



ちょっぴりDD

# Amazon CodeGuru Securityの紹介

Masahiro Eguchi

ISV / SaaS SA  
AWS Japan G.K

# 自己紹介

- ◆ 江口昌宏（えぐちまさひろ）
- ◆ 所属
  - ◆ ISV / SaaS SA
  - ◆ ソフトウェアベンダーや SaaS 事業者の支援
- ◆ 好きなAWSサービス  
AWS Lambda
- ◆ 最近買ったモノ  
ヒゲトリマー



早速ですが  
「デモ祭り」なので

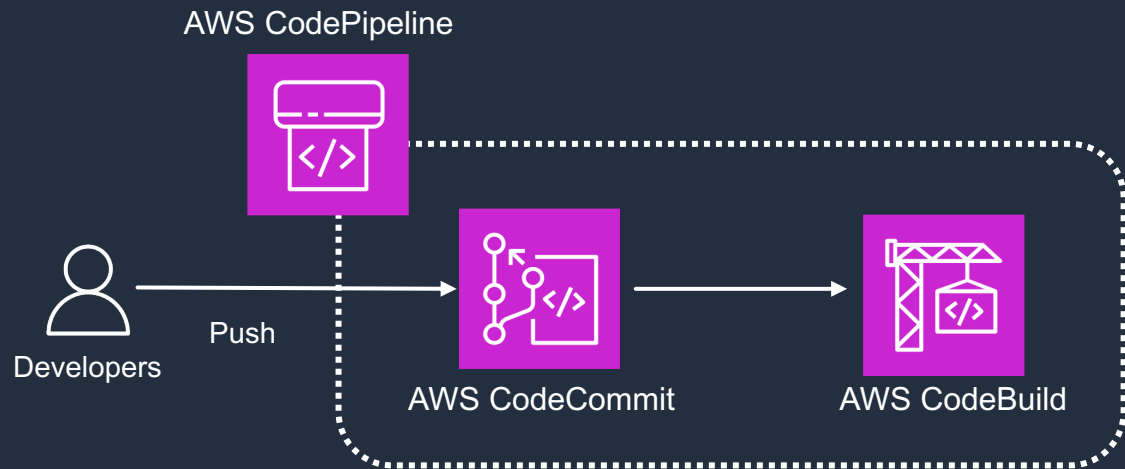
デモの説明

# Amazon CodeGuru Security

脆弱性を検知するサービス



# デモ内容



- Amazon CodeGuruSecurity 専用の AWS CodeBuild プロジェクトを実行して脆弱性がどのように検出されるかデモでお伝えします
- CI/CDパイプラインへの組み込みについては後ほどお伝えします。
- デモ内では検出を目的とした、**脆弱性**が存在するコードを投影しています
- ソースコードの取り扱いについてはご注意ください。

## CodeGuru



## ▼ セキュリティ

## ダッシュボード

統合

スキャン

検出結果

フィードバックを送信

## ▼ プロファイラー

グループのプロファイリング

## ▼ レビュー担当者

CI ワークフロー

リポジトリ

コードレビュー

## ▼ BugBust

開始方法

イベント

プレイヤーポータル

新着情報

CodeGuru &gt; セキュリティ: ダッシュボード

ダッシュボード 情報

.pdf をダウンロード

## 検出結果の概要

最終更新日: September 1, 2023, 10:44 (UTC+09:00)

## 未解決の重要な検出結果

データは週ごとに比較されます。

未解決の検出結果の合計

▼ 100% 前週から減少

0

重要な未解決の検出結果

▼ 100% 前週から減少

0

## 重要度の分布

すべての未解決の検出結果における重要度の全体的な分布。

[すべての検出結果を表示](#)

## 脆弱性の評価

最も多くの検出結果を生成した脆弱性。

## 検出結果

6

5

4



# Amazon CodeGuru Security とは

- 機械学習 (ML) と自動推論を組み合わせた静的アプリケーションセキュリティ検査 (SAST) ツールです。
- 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します。
- CI/CD パイプラインへの組み込みが可能で、アプリケーションの脆弱性検出に役立てることが可能です

開発者や、プルリクエスト時のコードレビューワーが注意すべき「アプリケーションコードの脆弱性」を検出するのに役立ち、開発者やレビューワーの負担軽減となります。

# どのような内容の脆弱性を検査しているのか

- Java, Python, JavaScript コードのセキュリティ脆弱性を検出することが可能
- コードを改善するための推奨事項を提示
- 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件の脆弱性（アクセスコントロール、インジェクション）
- CWEの上位25件の問題（クロスサイトスクリプティング、SQLインジェクション、OSコマンドインジェクション、CSRF ...）
- ログインジェクション、シークレット、AWS API と SDK の安全な使用について検出

