



2022年1月18日

# 30分でわかる！ Amazon Inspectorで脆弱性診断



# 自己紹介

---

## □ 馬場 潤一 (Junichi Baba)

### □ 株式会社スタイルズ

- ▶ AWS上でのアプリ開発・インフラ構築  
チームリーダー

### □ 好きなAWSサービス

- ▶ CloudFormation、Systems Manager、ECS(Fargate)



# 本日、お話しする内容

---

## □対象

- ▶ AWS上でサーバの脆弱性診断の実施を検討されている方  
(初級者向け：脆弱性診断がどういうものかあまり分からない方向け)
- ▶ Amazon Inspectorを導入しようか検討されている方

## □ゴール

- ▶ Amazon Inspectorはどのようなサービスなのかを理解する
- ▶ Amazon Inspectorの基本的な利用方法を理解する

## 脆弱性診断とは

# 脆弱性とは

## 脆弱性（ぜいじゃくせい）

情報漏洩等

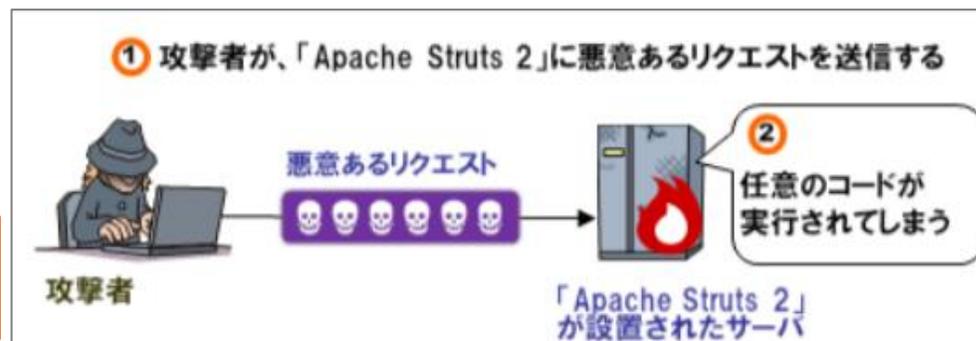
- OS、ミドルウェア、Webアプリケーション、ネットワークに潜むセキュリティ上の欠陥
- 脆弱性のある部分に対して攻撃を仕掛けることで、本来できない操作が可能になってしまう

### ◆ 例：[ CVE-2017-5638 ] Apache Struts2 に任意のコードが実行可能な脆弱性

- Javaのウェブアプリケーションを作成するためのソフトウェアフレームワーク
- ファイルアップロード処理に起因して、リモートで任意のコードが実行される脆弱性

[CVE-xxx] : 共通脆弱性識別子 (CVE番号)

スタイルズ：レガシーJAVAをリニューアル  
<https://www.stylez.co.jp/java-renew/>



# 脆弱性診断とは

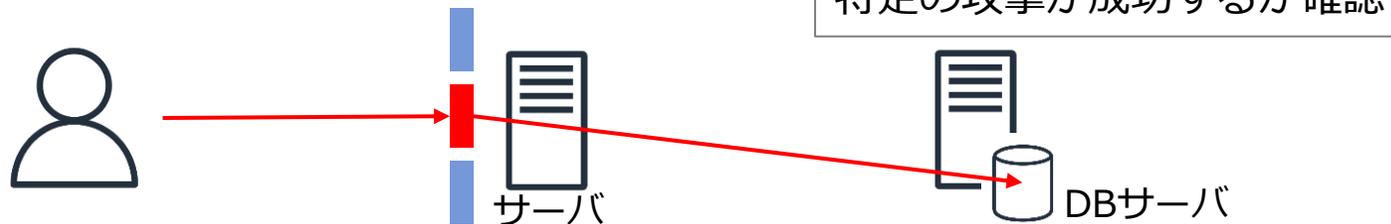
## 脆弱性診断

- ・ システムに対し、攻撃につながる脆弱性がないかを確認するセキュリティテスト
- ・ 網羅的に確認をし、セキュリティリスクを発見することが目的



## ペネトレーションテスト（侵入テスト）

- ・ 特定の攻撃シナリオを元に、どこまで被害を受けるかを確認するセキュリティテスト
- ・ 特定の攻撃に対する耐性を確認することが目的



# 脆弱性診断の必要性

## ▶ 脆弱性診断はなぜ必要なのか

- ・ 攻撃されうる箇所を特定し、具体的な対策を講じるため

## ▶ 脆弱性診断の実施頻度

- ・ 頻度が多い方が望ましい（ただし費用と運用ルール次第）

いつ新たな脆弱性が発覚するかわからないため

- ・ 診断サービスを利用する場合、たいてい実施回数毎に費用がかかる

- ・ 発覚した脆弱性への対策は基本的に手動となる。  
対策後に再チェックするケースが多い印象。

# Amazon Inspector

# Amazon Inspectorとは

## ▶ AWSが提供する脆弱性検出サービス

- 2021年11月末にv2がリリース
- EC2インスタンスとECRコンテナイメージを対象に脆弱性を検出、可視化
- インスタンス内のパッケージ情報を収集し、脆弱性に該当するかを判断

New !

