一般社団法人 電子情報通信学会　信学技報
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS　IEICE Technical Report

侵入防御のためのプロセス活動リンク付方式に向けた初期的検討

都丸 裕大† 橋本 正樹† 田中 英彦†

†情報セキュリティ大学院大学 〒221-0835 神奈川県横浜市神奈川区鶴屋町２丁目１４－１

E-mail: †{mgs144501, hashimoto, tanaka}@iisec.ac.jp

あらまし 近年，標的型攻撃などの対策として C&C サーバとの通信やマルウェアをブラックリストやシグネチャとして利用し，対策をしているものが多く存在している．また，検知できないマルウェアについては，その動作をつかむために，専門家のノウハウをもとにシステム内部の証跡からマルウェアであると判断してきた．そのため，マルウェアの発見には時間がかかり，機械的に判断することが困難である．そこで本研究では攻撃を機械的に識別するために，マルウェアの悪性活動の流れを見て不正であると判断する方式を提案する．具体的には，TOMOYO Linux を用いて，マルウェアを動的解析し，ファイルの実行，C&C サーバへの通信などのアクセス情報を収集し，マルウェアによる一連の活動について絶対パスでリンク付を行う．これにより，プロセス活動による侵入防御について，機械的に判定できる部分を広げ，より高度で知的な侵入防御システムを構築する基礎となることを期待する．

キーワード 標的型攻撃，リンク付，プロセス活動，TOMOYO Linux，アクセス制御

Preliminary Studies of Linkage Analysis among Process Behavior for Intrusion Prevention

Yudai TOMARU† Masaki Hashimoto† and Hidehiko TANAKA†

†INSTITUTE of INFORMATION SECURITY 2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohama-city, Kanagawa 221-0835, JAPAN

E-mail: †{mgs144501, hashimoto, tanaka}@iisec.ac.jp

Abstract Recently, there are many malware measures such as targeted attacks, communicate with C&C servers, and file, using as black lists or signatures. Malware cannot be detected, in order to grab malware behavior, has been determined that the expert is malware from such a variety of trails within the system on the basis of the know-how, such as their knowledge. Therefore, it takes time to discover the malware, it is difficult to mechanically determine now. So, in this study, to mechanically identify cyberattacks, we propose a scheme that is determined to be unauthorized access to see the flow of malignant activity by malware. Specifically, by using TOMOYO Linux, run the malwares that execution and creation files, they collect access information such as the communication to the C&C servers and analysis linkage with the absolute path among process behavior by malware. As a result, the intrusion prevention through the process behavior, to extend the portion can be determined mechanically. It is expected to become the basis for building a more advanced and intelligent intrusion prevention system.

Keywords Targeted Attack, Process Behavior , Linkage Analysis, TOMOYO Linux, Access Control

1. はじめに

本研究は，標的型攻撃を防御するために，原田ら[1]による TOMOYO Linux プロジェクトの成果を基礎に，ホスト内部でマルウェアの活動をリンク付する手法について検討し，提案することを目的とするものである．

本稿では，第１章はじめに以降，第２章で標的型攻撃について解説し，第３章で標的型攻撃の特徴と対策について説明する．その後，第４章で本研究の関連研究や本研究の実施環境である TOMOYO Linux について，原田らによる「アプリケーションの実行状況に基づく強制アクセス制御方式」[1]に基づく提案手法について説明する．そして，第５章で提案手法について実験結果をもとに説明し，第６章で評価を行い，第７章でまとめと課題を示す．

