Vol.2019-IOT-44 No.6
2019/3/7

標的型攻撃におけるマルウェアの波及範囲の推定 - 感染範囲と経路の特定と可視化方法の開発 -

佐々木京香† 佐々木良一† 猪俣敦夫†

概要：近年，特定の組織を対象に情報窃取を目的としてサイバー攻撃を行う標的型攻撃が社会的な問題となっている．標的型攻撃は初期潜入段階でマルウェアの侵入に成功した端末を起点に侵害範囲を拡大していく．当研究室で開発しているログ分析，対応ガイドシステムである LIFT システムの拡張機能の一つとして感染経路の特定方法を提案している．あわせて感染範囲の可視化機能の開発を行い，各感染端末の感染元端末の特定ができることを確認したので報告する．

キーワード：標的型攻撃，デジタルフォレンジック，ネットワークフォレンジック

Estimation of Spread range of malware against targeted attacks - Development of methods for identifying and visualizing infection route -

KYOKA SASAKI†1 RYOICHI SASAKI†2
ATSUO INOMATA†3

1. はじめに

近年，特定の組織を対象に情報窃取を目的としてサイバー攻撃を行う標的型攻撃が社会的な問題となっている[1]．標的型攻撃の中でも，攻撃対象の組織にマルウェアを添付したメールを送信し攻撃を行う標的型メール攻撃が問題となっている．日本では 2011 年の衆議院事務局、三菱重工への攻撃を境に増加している．また，2016 年には JTB が被害にあい 793 万件の個人情報が流出した可能性がある[2]．
IPA の報告書[3]によると標的型攻撃には 6 段階のシナリオが定義されている．

1. 計画立案段階：標的の組織の情報収集
2. 攻撃準備段階:攻撃に使用する C&C サーバなどの環境作り
3. 初期潜入段階：標的型メールの送信，マルウェア感染
4. 基盤構築段階：攻撃対象環境の調査
5. 内部侵入・調査段階：端末間での侵害の拡大
6. 目的遂行段階：機密情報の外部送信

攻撃者はまず，ソーシャルエンジニアリングなどで対象の内部の情報収集を行う．そこで収集した情報をもとに，初期侵入対象の端末および，侵入・攻撃手段の選定を行う．侵入手段がメールの場合は，悪性のファイルの添付や，メール本文へ悪性サイトのリンク埋め込みなどを行い，攻撃対象に対して送信する．マルウェアの侵入に成功後，次々と端末を乗っ取りながら侵害範囲を拡大していく．そして乗っ取ったサーバから機密情報の窃取を行う．

組織内に感染が拡大していく，内部侵入・調査段階が標的型攻撃の攻撃核心部であり[3]攻撃発覚後は被害範囲の想定が重要となる．
そこで本研究室では，標的型攻撃に適切に対処するため，2013 年に LIFT プロジェクトを立ち上げ，LIFT システムの開発と機能拡張を行っている．LIFT システムは，ログの分析と人工知能などを用いて攻撃への対策を支援するシステムである．本論文では，LIFT システムの拡張機能として特に内部侵入・調査段階に焦点を当て，複数の端末のプロセスとその通信試行のログを解析することで，マルウェアの感染経路を推定する手法を検討し，可視化を行う．これにより，被害範囲の想定や優先して調査すべき端末の特定が可能となると考える．

2. 関連研究

2.1 LIFT システム

本研究室では，収集したログの兆候から攻撃の推定，分析を行う LIFT(Live and Intelligent Network Forensic Technologies：LIFT)システムの開発を進めている．
LIFT システムと本研究との関係を図 1 に示す．
本研究は LIFT システムの拡張機能の開発を行う．当拡張機能は，LIFT システムにより推定された攻撃が，応急対策によって収束したのちに活用する．後述する Onmitsu により記録された端末のログを解析し推定されたマルウェアの波及範囲から，感染経路の推定と感染拡大の経路の可視化を行う．これにより被害範囲の推定や優先して調査すべき端末の特定を支援する．

