

このコンテンツは公開から3年以上経過しており内容が古い可能性があります  
最新情報については[サービス別資料](#)もしくはサービスのドキュメントをご確認ください

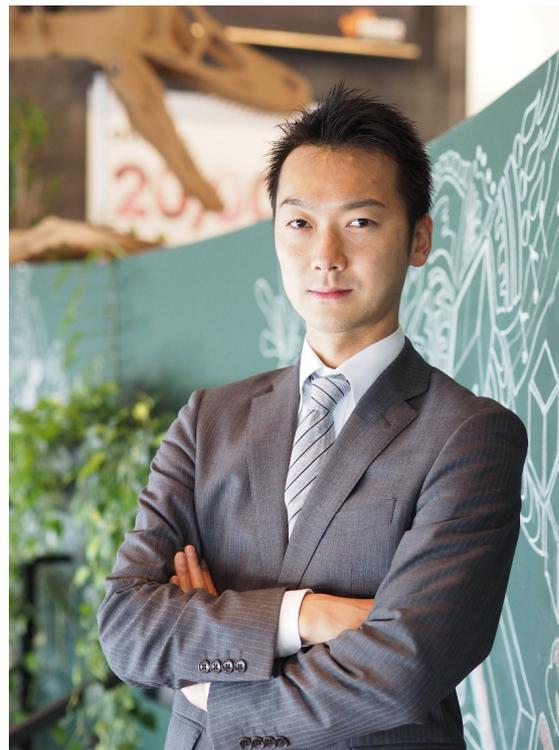


# 【AWS Black Belt Online Seminar】 Amazon Inspector

アマゾンウェブサービスジャパン株式会社  
セキュリティソリューションアーキテクト 桐山 隼人  
2016.06.22

# 自己紹介

- 氏名: 桐山 隼人
- 略歴
  - 組み込み/セキュリティ系開発エンジニア  
@ソフトウェア開発研究所
  - 技術営業@セキュリティ会社
  - ソリューションアーキテクト@AWS
- 好きなAWSサービス
  - Amazon Inspector



@hkiryam1

# 内容についての注意点

- ❏ 本資料では2016年6月22日時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(<http://aws.amazon.com>)にてご確認ください。
- ❏ 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。
- ❏ 価格は税抜表記となっております。日本居住者のお客様が東京リージョンを使用する場合、別途消費税をご請求させていただきます。

AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at <http://aws.amazon.com/agreement/>. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

# はじめに

- 本セミナーでは、自動セキュリティ診断サービスであるAmazon Inspectorを紹介します
- 様々な種類のセキュリティ診断の中でAmazon Inspectorの位置づけをご説明します
- Amazon Inspectorの効率的な使い方を例示します

# Agenda

- セキュリティ診断について
- Amazon Inspectorとは
- Amazon Inspectorの効率的な使い方



# Agenda

- セキュリティ診断について
- Amazon Inspectorとは
- Amazon Inspectorの効率的な使い方



# セキュリティ診断の目的：リスクの可視化



[> 本文へ](#) [> よくあるご質問](#) [> サイトマップ](#)

文字サイズ変更 小 **中** 大

サイト内検索  [> 拡張検索](#)

[ホーム](#)

[経済産業省について](#)

[お知らせ](#)

[政策について](#)

[統計](#)

[申請・お問合せ](#)

[English](#)

[お知らせ](#) > [ニュースリリース](#) > [2015年度一覧](#) > サイバーセキュリティ経営ガイドラインを策定しました

[> English](#)

## サイバーセキュリティ経営ガイドラインを策定しました

### 本件の概要

経済産業省は、独立行政法人情報処理推進機構とともに、「サイバーセキュリティ経営ガイドライン」を策定しました。これに基づき、経営者のリーダーシップの下でサイバーセキュリティ対策が推進されることを期待しています。

#### 1. 策定の背景

様々なビジネスの現場において、ITの利活用は企業の収益性向上に不可欠なものとなっている一方で、企業が保有する顧客の個人情報や重要な技術情報等を狙うサイバー攻撃は増加傾向にあり、その手口は巧妙化しています。

### お知らせ

[> 会見・スピーチ・談話](#)

[> ニュースリリース](#)

[> 2016年度一覧](#)

[> 2015年度一覧](#)

[> 2014年度一覧](#)

[> 2013年度一覧](#)

[> 政府広報](#)

経済産業省サイバーセキュリティ経営ガイドライン(2015年12月28日): <http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf>



# セキュリティ診断の目的：リスクの可視化

① **セキュリティリスク** 対策ポリシー策定

⑥ 予算や人材などの資源確保

② **セキュリティリスク** 対応策管理体制

⑦ 委託先のセキュリティ確認

③ **セキュリティリスク** 対処計画策定

⑧ 公的な情報共有活動への参加

④ PDCAと報告・開示

⑨ CSIRTやIRの整備と演習

⑤ サプライチェーンのセキュリティ

⑩ 経営者の説明責任

# セキュリティリスクの方程式

脅威

Threats



標的型攻撃  
マルウェア  
サイバー攻撃

脆弱性

Vulnerabilities



セキュリティホール  
設定ミス  
心理的要素

情報資産

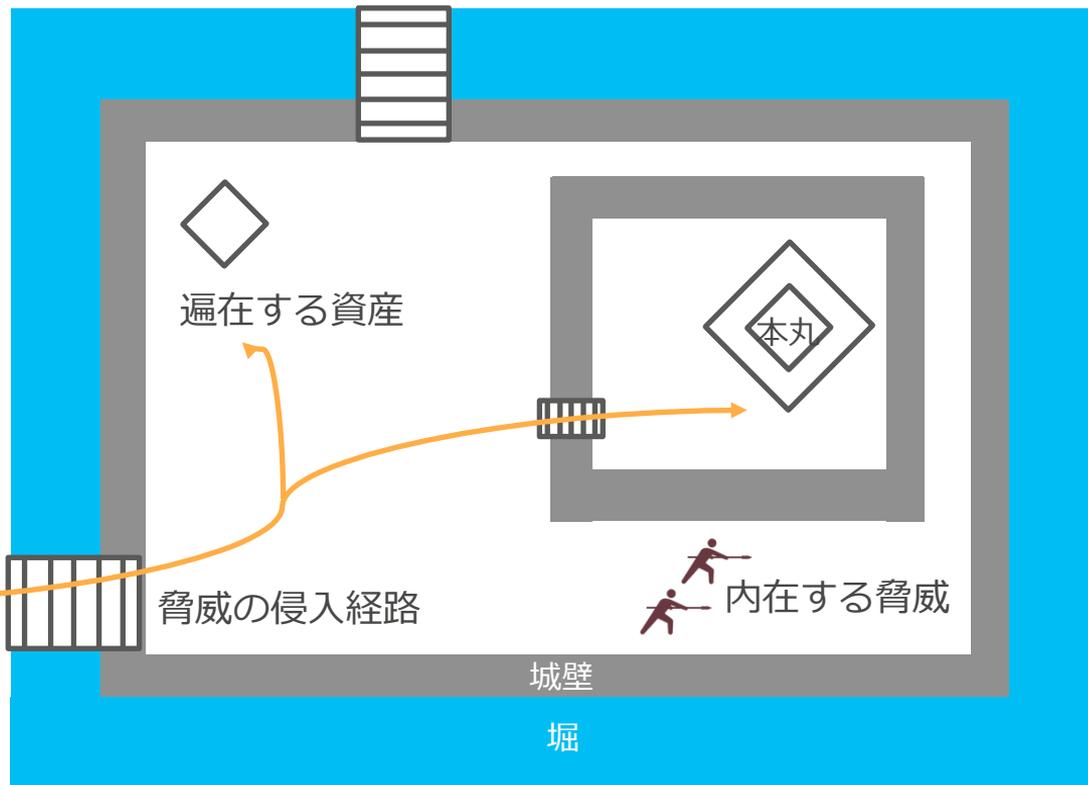
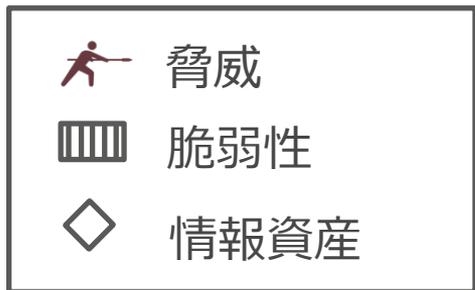
Assets



