CSA JAPAN SUMMIT 2024

AWSによる発見的統制のベストプラクティス

機械学習や生成AIによる自動分析/イベントの可視化/検出制御と自動対応

アマゾン ウェブ サービス ジャパン 合同会社

執行役員
パブリックセクター 技術統括本部長
瀧澤与一

Abstract

発見的統制により、潜在的なセキュリティ脅威やインシデントを特定できます。

これはガバナンスフレームワークの最重要機能であり、品質管理、コンプライアンス、脅威の特定に影響を与えます。AWSを利用すると、監査、機械学習や生成AIによる自動分析やアラート、監視、検出制御を実装できます。

本セッションでは、進化するビジネス要件に迅速に対応し、イノベーションを加速するための、セキュリティベストプラクティスを示します。

Agenda

1. 発見的統制と対応するAWSサービスの概要
2. 機械学習を用いた発見的統制のベストプラクティス
3. 進化するビジネス要件 – 生成AIにおけるセキュリティ
4. まとめ

Agenda

1. 発見的統制と対応するAWSサービスの概要
2. 機械学習を用いた発見的統制のベストプラクティス
3. 進化するビジネス要件 – 生成AIにおけるセキュリティ
4. まとめ

AWS セキュリティ ソリューション

IDとアクセス管理

AWS Identity and Access Management (IAM)

AWS IAM Identity Center

AWS Organizations

AWS Directory Service

Amazon Cognito

AWS Resource Access Manager

Amazon Verified Permissions

検出と対応

AWS Security Hub

Amazon GuardDuty

Amazon Security Lake

Amazon Inspector

Amazon Macie

Amazon Detective

Amazon CloudWatch

AWS Config

AWS CloudTrail

ネットワークとアプリケーション保護

AWS Firewall Manager

AWS Network Firewall

AWS Shield

AWS WAF

Amazon VPC

AWS PrivateLink

AWS Systems Manager

AWS Verified Access

データ保護

Amazon Macie

AWS Key Management Service (KMS)

AWS CloudHSM

AWS Certificate Manager

AWS Private CA

AWS Secrets Manager

AWS Payment Cryptography

Server-Side Encryption

コンプライアンス

AWS Artifact

AWS Audit Manager

発見的統制

発見的統制

可視性を高めることが重要
ビジネスに影響が出る前に問題を発見し、セキュリティ体制を改善し、リスク発生を軽減させる

セキュリティチームが直面する課題

可視性の欠如
セキュリティリスクと
その影響

組織のニーズに合わせて
セキュリティ対策を
スケールさせる必要性

セキュリティアラートの
複数の情報源

アラートが多すぎるる
コンテキストが足りない

発見的統制

AWS Security Hub
AWS セキュリティチェックを自動化し、セキュリティアラートを一元化します。

Amazon GuardDuty
インテリジェントな脅威検出で AWS アカウントを保護します。

Amazon Inspector
大規模な自動的かつ継続的な脆弱性管理。

Amazon CloudWatch
AWS、オンプレミス、その他のクラウド上のリソースとアプリケーションを観察および監視できます。

AWS Config
リソースの構成を評価、監査、評価します。

AWS CloudTrail
ユーザーアクティビティと API を追跡します。

VPC Flowlogs
VPC のネットワークインターフェースに出入りする IP トラフィックに関する情報を収集します。

Amazon Security lake
セキュリティデータを数ステップで自動的に一元化します。

Agenda

1. 発見的統制と対応するAWSサービスの概要
2. 機械学習を用いた発見的統制のベストプラクティス
3. 進化するビジネス要件 – 生成AIにおけるセキュリティ
4. まとめ

AWS 検出と対応サービス

AWS 上での検出と対応

AWS 環境全体の
セキュリティ体制を強化し、
セキュリティ運用を合理化す
るのに役立つ一連のサービス

Amazon GuardDuty
脅威と異常行動を検出

Amazon Macie
機密データの
検出と保護

Amazon Inspector
脆弱性の検出

AWS Security Hub
セキュリティ
チェックの自動化と
アラートの一元管理

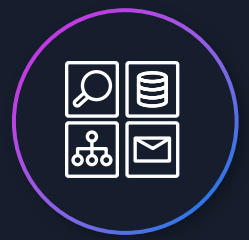
Amazon Detective
イベントと
検出結果の調査

Amazon Security Lake
セキュリティデータ
の正規化と分析

Amazon GuardDuty とは

機械学習 (ML) 、異常検知、サービスと統合された脅威インテリジェンスを使用して潜在的な脅威を特定し、優先順位を付ける
マネージド脅威検出サービス

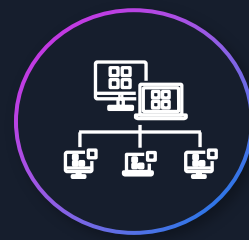
AWS 組織全体での
ワンステップ
アクティベーション



AWS アカウントと
リソースの継続的な
モニタリング

機械学習と
脅威インテリジェンスを
活用した独自の
検出機能

AWS および
リーディング企業の
脅威インテリジェンス



フルマネージド型の
AWS ワークロード
保護

Amazon GuardDuty の仕組み

基礎的なデータソース

VPC Flow Logs, DNS logs

CloudTrail イベント
(AWS IAM アクセスキーや
Amazon EC2等の情報)

AWS ワークロード保護毎のデータソース

- Amazon S3 データプレーンイベント
- Amazon EKS 監査ログ
- Amazon Aurora ログインイベント
- AWS Lambda ネットワークアクティビティ
- Runtime アクティビティ

セキュリティ分析

AI/ML

脅威インテリジェンス

継続的学習

セキュリティ検出結果

実用的

正確性

豊富な
コンテキスト情報

サービス統合と修復

Amazon
Detective

AWS
Security Hub

Amazon
EventBridge

AWS ワークロード保護のための GuardDuty

S3 Protection

S3 バケット内のデータに関する潜在的なセキュリティリスクを特定

EKS Protection

EKS 監査ログモニタリングは、Amazon EKS クラスターの Kubernetes 監査ログを分析して、潜在的に悪質で疑わしいアクティビティがないか調べます。

Malware Protection

マルウェアによって侵害されたリソースまたは危険にさらされているリソースを特定

RDS Protection

RDS ログインアクティビティを分析してプロファイリングし、Amazon Aurora データベースへの潜在的なアクセス脅威を特定[1]

