AWS

SUMMIT

AWS で実現する セキュリティ・オートメーション

桐山隼人
セキュリティソリューションアーキテクト
アマゾン ウェブ サービス ジャパン株式会社
2017年6月1日

amazon web services

自己紹介

氏名

- 桐山 隼人

役割

- セキュリティソリューションアーキテクト

関心事

- Security *by* the Cloud
- Security Automation
- Cloud SOC/CSIRT
- IoT Security

@hkiriyam1

本セッションのポイント

- オートメーションは戦略策定の礎
- セキュリティ・オートメーションを前提に設計されたAWSサービス
- セキュリティ戦略基盤となるAWSクラウド環境

オートメーションは戦略策定の礎

何のためのオートメーションなのか？

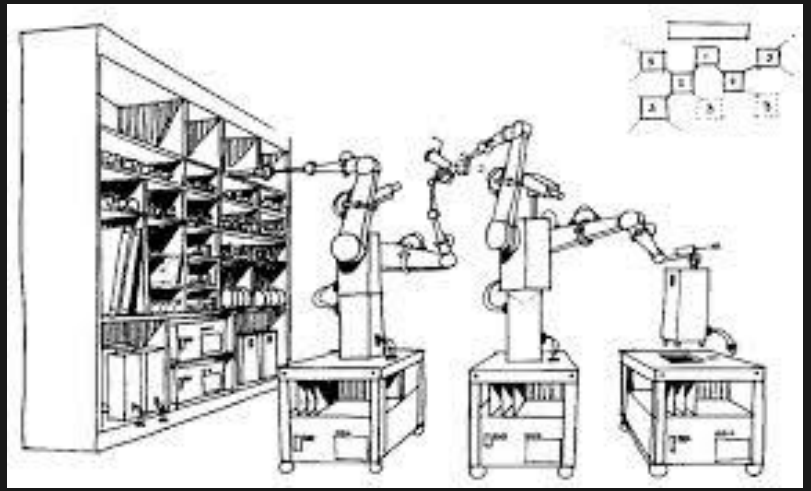
オートメーションとは

「自動化」のこと (Wikipedia)

オートメーションとは

「自動化」のこと (Wikipedia)

ある機構や機器が、人手の介入を要することなく、自動的に制御、動作、連携すること (IT用語辞典)



「自動化」によって得られる効率化

コスト削減　生産性向上　スピード向上　人為ミス削減

効率化だけではない価値

セールスフォースオートメーション

営業プロセスの効率化
✓ 報告作業の省力化
✓ 顧客情報データの共有

▼

営業活動の革新
✓ 分析による案件確度判断
✓ 見込み客への集中

効率化だけではない価値

セールスフォースオートメーション

営業プロセスの効率化
- ✓ 報告作業の省力化
- ✓ 顧客情報データの共有

▼

営業活動の革新
- ✓ 分析による案件確度判断
- ✓ 見込み客への集中

マーケティングオートメーション

マーケティングの効率化
- ✓ リード獲得漏れ防止
- ✓ ナーチャリング手段確立

▼

マーケティング活動の革新
- ✓ 案件化率の高いリードの判別
- ✓ 案件化に至るリソース最適化

効率化だけではない価値

セールスフォースオートメーション	マーケティングオートメーション
営業プロセスの効率化 ✓ 報告作業の省力化 ✓ 顧客情報データの共有	**マーケティングの効率化** ✓ リード獲得漏れ防止 ✓ ナーチャリング手段確立
▼	▼
営業活動の革新 ✓ 分析による案件確度判断 ✓ 見込み客への集中	**マーケティング活動の革新** ✓ 案件化率の高いリードの判別 ✓ 案件化に至るリソース最適化

「やること」と「やらないこと」を決められる = 戦略

オートメーションがもたらすもの

多種多様なデータ集約	可視化と効果測定	分析による意思決定
オートメーション		

このプロセスを継続することで良い戦略が策定できる

セキュリティ・オートメーションを前提に設計されたAWSサービス

何を自動化すべきなのか？

セキュリティ対策の分類

- 対策主体による分類
  - 人による対策・組織による対策・技術による対策
- 対策対象による分類
  - サーバー対策・ネットワーク対策・クライアント対策
- 対策場所による分類
  - 入口対策・内部対策・出口対策

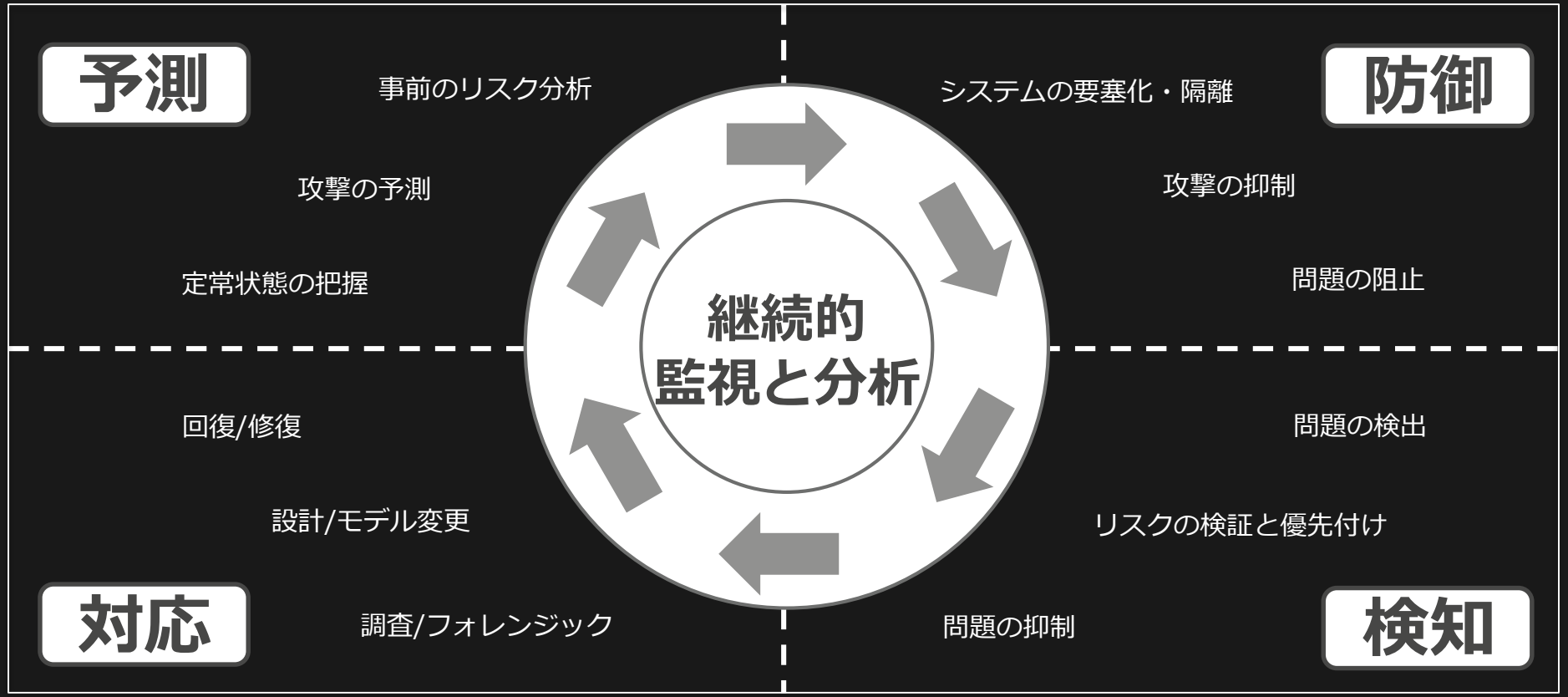
セキュリティ対策の分類

- 対策主体による分類
  - 人による対策・組織による対策・技術による対策
- 対策対象による分類
  - サーバー対策・ネットワーク対策・クライアント対策
- 対策場所による分類
  - 入口対策・内部対策・出口対策

・・・などがあるが、オートメーションを意識したプロセス・継続性を表現できる分類な何か？

適応型セキュリティアーキテクチャ

Gartner’s Adaptive Security Architecture



「防御」の考慮点

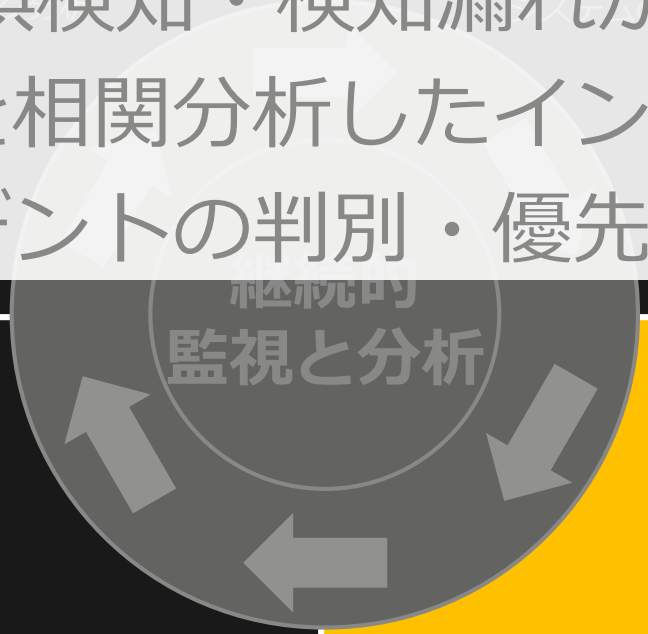
Gartner’s Adaptive Security Architecture