機密情報  
個人情報  
知的財産



# 城攻めに例えると・・・



# リスク要因の管理可能性

## 脅威

Threats



外部脅威の  
管理は困難

## 脆弱性

Vulnerabilities



脆弱性は社内にある  
ため対応は可能

## 情報資産

Assets



重要度はビジネス  
側の要請に依存

# リスク要因の管理可能性

## 脅威

Threats



外部脅威の  
管理は困難

## 脆弱性

Vulnerabilities



脆弱性は社内にある  
ため対応は可能

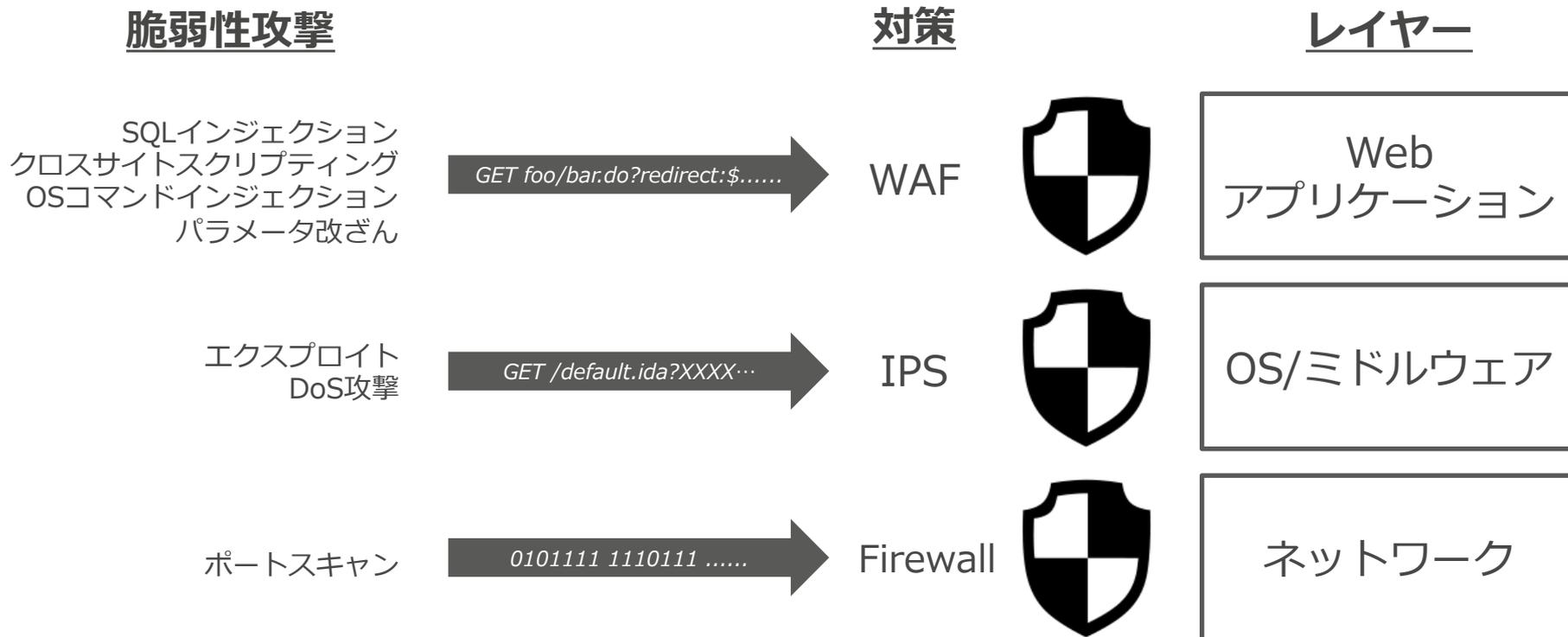