2. 標的型攻撃

標的型攻撃とは，特定の組織において機微な業務・情報を扱う特定の組織に対し，攻撃手段として電子メールに添付した不正プログラム等によって職員の端末に侵入を図るなど，

組織的・持続的な意図をもって行われる外部からの情報窃取・破壊等の攻撃を指す[2]．なお，欧米では，「Advanced Persistent Threat (APT)」と呼ばれている．APT は，高度（Advanced）な手法を用いて，目的を達成するために執拗（Persistent）にサイバー攻撃を行う能力を有する脅威（Threat）攻撃者のことであり，標的型攻撃においても高度な攻撃を指すことが多い．また，標的型攻撃に使われるメールによるなりすましの手法が年々巧妙化，高度化している．さらに，メールに添付するマルウェアは，RAT（Remote Access Trojan, Remote Administration tools）と呼ばれ，標的に合わせてカスタマイズされており，ウイルス対策ソフトによる検知を回避するための工夫がされている．そのため，標的型攻撃をシステムの入口で完全に防御することは困難である．この標的型攻撃と呼ばれる攻撃は増加傾向にあり，脅威は高まっており，早急な対策が必要な状況である（下図１参照）．

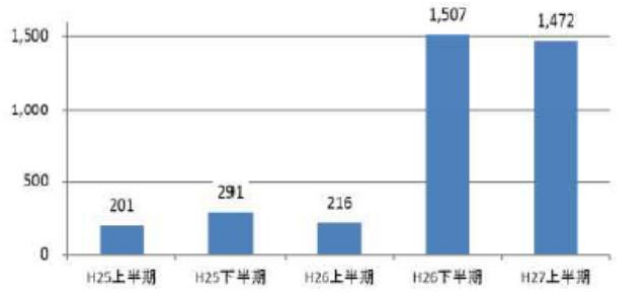

図１：警察庁が把握した標的型メール攻撃の件数[3]

3. 標的型攻撃の特徴と対策

標的型攻撃の特徴は，攻撃にステップがあり，目的達成までそのステップを踏んでいくことにある．

また，既存の対策としては，入口対策，内部対策，出口対策，多層防御，情報共有などがある．

このような標的型攻撃のステップの概要と既存の対策について下記の図２及び表１のとおりまとめた．

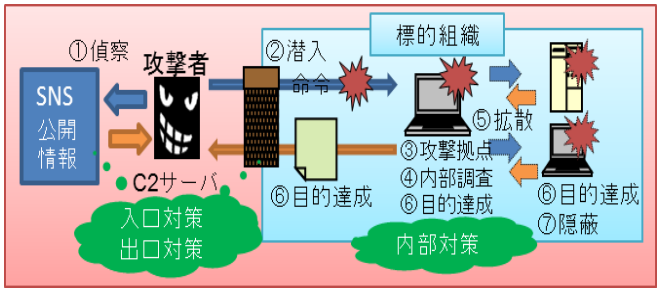

図２：標的型攻撃の概要

表１：標的型攻撃の概要及び対策

No.	ステップ	攻撃概要	対策
①	偵察・事前調査	標的に関する情報収集（システムの脆弱性の調査、名簿の入手など）	SNSの使用時についての注意喚起 公開情報の制限など（入口対策）
②	初期潜入	収集した情報からメール、USB、Webなどを通じてマルウェアに感染させ、標的PCに潜入	FW、IDS・IPS、ウィルス対策ソフト、Sandbox、USBメモリ等の使用制限、パッチ適用、教育・訓練など（入口対策）
③	攻撃拠点構築	攻撃者のC2サーバとの通信を確立し、攻撃拠点を構築	プロキシ認証、FW等のフィルタリング強化、ブラウザのオートコンプリートの禁止、ログ監視・検知、ホワイトリスト方式、PFWなど（内部対策）
④	内部調査	攻撃拠点となるPCから自ホスト情報や連接するホストの情報を収集	ログ監視・検知、SIEMなど（内部対策）
⑤	内部拡散	攻撃拠点から連接されたホストへ侵入	Windowsツールの検知、ログ監視・検知、認証強化、ファイル共有サービスの制限、リモート操作の制限、SIEMなど（内部対策）
⑥	目的達成	目的の情報のあるホストから機密情報等を窃取 システムの停止、改ざん	プロキシ認証、ログ監視・検知、暗号化、SIEMなど（出口対策）
⑦	隠蔽	攻撃の形跡の削除	ログ監視・検知、SIEMなど（内部対策）

