS クラウド。
- 再購入 (ドロップアンドショップ) — 通常、従来のライセンスから SaaS モデルに移行して、別の製品に切り替えます。例: 顧客関係管理 (CRM) システムを Salesforce.com に移行します。
- リホスト (リフトアンドシフト) — クラウド機能を活用するための変更を加えずに、アプリケーションをクラウドに移行します。例: オンプレミスの Oracle データベースを の EC2 インスタンス上の Oracle に移行します AWS クラウド。
- 再配置 (ハイパーバイザーレベルのリフトアンドシフト) – 新しいハードウェアを購入したり、アプリケーションを書き換えたり、既存の運用を変更したりすることなく、インフラストラクチャをクラウドに移行できます。サーバーをオンプレミスプラットフォームから同じプラットフォームのクラウドサービスに移行します。例: の移行 Microsoft Hyper-V アプリケーション AWS。
- 保持 (再アクセス) — アプリケーションをお客様のソース環境で保持します。これには、主要なリファクタリングを必要とするアプリケーションや、お客様がその作業を後日まで延期したいアプリケーション、およびそれらを移行するためのビジネス上の正当性がないため、お客様が保持するレガシーアプリケーションなどがあります。
- 使用停止 — お客様のソース環境で不要になったアプリケーションを停止または削除します。

A

ABAC

「属性ベースのアクセスコントロール」を参照してください。

抽象化されたサービス

「 マネージドサービス」を参照してください。

ACID

原子性、一貫性、分離性、耐久性を参照してください。

アクティブ - アクティブ移行

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

アクティブ - パッシブ移行

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

集計関数

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

AI

人工知能を参照してください。

AIOps

「人工知能オペレーション」を参照してください。

匿名化

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

アンチパターン

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

アプリケーションコントロール

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

アプリケーションポートフォリオ

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

人工知能 (AI)

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

人工知能オペレーション (AIOps)

機械学習技術を使用して運用上の問題を解決し、運用上のインシデントと人の介入を減らし、サービス品質を向上させるプロセス。AIOps が移行戦略で AWS どのように使用されるかの詳細については、「 オペレーション統合ガイド」を参照してください。

非対称暗号化

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

アトミック性、一貫性、分離性、耐久性 (ACID)

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

属性ベースのアクセスコントロール (ABAC)

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

信頼できるデータソース

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

アベイラビリティーゾーン

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

AWS クラウド導入フレームワーク (AWS CAF)

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

AWS ワークロード認定フレームワーク (AWS WQF)

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

B

不正なボット

個人または組織に混乱や損害を与えることを目的としたボット。

BCP

事業継続計画を参照してください。

動作グラフ

リソースの動作とインタラクションを経時的に示した、一元的なインタラクティブビュー。Amazon Detective で動作グラフを使用して、失敗したログオン試行、不審な API 呼び出し、および同様のアクションを調べることができます。詳細については、Detective ドキュメントのData in a behavior graphを参照してください。

ビッグエンディアンシステム

最上位バイトを最初に格納するシステム。エンディアンネスも参照してください。

二項分類

バイナリ結果 (2 つの可能なクラスのうちの 1 つ) を予測するプロセス。例えば、お客様の機械学習モデルで「この E メールはスパムですか、それともスパムではありませんか」などの問題を予測する必要があるかもしれません。または「この製品は書籍ですか、車ですか」などの問題を予測する必要があるかもしれません。

ブルームフィルター

要素がセットのメンバーであるかどうかをテストするために使用される、確率的でメモリ効率の高いデータ構造。

ブルー/グリーンデプロイ

2 つの異なる同一の環境を作成するデプロイ戦略。現在のアプリケーションバージョンを 1 つの環境 (ブルー) で実行し、新しいアプリケーションバージョンを他の環境 (グリーン) で実行します。この戦略は、影響を最小限に抑えながら迅速にロールバックするのに役立ちます。

