# 標的型攻撃検知に向けたプロセスの親子関係の記録

高城　貴丸*，高橋　健一，川村　尚生，菅原　一孔
(鳥取大学大学院 持続性社会創生科学研究科 工学専攻　情報エレクトロニクスコース)

# Capturing Parent-Child Process Relations for Detecting Targeted Attack

Takemaru Takagi, Kenichi Takahashi, Takao Kawamura, Kazunori Sugahara
(Graduate School of Engineering, Tottori University)

## 1　はじめに

近年，企業や機関では多くの機密情報の管理や共有がコンピュータを用いて行われるようになった．それに伴い，情報を狙った標的型攻撃が増加しており情報を守るセキュリティ技術が必要不可欠となっている．しかし，ゼロデイ攻撃やファイルレスマルウェアによる攻撃の巧妙化により，すべての攻撃を防ぐことは難しくなってきている．このため攻撃を防げないことを前提としてのセキュリティ対策が必要となっている [1].

そこで，プロセスの親子関係などのプロセス情報を事前に記録しておくことで，不正マクロのようなファイルレスマルウェアの挙動を記録する．本研究では，主な感染経路である添付ファイル付きメールからの感染に着目し，メールソフトから起動されたプロセスの情報を記録，出力する．

## 2　標的型攻撃

標的型攻撃は，攻撃者が特定の組織の情報を狙って行う攻撃である．標的とした組織内の人物に対してマルウェアが添付されたメールを送り，そのメールを開くことでその組織の端末やネットワークがマルウェアに感染する．侵入したマルウェアは，レジストリの改ざん，C&C サーバとの通信，ほかのソフトウェアへの悪性コードの注入などの不審な挙動を行う．

メールに添付されるマルウェアの一種としてファイルレスマルウェアが挙げられる．emotet[2] などのファイルレスマルウェアでは Microsoft Office のマクロ，PowerShell, Windows Management Instrumentation(WMI) などを悪用し，C&C サーバから emotet 本体のファイルをダウンロードする．ダウンロードしたファイルを実行することで攻撃活動を行う．このため，添付ファイルの実行履歴だけではなく，添付ファイルによって起動されたプロセスの情報の記録が必要となる．そこで，不審な挙動を行ったプロセスの親子関係を記録，出力する手法が求められている．

## 3　関連研究

プロセスの情報を用いることでマルウェアを特定する研究はいくつか存在する．

三村ら [3][4] の研究ではカーネルレベルでログを取得するためのカーネルモードドライバを作成した．そのドライバでは，プロセスの起動，通信などのプロセス情報を取得し，csv 形式のファイルとして保存する．

中里ら [5] の研究では，プロセス情報の取得などの機能を持ったエージェントツールを作成している．ツールでは収集された情報からプロセスの実行パス，実行時間，実行回数などを用いて，ユーザが今までに使用したことのないプロセスを不審なものの候補として挙げる．不審なプロセスの API の履歴などを利用して最終的な不審プロセスの判定を行う．

## 4　プロセス情報の記録と出力

メールソフトから起動された不審な挙動を行ったプロセスの親子関係を用いて，攻撃元のプロセスの実行経路を特定する手法を提案する．そこで，プロセス情報を取得し記録するプロセス情報記録機能と，記録した情報からプロセスの親子関係を出力するプロセス情報出力機能を実現する．

プロセスの実行経路を明らかにする情報として，プロセスの親子関係，起動時間が必要となる．プロセスの親子関係を記録するために，System.Diagnostics 名前空間に存在する Process.GetProcesses メソッドを利用し，実行中のプロセスの一覧を取得する．取得したプロセスのプロパティ情報からプロセス名，プロセス id，プロセスの稼働時間を取得できる．プロセスの起動時間は，取得時の時間から稼働時間を引くことで確認できる．

しかしここで取得したプロセスのプロパティには呼び出し元である親プロセスの id は含まれていない．そこで WMI の System.Management 名前空間を利用する．その中の ManagementObjectSearcher クラスを使用することで，親プロセスのプロセス id を取得することができる．

プロセスの親子関係を出力するために，取得したプロセス情報からプロセス id と親プロセス id を読み込む．プロセス id と親プロセス id が一致するものをプロセスの親子関係を持つプロセスとして結び付ける．結び付けた親子関係から不審な挙動を行ったプロセスの実行経路を特定することができる．

## 5　実験

### 5.1　疑似不正マクロ

メールの添付ファイルがメールソフトから起動されたことをプロセス情報として記録できるか確認する実験を行った．

疑似のファイルレスマルウェアとしてマクロを含んだエクセルファイルを作成した．これは，ユーザがファイルを開いた際，自動で cmd.exe を起動し ping コマンドを用いて

