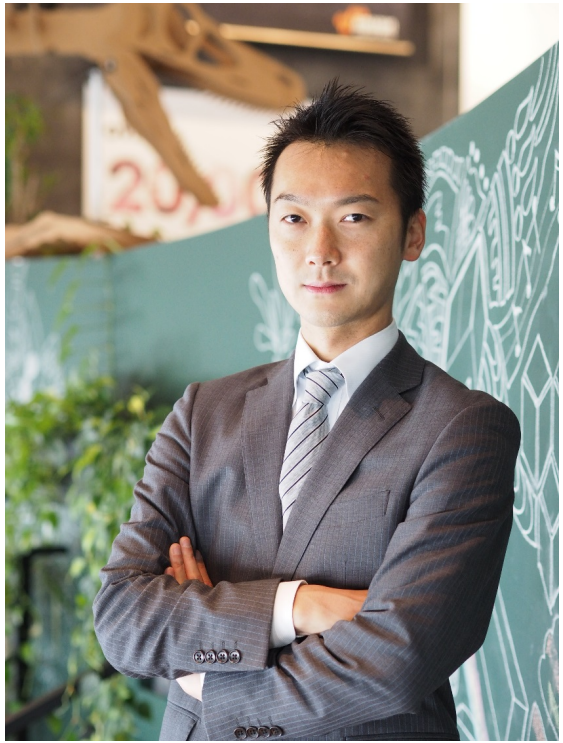
【AWS Black Belt Online Seminar】 Amazon Inspector

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



@hkiriyam1

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います。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