- 従来、セキュリティ対策と言われていたもの
- 標的型攻撃の台頭で100%防御は不可能

「検知」の考慮点

Gartner’s Adaptive Security Architecture

- 高い検知精度(誤検知・検知漏れが少ない)
- 各種イベントを相関分析したインシデント特定
- 重要なインシデントの判別・優先順位づけ



回復/修復

設計/モデル変更

対応

調査/フォレンジック

問題の検出

リスクの検証と優先付け

問題の抑制

検知

「対応」の考慮点

Gartner’s Adaptive Security Architecture

- 一次対応の早さ = 損害額の最小化
- 事後調査を意識したログ設計
- 恒久的な対応は仕組み化して事故の再発防止

回復/修復

設計/モデル変更

対応

調査/フォレンジック

問題の検出

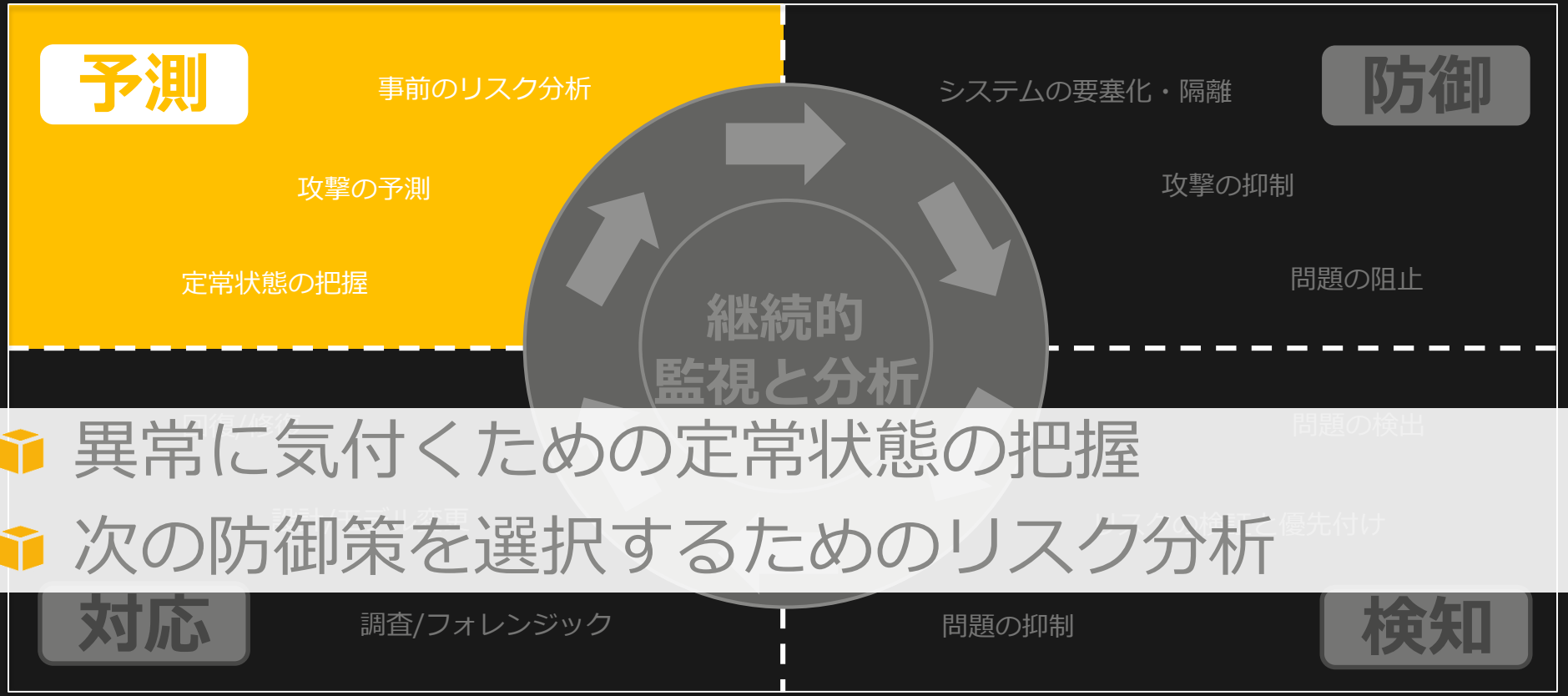
リスクの検証と優先付け

問題の抑制

検知

「予測」の考慮点

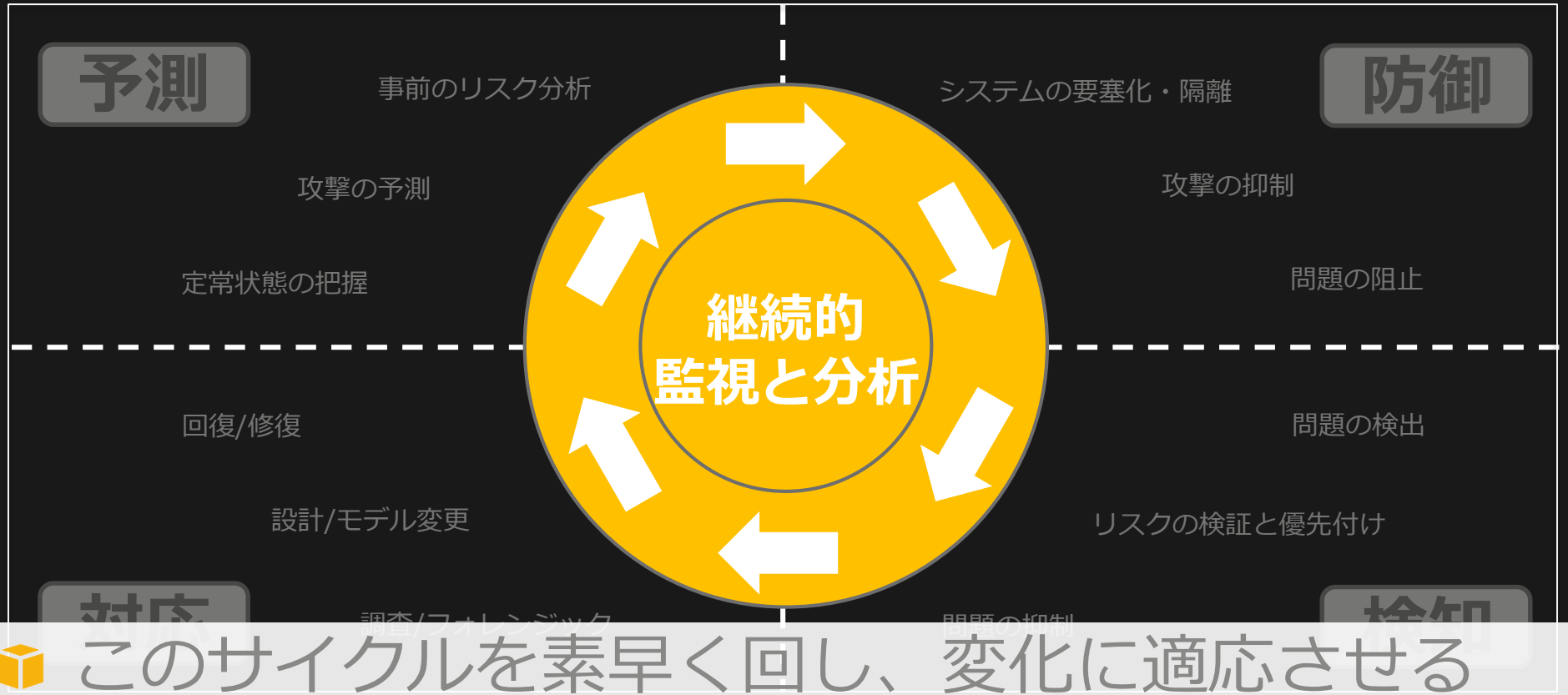
Gartner’s Adaptive Security Architecture



