令和元年度 情報工学コース卒業研究報告要旨

村瀬(勉) 研究室	氏　　名	熊 崎　真 仁
卒業研究題目	Web 上のリアルタイム情報を利用した WAF シグネチャ生成に関する研究	

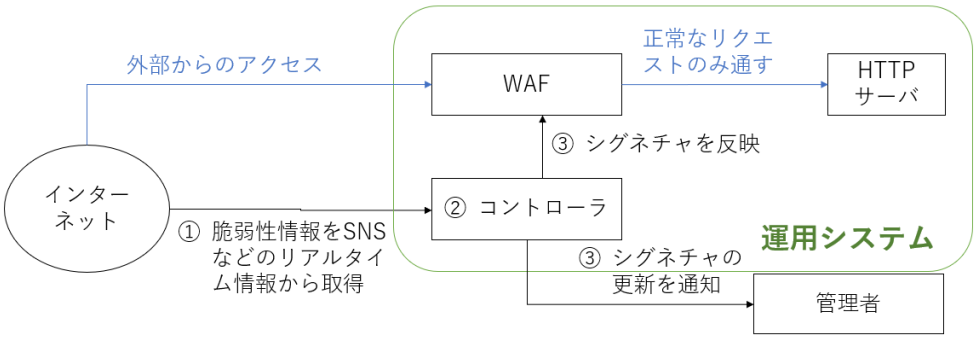
インターネットを利用した Web サービスの利用は、すでに社会のインフラストラクチャとして世間から認知されるまでになり、様々な Web アプリケーションが日々利用されている。その一方で、Web アプリケーションに対するサイバー攻撃は増加しており、その中でも公開済み脆弱性情報を利用した攻撃が特に増加している。また、ゼロデイ攻撃といった脆弱性の修正プログラムが提供される前に行われるサイバー攻撃も存在する。このような攻撃の被害を低減するためには、攻撃に対して無防備な時間を少しでも減らすことが重要である。

そこで、本研究では Web アプリケーションに関わる脆弱性情報をインターネット上のリアルタイム情報から収集し、それらの情報から WAF(Web Application Firewall) のシグネチャを生成するシステムを提案する。提案システムの構成を図 1 に示す。本手法について図 1 を用いて説明する。最初に、SNS などのインターネット上のリアルタイム情報から HTTP サーバ上で利用している Web アプリケーションに関する脆弱性情報を収集する (①)。収集した脆弱性情報はコントローラでデータクレンジングを行い、脆弱性の種類、対象バージョン、脅威度などの情報を抽出する。抽出した情報より、脆弱性が存在する Web アプリケーションに対するアクセスを遮断するルールを追加する WAF のシグネチャを生成する (②)。その後、生成したシグネチャを WAF に反映し、管理者に通知を行う (③)。これにより、パッチなどによって脆弱性の修正が行われるまでの間のサイバー攻撃を防ぐことが可能になる。

本研究ではその初期検討として、NVD(National Vulnerability Database) が提供している脆弱性データフィードから指定したキーワードが含まれる脆弱性情報を抽出し、それらの情報から WAF のシグネチャの自動生成を行った。その結果、抽出対象となるアプリケーションではなく、他のアプリケーションに対する WAF のシグネチャを生成されてしまう課題があることがわかった。

また、インターネット上のリアルタイム情報として、Twitter から Tweet データを実際に収集し、その中から 1 件の tweet を抽出してシグネチャ生成を実際に行った。その結果、アプリケーション名、脆弱性の種類、バージョン情報に関してパターンマッチングを行うことで情報の抽出が可能であることわかった。

今後は収集した脆弱性情報のデータクレンジングをどのように行うか、抽出対象以外のアプリケーションに対するシグネチャの生成をどのように防ぐかを研究する予定である。



提案システムの構成図