Lambda Protection

VPC フローログをはじめとするネットワークアクティビティを継続的に監視して、AWS Lambda 関数に対する脅威を検知

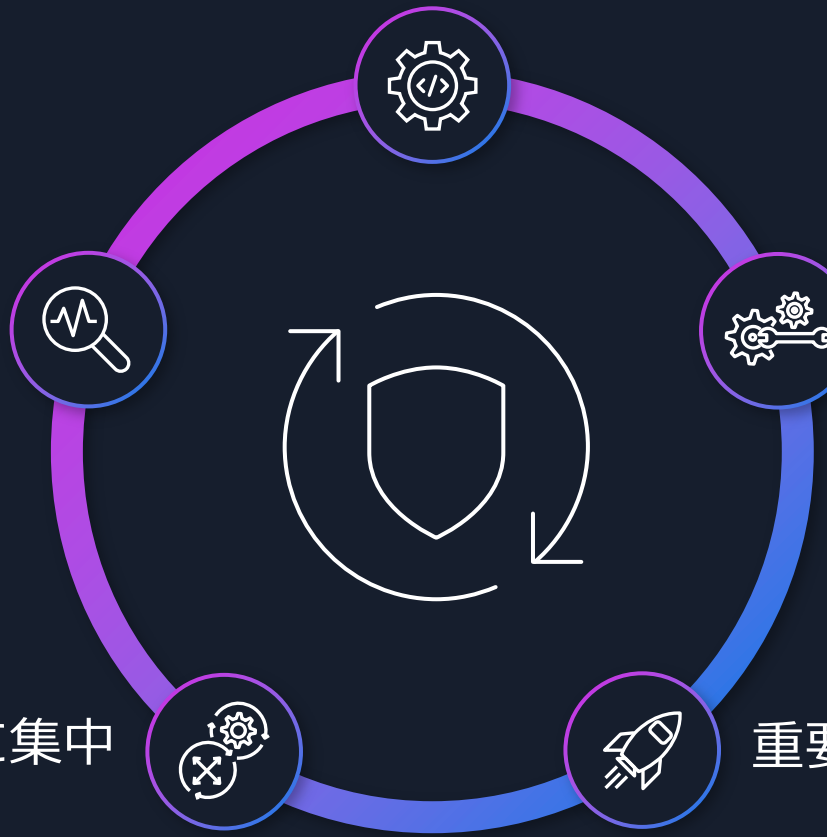
Runtime Monitoring

Amazon EKS、Amazon ECS (AWS Fargate を含む)、および Amazon EC2 のオペレーティングシステムレベルのイベントを監視および分析して、潜在的な脅威を検出

[1]Amazon Aurora MySQL-Compatible Edition and Aurora PostgreSQL-Compatible Edition

高度に統合されたサービスによる自動化とリスクの軽減

広範囲な API とセキュリティツールセット



継続的なモニタリングと保護

脅威の修復と対応

運用を効率化し重要課題に集中

重要システムの安全なデプロイ

AWS Security Hub

Security Hub は、セキュリティのベストプラクティスチェックを継続的に実施し、AWS とサードパーティのサービスからのセキュリティ結果をシームレスに集約して自動対応を可能にするクラウドセキュリティポスチャ管理サービスです。

自動化された継続的なベストプラクティスチェック

AWS セキュリティベストプラクティス (FSBP) 標準、CIS などへの対応

導入が簡単で、最大 10,000 アカウントまで拡張可能

アカウントとリージョンにわたる AWSおよびサードパーティサービスの結果集約

自動応答とエンリッチメントアクション

Security Hubを取り巻くアクション

標準と統制

PCIDSS

NICT

AWS FSBP

CIS AWS ファンデーションベンチマーク

サービス管理標準

検出結果の取り込み

AWS Config

Amazon Guard Duty

Amazon Inspector

AWS Identity and Access Management (IAM)

Amazon Macie

AWS Firewall Manager

その他

Security Hub

Amazon EventBridge

検出結果の統合

Amazon Detective

AWS Audit Manager

Amazon Security Lake

AWS Trusted Advisor

AWS Chatbot

修復アクション

AWS Lambda

AWS Systems Manager

AWS Step Functions

AWS パートナーとの連携

。。その他多数

これは完全なリストではありません。すべての AWS Security Hub パートナーを確認するには、Security Hub コンソールにアクセスしてください。このパートナーリストは、2023年11月28日現在のものです。