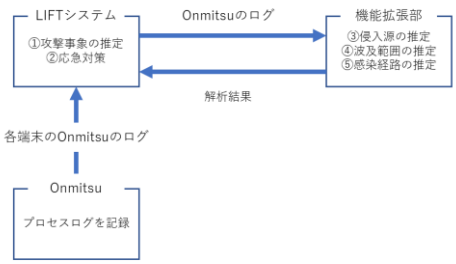

図 1　LIFT システムとの関係図

3. 関連技術

3.1 プロセス記録ツール：Onmitsu

Onmitsu とは不審な通信の原因特定のため，三村らによって開発されたプロセスログ記録ツールである[4]. Onmitsu は Windows の標準 API を利用し，カーネルドライバという形で記録を行う．プロセス情報とそのプロセス情報と関連付けたパケットを常時記録し続けるため，不正プログラムによるプロセス隠匿処理も回避できる可能性が高い．検証実験により，記録したログから不正なプログラムのプロセスと不正なプログラムに関連するプロセスによる通信を結び付けられることが確認されている．

次に Onmitsu に記録されるログについて説明する．表 1 に Onmitsu に記録される情報一覧を示す．Onmitsu で記録する対象はプロセスにおける起動・終了・モジュール読み込み・ネットワーク通信の 4 つの挙動(ログタイプ)である．ログの情報は CSV 形式で出力される．

表 1　Onmitsu により記録される情報一覧

挙動(ログタイプ)	記録内容
プロセス起動	起動時刻
	プロセス ID
	要求を行った親プロセス ID
	実行イメージファイルパス
	コマンドライン
プロセス終了	終了時刻
モジュール読み込み	読み込んだ時刻
	プロセス ID
	モジュールイメージパス
ネットワーク通信	通信確立時刻
	プロセス ID
	接続元 IP アドレス
	接続元ポート番号
	接続先 IP アドレス
	接続先ポート番号
	トランスポート層プロトコル ID

本研究では攻撃挙動をプロセスレベルで把握可能にするため Onmitsu を使用した．また，Onmitsu はプロセスとその通信試行を一つのログに記録することができ，CSV 形式での出力のため汎用的な処理が可能であることも Onmitsu を使用した理由の一つである．

3.2 オントロジ

オントロジとは概念間の関係性を定義する知識ベースのことであり，概念の構造化を行うのに用いられる[5]．オントロジを表現する手法として RDF(Resource Description Framework)がある．RDF は RDF トリプルと呼ばれる主語，述語，目的語の三つの要素を持ち，URI(Uniform Re-source Identifier)で記述されたリソースの関係性を表現する[6]．RDF トリプルは任意の粒度で情報を表現できる．

また，主語と目的語をノードに，述語を矢印にした有効グラフで情報を表現できるため，各情報機器での事象や標的型メール攻撃における各段階での攻撃活動を柔軟に表現することが可能である．プロセスログにオントロジを用いて表現した例を図 2 に示す．

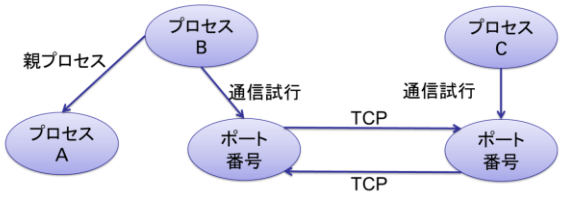

図 2　プロセスログの表現例

このようにプロセスログの情報の表現にオントロジを使用することによって，検知時間がプロセスログのみの場合と比べ約 1/24 となることが佐藤らの研究[7]によって確認されている．

4. 先行研究

4.1 マルウェアの侵入元と波及範囲の推定

佐藤らは Onmitsu から得られるプロセスログを用いてマルウェアの感染が検知された端末のプロセスログから，遡上的に調査していくことにより，同一ネットワーク上のマルウェア侵入源の端末の発見が可能であることを示している[7].

島川らは，それらに加え Onmitsu から得られるプロセスログを用いてマルウェアへの感染が検知された端末の波及範囲を推定する手法を開発してきた[8].