- 異常に気付くための定常状態の把握
- 次の防御策を選択するためのリスク分析

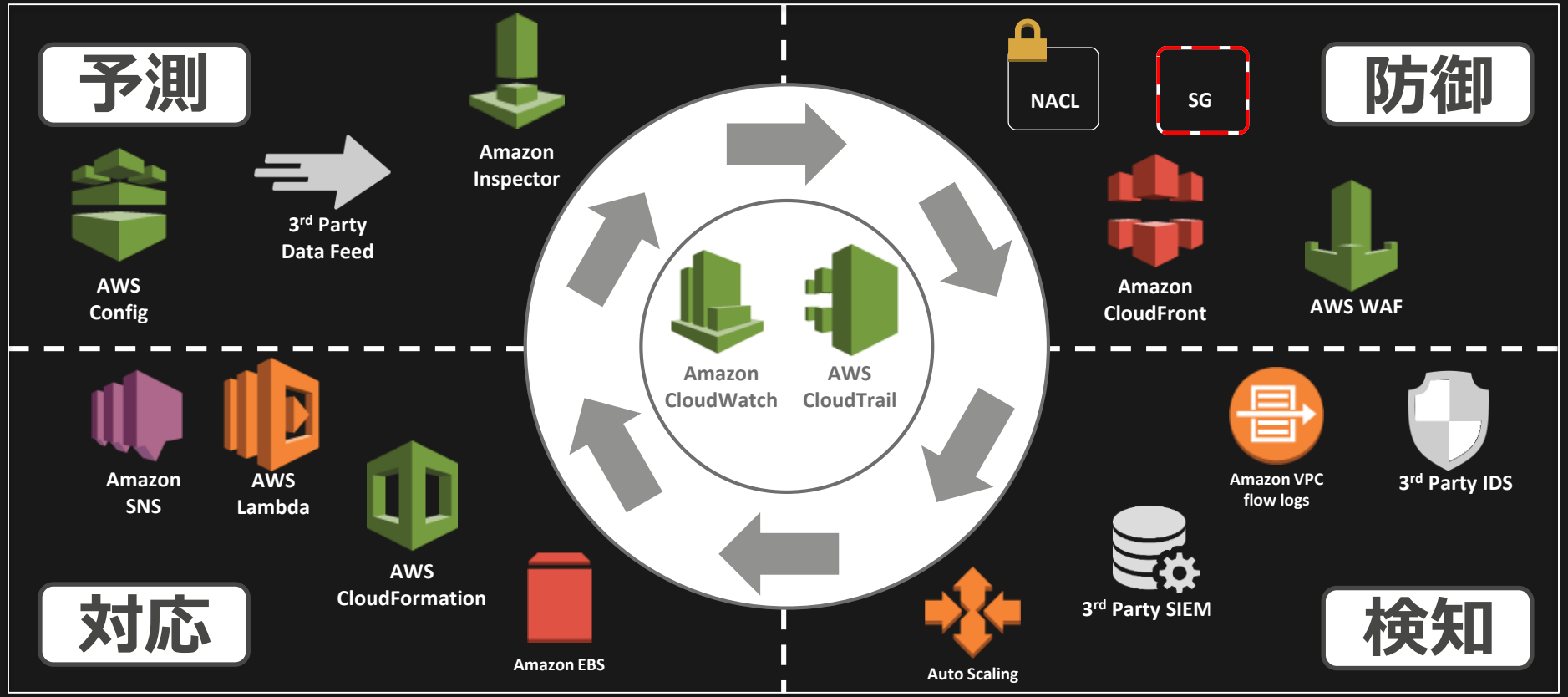
「継続的監視と分析」の考慮点

Gartner’s Adaptive Security Architecture

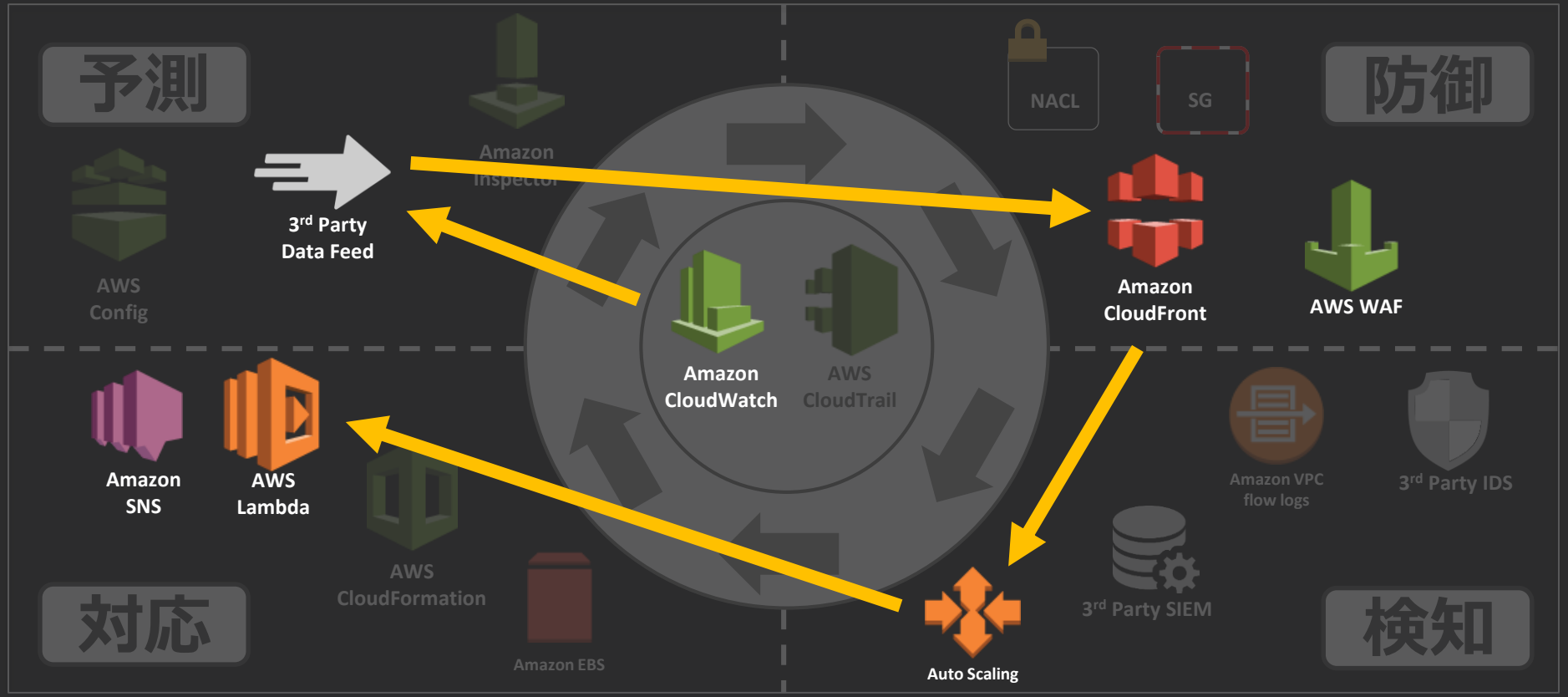


このサイクルを素早く回し、変化に適応させる

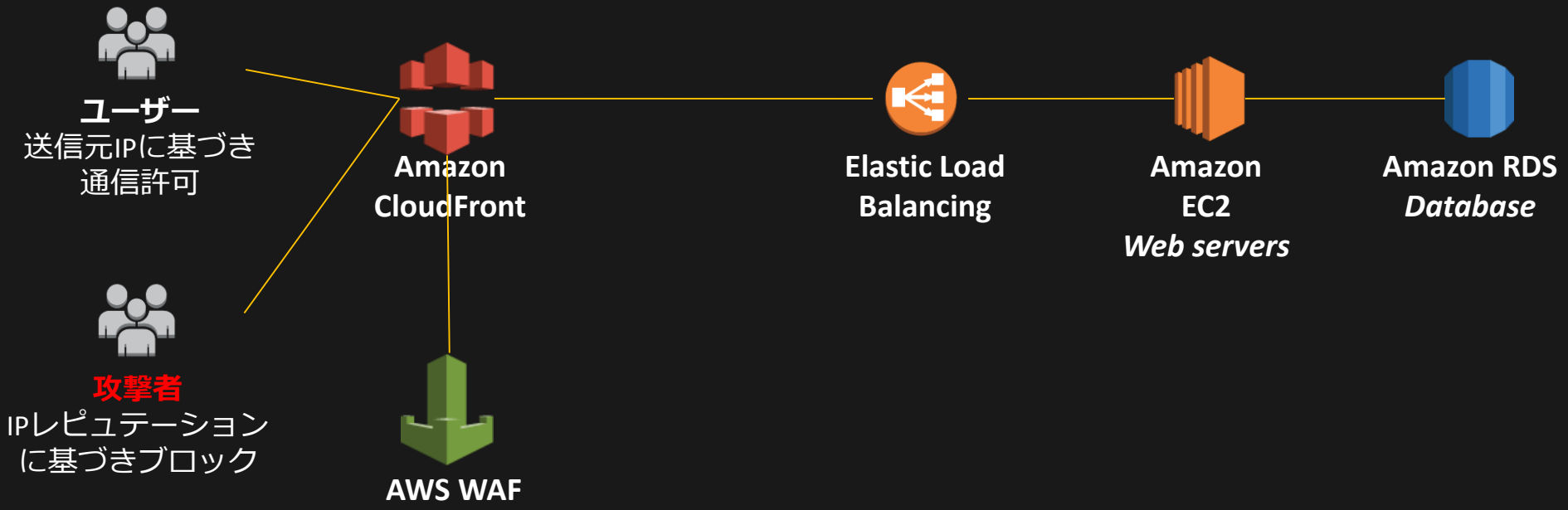
AWSサービスのマッピング



不正通信を起点とした入口対策フロー例

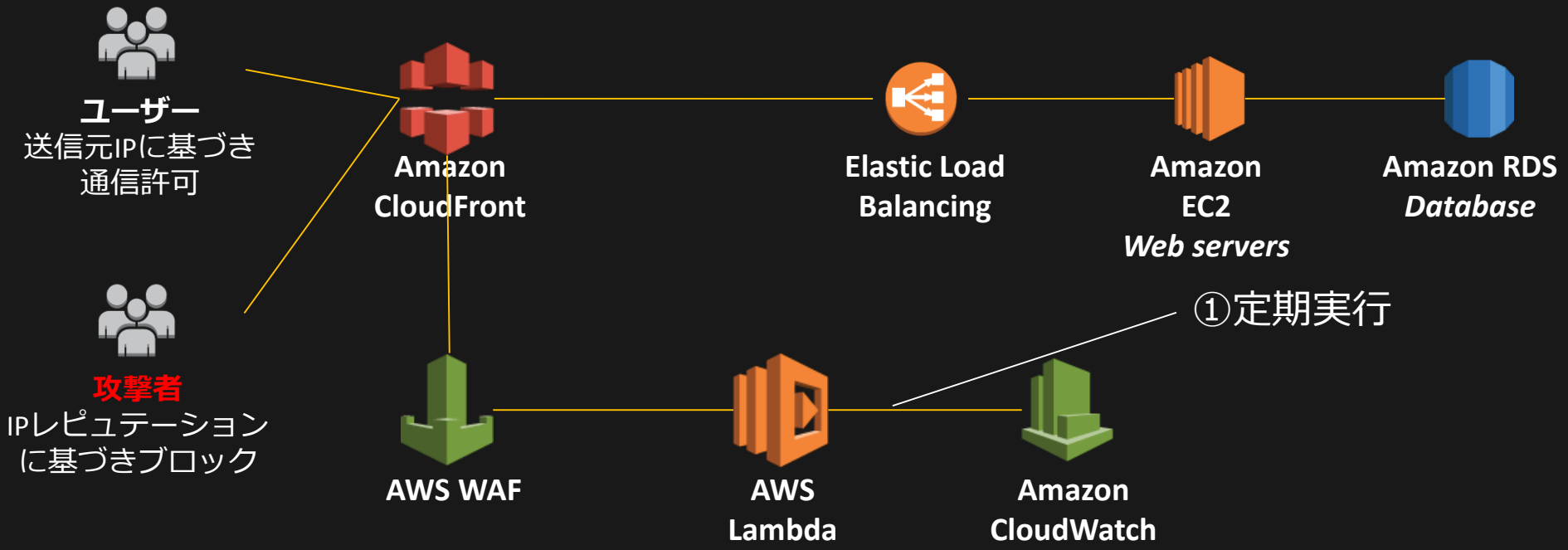


IPブラックリストをAWS WAFに自動反映



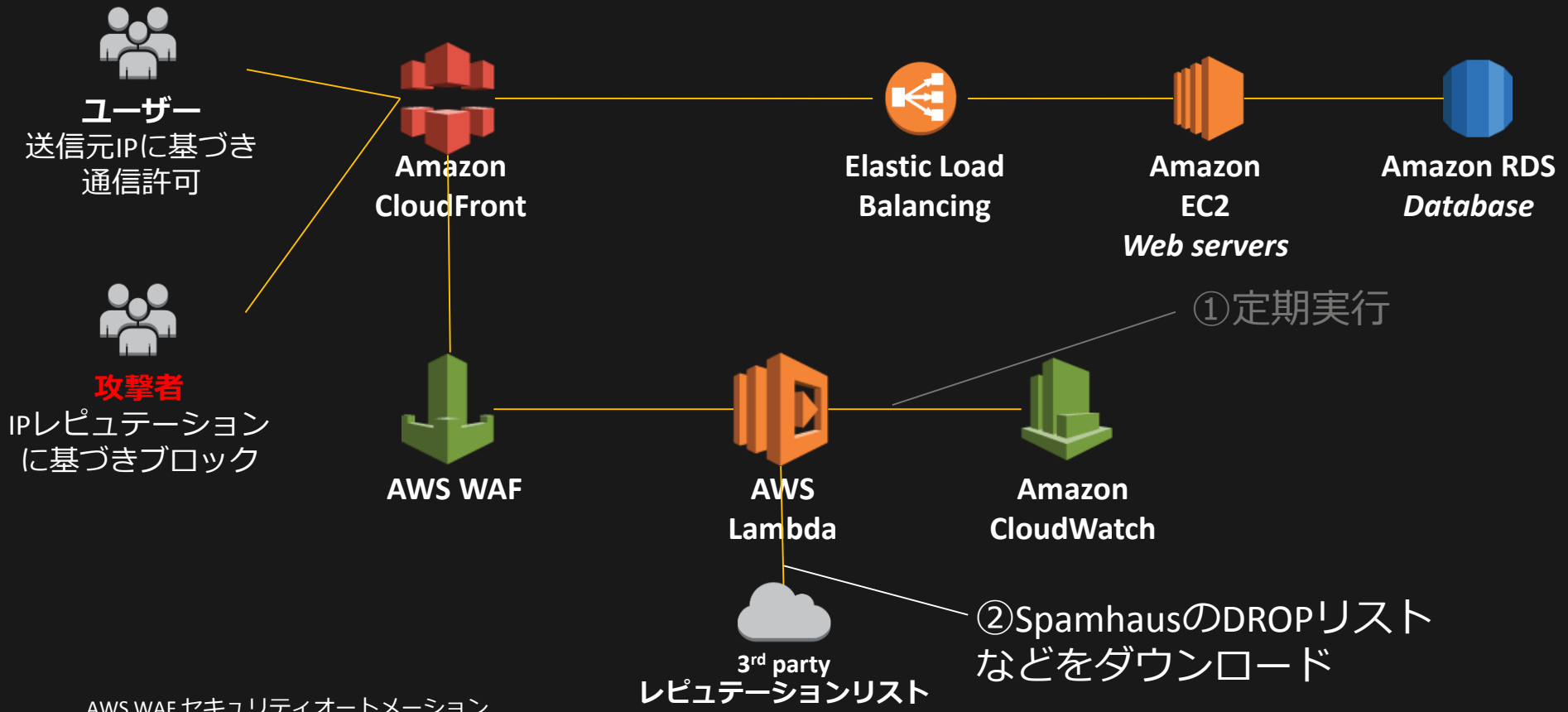
AWS WAF セキュリティオートメーション
https://aws.amazon.com/jp/answers/security/aws-waf-security-automations/

IPブラックリストをAWS WAFに自動反映



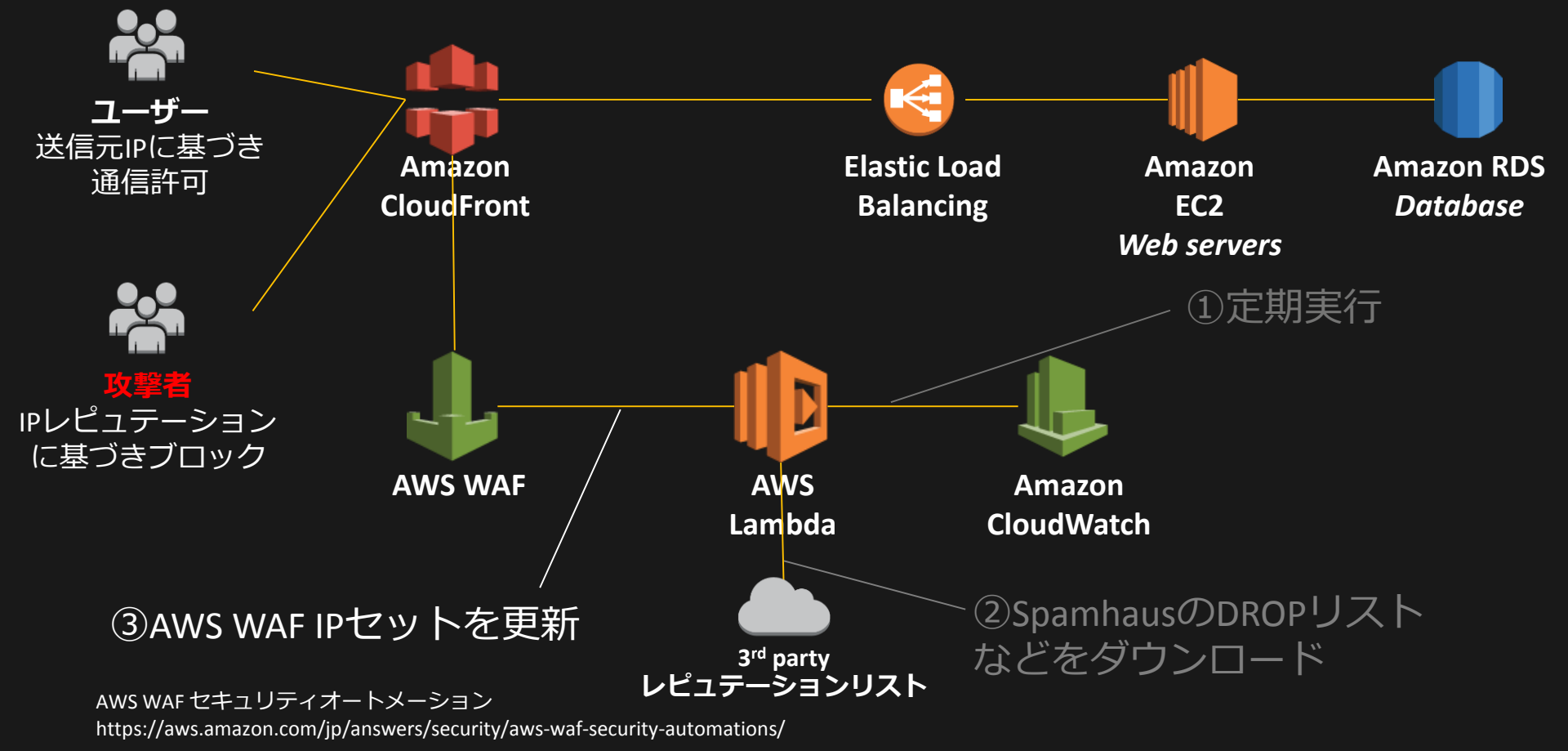
AWS WAF セキュリティオートメーション
https://aws.amazon.com/jp/answers/security/aws-waf-security-automations/

IPブラックリストをAWS WAFに自動反映



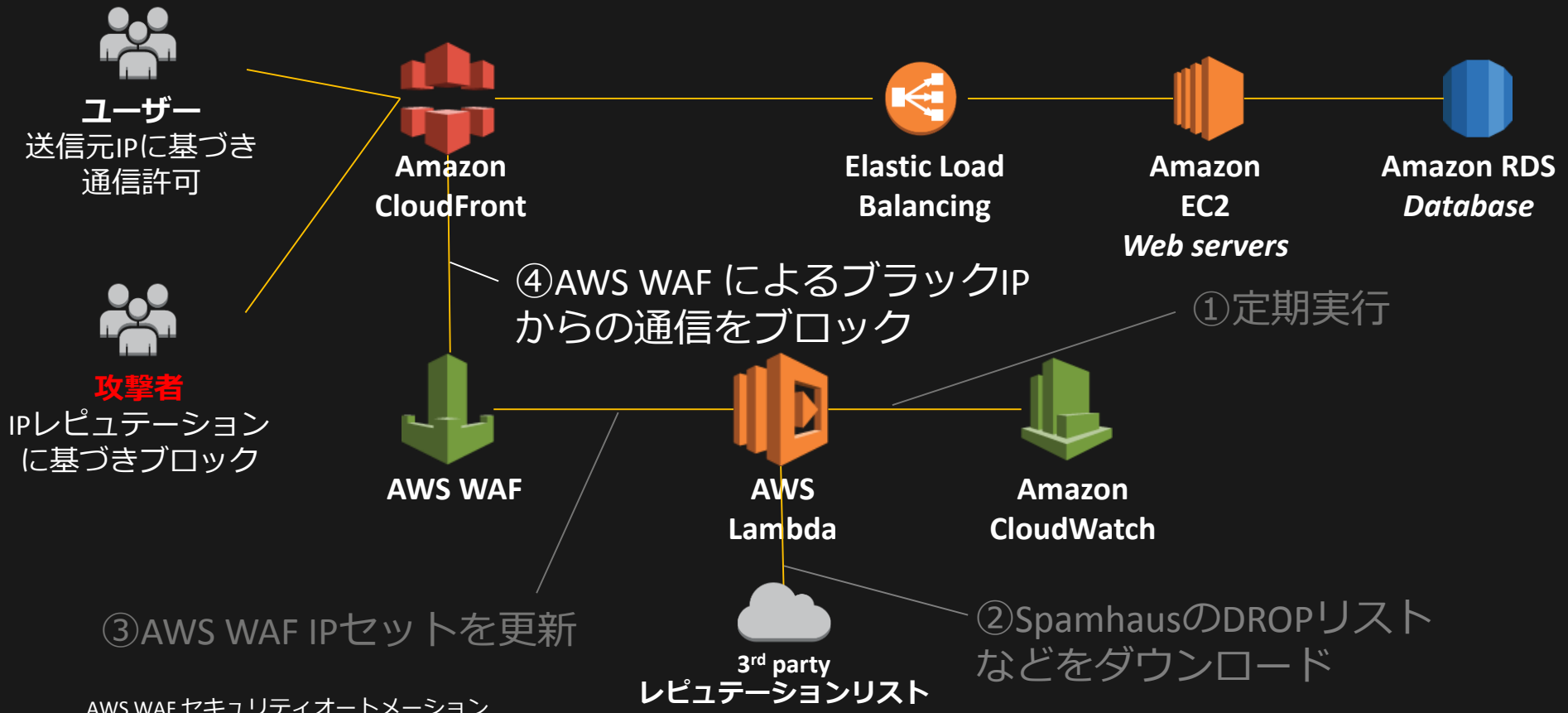
AWS WAF セキュリティオートメーション
https://aws.amazon.com/jp/answers/security/aws-waf-security-automations/