統合サービスによる自動化とリスクの軽減

包括的な API と
セキュリティツールのセット

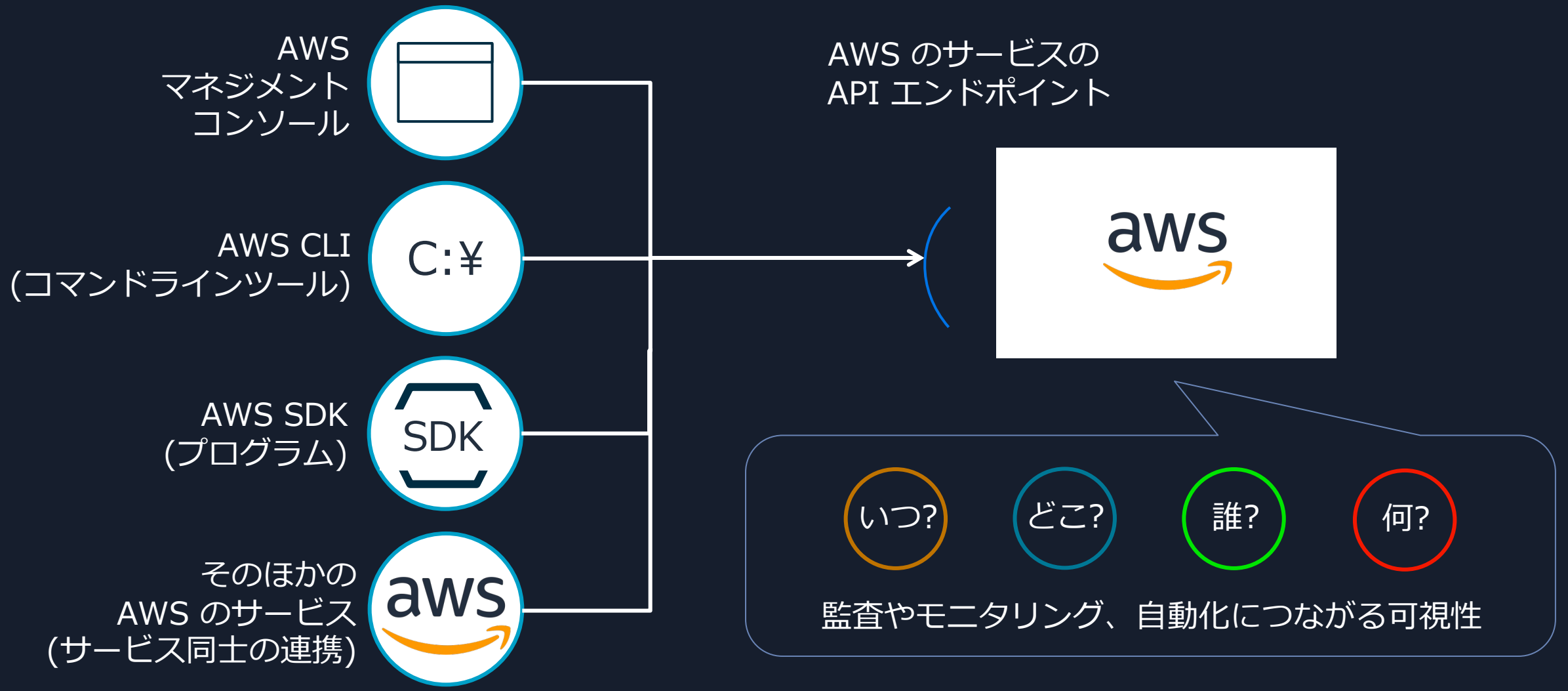
継続的モニタリングと
保護

脅威対策と
応答

重要な問題に
集中するための
業務効率化

ビジネスクリティカルな
アプリケーションを
安全にデプロイ

高い可視性の確保 –
AWS の操作は API を通じて提供される

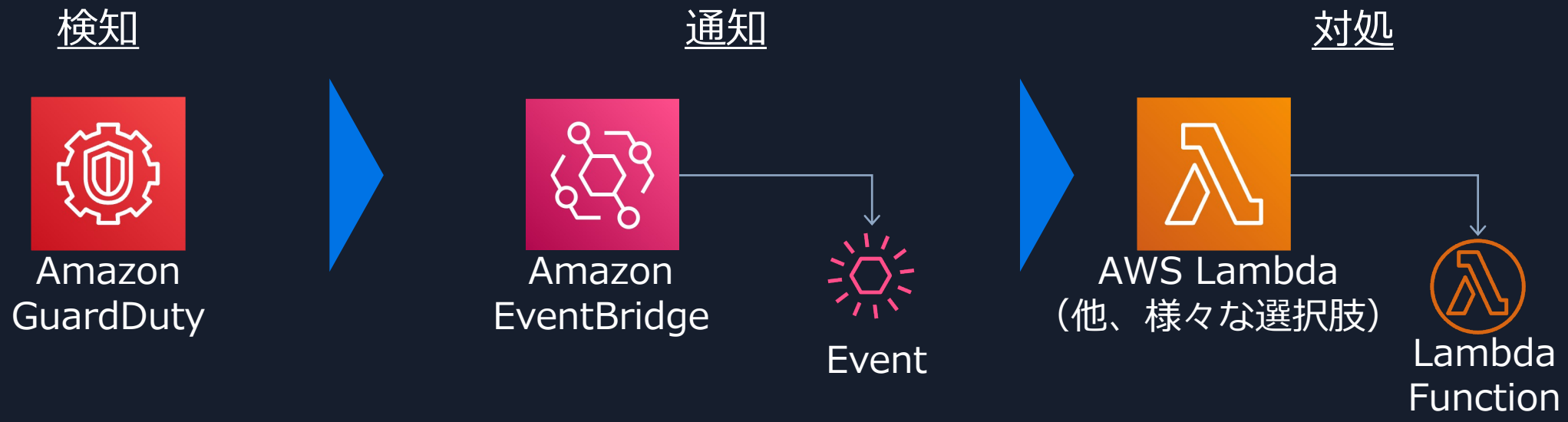


お客様のワークロードに対して幅広い観点での可視性を導入