ネットワーク上の端末を手当たり次第調査していくの

では波及範囲の推定を迅速に行うことが困難であり，再立ち上げまでの時間が多くかかり組織の損害は膨大となる．島川らの提案した手法を導入することにより正確な波及範囲の推定が可能となる．

先行研究では次のようにして時間を短縮している．まず，既存のマルウェア検知手法や IDS などによって検知されたマルウェア感染端末を起点とし，佐藤らの手法[7]を適用する．続いて，特定された端末群を調査対象とすることで優先して調査する端末の絞り込みを行う．

波及範囲推定手法は以下の手順である．

1. 侵入源の端末で検知されたマルウェアの子プロセスがクライアント端末の特徴を持つか調査
2. 調査結果から通信先の端末を特定
3. 通信先の端末がリモート端末の特徴を持つか調査
4. 特定した端末のリモート端末の特徴プロセスの子プロセスを調査しマルウェアの起動兆候を発見
5. その子プロセスがクライアント端末の特徴を持つか調査
6. 手順 2〜5 を繰り返す

4.2 感染拡大の模擬

JPCERT/CC の報告書[9]によると，感染拡大の際に使用する遠隔操作ツール・コマンドは表 2 に挙げたものが多いと確認されている．島川らの研究では感染範囲の拡大を模擬するために表 2 に示した遠隔操作ツール・コマンドを主な対象としている．実験において RAT/ボットシミュレータである ShinoBOT[10]を標的型攻撃に使用されるマルウェアに見立てて感染させ，感染端末で表 2 のツール・コマンドを用いて感染範囲の拡大を行っている．

表 2　悪用される遠隔操作ツールの特徴

ツール・コマンド	クライアント端末		リモート端末
	起動プロセス	通信施行時の宛先ポート番号	起動プロセス
PsExcec	psexec	135	PSEXESVC
wmic	wmic	135	WmiPrvSE
PowerShell	powershell	5985	Wsmprovhost
at	at	445	Taskeng

