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 の開発と機能拡張（その 3）
－侵入源と波及範囲の推定－

島川 貴裕[†1]　佐藤 信[†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メール攻撃が問題となっている．このような攻撃に適切に対処するため，著者らは，ログ分析と人工知能などを用いて対策をガイドするシステムである LIFT（Live and Intelligent Network Forensic Technologies）の開発並びに機能拡張を行っている．本稿では，機能拡張の 1 つとして，端末のプロセスと通信試行のログを関連付ける機能を追加し，応急対策に基づき事象が収束した後，複数の端末のそれらのデータを解析・突合することで侵入源や波及範囲を推定する方法を提案している．あわせて，プログラムを開発した上で実験により目的とする機能を達成できることを確認したので報告する．

キーワード：デジタルフォレンジック，ネットワークフォレンジック，標的型攻撃，ログ解析

Development and enhancement of intellectual network forensic system LIFT against targeted attacks (Part 3)
-Estimation of invasion source and spreading range-

Takahiro Shimakawa[†1]　Makoto Sato[†1]　Ryoichi Sasaki[†1]

Abstract: In recent years, targeted mail attacks targeting specific companies and organizations have become a problem. In order to cope with such attacks appropriately, the authors have developed and enhanced LIFT (Live and Intelligent Network Forensic Technologies) which is a system for guiding measures using log analysis and artificial intelligence. In this paper, we added a function to associate a process of a terminal with a log of a communication trial, and we propose a method to estimate invasion sources and spreading range by analyzing and matching those data of multiple terminals after convergence of events based on emergency measures. In addition, after developing the program, we confirmed that we can achieve the expected function by experiment.

Keywords: Digital forensic, Network forensic, Targeted attack, Log analysis

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]．その中でも，攻撃対象の組織にマルウェア付きのメールを送り込んでから攻撃を行う標的型メール攻撃が問題となっている．また，日本では，2011 年の衆議院事務局，三菱重工業等に対する攻撃を境に年々増加傾向にある[2]．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，標的型メール攻撃の攻撃シナリオは，以下の 6 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：偽装メールによるマルウェア感染
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

攻撃者は，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，標的組織に侵入する．その後，機密情報を窃取するために目的遂行段階を目指し気づかれないよう慎重に攻撃を進行していく．

この攻撃段階の中でも攻撃の核心部となっているのが内部侵入・調査段階であり，前段階で確保した攻撃基盤をベースに，近隣端末にマルウェア等の攻撃用ツールのコピー・リモート実行を繰り返し，次々と端末を乗っ取りながら侵害を拡大していく[3]．そのため，マルウェアに感染する端末が 1 台だけでなく組織内の複数端末に感染が拡大している恐れがあり，攻撃発覚後は被害範囲の想定が重要となる．被害範囲の想定を誤ると対応されていなかった端末から攻撃が再開され，さらに被害が拡大することも考えられる．

また，標的型攻撃の対策には，攻撃の痕跡が残っている可能性の高い各機器のログを組み合わせた分析により攻撃

†1 東京電機大学
Tokyo Denki University

を検知し，被害範囲の想定のために一端末内でおきた事象の解析だけでなく，複数端末の事象を組み合わせた解析が必要である．このように攻撃の対策も複雑化しており，適切に対処するためには高度な技術力が必要となっている．

そこで当研究室では，このような攻撃に適切に対処するために，2013 年に LIFT プロジェクトを立ち上げ，ログ分析と人工知能などを用いて対策をガイドするシステムである LIFT システムの開発並びに機能拡張を行っている．本稿では LIFT システムの機能拡張の 1 つとして，特に内部侵入・調査段階に焦点をあて，複数の端末のプロセスとその通信試行のログを解析・突合することで侵入源や波及範囲を推定する方法を提案する．これにより，応急対策により事象が収束した後，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. 先行研究・関連技術

