G-1

IoT デバイスを標的としたマルウェアの検知・分類に関する検討

A Study on Detection and Classification of Malware against IoT devices

○小寺 建輝[1]，泉 隆[2]
*Tateki Kodera[1], Takashi Izumi[2]

Malware against IoT devices is often new type or variant. Therefore, it is difficult to detect by the pattern matching method. In this research, we study to apply the malware classification technique with image recognition to detection and classification of malware against IoT devices. In this paper, we describe the experiment results of malware detection and classification with image recognition.

１．はじめに

近年，IoT デバイスの普及に伴い，IoT デバイスを標的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 等を標的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[1]．さらに，Mirai は作成者によってソースコードが公開されており，それに改良を加えた亜種が大量に作成されている．これに対し，ウイルス定義ファイルを用いてマルウェアを検知する従来のパターンマッチング法では，パターンが定義されていない新種や亜種のマルウェアを検知することは難しい．このような問題を解決するため，機械学習により新種や亜種のマルウェアを検知・分類する研究が取組まれている．その中でも，ファイルを画像化し，画像認識によって Windows 系マルウェアをファミリ毎(マルウェアの種別)に分類する研究[2]では，高い識別精度かつ高速処理でマルウェアを分類できたことが報告されている．

そこで本研究では，画像認識により Windows 系マルウェアを分類する技術を IoT を標的としたマルウェアの検知・分類へと応用することについて検討する．

本稿では，画像認識による IoT を標的としたマルウェアの検知・分類の実験を行い，識別精度を検証した結果について述べる．

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 Figure 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

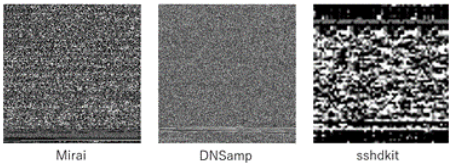

Figure 1. Example of malware images

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ファイル及びマルウェア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．また本稿では，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．

３.１ データセット

Mirai を代表とする，IoT デバイスを標的としたマルウェアの特徴は，様々な CPU アーキテクチャの Linux デバイスを対象としていることである．これを踏まえて本研究でも正常ファイルやマルウェアの検体として様々な CPU アーキテクチャの ELF ファイル(Linux で動作する実行ファイル)を採用する．本稿で利用するデータセットの内訳を Table 1 に示す．

Table 1 . Data set breakdown

Data type	Number of samples
Benign	7783
Malware	3783 (361 Family included)

３.２ SVM によるマルウェア検知の実験

マルウェア検知の実験では，Table 1 に示したデータセットを用いて，SVM により正常ファイルとマルウェアを識別する実験を行う．また，識別精度，検知率，誤検知率，見逃し率を評価指標とする．C=2.4，γ=2.4(ハイパーパラメータ)として，2x5 分割交差検証を行い，各評価指標を算出した結果を Table 2 に示す．

Table 2. Experiment result of malware detection

Accuracy	Detection	False Detection	Missed
96.32%	92.09%	2.03%	7.91%

Table 2 より識別精度は 96.32%，マルウェア検知率は 92.09%であり，高い精度で正常ファイルとマルウェアを識別することができた．このことから，正常ファイルとマルウェアの Gist 特徴量の類似度が低いことが推測でき，Gist 特徴量が IoT を標的にしたマルウェアの検知に有効と考えられる．しかし，正常ファイルとマルウェアの Gist 特徴量の類似度に差があることは，あくまで結果からの推測にすぎないため，正常ファイル

