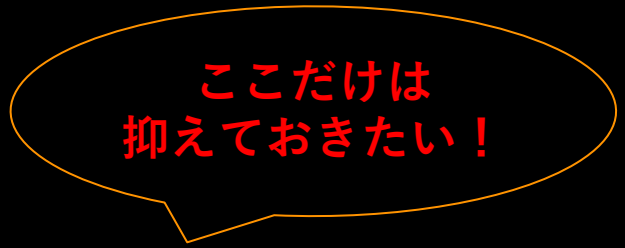


Amazon EC2 Security BestPractice

アマゾン ウェブ サービス ジャパン合同会社
シニアパートナーソリューションアーキテクト
大場 崇令

2021/11/04

Who am I ?

@takaohba

- 大場 崇令（オオバ タカノリ）
  - Senior Partner Solutions Architect @Amazon Web Services Japan G.K. (Joined 2015/12)
- Background
  - AWS テクニカルトレーナー@AWSJ G.K.
  - Web サービスのインフラエンジニア
  - 国内クラウドベンダーにてテクニカルサポート
- 好きな AWS サービス
  - AWS Well-Architected Tool
  - AWS Systems Manager
  - AWS Service Catalog

Well-Architected Lead

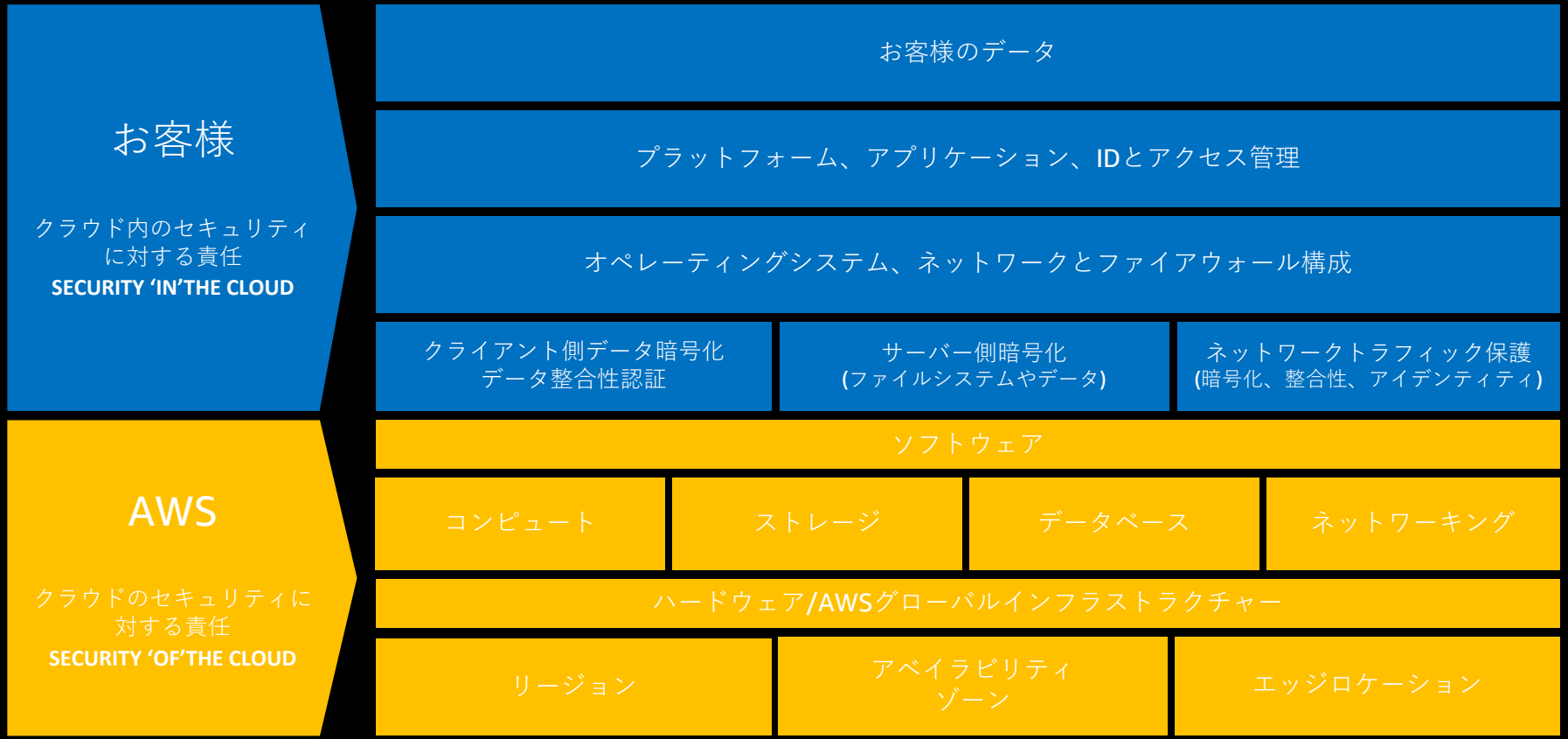
aws

今日のゴール

Amazon EC2 における、最低限実施すべき
セキュリティのベストプラクティスを理解いただくこと

AWS におけるセキュリティの考え方

責任共有モデル



https://aws.amazon.com/jp/compliance/shared-responsibility-model/

AWSのセキュリティ統制(Security “OF” the Cloud)

AWSは、お客様が使用するAWS サービスに関連した統制と、 それらがどう検証されているかの情報を提供します

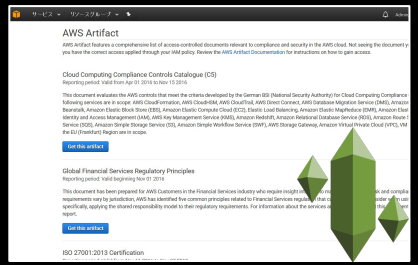
AWS

クラウドのセキュリティに対する責任

SECURITY ‘OF’THE CLOUD

第三者機関からの認定・認証

AWS統制に関するホワイトペーパーや公開文書



認定証明書や監査レポートの提供(要NDA)

お客様のセキュリティ統制(Security “IN” the Cloud)

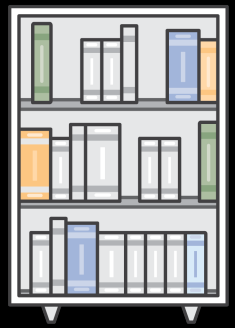
AWSは、お客様がお客様固有のセキュリティ要件を満たすための情報、サービス、ソリューションを提供します

お客様

クラウド内のセキュリティに対する責任

SECURITY ‘IN’THE CLOUD

AWSセキュリティサービス



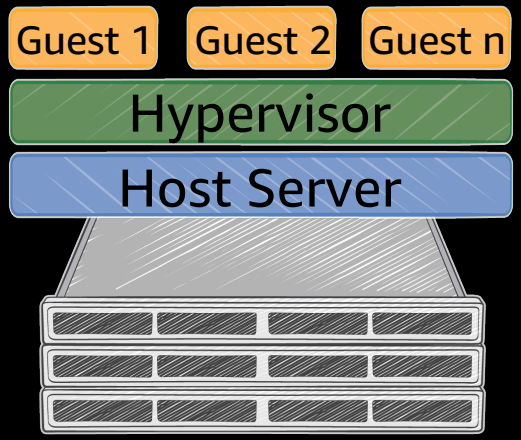
お客様の統制に関するベストプラクティス

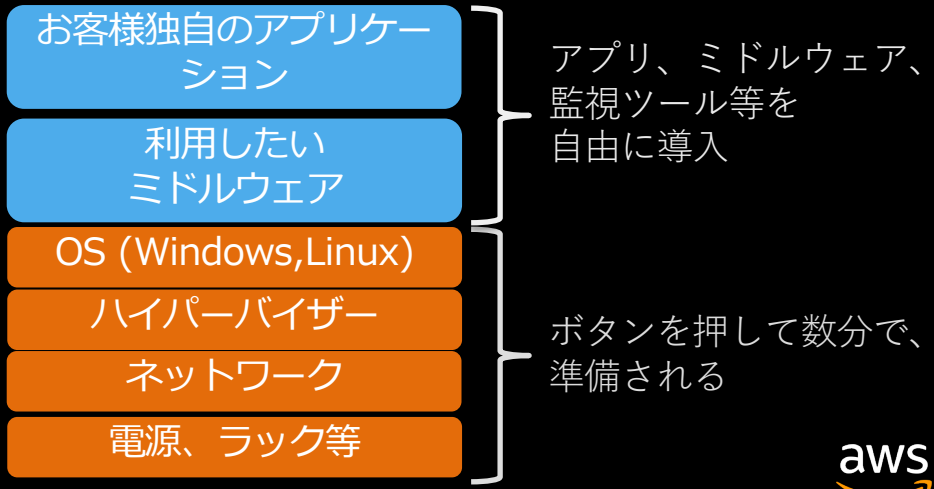
AWSパートナーソリューション

AWS Elastic Compute Cloud 概要

Amazon EC2 (Elastic Compute Cloud)

- 数分で起動、**1 秒ごとの従量課金**で利用可能な仮想サーバ
  - 一部OSは1時間単位の課金モデル
- 多数の OS をサポート、ライセンス費用込みで従量課金
- 自由にソフトウェアのインストールが可能
- スケールアップ/ダウン、アウト/インが容易に可能
- **管理者権限** (root / Administrator) で利用可能
- 任意のリージョン、アベイラビリティゾーンに配置可能





Amazon EC2 における セキュリティ対策

セキュリティ対策カテゴリー

	カテゴリー	内容
1	ID とアクセス管理	IAM ユーザーおよび IAM ロールによる権限付与 パスワードポリシー
2	検出	ログの取得・保管 ログの分析
3	インフラストラクチャー保護	ネットワーク設計（セグメンテーション等） Firewall 等の ACL 実装 DDoS 対策
4	データ保護	データの暗号化
5	インシデントレスポンス	インシデント通知、論理的隔離、封じ込め セキュリティ運用自動化

