表層情報を活用したマルウェア分類手法についての検討

Consideration on Malware classification Methods Using Surface Information

石井 龍生† 笠間 貴弘†† 宮保 憲治†

Tatsuki ISHII† Takahiro KASAMA†† Noriharu MIYAHO†

† 東京電機大学 情報システム工学科 ††国立研究開発法人情報通信研究機構

†Department of information System Engineering，Tokyo Denki University †† National Institute of Information and Communications Technology

1. はじめに

マルウェア解析の種類として表層解析や動的解析，静的解析があるが，一般的には動的解析がマルウェア種別のリアルタイム判別に適している．しかし，動的解析は以下の困難性が指摘されている．1．解析環境の作成に稼働を要する．2．解析環境が感染する恐れがある．3．解析難度に依存して処理時間を要する場合がある.更にマルウェアが解析環境を検知し，感染動作を中止することにも配慮する必要がある．

本稿では表層情報を用いてマルウェア種別を高速かつ安全に判別するための具体的な技術を述べる．

2. 研究概要

2.1 使用データ

使用した検体・データは，VirusTotal.com で取得した 5261 検体のマルウェアに FFRI Dataset 2021 の正規ファイルから無作為に抽出した 1000 データを合わせた合計 6261 個のデータとした．

使用した表層情報は FFRI Dataset Scripts[1]を用いて抽出し．92 種類の表層情報が取得できた．マルウェア名は VirusTotal API を用いて取得した．その中でも Kaspersky の解析結果のマルウェア名を使用した．

収集した 5261 個のマルウェアを VirusTotal API を用いてマルウェア名を解析した結果の上位 5 つを表 1 に示す．種類の多かった上位 3 つのマルウェア名を機械学習の正解ラベルとして使用した．

表 1 マルウェア名抽出結果上位 5 つ

マルウェア名	出現回数
HEUR:Trojan.Win32.Generic	927
Trojan.Win32.Agent.nevpvs	539
Worm.Win32.Ngrbot.bdiw	293
Worm.Win32.Ngrbot.dhx	283
Trojan.Win32.Inject.vcfz	141

2.2 分類手法

分類手法には機械学習を用い，アルゴリズムはランダムフォレストを選んだ．

2.3 評価用データ

データ全体の 25%を無作為に層化抽出したものを評価用データとした．

2.4 特徴量削減手法

特徴量削減の手法として RFE[2]を使用した．これは全ての特徴量からモデルを構築し，重要度が最も低い特徴量を 1 つ取り除く．これを指定した特徴量数になるまで繰り返す手法である．重要度の低い特徴量（ノイズ）を除去することで精度の向上や解析時間の短縮などの効果が期待できる．図 2 に 92 個の特徴量を 1 個まで RFE を用いて削減したときの F 値の推移を特徴量数 30 個以降に注目して示す．

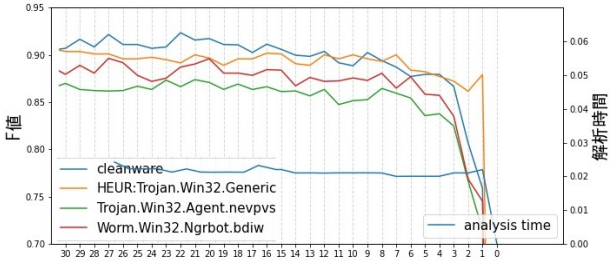

図 1 RFE を用いて特徴量削減を行った際の F 値の推移

図 2 より，F 値が下がり始める前である，20 個の特徴量を用いて分類性能の評価を行った．また、この 20 個の特徴量のうち上位 5 つを表 2 に示す．

表 2 重要度の高い特徴量上位 5 つ

1	lief.entrypoint
2	lief.optional_header.sizeof_image
3	lief.header.characteristics
4	lief.optional_header.sizeof_initialized_data
5	lief.optional_header.addressof_entrypoint

3. 実験結果

3.1 機械学習モデルの性能評価

機械学習アルゴリズムにランダムフォレストを用い，パラメータは全てデフォルト，特徴量は重要度の高い上位 20 個を使用して分類した結果を表 3 に示す．

表 3 特徴量重要度上位 20 個を適用した機械学習モデルの性能評価

	precision	recall	f1-score
Cleanware	0.929	0.884	0.902
HEUR:Trojan.Win32.Generic	0.864	0.944	0.902
Trojan.Win32.Agent.nevpvs	0.868	0.892	0.880
Worm.Win32.Ngrbot.bdiw	0.927	0.869	0.892

いずれの場合も F 値が 90%前後と高水準な結果になった．また、判定時間は 0.023 秒であり，実用上十分に高速性が図れることが判明した．

4. まとめ

90%前後の高い精度で判別することを検証した．また，マルウェアを動作させることなく安全にかつ高速に解析（判定時間 0.023 秒）できることを併せて検証した．

5. 参考文献

[1] FFRI Dataset Scripts : https://github.com/FFRI/ffridataset-scripts (2021/11/15 参照)

[2] sklearn.feature_selection.RFE : https://scikit-learn.org/stable/modules/generated/sklearn.feature_selection.RFE.html (2021/11/15 参照)