AWS Builders Online Series

T1-4

<2024 年版> デモで理解する！基本の Web システムアーキテクチャ - セキュリティ編 -

町田 友和
アマゾン ウェブ サービス ジャパン合同会社
ソリューションアーキテクト

aws

自己紹介

町田 友和 (まちだ ともかず)

ソリューションアーキテクト

業種・業態を問わず、様々なお客様の構成検討を支援

前職では、システムインテグレーターのインフラエンジニアに従事

対象者、本セッションで学べること

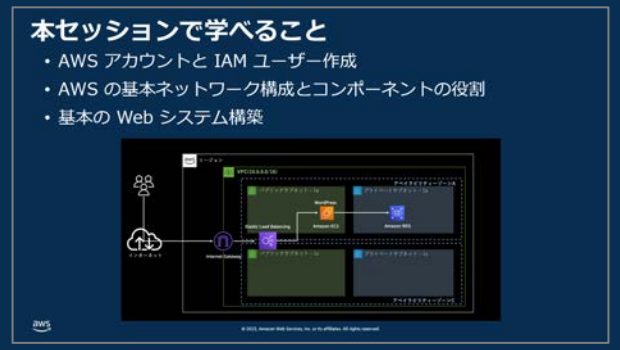
- **本セッションの対象者**
  - AWS をこれから触り始めようとする方
  - AWS 上で動かす Web システムのセキュリティ対策を検討される方
  - Amazon EC2 や Amazon RDS を使ったシステムをすでに運用されている方、または、同等の知識をお持ちの方

- **本セッションで学べること**
  - セキュリティ対策の重要性について
  - AWS サービスを使った基本的な Web システムのセキュリティ対策

T1 関連セッションについて

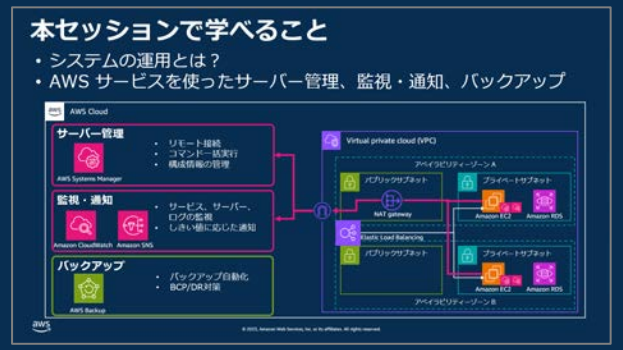
本セッションは、基礎編、スケーラビリティ向上編、運用編、
セキュリティ編の 4 セッションで構成しています

セキュリティ編で例示するアーキテクチャの構築デモは基礎編をご覧ください

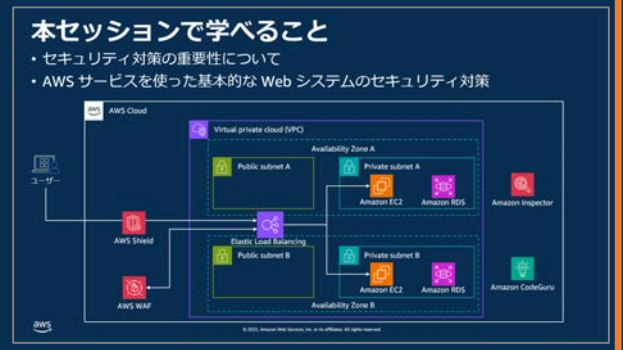


基礎編

スケーラビリティ向上編



運用編



セキュリティ編

※ 当日にご覧になれなかった場合でも、後日のオンデマンド配信でご覧頂くことができます

本セッションで扱わないこと

本セッションでご紹介しきれない AWS アカウントに対するセキュリティ対策のファーストステップや AWS におけるセキュリティの考え方については、

関連資料コーナー の

今日からスタート！AWS セキュリティ 初めの一歩

をご覧ください。

アジェンダ

- セキュリティ対策の重要性
- Web システムを悪意のあるリクエストから保護する
- Web システムの脆弱性を検知する
- まとめ

セキュリティ対策の重要性

セキュリティ対策にかける時間は皆様の日々の業務にどのように影響していますか？

“

セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要である。

”