IPブラックリストをAWS WAFに自動反映



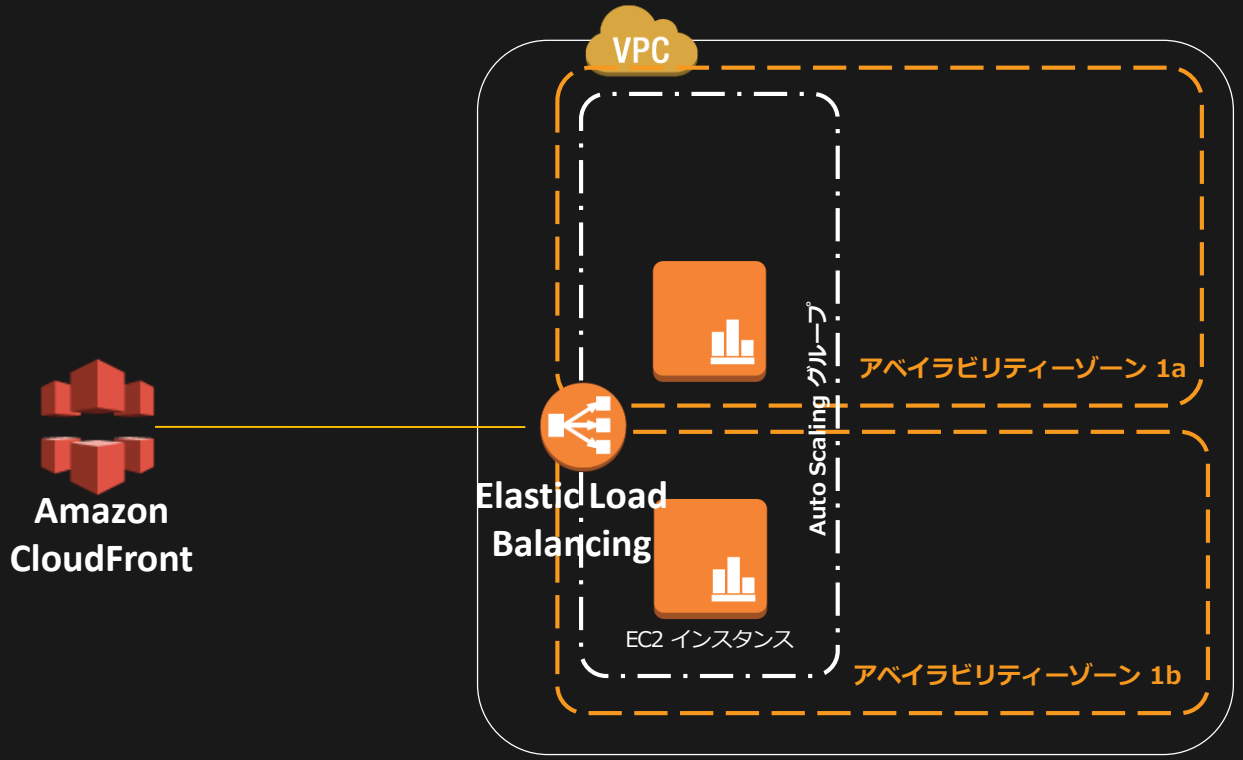
AWS WAF セキュリティオートメーション
https://aws.amazon.com/jp/answers/security/aws-waf-security-automations/

IPブラックリストをAWS WAFに自動反映

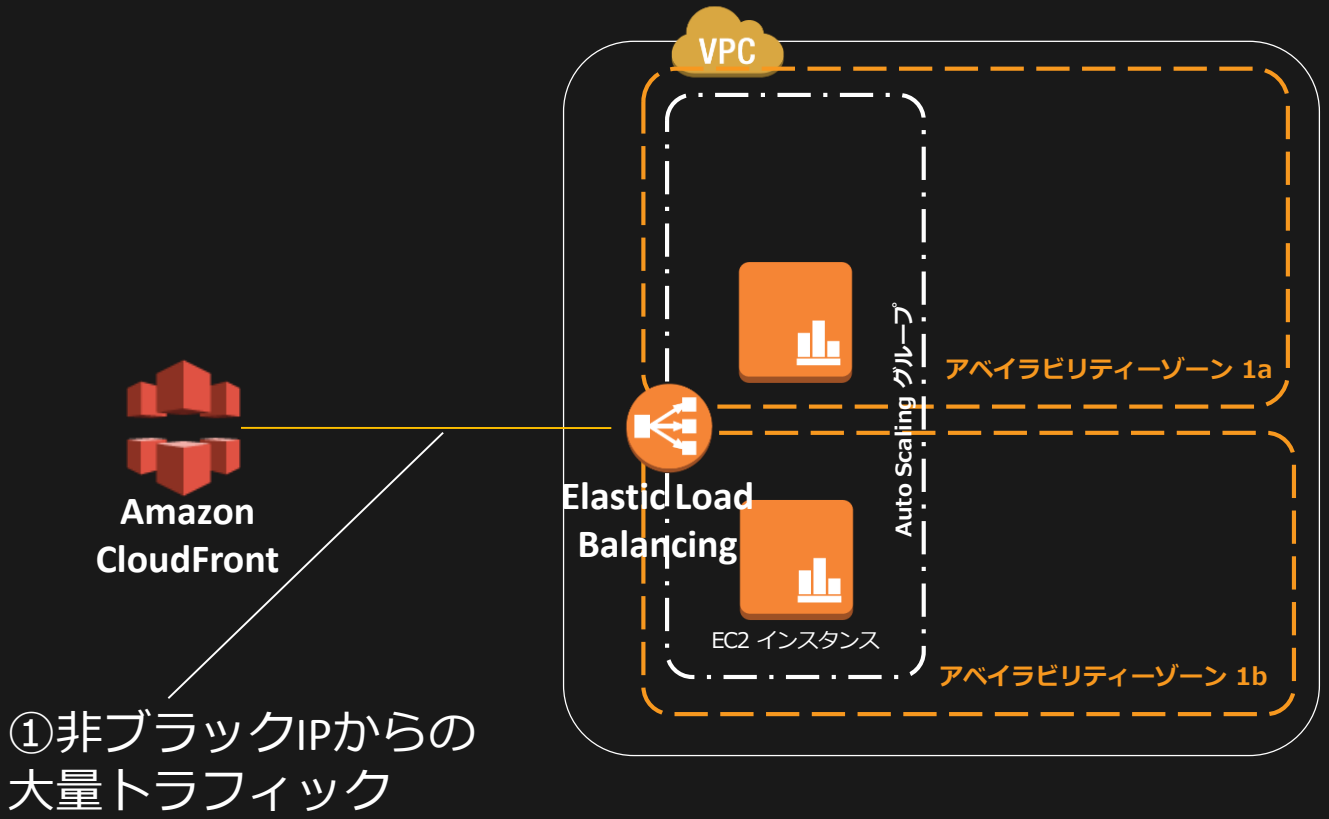


AWS WAF セキュリティオートメーション
https://aws.amazon.com/jp/answers/security/aws-waf-security-automations/