4. 関連研究

本章では，標的型攻撃への対策として，RAT 検知手法としてホストベースの検知手法とマルウェアなどのプロセスのリンク付としてテイント解析に関連するマルウェア検出の研究，また，プロセスとプロセスの関係をリンク付するために動的解析環境として活用した TOMOYO Linux に関する研究を紹介する．

足立らの手法[4]ではネットワーク通信を始めた攻撃拠点構築段階での情報をホスト上で取得しその情報を用いて RAT の検知を行う．ホストベースの場合，ネットワークの情報だけでなくホストの情報を用いて検知することで検知する能力が向上する．ネットワークから取得できるデータ量やパケット数などだけでなく，ホストのプロセスごとの IP アドレスやポート番号などを取得できる．また，これらの特徴にプロセス ID を結びつけることにより RAT のプロセス ID を特定することができる．

幾世らの研究[5]では，動的解析時の通信先とプログラムコード及びファイルの依存関係において，既存の悪性情報との合致項目を起点とした通信先の悪性判定手法を提案している．具体的には，テイント解析技術を用いて通信先とダウンロードデータの依存関係を抽出し，抽出された依存関係において既存の悪性情報との合致項目を起点とした分析によるマルウェアダウンロードサイト特定手法である．本手法では，まず，マルウェアの動的解析中に観測された OS 上のオブジェクト（ファイルとメモリ上のプログラムコード）と通信先

間の依存関係を抽出する．その後，公開ブラックリスト等により通信先やオブジェクトの悪性判定を実施し，悪性と判定された通信先やオブジェクトを起点に依存関係を遡ることでプログラムコードの取得元をマルウェアダウンロードサイトと判定する．これにより，動的解析で得られた通信先のうち，一部が悪性と判定できれば，関連する全てのサイトを悪性と判定できる．

原田らの研究[1]は，情報セキュリティを担保するための基礎技術であるアクセス制御について，アプリケーションの実行状況を考慮可能な新しいアクセス制御方式について提案しており，そのシステムの概念と実現方法について紹介し，それを Linux 上で実装した TOMOYO Linux における評価結果を報告している．従来のアクセス制御は，主体であるアプリケーションとそれがアクセスしようとするファイルなどの客体の組み合わせによってアクセス可否を判断していた．そのためアプリケーションの処理内容及びアクセスを認めることにより情報システムに与える影響を考慮することができなかった．しかしながら，原田らの提案方式では，アプリケーションの実行状況を，システム起動時以降から当該アプリケーションの実行に至るまでの履歴と，アプリケーションのコマンドライン引数や要求発生時の環境変数等の情報から解釈し，これらの情報を条件に用いることによりアクセス可否を判定することができる．また，情報の取得／判定／強制をカーネルで行うので，安全に漏れなくアクセス制御の強制を行うことができる．

5. 提案手法

本章では，TOMOYO Linux を使い，マルウェアの動的解析を行った．その結果に基づき，メールの受信からマルウェアを実行させ，マルウェアの活動をリンク付する手法について提案する．

5.1. 概要

本提案手法は動的解析によるプロセスのリンク付の構築である．本研究では，標的型メールを侵入経路として想定し，メールの受信からマルウェアの実行までを TOMOYO Linux を用いて動的解析し，マルウェアの実行によるプロセスの生成や削除などの関係について情報収集し，メールの受信からマルウェア感染までに関係するプロセスについてリンク付を構築する．このことにより，生成先のプロセスや生成元のプロセス，アクセス先などを特定することができる．提案手法のイメージについて以下の図３に示す．

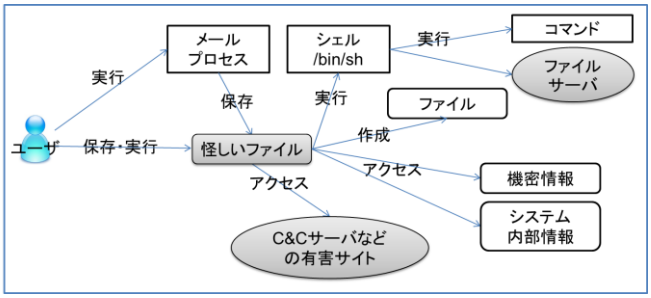

図３：プロセス活動リンク付構築イメージ

ホスト内部でファイルの実行・作成・削除などに対するリンク付を行うことで，マルウェアに関連するファイルやプロセスの特定や特定の場所からさかのぼってマルウェアを発見することができるなどのメリットがある．このようなファイルやプロセス同士のリンク付を行うことはマルウェア対策として有用である．

