Vol.2017-DPS-170 No.34
Vol.2017-CSEC-76 No.34
2017/3/3

標的型攻撃に対する侵害範囲特定ツールの開発と評価

島川貴裕[†1]　佐藤信[†1]　久山真宏[†1]　佐々木良一[†1]

概要：近年，特定の企業や組織を攻撃対象とする標的型攻撃が社会的な問題となっている．標的型攻撃は，段階的に攻撃を進めていく過程がある．中でも攻撃の核心部となるのは，初期段階で乗っ取った攻撃基盤をベースに，次々と端末を乗っ取りながら侵害範囲を拡大していく内部侵入・調査段階である．そのため，不正プログラムの感染を検知された端末から不正プログラムを調査・駆除するのみでは，被害範囲の想定ができず攻撃の対処を誤ってしまう可能性がある．そこで本稿では，内部侵入・調査段階に焦点をあて，複数の端末のプロセスログを解析・突合することで侵害範囲を特定する手法を提案する．また，提案手法を実現するプロトタイプのプログラムを開発し，攻撃者による侵害範囲の拡大を模擬した評価実験を行った．その結果，侵害範囲を約 120 秒で特定することができた．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であり，事故対応から事業の復旧までの時間を短縮できると考えられる．

キーワード：セキュリティ，標的型攻撃，ログ解析，RDF，侵害範囲，ツール

Development and Evaluation of Infringement Range Identifying Tool against Targeted Attacks

TAKAHIRO SHIMAKAWA[†1]　MAKOTO SATO[†1]
MASAHIRO KUYAMA[†1]　RYOICHI SASAKI[†1]

Abstract: In recent years, targeted attacks aiming at specific companies and organizations have become a social problem. Targeted attacks have a process of gradually advancing attacks. Especially, the core part of the attack is the internal invasion / investigation stage which will expand the range of infringement while taking over the terminal one after another based on the attack base taken over at the initial stage. Therefore, it is impossible to assume the scope of damage only by investigating and removing malicious program from terminals detected infection by a malicious program. As a result, there is a possibility of erroneously coping with the attack. In this paper, we propose a method to identify the range of infringement by analyzing and matching process logs of multiple terminals focusing on the internal invasion / investigation stage. We developed a prototype program that realizes the proposed method and conducted an evaluation experiment simulating expansion the range of infringement by an attacker. As a result of experiments, it was possible to identify the range of infringement in about 120 seconds. Thus, it is possible to assume the range of damage and identify terminals to be investigated preferentially, and it is considered that the time from accident response to restoration of business can be shortened.

Keywords: Security, Targeted attack, Log analysis, RDF, Infringement range, Tool

1. はじめに

近年，特定の企業や組織を攻撃対象とする標的型攻撃が社会的な問題となっている．標的型攻撃とは，金銭や知的財産等の機密情報の窃取を目的として特定の標的に対して行われるサイバー攻撃である[1]．日本では，2011 年に起きた衆議院事務局や三菱重工に対する攻撃を境に年々増加の傾向にある．2015 年には日本年金機構が被害に遭い 125 万件の個人情報が流出した[2].

IPA の報告書[3]によると，標的型攻撃の攻撃シナリオは，以下の 7 段階で定義されており，攻撃全体が計画的に進行されていく．

1. 計画立案段階：標的組織を設定し関連情報の収集
2. 攻撃準備段階：攻撃に必要となる環境の準備
3. 初期潜入段階：偽装メール，ウェブサイト閲覧等による不正プログラム感染
4. 基盤構築段階：感染端末を起点にして環境の調査
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：窃取した機密情報の外部送信
7. 再侵入段階：継続的に再侵入

まず，計画立案段階で収集した情報を基に，初期潜入段階で標的ユーザを確実に騙し，標的組織の端末を不正プログラムに感染させる．次に，基盤構築段階で感染した端末を起点にして標的組織のネットワーク環境の調査を行い，内部侵入・調査段階で他端末への乗っ取りを繰り返し，侵害範囲を拡大していき機密情報のある端末への乗っ取りを試みる．そして，目的遂行段階で機密情報のある端末から機密情報を収集し外部に送信する．再侵入段階では，確保した通信経路を用いて，継続的に再侵入し，標的組織のネットワーク内探索を継続する．この攻撃段階の中でも標的型攻撃の攻撃核心部は，基盤構築段階で確保した攻撃基盤をベースに，次々と端末を乗っ取りながら侵害範囲を拡大