4.3 感染端末の特定

感染拡大の模擬に対して島川らの感染範囲推定の手法[8]を適用したところ，図 3，4 の結果が得られている．

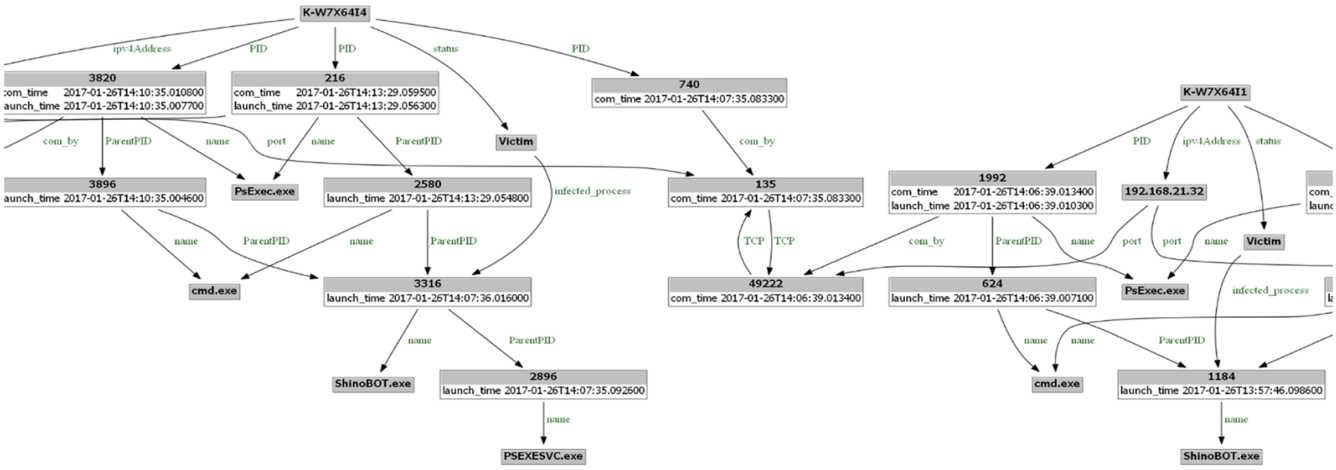

図 3　島川らの実験結果 1

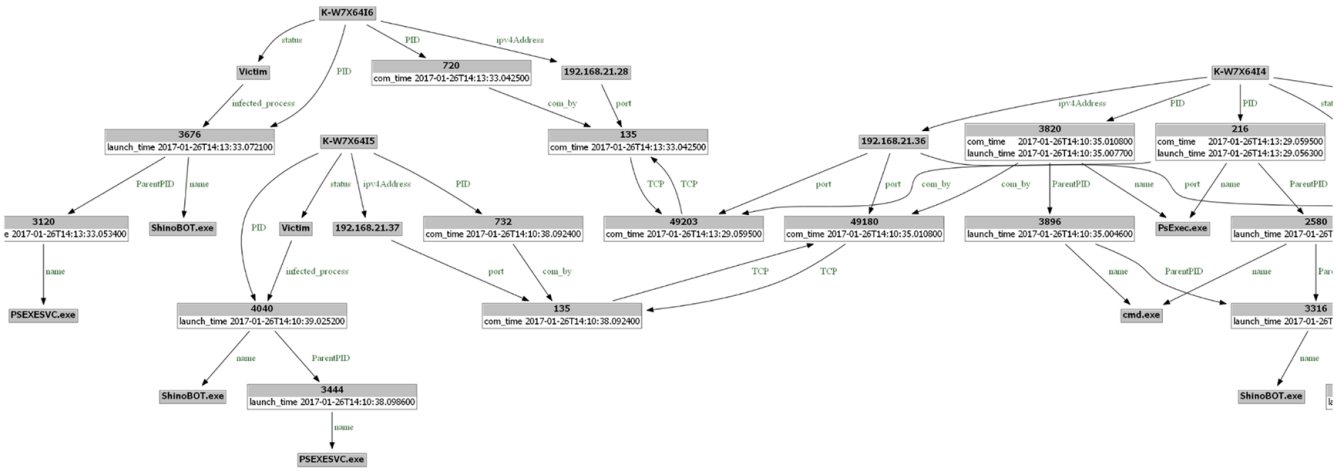

図 4　島川らの実験結果 2

図 4，5 は実験結果の一部を抜き出したもので，得られた RDF トリプルは以下の通りである．

・RDF トリプル(ホスト名，PID，プロセス ID)
・RDF トリプル(ホスト名，ipv4Address, IP アドレス)
・RDF トリプル(ホスト名，status，マルウェア感染状態)
・RDF トリプル(プロセス ID，name，プロセス名)
・RDF トリプル（プロセス ID，ParentPID，親プロセス ID）
・RDF トリプル（プロセス ID，launch_time，起動時間）
・RDF トリプル(プロセス ID，com_by，送信元ポート番号)
・RDF トリプル(プロセス ID，com_time，通信時間)
・RDF トリプル（IP アドレス，port，送信元ポート番号）
・RDF トリプル（送信元ポート番号，TCP，宛先ポート番号）
・RDF トリプル(マルウェアの感染状態, infected_process, マルウェアのプロセス ID）

これらの RDF トリプル群の主語と述語を照合していくことで以下のことがわかる．

・端末 1 で起動された ShinoBot.exe(PID：1184)により PsExcec.exe(PID：1992)により端末 4 への TCP 通信が行われている
・端末 1 からの通信後，端末 4 で PSEXESVC.exe(PID：2896)が起動され，ShinoBot.exe(PID：3316)が起動し，ShinoBot.exe により起動された PsExcec.exe(PID:3820)により端末 5 への通信が行われている．

以上より，侵入源である端末 1 内で起動されたマルウェア(ShinoBot.exe)を起因として感染範囲の拡大が生じていることが確認されている．

4.4 先行研究の残された問題点

島川らの手法は次のような問題点があった．

(1)感染経路を把握するためには解析者自身で RDF トリプルの主語と述語を照合していく必要があった．RDF トリプルを 1 つずつたどりながら感染プロセスを照合していく方法は，感染経路の迅速な判断が困難であり，専門的な知識が必要である．

