Computer Security Symposium 2017
23 - 25 October 2017

通信挙動に基づくマルウェア種別分類手法

寺田 成吾† 小林 峻† 瀬戸口 武研† 道根 慶治† 山下 康一†

概要：年々サイバー攻撃の巧妙化が進み，日々発生するインシデント対応の効率化が必要となっている．特に同時多発したインシデントを限りある人手で対処するためには，対応するインシデントの優先度を決定しなければならない（トリアージ）．本稿では，トリアージに利用できる情報として，端末が感染しているマルウェア種別が RAT なのか PUP なのかといった情報を提供することを考え，マルウェアの通信挙動に見られる特徴からマルウェアの種別を分類する手法を提案する．本手法では，端末の通信を監視し，攻撃者行動遷移モデルへ通信挙動を当てはめ，通信挙動の遷移を基にマルウェアが有する機能を推定し，マルウェア種別を判定する．

キーワード：ネットワーク通信，マルウェア種別分類

Malware Type Classification Method based on Network Communication Behavior

Seigo Terada† Takashi Kobayashi† Mugen Setoguchi†
Keiji Michine† Kouichi Yamashita†

Abstract: Annually, against improved Cyber Attacks, it needs to make more efficiently incident response for incidents caused daily. Particularly, in order to respond to simultaneous multiple incidents with limited resources, responders must decide which incident to investigate at first (triage). In this paper, we propose the malware type classification method based on network communication behavior of each malware to provide some information that the type of malware infects in the devices is RAT, PUP or another for triage. In this method, we estimate the malware type by estimating functions of malware by monitoring the network communication of each devices and applying the behaviors to the attacker behavior transition model.

Keywords: Network Communication, Malware Type Classification

1. はじめに

年々サイバー攻撃が巧妙化，高度化し，標的型攻撃等により機微情報を窃取される被害が後を絶たない[1]．高度な攻撃では，標的型メールやゼロデイ攻撃といった手法で組織ネットワーク内部に侵入してくる．そのため，近年のサイバーセキュリティ対策では侵入されることを前提とした内部対策の重要性が主張されている[2]，[3]．また，高度な攻撃が増加する一方で，ユーザにとって不要なポスティング広告の表示や不要なソフトウェアをインストールする Adware，ユーザ情報や端末情報を同意無く外部へ送信する Potentially Unwanted Program（PUP）といった従来の脅威も存在している[4], [5].

標的型攻撃や Adware 感染などの脅威の疑いが検出された場合, Security Operation Center（SOC）や Computer Security Incident Response Team（CSIRT）といったセキュリティ監視やインシデント対応を担当する組織は，関連するログや過去の対応実績，脅威の影響度等を加味して，検出された脅威の対応可否および優先度を判断し，最終的にインシデント対応するか否か決定する（トリアージ）[6]．Ponemon Institute LLC 社による調査[7]では，組織において実際に調査できるマルウェア感染に関するセキュリティアラートの平均件数は，検出された全アラート約 17,000 件の内，約 4%の 705 件ほどであった．つまり，インシデント対応の要否を決定するトリアージの段階でどれだけ信頼度の高い情報を提供できるかが重要になる. 信頼度の高い情報として，Indicator Of Compromise（IOC）を利用したインシデント対応方法があるが，巧妙な標的型攻撃では，攻撃者が標的組織ごとに攻撃インフラを変更してくることも報告[8]されており，IP アドレスやドメイン名といった過去の確定情報を用いた解析では不十分な場合がある．そのため，未知の IP アドレスやドメイン名に関するセキュリティアラートに対する有用な情報が必要と考える．

本研究の目的は，マルウェアに感染した端末の検出時にトリアージに利用できる情報の一つとして端末に感染しているマルウェアの種別情報を提供することである．提供するマルウェア種別情報は，感染しているマルウェアが，既知か未知かに関わらず，Remote Access Trojan/Tool (RAT)といった標的型攻撃で利用される脅威度の高いマルウェアなのか，Adware や PUP のような RAT に比べて脅威度の低いマルウェアなのかといった組織に対する脅威度を判断できる情報として提供することを考える．本研究では，マルウ

† 株式会社 PFU
PFU Limited

ェアのネットワーク通信における挙動を基にマルウェアの大まかな種別分類を行った．分類手法として，攻撃者およびマルウェアの活動をネットワーク通信の観点で 8 つのフェーズに整理した“攻撃者行動遷移モデル”を定義し，監視する端末に潜むマルウェアの通信と疑わしい通信を各フェーズに当てはめ，観測されたフェーズの遷移の検出結果を利用し，感染しているマルウェアの機能を推定する．そして，予めマルウェア種別ごとに持つ機能を過去の解析結果からルールとして定義し，分類に利用した．

