5D-03

One-Class SVM を用いたマルウェア PDF 検出の一考察

岩本舞† 小島俊輔† 中嶋卓雄‡
†熊本高等専門学校 ‡東海大学

1 はじめに

PDF（Portable Document Format）は，異なる環境下においても再現性の高い情報交換手段として，現在，広く利用されているファイル形式である．一般に，PDF ファイルは単なる静的な文書であり，実行可能なファイル（exe ファイル等）やマクロを含むファイル（MS Office ファイル等）と比べ，危険性が少ないと見なされている．しかし実際には，PDF は様々なコードを実行可能なファイル形式であり，攻撃に利用される．多くのユーザに危険性が認識されていないことから，PDF は攻撃者にとって有用性が高いファイル形式といえる．

そこで我々は，One-Class Support Vector Machine（以下 One-Class SVM）を利用し，教師なし学習によりマルウェアを検出する手法を提案する．本手法では，あらかじめ 正常な PDF ファイルのデータのみを学習しておき，外れ値を検出することでマルウェア PDF ファイルを検出する．

2 従来研究

マルウェアを解析する手法は，静的解析と動的解析に分類される．静的解析は，データの取り出しやコードの解析に実行を伴わない方法であり，動的解析には，コードを実行してデータを取り出す手法と，さらに取り出したデータを実行して挙動を解析する手法がある．静的解析には，JavaScript の解析を行うもののほか，メタデータの特徴や文書構造によりマルウェアと正常な PDF ファイルを判別する手法がある．

本手法は，静的解析に分類される．従来手法と異なり学習に正常 PDF のみを用いるため学習用マルウェアが必要なく，新手のマルウェアにも対応できるという特長がある．

3 提案手法

本稿では，各 PDF について，8 次元の特徴ベクトルを用意し，あらかじめ正常な PDF ファイルのベクトルのみを One-Class SVM で学習しておき，外れ値が検出された場合にマルウェアとみなす手法を提案する．今回特徴ベクトルに使用した 8 個の要素のうち 7 個は，マルウェア PDF ファイルに見られた 4 個の特徴および今回新たに追加した特徴 3 個について特徴あり (1)，なし (0) の 2 値情報で表現したものであり，残り 1 個は正常な PDF ファイルとマルウェア PDF ファイルに差が見られたファイルサイズを，0〜1 で正規化した値である．なお，PDF の解析には pdf-parser.py および pdfinfo 3.04 を用いた．今回特徴ベクトルに使用した 8 個の要素の詳細を以下に示す．

/JavaScript JavaScript の実行

不正な `/Length 0` ストリームオブジェクトにおいて，実際にはバイトデータがあるにもかかわらず，辞書に`/Length 0`と記述されている

ストリームデコードエラー ストリームオブジェクトが暗号化されていないにもかかわらず，指定された圧縮形式でデコードできない

application/x-javascript PDF1.5 で新たに実装された仕様を利用した JavaScript の実行

`%%EOF` **なし** PDF ファイルは `%%EOF` で終わるという仕様が守られていない

`%%EOF` **後のデータ** PDF の最後を示す`%%EOF` の後にデータが埋め込まれている

正常な PDF ファイルに含まれないシンタックスエラー pdfinfo にて PDF を解析した際のシンタックスエラーのうち，正常な PDF ファイルで見られた以外のエラーが含まれる

ファイルサイズ PDF ファイルのサイズ S Bytes から求めた値 $S_{\mathrm{N}} = \log_{10}(\min(10^8, S))/8$
上式より，100MBytes を上限としログスケールで 0〜1 に正規化した値となる

4 実験

4.1 データセット

今回の実験では，正常 PDF として，熊本高等専門学校八代キャンパスに設置されたプロキシサーバで収集した PDF ファイル 1035 個を用いた．また，マルウェア PDF として，2010 年から 2015 年の間に収集された

A Study of Malicious PDF Detection Technique using One-Class SVM
†Mai IWAMOTO †Shunsuke OSHIMA ‡Takuo NAKASHIMA
†National Institute of Technology, Kumamoto College
‡Tokai University

D3M データセット [1] に含まれる PDF ファイル 349 個のうち，VirusTotal にマルウェアとして登録されていた 221 個を用いた．実験に用いたファイルはすべてユニークであり，重複するものはない．