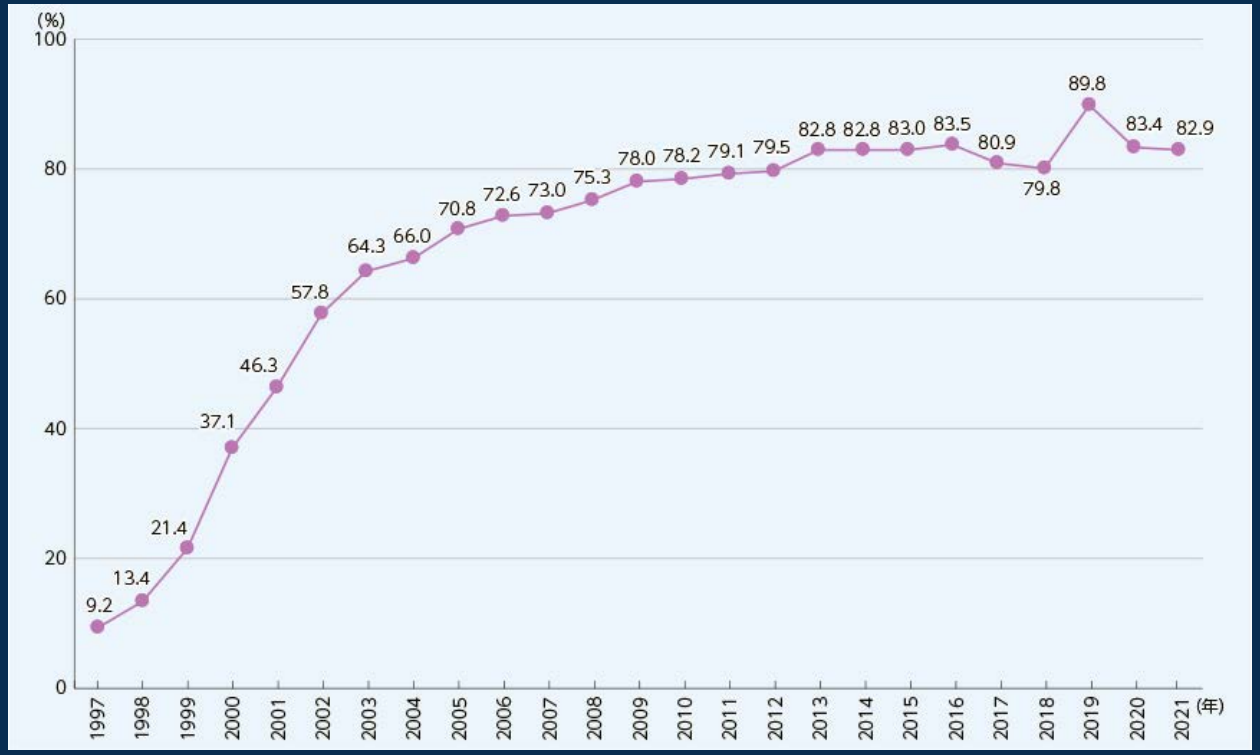
サイバーセキュリティ経営ガイドライン Ver 2.0

経済産業省、独立行政法人 情報処理推進機構

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

インターネット利用率の高さ

2021 年の**インターネット利用率**（個人）は **82.9%**



出典: 総務省 令和4年 通信利用動向調査
インターネットの利用動向

Web システムに対する様々な脅威の一例

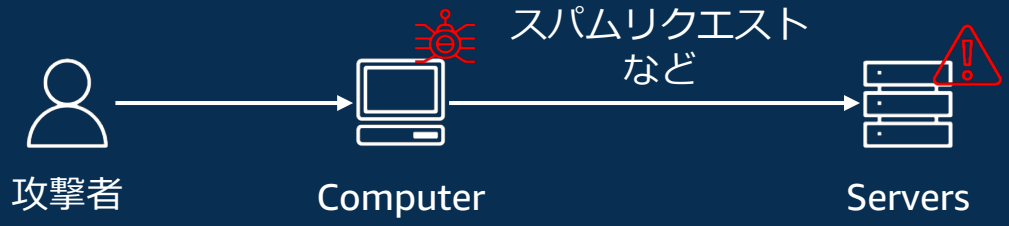
サービス拒否 (DDoS)

