情報処理学会論文誌 Vol.58 No.2 366–374 (Feb. 2017)

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

佐藤 信[1,a)] 杉本 暁彦[2] 林 直樹[2] 磯部 義明[2] 佐々木 良一[1]

受付日 2016年5月23日, 採録日 2016年11月1日

概要：標的型攻撃は攻撃対象のネットワーク内のすべての端末に影響を及ぼしうる．攻撃検知時には，その感染原因の調査を迅速に行わないと感染が拡大していく恐れがある．そのためには，一端末内の挙動解析だけでなく各端末の挙動を組み合わせて解析する必要がある．その際には内部侵入・調査段階における攻撃挙動が重要だが，これに着目した研究は少ない．そこで，本論文では標的型攻撃の内部侵入・調査段階の攻撃挙動に焦点をあて，プロセスレベルで感染経路を検知する手法を提案する．これにより従来のような不審ファイルの移動の検知だけでは明らかにならなかったマルウェアの挙動も含めた追跡が可能となると考えられる．そのために，内部侵入・調査段階で用いられるツールのプロセスと通信試行をプロセスログ記録ツール Onmitsu で解析し，その特徴を調査する．また，各端末の挙動を組み合わせて解析するために，ログと端末間の関係をオントロジで表現し統合化した．実験により，5 次感染までの感染経路がプロセスレベルで追跡でき，オントロジを用いることで従来の場合と比べ検知時間が約 1/24 となることを確認した．

キーワード：セキュリティ，標的型メール攻撃，ログ分析，RDF

A Development and Evaluation of an Infection Route Detecting Tool for Targeted Attacks Using Malware Behaviors in the Network

Makoto Sato[1,a)] Akihiko Sugimoto[2] Naoki Hayashi[2] Yoshiaki Isobe[2] Ryoichi Sasaki[1]

Received: May 23, 2016, Accepted: November 1, 2016

Abstract: A targeted attack affects all terminals in an attacked network. When the attack was detected, it is necessarily to quickly investigate the cause of infection because the infection is likely to expand. Therefore, it is necessary to analyze the event information for each terminal in the network as well as all event information within the terminal. Moreover, it is important that observables of the attack in the penetration/exploration phase of targeted attacks, but few studies have focused on the observables. In the present paper, we propose a method for detecting the route of infection at the process level that focus on the observables. Thereby, we expected that it is possible to tracing of the infection route considering observables of a malware that did not reveal just conventional detection method of suspicious file transfer. Then, we investigate the characteristic of the attack tools used in the penetration/exploration phase by analyzing the process and a communication attempt associated with the process using the Onmitsu of the process logging tool. We integrate logs and relationships between terminals with ontology to analyze the event information for each terminal. We confirmed the ability to detect the infection route at the process level in five primary infection, and the detection time is about 1/24 compared to the conventional method.

Keywords: security, targeted attack, log analysis, RDF

1. はじめに

近年，サイバー攻撃の一種である標的型攻撃が大きな脅

[1] 東京電機大学
Tokyo Denki University, Adachi, Tokyo 120–8551, Japan
[2] 株式会社日立製作所
Hitachi Ltd., Totsuka, Yokohama 244–0817, Japan
[a)] sato_m@isl.im.dencai.ac.jp

威となっている．標的型攻撃とは，特定の組織などを標的とし，組織が持つ知的財産などに関わる機密性の高い情報の取得を目的とする攻撃である [1]．その中でも，攻撃対象組織にマルウェア付きのメールを送りこんでから攻撃を行う標的型メール攻撃が問題となっており，日本では国内の大手重工メーカや衆議院 [2]，日本年金機構 [3] などが標的型メール攻撃の被害に遭っている．IPA の報告書 [1] によると，標的型メール攻撃の典型的手法は，偽装メールとマルウェアを組み合わせて行う方法である．この攻撃の実施は，次の 6 段階で定義されている．

(1) 計画立案段階：攻撃対象を決定し情報を収集
(2) 攻撃準備段階：偽装メールや C&C サーバを用意
(3) 初期侵入段階：偽装メールによるマルウェア感染
(4) 基盤構築段階：感染端末の情報を窃取し環境を調査
(5) 内部侵入・調査段階：端末間での侵害を拡大
(6) 目的遂行段階：窃取した情報を外部へ送信

攻撃者は段階 (3) で特定のユーザに対して特定の行為をとるよう誘導することで侵入する．その後，有用な情報を窃取するために段階 (6) を目指す．

現在の標的型メール攻撃への対策は主に入口対策，内部対策と呼ばれるものである [1]．入口対策とは段階 (3) で攻撃の侵入を防止する対策である．また，内部対策とは段階 (3)〜段階 (5) で，攻撃の侵入拡大を防止する対策である．

これらの対策において異常が検出された際，その異常が標的型メール攻撃に起因する否かを判断するのは困難である．さらに，検知された端末が段階 (3) で感染した端末か，段階 (5) で感染した端末か判断する必要がある．その理由は，段階 (5) で感染した端末ならば感染元の端末が存在し，その感染元端末から感染がさらに拡大していく恐れがあるためである．したがって，感染経路を調査しその感染源を迅速に発見することは重要である．

感染経路の追跡は，従来は専門家のチームが不正プログラムや各端末のログを解析することで追跡している．そのためには高度な専門知識が必要であり，また長い時間を要するため感染源の迅速な発見が困難であった．このとき，感染端末を特定後，端末内の不正プログラムを特定し，さらにその起動原因となる通信を特定する際に，端末のどのプロセスが行った通信なのか把握できれば，各端末のログを照会する手間が減り感染経路の調査が迅速にできる．