本論文の構成は，2 章では関連研究を紹介し，3 章で本稿におけるマルウェア種別分類手法について述べた後に，4 章で本手法の評価結果を記述する．最後に 5 章でまとめと今後の課題について述べる．

2. 関連研究

マルウェア分類手法として，ファイル自体を解析する静的解析とファイルの実行記録からマルウェアの挙動を解析する動的解析がある．静的解析の場合，攻撃者によってマルウェアの難読化やパックされることが多くなっており，マルウェア本来のコードを正しく分析するためには，これら難読化やパックを取り除く手間がかかってしまう[9]．動的解析の場合，利用される実行記録は，マルウェア本来のコードの実行結果が得られるため，マルウェア本来の挙動を解析できる可能性が高い．特に近年，組織のインターネット境界におけるファイアーウォールや端末のパーソナルファイアーウォールといったセキュリティ対策が普及し，組織外部から感染端末と通信を確立することが困難になったこともあり，マルウェアが組織内部から組織外部の Command & Control サーバ（C&C サーバ）へ接続を行い，攻撃者からの指令を受信する機能を有するようになったため，マルウェアのネットワーク通信の挙動を基にマルウェアを分類する研究が行われている．

文献[10]で S. Nari らは，マルウェア通信のフロー関係を挙動グラフという形式で表し，グラフの特徴から類似度を比較することでマルウェア種別を分類している．林らによる手法[11]は，マルウェア動作時のネットワークトラフィックのフローデータを抽出し，14 種の特徴を基にクラスタリングし，シーケンスパターンの類似度からマルウェア・ファミリーに分類している．畑田らによる手法[12]は，25 種類のマルウェア通信の特徴量を定義し，マルウェア通信をクラスタリングすることでマルウェアの分類を行っている．あるマルウェア通信の特徴量が，クラスタに分類する際に既存クラスタからある閾値以上の距離が離れていた場合，新種の未知検体候補を抽出できる特徴がある．

本研究は，ネットワーク上の挙動からマルウェアを分類するという取組みは同じであるが，機能を推定し，マルウェア種別を分類するという点で他の研究と異なる．

3. 提案手法

3.1 攻撃者行動遷移モデル

まず，本手法で定義する，“攻撃者行動遷移モデル”を説明する．本モデルは，攻撃者とマルウェアの活動をネットワーク通信の観点で 8 つのフェーズに整理（表 1）し，さらにそれぞれのフェーズから別のフェーズへの遷移を整理（図 1）したものである．

表 1 攻撃者およびマルウェアのフェーズ

番号	内容
Phase1 (P1)	ソフトウェアの脆弱性を悪用し，マルウェアのダウンロードとインストールを試みる．
Phase2 (P2)	ネットワーク環境の探索．グローバル IP アドレスの確認や近隣端末の探索など．
Phase3 (P3)	感染可能な端末へのマルウェアのコピーやリモート実行による感染拡大．
Phase4 (P4)	バイナリファイル（PE ファイル，設定ファイルなど）をダウンロードし，マルウェアの機能追加やツールの追加を行う．
Phase5 (P5)	遠隔操作を行うために接続可能な C&C サーバを検索する．
Phase6 (P6)	C&C 通信で遠隔操作が行われる．感染端末の生存確認も含まれる．
Phase7 (P7)	侵害した組織で収集した機密情報や端末のユーザ情報などを外部へ持ち出す．
Phase8 (P8)	DDoS 攻撃などを行うためのボットとして，攻撃活動に参加させる．