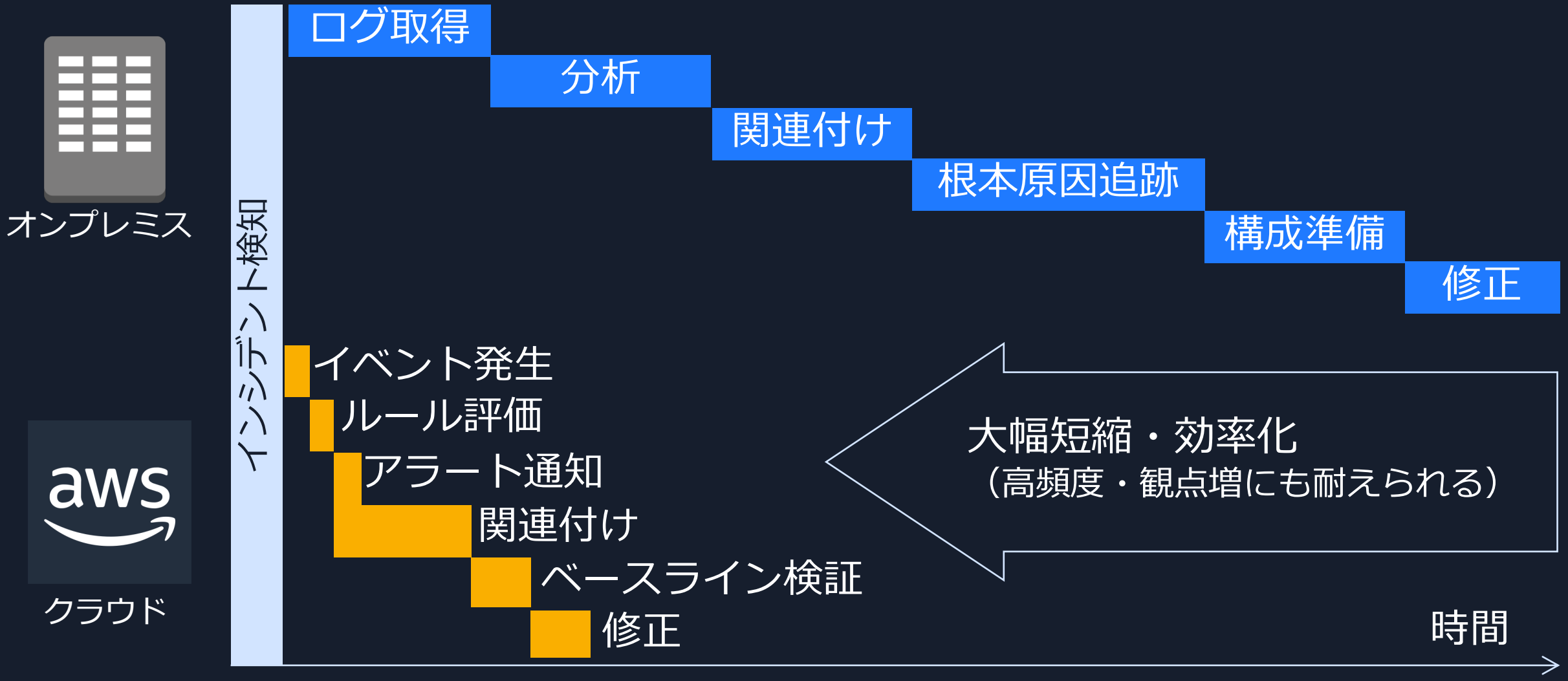
大規模運用に対応可能な「セキュリティモニタリング基盤」の実現

サービス連携によるセキュリティ自動化で、セキュリティ監視を素早いアクションへつなげていく

たとえば、自動化された脅威への対処（インシデントレスポンス）



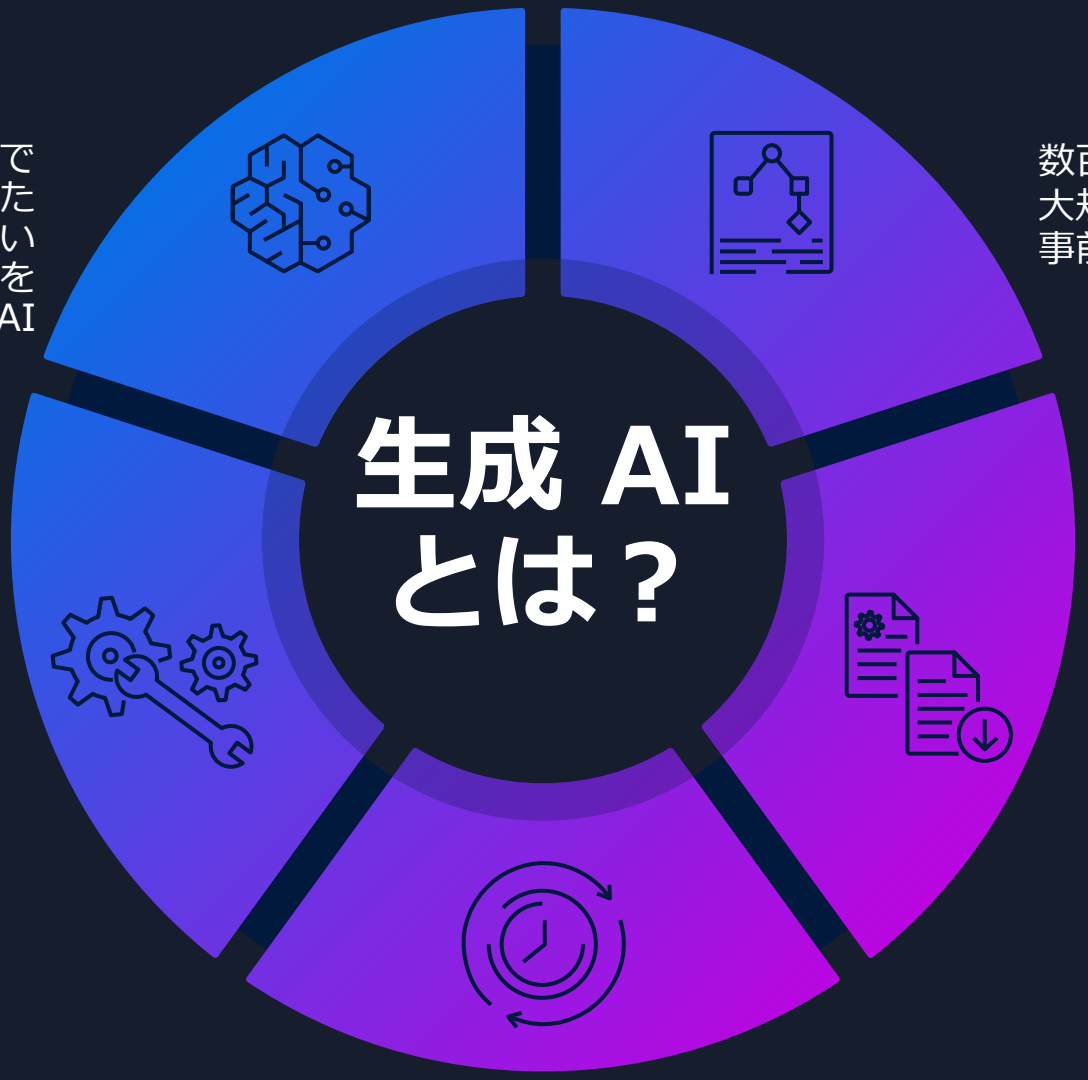
自動化による対応スピードの変化



Agenda

1. 発見的統制と対応するAWSサービスの概要
2. 機械学習を用いた発見的統制のベストプラクティス
3. 進化するビジネス要件 – 生成AIにおけるセキュリティ
4. まとめ