†1 東京電機大学
Tokyo Denki University

していく内部侵入・調査段階である[3]．そのため，不正プログラムの感染を検知された端末から不正プログラムを調査・駆除するのみでは，被害範囲の想定ができず攻撃の対処を誤ってしまう可能性がある．したがって，被害範囲を想定し適切な対処を行うためには，感染端末の特定後，不正プログラムの調査だけでなく端末内のプロセスや通信に関するログ等を解析し，他端末への侵害が行われていないか調査していき侵害範囲を特定する必要がある．また，侵害範囲の特定には，有用なログを常に記録し続け，有時の際に収集し，解析・突合することで特定可能である．しかし，ログの解析・突合には，高度な専門知識が必要であるうえに時間を要するため侵害範囲の迅速な特定が困難である．

そこで，本研究では内部侵入・調査段階に焦点をあて，複数の端末で記録したプロセスとその通信試行に関してのログであるプロセスログを解析・突合することで侵害範囲を特定する手法を提案する．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り，事故対応から事業の復旧までの時間が短縮可能になると考える．

本稿では，第 2 章で先行研究・関連技術，第 3 章で関連研究について述べる．次に，第 4 章で提案手法の詳細について述べ，第 5 章で性能評価実験について述べる．そして最後に第 6 章で今後の課題を含めたまとめを述べる．

2. 先行研究・関連技術

2.1 先行研究

これまで，著者の 1 人の佐藤を中心に標的型攻撃における内部侵入・調査段階で感染経路を検知する手法を検討してきた[4]．攻撃の発覚後に被害範囲を想定する上で，感染経路を迅速に検知することは重要である．これまで，不正プログラムに感染した端末を発見する手法は数多く研究されてきたが，自動的に他の端末への感染経路まで調査する手法は少ない．

そこで，佐藤らは後述するプロセスログを用いて不正プログラムが起動した子プロセスまで調査するプロセスレベルでの感染経路を検知する手法を検討してきた．この手法では，各端末のプロセスログに内部侵入・調査段階で用いられるツールのプロセスとそのプロセスによる通信試行が記録されているかを調査し，各端末のプロセスログを突合していくことで感染経路を検知する．また，プロセスログの調査は，既存の不正プログラム検知手法や IDS によるアラートなどを基点として，不正プログラムへの感染が検知された端末のプロセスログから感染源の端末が特定されるまで遡上的に調査していく．これまで，検証実験により，侵害範囲の拡大の際に発生する内部通信の特徴を用いることでプロセスレベルでの感染経路が適切に追跡可能であることが確認されている．しかし，佐藤らの手法では感染経路が分岐している場合，一連の感染経路のみの特定はできるが，範囲としての特定ができない．そのため，本研究では，佐藤らの研究により特定された感染経路上の端末を再調査してくことで経路上の端末が行った経路上以外の端末への侵害を発見することで侵害範囲を特定する．

2.2 関連技術

2.2.1 プロセスログ記録ツール：Onmitsu

Onmitsu とは，不審な通信の原因特定に有用な情報源である揮発性情報を記録するために三村らが開発したプロセスログ記録ツールである[5]．Onmitsu は，Windows の標準 API を利用しカーネルドライバという形でシステム内に導入する．そして，プロセス情報とそのプロセスが発した通信に関しての動作ログを常時記録し続ける．そのため，不正プログラムによるプロセス情報の隠匿処理も回避できる可能性が高い．また，検証実験により記録したログから不正プログラムのプロセスと不正プログラムに関するプロセスが発した通信とを結びつ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．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．また，ログに記録される情報は，以下の通りであり，CSV 形式で記録される．

年, 月, 日, 時, 分, 秒, ミリ秒, ログタイプ, PID, ParentPID, ファイルパス，コマンドライン，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，プロトコル番号

本研究では，以下の理由からプロセスログの記録に Onmitsu を用いた．

- 侵害範囲の特定にはプロセスレベルでの追跡が必要
- 不正プログラムによるプロセスの隠匿処理を回避できる可能性が高い
- 出力されるログファイルが CSV 形式であり汎用的に処理が可能

2.2.2 オントロジ

オントロジとは，知識をあるドメイン内の概念と概念間の関係を形式的に表現する手法である．オントロジを具体的に表現する一手法として RDF（Resource Description Framework）が存在する[6]．RDF では，主語，述語，目的語という 3 つの要素（RDF トリプル）でリソースに関する情報を表現する．主語は記述対象のリソース，述語は主語の特徴や主語と目的語の関係，目的語は主語との関係のあるリソースや述語の値を表現している．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向グラフで表現でき視覚化できる．さらに，RDF トリプルの集合と推論規則を組み合わせることで，異なる種類のデータを柔軟に繋ぎ合わせて，