１：日大理工・院（前）・情報　２：日大理工・教員・情報

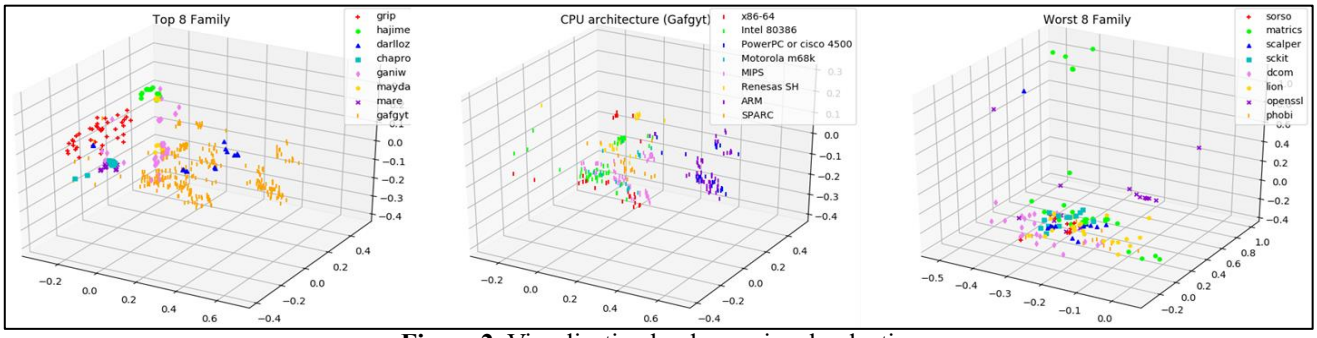

Figure 2. Visualization by demensional reduction
(Left:Scatter plot of Top 8 Family ,Center:Scatter plot of Gafgyt(by CPU architechture) ,Right:Scatter plot of Worst 8 Family)

の特徴とマルウェアの特徴をより明確に表現可能な特徴量について検討が必要である．

３．３ kNN によるマルウェア分類の実験

マルウェア分類の実験では，Table2 に示したデータセットに含まれるマルウェアの内, 27 ファミリ 1399 検体を用いて，kNN によりマルウェアをファミリ毎に分類する実験を行う．なお，kNN は高次元の特徴量による次元の呪いの影響を受けやすいため，本研究で利用する 320 次元の Gist 特徴量は，標準化と主成分分析により 23 次元に次元圧縮している．k=2 として，10 分割交差検証を行い，全体とファミリ毎の識別精度を算出した結果を Table 3 に示す．また，識別精度の上位 8 ファミリの分布，gafgyt ファミリの CPU アーキテクチャ毎の分布，識別精度の下位 8 ファミリの分布を 3 次元空間で可視化した結果を Figure 2 に示す．

Table 3. Experiment result of malware classification

Family	True identification	Number of samples	Accuracy
grip	41	41	100%
hajime	17	17	100%
darlloz	15	15	100%
chapro	14	14	100%
ganiw	243	246	98.8%
mayday	31	32	96.9%
gafgyt	354	368	96.2%
mare	19	20	95.0%
mrblack	104	111	93.7%
sshbrute	12	13	92.3%
ramen	27	30	90.0%
kaiten	91	109	83.5%
sshscan	10	12	83.3%
lotoor	32	39	82.1%
dnsamp	25	31	80.6%
telf	25	31	80.6%
race	32	40	80.0%
mirai	55	70	78.6%
brk	17	22	77.3%
sorso	10	14	71.4%
matrics	19	27	70.4%
scalper	9	13	69.2%
sckit	9	13	69.2%
dcom	13	20	65.0%
lion	14	22	63.7%
openssl	9	16	56.3%
phobi	7	13	53.8%
Total	1254	1399	89.7%

Table3 より，全体の識別精度は 89.7%であった．また，半分以上のファミリを 80%以上の識別精度で分類することができた．これは，Fgure 2(Left)に示した上位 8 ファミリの分布から分かるように，識別精度が上位であったファミリに関しては，Gist 特徴量で各ファミリの特徴を表現できており，これらの各ファミリではマルウェア間の Gist 特徴量の類似度が高くなっていることが考えられる．しかし，Figure 2(Left)中の gafgyt の分布に着目すると，他の上位ファミリに比べて分布がいくつかの集団に分散ついているようにみえる．これは，Figure 2(Center)に示したように，Gafgyt は実際に IoT デバイスを標的としたファミリであり,マルウェアが対象としている CPU アーキテクチャ毎に Gist 特徴量の類似性に差異があるためである．つまり，このような IoT を標的としたマルウェアでは，各 CPU アーキテクチャを対象としたマルウェアが学習データとして一定数以上必要になると考えられる．

また，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てしまった．これは，Figure 2(Right)より，学習データの不足等から Gist 特徴量でファミリの特徴を表現できておらず，他のファミリとの違いが現れていないためと考えられる．

４．まとめ

本稿では，マルウェアの検知・分類の実験を行い，画像認識による検知・分類手法が IoT を標的としたマルウェアに有効であることを確認した．

今後は，正常ファイルとマルウェア，及びマルウェアのファミリ毎の特徴をより明確に表現可能な特徴量について検討する．

５．参考文献

[1] Trend Micro Inc. : ”A Rundown of the Biggest Cybersecurity Incidents of 2016” , http://qq4q.biz/G9xj (2017-09)

[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)