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

②セキュリティリスク対応策管理体制

③セキュリティリスク対処計画策定

④PDCAと報告・開示

⑤サプライチェーンのセキュリティ

⑥予算や人材などの資源確保

⑦委託先のセキュリティ確認

⑧公的な情報共有活動への参加

⑨CSIRTやIRの整備と演習

⑩経営者の説明責任

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

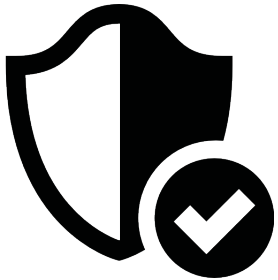
セキュリティリスクの方程式

脅威
Threats

標的型攻撃
マルウェア
サイバー攻撃

×

脆弱性
Vulnerabilities



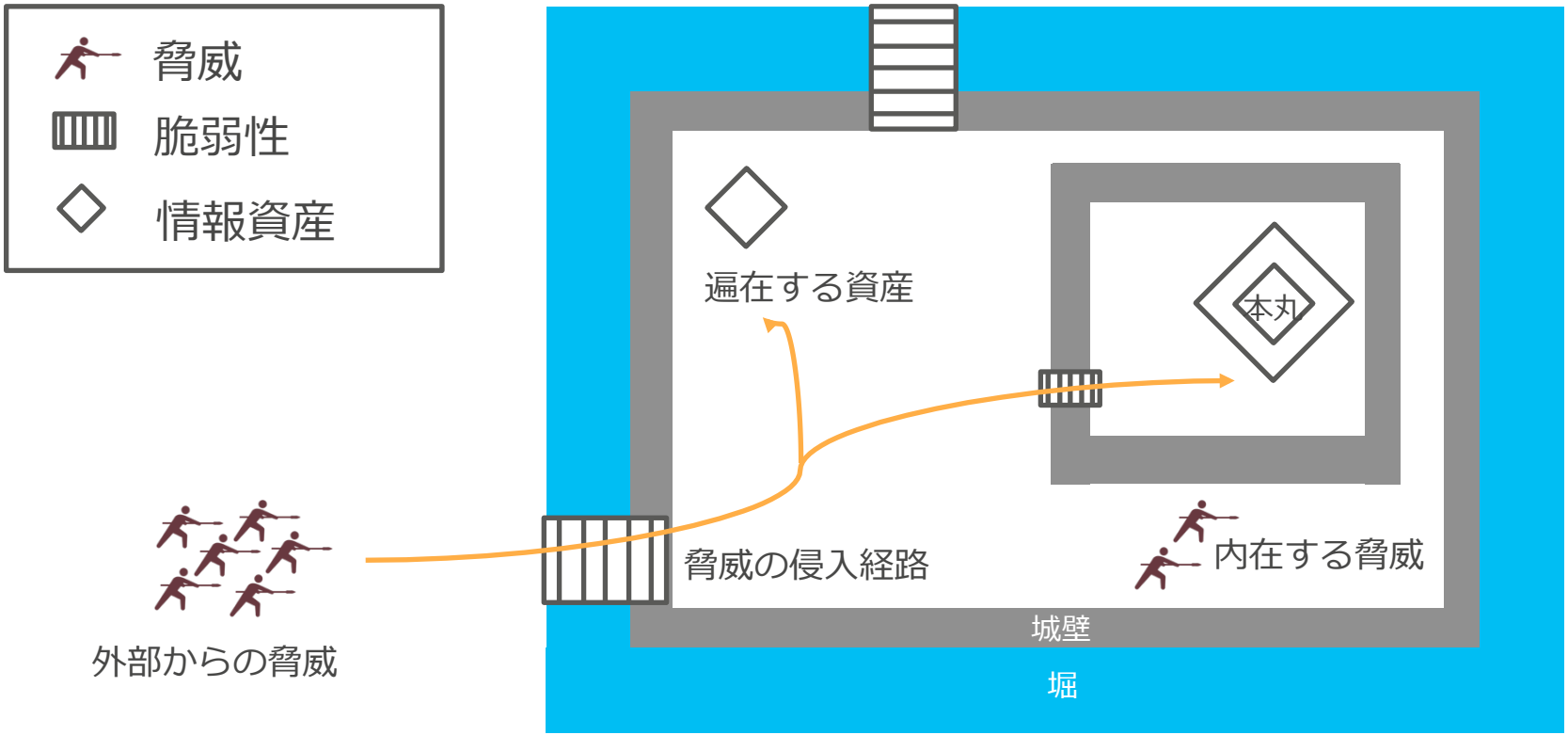
セキュリティホール
設定ミス
心理的要素

×

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・・・



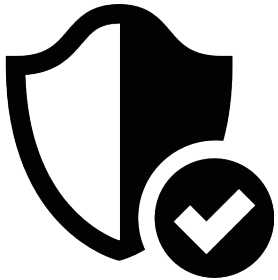
リスク要因の管理可能性

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

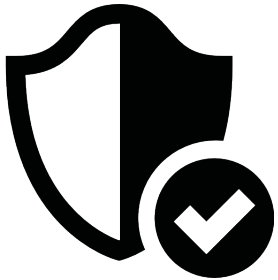
リスク要因の管理可能性

脅威
Threats

外部脅威の
管理は困難

×

脆弱性
Vulnerabilities



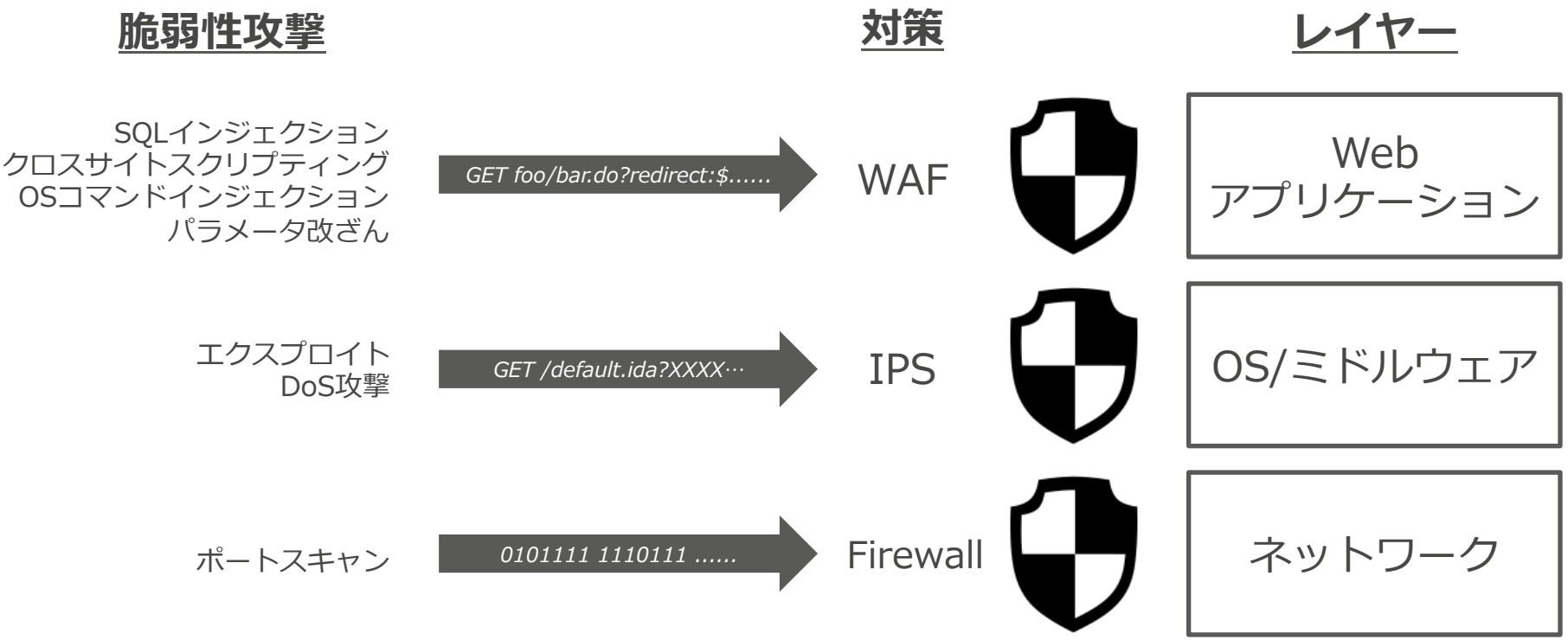
脆弱性は社内にある
ため対応は可能

×

情報資産
Assets

重要度はビジネス
側の要請に依存

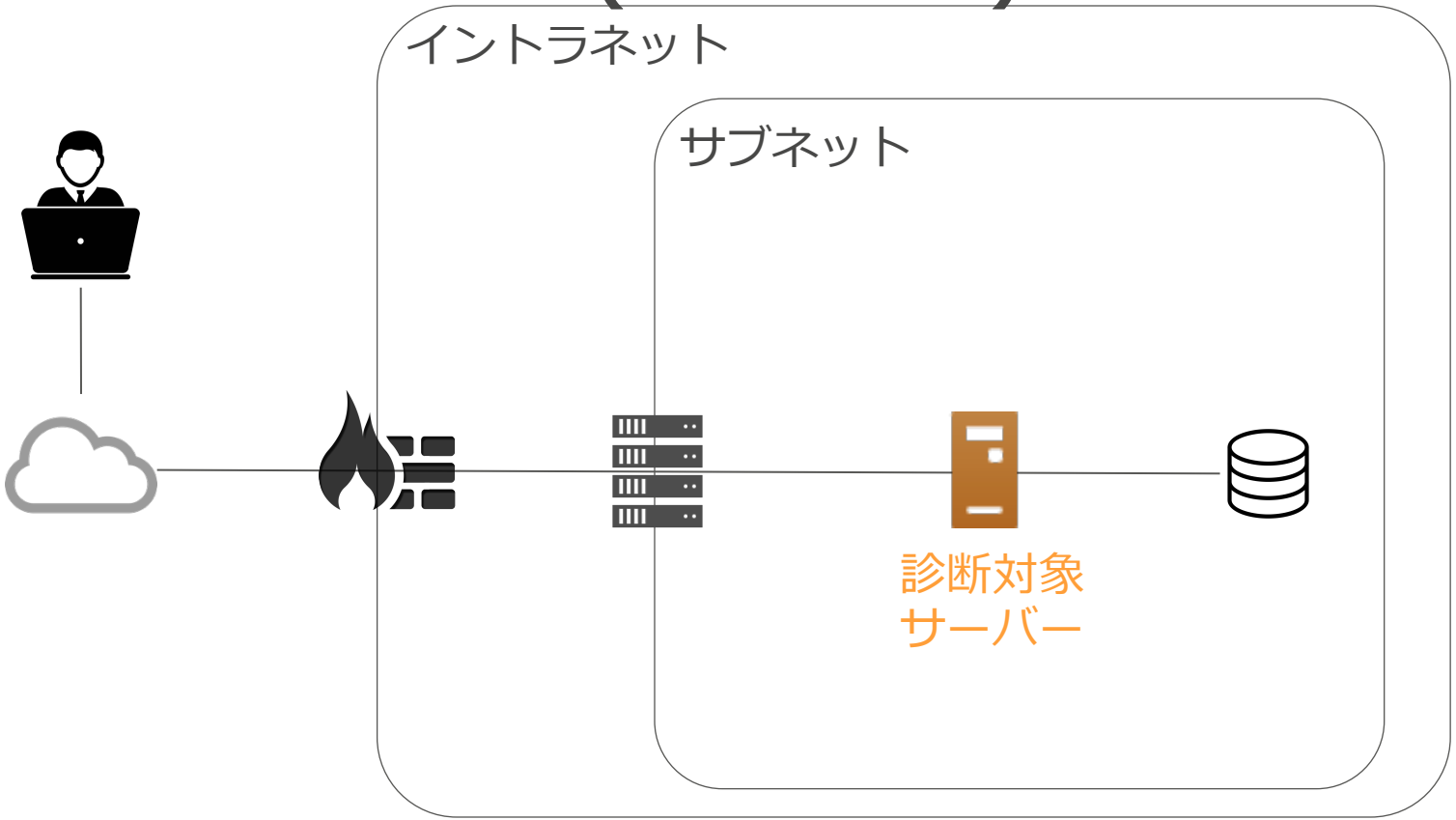
脆弱性診断の種類(レイヤー)