その部分和以上の総体を作ることができる．

本研究では，以下の理由からプロセスログの情報を表現する手法としてオントロジを採用した．

- 各端末ログの関係性を柔軟に表現が可能
- 共通する述語を繋ぎ合わせることで各端末ログの突合が容易
- 有向グラフで表現できるため視覚的な把握が容易

3. 関連研究

本章ではまず，標的型攻撃における内部侵入・調査段階に着目した関連研究との差異を述べる．次に，被害状況の把握を目的とした関連研究との差異について述べる．

標的型攻撃における内部侵入・調査段階に着目した研究として，川口らは複数の端末で行われるさまざまな種類の不審活動を関連づけることで拡散活動を検知する手法を提案している[7]．この手法では，攻撃者の拡散活動にともない不審性が高い端末が連鎖的に現れる現象を，被攻撃端末をノードとするグラフ構造として抽出する．そして，このグラフがある基準を満たすとき，標的型攻撃における拡散活動が発生していると判断してアラートをあげる．また，類似の研究として，海野らは標的型攻撃におけるシステム内部の諜報活動を検知する手法を提案している[8]．この手法では，標的型攻撃において攻撃基盤を拡大する過程に攻撃者が使わざるを得ない共通の攻撃手法をチョークポイントと定義し，このチョークポイントによるシステムのふるまい解析によって諜報活動の検知を行っている．これらの研究では，攻撃の検知を主な目的としているため攻撃の検知後の被害状況の把握については検討されていない．そのため，本研究はこれらの研究で攻撃を検知した後の被害状況の把握のための追加調査の研究として位置づけられる．

被害状況の把握を目的とした研究として，遠峰らは標的型攻撃の被害状況の把握やインシデントの分析に利用できるログの可視化手法を提案している[9]．この手法では，複数の端末で発生したさまざまなインベントログを集約し，一覧できるよう同一時間軸上に並べて可視化を行う．これにより，解析者は複数の端末を横断して発生したイベントを捉えることができるため，効率的な被害状況の把握の支援が行える．しかし，遠峰らの手法では，端末が侵害されているかどうかの判断は解析者が行わなければならないため，侵害範囲の特定までに時間を要する．遠峰らの手法に対し，本研究では，侵害拡大の際に使用されたプロセスのログを突合した結果を解析者に出力することにより，迅速な侵害範囲の特定を可能とする．

4. 侵害範囲特定ツールの開発

本章ではまず，侵害範囲の特定までの大まかな流れについて説明する．次に，4.1 節で侵害範囲拡大の際に悪用される遠隔操作ツールの特徴について述べ，4.2 節で提案する侵害範囲特定手法について述べる．そして，4.3 節で提案手法を実装したプロトタイプのプログラムの開発について述べる．

侵害範囲の特定までの大まかな流れは次の通りである．

1. 不正プログラムに感染した端末の検知
2. 検知した端末を起点に佐藤らの研究[4]による感染経路の検知
3. 感染経路上の端末の再調査による侵害範囲の特定

ネットワーク内の端末をやみくもに調査するのでは迅速な侵害範囲の特定が困難である．そこで，本研究では，既存の不正プログラム検知手法や IDS などによるアラートを利用し，不正プログラムに感染した端末を検知した後，佐藤らの研究により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．これにより，迅速な侵害範囲の特定を目指す．また，感染経路上の端末は初期感染端末から順に調査を行っていく．

4.1 悪用される遠隔操作ツールの特徴

JPCERT/CC の報告書[10]によると，攻撃者が侵害範囲を拡大する際に悪用する遠隔操作ツールには同じものが使用されることが多いと分かっている．また，JPCERT/CC の報告書[10]から悪用されることが多い代表的な遠隔操作ツールによる内部通信時の特徴を表 1 に示す．表 1 から，悪用される遠隔操作ツールによる内部通信時には特徴的なプロセス，ポート番号が用いられていることがわかる．また，本研究ではまず企業などで業務にも使用されることがある表 1 に示した遠隔操作ツールを主な対象とした．

表 1　悪用される遠隔操作ツールの特徴
Table 1　Features of remote control tool to be abused.

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	通信試行時の宛先ポート番号	起動プロセス
PsExec	psexec	135	PSEXESVC
WMIC	WMIC	135	WmiPrvSE
PowerShell	powershell	5985	Wsmprovhost
at	at	445	Taskeng

ここで，例として PsExec を用いて内部通信を行った場合の挙動について説明する．PsExec を用いた内部通信は以下の流れで行われる．

1. クライアント端末が PsExec のプロセスを起動
2. リモート端末へ向けて宛先ポート番号 135 で psexec

による通信が発生

3. リモート端末でクライアント端末へ向けて対応する通信が発生
4. リモート端末で PSEXESVC が起動
5. PSEXESVC が親プロセスとなりリモートコマンドを実行

表 1 の他のツール・コマンドを用いて内部通信を行った場合であっても，起動プロセスと通信試行時の宛先ポート番号が変わるだけでリモートコマンドの実行までの流れ自体は変わらない．