- SYN フラッド
- HTTP フラッド
- UDP フラッド
- …など

Computer 単体での実施は DoS

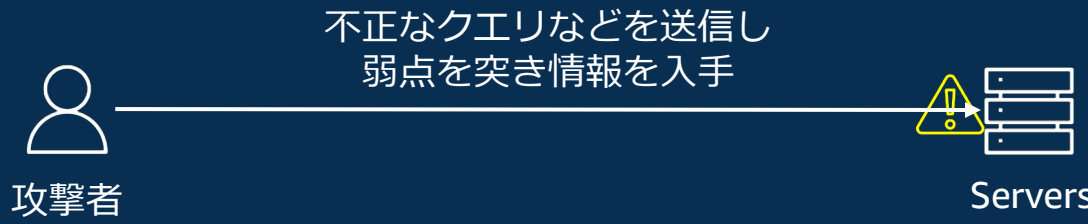
悪意のあるボット

- コメントスパム
- アカウント乗っ取り
- SEO スパム
- …など



アプリケーションの脆弱性を悪用する攻撃

- SQL インジェクション
- サーバサイドリクエストフォージェリ
- クロスサイトスクリプティング
- …など



Web システムへの脅威による影響の一例

影響の一例

- システムのダウンタイムと不安定性
- リソースの悪用とデータの盗難
- 認証情報の漏洩とスパム/フェイクレビューの発生
- …など

- ビジネスの中断
- 評判悪化による機会損失
- …など

セキュリティ対策は重要

Web システムにおけるセキュリティ対策例

セキュリティパッチの適用を迅速に対応する目的や
潜在的な弱点を確認するために
アプリケーションの脆弱性の検出を行う

悪意のあるリクエストで脅威にさらされないように
Web アプリケーションファイアウォールなどで保護
する

Web システムを悪意のあるリクエストから保護する

Web システムの保護は AWS WAF を中心に構成

デモ実施

AWS Shield

サービス拒否 (DDoS) 攻撃から保護する

AWS WAF

悪意のあるボット から保護する

Amazon Inspector

Amazon CodeGuru

アプリケーションの脆弱性を 悪用する攻撃から保護・検知する

AWS Shield

AWS サービスへの受信トラフィックを検査し、DDoS 攻撃を防御する

AWS Shield

AWS Shield Standard

- 最も一般的な DDoS 攻撃に対応した DDoS 攻撃緩和サービス
- すべてのお客様に無料で提供される
- 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透過的に適用され、インフラストラクチャ (レイヤー 3 ネットワーク層とレイヤー 4 トランスポート層) に対する DDoS を自動的に緩和

AWS Shield

AWS サービスへの受信トラフィックを検査し、DDoS 攻撃を防御する

AWS Shield

AWS Shield Advanced

- 有料で提供される
- レイヤー 3 およびレイヤー 4 の DDoS 攻撃の緩和に加え、レイヤー 7 アプリケーション層への攻撃を検出できる。また、AWS WAF を使用してレイヤー7 の攻撃を自動的に緩和
- 大規模かつ高度な攻撃に備えて、攻撃に対する可視性を高め、複雑な事例に関して DDoS エキスパート (Shield Response Team (SRT)) への年中無休のアクセスが提供される DDoS 緩和サービス

AWS WAF - 機能概要

Web システムの通信内容を検査し、不正なアクセスを遮断する

AWS WAF

機能概要

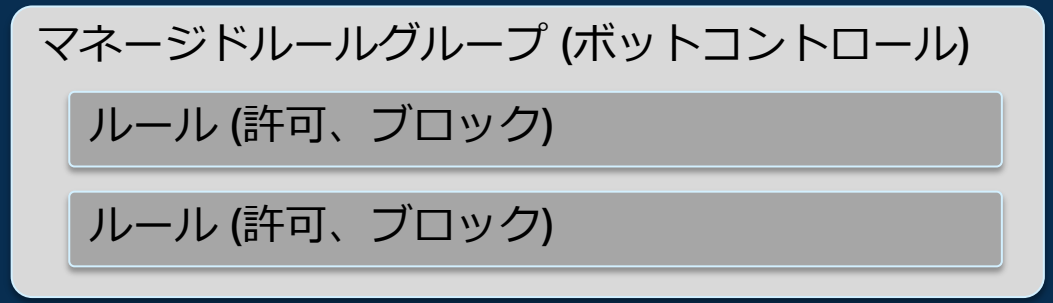
- ウェブアプリケーションに対する攻撃から保護するための Web アプリケーションファイアウォール
- ボットなど、アプリケーションの脆弱性に類する一般的な脅威からアプリケーションを保護するための事前設定ルールを簡単にデプロイするための AWS マネージドルール
- ルールに基づきウェブリクエストを許可、ブロックする

AWS WAF - マネージドルールグループ

Web システムの通信内容を検査し、不正なアクセスを遮断する

マネージドルールグループ

- 一般的な脅威からアプリケーションを保護するための**事前定義済みのルールセット**
  - OWASP Top 10 ※1、ボットコントロール、PHP アプリケーション、SQL データベース、Linux OS、 ...など
- **AWS もしくはサードパーティによって管理**されている
- 一部を除き**無料**で利用可能