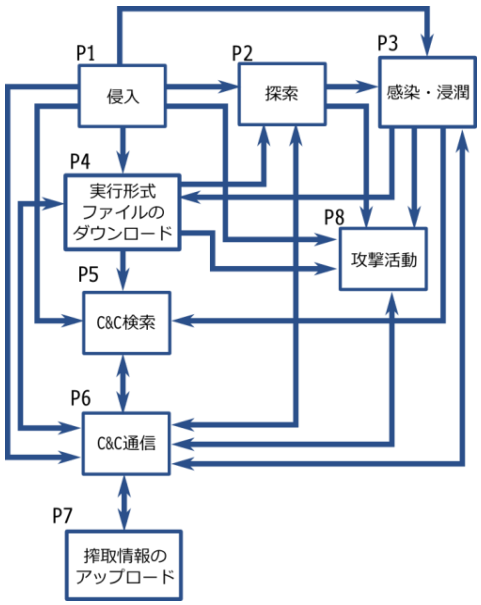

図 1 攻撃者行動遷移モデル

ネットワーク上で観測された C&C 通信やマルウェアによる疎通確認と疑われる通信をそれぞれイベントとして各フェーズへ当てはめ，それらイベントの遷移を通信の時間間隔や宛先などで関連性を判断することで，マルウェアを利用した攻撃活動を検知できる[13]．本稿におけるマルウェア種別の分類手法では，これら検知した攻撃活動をマルウェアが持つ機能として捉え，マルウェアが有する機能から端末が感染しているマルウェアの種別を推定することを考える．フェーズ遷移において中核となっているのが C&C 通信フェーズ（Phase6）であるが，このフェーズは“ブラウザと異なる怪しい通信”を主にイベントとして割当てている．ここでのブラウザと異なるとは，ブラウザが利用する User-Agent を偽装した HTTP 通信などを指す．

次に，マルウェア種別を分類するために，各フェーズへの遷移を機能観点でまとめる．

3.2 マルウェア種別の分類手法

3.2.1 フェーズ遷移とマルウェアの機能の対応付け

まず，攻撃者行動遷移モデルにおけるフェーズ遷移と遷移から推定されるマルウェアの機能の対応について説明する．

A：機密情報の窃取とアップロード機能

マルウェアの中には攻撃者からの指令により感染端末や侵害組織内で窃取した情報を C&C サーバへ送信する機能を持つマルウェアが存在する．このときサイズが大きいデータを外部へ送信するために HTTP の POST メソッドがしばしば利用される．そのため，Phase6 と同じく，ブラウザと異なる通信で，かつ POST メソッドを利用した外部へのファイル送出を Phase7 のイベントとし，Phase7 のイベント前後いずれかに C&C 通信に関連する Phase6 のイベントが存在した場合，情報の窃取に関する遷移があったと推定し，機能 A を有していると推定する．

B：疑わしいファイル（バイナリ）のダウンロード機能

疑わしいバイナリのダウンロード機能では，Drive-by Download 攻撃による侵入やスパムメールに添付されたダウンローダーによるマルウェアのダウンロードなどを検出する．また，C&C 通信後の新たなマルウェア（ツール），設定情報のダウンロードも検出する．これらのフェーズ遷移が検出された場合，機能 B を有していると推定する．

C：ネットワーク環境の調査機能

マルウェアの一機能として，外部ネットワークへの疎通確認機能がある．この機能は，外部ネットワークへアクセスできない場合に他主要機能の実行を待機する機能であり，サンドボックスや閉じられた環境での動的解析に対する妨害機能と考えられる．Phase6 と同じく，ブラウザと異なる通信で，かつ，Google や Yahoo!といった有名サイトへのアクセスを探索フェーズ(Phase2)のイベントとし，Phase2 から Phase6 への遷移，及び，Phase4 から Phase2 への遷移を検出した場合，機能 C を有していると推定する．

D：C&C サーバの検索機能

近年のマルウェアは複数の C&C サーバを設定として持っており，ある 1 つの C&C サーバと通信できない場合，他の C&C サーバと通信を確立できないか試行し，通信を確立できる C&C サーバを検索し続ける．そのため，複数の宛先に対する Phase6 のイベントが連続して検出された場合，機能 D を有していると推定する．

E：C&C サーバ通信機能

C&C サーバ通信機能としては，通信が確立した C&C サーバに対して定期的に指令を確認するビーコン通信などを検出する．Phase6 のイベントが連続するのは，“D：C&C サーバの検索機能”と同じであるが，1 つの C&C サーバと連続して通信を実施する点が異なる．つまり，1 つの宛先に対する Phase6 のイベントが連続して検出された場合，機能 E を有していると推定する．

F：リモートコントロール機能

リモートコントロール機能は，RAT に多く見られる通信機能である．RAT の通信の特徴的な部分として，攻撃者からの指令がないか定期的に確認するためのビーコン通信と攻撃者からの指令を受け，不定期に C&C 通信を行うリモートコントロール通信に分けられる．ここでの C&C 通信は，すべて Phase6 に該当するため，継続する Phase6 のイベントとその通信間隔を検査することで，ビーコン通信とリモートコントロール通信への切り替わりを検出し，機能 F を有していると推定する．