2.1 先行研究

2.1.1 LIFT システム

LIFT システムとは，収集するべきログの管理や徴候から人工知能技術を用いて攻撃の推定，分析を行い，高い技術力を持たない組織であってもインシデント発生時に応急対応を支援することを目的としたシステムであり，当研究室で開発を進めている[4]．LIFT システムでは，まず各ネットワーク機器や端末，検知ツールから攻撃事象における徴候を収集する．収集した徴候から人工知能技術を用いて攻撃事象を推定し，推定された事象に対する有効な対策案の算出を行い，運用者へガイドラインを表示する．これにより，高い技術力を持たない組織であってもインシデント発生時に攻撃の影響を軽減するために適切な応急対策が行えるよう支援する．

また，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 1 つであり，LIFT システムにより攻撃事象を推定し，応急対策に基づき事象が収束した後に活用する．LIFT システムにより収集された各端末の後述する Onmitsu により記録したログを解析することでマルウェアの侵入源となった端末とその波及範囲を推定する． 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を支援する．

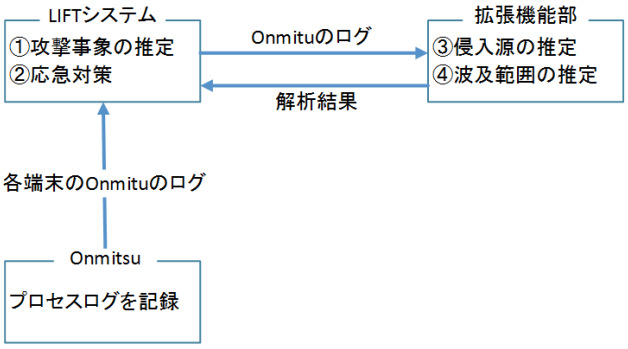

図 1　LIFT システムとの関係図

Figure 1　Relationship with LIFT system.

2.1.2 侵入源の推定

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[5]．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，マルウェア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マルウェア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，既存のマルウェア検知手法や IDS によるアラートなどを基点として，マルウェアへの感染が検知された端末のプロセスログから侵入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，感染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り，侵入源の端末を発見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いくことで経路上の端末が行った経路上以外の端末への感染を発見することで波及範囲を推定する．

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[6]．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，マルウェア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マルウェアのプロセスとマルウェア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．そのため，プロセスレベルでの攻撃挙動の把握が可能であり，感染範囲の拡大を追跡するのに有用である．

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と通信試行のログの記録に Onmitsu を用いた．

- 攻撃挙動をプロセスレベルでの把握可能
- プロセスとその通信試行を 1 つログに記録されるため複数のツールが不要
- マルウェア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[7]．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．

また，佐藤らの研究[5]によりプロセスログの情報の表現にオントロジを用いることで検知時間がプロセスログのみの場合と比べ約 1/24 となることが確認されている．

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
- プロセスログのみの場合と比べ検知時間の短縮が可能

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付けることで拡散活動を検知する手法を提案している[8]．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[9]．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[10]．この手法では，複数の端末で発生したさまざまなイ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，端末がマルウェアに感染し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，マルウェアの波及範囲の推定までに時間を要する．遠峰らの手法に対し，本研究では，感染範囲の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，迅速な波及範囲の推定を可能とする．

4. 提案手法

本章ではまず，マルウェアの波及範囲の推定までの大まかな流れについて説明する．次に，4.1 節で感染範囲の拡大の際に悪用される遠隔操作ツール・コマンドの特徴について述べ，4.2 節で提案する波及範囲の推定手法について

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開発について述べる．

マルウェアの波及範囲の推定までの大まかな流れは次の通りである．

1. マルウェア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[5]による感染経路の検知及び侵入源の端末の推定
3. 感染経路上の端末の再調査による波及範囲の推定

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波及範囲の推定が困難である．そこで，本研究では，既存のマルウェア検知手法やIDSなどによるアラートを利用し，マルウェアに感染した端末を検知した後，佐藤らの研究[5]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，迅速な波及範囲の推定を目指す．また，感染経路上の端末は侵入源の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・コマンドの特徴

JPCERT/CC の報告書[11]によると，攻撃者が感染範囲を拡大する際に悪用する遠隔操作ツール・コマンド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，JPCERR/CC の報告書[11]から悪用されることが多い代表的な遠隔操作ツール・コマンド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・コマンド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・コマンドを主な対象とした．

表 1　悪用される遠隔操作ツール・コマンドの特徴

Table 1　Features of abused remote control tool and command .