生成 AI とは？



現実世界のタスクで
人間が生成した
コンテンツに十分近い
オリジナルコンテンツを
作成できるAI

数百億のパラメータを含む
大規模なデータセットで
事前学習された基盤モデルを利用

最小限の
ファインチューニングで
特定のドメイン向けに
カスタマイズが可能

テキストの要約、質問への回答、
デジタルアートの創造、
コード生成など、
多くのユースケースに適用可能

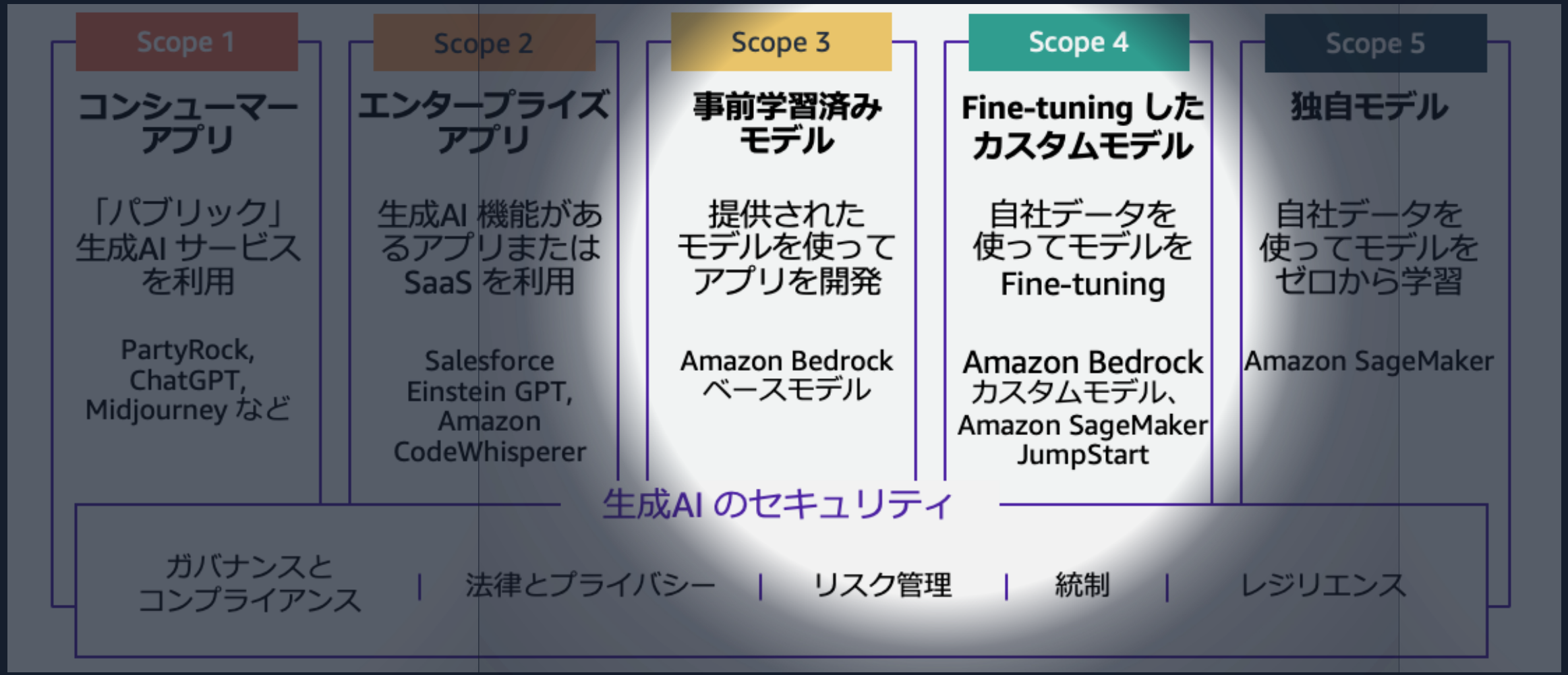
機械学習モデルの開発に関わる時間とコストを削減して
イノベーションを加速

生成 AI セキュリティスコーピングマトリックス

ユースケースを分類するメンタルモデル

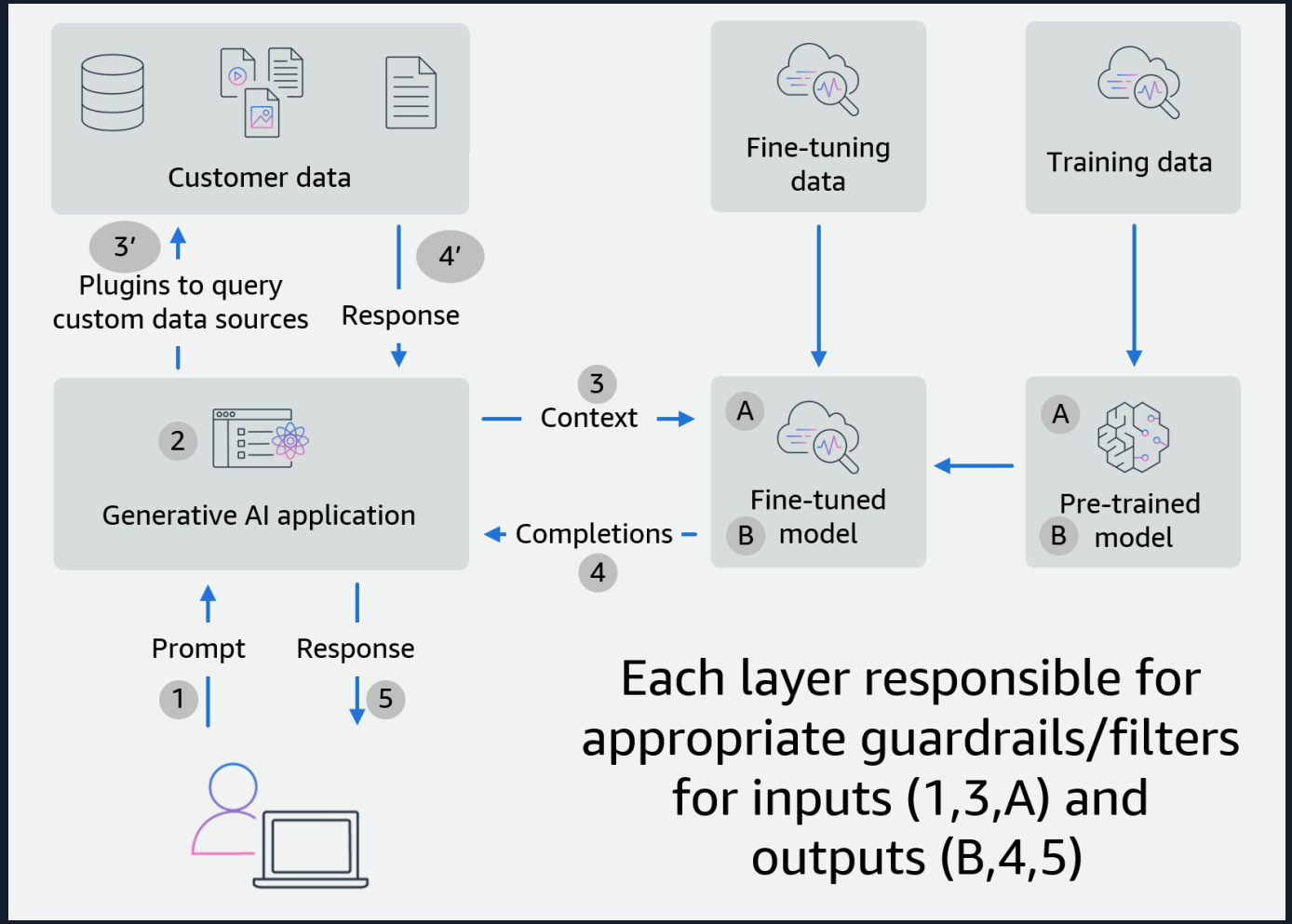
生成 AI セキュリティスコーピングマトリックス

ユースケースを分類するメンタルモデル



生成AI アプリケーションのデータフローの例

1. アプリケーションはユーザーからの入力を受け取ります
   - [オプション] アプリはカスタムデータソースからデータを照会します
2. アプリは、ユーザー入力と顧客データをフィルタリングしてプロンプトでフォーマットします
3. プロンプトはモデルによって拡張されてから完了されます
   - [オプション] Fine-tune モデルの使用
4. 入力内容はアプリケーションごとに処理/フィルタリングされます
5. レスポンスがユーザーに送信されます



責任ある AI とは

AWS の責任ある AI フレームワーク

公平性

システムがユーザーのさまざまなサブポピュレーションに与える影響 (性別、民族など)

説明可能性

AI システムのアウトプットを理解し評価するためのメカニズム

堅牢性 (Robustness)

AI システムが確実に動作することを保証する仕組み

プライバシーとセキュリティ

データはプライバシー上の考慮事項に従って使用され、盗難や漏洩から保護されています

ガバナンス

組織内で責任ある AI プラクティスを定義、実装、実施するためのプロセス

透明性

利害関係者がシステムの使用について情報に基づいた選択を行えるように、AI システムに関する情報を伝える

OWASP® トップ10の大規模言語モデル (LLM)

一部の項目には、技術的な対策だけでは不十分です。

LLM

プロンプト・インジェクション

これは大きな言語を操作します巧妙なインプットによるモデル（LLM）、
LLMによる意図しない行動を引き起こす。直接注入はシステムプロンプトを上書きし、間接注入は外部ソースからの入力を操作します。

LM02

安全でない出力処理

この脆弱性は、LLM 出力が精査されずに受け入れられ、バックエンドシステムが公開される場合に発生します。誤用すると、XSS、CSRF、SSRF、権限昇格、リモートコード実行などの重大な結果につながる可能性があります。

LLM

トレーニングデータポイズニング

これは、LLMトレーニングデータが改ざんされ、セキュリティ、有効性、または倫理的行動を損なう脆弱性や偏見が生じた場合に発生します。

LM04

モデルサービス拒否

攻撃者はLLMでリソースを大量に消費する操作を行い、サービスの劣化や高コストにつながります。LLMはリソースを大量に消費する性質とユーザー入力の予測不能性により、この脆弱性がさらに大きくなります。

LM05

サプライチェーンの脆弱性

LLMアプリケーションのライフサイクルは、脆弱なコンポーネントやサービスによって侵害され、セキュリティ攻撃につながる可能性があります。サードパーティのデータセット、事前にトレーニングされたモデル、およびプラグインを使用すると、脆弱性が追加される可能性があります。