### 【コンテナイメージ】

Dockerを始めとするアプリ仮想化技術において、アプリを動作させるための環境イメージ

yumやaptで管理されていないプログラムは検知対象外

- EC2における検知はSSM (Systems Manager) エージェント & IAMロールが必要

Amazon Linuxはプリインストール済  
Inspector v1は専用エージェントが必要

Systems Manager の IAM インスタンスプロファイルを作成する  
[https://docs.aws.amazon.com/ja\\_jp/systems-manager/latest/userguide/setup-instance-profile.html](https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/setup-instance-profile.html)

# Amazon Inspectorとは

## ▶ スキャンのタイミング(EC2)

- Inspectorによりインスタンスが検出された
- 新しいインスタンスを起動した
- 既存のインスタンスに新しいソフトウェアがインストールされた
- Inspectorが新たなCVE情報を追加

Inspector v1は定期的 or 手動で実施

## ▶ 料金

### 【EC2】

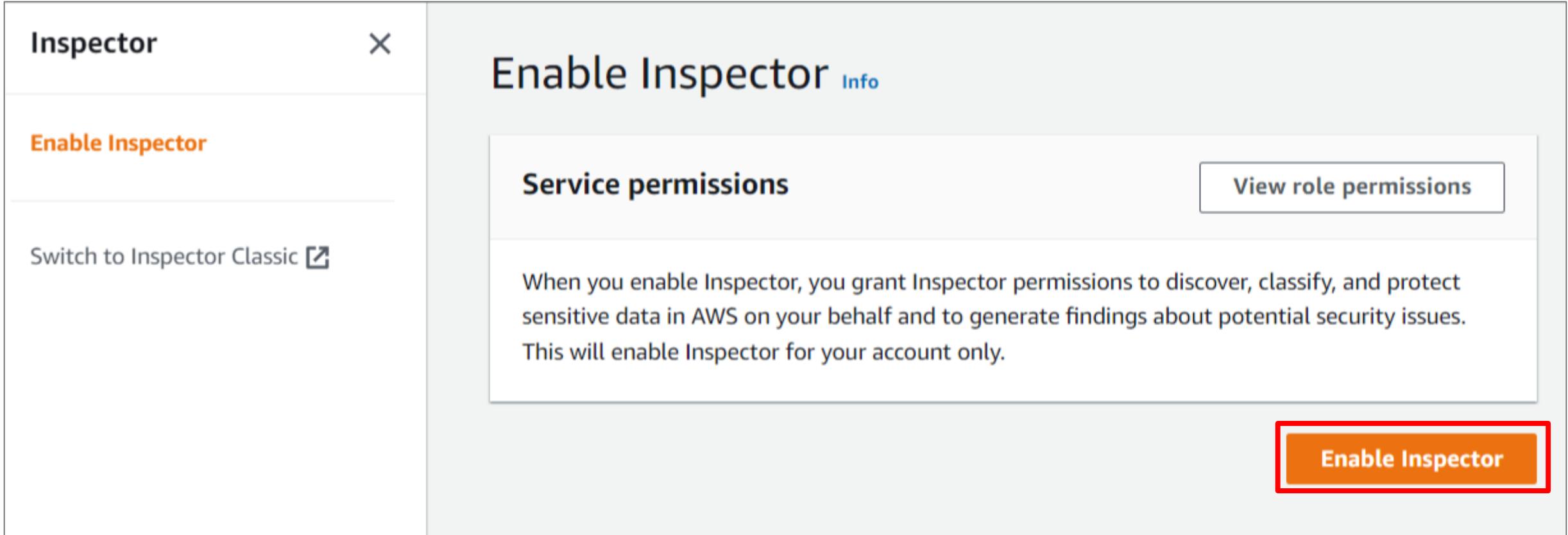
- スキャンされたEC2 インスタンス平均数 x \$1.512

### 【ECR】

- スキャンされたコンテナイメージ数 x \$0.11
- 自動再スキャン回数 x \$0.01

1ヵ月=720時間/1インスタンス として、  
スキャンが有効である稼働時間数の合計

# Amazon Inspectorの有効化



The screenshot displays the Amazon Inspector console interface. On the left, a sidebar contains the 'Inspector' header with a close button (X), the 'Enable Inspector' option in orange, and a 'Switch to Inspector Classic' link with an external icon. The main content area is titled 'Enable Inspector' with an 'Info' link. It features a 'Service permissions' section with a 'View role permissions' button. Below this, a text box explains that enabling Inspector grants permissions to discover, classify, and protect sensitive data in AWS, and that this action is account-specific. At the bottom right, the 'Enable Inspector' button is highlighted with a red border.