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 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，起動するプロセスと通信試行時の宛先ポート番号等が変わるだけでリモートコマンドの実行までの大まかな流れ自体は変わらない．

4.2 波及範囲推定手法

本研究で提案するマルウェアの波及範囲推定手法では，前節で述べた悪用される遠隔操作ツール・コマンド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感染範囲の拡大挙動を追跡していく．本提案手法は，佐藤らの研究[5]により推定された侵入源の端末を起点にネットワーク内の端末に対し，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. 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

4.3 プロトタイプの開発

提案手法を実現するプロトタイプの開発を行った．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 2 に示す佐藤らの研究[5]で使用されたものと同一のものを使用した．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[12]を用いて RDF により記述された波及範囲を可視化した．

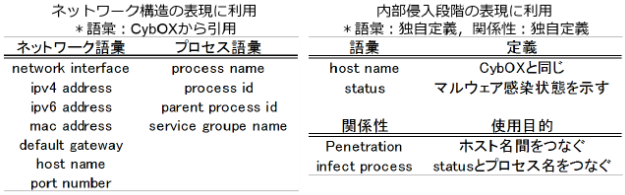

図 2　佐藤らにより定義されたオントロジの一部

Figure 2　A part of the Ontology defined by Sato et al.

5. 実験

5.1 実験概要

実験では，内部侵入・調査段階における攻撃者の感染範囲の拡大の際の行動を模擬する．その後，Onmitsu により記録していたプロセスログに対し，提案手法を適用し，その有効性を評価する．また，今回の実験では，主に佐藤らの研究[5]による遡上的な調査だけでは特定できない感染端末を特定可能であるかを確認する．

5.2 実験手順

感染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[14]を標的型攻撃に使われるマルウェアに見立て感染させ，感染端末で表 1 のツール・コマンドを用いて次の手順で感染範囲を拡大した．

1. 侵入源端末で ShinoBOT を実行
2. 他端末へ向けて内部通信を実行
3. 通信先端末でリモートコマンドの実行

実験 1 では，通信先端末へ ShinoBOT の転送と実行を繰り返し感染範囲の拡大を行っていく．また，感染経路が分岐していた場合の分岐先の感染端末群を特定可能であるかを確認するために，図 3 のように感染範囲の拡大を模擬した．そして，感染範囲の拡大を模擬した後，端末 1 から端末 3 までの一連の感染経路と侵入源である端末 1 が佐藤らの研究[5]により特定されたと仮定し，侵入源である端末 1 を起点に提案手法を適用する．

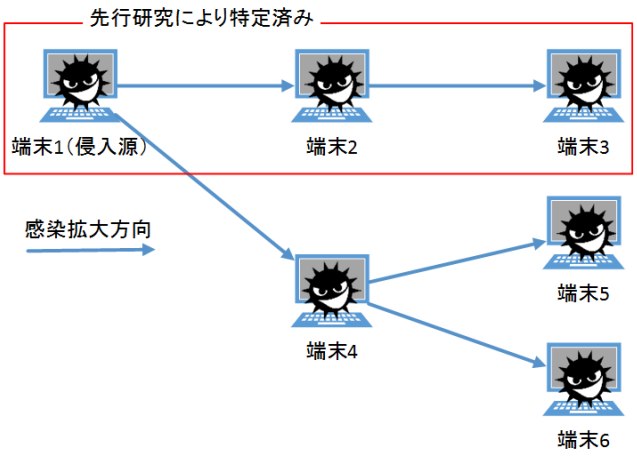

図 3　実験 1 における感染範囲の拡大

Figure 3　Expansion of infected range in experiment 1.