LM06

機密情報の開示

LLMは、回答時に機密データをうっかり公開してしまい、不正なデータアクセス、プライバシー侵害、セキュリティ侵害につながる可能性があります。これを軽減するには、データサニタイズと厳格なユーザーポリシーを実装することが重要です。

LM07

安全でないプラグイン設計

LLM プラグインの入力が安全でない場合や、アクセス制御が不十分である場合があります。このようにアプリケーションを制御できないと、悪用されやすくなり、リモートでコードが実行されるような結果になる可能性があります。

LM08

過剰なエージェンシー

LLMベースのシステムは、意図しない結果につながるアクションを実行する可能性があります。この問題は、LLM ベースのシステムに過剰な機能、権限、または自律性が与えられていることが原因で発生します。

LM09

オーバーリライアンス

LLMに過度に依存しているシステムや人々は、LLMによって生成された不正確または不適切なコンテンツが原因で、誤った情報、伝達ミス、法的問題、およびセキュリティ上の脆弱性に直面する可能性があります。

LM10

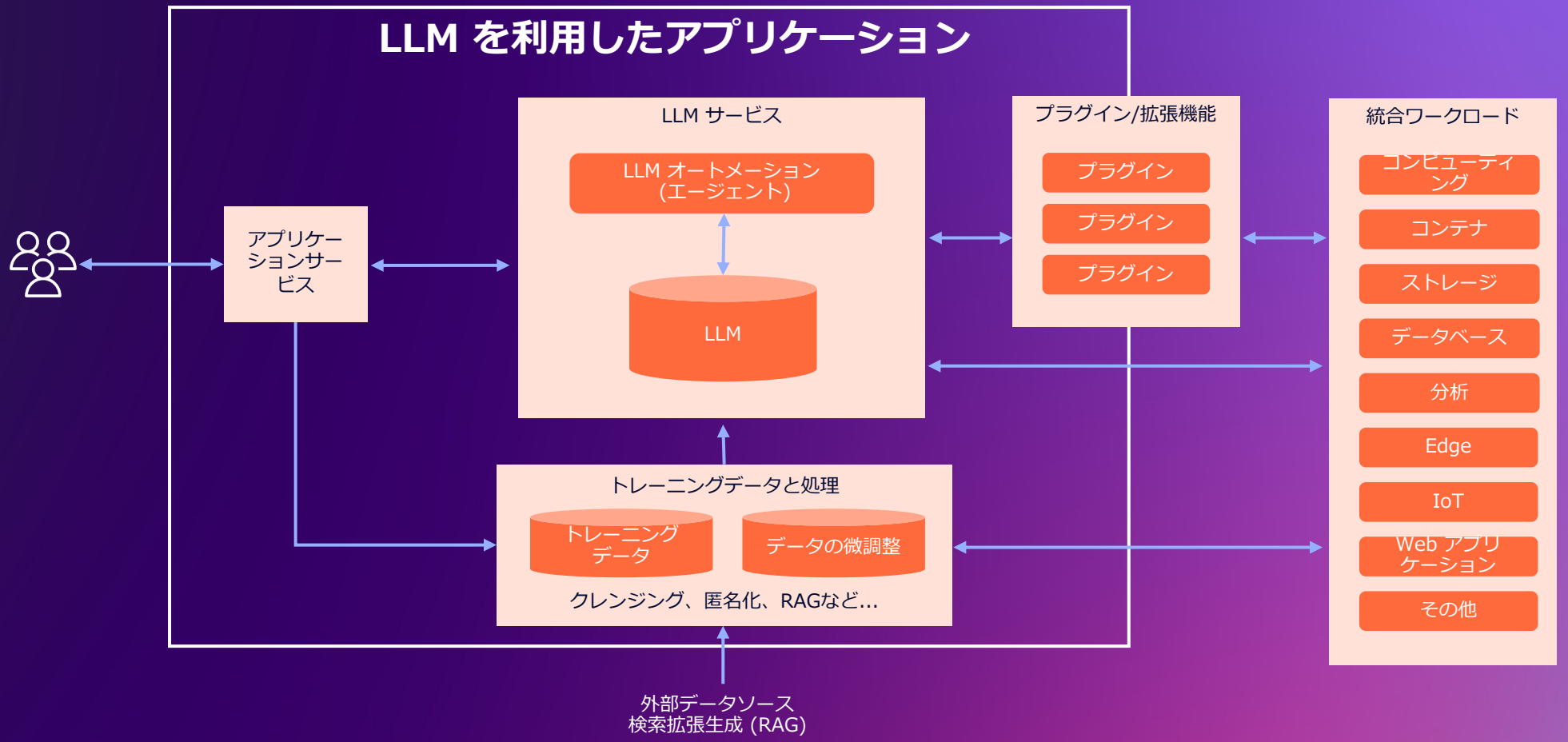
モデル盗難

これには、独自のLLMモデルへの不正アクセス、コピー、または盗用が含まれます。その影響には、経済的損失、競争上の優位性の低下、機密情報へのアクセスの可能性などが含まれます。

ソース:https://owasp.org/www-project-top-10-for-large-language-model-applications/

生成AI ワークロードの例

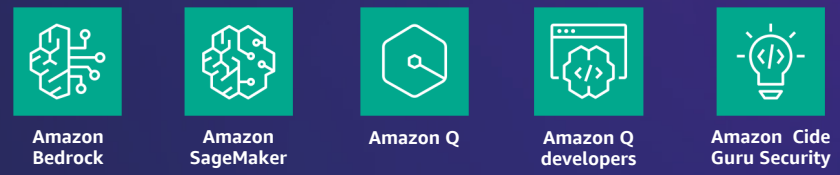
AI 搭載アプリのどこにセキュリティコントロールを適用するか



AWS 生成AI とセキュリティの統合

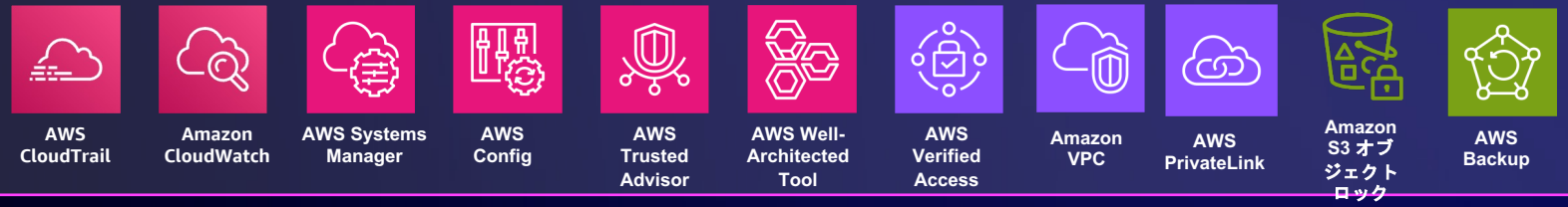
基本的な AWS セキュリティ＋生成AI サービスのその他のセキュリティ機能

AWS 生成 AI サービス



AWS セキュリティ、アイデンティティ、コンプライアンスサービス

AWS クラウドオペレーション、ネットワーキング、ストレージ



4 つの基本的な AWS セキュリティサービス

生成AIのための多層防御の基盤はどこから始めるべきか

インシデント
レスポンス

AWS Security Hub

Amazon GuardDuty

脅威
検知

データ
保護

AWS Key
Management
Service (AWS KMS)