4.2 実験手法

本稿では，提案手法と従来手法 [2] における正常 PDF およびマルウェア PDF 分類の正解率を，同じデータセットを用いて比較する．

従来手法については，PDF Malware Slayer (PDFMS) [2][3] を用いて実験を行った．PDFMS は機械学習に基づくマルウェア検出ツールで，PDF ファイルに出現するキーワードを正常セットとマルウェアセットに分類してクラスタリングし，機械学習により正常な PDF ファイルとマルウェア PDF ファイルを判別している．分類には Random Forest Classifier が用いられている．

提案手法は，正常 PDF ファイルの特徴ベクトルを +1 のクラスとして学習し，ある特徴ベクトルが +1 に分類されれば正常な PDF，−1 に分類されればマルウェア PDF であると判定されたとする．実験では，提案手法の 8 次元の特徴ベクトルを用いた学習およびクラス分類を行った．SVM には LIBSVM [4] に実装された One-Class SVM を，カーネル関数には，一般的に利用される RBF カーネル $k(x_i, x_j) = e^{-\|x_i - x_j\|^2/c}$ を用いた．RBF カーネルおよび One-Class SVM を使用するにあたっては，パラメタ c および ν を設定する必要がある．今回は，筆者らの研究 [5] の結果から，$c = 2^2$，$\nu = 0.001$ とした．

評価には，SVM を評価する際の一般的な手法である K-fold cross-validation を用いた．今回は，$K = 4$ として実験を行った．なお，提案手法では正常 PDF の特徴ベクトルのみを学習するため，学習用マルウェア PDF は，従来手法での学習のみに用いる．

実験では，4 つのデータセットについて正解率を算出し，平均値で評価する．なお，ここでいう正解率とは，正しいクラスに分類されたデータの数を評価データの総数で割った値である．

4.3 実験結果

実験の結果を 表 1 に示す．従来手法では，正常 PDF の正解率が 91.3%，マルウェア PDF の正解率が 94.6%，双方を合わせた正解率が 91.9% となった．一方，提案手法では，正常 PDF の正解率が 99.6%，マルウェア PDF の正解率が 100%，双方を合わせた正解率が 99.7%となり，提案手法の正解率が高くなった．従来手法では，解析エラーとなり分類ができなかったファイルが正常 PDF で 89 個，マルウェア PDF で 12 個あった．なお，提案手法でクラス +1 に分類されなかった正常 PDF（False-Negative）の内訳は，`/JavaScript` が含まれていたものが 1 個，`%%EOF` が記述されていなかったものが 1 個，ファイルサイズが 4090 Bytes や 4129 Bytes と小さかったものが 2 個であり，いずれも学習に用いた他の正常 PDF にない特徴を有していることから，外れ値に分類された．また，提案手法を用いた実験ではクラス +1 に分類されたマルウェア PDF（False-Positive）は 1 つも存在しなかった．

表 1: 従来手法と提案手法の正解率

Type	Accuracy (%)		
	All	Benign	Malware
PDFMS	91.9	91.3	94.6
Proposed Method	99.7	99.6	100

5 まとめ

本稿では，正常な PDF ファイルの特徴ベクトルのみを One-Class SVM で学習し，外れ値に分類されたファイルをマルウェアと判定する手法を提案した．

提案手法は，分類の正解率が 99.7% という高い数値になった．また，正常 PDF のみを学習するにも関わらず，正常 PDF とマルウェア PDF の双方を機械学習する従来手法の正解率を上回っていることからも，有用な手法であると言える．

参考文献

[1] 神薗雅紀, 秋山満昭, 笠間貴弘, 村上純一, 畑田充弘, 寺田真敏．マルウェア対策のための研究用データセット〜mws datasets 2015〜．Technical Report 6, jun 2015.

[2] Davide Maiorca, Giorgio Giacinto, and Igino Corona. *A Pattern Recognition System for Malicious PDF Files Detection*, pp. 510–524. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[3] Pattern Recognition and Applications Lab. Slayer. `https://pralab.diee.unica.it/en/Slayer`.

[4] Chih-Chung Chang and Chih-Jen Lin. Libsvm – a library for support vector machines. `https://www.csie.ntu.edu.tw/~cjlin/libsvm/`.

[5] 岩本舞, 小島俊輔, 中嶋卓雄. One-class svm を用いたマルウェア pdf 検出の一考察. 若手の会セミナー 2016 講演論文集, pp. 9–14, 2016.