※1: OWASP Top 10 とは

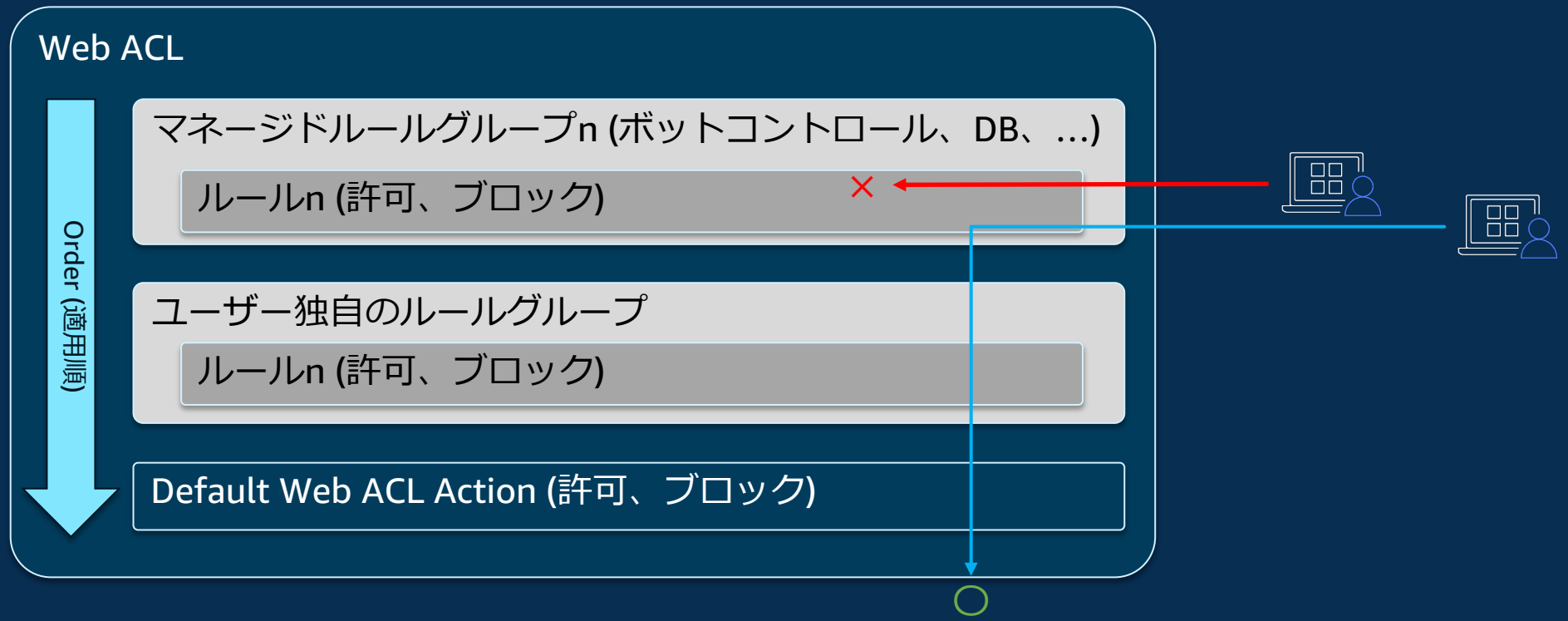
Web アプリケーションのセキュリティリスクをランク付けした OWASP のレポート
https://owasp.org/Top10/ja/

AWS WAF - Web ACL

Web システムの通信内容を検査し、不正なアクセスを遮断する

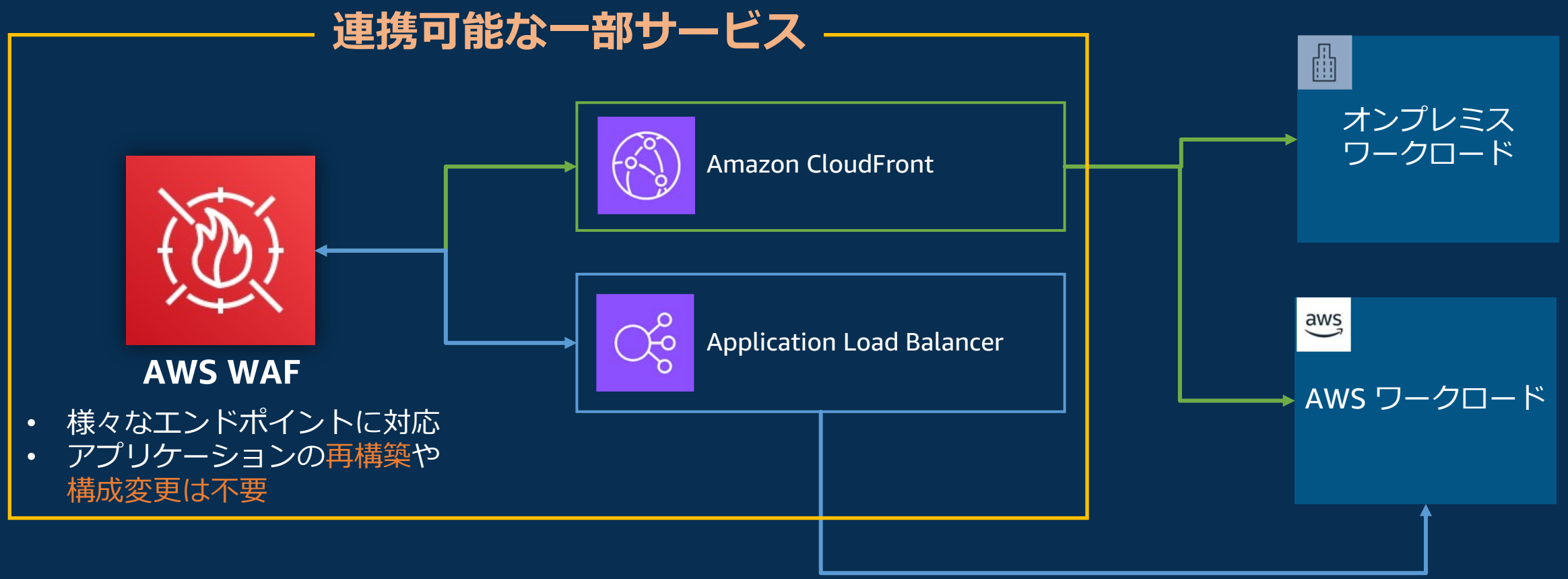
Web ACL

- ウェブリクエストに対する**ルールを定義するための枠組み**
- ルールで定義された条件に一致した時にウェブリクエストの処理方法が指定される
- 設定したルールに該当しない場合、Web ACL のデフォルトアクションにより処理される