ID とアクセス管理

サーバー（OS）・セキュリティ

OS の選択とハードニング

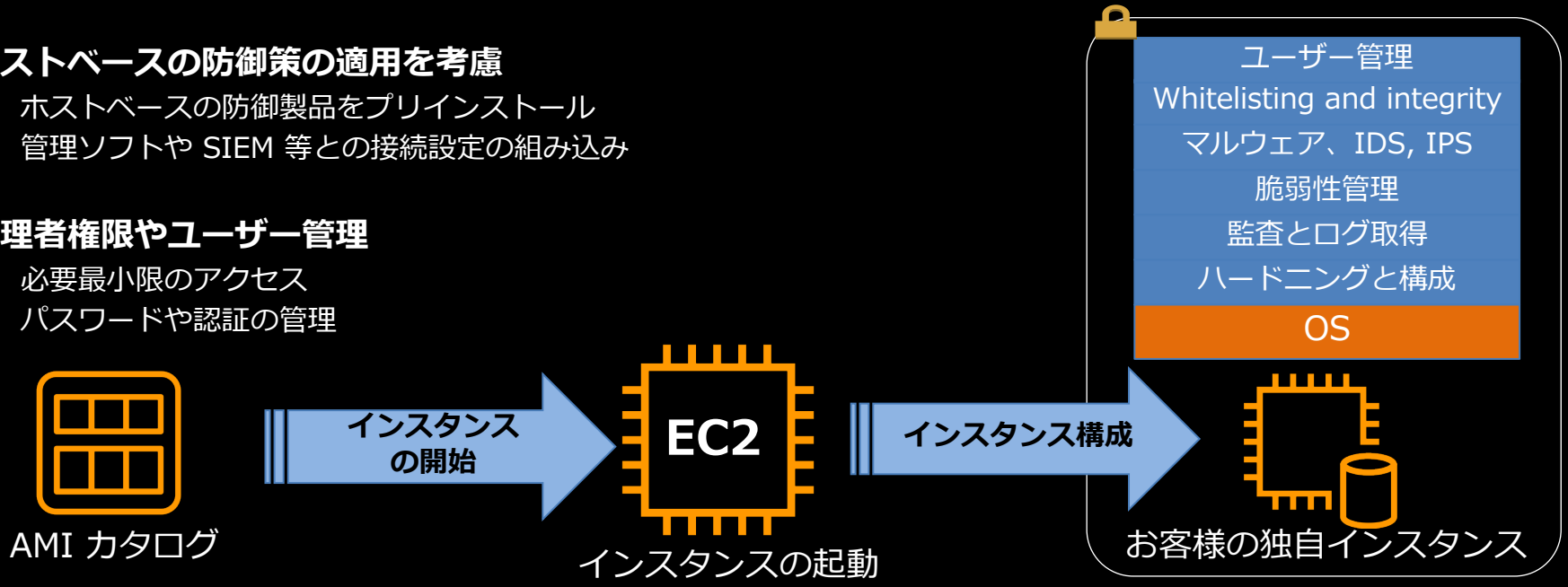
- インスタンスサイズ、OS の選択もお客様が柔軟に構成可能
- 標準的な OS のハードニングガイドとテクニックを活用
- 最新のセキュリティパッチの適用

ホストベースの防御策の適用を考慮

- ホストベースの防御製品をプリインストール
- 管理ソフトや SIEM 等との接続設定の組み込み

管理者権限やユーザー管理

- 必要最小限のアクセス
- パスワードや認証の管理

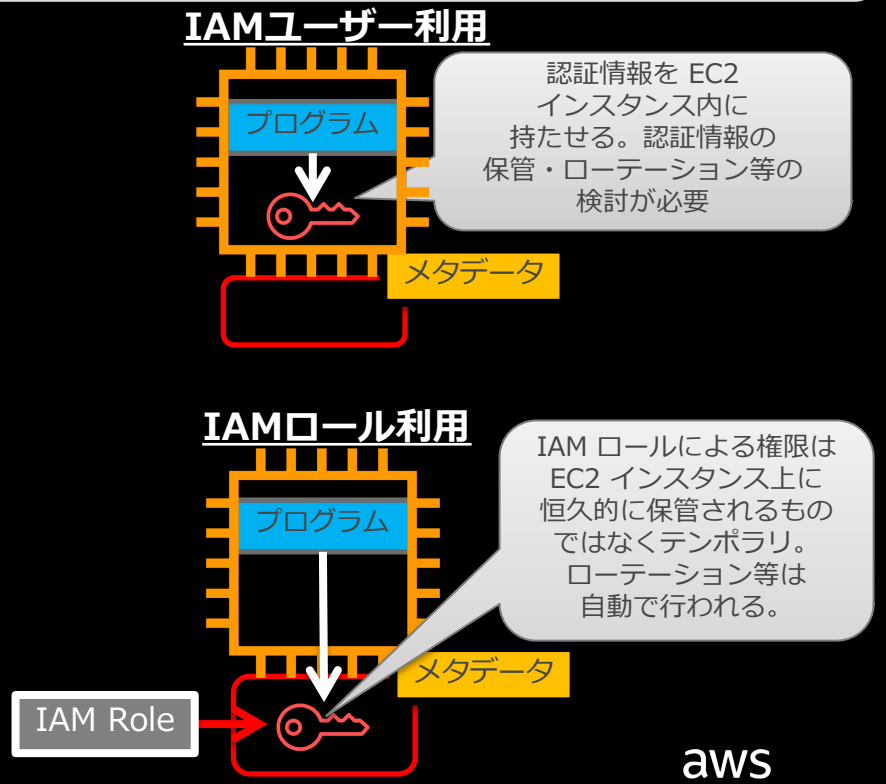


EC2 インスタンスには IAM ロールの利用

EC2 インスタンスのような AWS サービスに対して AWS の操作権限を付与するための仕組み。
IAM ユーザーの認証情報のようなものを OS/アプリケーション側に持たせる必要がなく、
認証情報の漏えいリスクが低くなります。IAM ロールによる認証情報は AWS が自動的にローテーションされます。

IAM ロール利用の利点

- EC2 インスタンス上の
  アクセスキーの管理が容易
- 自動的に認証情報の
  ローテーションが行われる
- EC2 インスタンス上のアプリケーション
  に最低権限を与えることに適している
- AWS SDK 及び AWS CLI のサポート
- IAM ユーザーの認証情報を外部に
  漏えいしてしまうリスクを低減させる



検出

AWS での監視の概要

- アプリ性能/死活監視
- リソース監視
- 死活監視
  (ログ,プロセス,OS)

アプリ
チェック

Agent経由等の
情報収集

CloudWatch/
API/SDK

Alarm

Application

Middleware

OS

aws

- Service Status 監視
- リソース監視
- Event 監視

aws

Amazon CloudWatch

AWSリソース、アプリケーション、
オンプレミスのモニタリングサービス

モニタリング

監視の集約

トラブルシュート

ログの分析

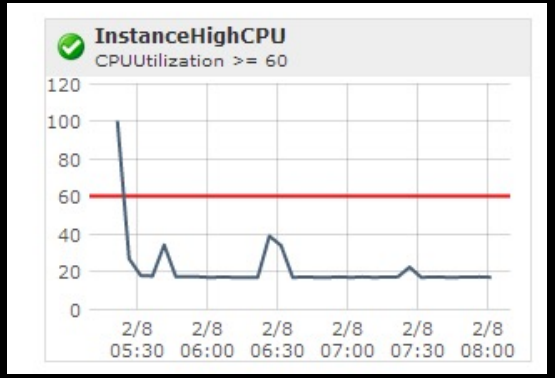
自動アクション

運用状況の把握

Amazon CloudWatch ができること

各 AWS サービスの**メトリクス監視**

- メトリクス = 監視項目（例：CPU使用率）
- メトリクスはあらかじめ定義され、構成済み
  - サービス開始時から監視開始
  - EC2ではハイパーバイザーから監視できる項目
- メトリクスを追加定義も可能
  - カスタムメトリクス
- メトリクス値を時系列にグラフ表示