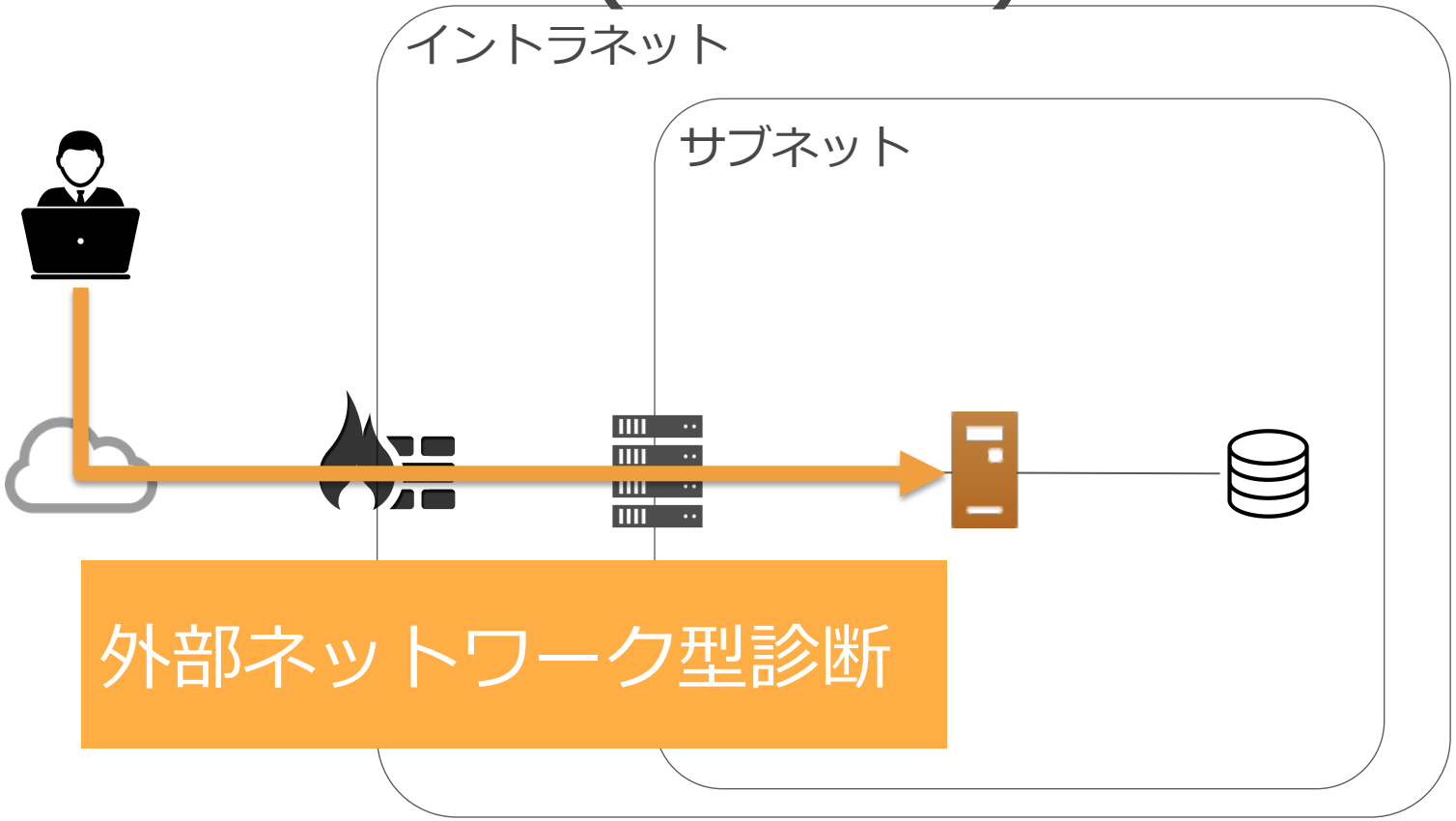
脆弱性診断の種類(レイヤー)