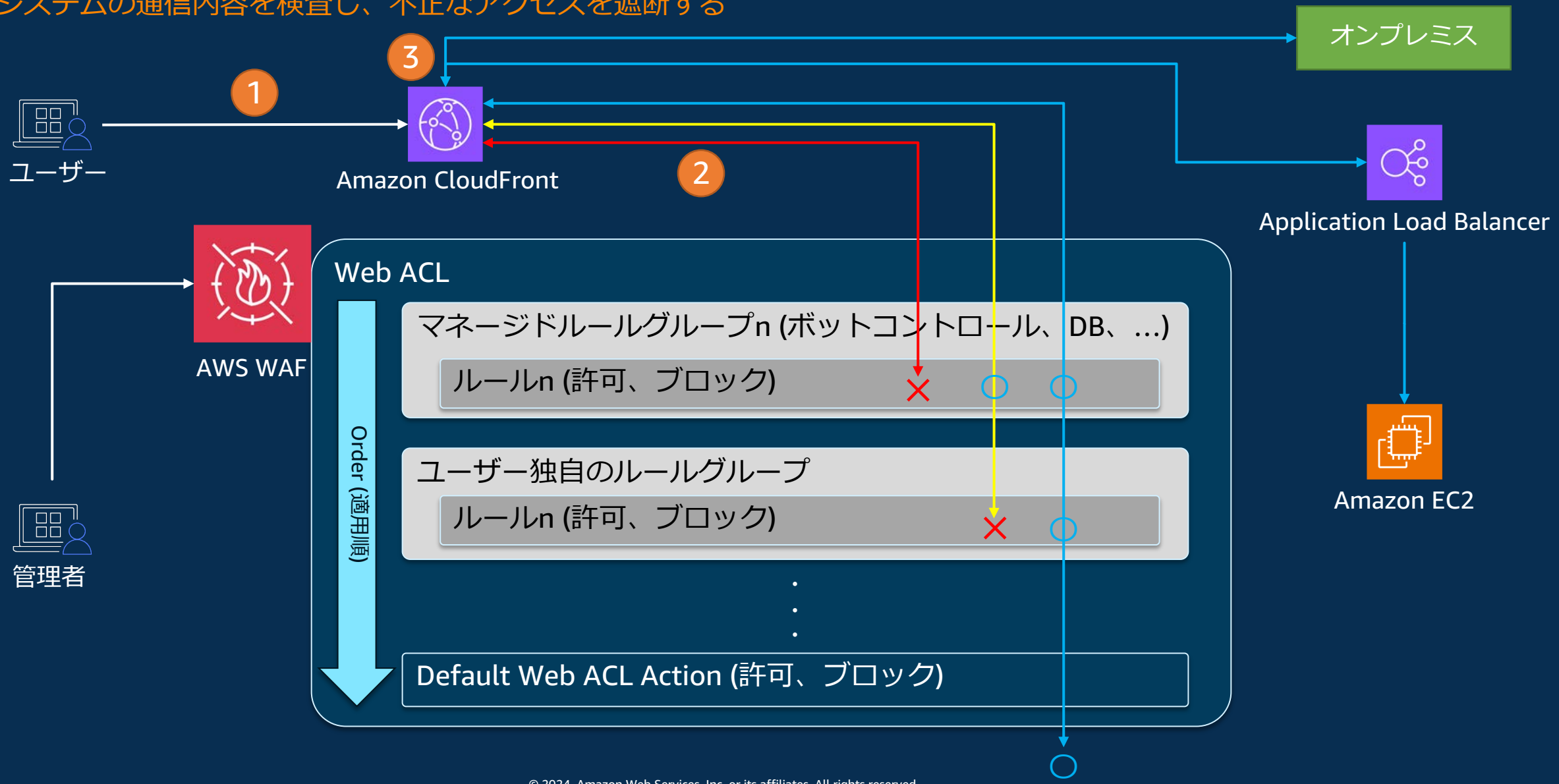
AWS WAF - 既存のアーキテクチャ変更不要

Web システムの通信内容を検査し、不正なアクセスを遮断する



AWS WAF - 利用イメージ

Web システムの通信内容を検査し、不正なアクセスを遮断する



AWS WAF - デモ

Web システムの通信内容を検査し、不正なアクセスを遮断する

動画をご覧ください

Web システムの脆弱性を検知する

アプリケーションの脆弱性を検知する

デモ実施

AWS Shield

サービス拒否 (DoS)
攻撃から保護する

AWS WAF

悪意のあるボット
から保護する

Amazon Inspector

Amazon CodeGuru

アプリケーションの脆弱性を
悪用する攻撃から保護・検知する

Amazon Inspector - 機能概要

自動化された脆弱性管理サービス

Amazon Inspector

機能概要

- ソフトウェアの脆弱性を継続的なスキャンで検出するサービス
  - パッケージの脆弱性
  - ネットワークの到達性
  - コードの脆弱性
- 数クリックで簡単に有効化することができる
- 対処すべき脆弱性リソースの優先順位付けを支援