(2)可視化されていないため，どこまで波及しているのかが多くの人に理解しくい．

そこで本研究では，感染拡大プロセスの特定を行い感染経路の自動判定を行う方法を提案する．併せて，自動判定によって得られた感染範囲について端末間の感染に焦点をあて，可視化することで被害状況の迅速な把握を可能とする手法を提案する．

5. 提案手法

5.1 感染拡大プロセスの特定

本研究では，先行研究で達成された攻撃挙動のプロセスの把握とマルウェア感染範囲の推定をもとに感染拡大プロセスの特定を行う．これにより、特定の端末がどの端末からの通信によってマルウェア感染に感染したのかという感染経路の自動判定機能の実装を目指す．

5.2 グラフの作成

標的型攻撃は初期感染端末を起点に侵害を拡大していくため，組織内の複数の端末がマルウェアに感染している恐れがある．そのため，攻撃発覚後の被害範囲の想定や対応の優先順位付けが重要となる．感染範囲の可視化により，インシデントレスポンスにおけるトリアージ段階において，被害範囲の想定を迅速に行えるよう支援する．

また，攻撃の対応担当者とその攻撃に関連する部署との情報共有の際に，可視化したグラフを用いることで被害状況の把握を迅速に行い攻撃への対応の連携を支援する．

6. 実装

6.1 感染拡大プロセス

感染拡大時のシーケンスは攻撃者が外部の C&C サーバを経由してマルウェアにコマンドを送り，リモート管理ツール・コマンドを起動する．その後内部通信を行い他端末にマルウェアを転送し起動する．

リモート管理ツールとして PsExcec 等を使用している場合，PsExcec の親プロセスをたどると必ず外部と通信を行っている．このため，リモート管理ツール・コマンドの親プロセスが外部と通信を行っていることを不審と定義する．

ShinoBOT を用いた感染拡大のプロセスは図 5 のようになっている．

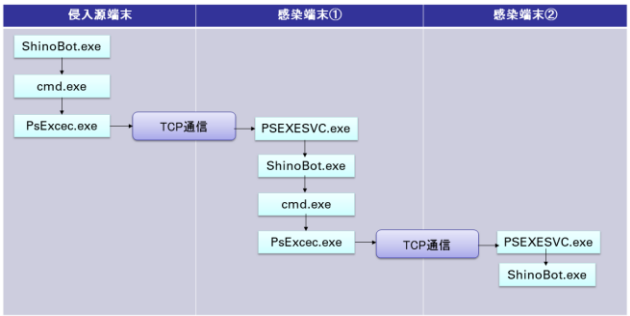

図 5　ShinoBOT 感染プロセス

まず感染源端末で ShinoBot.exe が親プロセスとなり cmd.exe を起動する．その後 PsExcec.exe が起動され TCP 通信を行う．感染源端末と TCP 通信を行ったことにより他の端末へ感染が広がっていく．特定した感染拡大プロセスが，各端末の RDF トリプル群に存在しているか調査してい