4.2 侵害範囲特定手法

本研究で提案する侵害範囲特定手法では，前節で述べた悪用される遠隔操作ツールの内部通信とその通信を行っているプロセスの関係を明確にすることで侵害挙動を追跡していく．本提案手法は，佐藤らの研究[4]により特定された感染経路上の端末に対し，表 1 の特徴がプロセスログに存在するか調査する手法である．

1. 初期感染端末で検知された不正プログラム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不正プログラムの起動を発見
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 の段階で不正プログラムの起動が発見できなかった場合，リモート端末の特徴プロセスの子プロセスがクライアント端末の特徴を持つか調査を行う．

4.3 プロトタイプの開発

機能評価を行うためにプロトタイプのプログラムの開発を行った．機能要件は次の 2 つである．

- 4.2 節で述べた手順の自動的な処理
- 各端末の調査結果の統合

各端末の調査結果を統合するために情報処理機器間の関係を RDF で表現した．また，情報処理機器間の関係を RDF で表現するために定義した語彙と関係性は，図 1 に示す佐藤らの研究[4]で使用されたものと同一のものを使用した．

ネットワーク構造の表現に利用
＊語彙：CybOXから引用

ネットワーク語彙	プロセス語彙
network interface	process name
ipv4 address	process id
ipv6 address	parent process id
mac address	service groupe name
default gateway	
host name	
port number	

内部侵入段階の表現に利用
＊語彙：独自定義，関係性：独自定義

語彙	定義
host name	CybOXと同じ
status	マルウェア感染状態を示す

関係性	使用目的
Penetration	ホスト名間をつなぐ
infect process	statusとプロセス名をつなぐ

図 1　佐藤らにより定義されたオントロジの一部
Figure 1　A part of the Ontology defined by Sato et al.

表 2 に侵害範囲特定プログラムの開発環境を示す．また，調査結果の可視化については，グラフ描画ツールである Graphviz[11]を用いて RDF により記述された侵害範囲を可視化した．

表 2　開発環境
Table2　Development environment.

OS	Windows7
開発言語	Python2.7
ステップ数	約 1100

5. 評価実験

5.1 実験概要

提案手法の有効性評価および，開発したプログラムの性能を評価するために，標的型攻撃における侵害範囲の拡大を模擬した実験を行った．実験では，以下のことを確認するために木構造を持つ感染経路で実験を行った．

1. 侵害経路が分岐していた場合であっても侵害が行われた端末群を特定可能
2. ネットワーク内の端末のうち，侵害が行われた端末のみを特定可能

また，今回の実験では，仮想環境上に 6 台の Windows 端末を用意し侵害範囲の拡大を模擬した．

5.2 実験手順

侵害範囲の拡大を模擬するために，RAT／ボットマルウェアシミュレータである ShinoBOT[13]と攻撃者に悪用されることが多い遠隔操作ツールである PsExec[14]を用いて次の手順で侵害範囲を拡大した．

1. 感染源端末で ShinoBOT を実行
2. 感染先端末へ向けて PsExec を用いて内部通信を実行
3. 感染先端末へ ShinoBOT を転送し，実行

また，実験中は， Onmitsu により各端末のプロセスログを記録する．

実験 1 では，侵害経路が分岐していた場合であっても侵害が行われた端末群を特定可能であるかを確認するために，図 2 のように侵害範囲の拡大を模擬した．そして，侵害範囲の拡大を模擬した後，端末 1 から端末 3 までの一連の侵

害経路が先行研究により特定されたと仮定し，感染源である端末 1 に対し提案手法を適用する．

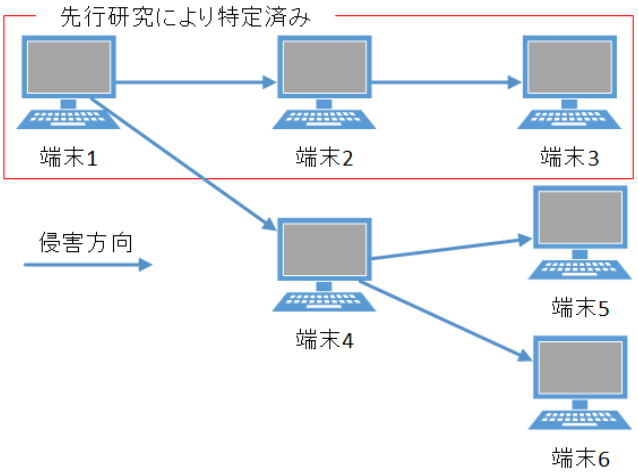

図 2　実験 1 における侵害範囲の拡大
Figure 2　Expansion of infringement range in experiment 1.