これまで，ネットワークトラフィックなどを用いることで感染端末を特定する手法は存在している．しかし，内部侵入・調査段階に焦点をあて，その攻撃の原因となるプロセスもあわせて感染経路を追跡する手法は，著者らの調査した範囲では存在しない．

そこで，本論文では内部侵入・調査段階に焦点をあて，複数端末のプロセスログを調査することで感染経路を追跡する手法を提案する．このとき，プロセスログの記録には後述する Onmitsu というツールを用いた．そして，プロセスログから抽出した特徴を利用する感染経路検知ツールを開発した．さらに，処理時間を短縮するためのアプローチとして，プロセスログの情報を適切に抽出する手法を検討した．そこで，情報を抽出し，様々な粒度で表現することが容易であるオントロジを採用した．

本論文で使われているシステム・製品名は，各社の商標または登録商標です．

2. 関連技術

2.1 プロセスログ記録ツール：Onmitsu

これまで，三村らは標的型攻撃の原因を類推するための有用な情報源として揮発性情報に着目しその取得方法を検討してきた [4]．攻撃の原因を検知するうえで，プロセスの挙動と通信状況を記録することは重要である．これまで，それぞれのログをとるツールは存在するが，攻撃に使用されるマルウェアがプロセスを隠蔽する処理を行う可能性が高く，不正通信を行ったプロセスが判明してもそのプロセスの起動における経緯が判明せずマルウェアの特定が困難となる可能性がある．

そこで，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記録する手法を検討し，Onmitsu というツールを開発した．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している．さらに，常駐して記録し続けるためマルウェアによるプロセスの隠蔽処理も回避できる可能性が高い．これまで，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起因した通信とが結び付けられることが確認されている．

次にログの内容について説明する．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・通信試行の 4 つの挙動（ログタイプ）である．CSV 形式で記録され，その内容は以下のとおりである．

> 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

本論文では標的型攻撃におけるプロセスレベルでの感染経路追跡手法を提案する．提案手法を実現するための 1 要素として，攻撃挙動をプロセスレベルで把握するために Onmitsu を利用した．ただし，Onmitsu は導入した端末内のプロセスとそのプロセスが発した通信のみを記録するプログラムであるため，各端末が属するネットワークとプロセスログを関連付ける機能はない．そこで，端末間のネットワーク構造を後述するオントロジで表記し，Onmitsu で記録されたプロセスログとネットワーク構造を組み合わせることで，ネットワーク全体で分析することによりプロセスレベルで感染経路を追跡する手法を検討する．

2.2 オントロジ

オントロジとは知識を形式的に表現するための一手法で，あるドメイン内の語彙とその関係性で表現される．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 [5]．RDF では，リソースに関する情報を RDF トリプル（主語，述語，目的語）で表現する．RDF トリプルにおいて，主語は記述対象のリソースを，述語はリソースの特徴や主語と目的語との関係を，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．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る．RDF では語彙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つなぎ合わせて，その部分和以上の総体を作ることができる．

RDF トリプルでは語彙とその関係性を定義することで任意の粒度で情報を表現できる．そのため，各情報処理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が柔軟に表現可能である．その際，標的型メール攻撃で生じる振舞いを効率的に記述し，標的型メール攻撃に対し柔軟な診断をするためには，各攻撃段階で必要となる情報処理機器の事象情報と標的型メール攻撃の活動情報の語彙と関係性を整理する必要がある．

さらに，オントロジを用いることで，各端末で記録されたログどうしにも関係性の意味を持たせることができる．そのため，関係性を基に探索ができ，探索が容易になると期待される．この関係性の情報がなければ，すべてのログの関連を調べる必要があり非効率な処理となる．

3. 関連研究

本章ではまず，プロセスログと類似のログ情報を用いた攻撃検知手法との差異を述べる．次に，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．最後に，現在の標的型メール攻撃対策の製品・サービスとの差異を述べる．

これまで，プロセスやネットワークトラフィックなどのログ情報から攻撃を検知する手法が数多く研究されてきた [6], [7], [8], [9]．しかし，これらの研究では感染端末自体の特定は可能だが，プロセスレベルで感染経路を追跡することは検討されていない．したがって，感染端末の特定後に感染経路を追跡するには，各ログ情報を逐次突き合わせていく必要があり時間を要する．そこで，ある端末でマルウェアを特定したあとに自動的に他の端末への感染経路まで調査するような，標的型メール攻撃の攻撃段階もふまえた追跡手法が必要となる．

標的型メール攻撃での内部侵入・調査段階における検知方式として，川口らは不審活動の端末間伝搬に着目し，拡散活動を検出する手法を提案している [10]．この手法では，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．このグラフがある基準を満たすとき，標的型攻撃によ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．この研究では，アラートされる不審端末が初期感染端末か否かを診断するような追加調査を実施する手法は検討されていない．一方，本研究では不審な端末が検知された後の追加調査としてプロセスレベルの感染経路検知を行うことで標的型メール攻撃の感染源を検知する研究である．したがって，本研究は川口らの手法と組み合わせて用いる手法の研究として位置づけられる．