## 情報資産

Assets



重要度はビジネス  
側の要請に依存

# 脆弱性診断の種類(レイヤー)



# 脆弱性診断の種類(レイヤー)

## 診断種類

## レイヤー

Webアプリケーション診断



Web  
アプリケーション

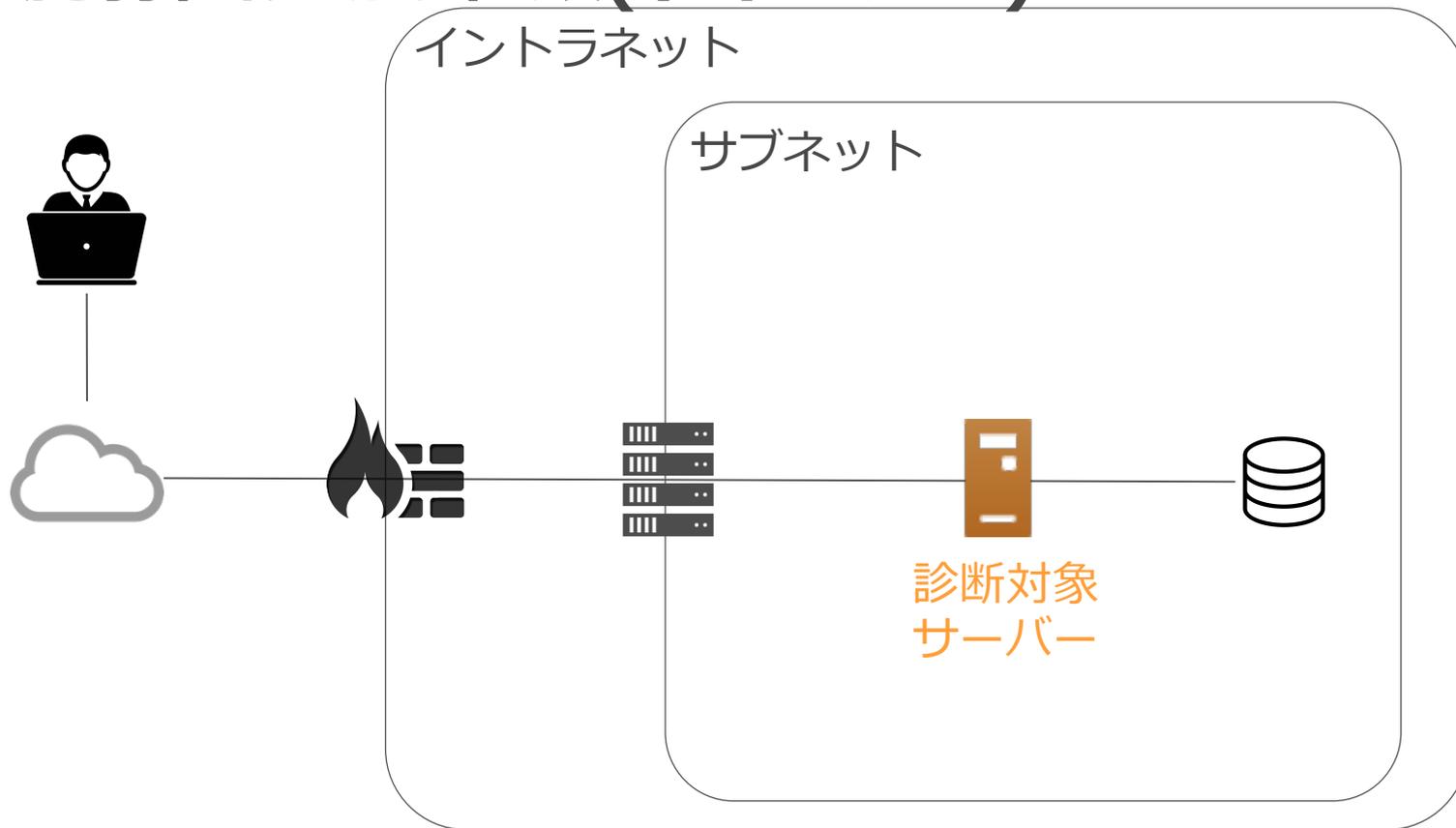
プラットフォーム診断



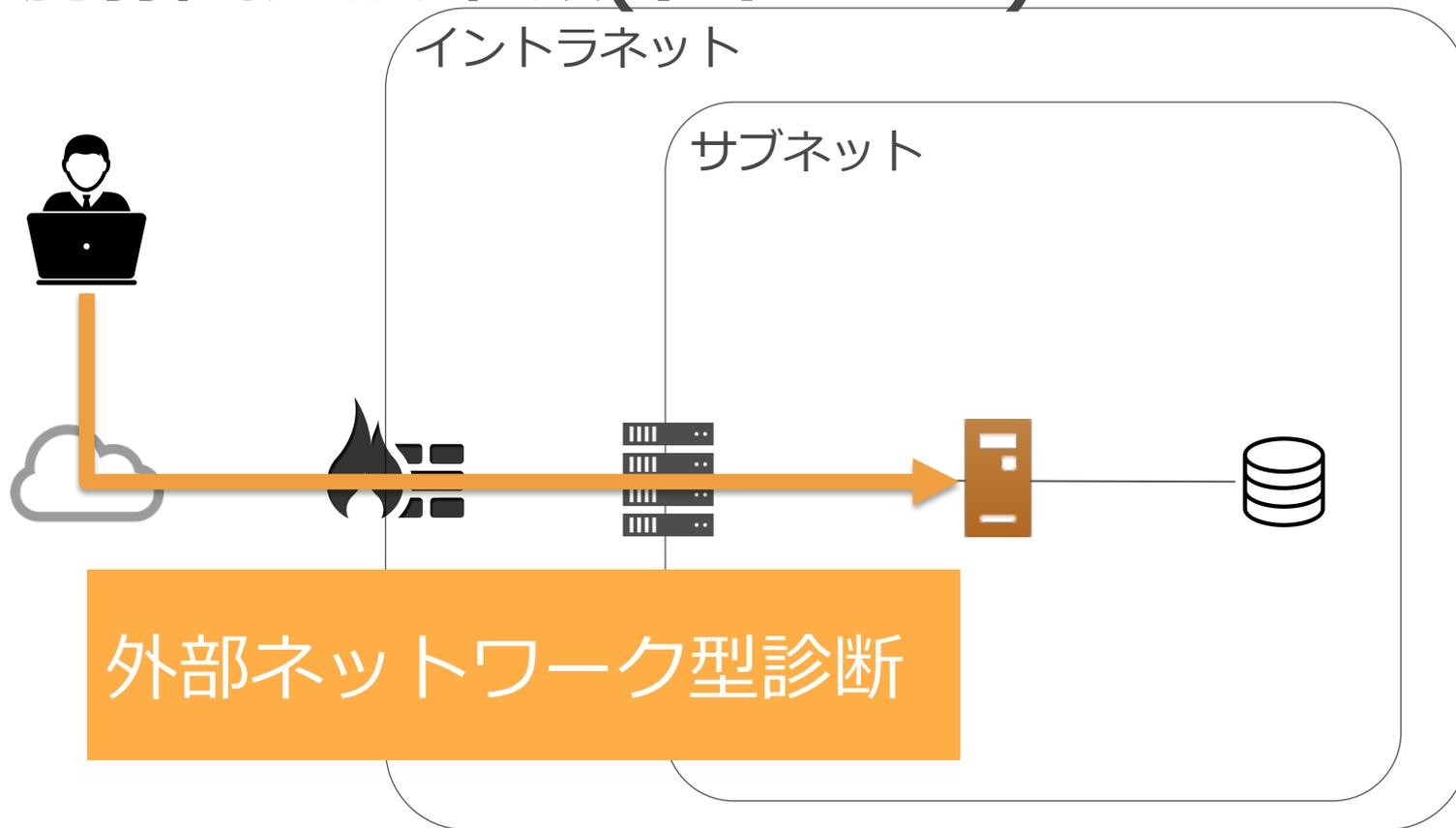
OS/ミドルウェア

ネットワーク

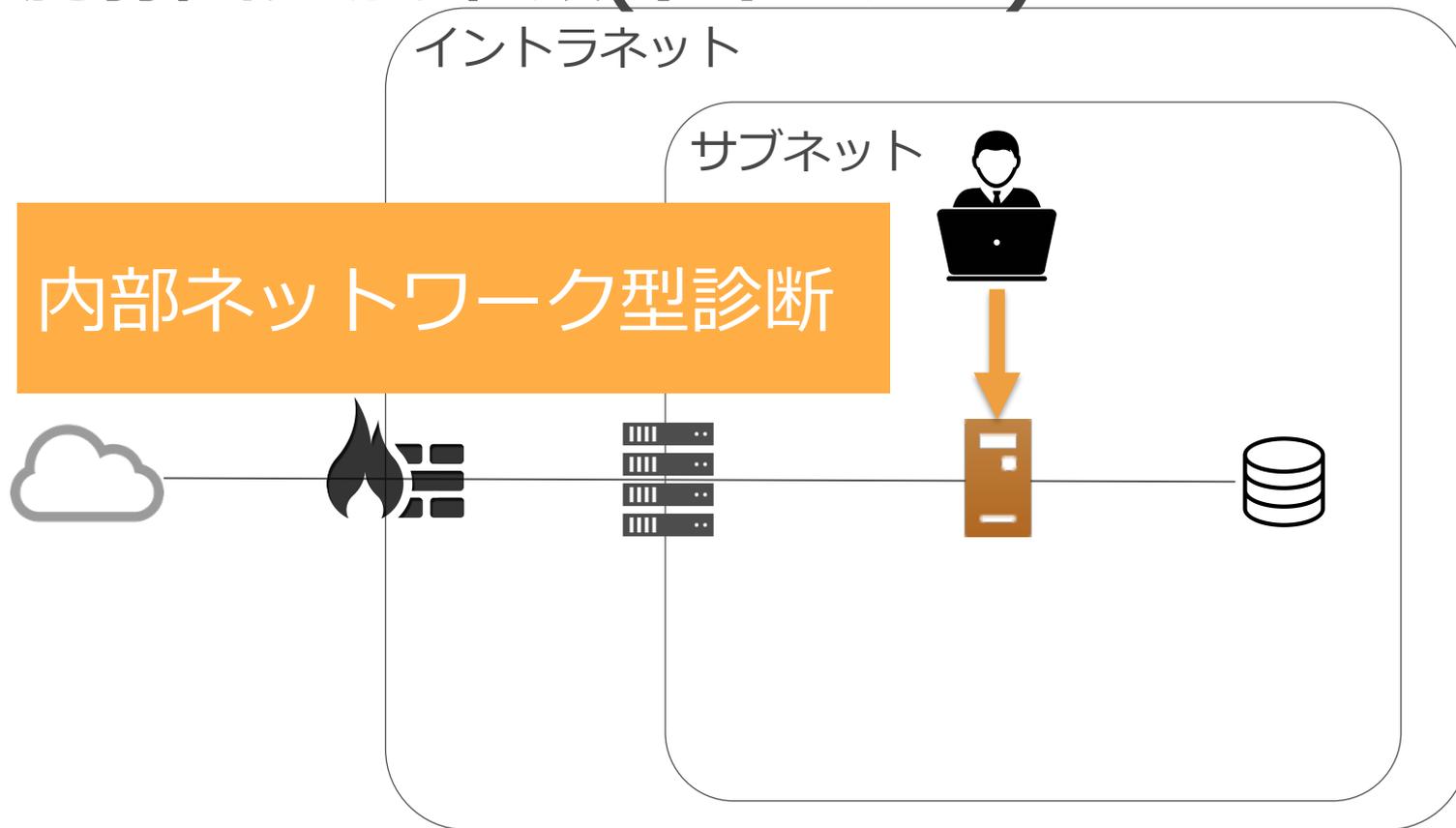
# 脆弱性診断の種類(トポロジ)