<https://aws.amazon.com/jp/codeguru/features/>  
より



# より具体的に

**CodeGuru**  
Detector Library

Find detectors (??+K)

**Java detectors (107/107)**

- Reflected cross site scripting
- Improper service shutdown
- Incorrect string equality operator
- Input and output values become out of sync
- Inefficient chain of AWS API calls
- Server-side request forgery
- OS command injection
- Missing Authorization for address id
- Mandatory method not called after object creation
- Do not catch and throw exception
- Unrestricted upload of dangerous file type
- Process empty record list in Amazon KCL

Code clone

## Noncompliant example

```
1 public void executeSqlStatementNoncompliant(HttpServletRequest request, java.sql.Connection
2     final String favoriteColor = request.getParameter("favoriteColor");
3     try {
4         String sql = "SELECT * FROM people WHERE favorite_color='" + favoriteColor + "'";
5         java.sql.Statement statement = connection.createStatement();
6         // Noncompliant: user-given input is not sanitized before use.
7         statement.execute(sql);
8     } catch (java.sql.SQLException e) {
9         throw new RuntimeException(e);
10    }
11 }
```

## Compliant example

```
1 public void executeSqlStatementCompliant(HttpServletRequest request, java.sql.Connection co
2     final String favoriteColor = request.getParameter("favoriteColor");
3     // Compliant: user-given input is sanitized before use.
4     if (!favoriteColor.matches("[a-z]+")) {
5         throw new IllegalArgumentException();
6     }
7     try {
8         String sql = "SELECT * FROM people WHERE favorite_color='" + favoriteColor + "'";
9         java.sql.Statement statement = connection.createStatement();
10        statement.execute(sql);
11    } catch (java.sql.SQLException e) {
12        throw new RuntimeException(e);
13    }
14 }
```

<https://docs.aws.amazon.com/codeguru/detector-library/index.html>


# CodeGuru Security ダッシュボード



# パイプライン統合

パイプライン統合


### GitHub



GitHub と統合して、GitHub Actions ワークフローファイルを設定することで、リポジトリのスキャン、脆弱性の検出、推奨される修正の表示を行うことができます。

[GitHub と統合](#)


### Bitbucket パイプライン



bitbucket-pipelines.yml ファイルを設定することで、Bitbucket CI ワークフローと統合して、コードスキャンとセキュリティの脆弱性の検出を自動化できます。

[Bitbucket パイプライン と統合](#)


### GitLab



GitLab と統合して、.gitlab-ci.yml ファイルを設定することで、リポジトリのスキャン、脆弱性の検出、推奨される修正の表示を行うことができます。

[GitLab と統合](#)


### AWS CodePipeline



AWS CodePipeline と統合することで、コードベースを頻繁にスキャンして保護し、セキュリティの脆弱性が存在しない状態を維持できます。

[AWS CodePipeline と統合](#)