各メトリクスに対して**アラーム**を作成可能

- しきい値を設定（例：CPU使用率60%以上）
- メトリクス値がしきい値を越えたら起こすアクションを定義（例：メールで通知）

EC2上の**ログ監視** ・・・Amazon CloudWatch Logs

- メトリクスとアラームも作成可能

Amazon CloudWatch 利用イメージ：メトリクス監視

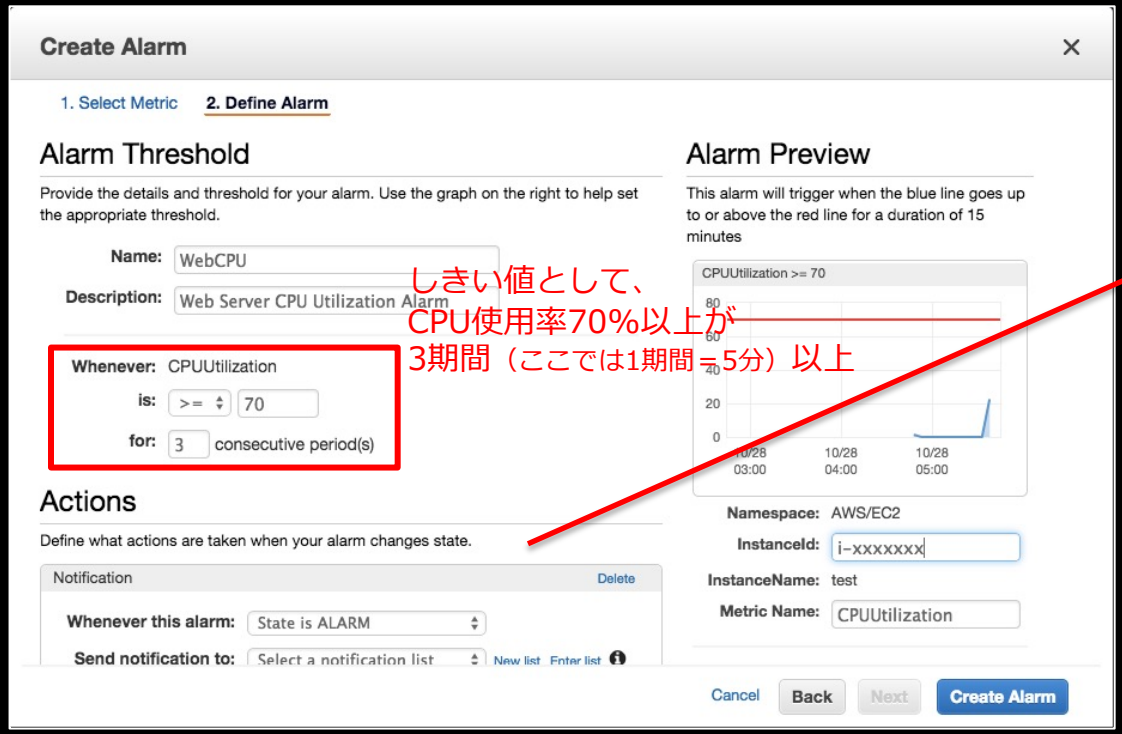
Amazon CloudWatch ができること：アラーム

アラーム設定

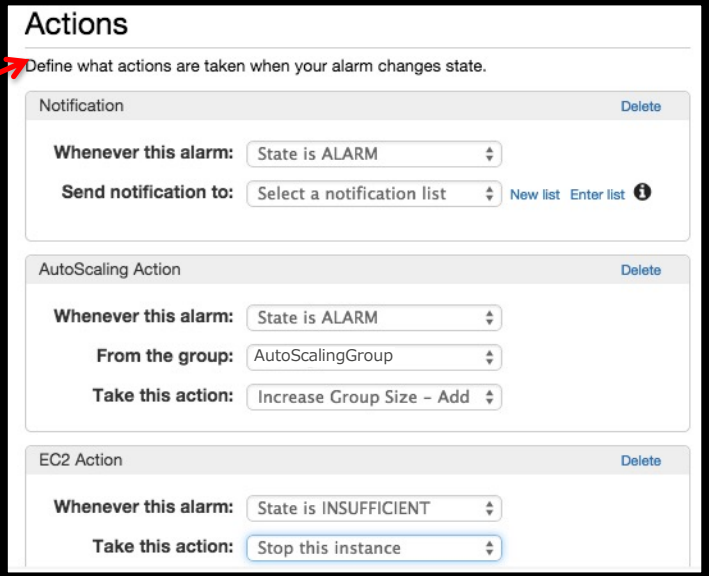
- メトリクス（e.g. CPU使用率）としきい値（e.g. 60%以上）で構成
- 3つのアラーム状態を管理
  - OK
    - メトリクスの値が、定義されたしきい値を下回っている
  - ALARM
    - メトリクスの値が、定義されたしきい値を上回っている
  - INSUFFICIENT_DATA
    - アラームが開始直後であるか、メトリクスが利用できないか、データが不足していていアラームの状態を判定できない
- 各アラーム状態に対してアクションを定義可能
  - 通知（Notification）
    - Amazon Simple Notification Service（SNS）を使って通知
    - メール送信やHTTP(S)送信、Amazon Simple Queue Service（SQS）への送信が可能
  - Auto Scalingアクション
    - Auto Scaling GroupのScaling Policyを指定し、インスタンスのスケールアウト／インが可能
  - EC2アクション
    - EC2インスタンスの停止およびTerminateが可能

Amazon CloudWatch 利用イメージ：アラーム設定

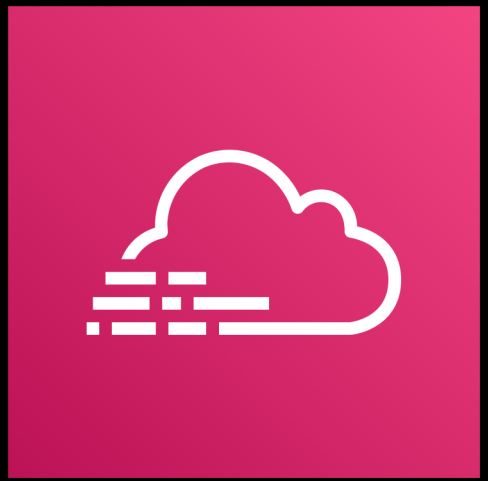
アラーム設定



アクション定義



AWS CloudTrail

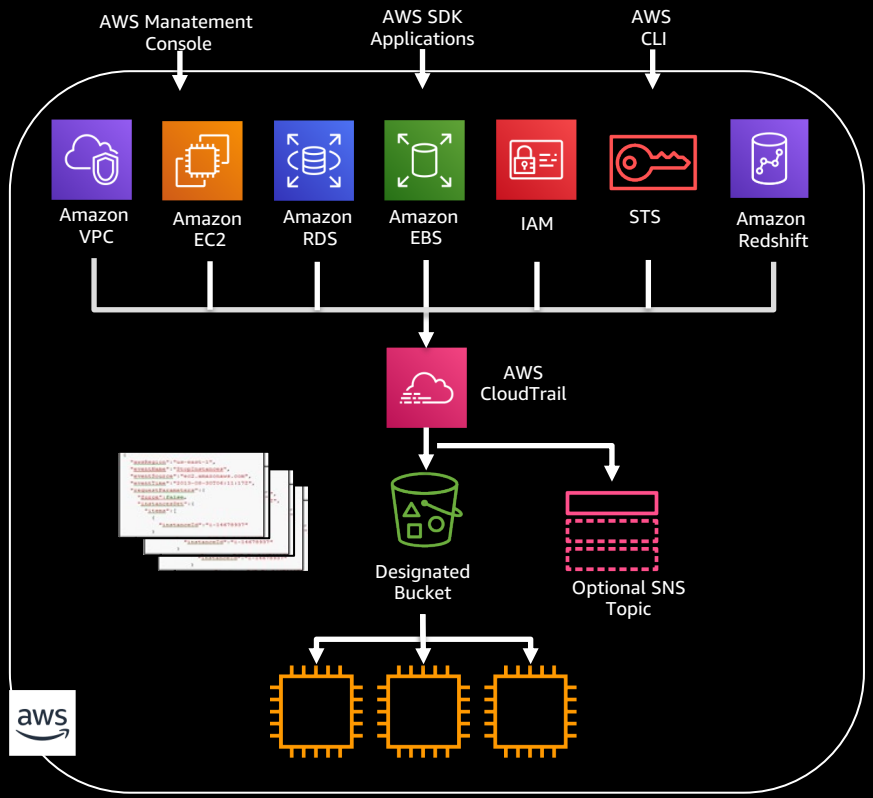


AWS CloudTrail

- **クラウド上のアクティビティを記録**
  - ユーザーのアクティビティをAPIレベルでトラッキング
- **安全**
  - ログファイルは**暗号化**され、gz 形式で堅牢な S3 に保存
- **無料**
  - 全てのアカウントで有効にすることを推奨
  - ログファイルの保存先となる **S3** や **CloudWatch Logs** の利用費用がかかる

AWS リソースに対する操作ログ

AWS CloudTrail でAWSのサービスに対する各種APIログを取得可能



- API を呼び出した身元（Who）
- API を呼び出した時間（When）
- API 呼び出し元の Source IP（Where）
- 呼び出された API（What）
- API の対象となる AWS リソース（What）
- 管理コンソールへのログインの成功・失敗

http://aws.amazon.com/jp/cloudtrail/

AWS CloudTrail にて監視すべきイベント例

CloudTrail ではサポートしている AWS サービスの操作のために使われた全ての API ログを取得しますが、どのようなログを監視するかについては監視要件に依存します。下記は代表的な重要イベントの例です。

Event	想定ケース
AttachInternetGateway AssociateRouteTable CreateRoute DeleteCustomerGateway DeleteInternetGateway DeleteRoute DeleteRouteTable DeleteDhcpOptions DisassociateRouteTable	• 意図せぬネットワーク構成の変更 • 未承認のインターネットゲートウェイの作成 • ルーティングの変更による未承認の経路の作成
CreateNetworkAcl CreateNetworkAclEntry DeleteNetworkAcl DeleteNetworkAclEntry ReplaceNetworkAclEntry ReplaceNetworkAclAssociation	• 意図せぬNetworkACLの変更 • 許されないポートの解放
RunInstances CreateInstances LaunchInstances TerminateInstances	• 未承認のEC2の作成 • 意図せぬEC2のTerminate

AWS CloudTrail にて監視すべきイベント例

Event	想定ケース
AuthorizeSecurityGroupIngress AuthorizeSecurityGroupEgress RevokeSecurityGroupIngress RevokeSecurityGroupEgress CreateSecurityGroup DeleteSecurityGroup	• 意図せぬ Security Group の変更 • 許されないポートの解放
StopLogging DeleteTrail UpdateTrail	• CloudTrail の停止/削除 • CloudTrail の設定変更
DeleteGroupPolicy DeleteRole DeleteRolePolicy DeleteUserPolicy PutGroupPolicy PutRolePolicy PutUserPolicy	• 許可されていない IAM ポリシーの削除 • 許可されていない IAM ポリシーの付与
Unauthorized* errorCode AccessDenied Failed authentication	• 許可されない操作の試行 • エラー
"type":"Root"	• AWS ルートアカウントでのログイン

AWS CloudTrail のよる監査ログ取得対象サービス※

対応サービス:

分析
- Amazon Elastic Map Reduce
- AWS Data Pipeline
- Amazon Kinesis Firehose
- Amazon Kinesis Streams
- Amazon Redshift
- Amazon Elasticsearch Service
- Amazon Machine Learning

アプリケーションサービス
- Amazon API Gateway
- Amazon Cloudsearch
- Amazon Elastic Transcoder
- Amazon Simple Email Service (Amazon SES)
- Amazon Simple Queue Service (Amazon SQS)
- Amazon Simple Workflow Service (Amazon SWF)

コンピューティング
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon EC2 Container Service (Amazon ECS)
- AWS Elastic Beanstalk
- AWS Lambda
- Auto Scaling
- Elastic Load Balancing (ELB)
- Amazon EC2 Container Registry (Amazon ECR)

データベース
- Amazon DynamoDB
- Amazon ElastiCache
- AWS Database Migration Service (AWS DMS)
- Amazon Relational Database Service (Amazon RDS)

開発者ツール
- AWS CodeDeploy
- AWS CodePipeline

エンタープライズアプリケーション
- Amazon WorkDocs
- Amazon WorkSpaces

モノのインターネット
- AWS IoT

ゲーム開発
- Amazon GameLift

管理ツール
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch Events
- Amazon CloudWatch Logs
- AWS Config
- AWS OpsWorks
- AWS Service Catalog