実験 2 では，PsExec の通信が受信可能な端末を限定することにより，侵害が可能な端末と不可能な端末を用意する．そして，全ての端末が侵害されるように侵害範囲の拡大を試みる．これにより，ネットワーク内の端末のうち，優先して調査すべき端末である侵害が行われた端末のみを特定可能であるかを確認する．また，今回の実験では，端末 2，端末 4 の 2 台のみ PsExec の通信が受信可能とし，図 3 のように侵害範囲の拡大を模擬した．そして，侵害範囲の拡大を模擬した後，端末 1 から端末 2 までの一連の侵害経路が先行研究により特定されたと仮定し，感染源である端末 1 に対し提案手法を適用する．

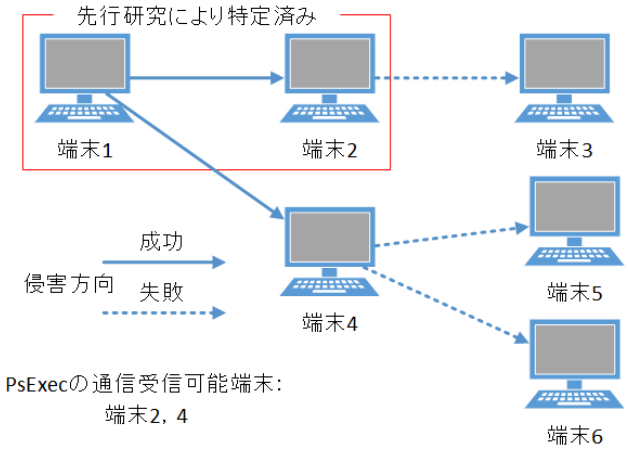

図 3　実験 2 における侵害範囲の拡大
Figure 3　Expansion of infringement range in experiment 2.

また，各実験において開発したプログラムによって侵害が行われた端末を全て特定するまでの時間を計測し，実用性を評価する．

5.3 実験結果

実験 1 の結果，提案手法により侵害が行われた端末を全て特定することができた．また，開発したプログラムによって侵害が行われた端末を全て特定するまでの時間は約 120 秒であった．図 4 は，実験 1 における侵害行為に関する結果の一部を抜き出したものである．図 4 中に示している 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，不正プログラム感染状態）
- 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（不正プログラム感染状態，infected_process，不正プログラムのプロセス ID）

図 4 中の RDF トリプル群の主語と述語を照合していくことにより以下のことがわかる．

- 端末 1（K-W7X64I1）で ShinoBOT.exe により起動された PsExec.exe により端末 2（K-W7X64I2）へ通信が行われている
- 端末 1 からの通信後，端末 2 で PSEXESVC.exe が起動され，PSEXESVC.exe により ShinoBOT.exe が起動されている
- 端末 2 で ShinoBOT.exe により起動された PsExec.exe により端末 3（K-W7X64I3）へ通信が行われている

このことから，感染源端末である端末 1 内で起動された不正プログラム（ShinoBOT.exe）を起因として侵害範囲が拡大しているということがわかる．

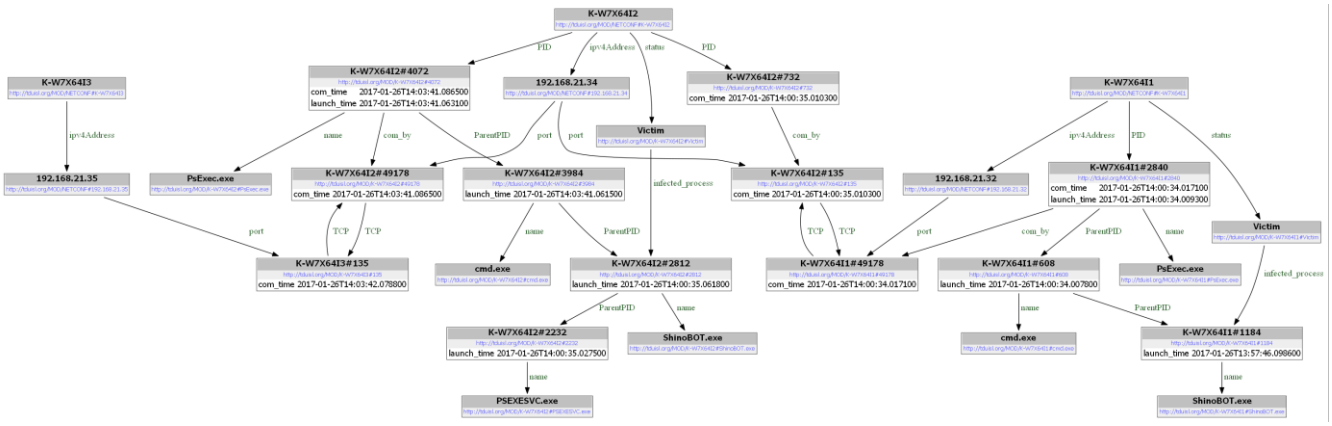

図 4　実験 1 における侵害行為に関する結果の一部

Figure 4　Part of the result on infringing acts in experiment 1.

