L-004

IoT デバイスを標的としたマルウェアの侵入前検知
Preemptive detection of malware against IoT devices

小寺 建輝† 泉 隆†
Tateki Kodera Takashi Izumi

1. はじめに

近年，IoT デバイスの普及に伴い，IoT デバイスをターゲットとしたマルウェアが出現している。従来のマルウェアは PC 等を対象に作成されていたため，IoT デバイスを標的としたマルウェアのほとんどが新種のマルウェアとなる。例えば，2016 年秋には「Mirai」と呼ばれるマルウェアが出現し，多くの IoT デバイスが感染の被害にあった。さらに，2017 年 1 月頃には「BrickerBot」と呼ばれるマルウェアが出現した[1]。BrickerBot は，ストレージを破壊して，IoT デバイスを使用不能にするマルウェアである。このように IoT デバイスのハードウェアに影響を与えるマルウェアは，復旧するための再起動ができないため，IoT デバイスで実行される前に防止する必要がある。しかし，多くの IoT デバイスでは，メモリ等のリソースが少なく，アンチウイルス等のセキュリティ機能を実装することが難しい。

また，従来のウイルス定義ファイルを用いてマルウェアを検知するパターンマッチング法では，定義されていない新種のマルウェアやマルウェアの亜種を検知することは不可能である。

これらを踏まえ本研究では，アンチウイルスゲートウェイを用いてマルウェアを，IoT デバイスに侵入する前のネットワークレベルで検知し遮断するシステムの構築を検討している。その中で，ファイル画像化と機械学習を組合せて新種のマルウェアにも対応した検知手法を検討する。また，検知したマルウェアに対し，ファミリを特定して通知することで，効率的なインシデント対応が可能になると考え，本研究では検知後のマルウェアをファミリ毎に分類する。

本稿では，ファイル画像化と機械学習アルゴリズムを組合せてマルウェアの検知・分類の実験を行い，識別精度を検証した結果を述べる。

2. ファイル画像化[2]

ファイルを画像化する手法を以下に示す。また実際にマルウェアをファイル画像化した例を図 1 に示す。

(1) 対象ファイルを 1Byte(8bit)ずつ読み込み 1 次元配列に格納する
(2) ファイルサイズ(配列の要素数)に応じて幅を決定し，2 次元配列に変換する
(3) 配列の要素の値は 1Byte であり，0-255 の範囲であるため，その値を画素値として 256 階調のグレースケール画像を生成する
(4) 画像の幅に合わせて画像を最近傍法により正方形にリサイズする

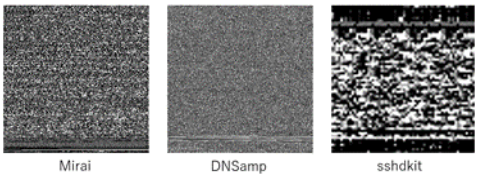

図 1 ファイル画像化の例

3. マルウェア検知・分類の実験

機械学習を行う前処理として，2 章で述べた手法により画像化した正常データ及びマルウェアデータに対して大域的画像特徴量である Gist 特徴量[3]を抽出する。1 画像あたりに得られる Gist 特徴量は 320 次元である。この特徴量を利用して識別器を作成する。本稿では，識別器作成のための機械学習アルゴリズムとして，マルウェア検知の実験ではサポートベクターマシン[4](以下，SVM)，マルウェア分類の実験では K 近傍法[5](以下，KNN)を利用する。また，利用するデータセットは，多くの IoT デバイスで採用されている Linux 環境で動作する ELF 形式の実行ファイルを採用する。本稿で利用するデータセットの内訳を表 1 に示す。

表 1 データセットの内訳

データセット	A	正常データ	3880 件
		マルウェア(281 ファミリ)	1855 件
	B	正常データ	3903 件
		マルウェア(283 ファミリ)	1928 件

3.1 SVM によるマルウェア検知の実験

SVM のカーネル関数には，RBF カーネルを採用する。RBF カーネルを用いた SVM では，カーネル関数のγと目的関数のCをパラメータとしてユーザが設定する必要がある。本稿では汎化性能が高い識別器を作成するために，データセット A とデータセット B を用いて 2x5 交差検証でグリッドサーチを行い，最適なパラメータを決定する。

3.1.1 実験結果

2x5 交差検証によるグリッドサーチを行った結果，最も汎化性能が高くなるパラメータは，$C = 2^{2.4}$，$\gamma = 2^{2.4}$であった。また，このときの識別精度，検知率，誤検知率，見逃し率を表 2 に示す。

表 2 マルウェア検知の実験結果

識別精度	検知率	誤検知率	見逃し率
96.32%	92.09%	2.03%	7.91%

表 2 より，パラメータを最適化した識別器のマルウェア検知率は 92.09%であり，汎化性能も高いため，IoT デバイスを標的とした新種のマルウェアの検知に有効と考えられる。