Amazon Inspector - パッケージの脆弱性

自動化された脆弱性管理サービス

検出結果

- Amazon EC2 インスタンス、Amazon ECR コンテナイメージ、Lambda 関数のソフトウェアパッケージをスキャンして検出した脆弱性に該当する CVE を示す。 ※1

利用イメージ

※1: CVE とは個別製品中の脆弱性を対象とした共通脆弱性識別子
https://cve.mitre.org/

Amazon Inspector - ネットワーク到達性

自動化された脆弱性管理サービス

検出結果

- Amazon EC2 インスタンスへの許可されたネットワークパスがあるかどうかを示す。インターネットゲートウェイ、ロードバランサー、VPC ピアリング接続、仮想ゲートウェイを介した VPN などの VPC から到達可能かどうかスキャンする。

利用イメージ

Amazon Inspector - コードの脆弱性

自動化された脆弱性管理サービス

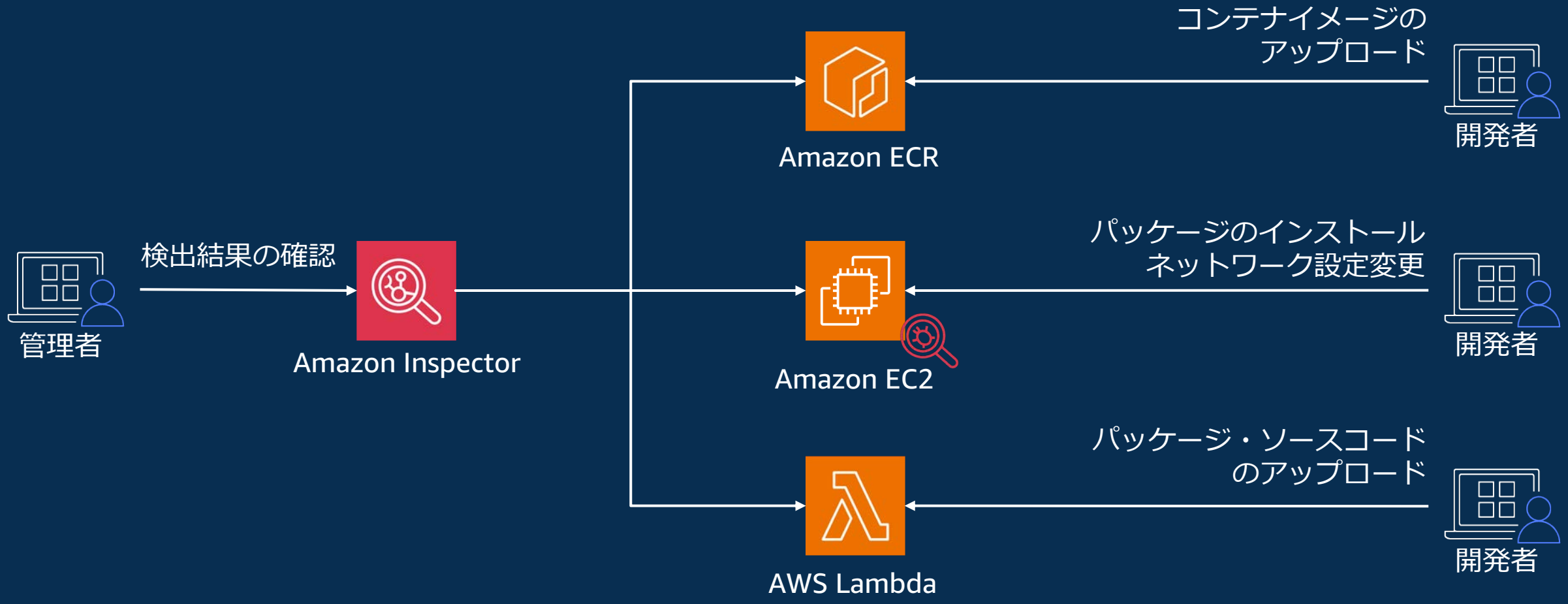
検出結果

- Lambda 関数内のアプリケーションコードをスキャンして、AWS セキュリティのベストプラクティスに基づいて、コードセキュリティの脆弱性がないかを確認する。

利用イメージ

Amazon Inspector - 利用イメージ

自動化された脆弱性管理サービス



Amazon Inspector - デモ

自動化された脆弱性管理サービス

動画をご覧ください

Amazon CodeGuru Security

静的アプリケーションセキュリティ検査 (SAST) を提供し、コードの脆弱性を検出する

Amazon CodeGuru

Amazon CodeGuru Security

- 機械学習を使用し、セキュリティポリシー違反と脆弱性を検出するためのツール
- コードの脆弱性を特定し、特定された脆弱性を修正する方法に関する推奨事項を提示する