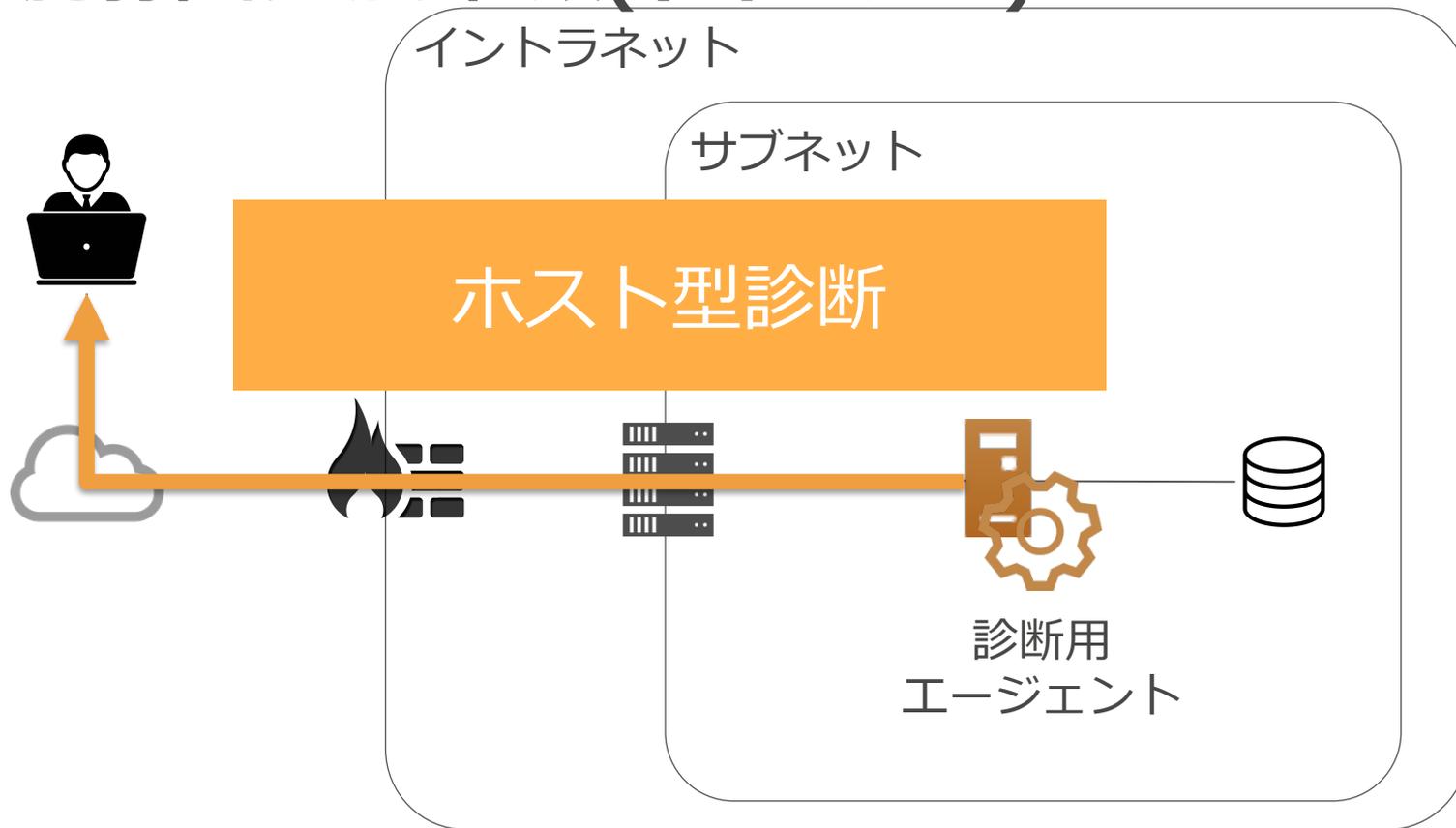
# 脆弱性診断の種類(トポロジー)



# 脆弱性診断の種類(トポロジ)



# 脆弱性診断の種類(トポロジー)



# 脆弱性診断の種類(トポロジー)

種類	目的	想定する脆弱性	実施時の例
外部ネットワーク型診断	外部攻撃からシステムを保護できるか	システム全体のセキュリティホール	システムのサービスイン時
内部ネットワーク型診断	<ul style="list-style-type: none"><li>・マルウェア感染した内部端末の攻撃からサーバーを保護できるか</li><li>・内部不正アクセスを防げるか</li></ul>	<ul style="list-style-type: none"><li>・サブネット内のセキュリティホール</li><li>・設定ミス・構成ミス</li></ul>	ネットワークやサーバー構成の変更時
ホスト型診断	各種設定が企業ポリシーに準拠しているか	設定ミス・構成ミス	監査のタイミング毎

# Agenda

- セキュリティ診断について
- Amazon Inspectorとは
- Amazon Inspectorの効率的な使い方



# Amazon Inspector が行うセキュリティ診断

Amazon EC2にエージェントを導入し、

プラットフォームの脆弱性を診断する、

ホスト型診断サービスです。



# Amazon Inspector の特長

## AWSリソースに対する



オンデマンド



自動的



詳細

## なセキュリティ評価サービス

# Amazon Inspector の特長

## AWSリソースに対する



事前申請\*いらずの



繰り返し/再利用可能な



推奨対応方法を教える

## なセキュリティ評価サービス

# Amazon Inspector が提供するもの

- ❏ システム設定や振る舞いの分析エンジン
- ❏ 組み込みルールパッケージ
- ❏ 推奨対応手順が含まれた詳細レポート
- ❏ API連携による開発プロセスとの統合

# ルールパッケージ

- 📦 CVE (Common Vulnerabilities & Exposures)
- 📦 CIS (Center for Internet Security)
  - OSのセキュリティ設定ベンチマーク
- 📦 セキュリティのベストプラクティス
- 📦 実行時の振る舞い分析

## ルールパッケージ

# CVE (Common Vulnerabilities & Exposures)

### 📦 CVEとは日本語で共通脆弱性識別子

- 個別製品中の脆弱性が対象
- 米国の非営利団体のMITRE社(<https://cve.mitre.org/>)が採番
- CVE識別番号は「CVE-西暦-連番」で構成

### 📦 EC2インスタンスが次のリストのCVEにさらされているかどうかを評価

- <https://s3-us-west-2.amazonaws.com/rules-engine/CVEList.txt>

### 📦 上記CVEリストは定期的に自動更新される

# CIS (Center for Internet Security)\*

📦 CISとは米国のインターネットセキュリティ標準化団体

- 業界標準のOSセキュリティ設定ガイド(ベンチマーク)を提供
- CIS準拠のAMIをAWS Marketplaceなどで提供



<https://benchmarks.cisecurity.org/>

Control		Set Correctly	
		Yes	No
<b>1</b>	<b>Initial Setup</b>		
<b>1.1</b>	<b>Filesystem Configuration</b>		
<b>1.1.1</b>	<b>Disable unused filesystems</b>		
1.1.1.1	Ensure mounting of cramfs filesystems is disabled (Scored)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.2	Ensure mounting of freevxfs filesystems is disabled (Scored)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.3	Ensure mounting of jffs2 filesystems is disabled (Scored)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.4	Ensure mounting of hfs filesystems is disabled (Scored)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.5	Ensure mounting of hfsplus filesystems is disabled (Scored)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.6	Ensure mounting of squashfs filesystems is disabled (Scored)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.7	Ensure mounting of udf filesystems is disabled (Scored)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.8	Ensure mounting of FAT filesystems is disabled (Scored)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	Ensure separate partition exists for /tmp (Scored)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	Ensure nodev option set on /tmp partition (Scored)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	Ensure nosuid option set on /tmp partition (Scored)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5	Ensure noexec option set on /tmp partition (Scored)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Amazon Linux Benchmarkの例

## ルールパッケージ

# セキュリティのベストプラクティス\*

項目	重要度
SSH経由のrootログインを無効化する	Medium
SSHバージョン2のみをサポート	Medium
SSH経由のパスワード認証を無効化する	Medium
パスワードの有効期限を設定する	Medium
パスワードの最小文字数を設定する	Medium
パスワードの複雑さを設定する	Medium
アドレス空間配置のランダム化(ASLR)の有効化	Medium
データ実行防止(DEP)の有効化	Medium
システムディレクトリに対するアクセス権限の設定	High