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

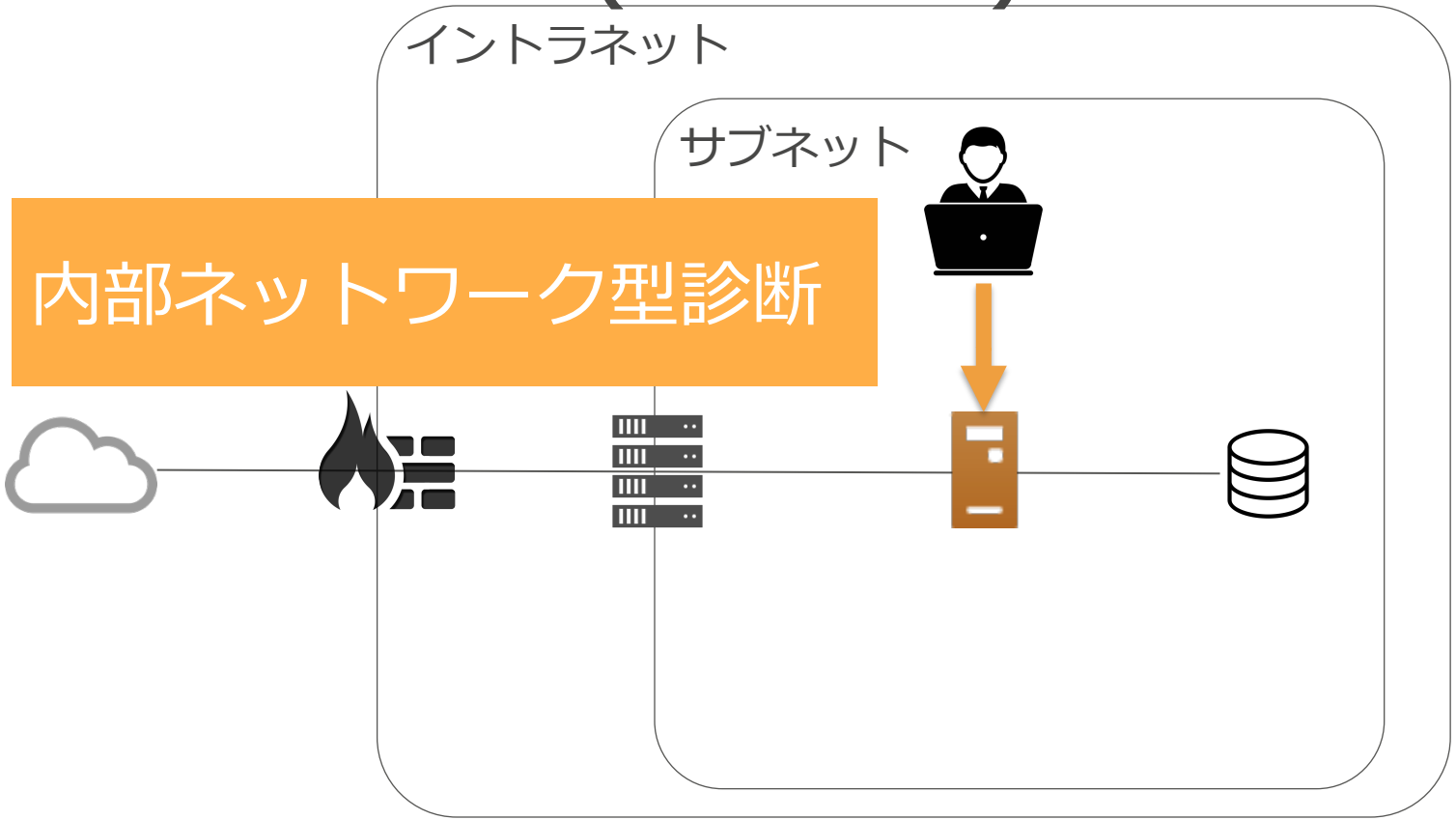
脆弱性診断の種類(トポロジー)



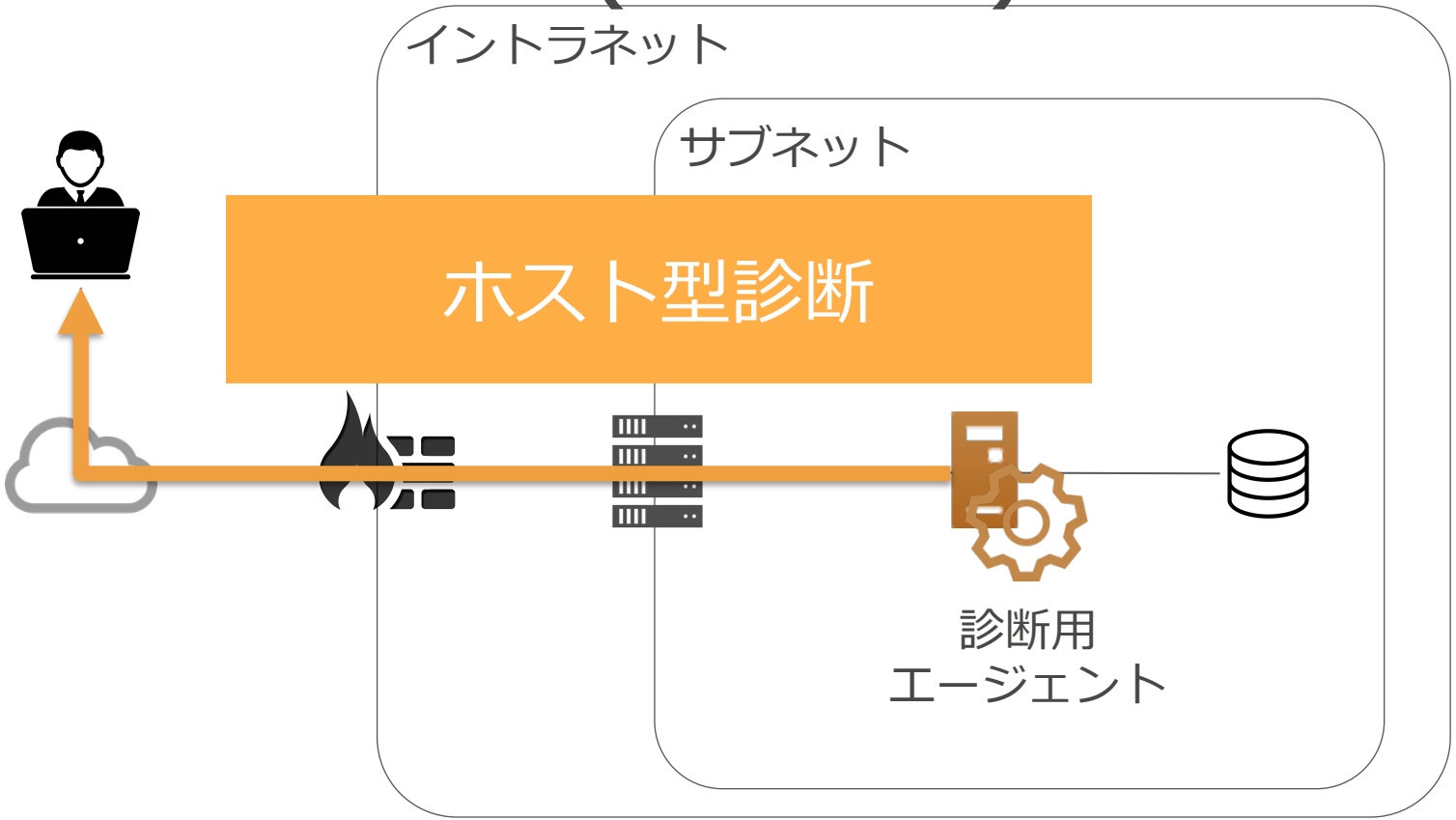
脆弱性診断の種類(トポロジー)