モバイルサービス
- Amazon Cognito
- AWS Device Farm
- Amazon Simple Notification Service （Amazon SNS）

ネットワーキング
- AWS Direct Connect
- Amazon Route 53
- Amazon Virtual Private Cloud

セキュリティとアイデンティティ
- AWS Certificate Manager
- AWS CloudHSM
- AWS Directory Service
- AWS Identity and Access Management (AWS IAM)
- Amazon Inspector
- AWS Key Management Service
- AWS Security Token Service
- AWS WAF

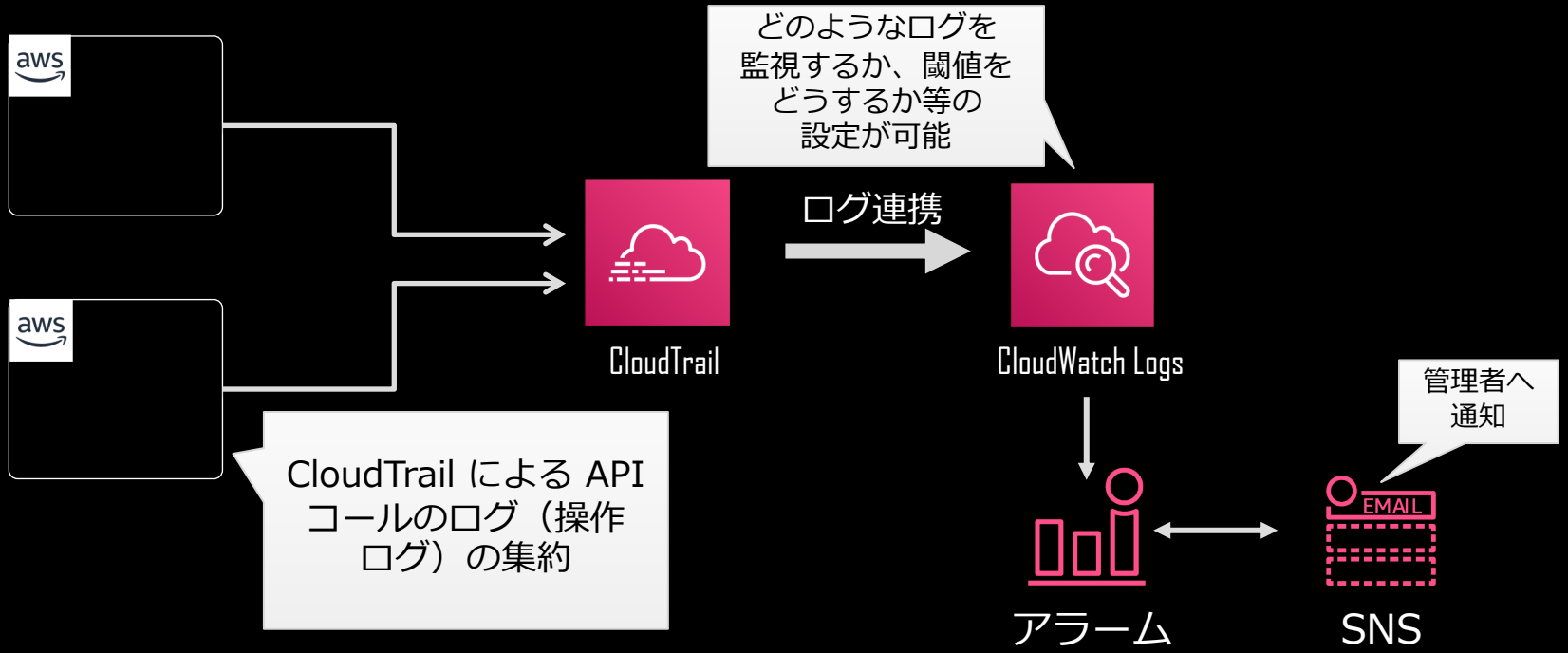
ストレージとコンテンツ配信
- Amazon CloudFront
- Amazon Elastic Block Store
- Amazon Simple Storage Service (Amazon S3)
- Amazon Elastic File System
- Amazon Glacier
- Amazon S3 bucket level events
- AWS Storage Gateway

サポート
- AWS Support

※ 最新情報は以下をご参照ください
http://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cloudtrail-supported-services.html