# ルールパッケージ 実行時の振る舞い分析

項目	重要度
安全でないクライアントプロトコル(ログイン)	Medium
安全でないクライアントプロトコル(一般)	Low
未使用のリッスンするTCPポート	Informational
安全でないサーバープロトコル	Informational
データ実行防止(DEP)のないソフトウェア*	Medium
スタックCookieがないソフトウェア*	Medium
安全でないアクセス権限を持つrootプロセス*	High



# Amazon Inspector

Amazon Inspector は、AWS リソースの動作を分析することができ、セキュリティ上の問題を識別するために役立ちます。

今すぐ始める



インストール



実行



分析

# Amazon Inspector 使用手順



インストール

1. 前提条件
2. 評価ターゲットの定義
3. 評価テンプレートの定義
4. 確認

## Amazon Inspector 前提条件 ?

---

### ロールを作成する

Amazon Inspector の AWS アカウントへのアクセスを許可するロールを作成します。 [詳細情報](#)。

Amazon Inspector ロール\* inspector ロールの選択または作成

---

### EC2 インスタンスへのタグの付加

Amazon Inspector は、AWS EC2 インフラストラクチャで実行中のリソースに対してセキュリティ評価を実行します。開始するには、最初に評価ターゲットに含めたい EC2 のインスタンスにタグ付けをする必要があります。 [詳細情報](#)。

[EC2 インスタンスへのタグの付加](#)

---

### AWS エージェントを EC2 インスタンスへインストール

AWS エージェントはそれ自身がインストールされている EC2 インスタンスの動作をモニタリングします。評価のターゲットに含めたいそれぞれの EC2 のインスタンスに AWS エージェントをインストールする必要があります。

[AWS エージェントのインストール](#)

---

\*必須 キャンセル 続行

# Amazon Inspector 使用手順



インストール

1. 前提条件
2. 評価ターゲットの定義
3. 評価テンプレートの定義
4. 確認

## Amazon Inspector 前提条件

ロールを作成する

Amazon Inspector の AWS アカウントへのアクセスを許可するロールを作成します。 [詳細情報](#)。

Amazon Inspector ロール\* inspector ロールの選択または作成

Amazon Inspector is requesting permission to use resources in your account

EC2 インスタンス Click Allow to give Amazon Inspector read-only access to resources in your account.

Amazon Inspector は  
に評価ターゲットに含め

[EC2 インスタンス](#)

▼ 詳細を非表示

ロールの概要 ⓘ

ロールの説明 Provides access to describe Amazon EC2 instances.

IAM ロール inspector

ポリシー名 新しいロールポリシーの作成

▶ ポリシードキュメントを表示

\*必須 許可しない 許可

# Amazon Inspector 使用手順



インストール

1. 前提条件
2. 評価ターゲットの定義
3. 評価テンプレートの定義
4. 確認

## Amazon Inspector 前提条件 ?

---

### ロールを作成する

Amazon Inspector の AWS アカウントへのアクセスを許可するロールを作成します。 [詳細情報](#).

Amazon Inspector ロール\* inspector ロールの選択または作成

---

### EC2 インスタンスへのタグの付加

Amazon Inspector は、AWS EC2 インフラストラクチャで実行中のリソースに対してセキュリティ評価を実行します。開始するには、最初に評価ターゲットに含めたい EC2 のインスタンスにタグ付けをする必要があります。 [詳細情報](#).

EC2 インスタンスへのタグの付加

---

### AWS エージェントを EC2 インスタンスへインストール

AWS エージェントはそれ自身がインストールされている EC2 インスタンスの動作をモニタリングします。評価のターゲットに含めたいそれぞれの EC2 のインスタンスに AWS エージェントをインストールする必要があります。

AWS エージェントのインストール

---

\*必須 キャンセル 続行

# Amazon Inspector 使用手順



インストール

1. 前提条件
2. 評価ターゲットの定義
3. 評価テンプレートの定義
4. 確認

## Amazon Inspector 前提条件

ロールを作成する

Amazon Inspector の AWS アカウントへのアクセスを許可するロールを作成します。 [詳細情報](#).

Amazon Inspector ロール\* inspector [ロールの選択または作成](#)

### EC2 インスタンスへのタグの付加

Amazon Inspector は、AWS EC2 インフラストラクチャで実行中のリソースに対してセキュリティ評価を実行します。開始するには、最初に評価ターゲットに含めたい EC2 のインスタンスにタグ付けをする必要があります。 [詳細情報](#).

[EC2 インスタンスへのタグの付加](#)

選択項目のタグの編集 [新しいタグキーの作成](#) 最終更新日

AWS

実行	リソースタイプ	リージョン	ID	Name
<input type="checkbox"/>	EC2 インスタンス	ap-northeast-1	i-61d6a1fe	InspectorEC2Instance

\*必須 [キャンセル](#) [続行](#)

# Amazon Inspector 使用手順



インストール

1. 前提条件
2. 評価ターゲットの定義
3. 評価テンプレートの定義
4. 確認

## Amazon Inspector 前提条件 ?

---

### ロールを作成する

Amazon Inspector の AWS アカウントへのアクセスを許可するロールを作成します。 [詳細情報](#).

Amazon Inspector ロール\* inspector ロールの選択または作成

---

### EC2 インスタンスへのタグの付加

Amazon Inspector は、AWS EC2 インフラストラクチャで実行中のリソースに対してセキュリティ評価を実行します。開始するには、最初に評価ターゲットに含めたい EC2 のインスタンスにタグ付けをする必要があります。 [詳細情報](#).

[EC2 インスタンスへのタグの付加](#)

---

### AWS エージェントを EC2 インスタンスへインストール

AWS エージェントはそれ自身がインストールされている EC2 インスタンスの動作をモニタリングします。評価のターゲットに含めたいそれぞれの EC2 のインスタンスに AWS エージェントをインストールする必要があります。

[AWS エージェントのインストール](#)

---

\*必須 キャンセル 続行

# Amazon Inspector 使用手順



インストール

1. 前提条件
2. 評価ターゲットの定義
3. 評価テンプレートの定義
4. 確認

## Amazon Inspector 前提条件

ロールを作成する

Amazon Inspector の AWS アカウントへのアクセスを許可するロールを作成します。 [詳細情報](#).

Amazon Inspector ロール\* inspector [ロールの選択または作成](#)

---

### EC2 インスタンスへのタグの付加

Amazon Inspector は、AWS EC2 インフラストラクチャで実行中のリソースに対してセキュリティ評価を実行します。開始するには、最初に評価ターゲットに含めたい EC2 のインスタンスにタグ付けをする必要があります。 [詳細情報](#).

[EC2 インスタンスへのタグの付加](#)

---

### AWS エージェントを EC2 インスタンスへインストール

AWS エージェントはそれ自身がインストールされている EC2 インスタンスの動作をモニタリングします。評価のターゲットに含めたいそれぞれの EC2 のインスタンスに AWS エージェントをインストールする必要があります。

[AWS エージェントのインストール](#)

```
user@hostname:~$ wget https://d1wk0tztpsntt1.cloudfront.net/linux/latest/install
user@hostname:~$ sudo bash install
```

# Amazon Inspector 使用手順



インストール

1. 前提条件
2. 評価ターゲットの定義
3. 評価テンプレートの定義
4. 確認

## Amazon Inspector 前提条件 ?

---

### ロールを作成する

Amazon Inspector の AWS アカウントへのアクセスを許可するロールを作成します。 [詳細情報](#).

Amazon Inspector ロール\* inspector ロールの選択または作成

---

### EC2 インスタンスへのタグの付加

Amazon Inspector は、AWS EC2 インフラストラクチャで実行中のリソースに対してセキュリティ評価を実行します。開始するには、最初に評価ターゲットに含めたい EC2 のインスタンスにタグ付けをする必要があります。 [詳細情報](#).