Amazon CodeGuru Security

静的アプリケーションセキュリティ検査 (SAST) を提供し、コードの脆弱性を検出する

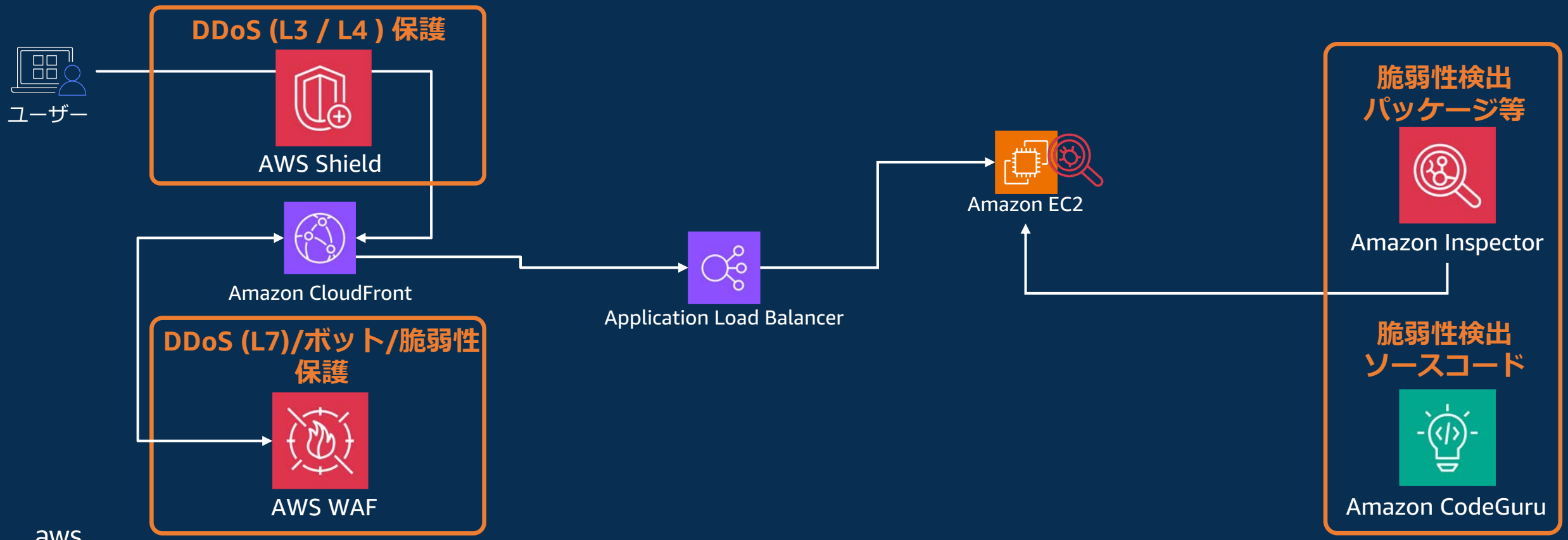
どのような内容の脆弱性を検査しているのか

- Java, Python, JavaScript, C#, TypeScript **コードの脆弱性を検出**することが可能
- **ハードコードされた認証情報**をスキャンできる
- **OWASP の上位 10 件**、CWE の上位 25 件の問題を検出できる