v1はスキャン対象設定を行う必要があったが、  
v2は有効化のみでスキャンが開始される。

# 有効化後のダッシュボード画面

Inspector > Dashboard

## Summary Info

Viewing data from all accounts

**Environment coverage**  
Your accounts, instances, and repositories that are enabled with Inspector.

<b>Instances</b> 100% 3 / 3 instances	<b>Repositories</b> 100% 10 / 10 repositories
---	---

EC2      ECR

**Critical findings**  
All active critical findings in your environment.

<b>ECR container</b> 14 Critical 240 total findings	<b>EC2 instance</b> 9 Critical 260 total findings	<b>Network reachability</b> 0 Critical 1 total finding
---	---	--

重要度が高い件数

Package name	Critical	All
openssl	7	30
libwebp	3	3
shell-quote	2	4

インスタンス別詳細画面

# インスタンス別表示画面

## Findings: By instance Info

Sorted by instances with the most critical findings.

カテゴリ別表示が可能

By vulnerability

By instance

By container image

By repository

All findings

絞り込み

### By instance (3)

Choose a row to view the instance's details and associated findings.

 Add filter



Create suppression rule

脆弱性の数が表示されている

①

②

③

EC2 instance	Account	Operating sy...	Amazon mac...	Open net... ▼	■ Critical ▼	■ High ▼	All ▼
<a href="#">i-072a14c43...</a>	588439015833	AMAZON_LIN...	ami-00f045a...	0	9	82	215
<a href="#">i-0a31841d3...</a>	588439015833	--	ami-0218d08...	1	0	1	1
<a href="#">i-00c4cc4e3b...</a>	588439015833	AMAZON_LIN...	ami-0abaa5b...	0	0	9	45

① 2年前に利用した後、停止していたインスタンス

② 最新のAmazon Linux2の素の状態

③ 最新のAmazon Linux2に少し古いhttpd(Apache)をインストール

# 特定EC2インスタンスの詳細画面

**Findings (45)** ← 表示の数値が脆弱性の数

Choose a row to view the finding details. All findings are related to this instance.

Active ▼  Resource ID EQUALS i-00c4cc4e3b10447a6  Add filter

条件による絞り込みが可能

< 1 2 3 4 5 > ⚙️

10件を超えた場合はページ別表示

Severity ▼	Title	Impacted resource	Type ▼	Age ▼
■ High	CVE-2021-39275 - httpd-tools, httpd	i-00c4cc4e3b10447a6	Package Vulnerability	6 hours
■ High	CVE-2021-40438 - httpd-tools, httpd	i-00c4cc4e3b10447a6	Package Vulnerability	6 hours
■ High	CVE-2021-26691 - httpd-tools, httpd	i-00c4cc4e3b10447a6	Package Vulnerability	6 hours
■ High	CVE-2019-0217 - httpd-tools, httpd	i-00c4cc4e3b10447a6	Package Vulnerability	6 hours
■ High	CVE-2019-0211 - httpd-tools, httpd	i-00c4cc4e3b10447a6	Package Vulnerability	6 hours
■ High	CVE-2020-11984 - httpd-tools, httpd	i-00c4cc4e3b10447a6	Package Vulnerability	6 hours
■ High	CVE-2021-42013 - httpd-tools, httpd	i-00c4cc4e3b10447a6	Package Vulnerability	6 hours
■ High	CVE-2021-3796 - vim-enhanced, vim-minimal a...	i-00c4cc4e3b10447a6	Package Vulnerability	7 hours
■ High	CVE-2021-3778 - vim-enhanced, vim-minimal a...	i-00c4cc4e3b10447a6	Package Vulnerability	7 hours
■ Medium	CVE-2021-4002 - kernel, kernel-tools	i-00c4cc4e3b10447a6	Package Vulnerability	7 hours

# 特定CVEの詳細画面

**Findings (45)** Refresh

Choose a row to view the finding details. All findings are related to this instance.