[EC2 インスタンスへのタグの付加](#)

---

### AWS エージェントを EC2 インスタンスへインストール

AWS エージェントはそれ自身がインストールされている EC2 インスタンスの動作をモニタリングします。評価のターゲットに含めたいそれぞれの EC2 のインスタンスに AWS エージェントをインストールする必要があります。

[AWS エージェントのインストール](#)

---

\*必須 キャンセル 続行

# Amazon Inspector 使用手順



インストール

1. 前提条件
2. 評価ターゲットの定義
3. 評価テンプレートの定義
4. 確認

### 評価ターゲットの定義

評価ターゲットは、ビジネスの目的を達成するために役立つ AWS リソースのコレクションを表します。 [詳細情報](#)

名前\*

タグ\*

キー	値	
<input type="text" value="Name"/>	<input type="text" value="InspectorEC2Instance"/>	<input type="button" value="✕"/>
<input type="text" value="新しいキーを追加"/>	<input type="text"/>	<input type="button" value="✕"/>

\*必須

# Amazon Inspector 使用手順



インストール

1. 前提条件
2. 評価ターゲットの定義
3. 評価テンプレートの定義
4. 確認

## 評価テンプレートの定義

評価テンプレートでは、ルールパッケージ、期間、SNS 通知、結果にラベルを付ける方法など、評価の実行用のさまざまなプロパティを指定できます。 [詳細情報](#)。

名前\*

ルールパッケージ\*

Amazon Inspector は、選択されたルールパッケージに対して評価ターゲットの評価を実行します。 [詳細情報](#)。

所要時間\*

Amazon Inspector のデフォルトの評価テンプレートの所要時間は 1 時間です。所要時間は変更できますが、所要時間が長い評価テンプレートでは、より詳細な結果が得られます。

\*必須

[キャンセル](#)

[戻る](#)

[続行](#)

# Amazon Inspector 使用手順



インストール

1. 前提条件
2. 評価ターゲットの定義
3. 評価テンプレートの定義
4. 確認

## 確認

ターゲットとテンプレートの詳細を確認します。その後 AWS エージェントをまだインストールしていない場合は **作成** を、AWS エージェントをインストールしている場合は **作成および実行** を選択します。

### 評価ターゲットの定義 編集

名前 MyTarget

タグ	キー	値
	<input type="text" value="Name"/>	<input type="text" value="InspectorEC2Instance"/>

### 評価テンプレートの定義 編集

名前 MyFirstTemplate

ルールパッケージ [Common Vulnerabilities and Exposures-1.1](#)

所要時間 1時間 (推奨)

評価の実行では、評価ターゲットを構成するすべての EC2 インスタンスで AWS エージェントを実行する必要があります。AWS エージェントをまだデプロイしていない場合は評価テンプレートを作成できますが、評価を実行する前に AWS エージェントのインストールをしてください。

キャンセル プレビュー 戻る **作成**

# Amazon Inspector 使用手順



実行

## 1. 評価の実行

### Amazon Inspector - 評価テンプレート

評価テンプレートでは、ルールパッケージ、期間、SNS 通知、結果にラベルを付ける方法など、評価の実行用のさまざまなプロパティを指定できます。[詳細情報](#)。

作成 **実行** 停止 削除 クローン Last updated on 2016/6/21 5:45:55 AM (0m ago)   

Filter 1 selected << < Viewing 1-1 of 1 > >>

<input type="checkbox"/>	名前	所要時間	ターゲット名	直前の実行	すべて...
<input checked="" type="checkbox"/>	▶ MyFirstTemplate	1 Hour	MyTarget	なし	0

### Amazon Inspector - 評価の実行

評価の実行は、選択されたルールパッケージに対する評価ターゲットの動作分析を通じて、セキュリティ上の問題を発見するプロセスです。[詳細情報](#)。

実行 停止 削除 Last updated on 2016/6/21 5:46:56 AM (0m ago)   

Filter << < Viewing 1-1 of 1 > >>

<input type="checkbox"/>	開始時刻	ステータス	テンプレート名	結果
<input type="checkbox"/>	▶ Today at 5:46 AM (GMT+9)	データを収集中	MyFirstTemplate	0

# Amazon Inspector 使用手順



分析

1. 分析結果の表示
2. 推奨事項の確認

### Amazon Inspector - 結果

結果は、指定された評価ターゲットに対して Amazon Inspector が評価を実行した後に発見された考えられるセキュリティ上の問題です。詳細情報。

属性の追加 編集 Last updated on 2016/6/21 6:49:50 AM (0m ago)   

Filter Viewing 1-10 of 60 >>

<input type="checkbox"/>	重要度 	結果	ターゲット	テンプレート	ルールパッケージ
<input type="checkbox"/>	High	Instance i-61d6a1fe is vulnerable to CVE-2016-3115	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1
<input type="checkbox"/>	High	Instance i-61d6a1fe is vulnerable to CVE-2014-2583	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1
<input type="checkbox"/>	High	Instance i-61d6a1fe is vulnerable to CVE-2015-7547	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1
<input type="checkbox"/>	High	Instance i-61d6a1fe is vulnerable to CVE-2015-2327	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1
<input type="checkbox"/>	High	Instance i-61d6a1fe is vulnerable to CVE-2015-8382	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1
<input type="checkbox"/>	High	Instance i-61d6a1fe is vulnerable to CVE-2015-8385	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1
<input type="checkbox"/>	High	Instance i-61d6a1fe is vulnerable to CVE-2016-2381	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1
<input type="checkbox"/>	High	Instance i-61d6a1fe is vulnerable to CVE-2015-3238	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1
<input type="checkbox"/>	High	Instance i-61d6a1fe is vulnerable to CVE-2015-7499	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1
<input type="checkbox"/>	High	Instance i-61d6a1fe is vulnerable to CVE-2016-2108	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1

# Amazon Inspector 使用手順



分析

1. 分析結果の表示
2. 推奨事項の確認

重要度	結果	ターゲット	テンプレート	ルールパッケージ
High	Instance i-61d6a1fe is vulnerable to CVE-2016-3115	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1

評価ターゲットの結果 - MyTarget

ターゲット名 MyTarget

テンプレート名 MyFirstTemplate

開始 Today at 5:46 AM (GMT+9)

終了 Today at 6:49 AM (GMT+9)