またこれまで，標的型攻撃対策として開発された製品の感染経路調査に関連した特徴を列挙し本研究との差異を述べる．IBM はネットワーク・セキュリティーの脅威を検出して防御する先進的ソフトウェアとして IBM Security QRadar Incident Forensics [11] がある．本研究との差異として，この製品は検知に特化しているが，本論文は上記のように異常検知後の正確な経路追跡を目的としている．したがって，川口らの手法との差異と同様に，結果を組み合わせて用いる手法の研究として位置づけられる．また，Cisco はファイルトラジェクトリ機能というネットワーク全体でファイルの送信を追跡することが可能な Cisco AMP for Network [12] がある．これにより，たとえば不審なファイルの送信履歴から攻撃者の感染拡大活動が追跡できる．著者らの研究ではさらにプロセスの振舞いを記録しているため，ファイルの移動ではなくファイルを移動させたプログラムの振舞いが分かる．そのため，不審ファイルの移動だけでなく，それを実行したマルウェアも含めた追跡ができると考えられる．

以上の内容をまとめると，本論文の新規性は次の 3 点を組み合わせることにより，プロセスレベルで標的型攻撃の感染経路を追跡する手法を検討し，そのツールを開発したことにある．

(1) 内部侵入・調査段階で頻繁に用いられるツールの挙動を解析することで内部感染の特徴を抽出
(2) Onmitsu により感染源となるプロセスも含めた感染経路の追跡が可能
(3) オントロジにより検知処理が高速かつ感染経路の視覚的な把握が容易

本論文では，(1) について 4.2 節で述べる．そして，(2) と (3) ついて 4.3 節で述べる．

4. 感染経路検知ツールの開発

4.1 標的型攻撃における内部侵入・調査段階の挙動

本節では内部侵入・調査段階の挙動を IPA [1] と FireEye [13] の報告書を基に説明する．この段階における攻撃者の目的はネットワーク内の認証情報を窃取しながら侵害範囲を拡大することである．

具体的には，次の手順で侵入を拡大する．

(1) 感染端末で管理者権限を窃取

表 1 内部通信時の特徴
Table 1 Features of the internal communication.

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	直前の通信試行時の実行プロセス	親プロセス
PsExec	psexec	135	RpcSs に属する svchost	PSEXECSVC.exe
at	at	445	Schedule に属する svchost	taskeng.exe
wmic	wmic	135	Schedule に属する svchost	wmiprvse.exe

(2) FTP サービスなどを使用して，近隣端末へ内部攻撃用ツールを転送
(3) 転送したツールをリモート実行し他端末へ侵入拡大
(4) イベントログなどの攻撃痕跡を消去

ネットワーク内の端末間で侵害を拡大する際には，基盤拡大用端末や情報収集用端末，情報送信用端末など役割を各端末にもたせている．役割を分散させることで攻撃の全容を把握しにくくさせていると考えられている．

さらに，FireEye の報告書によると，ネットワーク内の各端末が同一のローカル管理者パスワードを持っていたため，手順 (2) が容易となった事例がある．また，その際に攻撃者は転送ツールとして PsExec を使用したことが分かっている．PsExec とは Microsoft が提供しているソフトウェアである [14]．あわせて，JPCERT によると，攻撃者は Windows コマンドも多用していることが分かっている [15]．特に，at コマンドや wmic コマンドがリモート端末上でマルウェアを実行するために利用されている．

以上のことから，本論文ではまず侵入拡大時の活動に焦点を当てるため，手順 (3) までを主な対象とする．また，侵害拡大に使用するツールとして PsExec と at コマンド，wmic コマンドを用いることとした．

4.2 内部通信時の挙動解析

本論文で提案する感染経路検知手法のアプローチは内部通信とその通信を行っているプロセスの関係性を明確化することで他端末侵入の挙動を追跡することである．そこで，本節では PsExec，at コマンド，wmic コマンドの内部通信時の特徴的な挙動をプロセスログから抽出し，関係性を明確化する．このとき，抽出した特徴的な挙動の正否は，WireShark と Process Monitor のログとプロセスログを比較することで判断した．その結果得られた，内部ネットワーク通信時のクライアント端末とリモート端末のそれぞれの特徴を**表 1** に記述する．表 1 から，内部通信時には必ず特徴的なプロセス，ポート番号を用いられていることが分かる．

ここで，表 1 のうち，PsExec の特徴を説明する．PsExec を実行するクライアント端末で記録されたプロセスログのうち，プロセス起動と通信試行の一部を**図 1** に示す．図 1 はクライアント端末からリモート端末へマルウェアをコピーし実行する引数を PsExec に与えて実行している様子を示している．また，リモート端末で記録されたプロセスログのうち，プロセス起動と通信試行の一部を**図 2** に示す．図 2 はクライアント端末から通信を受け取り，コピーされたマルウェアが実行されている様子を示している．図 1 の上段と下段を比較すると，PsExec を実行すると PsExec のプロセスがリモート端末へ通信していると分かる．次に，図 2 から，通信を受け取ったリモート端末はクライアント端末と通信をした後に PSEXECSVC.exe を実行する．このときリモート端末はクライアント端末間で通信したことは図 1 の下部と図 2 の上部の IP アドレス・ポート番号を比較することで分かる．また，その際リモート端末が通信を行っているプロセスは RpcSs に属する svchost であることも分かる．その後，リモート端末では，起動された PSEXECSVC.exe が子プロセスを起動することでクライアント端末から与えられたコマンドを実行する．このような流れで PsExec はリモート端末で任意のコマンドが実行される．

```
2015,08,03,17,33,40,0664,PROCESS_LAUNCH,3084,2108,¥??¥C:¥Users¥Yui¥Downlo
ads¥PsExec.exe,"PsExec.exe  -accepteula -d ¥¥k-w7x64a -u Yui -c -f ""C:¥U
sers¥Yui¥downloads¥ShinoBOT.exe""",,,,,
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
2015,08,03,17,33,43,0927,NETWORKV6,3084,,,,fe80:0:0:0:c43c:d32:5aef:30a9,
49453,fe80:0:0:0:1405:c5b1:881:ec62,135,6
```