ボット

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

ボットネット

マルウェアに感染し、ボットのヘルダーまたはボットオペレーターとして知られる 1 人の当事者による管理下にあるボットのネットワーク。ボットは、ボットとその影響をスケールするための最もよく知られているメカニズムです。

ブランチ

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

ブレークグラスアクセス

例外的な状況では、承認されたプロセスを通じて、ユーザーが AWS アカウント 通常アクセス許可を持たない にすばやくアクセスできるようになります。詳細については、 Well-Architected ガイダンスの「ブレークグラス手順の実装」インジケータ AWS を参照してください。

ブラウンフィールド戦略

環境の既存インフラストラクチャ。システムアーキテクチャにブラウンフィールド戦略を導入する場合、現在のシステムとインフラストラクチャの制約に基づいてアーキテクチャを設計します。既存のインフラストラクチャを拡張している場合は、ブラウンフィールド戦略とグリーンフィールド戦略を融合させることもできます。

バッファキャッシュ

アクセス頻度が最も高いデータが保存されるメモリ領域。

ビジネス能力

価値を生み出すためにビジネスが行うこと (営業、カスタマーサービス、マーケティングなど)。マイクロサービスのアーキテクチャと開発の決定は、ビジネス能力によって推進できます。詳細については、ホワイトペーパー AWSでのコンテナ化されたマイクロサービスの実行 の ビジネス機能を中心に組織化 セクションを参照してください。

事業継続計画 (BCP)

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

C

CAF

AWS 「クラウド導入フレームワーク」を参照してください。

Canary デプロイ

エンドユーザーへのバージョンの低速かつ段階的なリリース。自信が持てたら、新しいバージョンをデプロイし、現在のバージョン全体を置き換えます。

CCoE

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

CDC

「データキャプチャの変更」を参照してください。

データキャプチャの変更 (CDC)

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

カオスエンジニアリング

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

CI/CD

継続的インテグレーションと継続的デリバリーを参照してください。

分類

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

クライアント側の暗号化

ターゲットがデータ AWS のサービス を受信する前に、ローカルでデータを暗号化します。

Cloud Center of Excellence (CCoE)

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

クラウドコンピューティング

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

クラウド運用モデル

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

導入のクラウドステージ

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

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

これらのステージは、 AWS クラウド エンタープライズ戦略ブログのブログ記事「クラウドファーストへのジャーニー」と「導入のステージ」で Stephen Orban によって定義されました。これらが AWS 移行戦略とどのように関連しているかについては、「移行準備ガイド」を参照してください。

CMDB

「設定管理データベース」を参照してください。

コードリポジトリ

ソースコードやその他の資産 (ドキュメント、サンプル、スクリプトなど) が保存され、バージョン管理プロセスを通じて更新される場所。一般的なクラウドリポジトリには、次のようなものがあります。GitHub または Bitbucket Cloud。 コードの各バージョンはブランチと呼ばれます。マイクロサービスの構造では、各リポジトリは 1 つの機能専用です。1 つの CI/CD パイプラインで複数のリポジトリを使用できます。

コールドキャッシュ

空である、または、かなり空きがある、もしくは、古いデータや無関係なデータが含まれているバッファキャッシュ。データベースインスタンスはメインメモリまたはディスクから読み取る必

要があり、バッファキャッシュから読み取るよりも時間がかかるため、パフォーマンスに影響します。

コールドデータ

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

コンピュータビジョン (CV)

機械学習を使用してデジタルイメージや動画などのビジュアル形式から情報を分析および抽出する AI の分野。例えば、 はオンプレミスのカメラネットワークに CV を追加するデバイス AWS Panorama を提供し、Amazon SageMaker は CV の画像処理アルゴリズムを提供します。

設定ドリフト

ワークロードの場合、設定は想定状態から変化します。これにより、ワークロードが非準拠になる可能性があり、通常は段階的かつ意図的ではありません。

設定管理データベース (CMDB)

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

コンフォーマンスパック

コンプライアンスチェックとセキュリティチェックをカスタマイズするためにアセンブルできる AWS Config ルールと修復アクションのコレクション。YAML テンプレートを使用して、コンフォーマンスパックを AWS アカウント とリージョン、または組織全体に 1 つのエンティティとしてデプロイできます。詳細については、 AWS Config ドキュメントの「コンフォーマンスパック」を参照してください。