CloudTrail の CloudWatch Logs との連携

CloudTrail のログを CloudWatch Logs に転送し監視が可能

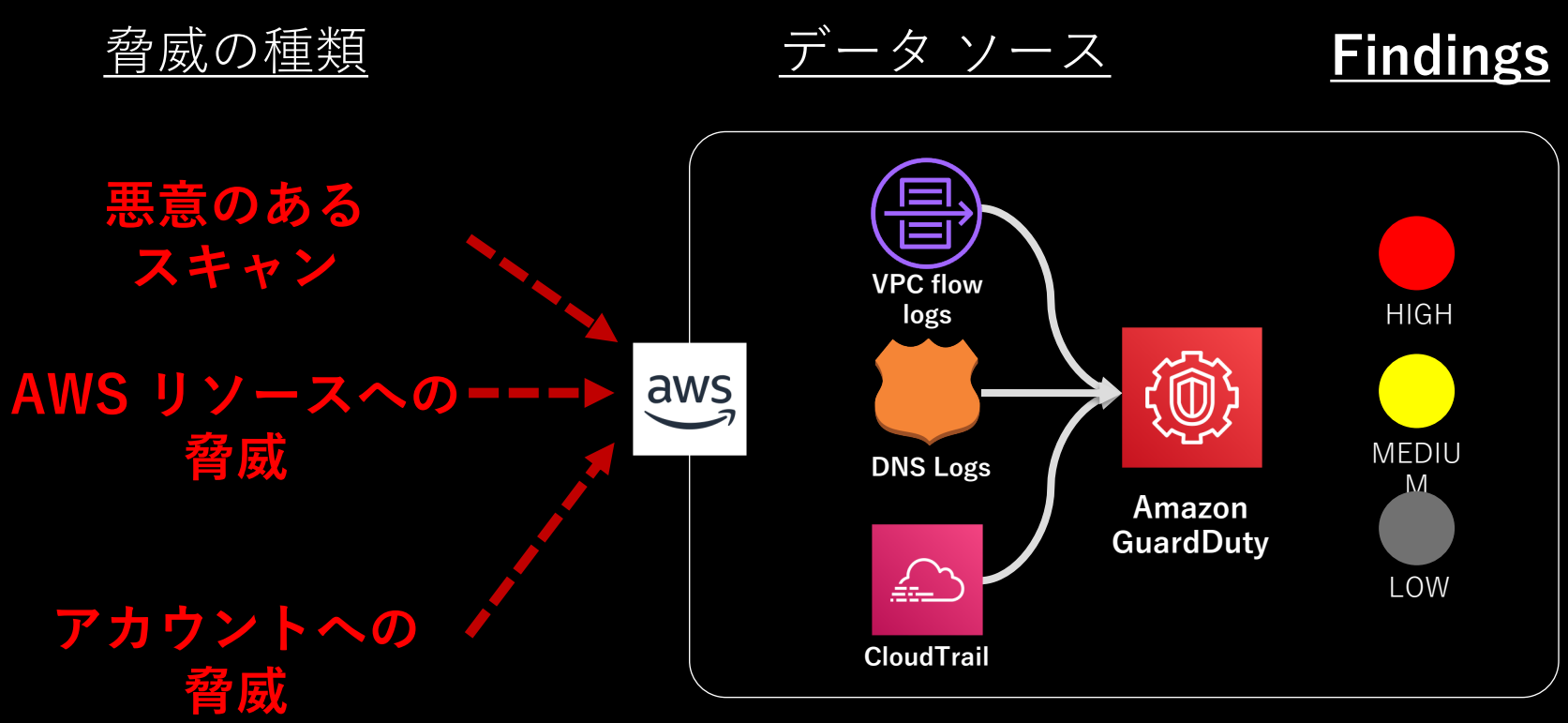


Amazon GuardDuty -マネージド型脅威検出サービス -

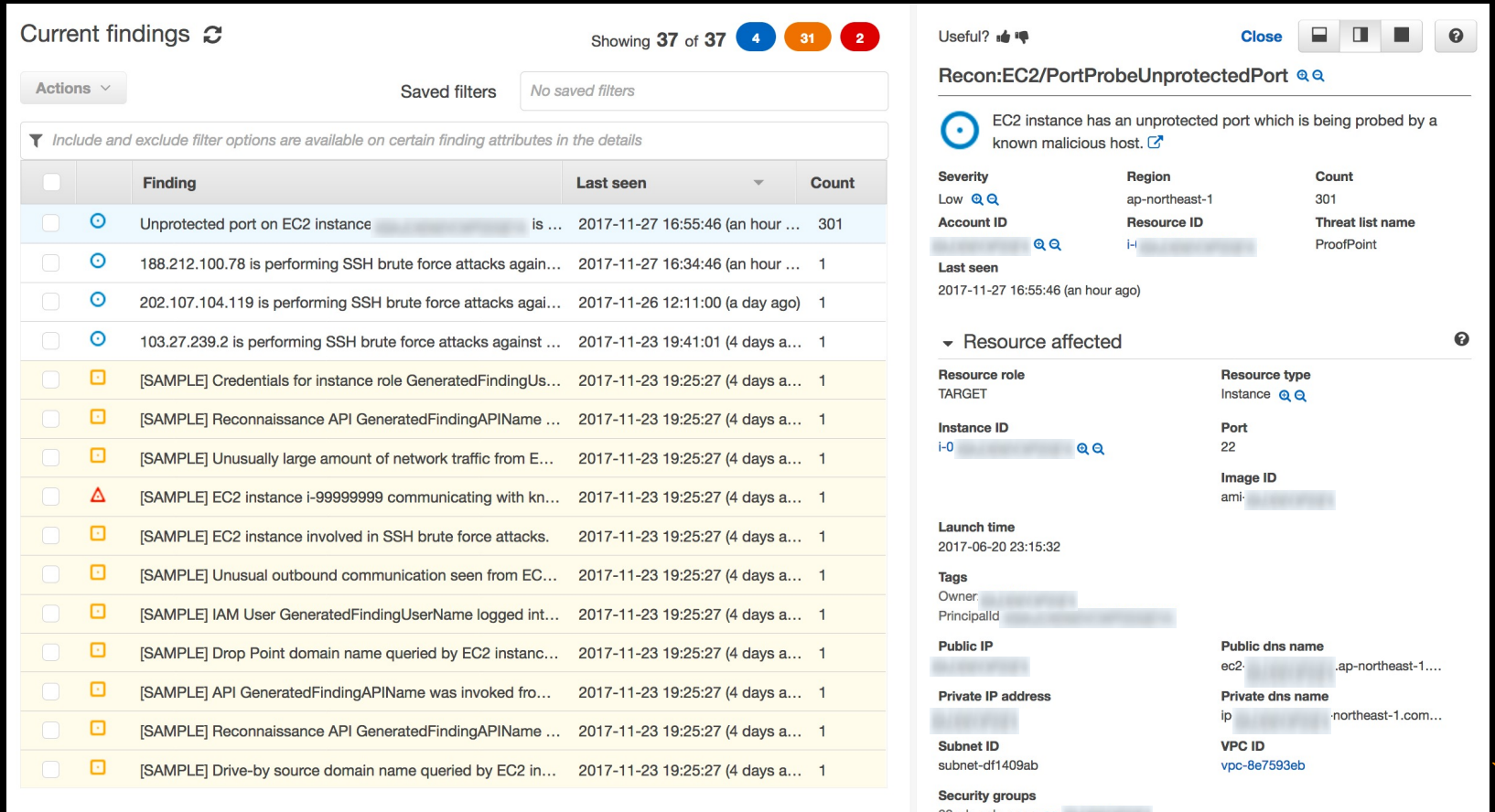
Amazon GuardDuty

- **脅威検出**
  - セキュリティの観点から
    セキュリティリスクを可視化・
    検知するAWS マネージドサービス
- **人的コストを削減**
  - 分析のソースには下記を利用し、
    メタデータの連続ストリームを分析
    - VPC Flow Logs
    - AWS CloudTrail Event Logs
    - DNS Logs
- **既知と未知の振る舞い検知**
  - 悪意のある IP アドレス、異常検出、
    機械学習などの統合脅威インテリジェンスを使用して脅威を認識

GuardDuty による脅威の検知と通知



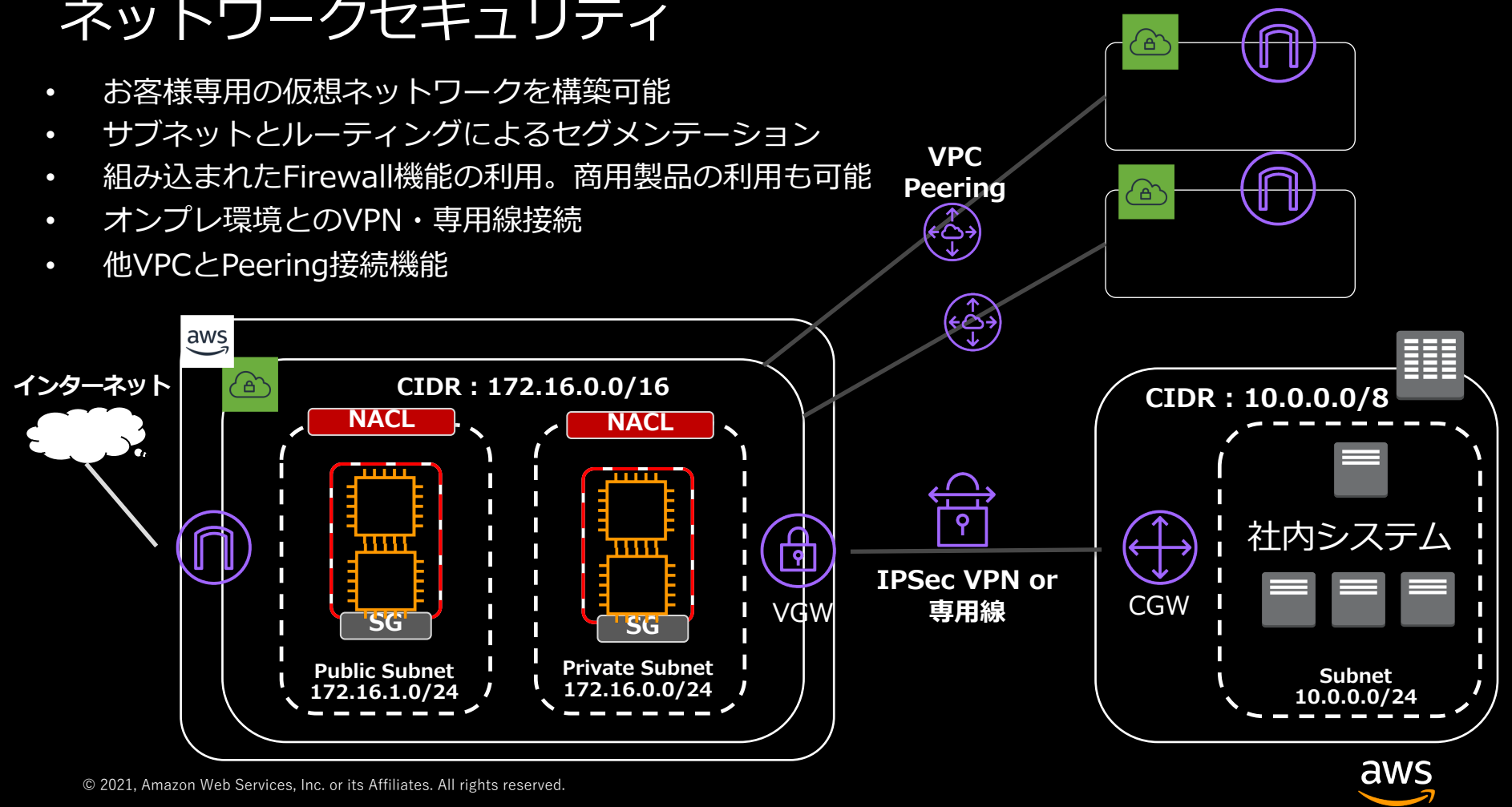
GuardDuty による脅威検出レポート



インフラストラクチャー保護

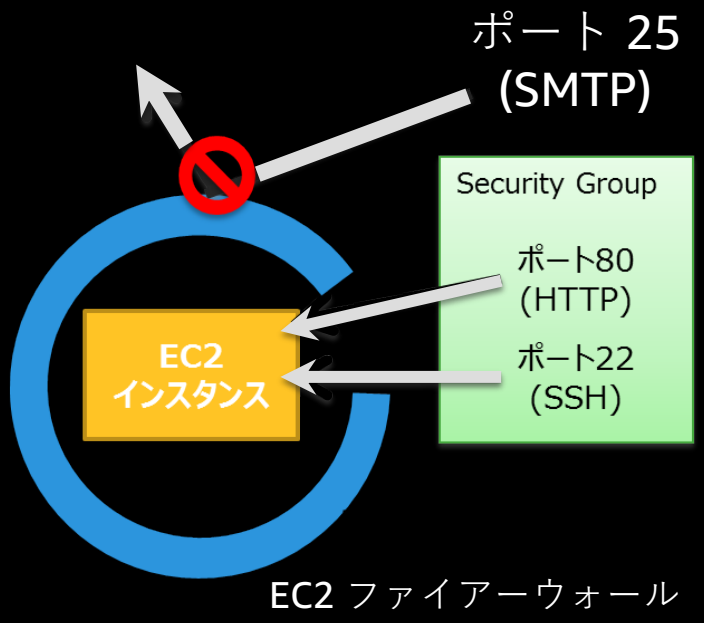
ネットワークセキュリティ

- お客様専用の仮想ネットワークを構築可能
- サブネットとルーティングによるセグメンテーション
- 組み込まれたFirewall機能の利用。商用製品の利用も可能
- オンプレ環境とのVPN・専用線接続
- 他VPCとPeering接続機能



セキュリティグループによるアクセスコントロール

各リソース間のアクセス制限にはセキュリティグループを利用しトラフィックを制限します。

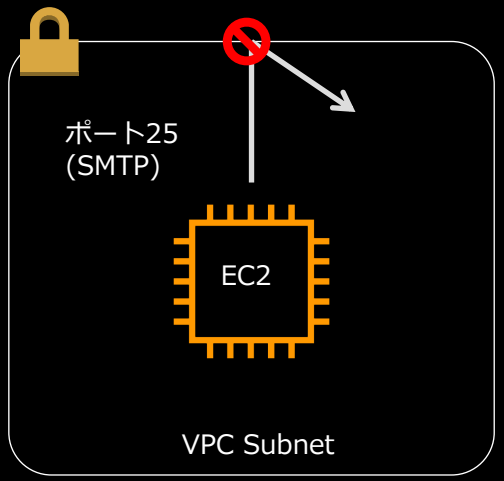


- 個別の仮想サーバへのトラフィックを制限します。
- インバウンドの制御、アウトバウンドの制御が可能です。
- デフォルトは全拒否。
- 必要な受信アクセスに対してアクセスルールを定義します。
  - プロトコル (TCP/UDP)
  - 宛先ポート
  - アクセス元IP / Security Group
- ルールをひとまとめにしたものをセキュリティグループと呼びます。
- 後から仮想サーバに異なるセキュリティグループに変更したり、複数のセキュリティグループを付与可能。即時反映されます。
- システムの通信要件を確認し、全公開（0.0.0.0/0）は極力避けるようにします。

VPC のセキュリティグループ
http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

ネットワーク ACL によるアクセスコントロール

サブネット単位でベースラインとなるポリシーを設定する場合にはネットワーク ACL を適用します。
（データベース群を設置するサブネット間の通信などでは、ACL で通信を相互に許可します）



- サブネットに一つだけ適用する ACL
- インバウンドの制御、アウトバウンドの制御が可能です。
- ベースラインのポリシーを設定するのに適しています
  - 例）このサブネットからは TFTP や SMTP の トラフィックは出ていかない
- サブネット間の通信のコントロールに適しています
  - 例）DMZ となるサブネットから直接 DB が 置かれているサブネットには通信できない
- シンプルなルール作りのためには VPC から出ていく方向のポリシーに使用を検討します。