脆弱性診断の種類(トポロジー)



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	・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 ・内部不正アクセスを防げるか	・サブネット内のセキュリティホール ・設定ミス・構成ミス	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 Web Services 侵入テスト
https://aws.amazon.com/jp/security/penetration-testing/

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

ルールパッケージ
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
1	**Initial Setup**		
1.1	**Filesystem Configuration**		
1.1.1	**Disable unused filesystems**		
1.1.1.1	Ensure mounting of cramfs filesystems is disabled (Scored)	☐	☐
1.1.1.2	Ensure mounting of freevxfs filesystems is disabled (Scored)	☐	☐
1.1.1.3	Ensure mounting of jffs2 filesystems is disabled (Scored)	☐	☐
1.1.1.4	Ensure mounting of hfs filesystems is disabled (Scored)	☐	☐
1.1.1.5	Ensure mounting of hfsplus filesystems is disabled (Scored)	☐	☐
1.1.1.6	Ensure mounting of squashfs filesystems is disabled (Scored)	☐	☐
1.1.1.7	Ensure mounting of udf filesystems is disabled (Scored)	☐	☐
1.1.1.8	Ensure mounting of FAT filesystems is disabled (Scored)	☐	☐
1.1.2	Ensure separate partition exists for /tmp (Scored)	☐	☐
1.1.3	Ensure nodev option set on /tmp partition (Scored)	☐	☐
1.1.4	Ensure nosuid option set on /tmp partition (Scored)	☐	☐
1.1.5	Ensure noexec option set on /tmp partition (Scored)	☐	☐

CIS Amazon Linux Benchmarkの例

*本ルールパッケージはAmazon Linux 2015.03を実行しているEC2インスタンスのみ有効(2016年6月22日時点)

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

*本ルールパッケージはLinuxベースのOSを実行しているEC2インスタンスのみ有効(2016年6月22日時点)

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

*の項目はLinuxベースのOSを実行しているEC2インスタンスのみ有効(2016年6月22日時点)

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

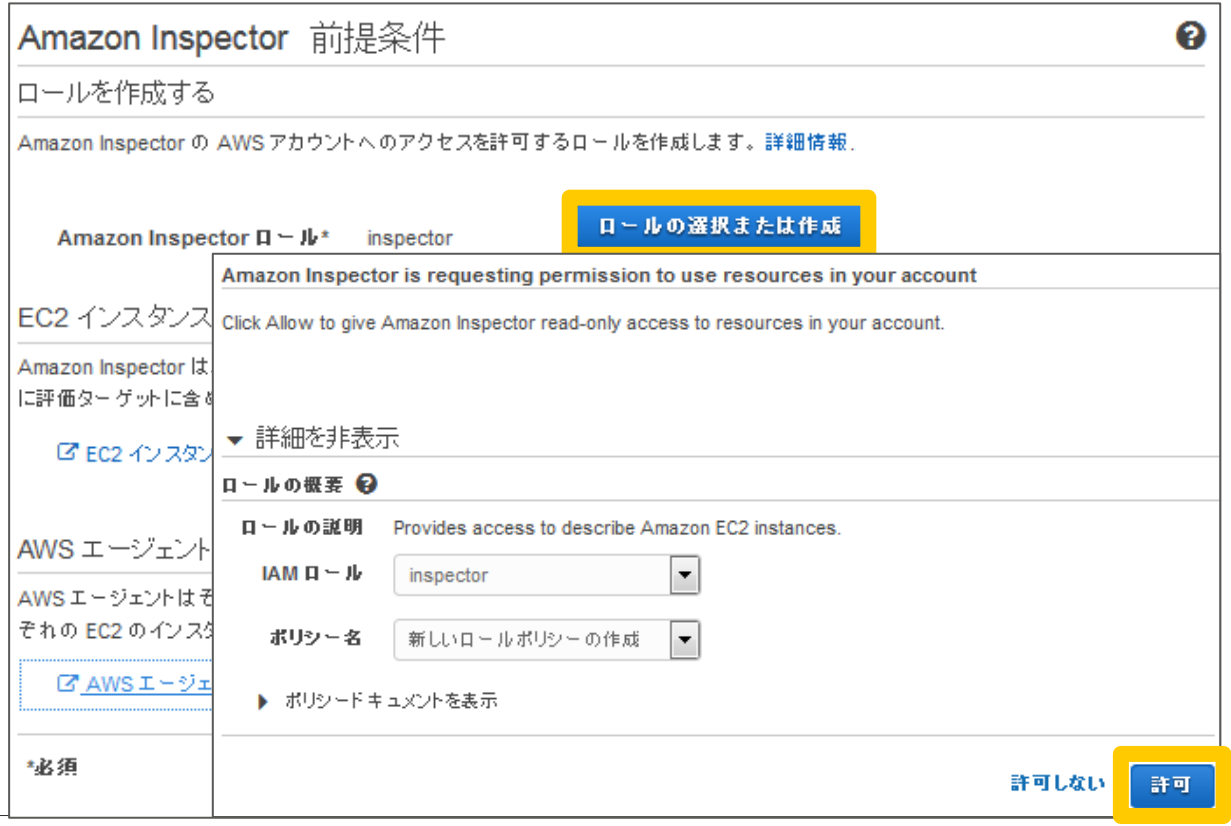
インストール

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 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 web services

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 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 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 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