G：感染拡大機能

主に標的型攻撃の場合，標的とする情報を持つ端末を探すために同一ネットワーク内の別端末へと感染を拡大する．そして，感染拡大直後に感染元の端末から継続して C&C 通信（Phase6）のイベントが発生する．そのため，感染拡大(Phase3)のイベントから Phase6 への遷移を検出した場合，機能 G を有していると推定する．

H：マルウェア侵入に起因した C&C 通信

ダウンローダー機能を持つマルウェアが新たに別マルウェアをダウンロードした後，そのマルウェアを実行した場合，実行されたマルウェアによる C&C 通信（Phase6）が発生する．そのため，Phase4 の直後に Phase6 への遷移が発生した場合，機能 H を有していると推定する．

Google は，Google Inc. の商標です．

3.2.2 マルウェアの機能と種別の対応付け

次に，本研究で対象とするマルウェア種別の定義と通信に現われる特徴を説明する．これらの特徴は，Malware Traffic Analysis.net[14]や reverse.it[15]で入手できるマルウェアの動的解析結果を基にマルウェア種別ごとに分類した．マルウェア種別は，解析されたマルウェアの Virustotal[16]における検知結果のラベル名を参考に分類した．

なお，本分類手法は，下記に説明する順番で条件判定を行い，最初に条件を満たしたマルウェア種別を最終的な判定結果とする．

Backdoor/RAT

Backdoor/RAT は，標的型攻撃で主に利用されるマルウェアであり，多数の機能を有する．特に，リモートシェルを利用して任意コマンドを実行できる機能を持つため，機能 F に記したリモートコントロール機能が検出される．そのため，機能 F を持つマルウェアと判定された場合，Backdoor/RAT として判定する．

Bot

Bot は，Pushdo のように感染端末に潜み，C&C サーバからの命令に従って DDoS 攻撃やスパムメールの送信など攻撃活動に利用される．攻撃指令を受信するために，Bot は，C&C サーバへ定期的なビーコン通信を行い，攻撃者からの指令を待ち受ける．そのため，C&C サーバとのビーコン通信として機能 E, C&C サーバを切り替えるための機能 D の通信挙動が特徴的に多く検出される．

Spyware

Spyware は，Banking Trojan に代表されるマルウェアであり，ユーザの認証情報やキー入力情報，画面キャプチャ情報などを不正に窃取する．通信の特徴としては，C&C サーバの命令に応じて，ユーザ端末から窃取した認証情報や画面キャプチャなどを攻撃者のサーバへアップロードする．そのため，アップロード通信が Phase7 として捉えられ，その前後で指令を受信するための C&C 通信が Phase6 として検出される．そのため，機能 A が特徴的に検出される．また，Bot としての機能を持つマルウェアも存在するため，機能 D，機能 E も検出される．

Ransomware

Ransomware は，主に感染端末のデータを強制的に暗号化し，復号するために金銭を要求するような脅迫行為を行うマルウェアであり，近年被害が増加している．通信の特徴として，感染直後に暗号化・復号化に必要な鍵交換，または，感染端末情報の通知のために C&C 通信を行うことが多い．また，侵入手段として，Drive-by Download 攻撃やダウンローダーによるマルウェア本体のダウンロード通信として機能 B の挙動が観測される．

検出されない挙動として，Ransomware は感染後，新たなマルウェアやツールのダウンロードを行わないため，感染後に Phase4 に関する遷移が見られない．そのため，機能 H は検出されない．

Generic Trojan

Generic Trojan は，ここまでに示したマルウェア種別のように明確な特徴が現われないマルウェアとしている．そのため，ここまでに示した各種マルウェア種別に分類できなかったマルウェアを Generic Trojan として判定している．

ここまで説明したマルウェア種別とそれぞれ有する機能をまとめると，下記表 2 のとおりである．

表 2 マルウェア種別と機能の対応まとめ

機能	フェーズ遷移	RAT	Bot	Spy	Rsm	Gen
A	P4→P7	×	×	○	×	×
	P6→P7	○	○	○	○	×
	P7→P6	○	×	○	×	×
B	P1→P4	△	△	△	△	△
	P4→P4	△	△	△	△	△
	P6→P4	○	○	○	×	○
C	P2→P6	○	○	○	○	○
	P4→P2	○	○	○	×	○
D	P6→P6	○	○	○	○	○
E	P6→P6（定期的）	○	○	○	×	○
	P6→P6（不定期）	○	○	○	×	○
F	P6→P6（リモートコントロール）	○	×	×	×	×
G	P6→P3	○	○	×	×	○
H	P4→P6	○	○	○	×	○

