# Web アプリケーションにおける MVC に着目した脆弱性検知プログラムの提案

猿渡翔一郎 山森一人 相川勝
(宮崎大学)

## 1 はじめに

Web アプリケーションの脆弱性による実世界への影響は大きく，その対策が急務である．本稿では，Web アプリケーション作成時に用いられる MVC フレームワークに着目し，フレームワークの特徴に応じた検査を行うことで誤検知を減らす脆弱性検査手法を提案する．

## 2 MVC フレームワーク

Web アプリケーションにおける MVC フレームワークの動作について図 1 を用いて説明する [1].

1. クライアントは，Web ブラウザなどを用いてリスエストを送信する．
2. リクエストを受信したコントローラは，Web ページに必要となるデータをモデルから呼び出す．
3. モデルはコントローラから要求のあったデータをデータベースより取得し，結果をコントローラに返す．
4. コントローラは Web ページを生成するためモデルより得たデータをビューに渡す．
5. ビューは受け取ったデータを用いて HTML を生成し，コントローラに返す．
6. コントローラはビューが生成した HTML をクライアントに送信する．

## 3 Web アプリケーションで発生する脆弱性

### 3.1 SQL インジェクション

SQL インジェクションは，データベースを操作する際，ユーザから受け取った入力から，適切なエスケープ処理を行わず SQL 文を生成することにより，攻撃者による意図しない SQL 文 (ユーザの個人情報取得，データベースの破壊など) を実行される脆弱性である．

### 3.2 クロスサイトスクリプティング (XSS)

XSS は，HTML の入力フォームなどで，ユーザの入力に対し適切なエスケープ処理が行われていなかった場合，攻撃者が任意のスクリプトを実行できる脆弱性である．

### 3.3 クロスサイトリクエストフォージェリ (CSRF)

CSRF は，正常なサイト A にログイン状態で，攻撃者の罠サイトを閲覧することにより，正常なサイト A で認証後にのみ可能な処理 (購入処理，退会処理など) を実行される脆弱性である．

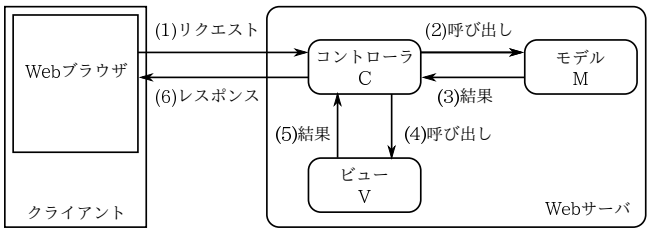


図 1: MVC フレームワークとクライアントの関係

表 1: MVC と各機能に発生しうる脆弱性の関係

| 機能 | 脆弱性 |
|---|---|
| モデル | SQL インジェクション |
| ビュー | XSS |
| コントローラ | CSRF |

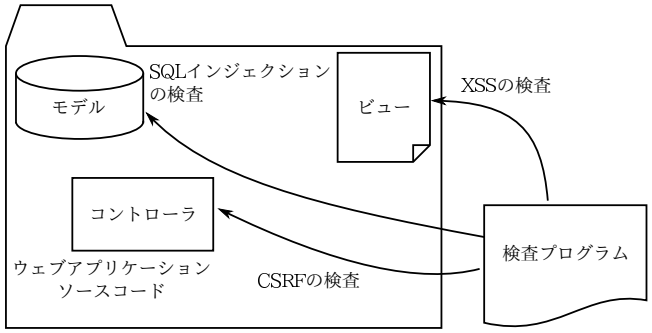


図 2: 検査プログラムの動作イメージ

## 4 提案手法

MVC フレームワークでは，それぞれモデル，ビュー，コントローラの機能毎に分けて実装を行う．そのため 3 節で述べた脆弱性は，表 1 のようにそれぞれの機能に対応した脆弱性が表れるはずである．例えば SQL インジェクションの検査を行う場合，ソースコード全体で検査を行うのでなく，データベースを扱うモデルを重点的に検査する．すると，検査範囲を限定できるため誤検知を減らしつつ，ソースコード全体の検査より効率的に脆弱性検査が行えると考えられる．他の脆弱性についても同様で, 検査プログラムのイメージを図 2 に示す.

## 5 試作結果と考察

現在，FuelPHP に対しての検査プログラムを作成しており，SQL インジェクションの検知を行うことができた．

CakePHP など，他の PHP で書かれている Web アプリケーションフレームワークの対応について考えると，モデル，コントローラについては少しの変更で対応できると考えている．しかし，ビューについては各フレームワークで書式が大幅に異なることが多いため，XSS の検査はフレームワーク毎に対応することとする．

## 6 おわりに

本稿では，MVC フレームワークに着目した脆弱性検知プログラムの提案を行った．MVC フレームワークを用いることで誤検知を減らし，効率的に検査が行えることを説明した．今後は，残りの脆弱性を検知するプログラムを作成する．

## 参考文献

[1] 鈴木憲治. はじめてのフレームワークとしての FuelPHP 改訂版. ラトルズ, (2014).