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

Amazon Inspector 使用手順

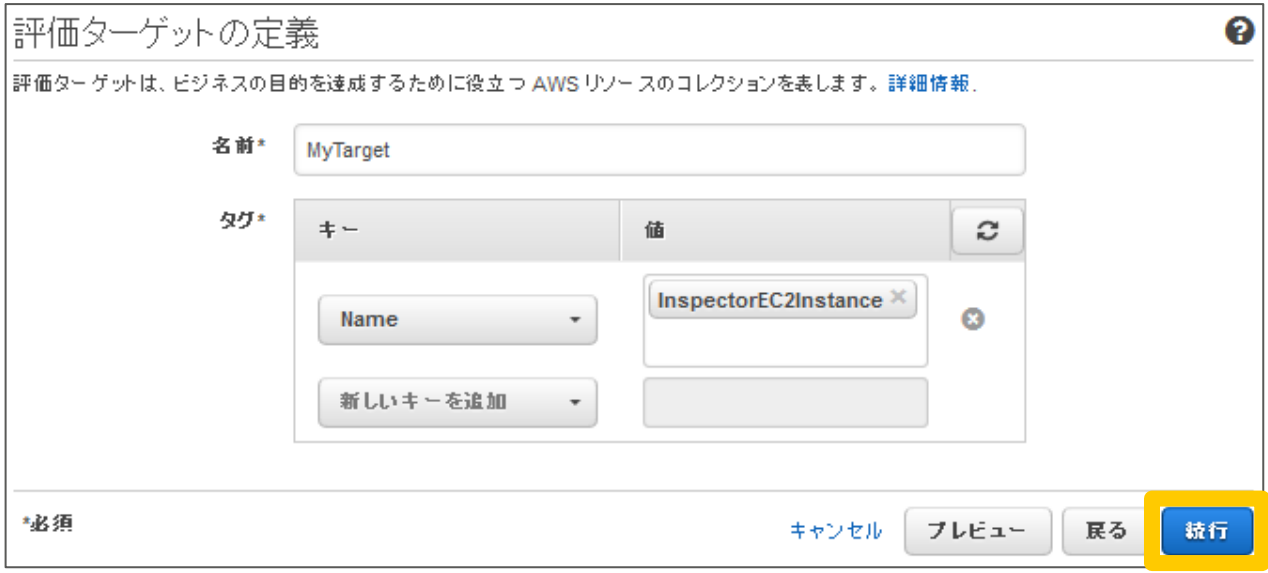
インストール

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 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 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 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
Name	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)

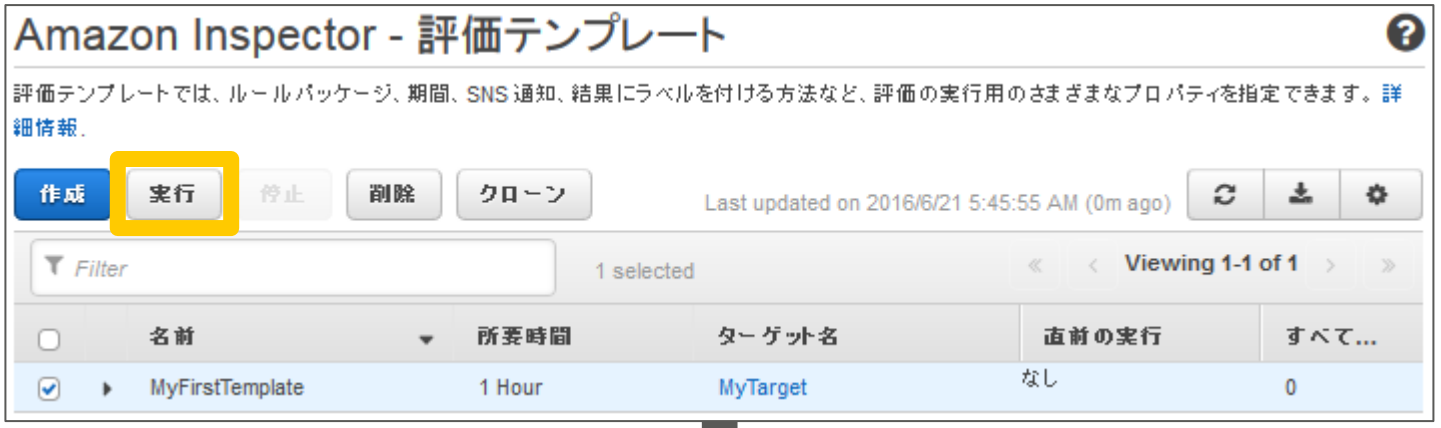
評価の実行では、評価ターゲットを構成するすべての EC2 インスタンスで AWS エージェントを実行する必要があります。AWS エージェントをまだデプロイしていない場合は評価テンプレートを作成できますが、評価を実行する前に AWS エージェントのインストールをしてください。

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 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

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
High	Instance i-61d6a1fe is vulnerable to CVE-2014-2583	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1
High	Instance i-61d6a1fe is vulnerable to CVE-2015-7547	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1
High	Instance i-61d6a1fe is vulnerable to CVE-2015-2327	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1
High	Instance i-61d6a1fe is vulnerable to CVE-2015-8382	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1
High	Instance i-61d6a1fe is vulnerable to CVE-2015-8385	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1
High	Instance i-61d6a1fe is vulnerable to CVE-2016-2381	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1
High	Instance i-61d6a1fe is vulnerable to CVE-2015-3238	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1
High	Instance i-61d6a1fe is vulnerable to CVE-2015-7499	MyTarget	MyFirstTemplate	Common Vulnerabilities and Exposures-1.1
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