継続的インテグレーションと継続的デリバリー (CI/CD)

ソフトウェアリリースプロセスのソース、ビルド、テスト、ステージング、本番の各ステージを自動化するプロセス。CI/CD is commonly described as a pipeline. CI/CD は、プロセスの自動化、生産性の向上、コード品質の向上、より迅速な提供に役立ちます。詳細については、「継続的デリバリーの利点」を参照してください。CD は継続的デプロイ (Continuous Deployment) の略語でもあります。詳細については「継続的デリバリーと継続的なデプロイ」を参照してください。

CV

「コンピュータビジョン」を参照してください。

D

保管中のデータ

ストレージ内にあるデータなど、常に自社のネットワーク内にあるデータ。

データ分類

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

データドリフト

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

転送中のデータ

ネットワーク内 (ネットワークリソース間など) を活発に移動するデータ。

データメッシュ

一元的な管理とガバナンスにより、分散型の分散データ所有権を提供するアーキテクチャフレームワーク。

データ最小化

厳密に必要なデータのみを収集し、処理するという原則。でデータ最小化を実践 AWS クラウドすることで、プライバシーリスク、コスト、分析のカーボンフットプリントを削減できます。

データ境界

AWS 環境内の一連の予防ガードレール。信頼できる ID のみが、期待されるネットワークから信頼できるリソースにアクセスしていることを確実にします。詳細については、「 でのデータ境界の構築 AWS」を参照してください。

データの前処理

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

データ出所

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

データ件名

データを収集、処理している個人。

データウェアハウス

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

データベース定義言語 (DDL)

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

データベース操作言語 (DML)

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

DDL

「データベース定義言語」を参照してください。

ディープアンサンブル

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

ディープラーニング

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

defense-in-depth

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

ティの手法。この戦略を採用するときは AWS、 AWS Organizations 構造の異なるレイヤーに複数のコントロールを追加して、リソースの安全性を確保します。例えば、a defense-in-depth アプローチでは、多要素認証、ネットワークセグメンテーション、暗号化を組み合わせることができます。

委任管理者

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

デプロイメント

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

開発環境

「環境」を参照してください。

検出管理

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

開発値ストリームマッピング (DVSM)

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

デジタルツイン

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

ディメンションテーブル

スタースキーマでは、ファクトテーブル内の量的データに関するデータ属性を含む小さなテーブル。ディメンションテーブル属性は通常、テキストフィールドまたはテキストのように動作する

離散数値です。これらの属性は、クエリの制約、フィルタリング、結果セットのラベル付けによく使用されます。

ディザスタ

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

ディザスタリカバリ (DR)

災害によるダウンタイムとデータ損失を最小限に抑えるために使用する戦略とプロセス。詳細については、 AWS Well-Architected フレームワークの「 でのワークロードのディザスタリカバリ AWS: クラウドでのリカバリ」を参照してください。

DML

「データベース操作言語」を参照してください。

ドメイン駆動型設計

各コンポーネントが提供している変化を続けるドメイン、またはコアビジネス目標にコンポーネントを接続して、複雑なソフトウェアシステムを開発するアプローチ。この概念は、エリック・ エヴァンスの著書、Domain-Driven Design: Tackling Complexity in the Heart of Software (ドメイン駆動設計:ソフトウェアの中心における複雑さへの取り組み) で紹介されています (ボストン: Addison-Wesley Professional、2003)。strangler fig パターンでドメイン駆動型設計を使用する方法については、「コンテナと Amazon Word API Gateway を使用してレガシー Microsoft ASP.NET (ASMX) ウェブサービスを段階的にモダナイズする」を参照してください。