くことで感染拡大の経路を特定する．

感染経路の特定に用いたフローチャートを図 6 に示す．

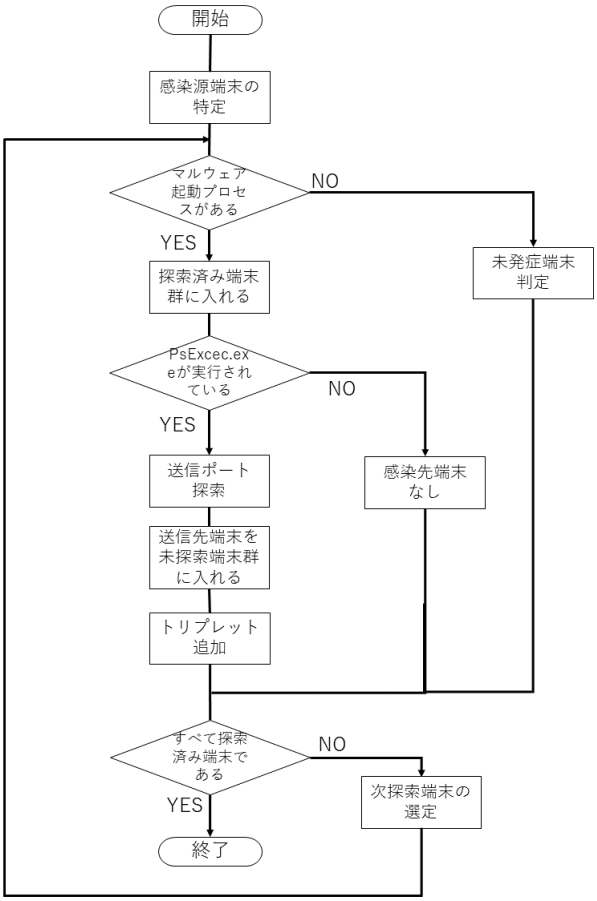

図 6　感染経路特定フロチャート

感染経路特定の手法は以下の通りである．

① まず，佐藤らの手法[7]で感染源端末を特定する．

② 次に島川らの手法[8]によって得られた RDF トリプルに対して以降の判定を行う．

③ 感染源端末を調査対象端末とし，マルウェアである ShinoBOT の起動プロセスの有無の判定を行う．ShinoBOT が起動されていなかった場合，その端末をウイルス未発症端末群とする．ShinoBOT が起動されていた場合，調査済み端末群にし，次の判定を行う．

④ PsExcec の実行プロセスの有無の判定を行う．実行されていなかった場合，調査対象端末の感染先端末なしとする．実行されていた場合，TCP 通信の送信ポートを特定する．

⑤ 送信ポートの通信先端末を未調査端末群にする．

⑥ RDF トリプル(送信元端末，Infected ，通信先端末)を追加する．

⑦ すべて調査済み端末であるか判定を行う．未調査端末群が残っていた場合，次の調査対象端末を選定し③から⑦を繰り返す．

⑧ すべて調査済み端末の場合，調査を終了する．

このアルゴリズムを島川らの実験 1[8]に適用した結果，感染元端末と感染先端末を特定可能となった．また，追加されたトリプレットを突合することにより，すべての端末の感染経路の特定が可能であった．

6.2　感染範囲の可視化

本研究では，感染範囲の可視化のため 2 つのグラフを作成する機能を実装した．

(1)感染推移サークルグラフ

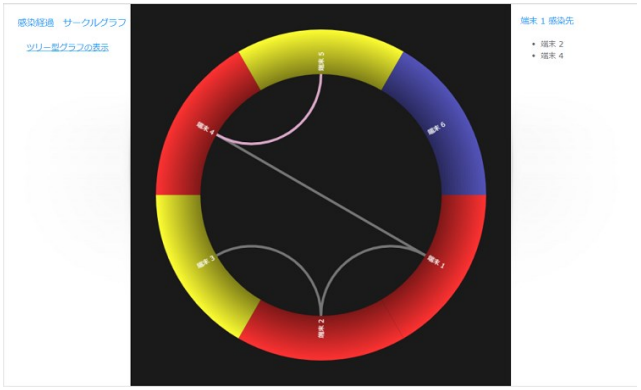

図 7　サークルグラフ

感染拡大プロセスと感染経路の特定機能の実装の際に追加された RDF トリプル(送信元端末，Infected，送信先端末)から JavaScript でサークルグラフを作成する機能を実装した．各端末を円状に配置し，感染拡大の経路が線円グラフ内の線で表され，同一ネットワーク全体の端末の感染経路を把握することができる．各端末の感染状況が色で判別可能であり，以下の通りである．

・青，未感染

・黄，感染しているが他端末への感染拡大なし

・赤，感染しており，他端末への感染拡大あり

島川らの手法[8]では RDF の突合を一つずつ行うため，全端末の感染状況を一度で把握することは困難であったが，サークルグラフを用いることで感染推移の把握を迅速に行うことができる．

(2)ツリー型グラフ

図 8　ツリー型グラフ

ツリー型グラフは感染源端末を頂点として，感染端末を階

層で表現するグラフである. 任意の端末を選択することで, その端末から感染が拡大した感染先端末群の表示が可能である.

ツリー型グラフは同一ネットワーク上の端末が多い場合であっても感染元端末，感染先端末の関係性の把握が容易である．また感染源端末からの深さによって，端末が感染源端末から何次感染であるかが判断可能であり，影響範囲を迅速に把握することができる.