実験 2 では，通信先端末で ShinoBOT を実行せず転送のみを行いマルウェアが潜伏状態にある端末を用意する．これにより，通信先の端末のうちマルウェアが実行されずに潜伏状態にある端末も特定可能であるかを確認する．今回の実験では，図 4 のように感染範囲の拡大を模擬し，端末 2 では ShinoBOT を実行し，端末 3 では転送のみを行うようにした．また，IPA の報告書[3]によると，攻撃者はマルウェア等の攻撃用ツールの転送には，Windows ファイル管理共有等を利用することが分かっている．そのため，端末 1 上に共有フォルダを用意し，その中に ShinoBOT を配置した．ファイルの移動には，JPCERR/CC の報告書[11]からバックグラウンドでファイルの送受信を可能とするサービスである BITS が利用されることが分かっている．そのため，端末 3 へのリモートコマンドでは，BITS を利用するために bitsadmin を実行し端末 1 上の共有フォルダから ShinoBOT をダウンロードするようにした．そして，感染範囲の拡大を模擬した後，端末 1 から端末 2 までの一連の感染経路と侵入源である端末 1 が佐藤らの研究[5]により特定されたと仮定し，侵入源である端末 1 を起点に提案手法を適用する．

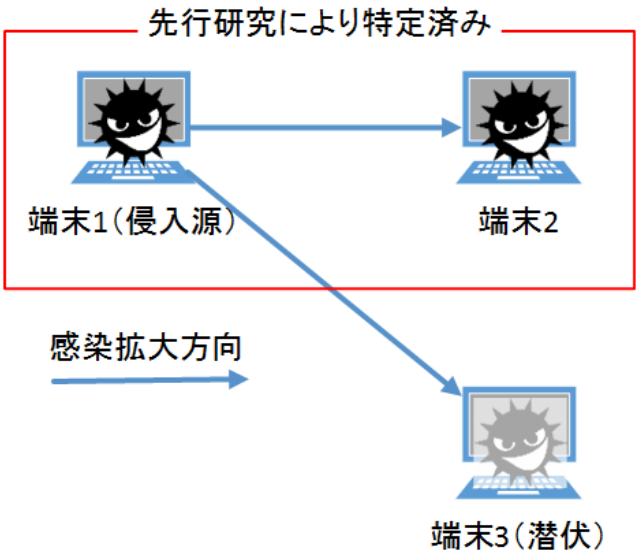

図 4　実験 2 における感染範囲の拡大

Figure 4　Expansion of infected range in experiment 2.

5.3 実験結果

実験 1 の結果，提案手法により感染端末を全て特定することができた．図 5 は，実験 1 の結果の一部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，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）

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（K-W7X64I1）で ShinoBOT.exe（PID：1184）により起動された PsExec.exe（PID：1992）により端末 4（K-W7X64I4）へ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，PSEXESVC.exe（PID：2896）により ShinoBOT.exe（PID：3316）が起動されている
- 端末 4 で ShinoBOT.exe（PID：3316）により起動された PsExec.exe（PID：3820）により端末 5（K-W7X64I5）へ通信が行われている
- 端末 4 からの通信後，端末 5 で PSEXESVC.exe（PID：3444）が起動され，PSEXESVC.exe（PID：3444）により ShinoBOT.exe（PID：4040）が起動されている
- 端末 4 で ShinoBOT.exe（PID：3316）により起動された PsExec.exe（PID：216）により端末 6（K-W7X64I6）へ通信が行われている
- 端末 4 からの通信後，端末 6 で PSEXESVC.exe（PID：3120）が起動され，PSEXESVC.exe（PID：3120）により ShinoBOT.exe（PID：3676）が起動されている