DR

「ディザスタリカバリ」を参照してください。

ドリフト検出

ベースライン設定からの逸脱の追跡。例えば、 AWS CloudFormation を使用してシステムリソースのドリフトを検出したり、 を使用して AWS Control Tower ガバナンス要件のコンプライアンスに影響を与える可能性のあるランディングゾーンの変更を検出したりできます。

DVSM

「開発値ストリームマッピング」を参照してください。

E

EDA

「探索的データ分析」を参照してください。

EDI

「電子データ交換」を参照してください。

エッジコンピューティング

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

電子データ交換 (EDI)

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

暗号化

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

暗号化キー

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

エンディアン

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

エンドポイント

「 サービスエンドポイント」を参照してください。

エンドポイントサービス

Virtual Private Cloud (VPC) でホストして他のユーザーと共有できるサービス。を使用してエンドポイントサービスを作成し AWS PrivateLink 、他の AWS アカウント または AWS Identity and

Access Management （ IAM) プリンシパルにアクセス許可を付与できます。これらのアカウントまたはプリンシパルは、インターフェイス VPC エンドポイントを作成することで、エンドポイントサービスにプライベートに接続できます。詳細については、Amazon Virtual Private Cloud (Amazon Word) ドキュメントの「エンドポイントサービスの作成」を参照してください。 VPC

エンタープライズリソースプランニング (ERP)

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

エンベロープ暗号化

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

環境

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

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

エピック

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

ERP

「エンタープライズリソース計画」を参照してください。

探索的データ分析 (EDA)

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

F

ファクトテーブル

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

フェイルファスト

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

障害分離の境界

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

機能ブランチ

「ブランチ」を参照してください。

特徴量

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

特徴量重要度

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

機能変換

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

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

数ショットプロンプト

同様のタスクを実行するように求める前に、タスクと必要な出力を示す少数の例を LLM に提供します。この手法は、プロンプトに埋め込まれた例 (ショット) からモデルが学習するコンテキスト内学習のアプリケーションです。少数ショットプロンプトは、特定のフォーマット、推論、またはドメイン知識を必要とするタスクに効果的です。ゼロショットプロンプトも参照してください。

FGAC

「きめ細かなアクセスコントロール」を参照してください。

きめ細かなアクセスコントロール (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

フラッシュカット移行

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

FM

「基盤モデル」を参照してください。

基盤モデル (FM)

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

G

生成 AI

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

ジオブロッキング

地理的制限を参照してください。

地理的制限 (ジオブロッキング)

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

Gitflow ワークフロー

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

ゴールデンイメージ

システムまたはソフトウェアの新しいインスタンスをデプロイするためのテンプレートとして使用されるシステムまたはソフトウェアのスナップショット。例えば、製造では、ゴールデンイメージを使用して複数のデバイスにソフトウェアをプロビジョニングし、デバイスの製造オペレーションの速度、スケーラビリティ、生産性を向上させることができます。

グリーンフィールド戦略

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

ガードレール

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

H

HA

高可用性を参照してください。

異種混在データベースの移行

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

ハイアベイラビリティ (HA)

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

ヒストリアンのモダナイゼーション

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

ホールドアウトデータ

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

同種データベースの移行

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

ホットデータ

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

ホットフィックス

本番環境の重大な問題を修正するために緊急で配布されるプログラム。緊急性のため、通常、ホットフィックスは一般的な DevOps リリースワークフローの外部で行われます。

ハイパーケア期間

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

I

IaC

Infrastructure as Code を参照してください。

ID ベースのポリシー

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

アイドル状態のアプリケーション

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

IIoT

「産業モノのインターネット」を参照してください。

イミュータブルインフラストラクチャ

既存のインフラストラクチャを更新、パッチ適用、または変更するのではなく、本番環境のワークロードに新しいインフラストラクチャをデプロイするモデル。イミュータブルなインフラストラクチャは、本質的にミュータブルなインフラストラクチャよりも一貫性、信頼性、予測性が高くなります。詳細については、 AWS 「 Well-Architected フレームワーク」の「イミュータブルインフラストラクチャを使用したデプロイ」のベストプラクティスを参照してください。