また，識別精度は 96.32%であり，高い精度で正常データとマルウェアを識別することができた。このことから，

† 日本大学 Nihon University

正常データとマルウェアを画像化した際の Gist 特徴量の類似性が低く，Gist 特徴量が識別に有効と考えられる。

3.2 KNN によるマルウェア分類の実験

KNN において，学習データとの類似度算出には，ユークリッド距離を採用する。また，パラメータKは$K = 1$~5 の範囲で 10 分割交差検証を行い決定する。分類実験では，データセット A，B に含まれるマルウェアからサンプル数が少ないファミリを除いた 28 ファミリ 1399 検体の分類を行う。

3.2.1 実験結果

$K = 1$~5の範囲で 10 分割交差検証を行い，識別精度を算出した結果を図 2 に示す。図 2 より，$K = 1$の時に最も識別精度が高くなり，Kの値が大きいほど識別精度が低くなった。また，$K = 1$のときのファミリ毎の識別精度を算出した結果を表 3 に示す。

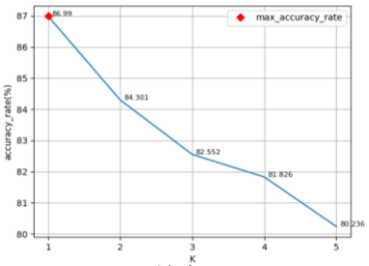

図 2　識別精度($K = 1$~5)

表 3　マルウェア分類の実験結果

ファミリ名	正識別数	サンプル数	識別精度
grip	41	41	100%
hajime	17	17	100%
darlloz	15	15	100%
chapro	14	14	100%
ganiw	242	246	98.4%
mayday	31	32	96.9%
mare	19	20	95.0%
gafgyt	347	368	94.3%
mrblack	103	111	92.8%
sshbrute	12	13	92.3%
ramen	25	30	83.3%
sshscan	10	12	83.3%
matrics	22	27	81.5%
brk	17	22	77.3%
mirai	54	70	77.1%
dcom	15	20	75.0%
lotoor	29	39	74.4%
telf	23	31	74.2%
dnsamp	23	31	74.2%
kaiten	80	109	73.4%
scalper	9	13	69.2%
race	27	40	67.5%
sorso	9	14	64.3%
openssl	9	16	56.3%
lion	12	22	54.5%
sckit	6	13	46.2%
phobi	6	13	46.2%
Total	1217	1399	87.0%

表 3 より，全体の識別精度は 87.0%であった。その中でも，grip，hajime，darlloz，chapro といったファミリは識別精度 100%であり，その他のファミリに関しても約半分のファミリを 80%以上の識別精度で分類することができた。また，IoT デバイスを標的としたファミリであり，亜種が非常に多いとされている hajime，gafgyt，mirai に関しても高い識別精度を示した。これより，多くのファミリでは，マルウェア間の Gist 特徴量の類似性が高く，Gist 特徴量が亜種を含むマルウェアのファミリ特定に有効であると考えられる。

一方，openssl，lion，sckit，phobi といった一部のファミリでは 60%以下という比較的低い識別精度となった。一部のファミリで識別精度が低くなった要因の一つとしてデータセット内のマルウェアサンプルに対して正しい正解ラベルが付与されていないことが考えられる。本稿では，データセット内のマルウェアサンプルを複数のウイルス対策ソフトでスキャンし，その判定結果の多数決によりファミリを決定して正解ラベルを付与している。しかし，ウイルス対策ソフトごとに異なるファミリで判定される場合もあり，単純な多数決では正しい正解ラベルが割り当てられない可能性がある。特に，openssl や phobi では，ウイルス対策ソフトごとに様々なファミリで判定されたサンプルが多く，誤った正解ラベルが割り当てられたことから識別精度が低くなった。また，サンプル数が不足していることも要因と考えられる。表 3 よりサンプル数が少ない場合でも，高い識別精度を示しているものも存在するが，サンプル数が 100 以上のファミリでは，70%以上の識別精度を記録している。このようなことから，サンプル数が少ない且つ識別精度が低いファミリに関しては，サンプル数を増やすことで，識別精度に向上がみられるかを確認する必要がある。

4. まとめ

本稿では，ファイル画像化と機械学習アルゴリズムを組合せた手法により，マルウェア検知・分類の実験を行い，の識別精度の検証を行った。

今後は，実際にアンチウイルスゲートウェイに識別器を搭載し，侵入前に検知するシステムの構築を検討する。

参考文献

[1] TrendMicro：「IoT 機器を標的使用不能にするマルウェア，Brickerbot」， http://blog.trendmicro.co.jp/archives/14757(2017-06)
[2] L. Nataraj, et al. : ” Malware Images:Visualization and Automatic Classification”，VizSec’11(2011-07)
[3] A. Olivia and A. Torralba : ” Modeling the shape of a scene: a holistic representation of the spatial envelope”, Intl. Journal of Computer Vision, Vol.42, No.3, pp.145–175(2001)
[4] V. Vapnik and A. Lerner : ” Pattern recognition using generalized portrait method”, Automation and Remote Control. 24, pp.774-780(1963)
[5] E.Fix and J.L.Hodges, Jr. : " Discriminatory analysis, nonparametric discrimination: Consistency properties.”, USAF School of Aviation Medicine, Randolph Field, Texas, Report 4(1951)