図 1 PsExec を実行したクライアント端末のプロセスログ
Fig. 1 Process log in the client terminal that performed PsExec.

```
2015,08,03,17,33,43,0796,NETWORKV6,732,,,,fe80:0:0:0:1405:c5b1:881:ec62,1
35,fe80:0:0:0:c43c:d32:5aef:30a9,49453,6
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
2015,08,03,17,34,04,0841,PROCESS_LAUNCH,3556,536,¥??¥C:¥Windows¥PSEXESVC.
exe,C:¥Windows¥PSEXESVC.exe,,,,,
2015,08,03,17,34,04,0981,PROCESS_LAUNCH,2504,652,¥??¥C:¥Windows¥system32¥
DllHost.exe,C:¥Windows¥system32¥DllHost.exe /Processid:{E10F6C3A-F1AE-4AD
C-AA9D-2FE65525666E},,,,,
2015,08,03,17,34,05,0059,PROCESS_LAUNCH,4092,3556,¥??¥C:¥Windows¥ShinoBOT.
exe,ShinoBOT.exe ,,,,,

-----------process information-----------
ProcessName  PID    Group
svchost.exe  732    RpcEptMapper,RpcSs
```

図 2 リモート端末のプロセスログとプロセス情報
Fig. 2 Process log and process information in the remote terminal.

以上の結果から，PsExec で内部通信を行う際には次の特徴があると分かった．
(1) クライアント端末が PsExec のプロセスを起動し，PsExec がリモート端末へ向けて通信
(2) リモート端末が PsExec による通信試行と同一の IP・

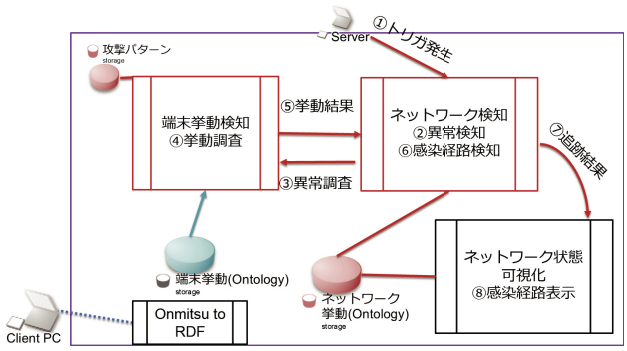

図 3 開発プログラムの概要
Fig. 3 Overview of the development system.

ポート番号を持つ通信を RpcSs に属する svchost でクライアント端末へ向けて通信
(3) リモート端末で PSEXECSVC が起動
(4) PSEXECSVC が親プロセスとなりリモートコマンドを実行

4.3 感染経路検知手法

前節で述べた特徴を用いて感染端末内のプロセス挙動も含めた感染経路を検知する手法を提案する．基本的には，端末のプロセスログに表 1 の特徴が存在するか検索する手法である．

(1) 不審な通信またはプロセスの検知
(2) 検知したプロセスの特定
(3) 親プロセスの起動とその直前の通信試行が表 1 のリモート端末の特徴を持つか調査
(4) 調査結果から通信元の端末を特定
(5) 特定した端末のプロセスログが表 1 のクライアント端末の特徴を持つか調査
(6) 調査結果から内部通信を行ったプロセスの特定
(7) そのプロセスの親プロセスを調査していくことで不審なプロセス起動を発見
(8) 手順 (2) をその端末で繰り返す

以上より，感染経路検知プログラムを開発した．開発したプログラムの概要を**図 3** に示す．機能要件は次の 2 つである．1 つめは，上記手順の自動的な処理である．そのために，開発プログラムは主にネットワーク検知処理，端末挙動検知処理，ネットワーク状態可視化処理の 3 つに分かれている．図 3 では，トリガ発生として入力される．また，手順 (3) と手順 (5) で調査する特徴は事前に攻撃パターン DB に保存する．このとき，手順 (1) は既存のマルウェア検知手法や，IDS によるアラートなどが利用できる．これが図 3 におけるトリガ発生である．2 つめは，情報処理機器間の関係と端末のログを統合することである．そのために，情報処理機器間の関係を RDF で表現した．ここで，情報処理機器間の関係などを RDF で表現するために定義した語彙と関係性の定義を**図 4** に示す．また，この情報

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 4 本手法で定義したオントロジの一部
Fig. 4 A Part of the Ontology defined by this method.