インバウンド (イングレス) VPC

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

は、アプリケーションとより広範なインターネット間の双方向インターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションVPCsを使用してネットワークアカウントを設定することをお勧めします。

増分移行

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

インダストリー 4.0

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

インフラストラクチャ

アプリケーションの環境に含まれるすべてのリソースとアセット。

Infrastructure as Code (IaC)

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

産業モノのインターネット (IIoT)

製造、エネルギー、自動車、ヘルスケア、ライフサイエンス、農業などの産業部門におけるインターネットに接続されたセンサーやデバイスの使用。詳細については、「産業モノのインターネット (IIoT) デジタルトランスフォーメーション戦略の構築」を参照してください。

検査VPC

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

IoT

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

解釈可能性

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

IoT

「モノのインターネット」を参照してください。

IT 情報ライブラリ (ITIL)

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

IT サービス管理 (ITSM)

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

ITIL

「IT 情報ライブラリ」を参照してください。

ITSM

「IT サービス管理」を参照してください。

L

ラベルベースのアクセスコントロール (LBAC)

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

ランディングゾーン

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

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

大規模言語モデル (LLM)

大量のデータに基づいて事前トレーニングされた深層学習 AI モデル。LLM は、質問への回答、ドキュメントの要約、テキストの他の言語への翻訳、文の完了など、複数のタスクを実行できます。詳細については、LLMs とは」を参照してください。

大規模な移行

300 台以上のサーバの移行。

LBAC

「ラベルベースのアクセスコントロール」を参照してください。

最小特権

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

リフトアンドシフト

「7 R」を参照してください。

リトルエンディアンシステム

最下位バイトを最初に格納するシステム。エンディアンネスも参照してください。

LLM

「大規模言語モデル」を参照してください。

下位環境

「環境」を参照してください。

M

機械学習 (ML)

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

メインブランチ

「ブランチ」を参照してください。

マルウェア

コンピュータのセキュリティまたはプライバシーを侵害するように設計されているソフトウェア。マルウェアは、コンピュータシステムの中断、機密情報の漏洩、不正アクセスにつながる可能性があります。マルウェアの例としては、ウイルス、ワーム、ランサムウェア、トロイの木馬、スパイウェア、キーロガーなどがあります。

マネージドサービス

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

製造実行システム (MES)

生産プロセスを追跡、モニタリング、文書化、制御するためのソフトウェアシステム。これにより、生産現場の生産物が完成した製品に変換されます。

MAP

「移行促進プログラム」を参照してください。

メカニズム

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

メンバーアカウント

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

MES

「製造実行システム」を参照してください。

メッセージキューイングテレメトリトランスポート (MQTT)

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

マイクロサービス

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

マイクロサービスアーキテクチャ

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

Migration Acceleration Program (MAP)

コンサルティングサポート、トレーニング、サービスを提供する AWS プログラム。組織がクラウドへの移行のための強固な運用基盤を構築し、移行の初期コストを相殺するのに役立ちます。MAP には、従来の移行を体系的に実行するための移行方法論と、一般的な移行シナリオを自動化および高速化するための一連のツールが含まれています。

大規模な移行

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

移行ファクトリー

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

移行メタデータ

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

移行パターン

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

移行ポートフォリオ評価 (MPA)

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

移行準備状況評価 (MRA)

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

移行戦略

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

ML

???「機械学習」を参照してください。

モダナイゼーション

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

モダナイゼーション準備状況評価

組織のアプリケーションのモダナイゼーションの準備状況を判断し、利点、リスク、依存関係を特定し、組織がこれらのアプリケーションの将来の状態をどの程度適切にサポートできるかを決定するのに役立つ評価。評価の結果として、ターゲットアーキテクチャのブループリント、モダナイゼーションプロセスの開発段階とマイルストーンを詳述したロードマップ、特定されたギャップに対処するためのアクションプランが得られます。詳細については、「」の「アプリケーションのモダナイゼーション準備状況の評価 AWS クラウド」を参照してください。

モノリシックアプリケーション (モノリス)