7. 考察

本論文の提案手法により, 一つずつ RDF トリプルをたどらずとも感染拡大プロセスの特定が可能となり，感染元の端末が特定できることができた.

また，提案手法により特定された感染経路を 2 つのグラフで可視化することで, ログの解析や RDF の照合方法などの専門知識を持たずとも感染端末の把握が容易となった. 感染範囲の可視化を行うことでより迅速に被害状況の把握が可能となり，事後対応を行うことができる.

8. 今後の課題

今回の研究では ShinoBOT を用いた検証実験で得られた結果に対して感染元端末の特定，感染経路の解析を行っているが，実際の標的型攻撃では ShinoBOT 以外も使用されるため，ShinoBOT 以外の攻撃においても感染プロセスを特定し，提案手法が適用可能か評価する必要がある.

また，本研究は組織内の感染端末についてプロセスレベルでの調査を行っているが，攻撃による被害を受けたファイルなどを調査する，各 1 端末内での影響範囲を調査する手法が Md Nahid Hossain らにより提案されている[11]. 本研究で特定した端末群に対し，Md Nahid Hossain らの提案手法を用いることでより詳細な被害の推定を行うことができると考える.

9. おわりに

本研究では，標的型攻撃における内部侵入・調査段階に焦点を当て，複数端末のプロセスログの解析，突合の自動化の手法を提案した．また，提案手法によって得られた感染範囲の解析結果の可視化を行う手法を提案した.

今後は今回検証した ShinoBOT 以外を用いた標的型攻撃においても感染端末の解析を検討していくとともに，被害を受けたファイルなどの 1 端末内の影響範囲を推定する手法について検討していく.

参考文献

[1] マカフィー株式会社：マカフィー公式ブログ，標的型攻撃とは？高度化するサイバー攻撃の特徴と手口を徹底解説，https://blogs.mcafee.jp/targeted-attack-threat-feature，(参照 2018-12-15).

[2] 株式会社 JTB：不正アクセスによる個人情報流出の可能性について - 現状報告と再発増資策 - , https://www.jtbcorp.jp/jp/160824.html，(参照 2018-12-15).

[3] IPA 独立法人情報処理推進機構：「高度標的型攻撃」対策に向けたシステム設計ガイド，https://www.ipa.go.jp/files/000046236.pdf，(参照 2018-12-15).

[4] 三村聡志，佐々木良一：プロセス情報と関連付けた通信情報保全手法の提案，情報処理学会論文誌，Vol57，No.9，pp.1944-1953(2016)

[5] 東京大学政策ビジョン研究センター：政策関連用語集 , http://pari.u-tokyo.ac.jp/publications/words/words_a/a_17.html , (参照 2018-12-15).

[6] 兼岩憲 : RDF と RDF スキーマの推論，人工知能学会論文誌，26 巻 5 号 a(2011) ，(参照 2018-12-15).

[7] 佐藤信，杉本暁彦，林直樹，磯部義明，佐々木良一：マルウェアによるネットワーク内の挙動を利用した標的型攻撃における感染経路検知ツールの開発と評価，情報処理学会論文誌, Vol.58, No.2, pp.366-374（2017）

[8] 島川貴裕，佐藤信，佐々木良一：標的型攻撃に対する知的ネットワークフォレンジックシステム LIFT の開発と拡張機能(その 3)-侵入源と波及範囲の推定-，Computer Security Symposium 2017

[9] JPCERT/CC：インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書，https://www.jpcert.or.jp/research/ir_research.html. ，（参照 2018-12-15).

[10] Shota Shinogi : ShinoBOT -the rat/bot malware simu-lator，ShinoBOT Can you detect an APT like me？，http://shinobot.com/top.php，(参照 2018-12-15).

[11] Md Nahid Hossain， Sadegh M. Milajerdi， Junao Wang，Birhanu Eshete， Rigel Gjomemo，R. Sekar，Scott D. Stoller，V.N. Venkatakrishnan : Real-time Attack Scenario Reconstruction from COTS Audit Data，26th USENIX Security Symposium