処理機器間の関係はネットワーク挙動 DB に保存する．あわせて，グラフ描画ツールである Graphviz を用いて RDF で記述された感染経路を可視化した．さらに，手順 (2)〜手順 (7) はプロセスログだけでも実現可能だが，処理時間短縮のためにプロセスログを RDF に変換し，その結果を端末挙動 DB に保存し，問い合わせる処理を追加した．なお，この問合せ処理は端末挙動検知処理で実現している．

5. 実験

この章ではシミュレーション実験について記述する．この実験では，内部侵入段階における攻撃者の行動をシミュレートする．その後，提案した感染経路検知手法を適用し，その有効性と開発したプログラムの性能を評価する．

5.1 実験環境

実験環境は VMWare ESXi 5.5 を用いて仮想ネットワーク環境を構築した．構築したシステムの構成を**図 5** に示す．最低限の組織ネットワークを作成し，ローカルネットワークと DMZ に分割した．IDS とプロキシサーバは標的型メール攻撃のトリガを発生するために設置した．ローカルネットワークには業務を行う端末として Windows 端末を 10 台設置した．この Windows 端末には 4.1 節で述べたように，これまでの事例 [13] から，各端末で同一のローカル管理パスワードを設定した．これにより 1 つの端末の管理者情報を窃取すれば，他端末へ容易に侵入できる．同様に，各端末は PsExec を利用可能な環境を構築した．

次に，標的型メール攻撃をシミュレートするために利用した攻撃ツールについて述べる．標的型メール攻撃をより現実的にシミュレートするため，初期感染に用いる RAT として ShinoBOT と Metasploit を用いた．ShinoBOT を実行すると，自動的に PC のネットワーク構成やシステム情報などが収集され ShinoBOT サーバに送信される．また，ShinoBOT サーバにアクセスすると ShinoBOT を実行した端末の情報を閲覧し，端末に対して自由にコマンドを実行させることができる．同様に，Metasploit を用いることで感染端末の権限昇格が可能であり，侵入を拡大することが可能である．今回は Metasploit を用いて RAT を埋め込んだ Word ファイルを作成した．RAT を埋め込んだ Word ファイルの作成には Word の脆弱性，特に「MS10-087」[16] を利用した．

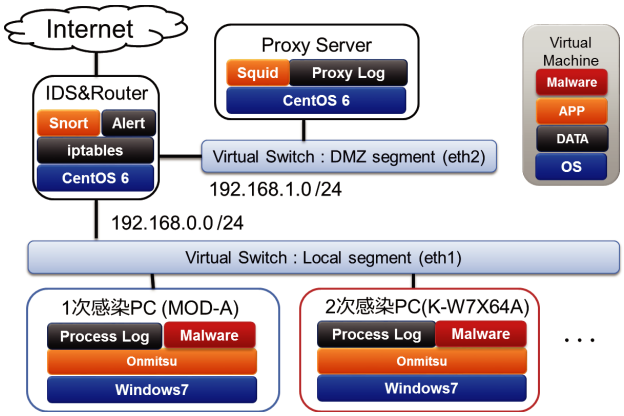

図 5 実験システムの概要
Fig. 5 Overview of the experimental system.

表 2 攻撃手法と検知手法の分類
Table 2 Classification of attack techniques and the detection method.

攻撃ツール	内部通信	検知手法
ShinoBOT	PsExec	プロセスログのみ
Metasploit	at	RDF 集約あり
	wmic	RDF 集約なし

そして，内部侵入段階でリモート端末に送信するマルウェアとして，上記と同様に ShinoBOT と Metasploit を用いた．ここで，Metasploit は「Meterpreter reverse_https」を用いてマルウェアを作成した．これをリモート端末で実行することで，攻撃者が初期感染端末と同様にリモート端末を制御可能となる．

5.2 実験手順

標的型メール攻撃をシミュレートするために次の手順で内部調査段階までの攻撃を実施した．このときシミュレートする感染経路は 5 次感染までを実験対象とした．その理由は，FireEye の報告書などで，これまでの標的型メール攻撃の事例を調査した結果，内部調査段階で 5 次感染以上に広がった事例がなかったためである．よって，今回の小規模な実験環境でも現実的な評価が可能だと考えている．また感染拡大をする際の攻撃者行動は C&C サーバを逐次介するものとした．

(1) 感染源端末でマルウェアを実行
(2) 感染源端末の管理者情報を窃取
(3) 感染先端末へ向けて内部通信を実行
　(a) 感染先端末の情報収集
　(b) 感染先端末へマルウェアを転送し，実行

上記の手順を 5 次感染まで実施する．具体的には，感染次数が増すごとに 1 台ずつ拡散し，5 次感染合計 5 台まで拡大した．さらに，使用するマルウェアや内部通信に用いるツールを**表 2** の場合に分けて記述する．

実験中，各感染 PC は Onmitsu によりプロセスログが記録される．各端末のプロセスログを RDF に変換し，提案手法を適用する．このとき，RDF を用いた手法は「RDF 集約あり」と「RDF 集約なし」で適用した．「RDF 集約あり」とは，各端末のログを集約してから提案手法を適用することで感染経路を一度に検知する手法である．「RDF 集約なし」とは，1 端末のログに提案手法を適用し，次に調査すべき端末のログを特定していくことで追跡する手法である．以上の 2 つの結果とプロセスログのみで適用した結果の計 3 パターンの処理時間を比較することで，実世界に適用可能か評価する．このとき，各実験を 3 回ずつ実行した結果の平均を処理時間とした．

表 3 感染経路検知結果
Table 3 The identify result of the route of infection.