ステータス 分析完了

ルールパッケージ Common Vulnerabilities and Exposures-1.1

AWS エージェント ID i-61d6a1fe

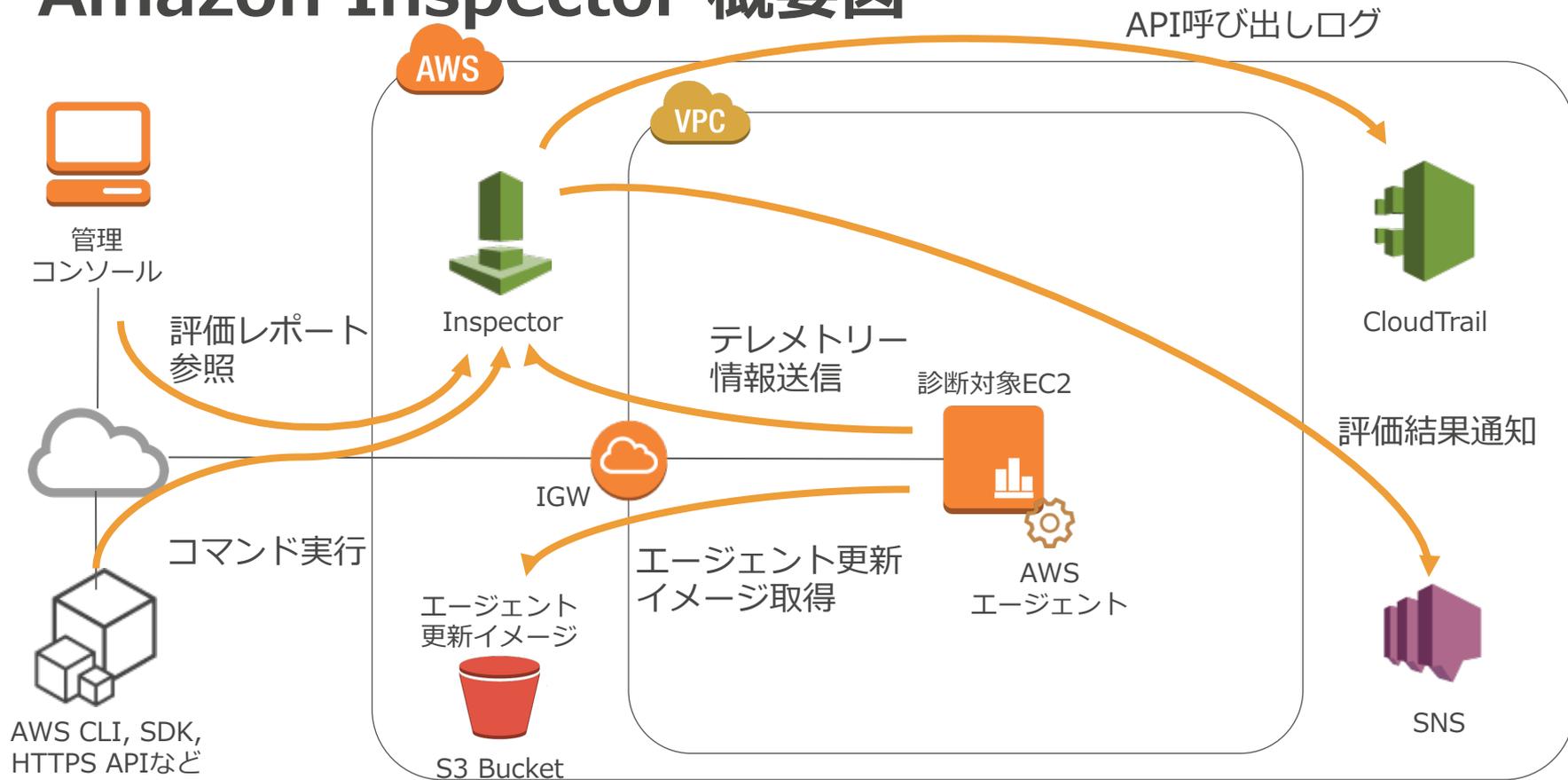
結果 Instance i-61d6a1fe is vulnerable to CVE-2016-3115

重要度 High

説明 Multiple CRLF injection vulnerabilities in session.c in sshd in OpenSSH before 7.2p2 allow remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data, related to the (1) `doauthenticated1` and (2) `sessionx11_req` functions.

**推奨事項** Use your Operating System's update feature to update package `openssh-server`, `openssh-server-1:6.6p1-2ubuntu2.4`. For more information see <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3115>

# Amazon Inspector 概要図



# AWSエージェント要件

- ❏ パブリックエンドポイントへのネットワークパス
  - Amazon Inspectorサービスエンドポイント
  - Amazon S3サービスエンドポイント
- ❏ サービスエンドポイントとのTLS通信
  - 全ての接続はAWSエージェントからのアウトバウンド通信で確立
  - セキュリティグループでインバウンド通信を許可する必要なし
  - 経路中にプロキシサーバーがある場合は利用不可
- ❏ インストールにはOSの管理者権限が必要

# AWSエージェントのサポートOS

- 📦 Red Hat Enterprise Linux (7.2 or later)
- 📦 CentOS (7.2 or later)
- 📦 Ubuntu (14.04 LTS or later)
- 📦 Amazon Linux (2015.03 or later)
- 📦 Microsoft Windows (2012, 2008 R2) - Preview

# 使用可能リージョン

- 📦 米国東部 (バージニア北部) [us-east-1]
- 📦 米国西部 (オレゴン) [us-west-2]
- 📦 EU (アイルランド) [eu-west-1]
- 📦 アジアパシフィック (東京) [ap-northeast-1]

# 料金

\*エージェント評価 = 1 エージェント1 評価あたり

任意の月	エージェント評価*ごとの料金
最初の250回のエージェント評価	0.30 USD
次の750回のエージェント評価	0.25 USD
次の4,000回のエージェント評価	0.15 USD
次の45,000回のエージェント評価	0.10 USD
その他すべてのエージェント評価	0.05 USD