利用イメージ

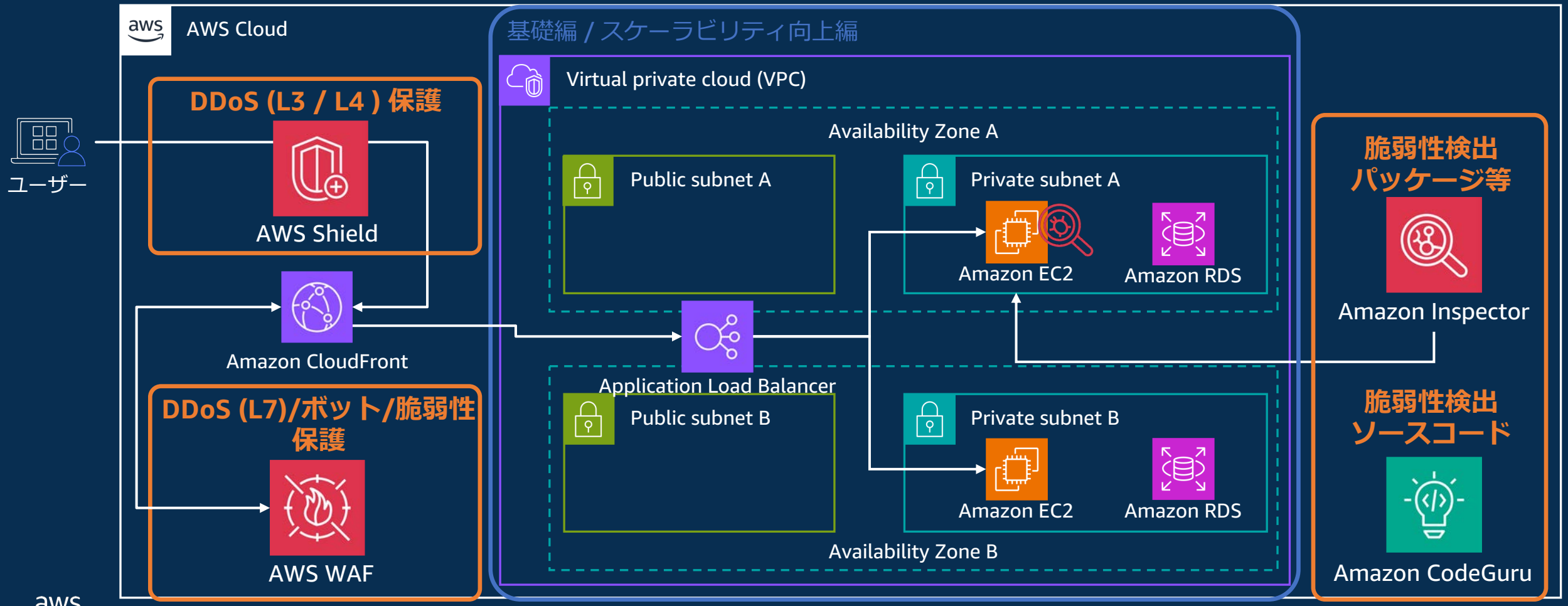
AWS サービスを活用した Web システム

- 基本的な Web システムにセキュリティリスクを軽減するための AWS サービスを組み合わせた構成例



AWS サービスを活用した Web システム

- 基本的な Web システムにセキュリティリスクを軽減するための AWS サービスを組み合わせた構成例



まとめ

Webシステムへのセキュリティ対策のソリューション

- DDoS対策
  - AWS Shield
- Webアプリケーションの脆弱性対策
  - AWS WAF
- プラットフォームの脆弱性管理
  - Amazon Inspector
- カスタムコードの脆弱性対策
  - Amazon CodeGuru Security

料金

本セッションで登場するサービス・機能で料金が発生する要素について概要レベルでご紹介
詳細は各サービスの料金ページをご確認ください

AWS Shield Standard

無料

AWS Shield Advanced

- 月額料金
- データ転送 (OUT) 使用料金

AWS Shield 料金ページ
https://aws.amazon.com/jp/shield/pricing/

AWS WAF

- Web ACL
- ルール
- リクエスト
- Paid rule groups

AWS WAF 料金ページ
https://aws.amazon.com/jp/waf/pricing/

Amazon Inspector

- Amazon EC2 インスタンススキャン
- Amazon ECR コンテナイメージスキャン
- AWS Lambda 標準スキャン
- AWS Lambda コードスキャン

Amazon Inspector 料金ページ
https://aws.amazon.com/jp/inspector/pricing/

Amazon CodeGuru Security

- パブリックプレビュー中のため無料 (2023/12/05 時点)
- 統合開発環境については、個人利用無料、組織利用有料 (詳細は Amazon CodeWhisperer 料金ページ参照)

Amazon CodeGuru 料金ページ
https://aws.amazon.com/jp/codeguru/pricing/

Amazon CodeWhisperer 料金ページ
https://aws.amazon.com/jp/codewhisperer/pricing/

セキュリティ関連サービス

AWS のセキュリティ、アイデンティティ、コンプライアンスサービスを
以下の Web ページで一覧にして公開しております。

https://aws.amazon.com/jp/products/security/

今後に向けて

本セッションでご紹介した内容を具体的な画面を見ながら進めることができるハンズオンです
AWS Builders Online Series の Web ページ内にある **関連資料コーナー** から
お試しいただけます

- **Amazon CloudFrontおよびAWS WAFを用いて エッジサービスの活用方法を学ぼう**

さいごに

- セキュリティ対策を、クラウドサービスの特徴も活かして実現し、ビジネスを成長させる下地にする

- AWS サービスを使うことで、セキュリティリスクの軽減やセキュリティリスクを特定して優先順位付けすることができる

- 自社のセキュリティ対策状況について改めて振り返る

Thank you!

AWS TRAINING & CERTIFICATION

600+ ある AWS Skill Builder の無料デジタルコースで学ぼう

30 以上の AWS ソリューションの中から、自分にもっとも関係のあるクラウドスキルとサービスにフォーカスし、自習用のデジタル学習プランとランプアップガイドで学ぶことができます。

自分に合ったスキルアップ方法で学ぼう

EXPLORE.SKILLBUILDER.AWS »

あなたのクラウドスキルを AWS 認定で証明しよう

業界で認められた資格を取得して、スキルアップの一歩を踏み出しましょう。AWS Certified の取得方法と、準備に役立つ AWS のリソースをご覧ください。

受験準備のためのリソースにアクセスしよう»

AWS Builders Online Series に ご参加いただきありがとうございます

楽しんでいただけましたか? ぜひアンケートにご協力ください。
本日のイベントに関するご意見/ご感想や今後のイベントについての
ご希望や改善のご提案などがございましたら、ぜひお聞かせください。


aws-apj-marketing@amazon.com


twitter.com/awscloud_jp


facebook.com/600986860012140


https://www.youtube.com/user/AmazonWebServicesJP


https://www.linkedin.com/showcase/aws-careers/


twitch.tv/aws