○：フェーズ遷移を検出する．
×：フェーズ遷移を検出しない．
△：侵入手段として検出する場合がある．

4. 評価

4.1 評価方法

マルウェア種別を分類する前段階の検知プログラムは，ネットワーク通信をモニタリングし，リアルタイムで解析するプログラムとして実装されているが，効率的に評価す

るために解析プログラムにキャプチャファイルを直接読み込む改造を行い，タイムスタンプを基準に処理するプログラムを作成した．このプログラムに，評価するキャプチャファイルを順番に処理させ，検出結果としてイベント情報とフェーズ遷移情報が記録されたテキストファイルを取得し，フェーズ遷移情報からマルウェア種別を推定した．

評価データとして，まず，調査に利用した reverse.it で入手した公開データによる分類確認を行い，MWS Datasets 2017 [17]の BOS（Behavior Observable System）データセット[18]，[19]を用いた RAT の分類性能を評価した．

4.2 公開データでの評価

公開データを用いた評価結果は，表 3 に示す通りの結果となった. 各行が Virustotal の分析結果を基に事前に分類したパケットキャプチャの分類結果を示し，各列が本手法で分類された各パケットキャプチャのマルウェア種別を示す. Unclassified は，キャプチャデータが不十分でマルウェア感染と判定できず, 種別分類されなかったデータ個数を示す. この理由として，reverse.it で入手できるパケットキャプチャデータは，サンドボックス上で動作したマルウェア感染初期の通信になるため，マルウェアに感染していると判断するための通信データが不足していたからである．

表 3 評価結果

データの種別	分類結果					
	RAT	Bot	Spy	Rsm	Gen	Unclas-sified
RAT	10	0	1	0	11	102
Bot	0	13	3	0	40	49
Spy	1	3	26	0	73	179
Rsm	0	1	0	3	34	108
Gen	0	0	1	0	83	125
合計	11	17	31	3	241	563

結果として, 多くの判定結果が Generic Trojan になっているが，Unclassified が多くなっている理由と同じく，サンドボックス上での解析で採取されたパケットデータであり，マルウェア感染の判定時点で，マルウェア種別を判定するには，まだ不十分なデータであったからである．

また，Ransomware の分類結果が著しく悪いが，分類ルールとして侵入段階の機能 B の挙動が観測されていることを含めたため，サンドボックスでのマルウェア本体の挙動解析では，機能 B の挙動が観測されず，分類できていなかった．

4.3 BOS（Behavior Observable System）データセット

寺田ら[18]，[19]により作成されたデータセットを利用してマルウェア種別を正しく分類できるか評価した．BOS は，標的型攻撃で利用される RAT の挙動と攻撃者の行動を組合せることで，攻撃者行動視点での脅威の特徴付けを行う試みである．サンドボックスによる解析結果から得られる情報よりも実環境に近いデータが得られ，より精度高くマルウェア種別を分類できることが予想される．

本評価では，データセットの内，パケットキャプチャを含み，攻撃活動が観測された BOS2014，BOS2015 の一部で評価した．

表 4 BOS 2015 による評価結果

	Case 番号	分類結果
BOS2014	c21 (IsSpace)	Backdoor/RAT
BOS2015	d18 (Emdivi)	Backdoor/RAT
	d19 (Emdivi)	Backdoor/RAT
	d37 (Emdivi)	Backdoor/RAT

評価結果としては，4 検体すべてにおいて，正しく Backdoor/RAT として分類できた．この結果は，機能 F で示したリモートコントロール操作の挙動を検出したためであるが，Emdivi と C&C サーバとの一連のビーコン通信の一部を誤ってリモートコントロール操作の通信として誤検出していた．これは，ビーコン通信中に一時的に通信間隔が狂った挙動があり，その挙動をビーコン通信からリモートコントロール操作に切り替わったと誤検出したためであった．長時間挙動を監視した場合，他のマルウェア種別を誤分類してしまう可能性があるため，見直しが必要である．

5. まとめ

マルウェアの実行時に得られるネットワーク通信の挙動を攻撃者行動遷移モデルに当てはめ，フェーズ遷移からマルウェアの機能を推定することで，マルウェア種別を分類する手法を提案した．