このことから，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が拡大していることがわかる．

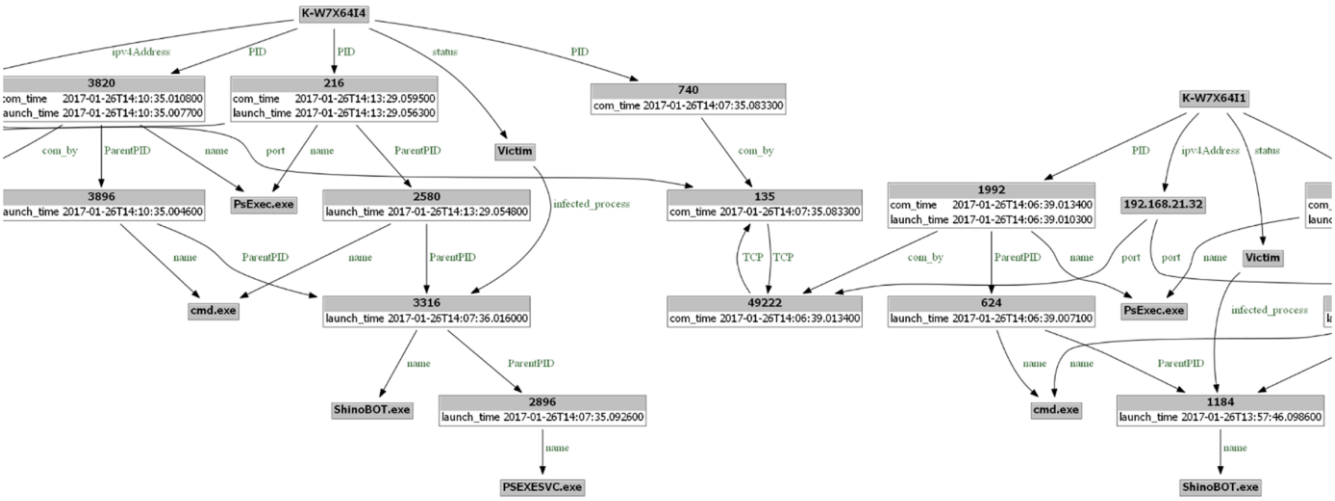

図 5-1　実験 1 の結果 1

Figure 5-1　Illustrated Result 1 of experiment1 using RDF Triple.

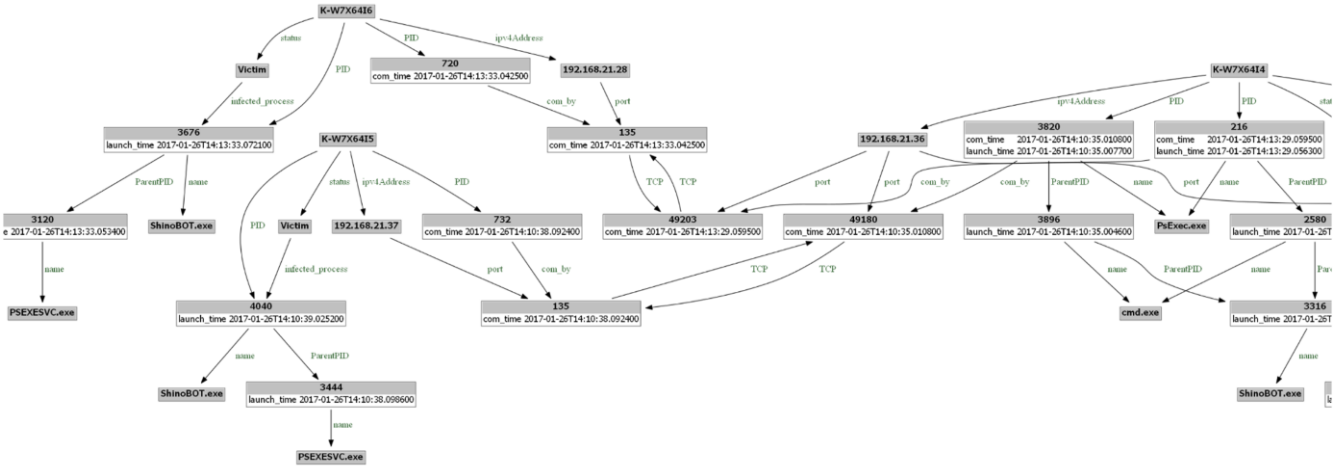

図 5-2　実験 1 の結果 2

Figure 5-2　Illustrated Result 2 of experiment1 using RDF Triple.