5.2. TOMOYO Linux によるプロセス活動の捕捉

TOMOYO Linux では，学習モードを起動させることでプログラムの実行履歴（ドメイン一覧）と各ドメインのアクセス要求の情報を収集することができる．すべてのプログラムがそれぞれ独立したドメインになり，基点となる<kernel>から現在に至るまで実行されたすべてのプログラムのパス名を結合したものを示すことができる．この環境を使い，マルウェアと考えられるファイルを実行させ，プロセスなどの動作を解析し，マルウェアによるプロセスをリンク付した活動の流れを作成することができる．

5.3. 実験概要及び実験環境

マルウェアの感染ケースを標的型メールと想定し，その動作を TOMOYO Linux 上で確認した．ユーザによるメールの受信から添付ファイルの実行まで行い，マルウェアの動作を確認した．また，本実験においては，java（ハッシュ値 MD5: 15293d54a15e7ffe3e23c5c15d895cd7）というマルウェアを使用し，TOMOYO Linux を使った環境で実験を行った．メーラには tunderbird を使用した．

5.4. 実験結果

まず，メールの受信から見てみると，TOMOYO Lunux の[domain transition]を確認すると，メーラが呼び出したプロセスを示している．[domain transition]は実行したファイルであるプロセスの実行履歴を表示することができる．

/usr/bin/thunderbird が起動され，/usr/bin/which，/usr/lib/thunderbird/thunderbird の順番でメーラを呼び出している．そして，thunderbird のプロセスの活動の中身を見るために，[domain Policy]を確認する．[domain Plicy]はそのプロセスのファイル作成，削除などアクセス情報を確認することができる．thunderbird がメールで受信したマルウェア java を絶対パス/home/tomaru/java に 0644 はパーミッションでマルウェアを保存していることが判明した．次に，マルウェア java を実行し，その動作について確認する．先ほど，メーラが保存したマルウェア java（/home/tomaru/java）が/bin/sh でシェルを呼び出し，/sbin/insmod でモジュールを読み込んでいることがわかる．そして，java の[domain policy]のアクセス情報を確認する．/etc/init.d/DbSecuritySpt，/home/tomaru/conf.n，/tmp/gates.lod を作成おり，/bin/sh を実行して，その後，作成したファイルなどを読み込んだり，書き込んだりしている．最後に，IP アドレス 61.160.212.172 にポート番号 25000（TCP）でアクセスしている．この IP アドレスを Virustotal[6]で調べると，中国のサイトであり，検出率が 3/65 で有害なサイトである可能性がある．以上の実行結果から，プロセスのリンク付を構築すると，図４及び表２のとおりとなる．

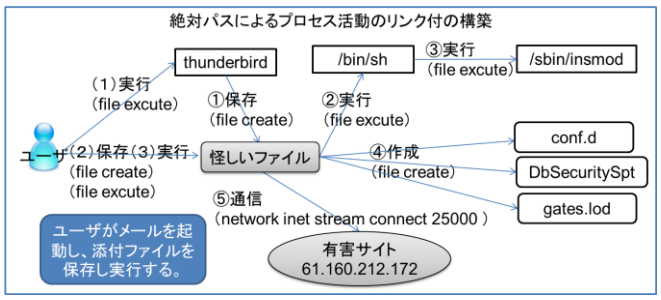

図４：プロセス活動のリンク付による一連の動作

表２：実験結果の整理

ケース	Domain Transition	Domain Policy
標的型メール	/usr/bin/thunderbird /usr/bin/which /usr/lib/thuderbird/thuderbird /home/tomaru/java /bin/sh /sbin/insmod	file create /home/tomaru/java 0664 など file create /etc/init.d/DbSecuritySpt 0755 /etc/init.d/conf.n 0644 /tmp/gates.lod 0755 fie excute /bin/sh など