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

MPA

「移行ポートフォリオ評価」を参照してください。

MQTT

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

多クラス分類

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

ミュータブルインフラストラクチャ

本番ワークロードの既存のインフラストラクチャを更新および変更するモデル。Well-Architected AWS フレームワークでは、一貫性、信頼性、予測可能性を向上させるために、イミュータブルインフラストラクチャをベストプラクティスとして使用することを推奨しています。

O

OAC

「オリジンアクセスコントロール」を参照してください。

OAI

「オリジンアクセスアイデンティティ」を参照してください。

OCM

「組織の変更管理」を参照してください。

オフライン移行

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

OI

「 オペレーションの統合」を参照してください。

OLA

「運用レベルの契約」を参照してください。

オンライン移行

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

OPC UA

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

オープンプロセス通信 - 統合アーキテクチャ (OPC-UA)

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

運用レベルの契約 (OLA)

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

運用準備状況レビュー (ORR)

インシデントや潜在的な障害の理解、評価、防止、または範囲の縮小に役立つ質問のチェックリストと関連するベストプラクティス。詳細については、 AWS Well-Architected フレームワークの「運用準備状況レビュー (ORR)」を参照してください。

運用テクノロジー (OT)

物理環境と連携して産業運用、機器、インフラストラクチャを制御するハードウェアおよびソフトウェアシステム。製造では、OT と情報技術 (IT) システムの統合が、Industry 4.0 トランスフォーメーションの主要な焦点です。

オペレーション統合 (OI)

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

組織の証跡

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

組織変更管理 (OCM)

人材、文化、リーダーシップの観点から、主要な破壊的なビジネス変革を管理するためのフレームワーク。OCM は、変化の採用を加速し、移行に伴う問題に対処し、文化や組織の変化を推進することで、組織が新しいシステムや戦略に備え、移行するのに役立ちます。 AWS 移行戦略では、クラウド導入プロジェクトに必要な変化のスピードから、このフレームワークは人材アクセラレーションと呼ばれます。詳細については、 OCM ガイドを参照してください。

オリジンアクセスコントロール (OAC)

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

オリジンアクセスアイデンティティ (OAI)

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

ORR

「運用準備状況レビュー」を参照してください。

OT

「運用技術」を参照してください。

アウトバウンド (出力) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーション内から開始されたネットワーク接続を処理する VPC。AWS セキュリティリファレンスアーキテクチャでは、アプリケーションとより広範なインターネット間の双方向インターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションVPCsを使用してネットワークアカウントを設定することをお勧めします。

P

アクセス許可の境界

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

個人を特定できる情報 (PII)

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

PII

個人を特定できる情報を参照してください。

プレイブック

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

PLC

「プログラム可能なロジックコントローラー」を参照してください。

PLM

「製品ライフサイクル管理」を参照してください。

ポリシー

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

多言語の永続性

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

ポートフォリオ評価

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

述語

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

述語プッシュダウン

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

予防的コントロール

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

プリンシパル

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

プライバシーバイデザイン

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

プライベートホストゾーン

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

プロアクティブコントロール

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

製品ライフサイクル管理 (PLM)

設計、開発、発売、成長と成熟、辞退と削除まで、ライフサイクル全体にわたる製品のデータとプロセスの管理。

本番環境

「環境」を参照してください。

プログラム可能なロジックコントローラー (PLC)

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

プロンプトの連鎖

1 つの LLM プロンプトの出力を次のプロンプトの入力として使用して、より良いレスポンスを生成します。この手法は、複雑なタスクをサブタスクに分割したり、事前対応を繰り返し調整または拡張したりするために使用されます。これにより、モデルのレスポンスの精度と関連性が向上し、より詳細でパーソナライズされた結果が得られます。

仮名化

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

publish/subscribe (pub/sub)

