ディープニューラルネットワークによる Web 攻撃検知

藤田良介（福井大学大学院工学研究科）
小高知宏・黒岩丈介（福井大学大学院工学研究科）
諏訪いずみ（仁愛女子短期大学）
白井治彦（福井大学工学部）

1　はじめに

近年、Web は発展しており、日常での様々なサービスの利用に加え、会社での業務システムに Web アプリケーションを活用している例も多くなっている。Web 上でのデータが増えると共に、Web におけるセキュリティはより重大なものとなっている。

先行研究では Web に対しての未知の攻撃を検知するために HTTP リクエスト系列に含まれる特殊文字の数という特徴量を用いた SVM やランダムフォレストによる手法を提案した。[1]

本研究では Web システムの破壊や情報搾取を狙った攻撃を検知するためにディープニューラルネットワークを用いた判別機を作成する。HTTP リクエスト系列に含まれる特殊文字の数を特徴量としてディープニューラルネットワークによって学習させることで、攻撃を検知することを目指す。

2　ディープニューラルネットワークについて

ディープニューラルネットワークはデータを入力する入力層、中間にある隠れ層、出力を行う出力層から構成されている多層パーセプトロンの隠れ層を増やし、多層にしたものである。

ディープニューラルネットワークでは隠れ層を増やすことで、より複雑な関数を表現することができ、複雑な問題を解決することができると考えられている。

本研究では入力層、隠れ層 5 つ、出力層の計 7 つから構成される全結合型のディープニューラルネットワークを用いて、HTTP リクエスト系列が正常か異常かの判別を行う。

3　実験方法

本研究では先行研究と同じく HTTP リクエスト系列に含まれる特殊文字の数を特徴量とする。データセットも先行研究と同じく、ECML/PKDD2007 Discovery Challenge Dataset[2] を使用する。

このデータセットから HTTP リクエスト系列を抜き出し、正常なリクエストには 0 のラベルを与え、攻撃が行われている異常なリクエストには 1 のラベルを与える。このリクエストから特殊文字それぞれの数を抽出し、入力データを作成する。

図 1 に実験方法を示す。まず、入力データを訓練データとテストデータに分け、訓練データを用いてディープニューラルネットワークを学習させる。学習を終えたネットワークに検証データを入力し、その出力結果から、正解率、真陰性率、真陽性率などを計算して、ネットワークの精度を確認する。

4　考察とまとめ

Web でのセキュリティは重大さを増す一方で、利便性を保ったままセキュリティを高める事は非常に難しいものでもある。ディープニューラルネットワークを始めとした深層学習はより柔軟にセキュリティを高める一助となると考えている。

参考文献

[1] 清水 大貴　小高 知宏　黒岩 丈介　諏訪いずみ　白井治彦“機械学習を用いた Web アプリケーション攻撃検知手法の提案”, 福井大学 大学院工学研究科 研究報告 第 68 巻 2020 年 3 月,p51-58.

[2] Analyzing web traffic:Ecml/pkdd 2007 discovery challenge., http://www.lirmm.fr/ pkdd2007-challenge/

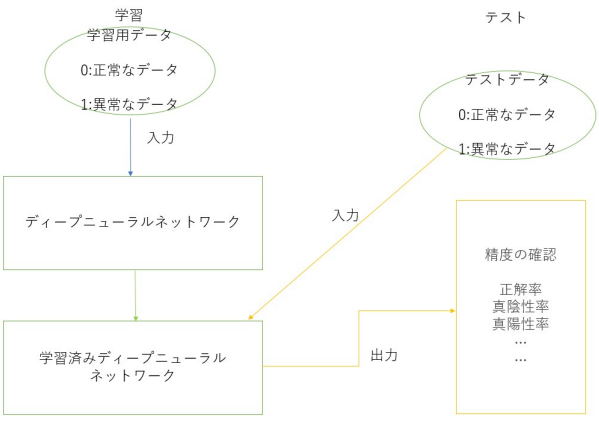

図 1: 実験方法