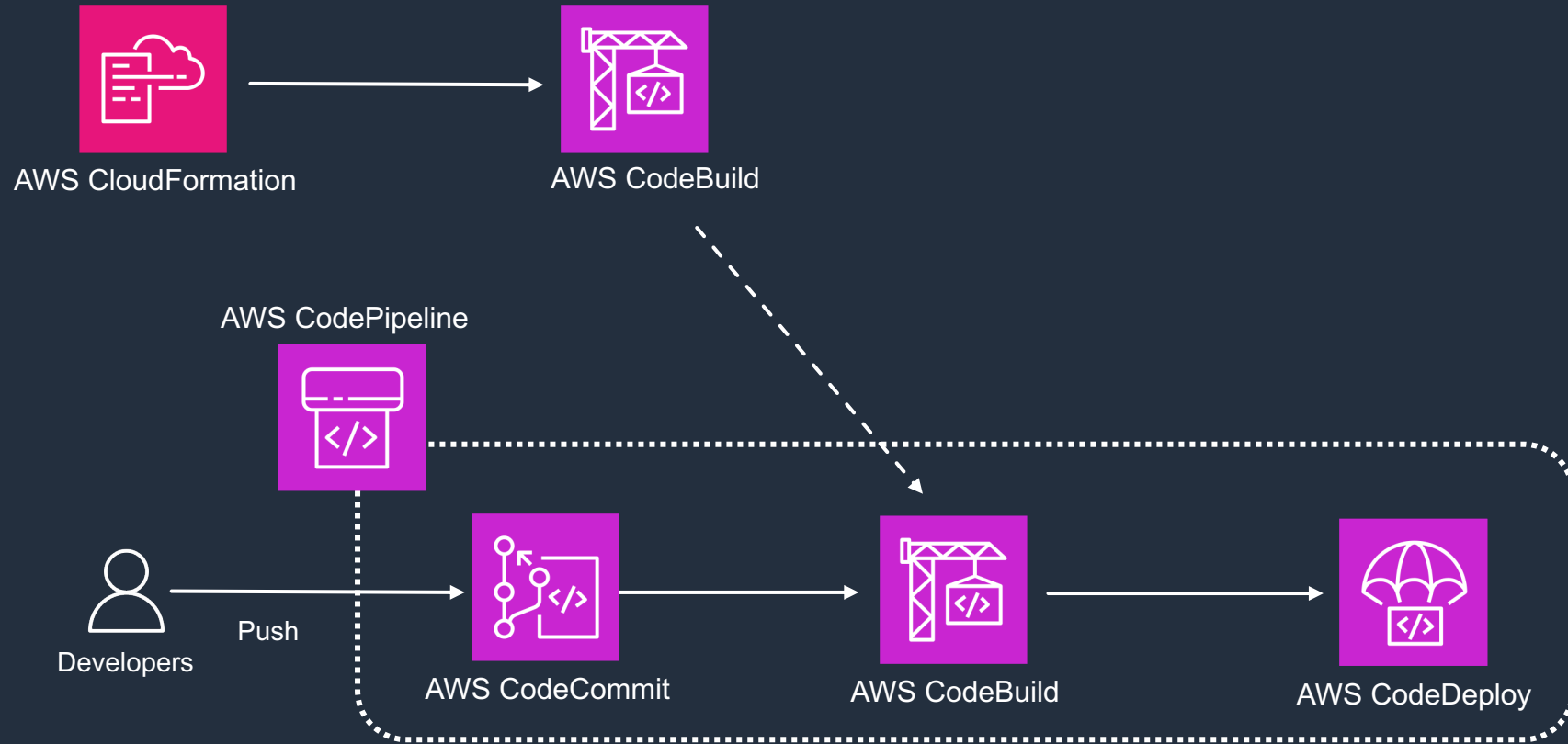
### AWS CLI



AWS CLI を使用して CodeGuru Security スキャンをローカルで実行することも、または bash スクリプトを呼び出すことで CI/CD パイプラインと統合することもできます。

[AWS CLI と統合](#)

# AWS CodePipelineとの統合




# ファイルアップロードでのスキャンにも対応

CodeGuru > セキュリティ: スキャン

## スキャン 情報

▼ 概要


**スキャンを作成**



ローカルコンピュータからコードを含む .zip ファイルを選択してスキャンを作成します。自動的にスキャンを開始する前に、ファイルがアップロードされます。

[新しいスキャンを作成](#)


**結果を表示**



スキャンが完了したら、コードで見つかったポリシー違反とセキュリティの脆弱性の詳細とともに検出結果を表示します。

[結果を表示](#)

**改定されたファイルのスキャン**



改定されたファイルに対してスキャンを再実行することで、ファイルのリビジョン全体におけるセキュリティの脆弱性の解決をモニタリングします。検出結果のレコメンデーションに基づいてコードを更新した後、適切なスキャン名を選択します。

[詳細はこちら](#)

**スキャン (5)** [改定されたファイルのスキャン](#) [新しいスキャンを作成](#)

🔍 スキャン名、ステータス、または作成日で検索 < 1 > ⚙️

	スキャン名	ステータス	未解決の検出結果	前回のスキャン日	リビジョン番号
○	codepipeline-CodeGuru	🟢 完了	2	July 21, 2023, 09:15 (UT...	14
○	TestHandler.java.zip-202...	🟢 完了	2	July 21, 2023, 09:07 (UT...	1
○	TestHandler.java.zip-202...	🟢 完了	0	July 21, 2023, 09:00 (UT...	1

# まとめ

- ✓ Amazon CodeGuru Security
  - ✓ アプリケーションコードの脆弱性を検出するツール
  - ✓ CI/CDパイプラインへの組み込み等も可能
  - ✓ 活用することで開発者、レビュワーの負担軽減につながる
  - ✓ Amazon CodeGuru Securityの画面から検出された脆弱性の一覧を確認できるのでセキュリティ担当者にとっても活用可能
  - ✓ 2023年9月現在はパブリックプレビュー中につき無料で利用可能
  - ✓ 2023年9月現在の対応言語は Java, JavaScript, Python の3つ



**Thank you!**