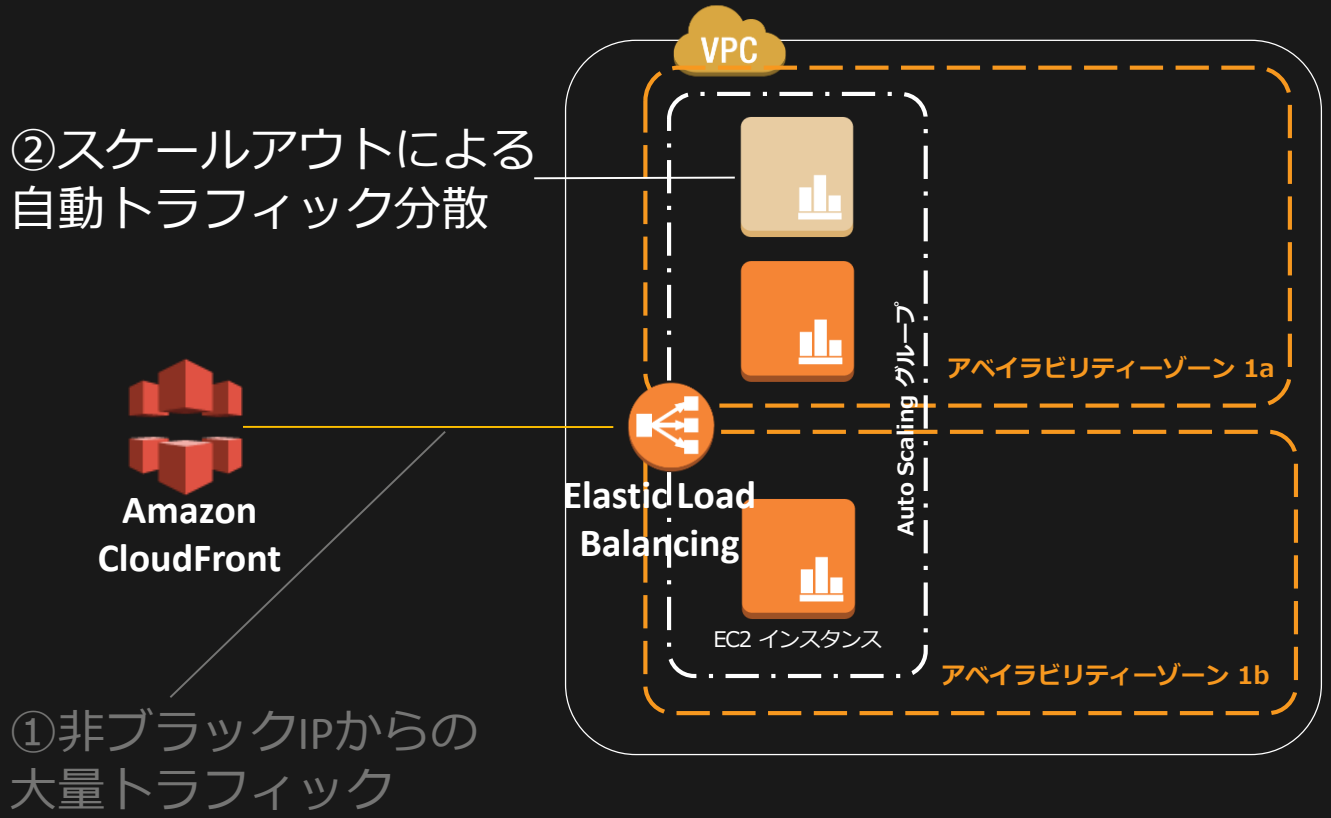
スケールアウトによる問題の抑制と通知



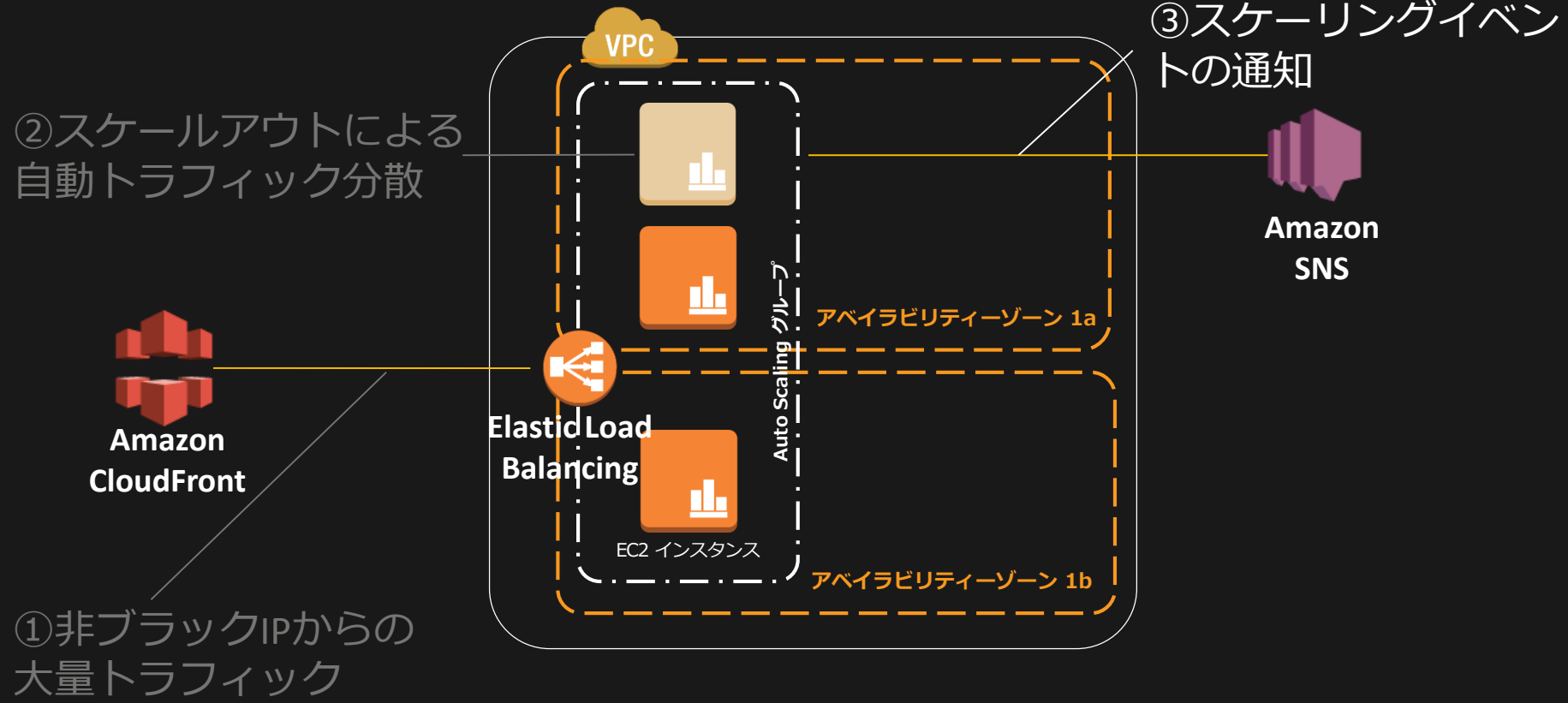
スケールアウトによる問題の抑制と通知



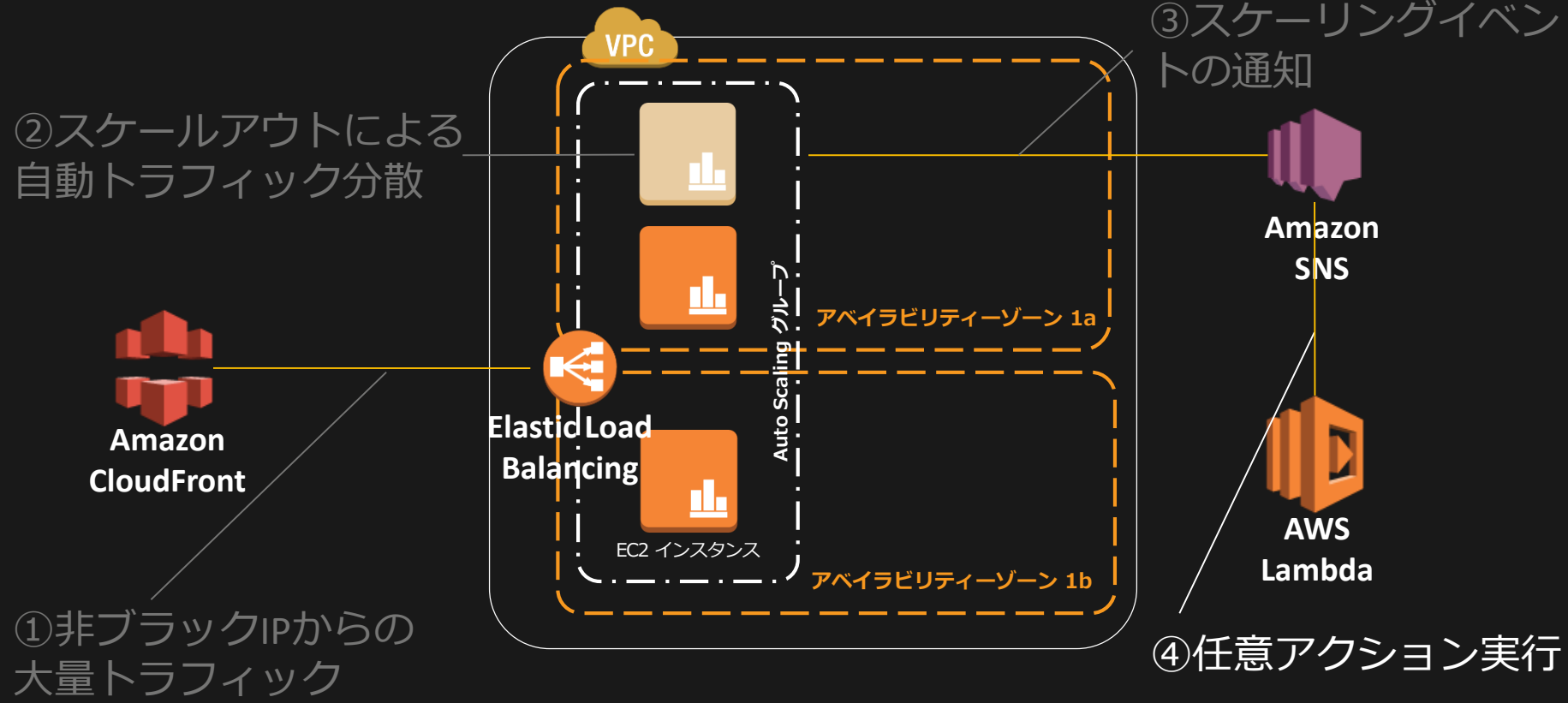
スケールアウトによる問題の抑制と通知



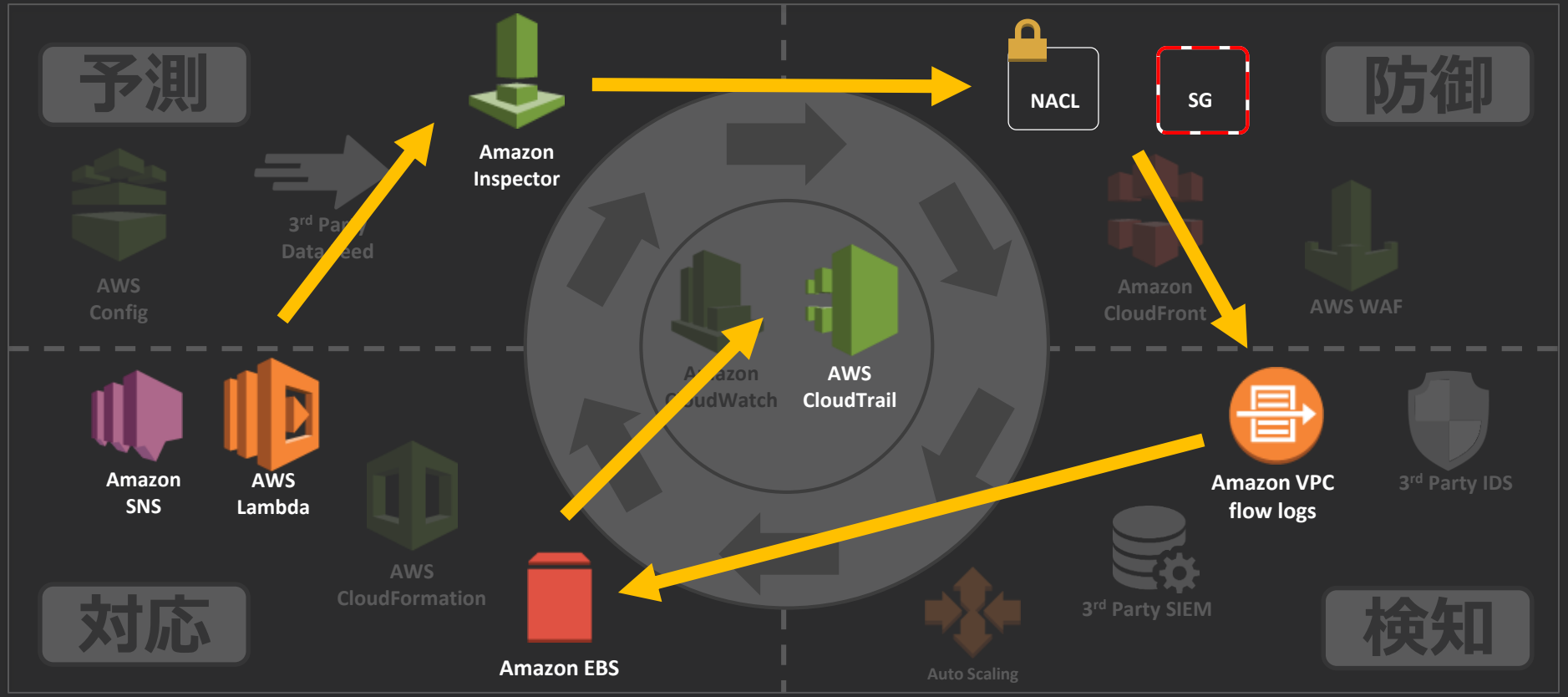
スケールアウトによる問題の抑制と通知



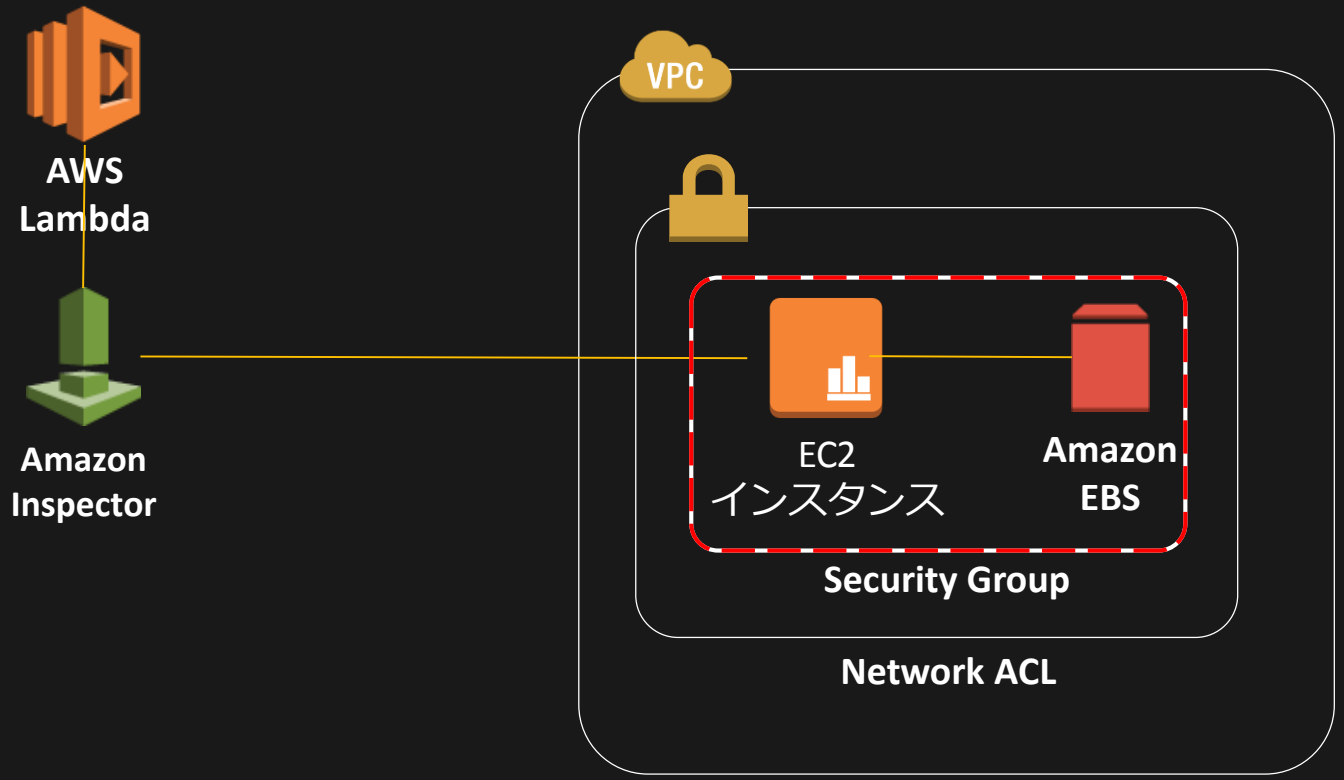
スケールアウトによる問題の抑制と通知



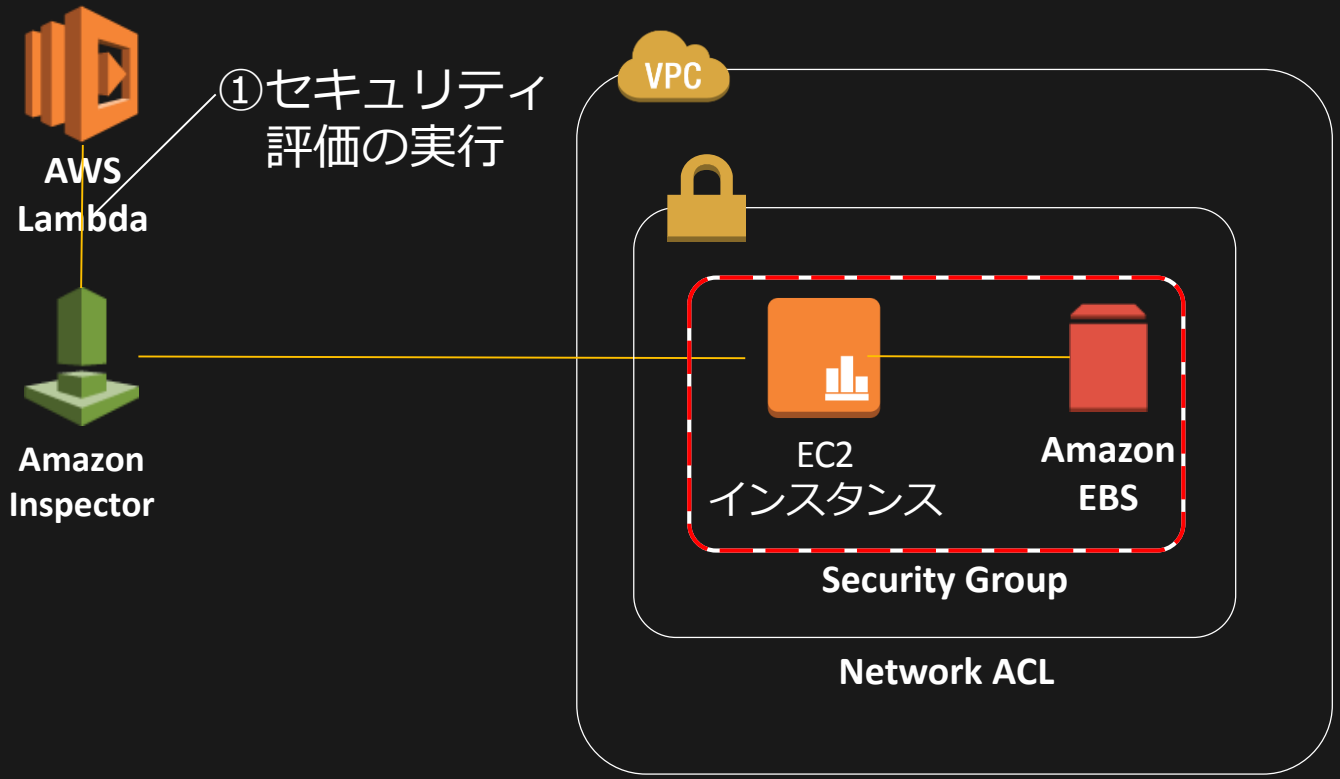
高リスク端末に対する内部対策フロー例



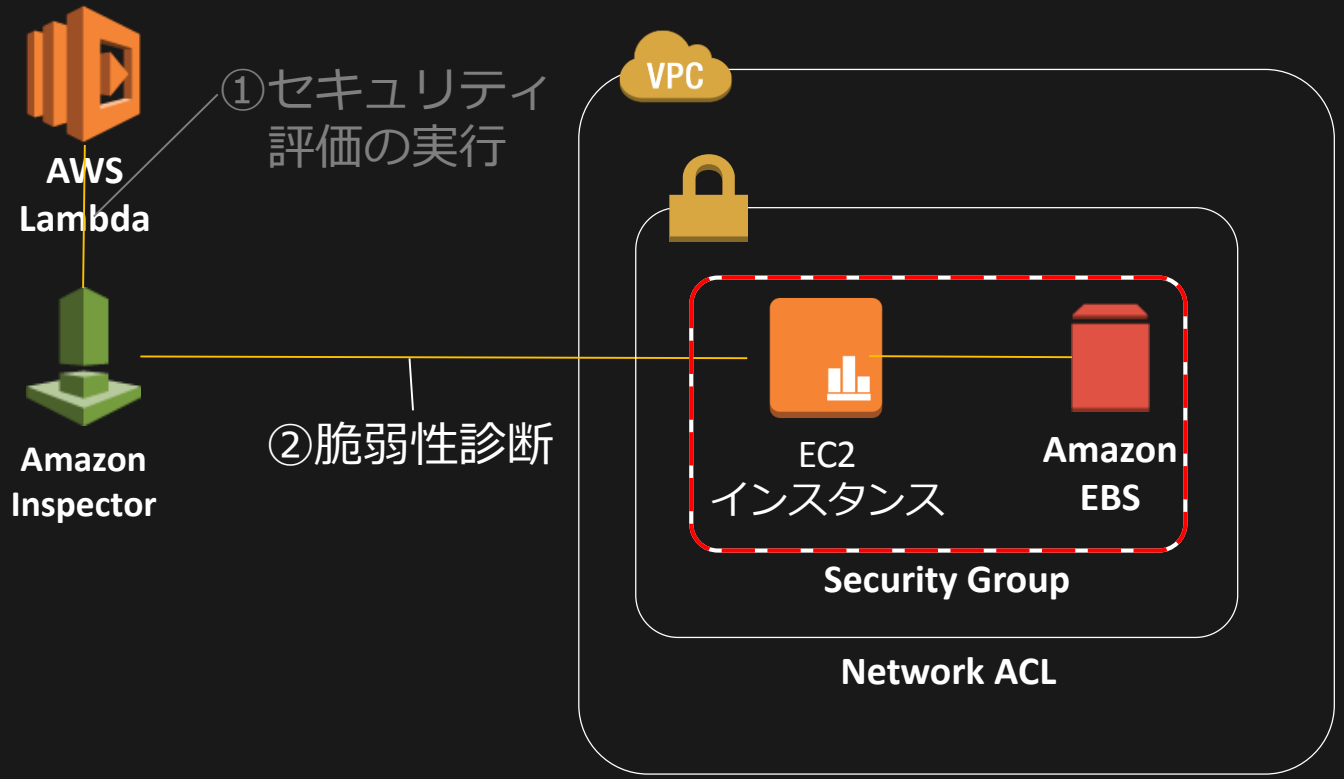
端末自動隔離とバックアップ



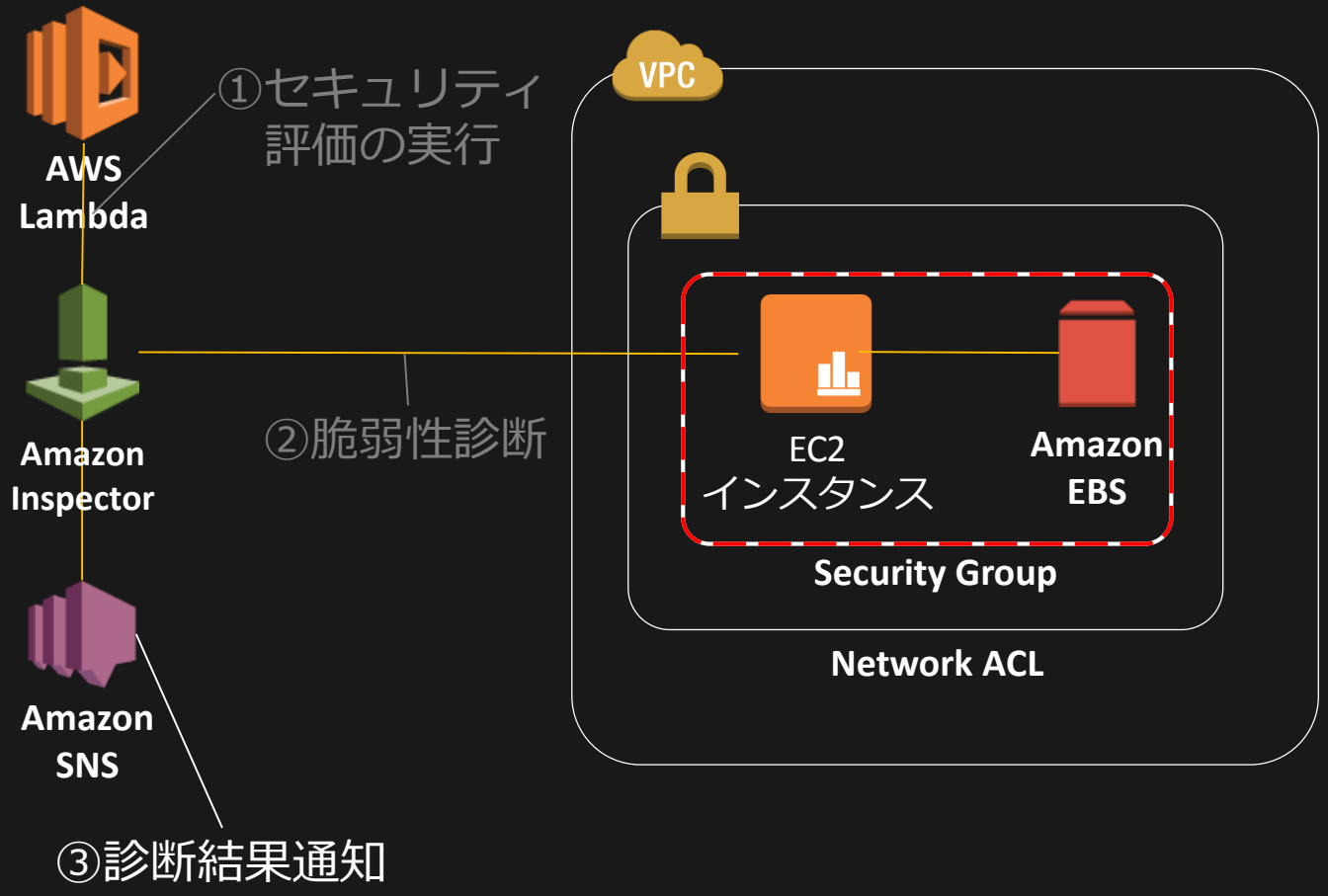
端末自動隔離とバックアップ



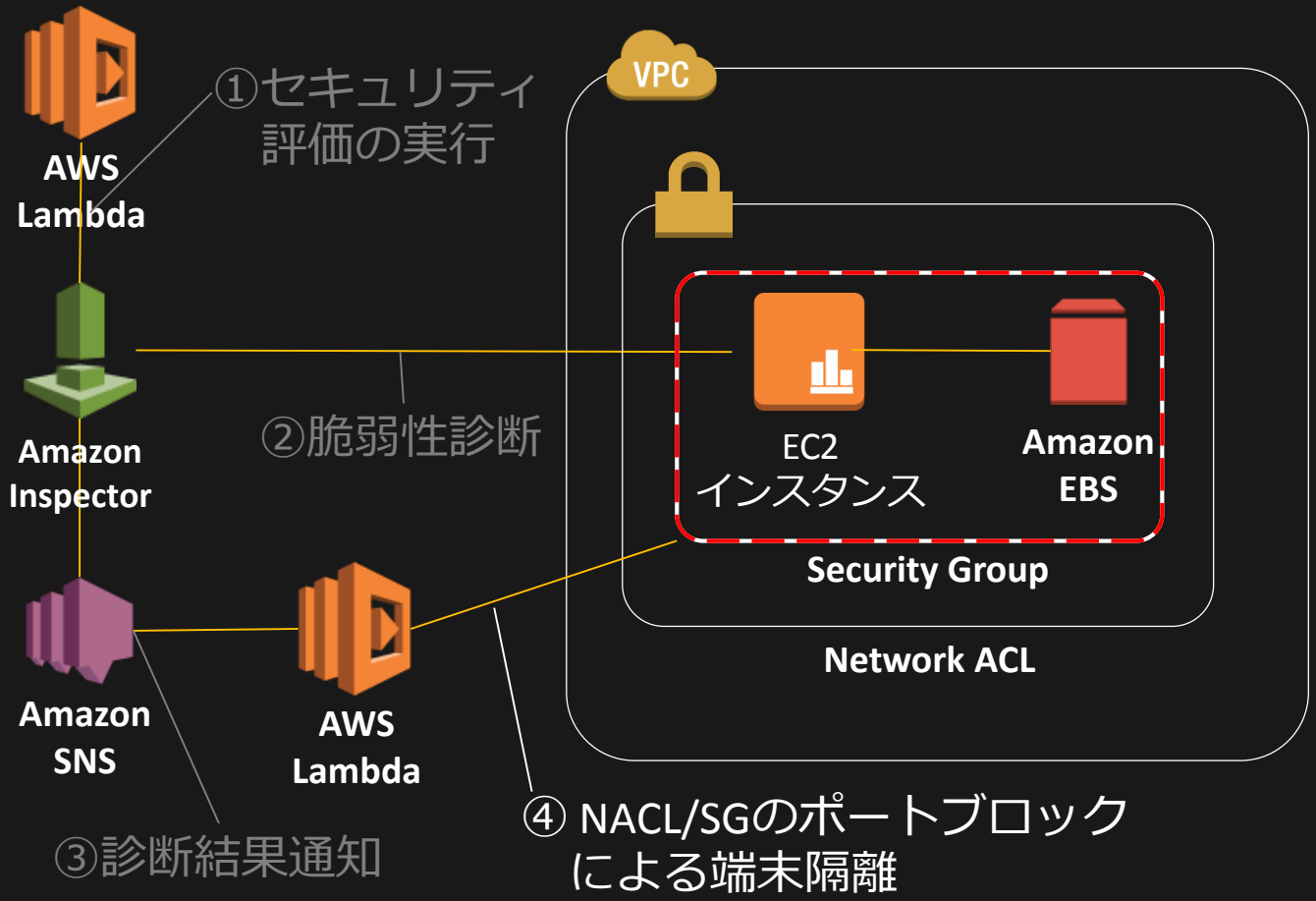
端末自動隔離とバックアップ



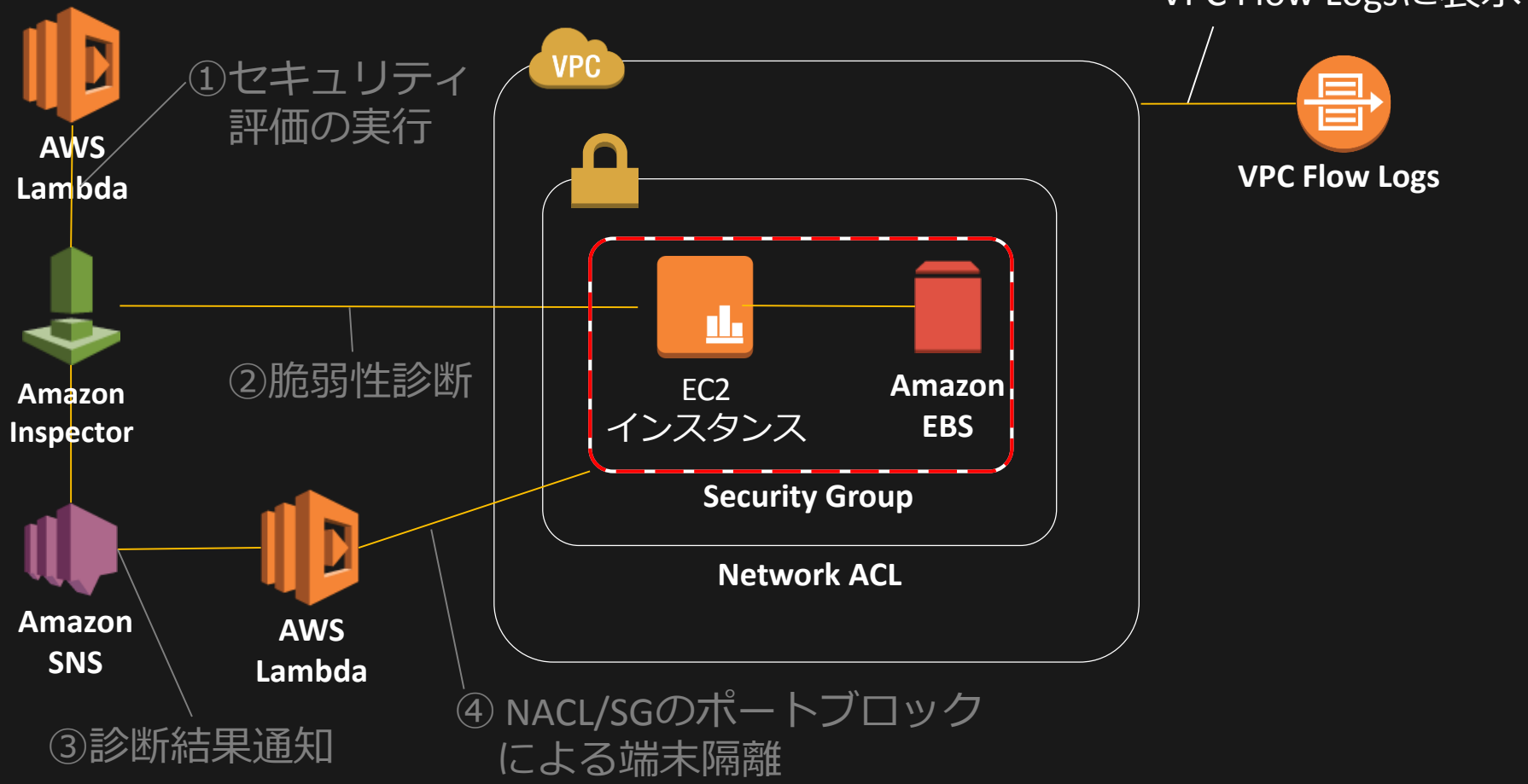
端末自動隔離とバックアップ



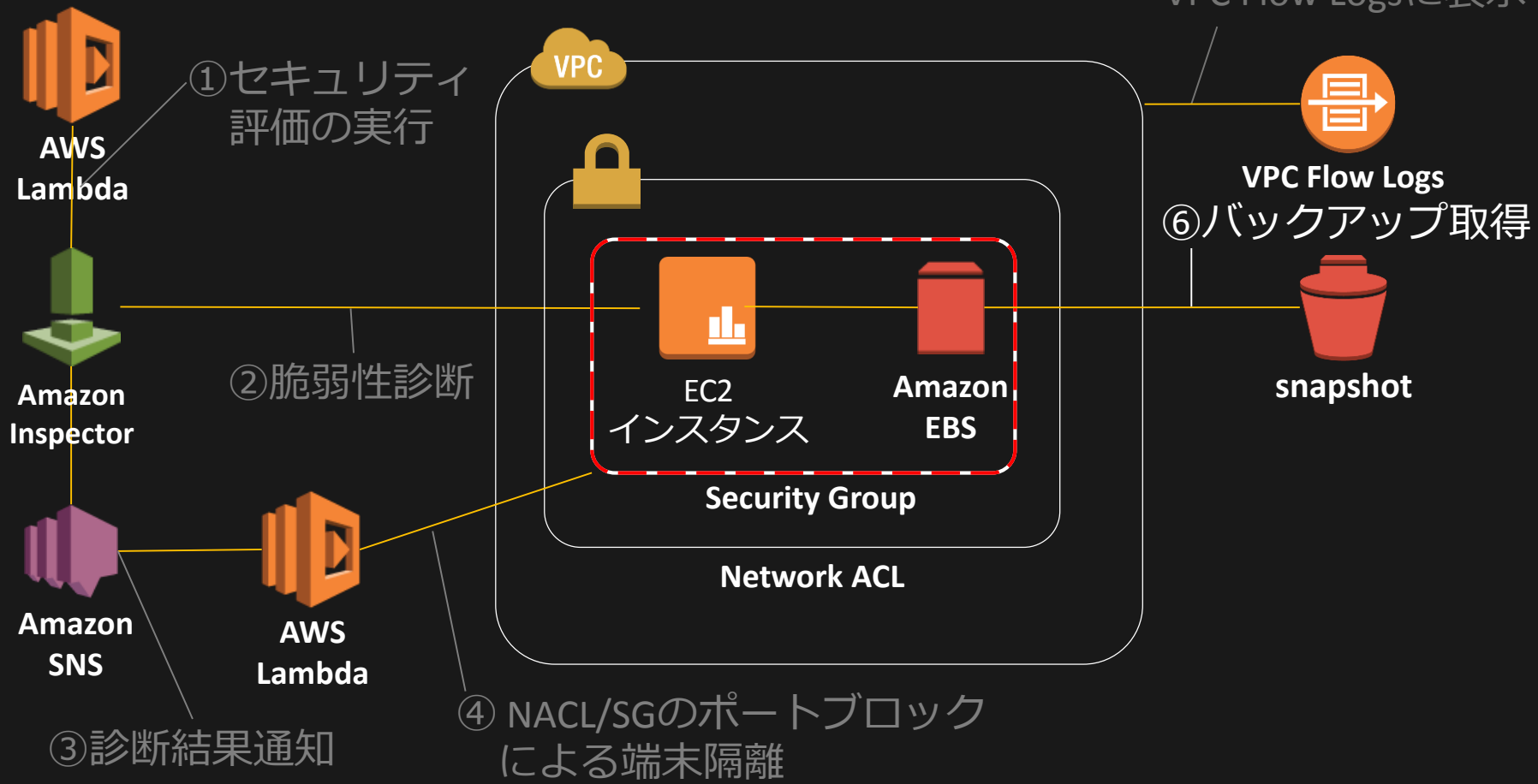
端末自動隔離とバックアップ



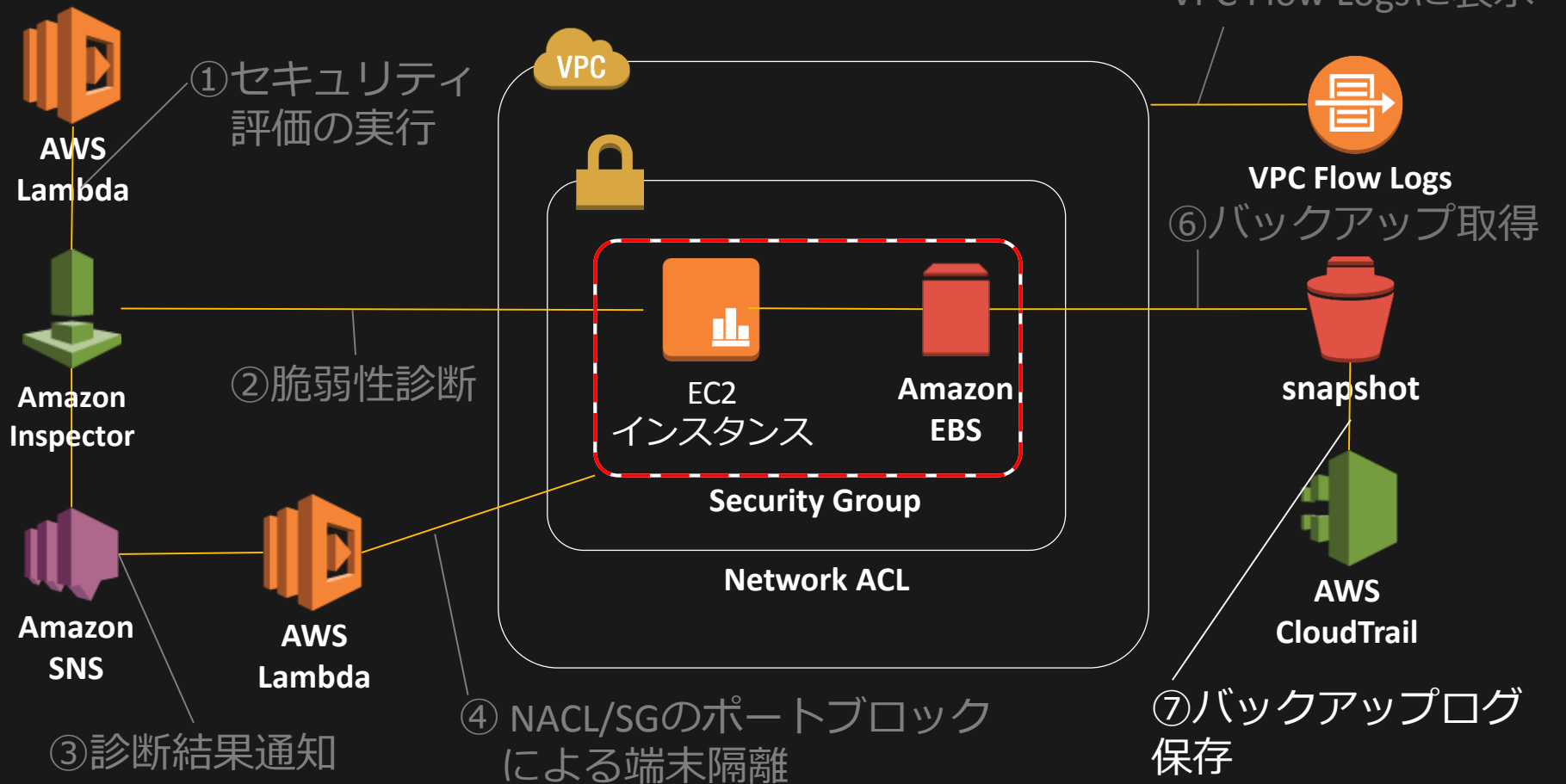
端末自動隔離とバックアップ



端末自動隔離とバックアップ



端末自動隔離とバックアップ



セキュリティ戦略基盤となるAWSクラウド環境

セキュリティ・オートメーションはどこに向かうのか？

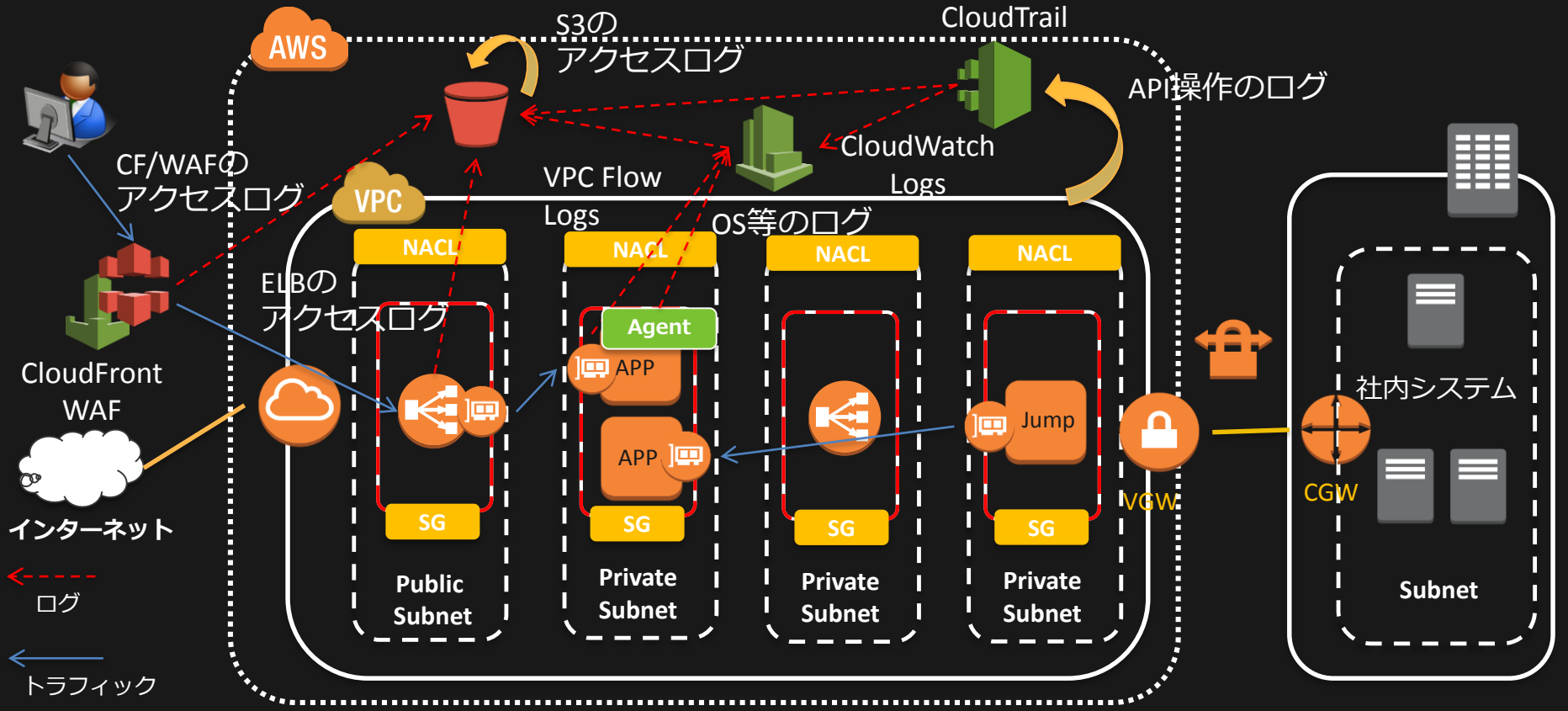
オートメーションがもたらすもの（再掲）

多種多様なデータ集約	可視化と効果測定	分析による意思決定
オートメーション		

このプロセスを継続することで良い戦略が策定できる

AWSインフラ全体のログ取得が可能

データ集約