5.5. 考察

TOMOYO Linux では，アプリケーションによるプロセスの実行履歴を表示することができ，そのプロセスがアクセスしたファイルの情報を収集することができる．そして，マルウェアの絶対パスによるファイル名で，メールの受信からマルウェアの実行による C&C までの通信をリンク付することができる．また，TOMOYO Linux はアクセス制御の対象としてファイル名の絶対パスを使用している．その絶対パスを活用しプロセスのリンク付を行う．絶対パスは一意なので，プロセスのリンク付を構築することができる．また，ファイルの動作として，パス名の変更（file rename），ファイルの作成（file create），パーミッションの変更（file chmod），ファイルの実行（file excute），ファイルの読み込み（file read）などがある．実行可能なファイルを実行した場合，プロセスが起動し，その動作を捕捉することができる．

5.6. TOMOYO Linux を用いたプロセス活動のリンク付の提案

TOMOYO Linux はセキュア OS であり，セキュリティポリシーを定義し，それに従い，アクセス制御することが可能である．上記の実験結果から添付ファイルでマルウェアを受信してから実行し，マルウェアの動作を制限することをセキュリティポリシーにして提案することができる．

さらに TOMOYO Linux は，強制アクセス制御方式としてファイル名の絶対パスを使っており，メールのプロセスにより，保存されたファイルを実行し，実行されたファイルの動作が重要なファイルや外部に内部情報を発信する場合に動作を止めることができる．

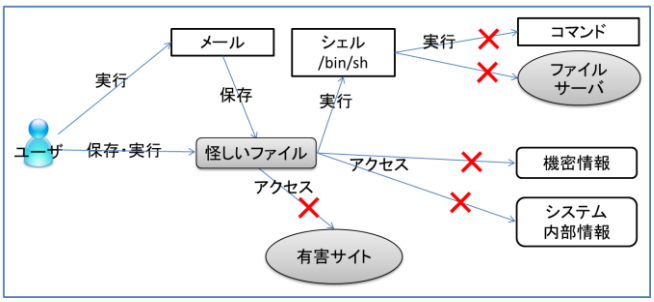

図５：ポリシー策定イメージ

上記の実験の例で説明すると，メーラにより保存された java のようなファイルを絶対パスで定義し，保存できる場所を指定し，ファイルをグレーなファイル（マルウェアであるか不明な怪しいファイル）として扱う（以下ファイルＡという）．そして，そのファイルが実行された場合，そのプロ

セスの実行履歴をドメインとして管理し，そのプロセスがアクセスする情報を制限し，重要なファイルにアクセスし，外部と通信する場合に通信をできないように定義することを提案する．具体的には，ファイルＡがシェルを起動し，内部情報を取得するコマンド，ファイルサーバへのアクセス，機密情報やシステム内部情報へのアクセス，有害サイトへのアクセスなどをセキュリティポリシーとして制御することができる．また，発信元がファイルＡとして特定できるため，マルウェアとして判断することができ，感染源の特定も可能である．マルウェアが使う可能性がある主なコマンドとアクセスするファイルやアクセス先を以下に示す．

マルウェアが使う可能性がある主な内部情報を取得するコマンドとしては，gnome-screenshot（スナップショットの取得），ifconfig（IP アドレス取得），ps（プロセスリスト取得），netstat（ネットワークの接続状況取得），sysinfo（システム情報取得），find（ファイル検索），wget（ファイルのダウンロード）などがある．アクセスファイルとしては，/etc/passwd，/etc/shadow，注意，秘，顧客，個人情報などの言葉が含まれるファイルなどがある．アクセス先としては，ファイルサーバなどの近接サーバ，近接端末，認証サーバ，DB サーバ，C&C サーバ（ブラックリスト URL）などがある．