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

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

Q

クエリプラン

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

クエリプランのリグレッション

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

R

RACIマトリックス

「責任者」、「説明責任者」、「相談先」、「通知先」 (RACI) を参照してください。

RAG

「取得拡張生成」を参照してください。

ランサムウェア

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

RASCIマトリックス

「責任者」、「説明責任者」、「相談先」、「通知先」 (RACI) を参照してください。

RCAC

「行と列のアクセスコントロール」を参照してください。

リードレプリカ

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

再設計

「7 R」を参照してください。

目標復旧時点 (RPO)

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

目標復旧時間 (RTO)

サービスの中断から復旧までの最大許容遅延時間。

リファクタリング

「7 R」を参照してください。

リージョン

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

回帰

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

リホスト

「7 R」を参照してください。

リリース

デプロイプロセスで、変更を本番環境に昇格させること。

再配置

「7 R」を参照してください。

プラットフォーム変更

「7 R」を参照してください。

再購入

「7 R」を参照してください。

回復性

中断に耐えたり、中断から回復したりするアプリケーションの機能。で障害耐性を計画する場合、高可用性とディザスタリカバリがよく考慮されます AWS クラウド。詳細については、AWS クラウド「レジリエンス」を参照してください。

リソースベースのポリシー

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

責任、説明責任、相談、情報提供 (RACI) マトリックス

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

レスポンシブコントロール

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

保持

「7 R」を参照してください。

廃止

「7 R」を参照してください。

取得拡張生成 (RAG)

レスポンスを生成する前に、LLM がトレーニングデータソースの外部にある信頼できるデータソースを参照する生成 AI テクノロジー。例えば、RAG モデルは組織のナレッジベースやカスタムデータのセマンティック検索を実行する場合があります。詳細については、RAG とは」を参照してください。

ローテーション

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

行と列のアクセスコントロール (RCAC)

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

RPO

「目標復旧時点」を参照してください。

RTO

目標復旧時間を参照してください。

ランブック

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

S

SAML 2.0

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

SCADA

「監視コントロールとデータ収集」を参照してください。

SCP

「サービスコントロールポリシー」を参照してください。

シークレット

暗号化された形式で保存する AWS Secrets Managerパスワードやユーザー認証情報などの機密情報または制限付き情報。シークレット値とそのメタデータで構成されます。シークレット値は、バイナリ、単一の文字列、または複数の文字列にすることができます。詳細については、Secrets Manager ドキュメントの「Secrets Manager シークレットの内容」を参照してください。

設計によるセキュリティ

開発プロセス全体を通じてセキュリティを考慮したシステムエンジニアリングアプローチ。

セキュリティコントロール

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

セキュリティ強化

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

セキュリティ情報とイベント管理 (SIEM) システム

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

セキュリティレスポンスの自動化

セキュリティイベントに自動的に対応または修正するように設計された、事前定義されプログラムされたアクション。これらの自動化は、セキュリティのベストプラクティスの実装に役立つ検出的または応答的な AWS セキュリティコントロールとして機能します。自動応答アクションの例としては、VPC セキュリティグループの変更、Amazon EC2 インスタンスへのパッチ適用、認証情報のローテーションなどがあります。

サーバー側の暗号化

送信先にあるデータの、それ AWS のサービス を受け取る による暗号化。

サービスコントロールポリシー (SCP)

AWS Organizationsの組織内の、すべてのアカウントのアクセス許可を一元的に管理するポリシー。SCPsは、管理者がユーザーまたはロールに委任できるアクションのガードレールを定義するか、制限を設定します。SCPs を許可リストまたは拒否リストとして使用して、許可または禁止されるサービスまたはアクションを指定できます。詳細については、 AWS Organizations ドキュメントの「サービスコントロールポリシー」を参照してください。

サービスエンドポイント

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

サービスレベルアグリーメント (SLA)

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

サービスレベルインジケータ (SLI)

エラー率、可用性、スループットなど、サービスのパフォーマンス側面の測定。

サービスレベルの目標 (SLO)

サービスレベルのインジケータによって測定される、サービスの状態を表すターゲットメトリクス。

責任共有モデル

クラウドのセキュリティとコンプライアンス AWS について と共有する責任を説明するモデル。AWS はクラウドのセキュリティを担当しますが、ユーザーはクラウドのセキュリティを担当します。詳細については、責任共有モデルを参照してください。