図 5 は，実験 1 における侵害を行った際に発生した内部通信部分のみを抜き出したものである．図 5 中に示している RDF トリプルは以下の通りである．

- RDF トリプル（ホスト名，ipv4Address，IP アドレス）
- 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）

図 5 中の RDF トリプル群の主語と述語を照合していくことにより以下のことがわかる．

- 端末 1 から端末 2，端末 4（K-W7X64I4）へ通信が行われている
- 端末 2 から端末 3 へ通信が行われている
- 端末 4 から端末 5（K-W7X64I5），端末 6（K-W7X64I6）へ通信が行われている

また，端末 5 と端末 6 の RDF トリプル群を見ると通信を行ったのは端末 4 のみであり，端末 1 から端末 3 までの経路上の端末と通信をしていないということもわかる．

以上の結果から，プロセスレベルで追跡を行うことにより，不正プログラムに起因した通信を特定することができ侵害範囲の拡大を特定可能であることがわかった．

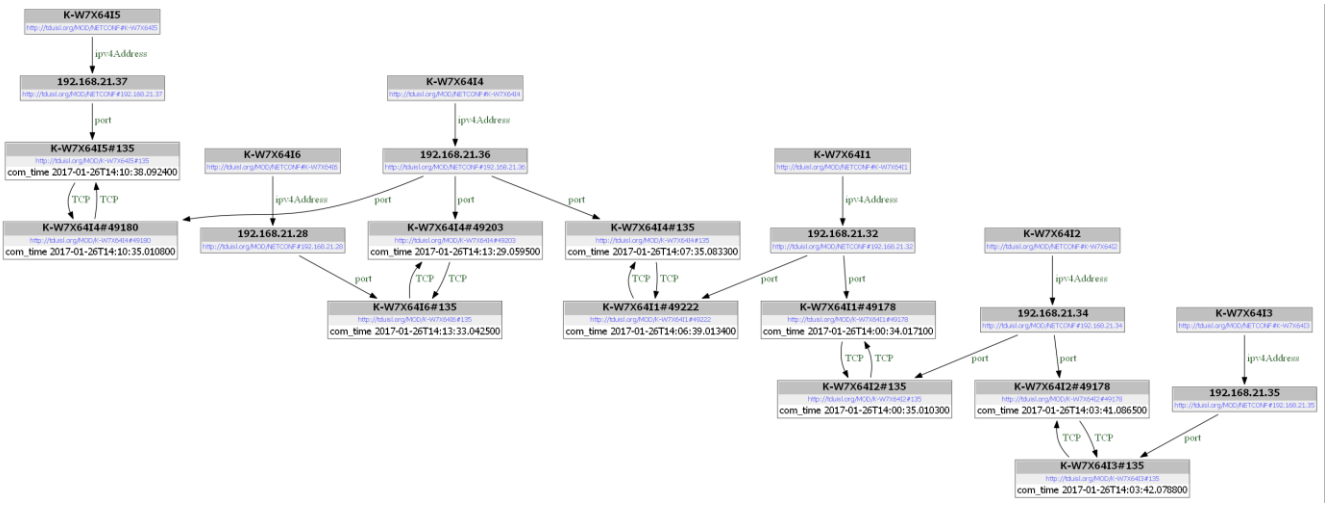

図 5　実験 1 における内部通信部分

Figure 5　Internal communication part in experiment 1.

実験 2 の結果，提案手法によりネットワーク内の端末のうち，侵害が行われた端末のみを特定することができた．また，開発したプログラムによって侵害が行われた端末を全て特定するまでの時間は約 84 秒であった．図 6 に実験 2 の結果を示す．図 6 中に示している RDF トリプルは図 4 と同様であり，RDF トリプル群から侵害が行われた端末は端末 1，端末 2，端末 4 のみであることがわかる．これは，実験 2 では PsExec の通信を受信可能と設定していた端末が端末 2，端末 4 のみであり，他の端末への侵害が行えなかったためである．