実験ケース		経路追跡	感染源の特定
ShinoBOT	PsExec…case1	○	○
	at…case2	○	○
	wmic…case3	○	○
Metasploit	PsExec…case4	○	○
	at…case5	○	○
	wmic…case6	○	○

5.3 実験結果

各実験における感染経路検知結果を**表 3** に示す．すべての実験において，感染経路が検知できた．その中で，case1 における感染経路追跡結果の一部を**図 6** に示す．左端で囲われた RDF トリプル（MOD-A，Penetration，K-W7X64）は感染経路が検知されたことを示している．また，上部で囲われた RDF トリプル群から感染源となるプロセス（ShinoBOT）が追跡できたと分かる．

次に，各手法における平均追跡時間のグラフを**図 7** に示す．縦軸が追跡時間，横軸は追跡調査に用いた各端末を示している．各手法での平均追跡時間は CybOX では約 120 秒，RDF ログ集約ありでは約 20 秒，RDF ログ集約なしでは約 5 秒であった．図 7 から，RDF ログ集約なしの手法がより短時間で処理できたことが分かる．このとき，本実験で攻撃をシミュレートして得られたログの量は平均で約 40 MB であった．

5.4 考察

5.4.1 感染経路検知手法の検証

はじめに，感染経路検知結果について考察する．

初期感染端末での手順 (1) と手順 (3) の結果の一部を**図 8** に示す．このとき，手順 (1) の結果が①を手順 (3) の結果が②～④に対応している．図 8 の上段のコマンドラインは ShinoBOT の実行を示している．中段は ShinoBOT が PsExec を実行し（②，③），2 次感染端末へ向けて通信した（④）ことを示している．このとき，リモート端末への命令は③のコマンドラインから ShinoBOT の転送であると

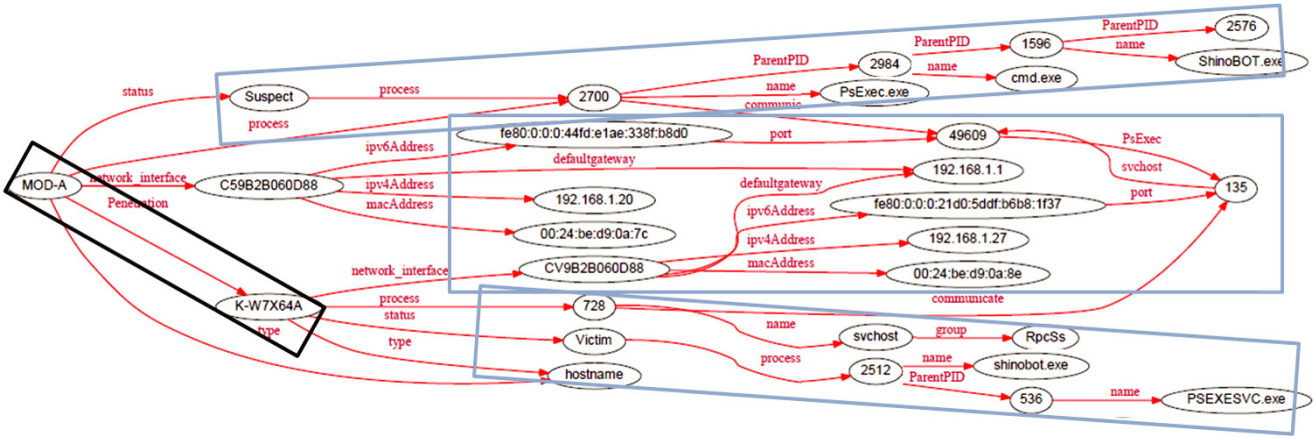

図 6 感染経路検知結果の一部（ShinoBOT）
Fig. 6 A part of the detecting result of the route of infection (ShinoBOT).

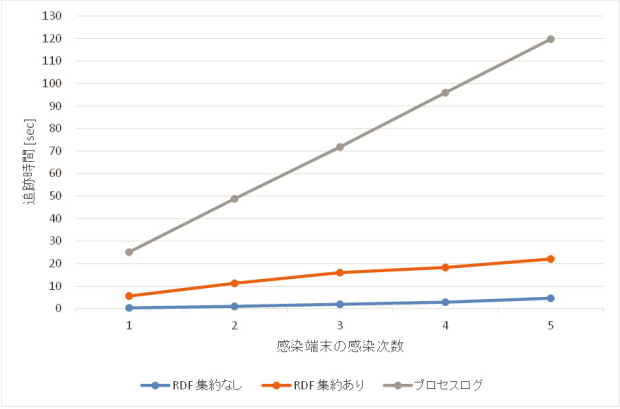

図 7 処理時間の平均 [sec]
Fig. 7 Average of Processing times [sec].

分かる．2 次感染端末での手順 (3) の結果の一部を**図 9** に示す．ShinoBOT の実行（④）とその直前の通信試行（③）を示している．なお，このとき実行された ShinoBOT が PsExec によって実行されたマルウェアである．

図 6 の下部の RDF トリプル群と図 9 の②と④を比較すると 2 次感染端末で実行されたマルウェアの親プロセスがたどれていることが分かる．図 6 の中央の RDF トリプル群と図 9 の①，図 8 の④を比較すると内部通信が適切に関連づけられていると分かる．図 6 の上部の RDF トリプル群と図 8 の①を比較すると初期感染端末で実行されたマルウェアがたどれていることが分かる．

以上の結果から，感染経路が検知でき，さらに感染源となるプロセスも追跡できたことが分かった．

5.4.2 開発プログラムの検証

作成したプログラムの性能評価について考察する．

図 7 から，感染経路検知時間はプロセスログの手法は RDF 集約ありの手法と比べて約 6 倍の時間が必要であった．また，RDF 集約なしの手法と比べると約 24 倍の時間が必要であった．これは，RDF の手法では抽出し情報に対して問い合わせるだけで感染経路が導出できる．それに