ネットワークACL
http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_ACLs.html

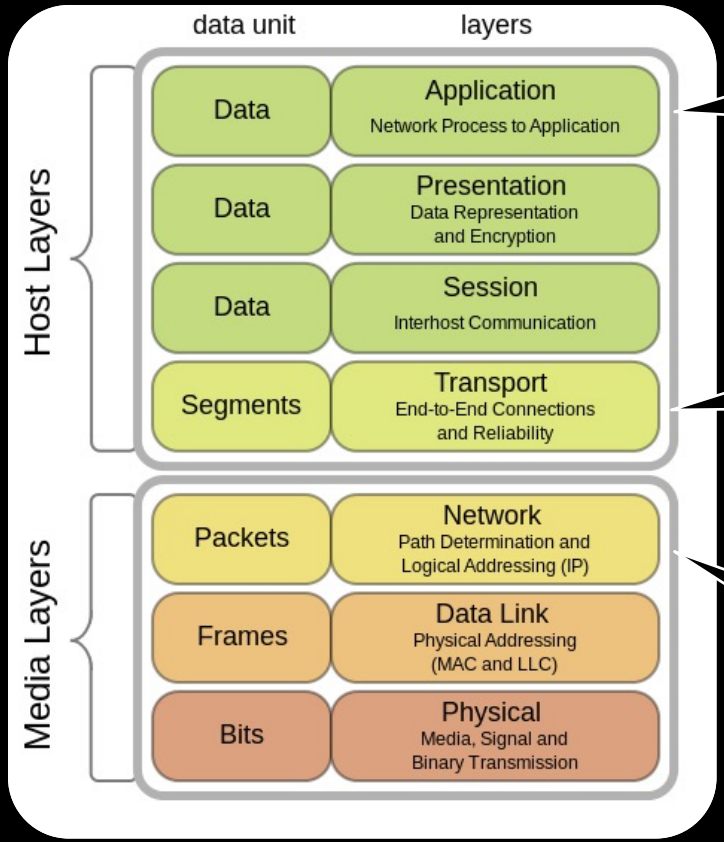
（参考）ネットワーク ACL とセキュリティグループ

セキュリティグループは、個別に許可するポート、Source、宛先を設定します。
拒否ルールをセキュリティグループで設定することはできないためその場合NACLの使用を検討します。

ネットワークACL	セキュリティグループ
各サブネットに設定	各インスタンス（ENI）に設定
ステートレス	ステートフル
AllowとDenyが設定可能（BlackListの作成が可能）	Allowのみ設定（WhiteListの作成が可能） デフォルトDeny
ルール順番通りに処理される	全てのルールが検証される
• ベースラインのポリシーを設定するのに適している 例）このサブネットからはTFTPやSMTPのトラフィックは出ていかない • サブネット間の通信のコントロールに適している 例）DMZとなるサブネットから直接DBが置かれているサブネットには通信できない • ネットワーク担当とサーバー担当の権限分掌にも利用可能	• サーバーの機能に応じたルールの作成 例）SMTPサーバー向けのSG • 用途に応じたルールの作成 例）管理用トラフィックのためのSG

VPC のセキュリティ
http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_Security.html

DDoS 攻撃の種類



アプリケーション層攻撃

一見、適切に構成されているが悪意のある要求を使用して、アプリケーションリソースを消費する
(例： HTTP GET, DNS クエリフラッド)

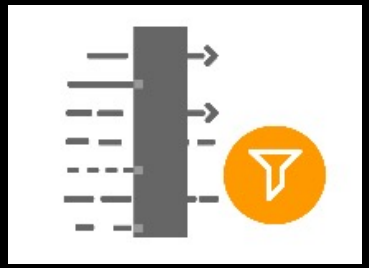
状態枯渇攻撃

ファイヤウォールや、IPS,ロードバランサなどの状態を管理しなければならないプロトコルに負荷をかける
(例：TCP SYN フラッド)

ボリューム攻撃

処理出来る能力を超えたトラフィックを送りつける
(例：UDP 反射攻撃)

AWS WAF – Layer 7 application protection



カスタムルールによる
Webトラフィック
フィルタ

悪意のあるリクエストの
ブロック

アクティブな監視と
チューニング

AWS Shield Standard

AWS Shield Standard

Layer 3/4 防御

✓ すべてのインターネットに面したAWSのサービスに対してネットワークレイヤーとトランスポートレイヤーに対するDDoS攻撃を防御

AWS WAF

Layer 7 防御 / AWS WAF

✓ ルールを利用したWeb層への攻撃の防御

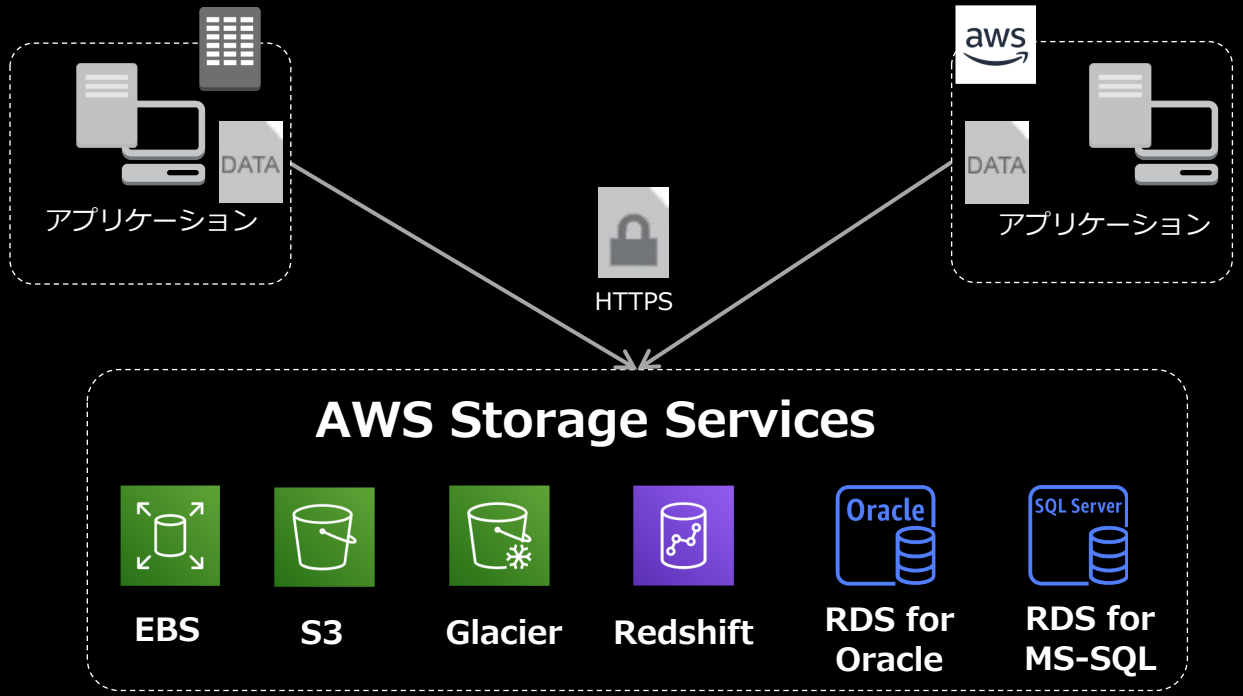
✓ レートコントロールを利用したWeb層へのDDoS攻撃を防御

データ保護

暗号化手法の特徴と選択肢

暗号化処理	鍵の保管	鍵の管理	管理負荷	AWSサービス	ユースケース
利用者環境（CSE）	利用者	利用者	最高	クライアント側で全て実施するため特に限定なし	• End to Endで暗号化と鍵の統制を完全に利用者の統制下に置く必要のあるデータの保護
利用者環境（CSE）	AWS	利用者	高	CSE with KMS CSE with CloudHSM	• 鍵の保管についてはAWSが提供するサービスの利用を許容できる • 暗号/復号化できる利用者を限定するなど，暗号鍵管理の統制は利用者側で実施
AWS環境（SSE）	AWS	利用者	中	SSE with KMS SSE with CloudHSM	• AWSのDCからのストレージ盗難・紛失というリスクには対応可能 • 暗号鍵の生成やローテーションといった管理はユーザー側で統制を行いたい場合
AWS環境（SSE）	AWS	AWS	低	SSE（S3, EBS, RDS, Redshift, Glacier)	• AWSのDCからのストレージ盗難・紛失というリスクには対応可能 • AWSが鍵管理を実施することを許容できる • 暗号に関する利用者の負荷は最も軽い

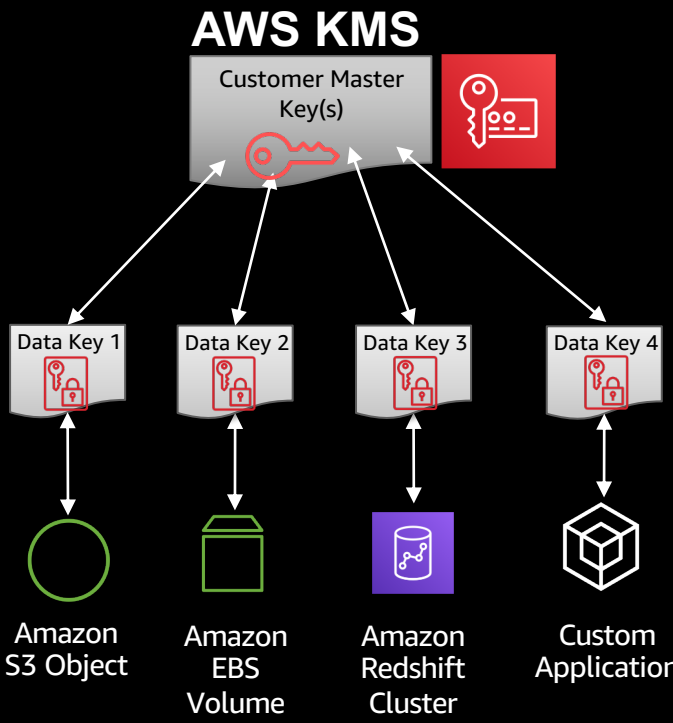
AWS のサーバーサイド暗号化（SSE）



- S3, EBS and Redshift・・・サーバーサイド暗号化のオプションあり
- Glacier・・・全てのデータが標準で暗号化
- RDS for Oracle and Microsoft SQL・・・TDE（Transparent Data Encryption）機能で暗号化