SIEM

セキュリティ情報とイベント管理システムを参照してください。

単一障害点 (SPOF)

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

SLA

「サービスレベルアグリーメント」を参照してください。

SLI

「サービスレベルインジケータ」を参照してください。

SLO

「サービスレベルの目標」を参照してください。

split-and-seed モデル

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

SPOF

単一障害点を参照してください。

star スキーマ

トランザクションデータまたは測定データを保存するために 1 つの大きなファクトテーブルを使用し、データ属性を保存するために 1 つ以上の小さなディメンションテーブルを使用するデータベースの組織構造。この構造は、データウェアハウスまたはビジネスインテリジェンスの目的で使用するために設計されています。

strangler fig パターン

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

サブネット

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

監視コントロールとデータ収集 (SCADA)

製造では、ハードウェアとソフトウェアを使用して物理アセットと生産オペレーションをモニタリングするシステム。

対称暗号化

データの暗号化と復号に同じキーを使用する暗号化のアルゴリズム。

合成テスト

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

システムプロンプト

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

T

タグ

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

ターゲット変数

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

タスクリスト

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

テスト環境

「環境」を参照してください。

トレーニング

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

トランジットゲートウェイ

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

トランクベースのワークフロー

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

信頼されたアクセス

ユーザーに代わって AWS Organizations およびそのアカウントで組織内のタスクを実行するために指定したサービスにアクセス許可を付与します。信頼されたサービスは、サービスにリンクされたロールを必要なときに各アカウントに作成し、ユーザーに代わって管理タスクを実行します。詳細については、 ドキュメントの「 AWS Organizations を他の AWS のサービスで使用する AWS Organizations 」を参照してください。

チューニング

機械学習モデルの精度を向上させるために、お客様のトレーニングプロセスの側面を変更する。例えば、お客様が機械学習モデルをトレーニングするには、ラベル付けセットを生成し、ラベルを追加します。これらのステップを、異なる設定で複数回繰り返して、モデルを最適化します。

ツーピザチーム

2 つのピザを食べることができる small DevOps チーム。ツーピザチームの規模では、ソフトウェア開発におけるコラボレーションに最適な機会が確保されます。

U

不確実性

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

未分化なタスク

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

上位環境

「環境」を参照してください。

V

バキューミング

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

バージョンコントロール

リポジトリ内のソースコードへの変更など、変更を追跡するプロセスとツール。

VPCピアリング

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

脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

W

ウォームキャッシュ

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

ウォームデータ

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

ウィンドウ関数

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

ワークロード

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

ワークストリーム

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

WORM

「書き込み 1 回」、「読み取り多数」を参照してください。

WQF

AWS 「Word Workload Qualification Framework」を参照してください。

Write Once, Read Many (WORM)

データを 1 回書き込み、データの削除や変更を防ぐストレージモデル。承認されたユーザーは、必要な回数だけデータを読み取ることができますが、変更することはできません。このデータストレージインフラストラクチャはイミュータブルと見なされます。

Z

ゼロデイエクスプロイト

ゼロデイ脆弱性を利用する攻撃、通常はマルウェア。

ゼロデイ脆弱性

実稼働システムにおける未解決の欠陥または脆弱性。脅威アクターは、このような脆弱性を利用してシステムを攻撃する可能性があります。開発者は、よく攻撃の結果で脆弱性に気付きます。

ゼロショットプロンプト

タスクを実行するための指示を LLM に提供しますが、タスクのガイドに役立つ例 (ショット) はありません。LLM は、事前トレーニング済みの知識を使用してタスクを処理する必要があります。ゼロショットプロンプトの有効性は、タスクの複雑さとプロンプトの品質によって異なります。「数ショットプロンプト」も参照してください。

ゾンビアプリケーション

CPU とメモリの平均使用量が 5% 未満のアプリケーション。移行プロジェクトでは、これらのアプリケーションを廃止するのが一般的です。

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