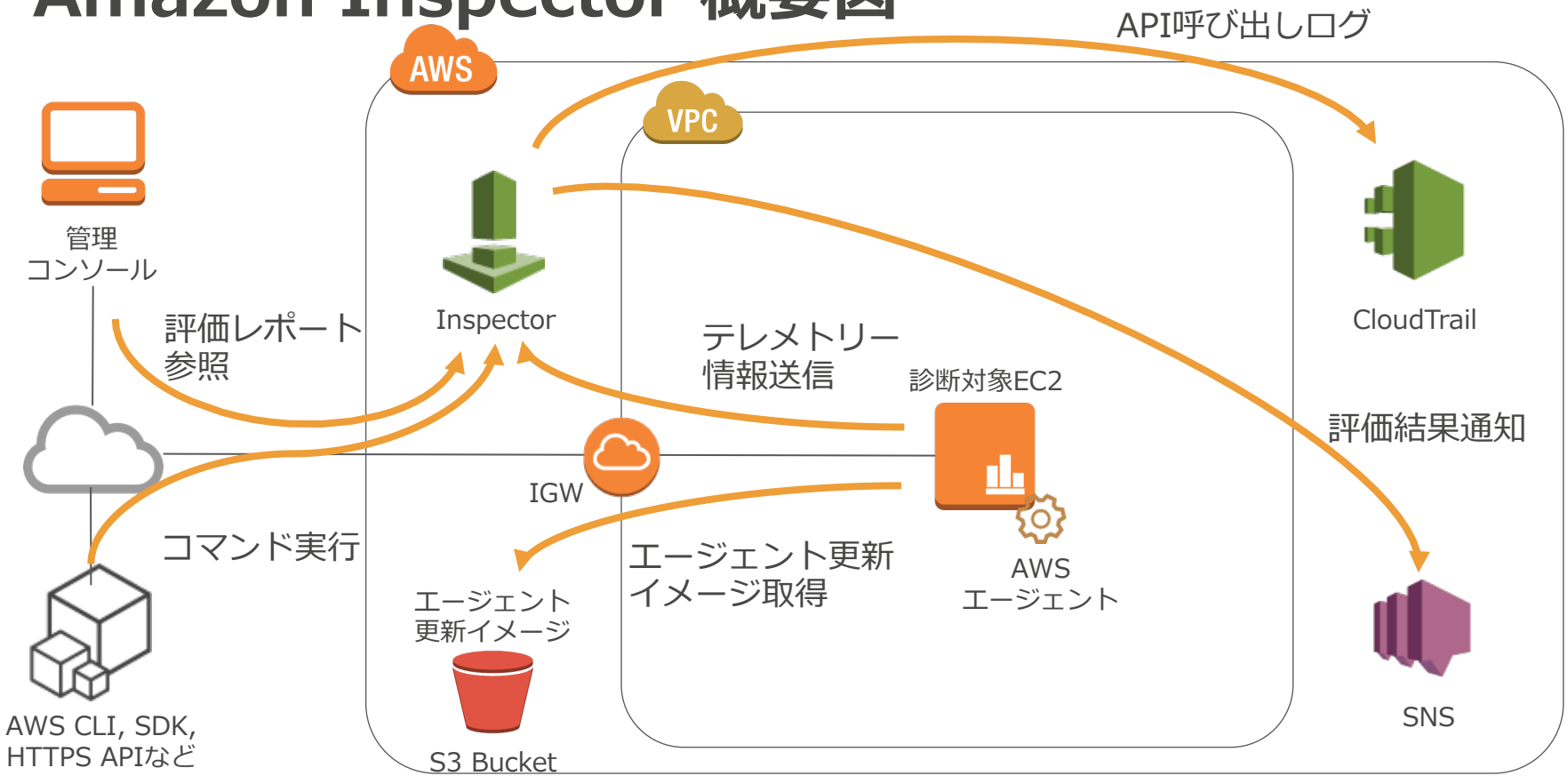
1. 分析結果の表示
2. 推奨事項の確認

	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) do*authenticated1 and (2) session*x11_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

最新情報は以下をご確認ください
https://docs.aws.amazon.com/ja_jp/inspector/latest/userguide/inspector_working-with-agents.html#inspector-agent-os

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]

最新情報は以下をご確認ください
https://docs.aws.amazon.com/ja_jp/inspector/latest/userguide/inspector_working-with-agents.html#inspector-agent-os