CloudTrailのよる監査ログ取得対象サービス※

データ集約

分析
- Amazon Athena
- Amazon Cloud Search
- Amazon EMR
- AWS Data Pipeline
- Amazon Kinesis Firehose
- Amazon Kinesis Streams
- Amazon QuickSight

アプリケーションサービス
- Amazon API Gateway
- Amazon Elastic Transcoder
- Amazon Elasticsearch Service
- Amazon Simple Workflow Service
- AWS Step Functions

人工知能
- Amazon Machine Learning
- Amazon Polly

ビジネス生産性
- Amazon WorkDocs

コンピューティング
- Application Auto Scaling
- Auto Scaling
- Amazon EC2 Container Registry
- Amazon EC2 Container Service
- AWS Elastic Beanstalk
- Amazon Elastic Compute Cloud
- Elastic Load Balancing
- AWS Lambda
- Amazon Lightsail

データベース
- Amazon DynamoDB
- Amazon ElastiCache
- Amazon Redshift
- Amazon Relational Database Service

デスクトップ
- Amazon WorkSpaces

開発者ツール
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline

ゲーム開発
- Amazon GameLift

モノのインターネット
- AWS IoT

管理ツール
- AWS Application Directory Service
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch Events
- Amazon CloudWatch Logs
- AWS Config
- AWS Managed Services
- AWS OpsWorks
- AWS OpsWorks for Chef Automate
- AWS Organizations
- AWS Service Catalog

メッセージング
- Amazon Simple Email Service
- Amazon Simple Notification Service
- Amazon Simple Queue Service

移行
- AWS Database Migration Service
- AWS Server Migration Service

モバイルサービス
- Amazon Cognito
- AWS Device Farm

ネットワーキング & 配信
- Amazon CloudFront
- 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
- Amazon Cloud Directory
- AWS CloudHSM
- AWS Directory Service
- AWS Identity and Access Management
- Amazon Inspector
- AWS Key Management Service
- AWS Security Token Service
- AWS WAF

ストレージ
- Amazon Elastic Block Store
- Amazon Elastic File System
- Amazon Glacier
- Amazon Simple Storage Service
- AWS Storage Gateway

サポート
- AWS Personal Health Dashboard
- AWS Support

その他ソフトウェア & サービス
- AWS Marketplace

※最新情報は http://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cloudtrail-supported-services.html