① 2015,07,22,11,40,04,0216,PROCESS_LAUNCH,1596,2576,¥??¥C:¥Users¥Yui¥Downloads¥ShinoBOT.exe,"C:¥Users¥Yui¥Downloads¥ShinoBOT.exe",,,
② 2015,07,22,12,07,34,0377,PROCESS_LAUNCH,2984,1596,¥??¥C:¥Windows¥SysWOW64¥cmd.exe,"C:¥Windows¥system32¥cmd.exe" /c C:¥Users¥Yui¥Downloads¥PsExec.exe -s ¥¥K-W7X64A -c "C:¥Users¥Yui¥Downloads¥ShinoBOT.exe",,,,,
③ 2015,07,22,12,07,34,0424,PROCESS_LAUNCH,2700,2984,¥??¥C:¥Users¥Yui¥Downloads¥PsExec.exe,C:¥Users¥Yui¥Downloads¥PsExec.exe -s ¥¥K-W7X64A -c "C:¥Users¥Yui¥Downloads¥ShinoBOT.exe",,,,,
④ 2015,07,22,12,07,34,0440,NETWORKV6,2700,,,,fe80:0:0:0:44fd:e1ae:338f:b8d0,49609,fe80:0:0:0:21d0:5ddf:b6b8:1f37,135,6

図 8 初期感染 PC のプロセスログ（ShinoBOT）
Fig. 8 Process log in the Attacked PC (ShinoBOT).

① 2015,07,22,11,56,33,0753,NETWORKV6,728,,,,fe80:0:0:0:21d0:5ddf:b6b8:1f37,135,fe80:0:0:0:44fd:e1ae:338f:b8d0,49609,6
② 2015,07,22,11,56,55,0359,PROCESS_LAUNCH,536,496,¥??¥C:¥Windows¥PSEXESVC.exe,C:¥Windows¥PSEXESVC.exe,,,,,
③ 2015,07,22,12,07,34,0477,NETWORKV6,728,,,,fe80:0:0:0:21d0:5ddf:b6b8:1f37,135,fe80:0:0:0:44fd:e1ae:338f:b8d0,49695,6
④ 2015,07,22,12,07,55,0537,PROCESS_LAUNCH,2512,536,¥??¥C:¥Windows¥ShinoBOT.exe,"ShinoBOT.exe",,,,,

図 9 2 次感染 PC のプロセスログ（ShinoBOT）
Fig. 9 Process log in the Secondarily Infected PC (ShinoBOT).

対し，プロセスログの手法では各端末のログのすべてを逐次読み込んで判断する必要がある．このように，オントロジを用いることでプロセスログの場合と比べ検知時間が約 1/24 となることが確認できた．さらに，RDF 集約ありの手法は RDF 集約なしの手法と比べると約 4 倍の時間が必要であった．これは，RDF 集約ありの場合では 10 端末の集約した情報を 1 次感染ごとに調査するのに対して，RDF 集約なしの手法では 1 次感染ごとに 1 端末の情報を調査するだけでよいため，RDF 集約なしの手法がより効率的であることが分かった．

これらの性能結果から，感染経路を検知する際には RDF 集約なしの手法がより効率的であると分かる．また図 7 の処理時間の傾きから，感染経路を検知する際，感染次数に比例した時間を要している．しかし，5.1 節でも述べたように標的型攻撃において 10 次感染以上に感染を拡大することはほとんど考えらない．仮に 10 次感染を想定した場合でも今回の実験結果から推察すれば 10 秒程で検知可能

であることが分かる．さらに，本手法では端末間のプロセスレベルでの関連を調査するため，すべての端末のログを調査するのではなく，感染端末のログのみ調査すればよい．そのため，今回の実験環境である PC10 台で連続した 5 次までの感染追跡という環境は実用性と関連が高いと考えている．そのため，この検知ツールを実世界に適用しても処理時間に大きな問題は生じないと期待される．

しかし，今後は感染源のプロセスまで遡上的な感染経路以外にも，どのような経路で拡散したのかという前進的な感染経路の追跡も検討する．この前進的な感染経路の追跡には，ネットワーク内の全端末を調査する可能性もある．このとき，RDF ログ集約なしの手法では 1 端末の調査あたり平均 1 秒程度であったが，これをネットワーク内の全端末に適用することを考えると，1,000 端末では 1,000 秒程度かかると予想され，より高速化が求められる．一方で，大規模な RDF データの問合せを高速化する研究が進められている [17]．これにより，前進的な感染経路の追跡でも RDF の手法はより短時間で検知できると期待される．

以上の結果から，内部通信の特徴を用いることでプロセスも含めた感染経路が適切に追跡可能だと分かった．これにより，標的型メール攻撃の内部侵入・調査段階で侵害範囲が拡大された際にその感染経路が追跡可能となる見通しが得られた．

6. 結論と今後の課題

本論文では複数端末のプロセスログを解析することで標的型メール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について検討した．このとき，機器間の関係をオントロジで記述した．これにより各端末のログとネットワーク構造を統合でき，感染経路が検知可能となった．実験で感染経路検知手法の有効性を検証した．実験の結果，マルウェアを検知した 5 次感染端末から初期感染端末の感染源プロセスを発見することができた．また，開発プログラムでの処理時間は RDF 集約なしの手法を用いるとたかだか 5 秒程度だった．これにより，感染経路を検知する手法に対する解決の見通しを得た．

今後は次のような課題を検討しながら標的型メール攻撃における動的かつ総合的な攻撃検知手法についての検討を進めていく．より多くの内部侵入ツールの適用を検討する．さらに，拡散経路を追跡する前進的な経路検知も検討する．このとき，遡上的な経路と異なり，調査端末が増大することが予想される．そのため，感染経路の検知時間の短縮方法の検討が必要である．本方式はすべての端末で Onmitsu によりプロセスログが記録される場合を前提とするものであるが，1 つ以上記録が抜けた端末がある場合の感染経路追跡手法も今後，重要となるので将来の課題として検討していきたい．