６．評価

TOMOYO Linux は学習機能を有しているため，許可したい動作を実行することで，ホワイトリストの作成を自動化し，利便性を向上している．その学習機能をマルウェア自動解析に活用することで，マルウェアの動作を捕捉した．この学習機能でシステムを稼働させ，ファイルを実行すると，そのプロセスの実行履歴やファイルのアクセス情報，通信先などの詳細な情報を自動的に収集することができる．この機能を活用することで，マルウェアの動作の流れを捕捉することができ，マルウェアの収集する情報や感染原因の特定などに有用である．このことから Linux 系のマルウェアの自動解析を行う場合は，TOMOYO Linux の活用が有用であると言える．

また，動的解析として最近普及しているサンドボックスの仕組みと TOMOYO Linux の学習モードによる動的解析を比較した場合，TOMOYO Linux は，検体の挙動をトレースすることができるが，状態遷移情報を悪性スコアと紐づけ，判定ルールは保持していないため，人が検体の挙動を直接確認し，マルウェアかどうかを判断する必要がある．しかし，マルウェアと判断された場合その動作を禁止することを目的としてポリシーに書き込むことで，アクセス制御することができる．

７．まとめと課題

第５章において TOMOYO Linux を用いてマルウェアの動的解析を行い，マルウェアのプロセス活動を収集し，リンク付けを絶対パスで行う手法について提案した．また，提案した手法で TOMOYO Linux においてセキュリティポリシーを策定すれば，メールで受信したマルウェアの活動を紐付けることができ，アクセス制御を行うことができる．さらに，マルウェアの活動をさかのぼることで感染原因を特定することができることを示した．

今後の課題として以下の３つがあげられる．

１つ目は，実装である．本研究は TOMOYO Linux で動的解析をし，マルウェアの動作をリンク付ける考え方について提案したが，それを実際にセキュリティポリシーとして記述し，動作を検証することができていない．今後はセキュリティポリシーを策定し，期待通り動作するかの検証が必要である．

２つ目は，本研究の対象は，ホスト内部での活動のみであった．総合的な実証として，実際のシステムを想定しファイアウォール，IDS，各種サーバなど，情報システム全体としてのマルウェアの活動を制御する手法についても検討が必要である．また，マルウェアが C&C サーバにアクセスし，他のマルウェアをダウンロードし，実行する場合についても検証が必要である．

３つ目は，本研究では，メール添付型の標的型攻撃について実験を行った．そのほかにも，想定される標的型攻撃として，Web リンクをメールで送付して攻撃するものやドライブバイダウンロード，USB などの可搬記憶媒体を経由した攻撃などがあり，その攻撃に対する有用性についても検証する必要がある．ただし，TOMOYO Linux においては，プロセスの活動やファイルアクセス情報をすべて取得することができるため，ディレクトリ構造が破壊されない限り，プロセスの実行履歴やファイルのアクセス情報を取得することができるため，様々な攻撃パターンにも対応することができると考える．

文 献

[1] 原田季栄，半田哲夫，橋本正樹，田中英彦，「アプリケーションの実行状況に基づく強制アクセス制御方式」，情報処理学会論文誌，Vol.53 No.9 1-18 (2012)

[2] 岩井博樹，「標的型攻撃セキュリティガイド」，ソフトバンククリエイティブ (2013)

[3] 警察庁，「平成 27 年上半期のサイバー空間をめぐる脅威の情勢について」，http://www.npa.go.jp/kanbou/cybersecurity/H27_kami_jousei.pdf（2015.10.2 アクセス）

[4] 足立大地，面和成，「ホストベース Remote Access Trojan(RAT) の早期検知手法」，Computer Security Symposium (CSS) 2015

[5] 幾世知範，青木一史，八木毅，針生剛男，「通信先と端末内の挙動との依存関係に基づくマルウェアダウンロードサイト特定手法」，Computer Security Symposium (CSS) 2014

[6] Virustotal，https://www.virustotal.com/ja/（2016.1.16 アクセス）