Active Filter Resource ID EQUALS i-00c4cc4e3b10447a6 Close

< 1 2 3 4 5 > Settings

Severity	Title	Impacted resource
High	CVE-2021-39275 - httpd-tools, httpd	i-00c4cc4e3b10447a6
High	CVE-2021-40438 - httpd-tools, httpd	i-00c4cc4e3b10447a6
High	CVE-2021-26691 - httpd-tools, httpd	i-00c4cc4e3b10447a6

## ■ 10段階評価

- ・ 10に近いほど深刻度が高い

## ■ CVSS v3

- ・ 共通脆弱性評価システム（世界で標準的に利用）
- ・ 深刻度を定量的に評価したスコア

## ■ Inspector

- ・ ネットワーク到達可能性、悪用可能性、CVEを加味したスコア

**CVE-2021-40438 - httpd-tools, httpd** Close

Finding ID: [arn:aws:inspector2:ap-northeast-1:588439015833:finding/460fed80ad0f50fd7ca7bc87b11e962f](#)

A Server-Side Request Forgery (SSRF) flaw was found in mod\_proxy of httpd. This flaw allows a remote, unauthenticated attacker to make the httpd server forward requests to an arbitrary server. The attacker could get, modify, or delete resources on other services that may be behind a firewall and inaccessible otherwise. The impact of this flaw varies based on what services and resources are available on the httpd network.

Finding details Inspector Score

CVSS v3 (REDHAT_CVE)	Inspector
9	8.2

The Inspector score is lower. Changed metrics: Attack Vector

CVSS score metrics

Metric	CVSS	Inspector
Attack Vector	Network	<span>Local</span>
Attack Complexity	High	High

# 特定CVEの詳細画面

## Remediation

Red Hat has investigated whether a possible mitigation exists for this issue, and has not been able to identify a practical example. Please update the affected package as soon as possible.

## 改善

Red Hat は、この問題に対して可能な緩和策が存在するかどうかを調査しましたが、実用的な例を特定することはできませんでした。  
できるだけ早く該当するパッケージを更新してください。

⇒ yum update http というコマンドを実行し対処

アップデートにより、システムが想定通りの挙動をしなくなる可能性もあるので、事前に動作検証の実施を推奨。

ケースによりコメント内容は様々。  
設定値レベルの対処を推奨されるケースや対処自体が記載されないケースもある。

## ▶ 検出された脆弱性全てを対応しないといけないということではない

- ・ソフトウェアとしては脆弱性が存在するが、設定値や構成次第では無害となる場合。
- ・ポリシー上、重要度が高いものだけ対応したい。



一覧から対応不要な脆弱性情報を非表示にしたい。

# 表示の抑制

**Inspector** ×

Dashboard

Findings

- By vulnerability
- By instance
- By container image
- By repository
- All findings
- Suppression rules**

Settings

- Account management
- General
- Usage

**You are in a 15-day free trial of: EC2 scanning , ECR container scanning** ×

To review free trial details, go to [Usage](#).

Inspector > Suppression rules

## Suppression rules Info

A suppression rule allows you to hide findings that match specific filters.

**Suppression rules (0)** Refresh Delete rule **Create rule**

<input type="checkbox"/>	Name	Created at
No suppression rules No suppression rules to display.		

表示抑制ルール管理画面

# 表示の抑制

### Suppression rule details

Name

Description

Suppression rule filters

Tags  
No tags associated with the resource.  
  
You can add up to 50 more tags.

重要度Low(低)を除外するルール

**Name** : LOW

(ルール表示上の名称、任意の文字列で良い)

**Description** : LOW

(ルール表示上の名称、任意の文字列で良い)

**Suppression rule filters** : Severity : Low

重要度以外にも様々な条件で指定可能。

- ・ 件名
- ・ CVE番号
- ・ パッケージ名
- ・ スコア Etc...

# 表示の抑制

**Findings (45)**  
Choose a row to view the finding details. All findings are related to this instance.

Active ▼  ● Resource ID EQUALS i-00c4cc4e3b10447a6  Add filter



**Findings (38)** 重要度Low以下の表示抑制により、件数が減った  
Choose a row to view the finding details. All findings are related to this instance.

Active ▼  ● Resource ID EQUALS i-00c4cc4e3b10447a6  Add filter

## まとめ

# まとめ

---

## □ 脆弱性診断とは

- ▶ 脆弱性とはOSやアプリケーション等に潜むセキュリティ上の欠陥
- ▶ 脆弱性診断とはシステムに対して脆弱性があるかどうか網羅的に確認するテスト
- ▶ 高頻度で再確認をした方が望ましいが、費用や運用に合わせて実施するとよい

## □ Amazon Inspector

- ▶ サービスの有効化
- ▶ 検出された脆弱性の確認方法
- ▶ 表示の抑制方法



実績豊富なエンジニア集団の技術と開発ツールで  
「開発期間/コスト削減」「品質向上」を実現

株式会社スタイルズ

<https://www.stylez.co.jp>

東京都千代田区神田小川町1-2 風雲堂ビル6階

Tel:03-5244-4111

オープンソースソフトウェア推進