実験 2 の結果，提案手法によりマルウェアが潜伏状態にある端末も含めて感染端末を全て特定することができた．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 5 と同様である．図 6 中の RDF トリプル群から端末 1（K-W7X64I1）から端末 2（K-W7X64I2）へ，端末 1（K-W7X64I1）から端末 3（K-W7X64I3）へマルウェア（ShinoBOT.exe）を起因とした内部通信が行われていることがわかる．また，端末 2 では端末 1 からの内部通信後に ShinoBOT.exe が起動していることが確認できるが，端末 3 では確認できない．しかし，図 7 の端末 3 のプロセスログを確認すると端末 1 からの内部通信（①）後に PSEXESVC.exe が起動（②）し，親プロセスとなり bitsadmin.exe の起動 (③) がされ，端末 1 から ShinoBOT.exe をダウンロードしていることが確認できる．

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，マルウェアに起因した内部通信を特定することができ感染範囲の拡大を特定可能であることがわかった．

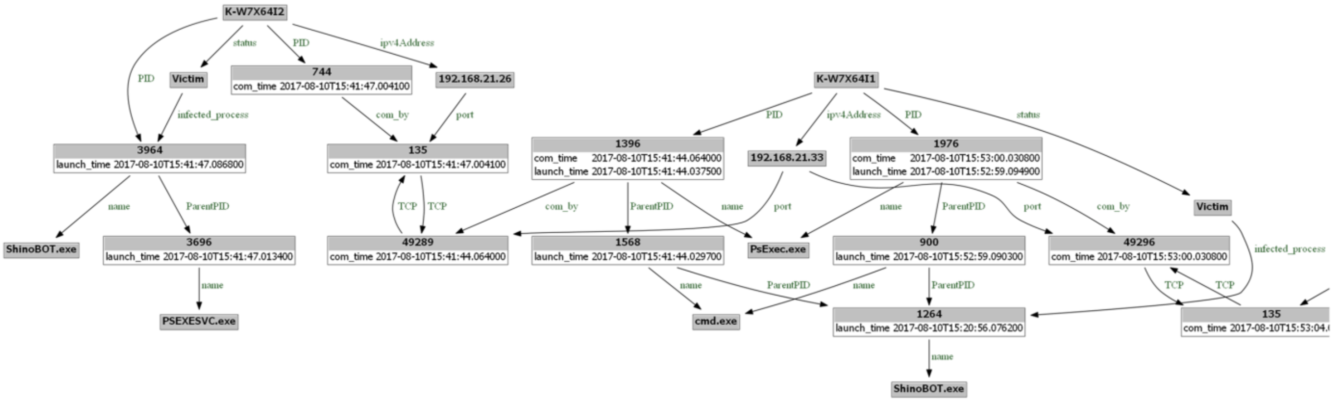

図 6-1　実験 2 の結果 1

Figure 6-1　Illustrated Result 1 of experiment2 using RDF Triple.