無料トライアル：

利用開始から90日間、最初の250回のエージェント評価は**無料**

# Agenda

- セキュリティ診断について
- Amazon Inspectorとは
- Amazon Inspectorの効率的な使い方



# Amazon Inspectorの使い時



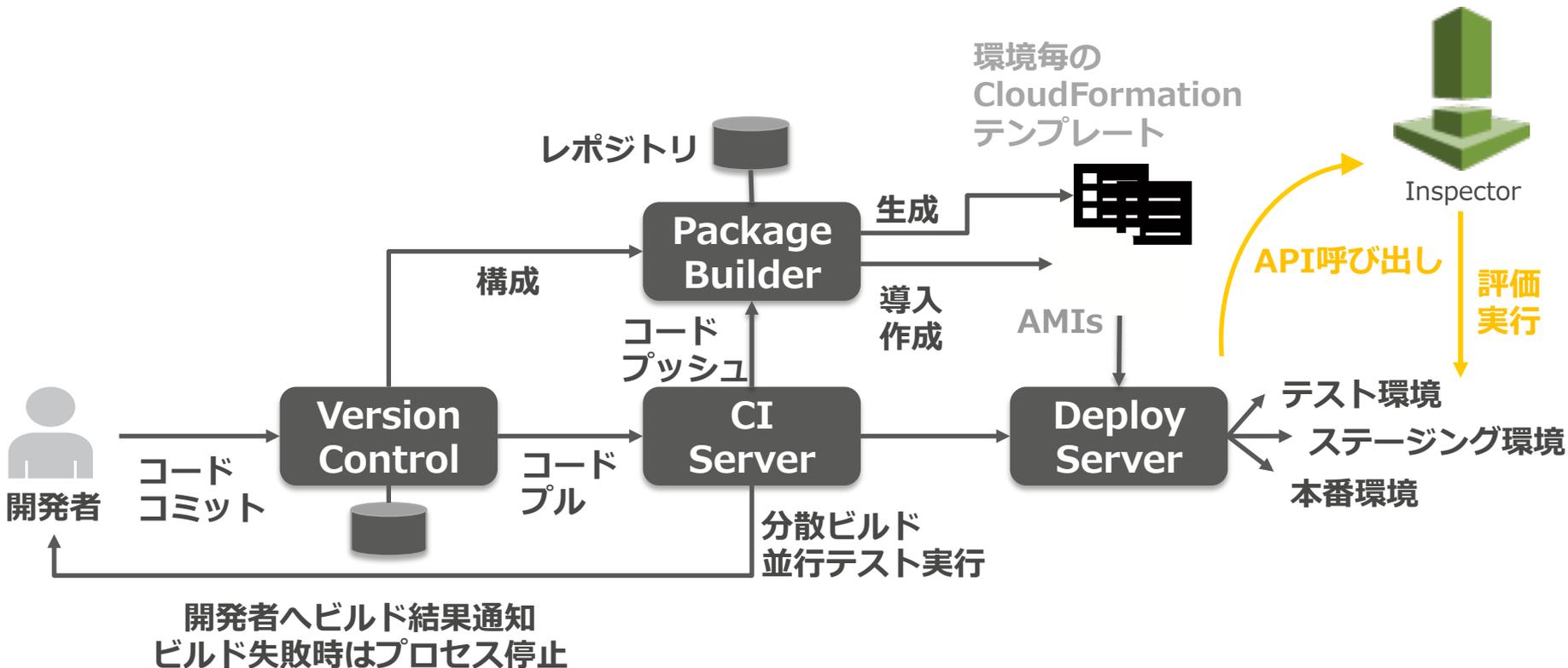
設計開発時



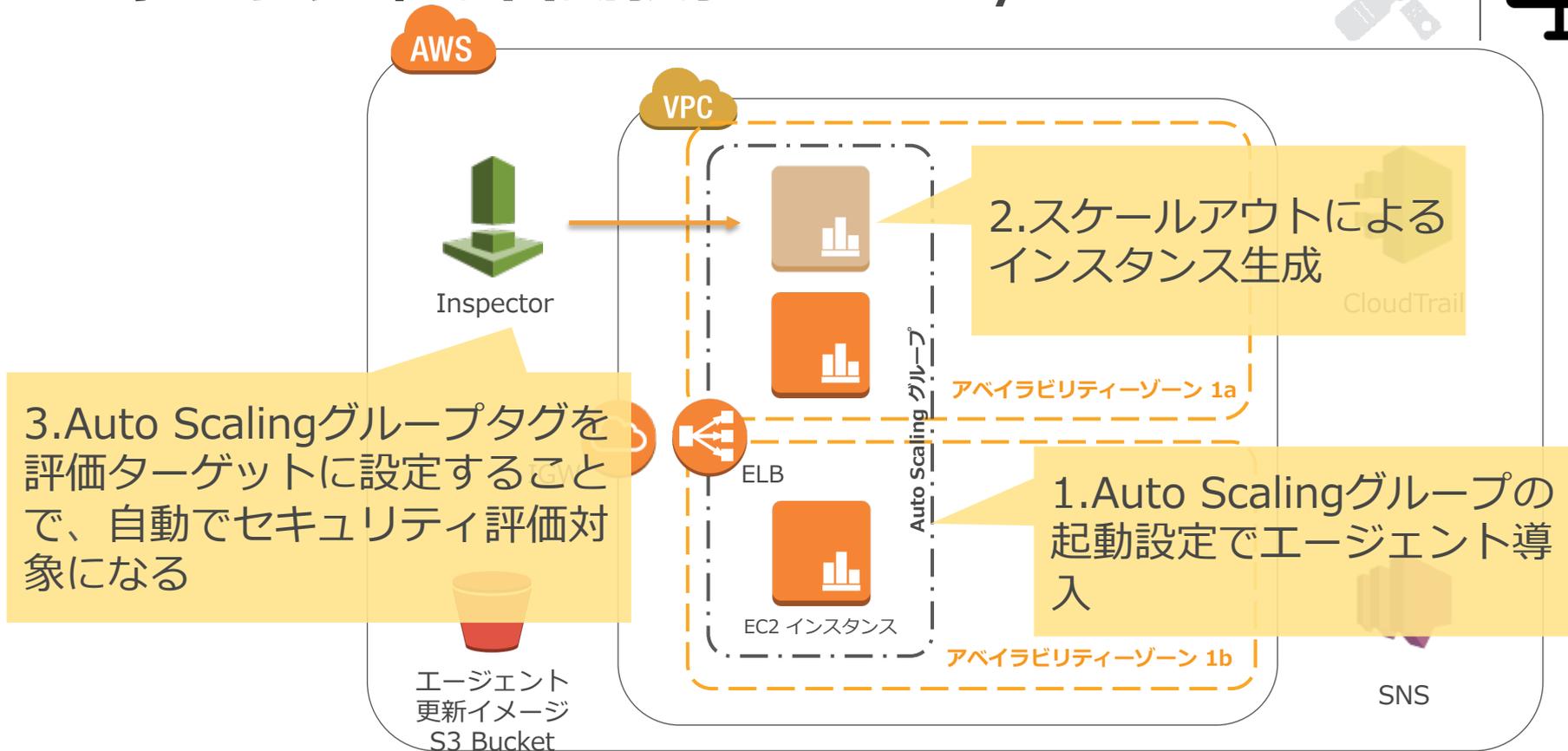
本番運用時

どちらのフェーズでも使用できる

# 継続的なデプロイ+セキュリティ評価



# セキュリティの自動拡張 - Security at Scale -



# 評価結果対応の簡易ワークフロー



Amazon Inspector - 結果

結果は、指定された評価ターゲットに対して Amazon Inspector が評価を実行した後に発見された考えられるセキュリティ上の問題です。詳細情報。

属性の追加編集

Last updated on 2016/6/21 7:35:42 AM (0m ago)

属性の設定

キー	値
新しいキーを追加	新しい値を追加

キャンセル 保存

評価結果に属性を追加することで、  
対応処理の簡易ワークフローが実現可能  
例) キー:状況, 値:緊急  
      キー:担当者, 値:田中

評価テンプレート - MyFirstTemplate

名前\* MyFirstTemplate

ターゲット名\* MyTarget

ルールパッケージ\* Common Vulnerabilities and Exposures-1.1  
Inspector ルールパッケージの選択

所要時間\* 1時間 (推奨)

タグ

キー	値
新しいキーを追加	

結果に追加された属性

キー	値
新しいキーを追加	新しい値を追加

評価結果のデフォルト属性を設定可  
例) キー:担当者, 値:共通基盤チーム

## まとめ : Amazon Inspectorは . . .

- 📦 ホスト型プラットフォーム脆弱性診断
- 📦 オンデマンド・自動化・詳細なサービス
- 📦 いつでも何度でも簡単に使える

# 参考資料

- Amazon Inspector メインページ:
  - <http://aws.amazon.com/inspector>
- クイックスタート演習:
  - [https://docs.aws.amazon.com/inspector/latest/userguide/inspector\\_quickstart.html](https://docs.aws.amazon.com/inspector/latest/userguide/inspector_quickstart.html)
- FAQ:
  - <http://aws.amazon.com/inspector/faqs>
- 料金:
  - <http://aws.amazon.com/inspector/pricing>
- お客様の声:
  - <http://aws.amazon.com/inspector/customers>
- パートナー:
  - <http://aws.amazon.com/inspector/partners>

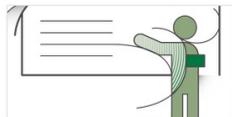
# オンラインセミナー資料の配置場所

- AWS クラウドサービス活用資料集

- <http://aws.amazon.com/jp/aws-jp-introduction/>

## 日本語資料のカテゴリ一覧

本資料集では、この利便性を皆様にも活用していただけるよう、トレーニング、ソリューション/事例、ブログト別、セキュリティ・コンプライアンス、その他という5つのカテゴリで資料をご用意いたしております。



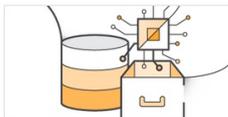
トレーニング資料

はじめてAWSをご利用いただくお客様向けに、AWSの概要、アカウント作成に関するご案内をいたします。



ソリューション・事例紹介資料

実際に他のお客様がどのようにAWSをご利用いただいているかをご覧いただける参考資料をご覧いただけます。



製品・サービス別資料

無料オンラインセミナー「AWS Black Belt Tech Webinar」や各種セミナーで紹介された、ソリューションアーキテクトによる各サービスの解説資料をご覧いただけます。

- AWS Solutions Architect ブログ

- 最新の情報、セミナー中のQ&A等が掲載されています

- <http://aws.typepad.com/sajp/>

# 公式Twitter/Facebook AWSの最新情報をお届けします



@awscloud\_jp



検索



もしくは  
<http://on.fb.me/1vR8yWm>

最新技術情報、イベント情報、お役立ち情報、  
お得なキャンペーン情報などを日々更新しています！

# AWSの導入、お問い合わせのご相談

- AWSクラウド導入に関するご質問、お見積り、資料請求をご希望のお客様は、以下のリンクよりお気軽にご相談ください

<https://aws.amazon.com/jp/contact-us/aws-sales/>

<p>お問い合わせ</p> <p>日本担当チームへのお問い合わせ &gt;</p> <p>関連リンク</p> <p>フォーラム</p>	<h2>日本担当チームへのお問い合わせ</h2> <p>AWS クラウド導入に関するご質問、お見積り、資料請求をご希望のお客様は、以下のフォームよりお気軽にご相談ください。平日営業時間内に日本オフィス担当者よりご連絡させていただきます。</p> <p>※ご請求金額またはアカウントに関する質問は<a href="#">こちらからお問い合わせください</a>。 ※Amazon.com または Kindle のサポートにお問い合わせは<a href="#">こちらからお問い合わせください</a>。</p> <p>アスタリスク(*)は必須情報となります。</p> <p>姓*</p> <input type="text"/> 名* <input type="text"/>
---	--