AWS Key Management Service (KMS)

フルマネージドの暗号鍵管理サービス



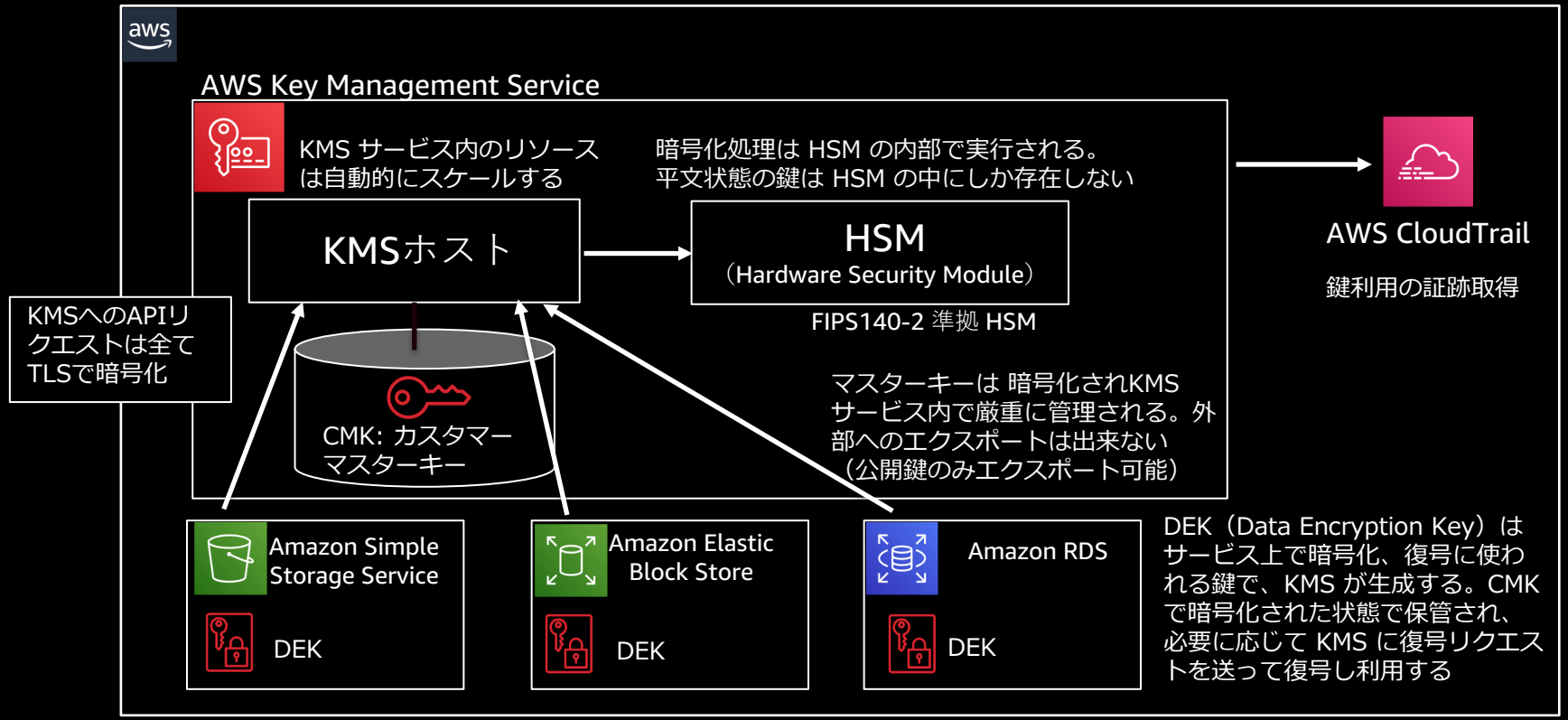
特徴 (http://aws.amazon.com/jp/kms/)

- 暗号鍵の管理を一元化
- 鍵の機密性、可用性を確保
- アクセスニーズに合わせて自動的にスケール
- 様々な AWS サービスとのインテグレーション

価格体系 (http://aws.amazon.com/jp/kms/pricing/)

- 1 つの鍵につき月間 $1 で利用可能
- API リクエストは 10,000 リクエストごとに $0.03
- 20,000 リクエストまでは無料

AWS KMS と AWS サービスの連携



※ KMS と連携して CMK を利用した暗号化ができるサービスは上記 3 種類以外にも多数ある

(参考) データセキュリティ

CloudHSM を用いた暗号化

専用ハードウェアアプライアンス

高いコンプライアンス要求に対応

AWS Key Management Service

暗号鍵は AWS 上に Secure に保管、管理は User にて実施

SDK と連携することで、3rd Party製ソフトにも適応可能

オンプレミスからの利用も可能

User による暗号鍵の持ち込みによる暗号化

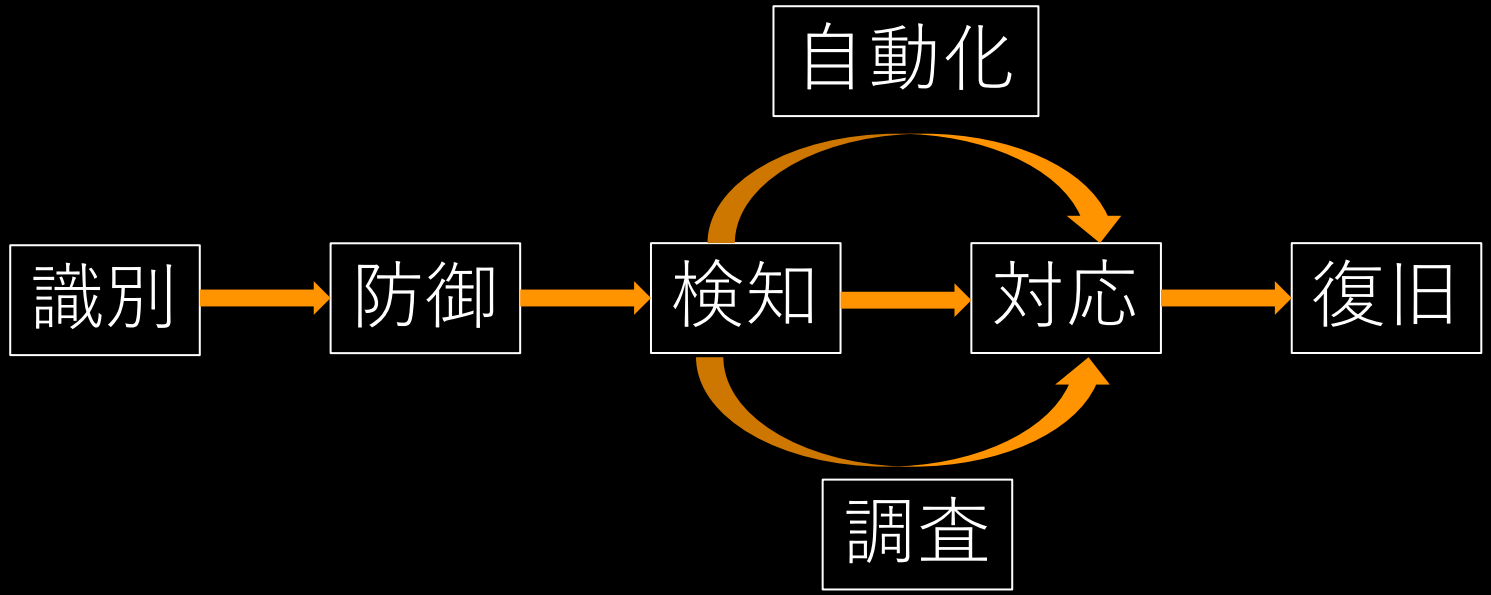
暗号化の範囲指定、暗号化鍵のローテーション等、実行管理がユーザで実施

S3、EBS 等に実装されたAWSによる暗号化（**AWS による鍵管理**）

ユーザが暗号化鍵に対するコントロールをもっていない

インシデントレスポンス

セキュリティレスポンスの自動化 (NIST CSF)