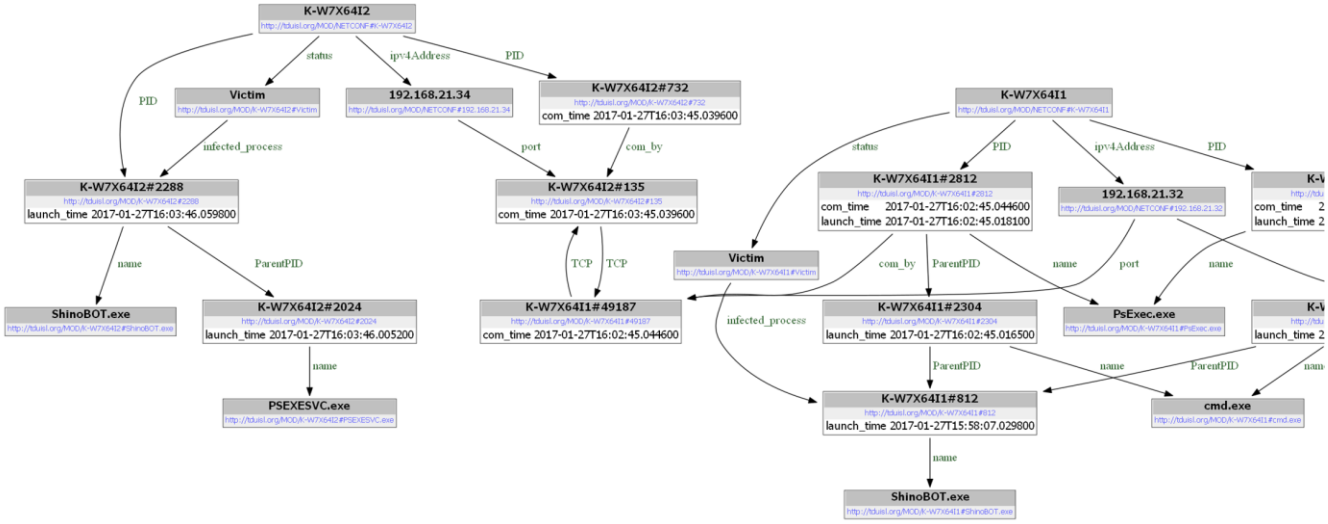

図 6-1　実験 2 の結果 1

Figure 6-1　Result 1 of experiment 2.

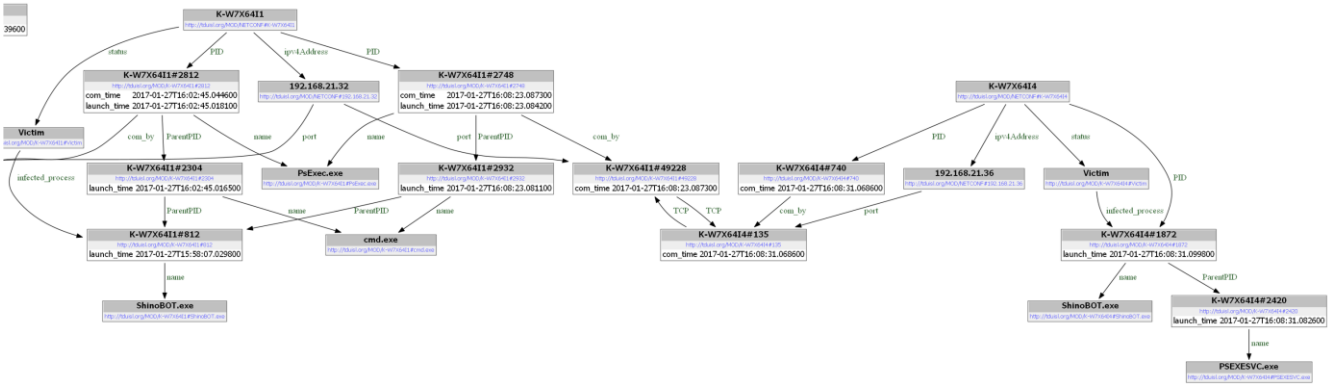

図 6-2　実験 2 の結果 2

Figure 6-2　Result 2 of experiment 2.

5.4 考察

今回の実験で提案手法により，侵害経路が分岐している場合であっても侵害が行われた端末を特定することができた．また，分岐した先の端末を調査していくことで特定済みの侵害経路上の端末と直接は内部通信を行っていない端末を特定することもできた．さらに，提案手法によりネットワーク内の端末のうち侵害された端末のみを特定することができた．そのため，提案手法により侵害範囲を特定でき，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になると考えられる．また，提案手法により特定された端末を詳細に調査することで駆除されずに潜伏していた不正プログラムの早期発見に繋がり，再侵入の防止にも貢献することができると考える．

侵害が行われた端末を特定するためには，特定の URL に対する通信が行われていないかを調査するといった外部通信を調査する手法がある．しかし，この手法では，外部への該当する通信が発生していなければ侵害範囲が拡大していても直ちに認知することはできない．これに対して，提案手法では，侵害範囲を拡大する際に行われる内部通信を調査することで侵害が行われた端末を特定していくため，外部へ該当する通信が発生していなくとも侵害範囲を特定することができる．そのため，提案手法は外部通信を調査する手法を補完することができる．

今回の実験では，攻撃の再現のために必要最小限な環境

での実験であったため，実際の企業等のネットワークと比べると小規模なネットワークであった．そのため，大規模なネットワーク環境を構築し，より実環境に近い実験環境で提案手法の有効性を評価する必要がある．また，実験中の端末内での操作は攻撃の再現のみを行ったため，攻撃の再現以外のログはそれほど多く出力されておらず，ログサイズは平均 282KB であった. 実際に業務などが行われる環境となれば膨大な量のログが出力されることが予想される. また，三村ら[5]が，エディタ操作とブラウザによるウェブサイト閲覧を行いながらログを記録した結果，ログサイズは平均 1 時間あたり 3.46MB であり，1 日 8 時間稼動させると 30MB ほどに肥大化することが予想されている．今回の実験の結果，開発したプログラムによって侵害が行われた端末を全て特定するまでの時間は約 120 秒であったが，ログの量が膨大となれば処理時間にも影響が出ると考えられるため，高速化のために効率的な探索手法を検討する必要がある.