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**

最新情報は以下をご確認ください
http://aws.amazon.com/inspector/pricing

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

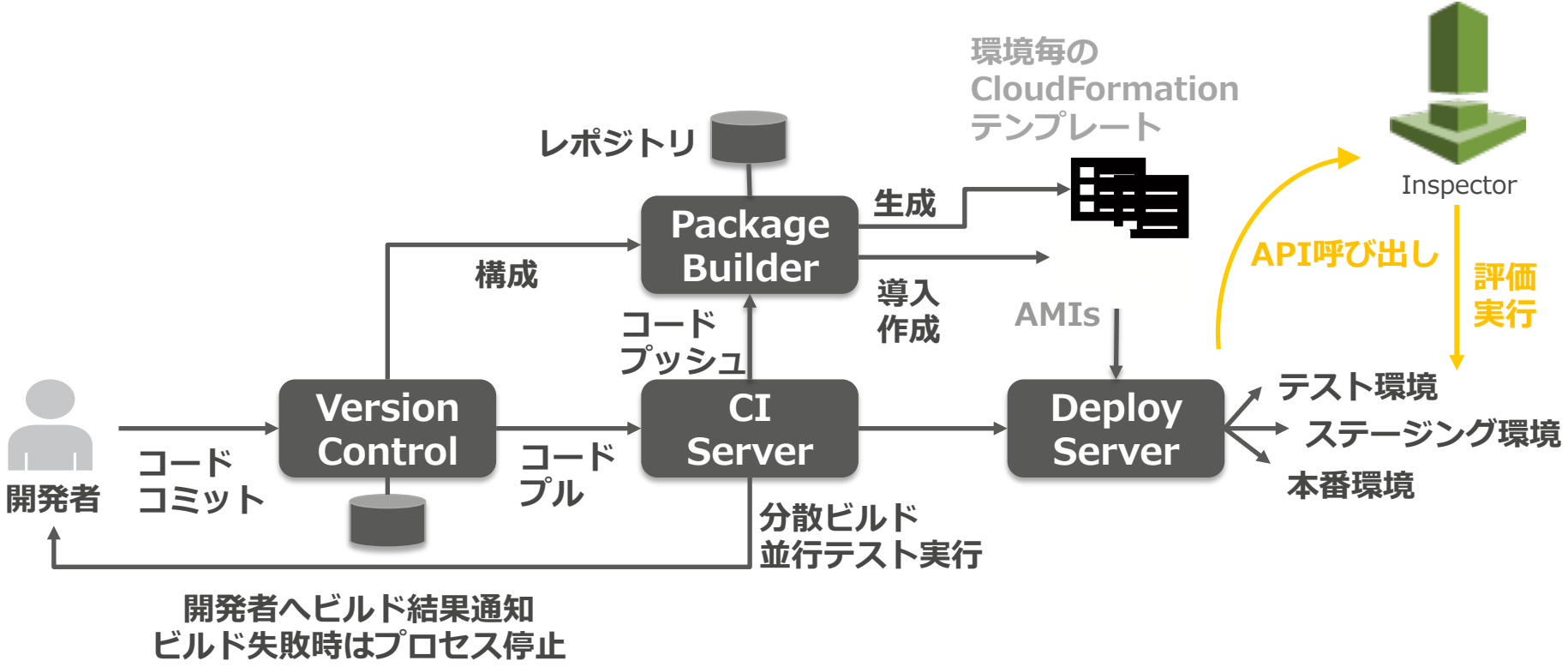
Amazon Inspectorの使い時

設計開発時

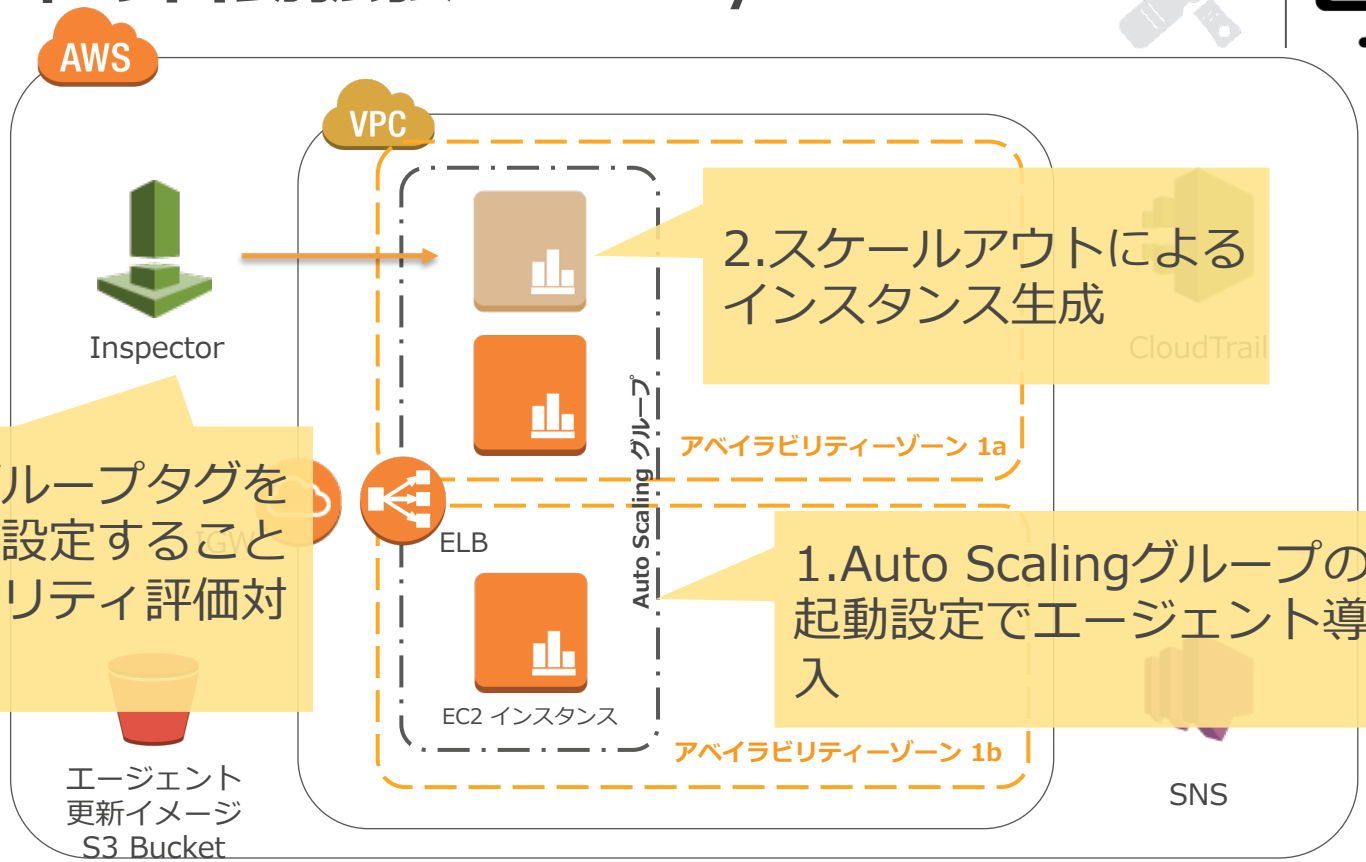
本番運用時

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

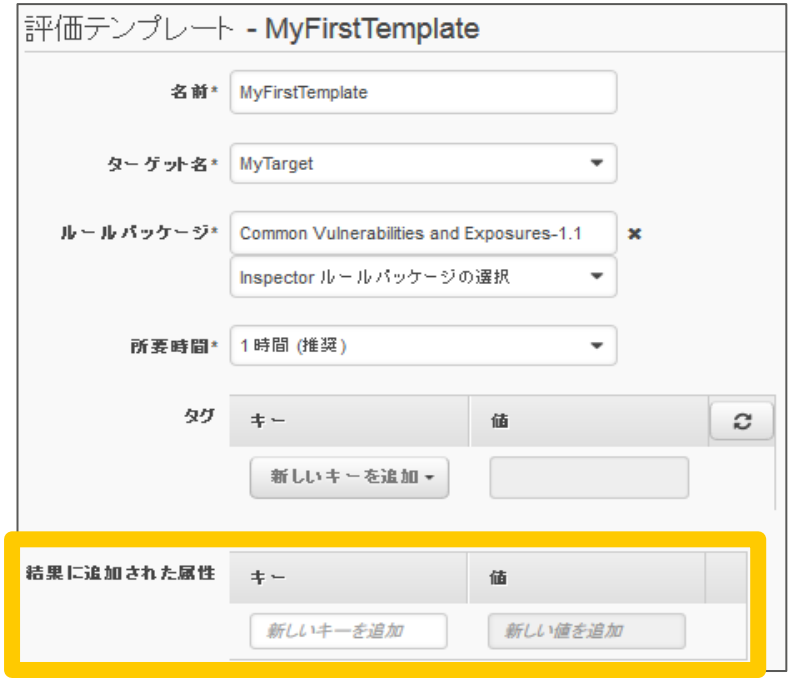


セキュリティの自動拡張 - Security at Scale -



評価結果対応の簡易ワークフロー

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
- 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/

- 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

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/

※「AWS　問い合わせ」で検索してください