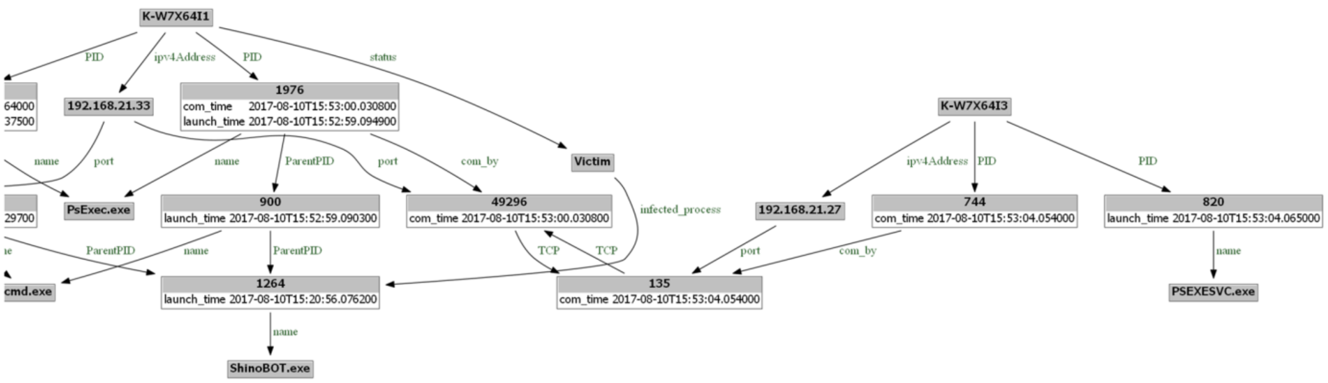

図 6-2　実験 2 の結果 2

Figure 6-2　Illustrated Result 2 of experiment2 using RDF Triple.

```
①
2017,08,10,15,53,04,0540,NETWORKV4,744,,,,192.168.21.27,135,192.1
68.21.33,49296,6
～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～
②
2017,08,10,15,53,04,0650,PROCESS_LAUNCH,820,544,¥??¥C:¥Windows
¥PSEXESVC.exe,C:Windows¥PSEXESVC.exe,,,,
～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～
③
2017,08,10,15,53,04,0837,PROCESS_LAUNCH,3188,820,¥??¥C:¥Windows
¥bitsadmin.exe,"bitsadmin.exe" /TRANSFER dl
¥¥192.168.21.33¥SHARE¥ShinoBOT.exe C:¥Users¥Yui¥AppData¥Local
¥Temp¥ShinoBOT.exe,,,,
```

図 7　端末 3 のプロセスログ

Figure 7　Process log of terminal 3.

5.4 考察

今回の実験で提案手法により，感染経路が分岐している場合であっても全ての感染端末を特定することができた．さらに，内部通信の通信先の端末でマルウェアが実行されずに潜伏状態にある端末も提案手法により特定することができた．そのため，提案手法によりマルウェアの波及範囲を推定でき，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となると考える．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マルウェア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．

感染端末を特定するためには，マルウェアの通信先の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感染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，感染範囲を拡大する際に行われる内部通信を調査するため，外部へ該当する通信が発生しなくとも感染端末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，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，約 30MB を記録したログでの提案手法を適用した結果，調査時間は 1 端末あたり約 2 秒ほどであった．しかし，端末内で実際の業務などが行われる環境となれば記録されるログの量もより膨大となると予想される．また，攻撃開始から攻撃発覚までの期間が長くなればなるほど感染端末の台数も増加する恐れがあり，調査に必要となるログも増加する．そのため，膨大な量のログから見るべき箇所の絞り込みを行い調査の高速化について検討する必要がある．特に，本研究では内部通信を調査するため，ログ内の内部通信及び内部通信に関わるプロセスとそのプロセスの親・子プロセスを抽出するようにすることで調査の際に用いるログの量を削減できると考える．

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・突合することでマルウェアの波及範囲を推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調査の高速化について検討していく．

謝辞　本研究に際して，様々なご指導いただきました 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 2015-02-12).

[2] サイバーセキュリティ戦略本部：日本年金機構における個人情報流出事案に関する原因調査結果，サイバーセキュリティ戦略本部（オンライン），入手先．〈https://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] 鈴木文仁，上原哲太郎，名和利夫，桂山こうせつ，村上弘和，堀添裕太，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 の開発と機能拡張（その 1）－LIFT の全体像－，CSS2017，（2017）．

[5] 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）．

[6] 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）．

[7] Guuns Schreiber, Yves Raimond, Frank Manola, Eric Miller, Brian McBride：RDF 1.1 Primer, W3C Working Group Note（online），available from〈https://www.w3c.org/TR/rdf11-primer/〉（accessed2016-11-19）．

[8] 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）．

[9] 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）．

[10] 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，信学技法，Vol.113，No.502，pp.125-139（2014）．

[11] 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）．

[12] AT&T Research：Graphviz– Graph Visualization Software Envisioning connections, Graphvizq（online），available from〈http://www.graphviz.org/〉（accessed2016-11-19）．

[13] Shota Shinogi：ShinoBOT –the rat/bot malware simulator, ShinoBOT Can you detect an APT like me?（online），available from〈http://shinobot.com/top.php〉（accessed2016-07-23）．