NIST CSF に基づいた AWS サービスの活用

脅威検知: 通知/トリガー

AWS Config rules

継続的にリソース変更を監視し
定義ルールへの準拠状況を通知

Amazon CloudWatch Events

AWSリソースの変更イベントを
ニアリアルタイムで通知

脅威対応

AWS Lambda

アプリケーションやバックエンドサービスのコードを自動実行

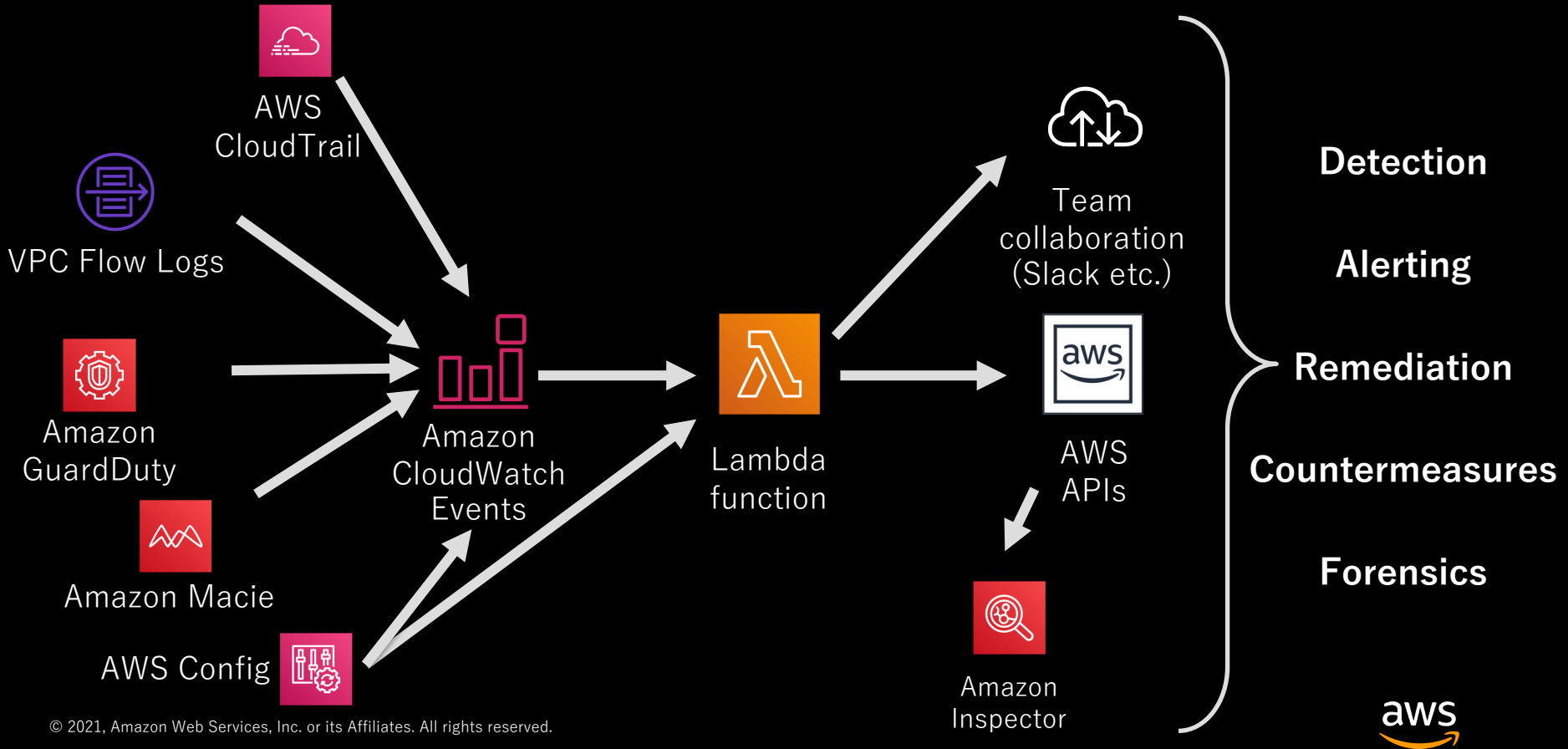
AWS Systems Manager

AWSリソースに関する運用情報取得や実行

Amazon Inspector

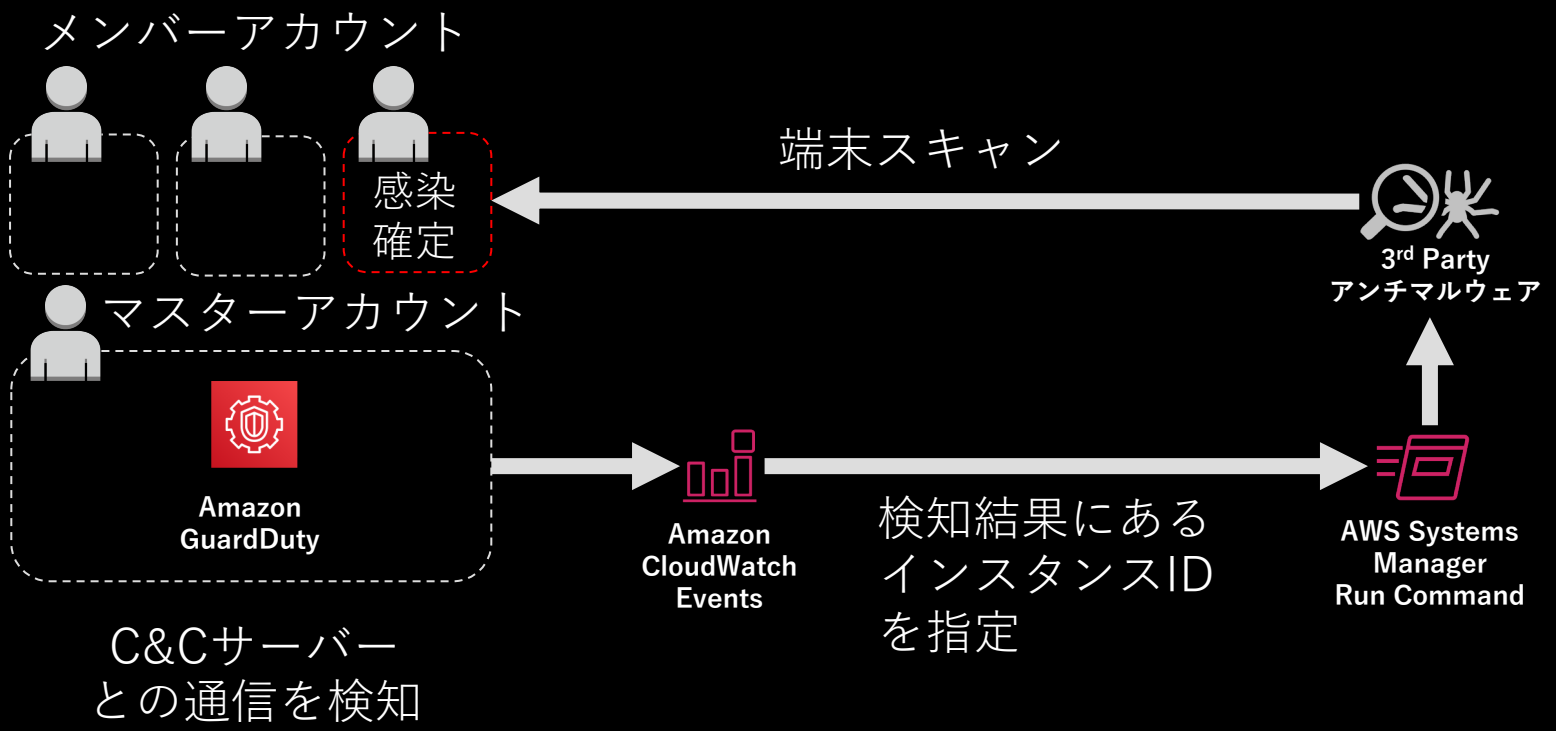
EC2 インスタンスへの自動セキュリティ評価

セキュリティオートメーションの流れ



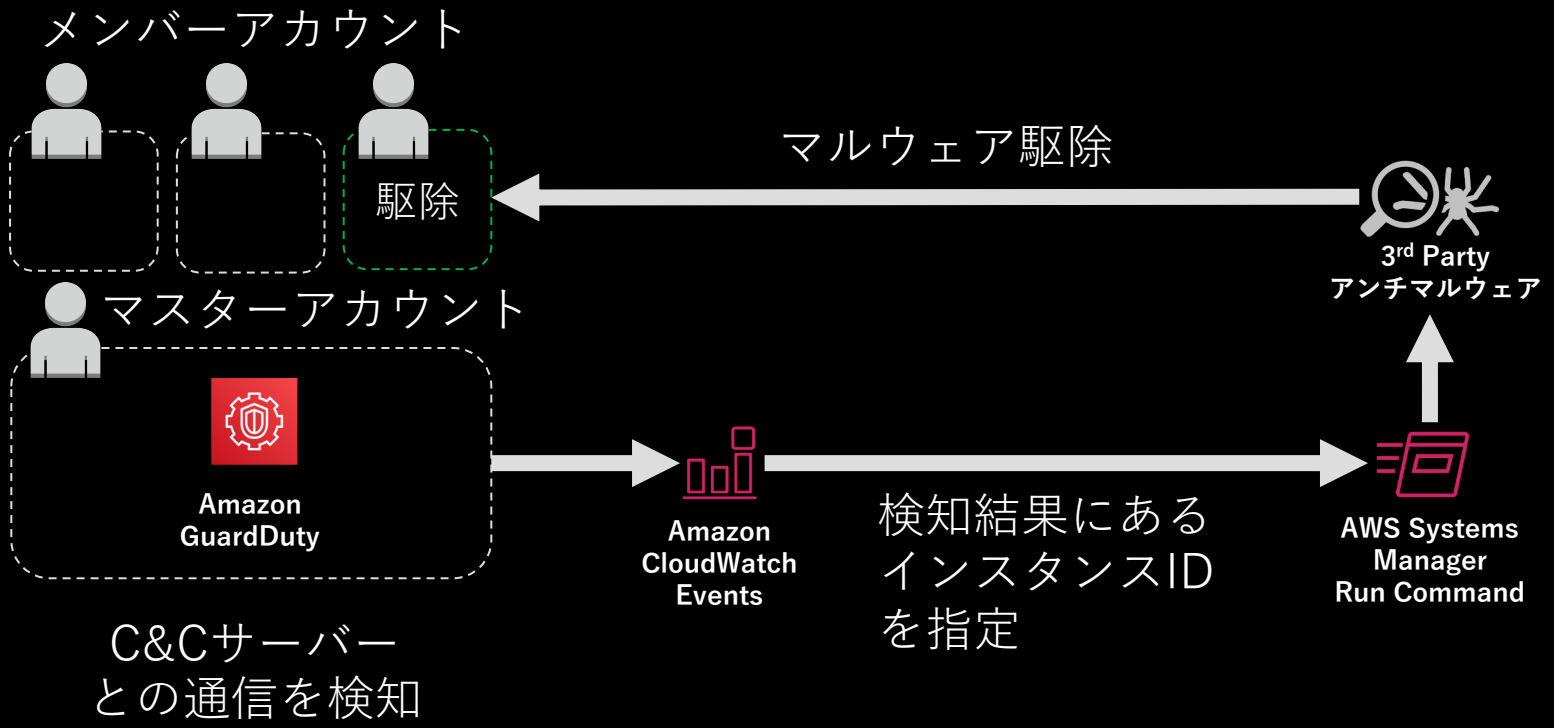
EC2 インスタンスの端末感染検知

感染端末の初期対応



EC2 インスタンスのマルウェア駆除

感染端末のマルウェア駆除



まとめ

まとめ

- 責任共有モデルに基づき、
  実施すべきセキュリティ対策を検討する

- Amazon EC2 において、
  最低限実施すべきセキュリティベストプラクティス：
  - ID とアクセス管理：インスタンスの保護, IAM ロール
  - 検出：CloudWatch, CloudTrail, GuardDuty
  - インフラストラクチャー保護：ネットワーク ACL, セキュリティグループ, AWS WAF, AWS Shield
  - データ保護：AWS KMS
  - インシデントレスポンス：Amazon CloudWatch Events, AWS Systems Manager

Thank you!