第 212 回ソフトウェア工学研究発表会に参加して

平　田　　悠
Haruka HIRATA
情報メディア学専攻修士課程　2022 年度修了

1. はじめに

2022 年 12 月 10 日に行われた第 212 回ソフトウェア工学研究発表会に参加し，LSTM を用いたソースコード内の SQL インジェクション脆弱性検知手法というテーマで発表を行った．

2. 研究の背景・目的

近年，ソフトウェアは生活に欠かせないものとなっている．だが，ソフトウェアの脆弱性は完全に対策を施すことが困難であり，次々と新たな脆弱性が発見されているのが現状である．最も多く報告されている脆弱性のひとつが，SQL インジェクションである．

そこで，本研究では，ソースコード自体に SQL インジェクションを起こす可能性がある脆弱性が含まれているかを検知する手法を提案した．具体的には，ソースコードから SQL に使用される関数や変数を取得し，メソッド片として，ラベル付を行なった．その後，LSTM（Long Short Term Memory）で学習を行い，SQL インジェクション脆弱性が含まれているかを評価した．

3. 提案手法

図 1 に本手法の概要図を示す．本手法は Java でソースコードが記述されていると想定する．Java では JDBC（Java Database Connectivity）と呼ばれる，Java からデータベースにアクセスするための API を使用して SQL 文を実行する．つまり，この API を使用している箇所に脆弱性があった場合，SQL インジェクションが起こり得る可能性が高いはずである．よって本研究では，”java.sql.*” クラスに関連しているコード行を抜き出して学習させる手法を提案する．具体的には，Eclipse プラグインの ASTParser を用いて，ソースコードのメソッドから JDBC の API である ”java.sql.*” クラスに関係するコード行の抽出を行う．抽出したソースコード片のことを，メソッド片と呼ぶ．その後，それらのメソッド片に対して脆弱性があるかないかのラベル付けを行いデータセットを作成して，学習させた．

学習には，単語埋め込み層，LSTM 層，全結合層を持つ 3 層の学習モデルを構築して使用した．このモデルに対してメソッド片を使用したテキスト分類として，メソッド片を脆弱性あり・なしに分類し，この結果からメソッド片が脆弱性を含んでいるかどうかを判定できているかどうかを評価する．モデルの構築には Keras を用いた．

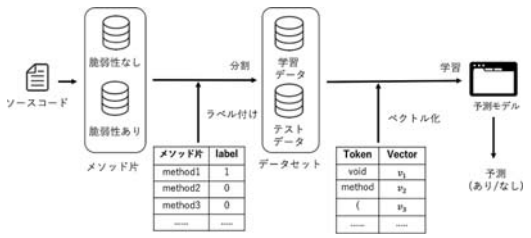

図 1　手法の概要図

4. 評価実験

評価実験では，メソッド片に対して脆弱性を含んでいるかどうかの予測を行った．データセットとして，NIST（米国国立標準技術研究所）の Juliet Java Suite と GitHub から収集した Java のソースコードを用いた．

表 1 に作成したデータセットの総数と脆弱性あり・なしの件数を示す．データセット 1 は Juliet Java Suite から収集したもの，データセット 2 は GitHub から収集したもの，データセット 3 は 2 と 3 の混合である．

表 1　データセットの各件数

データセット名	総数	脆弱性あり	脆弱性なし
データセット 1	6691	3345	3346
データセット 2	647	323	324
データセット 3	7338	3668	3670

実験結果の評価指標として，正解率（Accuracy），再現率（Recall），F1 値を用いた．これらは 2 値分類においてよく用いられる指標である．

5. 実験結果と検証

構築した学習モデルを用いてメソッド片に含まれる脆弱性の 2 値分類を行った結果を表 2, 3, 4 に示す．表は，それぞれのデータセットの各エポックでの評価指標の値である．

表 2　データセット 1 の結果

Epoch	10	20	30	40
Accuracy	0.769	0.798	0.815	0.997
Recall	1	1	1	0.998
F1 score	0.809	0.829	0.845	0.997

表 3　データセット 2 の結果

Epoch	10	20	30	40
Accuracy	0.892	0.915	0.923	0.935
Recall	0.865	0.897	0.918	0.932
F1 score	0.865	0.897	0.918	0.932

表 4　データセット 3 の結果

Epoch	10	20	30	40
Accuracy	0.823	0.830	0.975	0.995
Recall	0.981	0.983	0.987	0.998
F1 score	0.809	0.829	0.845	0.997

実験結果より，本研究で提案した手法が SQL インジェクション脆弱性の検知に対して有効かどうかを検証した．

Nicholas らの研究では 29 種の脆弱性に対し脆弱性の予測を行っており，SQL インジェクション脆弱性の精度は，Epoch10 で 0.868, Epoch20 で 0.928, Epoch40 で 0.934 である．表よりいずれのデータセットでも Epoch10, Epoch20 では精度は劣るが，Epoch40 の時では，それぞれ 0.935, 0.997, 0.995 と上回っている．また，いずれのデータセットでも Epoch40 のとき再現率が 0.9 を超えているため，誤検知が非常に少ないことがわかる．これらのことより，本手法は SQL 脆弱性の検知に対して有効的であると考える．

6. おわりに

発表を通して，貴重な意見を頂くことができ，今後の課題が明確になった．