# 機械学習によるWebアプリ脆弱性の検出に関する研究

## Web Application Vulnerability Detection by Machine Learning

陳 含悦・システム分科会・情報セキュリティ大学院大学

In recent years, with the spread of Web technology,the ways for computer attack according to the web application vulnerability are becoming more and more ingenious and complicated. We think that we can expect early identification of vulnerability of Web application and improvement of efficiency of detection work by using deep learning recursive type neural network.We propose a method to we can learn sequence pairs with attack syntax from normal SQL query sentence and attack by the pseudo attack code to dynamically detect SQL injection vulnerability. We verified its effectiveness using the vulnerability Web application "OWASP Broken Web Applications".

## 背景

近年，Web技術の進化とともに，一般企業や行政機関のWebサイトの改ざん及び個人情報，金銭目的を狙った悪質な攻撃による被害が多く見られる．組織の**社会的信用の失墜**や**ブランド力低下**など，場合によっては被害を拡大させる**加害者ともなりかねない**．Webアプリの脆弱性を修正し、根本的な対策とるため、**脆弱性診断**が非常に**重要**である．

## 目的

従来の脆弱性診断手法における「**人への負荷が高い**」という課題を改善する．

主に以下2点の方針である．

- 専門家による「コード解析」「シグネチャ定義」「結果精査」といった作業負荷の軽減と短時間で実現する
- 人が介在する作業を最低限にする

## 提案手法

本研究では，深層学習技術Seq2Seq(sequence to sequence)モデルの可変長シーケンスペア学習可能という特徴に着目し，正常構文のシーケンスから攻撃構文のシーケンスを生成することで，擬似攻撃による動的診断を行い，脆弱性検知する手法を考案した．

そして，診断対象となるWebアプリケーションを修正することなく，ブラックボックスのままSQL構文の解析を実現可能にする方法も検討した．

## 実験

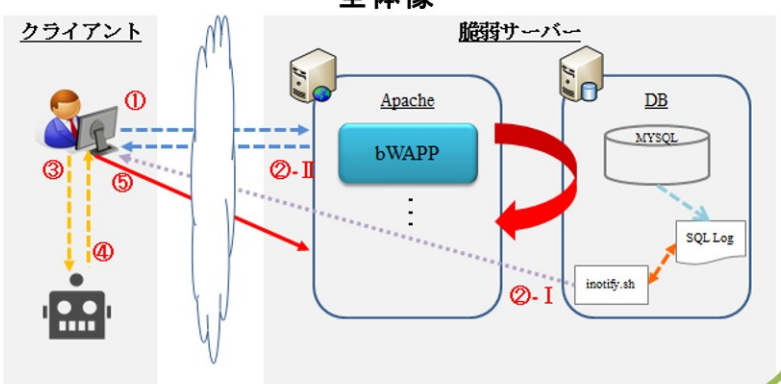
Seq2Seqモデルを構築し，「OWASP BWA」を用いてSQLインジェクションとクロスサイトスクリプティングの脆弱性検出に対する有効性を検証した．

**学習データの例**

```
SELECT * FROM table WHERE id='ID01'
SELECT * FROM table WHERE id=('ID01')
...省略...
```

```
' OR '1'='1
') OR ('1'='1
...省略...
```

**全体像**




## 結果

本研究の実験では一度だけの擬似攻撃を行い、その成功率についてSQLインジェクションが「**82%**」，クロスサイトスクリプティングが「**66%**」の攻撃に成功した．学習データ増やせば，さらに成功率が向上することが高いと考える．