AWS Shield
Advance

ネットワークと
アプリケーション保護

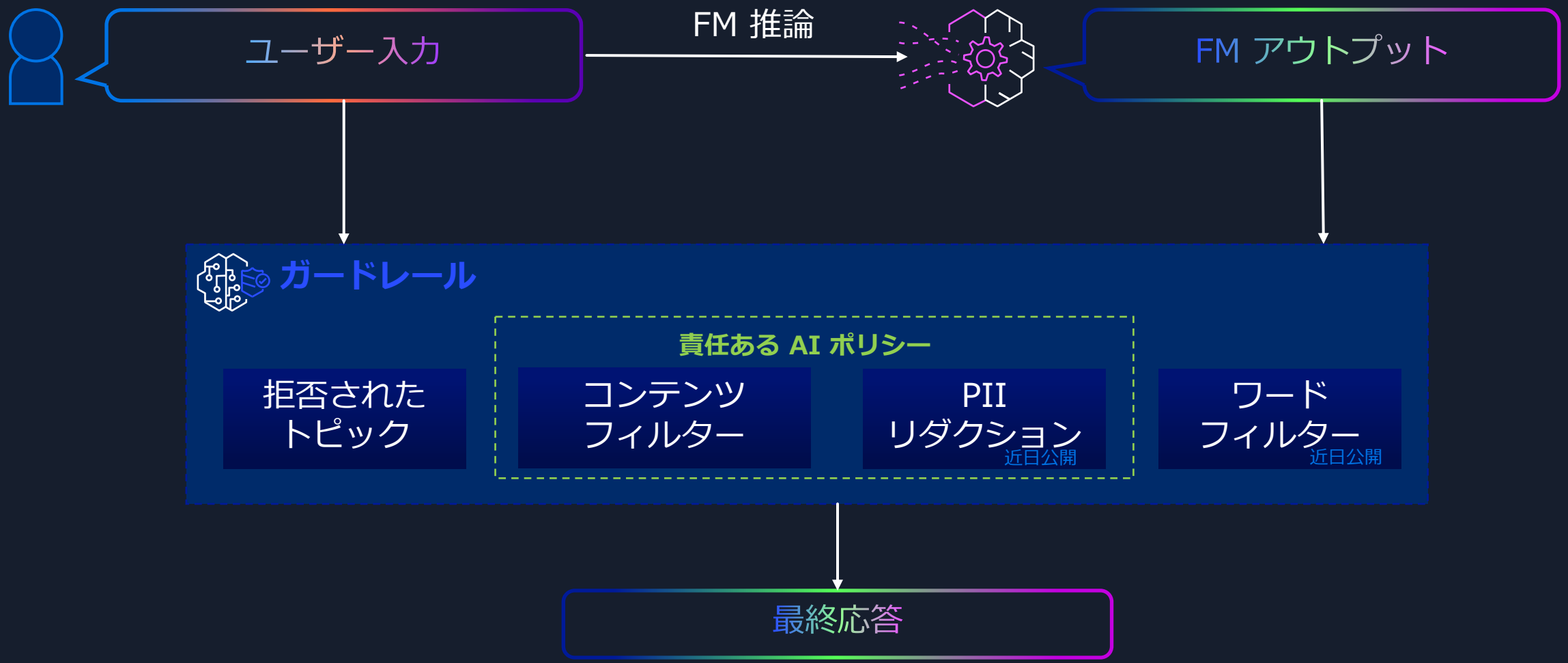
基盤モデルの意図しない振る舞いに対するセーフガード

AMAZON BEDROCK GURDRAILS

Amazon Bedrock Guardrails

- Amazon Bedrock Guardrails を使用すると、責任ある AI ポリシーに基づいて有害コンテンツフィルタリングを簡単に設定可能。
- 拒否されたトピック、コンテンツフィルター、ワードフィルター、および プライバシーを保護するための機密情報（PII）のマスキングなどの、ポリシーを設定可能。
- ガードレールを任意の 基盤モデルまたはエージェントに適用可能

Amazon Bedrock Guardrailsの仕組み

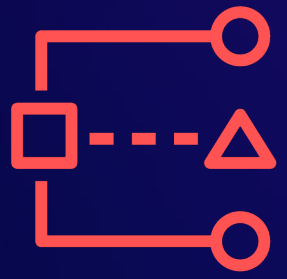


AWS に組み込まれている自動推論の例

保証と確実性を数学的に証明するユニバーサルステートメント

Amazon S3

S3 バケットは
パブリックにアクセス
不可にしたい



IAM
Access Analyzer

意図しない
S3 バケットへの
外部アクセスを防ぎたい

Amazon Inspector

EC2インスタンスは常に
意図せずに
公開されないようにしたい

Amazon VPC
Network Access
Analyzer

インスタンスへの
SSHトラフィックはすべて
ファイアウォールを通過させたい

Agenda

1. 発見的統制と対応するAWSサービスの概要
2. 機械学習を用いた発見的統制のベストプラクティス
3. 進化するビジネス要件 – 生成AIにおけるセキュリティ
4. まとめ