評価結果として，公開データを用いた感染初期段階における分類精度は，データ不足のためほぼ Generic Trojan へ分類してしまった．BOS データセットによる評価では，データ数が少ないものの，すべて正しく Backdoor/RAT へ分類することができた．本評価結果より，本手法は正しく分類するためには，マルウェア種別ごとの特徴が現れるまでの一定時間を要し，感染発覚直後では正しく分類できないことが多いと思われる．そのため課題として，より少ない挙動，より感染の初期段階で感染したマルウェアの種別を判別する必要がある．今後の方向性としては，判別ルールの改良やより多くのデータを収集した上で，機械学習を活用し，精度向上するか確認する予定である．

参考文献

[1] “国内標的型サイバー攻撃分析レポート 2017 年版 ～巧妙化と高度化を続ける『気づけない』攻撃～”，ト

レンドマイクロ株式会社, 2017.
[2] “国内標的型サイバー攻撃分析レポート 2016 年版 ～状況と目的に応じて攻撃を変化させる攻撃者～”, トレンドマイクロ株式会社, 2016.
[3] “高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて”, *JPCERT/CC,* http://www.jpcert.or.jp/research/apt-guide.html, (参照 2017-08-22)
[4] “FIREBALL - The Chinese Malware of 250 Million Computers Infected”, *Check Point Blog*, 01-6 月-2017, http://blog.checkpoint.com/2017/06/01/fireball-chinese-malware-250-million-infection/, (参照 2017-08-22)
[5] Kurt, T., Juan, A. E. C., Ryan, R, et al, “Investigating Commercial Pay-Per-Install and the Distribution of Unwanted Software”, *25th USENIX Secur. Symp.*, 8 月 2016.
[6] “インシデントハンドリングマニュアル. 一般社団法人 JPCERT コーディネーションセンター”, 2015.
[7] “The Cost of Malware Containment”, Ponemon Institute LLC, 1 月 2015.
[8] “日本企業を狙う高度なサイバー攻撃の全貌 – BRONZE BUTLER”, https://www.secureworks.jp/resources/rp-bronze-butler, (参照 2017-08-22)
[9] 伊沢亮一, 森井昌克, 井上大介, “実効命令系列の比較によるアンパッキング手法の提案”, *コンピュータセキュリティシンポジウム 2016 論文集*, vol. 2016, pp. 662–667, 10 月 2016.
[10] Saeed, N., Ali, A. G., “Automated malware classification based on network behavior”, International Conference on Computing, Networking and Communications (ICNC), 2013, pp. 642–647.
[11] 林孝英, 山口由紀子, 嶋田創, 高倉弘喜, “ネットワークトラフィックフローにおけるシーケンスパターンに基づくマルウェア分類手法”, *コンピュータセキュリティシンポジウム 2014 論文集*, vol. 2014, pp. 394–401, 10 月 2014.
[12] 畑田充弘, 森達哉, “実行時の通信挙動を用いたマルウェアの分類と未知検体検出への応用”, *コンピュータセキュリティシンポジウム 2016 論文集*, vol. 2016, no. 2, pp. 647–654, 2016.
[13] 小林峻, 寺田成吾, 瀬戸口武研, 道根慶治, 山下康一, “Drive-by Download 攻撃検知手法の継続的評価と Exploit Kit に対する考察”, *コンピュータセキュリティシンポジウム 2016 論文集*, vol. 2016, no. 2, pp. 964–970, 2016.
[14] “Malware-Traffic-Analysis.net”, http://www.malware-traffic-analysis.net/, (参照 2017-08-22)
[15] “Free Automated Malware Analysis Service - powered by VxStream Sandbox”, https://www.reverse.it/, (参照 2017-08-22)
[16] “VirusTotal”, https://www.virustotal.com/ja/, (参照 2017-08-22)
[17] MWS2017 実行委員会, “研究用データセット MWS Datasets 2017 について”, http://www.iwsec.org/mws/2017/about.html, (参照 2017-08-22)
[18] 寺田真敏, 堀健太郎, 成島佳孝, 吉野龍平, 萩原健太, “研究用データセット『動的活動観測 2015』”, *コンピュータセキュリティシンポジウム 2015 論文集*, vol. 2015, no. 3, pp. 1387–1393, 2015.
[19] 寺田真敏, 佐藤隆行, 堀健太郎, 吉野龍平, 萩原健太, “研究用データセット『動的活動観測 2016』”, *コンピュータセキュリティシンポジウム 2016 論文集*, vol. 2016, no. 2, pp. 892–895, 2016.