謝辞 本手法の基礎となったプロセスログ記録ツールである Onmitsu を開発し，本研究に助力してくれた著者等の研究室の三村聡志君に感謝します．

参考文献

[1] 独立行政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（オンライン），入手先 ⟨https://www.ipa.go.jp/security/vuln/newattack.html⟩（参照 2015-03-09）．

[2] 独立行政法人情報処理推進機構：標的型サイバー攻撃の事例分析と対策レポート 2012（オンライン），入手先 ⟨https://www.ipa.go.jp/files/000014188.pdf⟩（参照 2015-03-09）．

[3] 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究明調査結果，内閣サイバーセキュリティセンター（オンライン），入手先 ⟨http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf⟩（参照 2015-08-30）．

[4] Mimura, S. and Sasaki, R.: Method for Estimating Unjust Communication Causes Using Network Packets Associated with Process Information, *The International Conference on Information Security and Cyber Forensics* (*InfoSec2014*), pp.44–49, The Society of Digital Information and Wireless Communication (2014).

[5] Consortium, W.W.W., et al.: RDF 1.1 Primer, available from ⟨http://www.w3.org/TR/rdf11-primer/⟩ (accessed 2015-03-09).

[6] 田中功一，堀川博史，峰野博史，西垣正勝：ログ解析によるマルウェア侵入検知手法の提案，マルチメディア，分散協調とモバイルシンポジウム 2014 論文集，Vol.2014, pp.522–529 (2014).

[7] Skrzewski, M.: System Network Activity Monitoring for Malware Threats Detection, *Computer Networks*, pp.138–146 (2014).

[8] Nakazato, J., Tsuda, Y., Takagi, Y., Eto, M., Inoue, D. and Nakao, K.: A Suspicious Processes Detection Scheme using Host Based IDS, *Proc. Symposium on Cryptography and Information Security*, No.2A1-5 (2015).

[9] Slot, T.: Detection of APT Malware through External and Internal Network Traffic Correlation, Master's thesis, Univ. of Twente (2015).

[10] 川口信隆，築地原護，井手口恒太，谷川嘉伸，冨村英勤：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).

[11] Coros, S.: IBM Security QRadar Incident Forensics, IBM Corp. (online), available from ⟨http://www-03.ibm.com/software/products/ja/qradar-incident-forensics⟩ (accessed 2016-01-01).

[12] Cisco Advanced Malware Protection (AMP) for Networks, Cisco (online), available from ⟨http://www.cisco.com/c/en/us/products/security/amp-appliances/index.html⟩ (accessed 2016-01-01).

[13] Mandiant: M-Trends®2015:A VIEW FROM THE FRONT LINES, Technical Report, a FireEye Company (2015).

[14] Microsoft: Microsoft Technet Windows Sysinternals PSEXEC, Microsoft (online), available from ⟨http://technet.microsoft.com/ja-jp/sysinternals/bb897553.aspx⟩ (accessed 2015-03-09).

[15] 朝長秀誠：攻撃者が悪用する Windows コマンド (2015-12-02)，JPCERT/CC（オンライン），入手先 ⟨https://www.jpcert.or.jp/magazine/acreport-wincommand.html⟩（参照 2016-01-01）．

[16] マイクロソフトセキュリティ情報 MS10-087，Microsoft

（オンライン），入手先 ⟨https://technet.microsoft.com/ja-jp/library/security/ms10-087.aspx⟩（参照 2016-01-01）.
[17] 藤原浩司，兼岩 憲：大規模 RDF グラフのための効率的なクエリ解決，人工知能学会論文誌，Vol.29, No.4, pp.364–374 (2014).

佐藤 信 （正会員）

2013 年創価大学大学院工学部研究科修士課程修了．同年東京電機大学大学院先端科学技術研究科入学．センサネットワーク，ネットワークフォレンジック技術に関する研究に従事．

杉本 暁彦

2011 年東京大学大学院知能機械学専攻修士課程修了．同年（株）日立製作所横浜研究所（現システムイノベーションセンタ）に入所．公共システム向け国民 ID 管理技術の研究開発に従事．現在は脆弱性管理技術に関する研究開発に従事．

林 直樹 （正会員）

2007 年京都大学大学院情報学研究科数理工学専攻修士課程修了．同年（株）日立製作所システム開発研究所（現システムイノベーションセンタ）に入所．次世代ネットワーク向け認証連携技術の研究開発に従事．現在はネットワークセキュリティ技術に関する研究開発に従事．

磯部 義明

1993 年豊橋技術科学大学大学院知識情報工学専攻修士課程修了．同年（株）日立製作所システム開発研究所（現システムイノベーションセンタ）に入所．以来，医用画像処理，医用情報システム，指紋画像処理，生体認証システム，情報セキュリティの研究開発に従事．

佐々木 良一 （正会員）

1971 年 3 月東京大学卒業．同年 4 月日立製作所入社．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．2001 年 4 月より東京電機大学教授，工学博士（東京大学）．平成 14 年情報処理学会論文賞受賞．2007 年総務大臣表彰等．著書に，『IT リスクの考え方』（岩波新書，2008 年）等．日本セキュリティ・マネジメント学会前会長，内閣官房サイバーセキュリティ補佐官．本会フェロー．