オンプレミスでは…

開発や運用の
俊敏性/利便性

OR

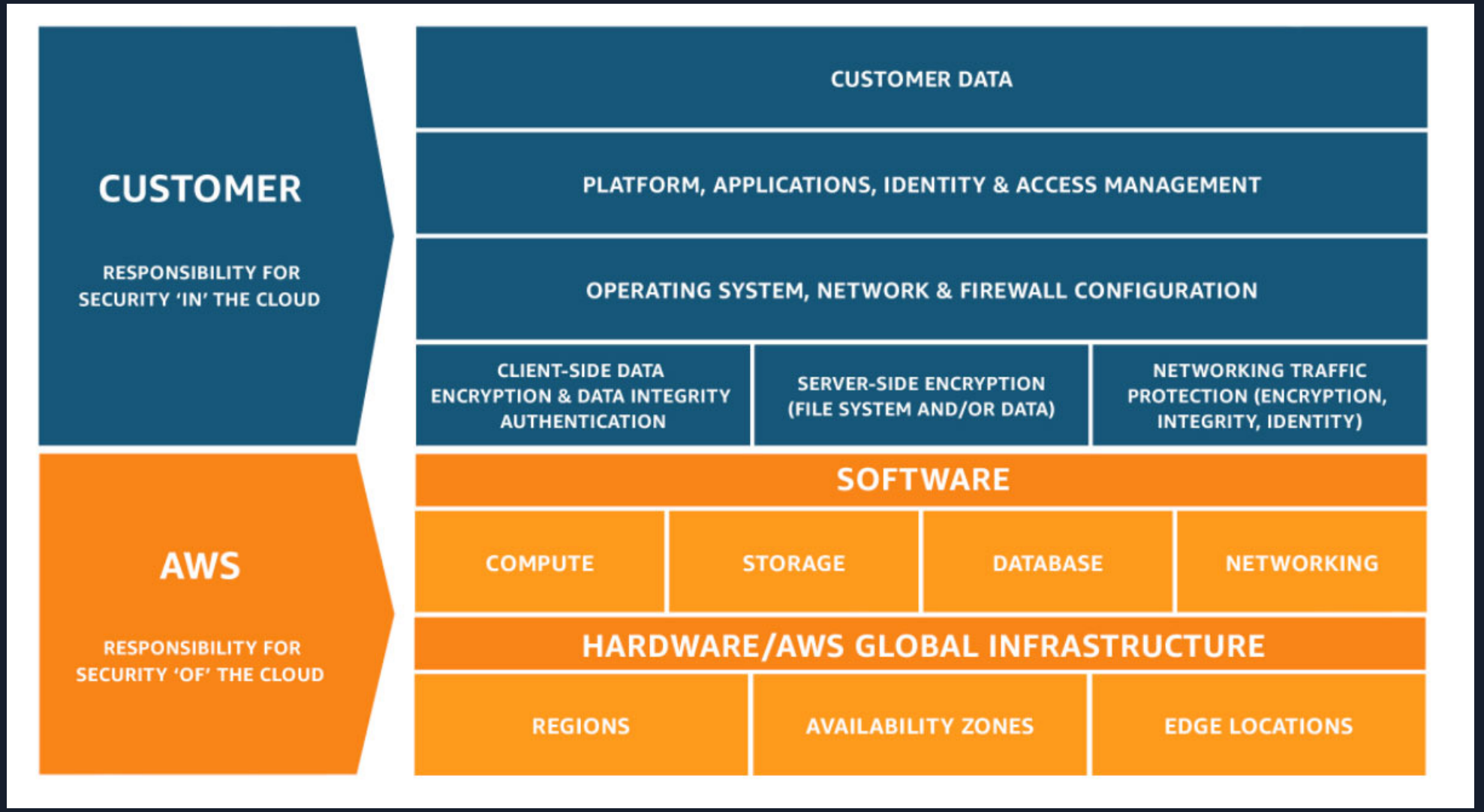
セキュリティの
確保

クラウドでは…

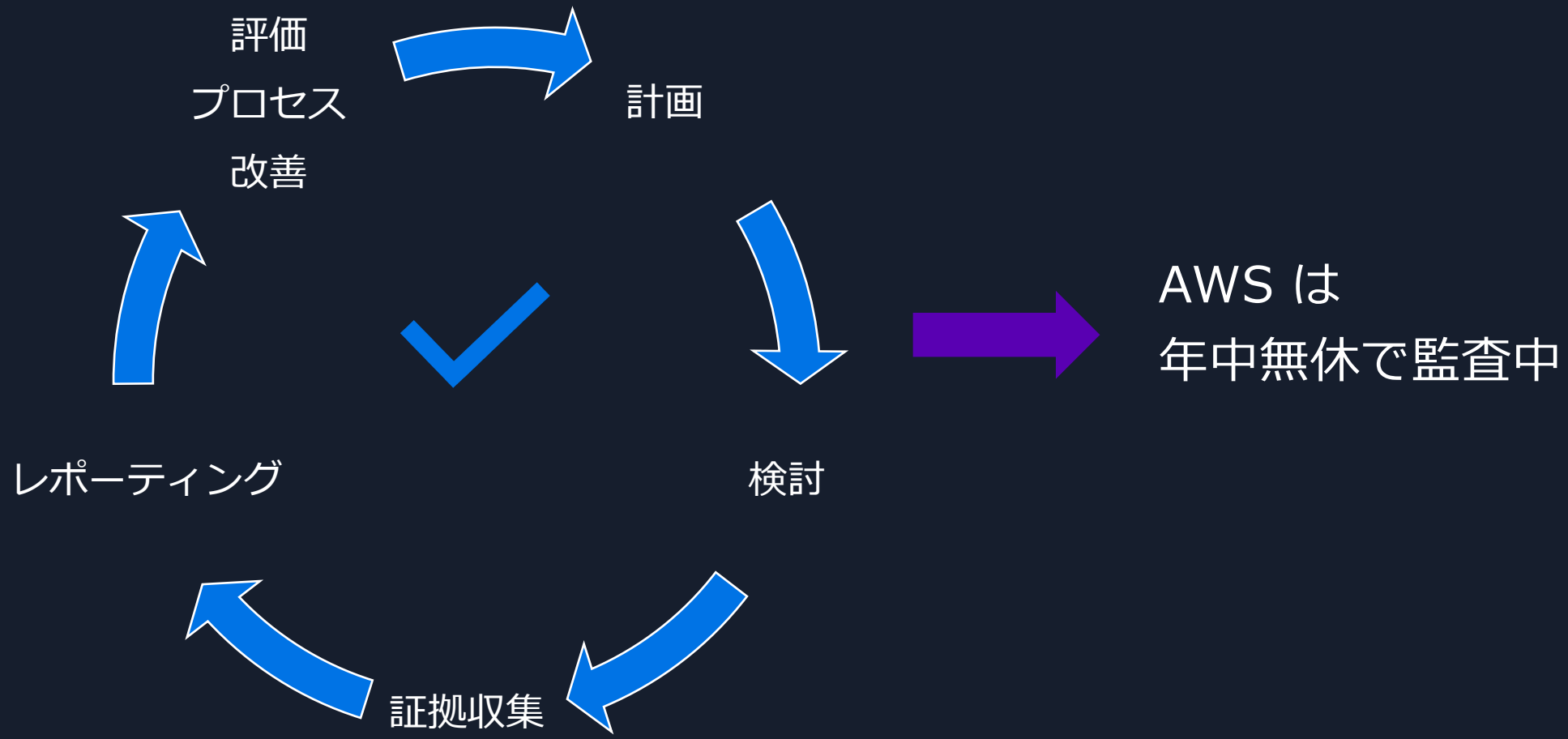
開発や運用の
俊敏性/利便性

セキュリティの
確保

責任共有モデル



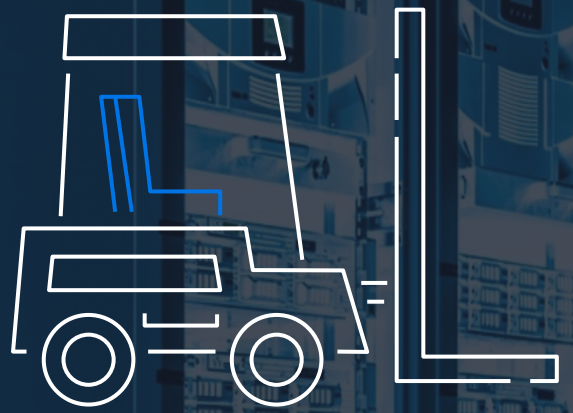
継続的監査 - 可視性を高める



AWS は
年中無休で監査中

優れたセキュリティ実現に
不可欠なAWS が備える特性

高い可視性の確保



柔軟かつ多様な
自動化と機能連携

Thank you!

Yoichi Takizawa

Director,

Public Sector Tech Business Unit,

Amazon Web Services Japan G.K.