セキュリティ・ダッシュボード

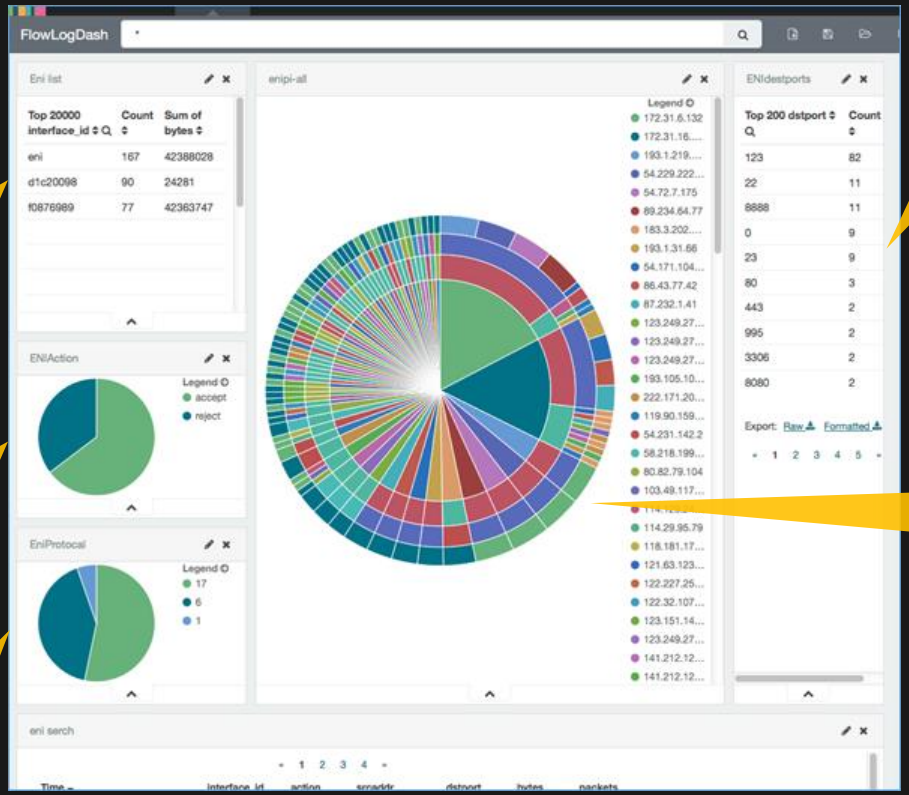
可視化

VPC Flow Logs/Amazon Elasticsearch Service/Kibana によるセキュリティグループの可視化

通信回数
と通信量

許可 or 遮断

プロトコル



宛先ポート

通信IP
アドレス

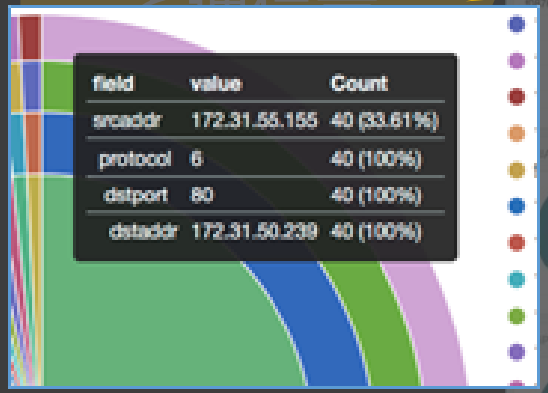
How to Optimize and Visualize Your Security Groups
https://aws.amazon.com/jp/blogs/security/how-to-optimize-and-visualize-your-security-groups/

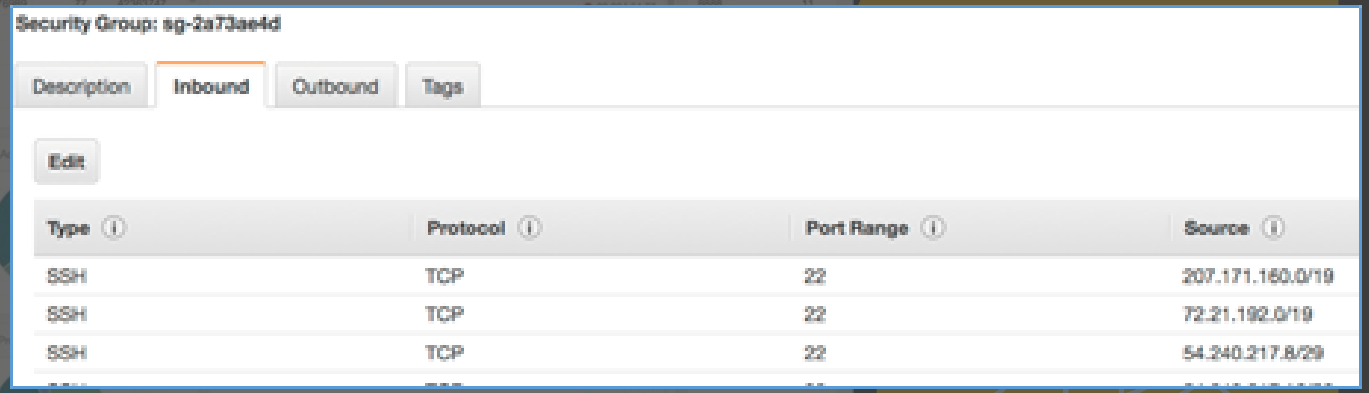
セキュリティ・ダッシュボード

可視化

VPC Flow Logs/Amazon Elasticsearch Service/Kibana によるセキュリティグループの可視化

ドリルダウンによる詳細解析





個別の通信ログレコード参照

How to Optimize and Visualize Your Security Groups
https://aws.amazon.com/jp/blogs/security/how-to-optimize-and-visualize-your-security-groups/

Domain Generation Algorithms

意思決定

課題

Domain Generation Algorithms(DGA)によるドメイン名からの通信をブロックしたい

CloudFront のログの例

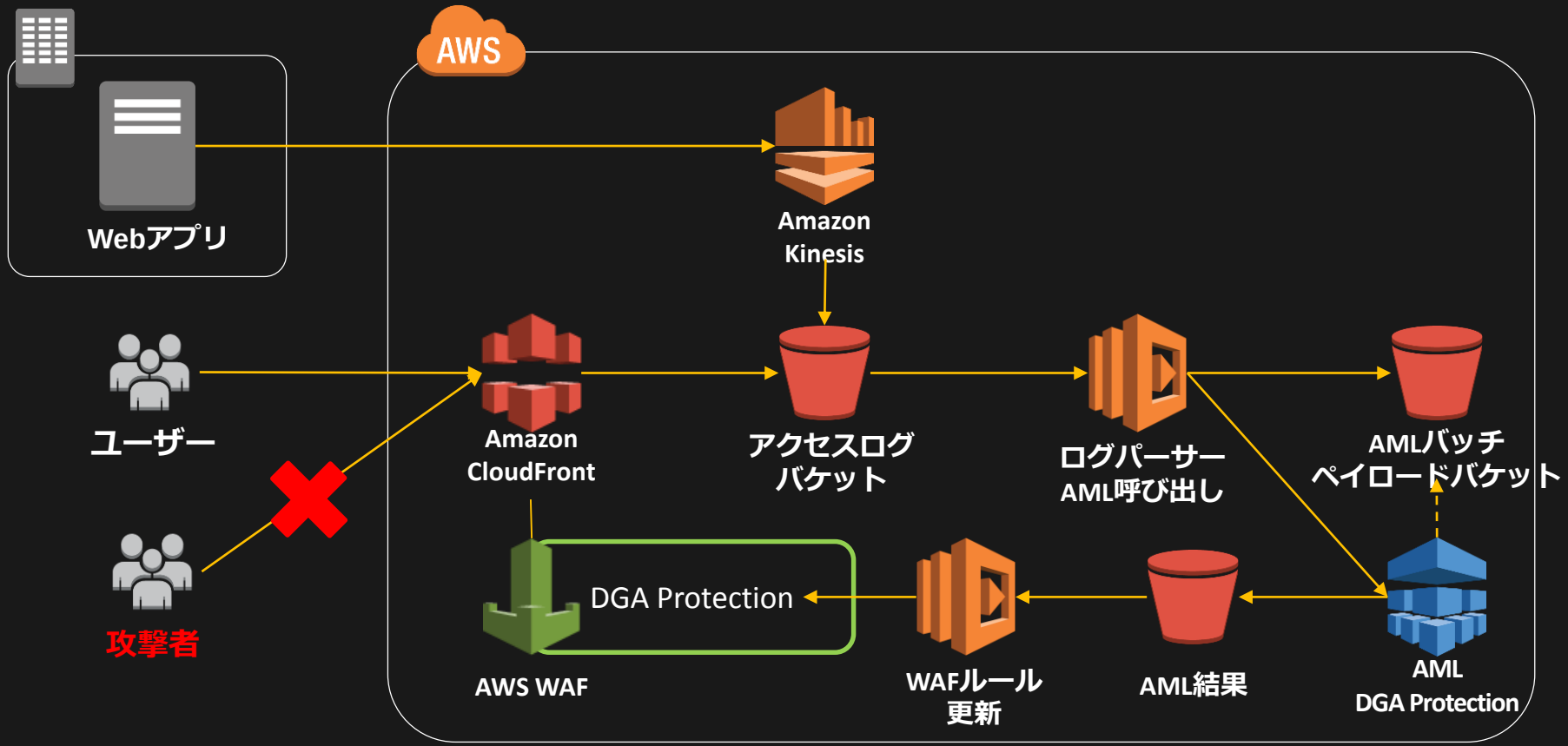
#Version: 1.0
#Fields: date time x-edge-location sc-bytes c-ip cs-method cs(Host) cs-uri-stem sc-status **cs(Referer)** cs(User-Agent) cs-uri-query cs(Cookie) x-edge-result-type x-edge-request-id x-host-header cs-protocol cs-bytes time-taken x-forwarded-for ssl-protocol ssl-cipher x-edge-response-result-type cs-protocol-version 2014-05-23 01:13:11 FRA2 182 192.0.2.10 GET d111111abcdef8.cloudfront.net /view/my/file.html 200 **www.displaymyfiles.com** Mozilla/4.0%20(compatible;%20MSIE%205.0b1;%20Mac_PowerPC) - zip=98101 RefreshHit MRVMF7KydIvxMWfJIglgwHQwZsbG2IhRJ07sn9AkKUFSHS9EXAMPLE== d111111abcdef8.cloudfront.net http - 0.001 - - - RefreshHit HTTP/1.1 2014-05-23 01:13:12 LAX1 2390282 192.0.2.202 GET d111111abcdef8.cloudfront.net /soundtrack/happy.mp3 304 www.unknownsingers.com Mozilla/4.0%20(compatible;%20MSIE%207.0;%20Windows%20NT%205.1) a=b&c=d zip=50158 Hit xGN7KWpVEmB9Dp7ctcVFQC4E-nrcOcEKS3QyAez--06dV7TEXAMPLE== d111111abcdef8.cloudfront.net http - 0.002 - - - Hit HTTP/1.1

正しいドメイン名の例：images-amazon

DGAによるドメイン名の例：30acd347397c34fc273e996b22951002

AWS WAF + Amazon Machine Learning

意思
決定



https://www.slideshare.net/AmazonWebServices/web-security-automation-spend-less-time-securing-your-applications

リスクベースのセキュリティ戦略

- リスク分析
  - 脅威分析
  - 脆弱性分析
  - 情報資産分析

リスクベースのセキュリティ戦略

意思決定

リスク分析

脅威分析

✓異常検知
✓ヒューリスティック分析
✓脅威インテリジェンス

Amazon Route 53

Amazon VPC Flow Logs

Security Credential

脆弱性分析

情報資産分析

リスクベースのセキュリティ戦略

意思決定

リスク分析

脅威分析

✓異常検知
✓ヒューリスティック分析
✓脅威インテリジェンス

Amazon Route 53

Amazon VPC Flow Logs

Security Credential

脆弱性分析

✓脆弱性スキャン
✓ベンチマーク評価
✓パッチ管理

Amazon Inspector

AWS Trusted Advisor

Amazon EC2 Systems Manager

情報資産分析

リスクベースのセキュリティ戦略

意思決定

リスク分析

脅威分析

✓異常検知
✓ヒューリスティック分析
✓脅威インテリジェンス

Amazon Route 53

Amazon VPC Flow Logs

Security Credential

脆弱性分析

✓脆弱性スキャン
✓ベンチマーク評価
✓パッチ管理

Amazon Inspector

AWS Trusted Advisor

Amazon EC2 Systems Manager

情報資産分析

✓ユーザー振る舞い分析
✓情報漏洩防止
✓機械学習

AWS CloudTrail

Amazon S3

Amazon Machine Learning

リスクベースのセキュリティ戦略

意思決定

リスク分析

脅威分析

✓異常検知
✓ヒューリスティック分析
✓脅威インテリジェンス

Amazon Route 53

Amazon VPC Flow Logs

Security Credential

脆弱性分析

✓脆弱性スキャン
✓ベンチマーク評価
✓パッチ管理

Amazon Inspector

AWS Trusted Advisor

Amazon EC2 Systems Manager

情報資産分析

✓ユーザー振る舞い分析
✓情報漏洩防止
✓機械学習

AWS CloudTrail

Amazon S3

Amazon Machine Learning

リスクに基づいたセキュリティ対策の意思決定

本セッションのポイント（再掲）

- オートメーションは戦略策定の礎
- セキュリティ・オートメーションを前提に設計されたAWSサービス
- セキュリティ戦略基盤となるAWSクラウド環境

関連セッション

D2T1-5（AWS Techトラック 1） 2017/5/31　16:20 ～ 17:00

よくある問題を解決する～ 5 分でそのままつかえるソリューション by AWS ソリューションズビルダチーム

D3T7-2（Dev Day トラック 1）2017/6/1　13:20～14:00

DevSecOps on AWS - Policy in Code

D4T1-6（AWS Techトラック 1） 2017/6/2　17:20 ～ 18:00

AWS 環境での CSIRT ソリューション

AWS

SUMMIT

ありがとうございました

amazon web services

本セッションのFeedbackをお願いします

受付でお配りしたアンケートに本セッションの満足度やご感想などをご記入ください
アンケートをご提出いただきました方には、もれなく素敵なAWSオリジナルグッズを
プレゼントさせていただきます

アンケートは受付、パミール3FのEXPO展示会場内にて回収させて頂きます