また，現状の提案手法では，侵害経路を 1 つのクライアント端末が複数のリモート端末を持つような木構造であることを想定している．しかし，初期感染端末が複数あった場合など侵害経路が，1 つのリモート端末に対し複数のクライアント端末がある様な別の構造となる可能性もあると考えられる．そのため，侵害経路が別の構造を持つ場合であっても対応可能となるよう, 手法を検討する必要がある.

6. おわりに

本研究では，標的型攻撃における内部侵入・調査段階に焦点をあて，複数の端末のプロセスログを解析・突合することで侵害範囲を特定する手法を提案した．また，提案手法を実現するプログラムを実際に開発して実験を行うことにより，基本的有効性を確認することができた.

今後は，実環境により近い実験環境で提案手法の有効性を評価するとともに高速化のためにより効率的な探索手法を検討していく．また，現状の提案手法では侵害経路を 1 つの木構造であることを想定しているため，別の構造を持つ場合であっても対応可能となるよう，手法を検討する.

謝辞 本研究に際して，様々なご指導をいただきました LIFT プロジェクトの関係者に深謝いたします.

参考文献

[1] シマンテック :「標的型攻撃」に備える - サイバー攻撃 : 標的型攻撃とは，APT とは，シマンテック（オンライン），入手先〈https://www.symantec.com/ja/jp/theme.jsp?themeid=apt_insight〉（参照 2015-02-15）

[2] サイバーセキュリティ戦略本部：日本年機構における個人情報流出事案に関する原因究明調査結果，サイバーセキュリティ戦略本部（オンライン），入手先〈http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf〉（参照 2015-08-20）.

[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, IPA 独立法人情報処理推進機構（オンライン），入手先〈https://www.ipa.go.jp/files/000046236.pdf〉（参照 2015-02-17）.

[4] Sato, M. , Sasaki, R. , Sugimoto, A. , Hayashi, N. , and Isobe, Y, . : Proposal of a Method for Identifying the Infection Route for Targeted Attacks Based on Malware Behavior in a Network，2015 Fourth International Conference on Cyber Security，Cyber Warfare, and Digital Forensic(CyberSec)，pp.40-45（2015）.

[5] 三村聡志，佐々木良一：プロセス情報と関連づけた通信情報保全手法の提案，情報処理学会論文誌，Vol.57，No.9，pp.1944-1953（2016）.

[6] Guus Schreiber，Yves Raimond，Frank Manola，Eric Miller，Brian McBride : RDF 1.1 Primer，W3C Working Group Note（online），available from〈https://www.w3.org/TR/rdf11-primer/〉（accessed 2016-11-19）.

[7] 川口信隆，築地原護，井手口恒太，谷川嘉信，冨岡英勤：不審活動の端末間伝搬に着目した標的型攻撃検知方式，情報処理学会論文誌，Vol.57，No.3，pp.1022-1039（2016）.

[8] 海野由紀，森永正信，山田正弘，鳥居悟：標的型サイバー攻撃におけるシステム内部の諜報活動検知の提案，コンピュータセキュリティシンポジウム 2012 論文集，Vol.2012，No.3，pp.360-367（2012）.

[9] 遠峰隆史，津田侑，神薗雅紀，杉浦一徳，井上大介，中尾康二：複数ホストを横断可能なタイムライン型イベントログ閲覧システム，信学技報，Vol.113，No.502，pp.125-130（2014）.

[10] 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，JPCERT/CC（オンライン），入手先〈https://www.jpcert.or.jp/research/ir_research.html〉（参照 2016-07-01）.

[11] AT&T Research：Graphviz - Graph Visualization Software Envisioning connections，Graphviz（online），available from〈http://www.graphviz.org/〉（accessed 2016-11-19）.

[12] Shota Shinogi：ShinoBOT -the rat/bot malware simulator，ShinoBOT Can you detect an APT like me? （online），available from〈http://shinobot.com/top.php〉（accessed 2016-07-23）.

[13] Microsoft : PsExec, Windows Sysinternals（online）, available from〈https://technet.microsoft.com/ja-jp/sysinternals/pxexec.aspx〉（accessed 2016-07-23）.