通信を行う．マクロの作成には VBA を用い，exec 関数で excel.exe の子プロセスとして cmd.exe を起動する．これらの動作を図 1 に示す．

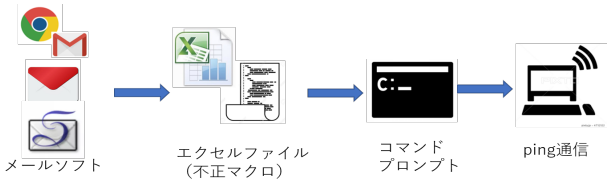


図 1　疑似不正マクロの動作

### 5.2　実験結果

エクセルファイルをメールに添付し，送信した．受信したメールを web メールサービスである Gmail で開き，ブラウザ（chrome）上で添付ファイルの起動を行った．この時に記録されたプロセス情報を表 1 に示す．

表 1　プロセス情報の記録

| log 記録時間 | name | プロセス id | 親プロセス id | 起動時間 |
|---|---|---|---|---|
| 15:36:10 | explorer | 16680 | 9852 | 11:37:57 |
| | chrome | 13992 | 16680 | 11:50:30 |
| 15:36:44 | EXCEL | 19768 | 13992 | 15:36:41 |
| | Runtime | 19316 | 548 | 15:36:41 |
| | sppsvc | 20416 | 784 | 15:36:41 |
| | EXCEL | 10832 | 19768 | 15:36:41 |
| 15:36:48 | cmd | 6016 | 19768 | 15:36:47 |
| | conhost | 1756 | 6016 | 15:36:47 |
| | PING | 9340 | 6016 | 15:36:47 |
| 15:36:53 | | | | |
| 15:36:57 | background | 6728 | 548 | 15:36:53 |
| | svchost | 20552 | 784 | 15:36:53 |
| | Runtime | 19452 | 548 | 15:36:53 |

出力された表には 12 のプロセスが表示されている．通信を行った PING プロセスの親プロセス id は 6016 であり，cmd プロセスのプロセス id が 6016 であることから，PING プロセスの親プロセスは cmd プロセスであることが確認できる．同様に，cmd プロセスは EXCEL プロセスから，EXCEL プロセスは chrome プロセスから，chrome プロセスは explorer プロセスから起動されたことがわかる．このことから通信を行った PING プロセスからメールを開いた chrome プロセスまでの実行経路を特定できる．特定できたプロセスの親子関係を図 2 にまとめる．

sylpheed や opera mail など他の電子メールソフトを用いた実験でも同様の結果が得られた．

## 6　考察

本研究では，メールソフトから起動されたプロセスの親子関係を記録することで，不審な挙動を行ったプロセスの実行経路を記録した．しかし，親子関係が記録できただけであり，プロセスがどのような挙動を行ったかや，どのような通信を行ったかはわからない．そこで，プロセス情報だけでなく，通信や API の呼び出しを記録，分析すること

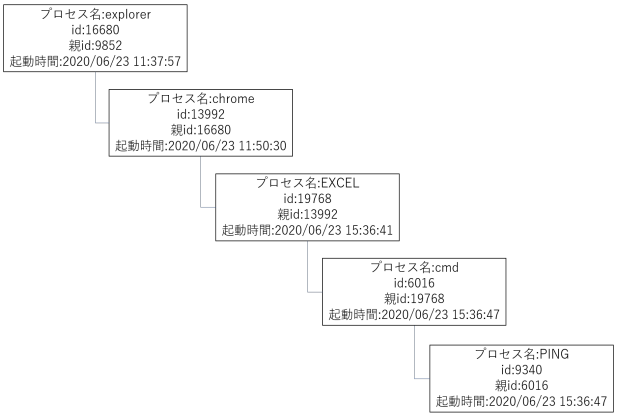


図 2　プロセス出力結果

を検討している．Wire Shark などのパケットキャプチャツールや API monitor などの API 監視ツールなどの既存のツールを用いることでこれらの情報を取得できる．これによって，マルウェア感染から攻撃までの挙動の一連の流れを記録することができると考える．

## 7　おわりに

本論文では，メールソフトから起動したプロセスの親子関係を記録することでマルウェアの実行経路を出力する手法を提案した．さらに疑似的なファイルレスマルウェアとして不正マクロを用いた実験を行った結果，疑似マルウェアの実行経路を特定できた．今後の課題として，通信や API の呼び出しを記録することが挙げられる．

## 謝辞

本研究は JSPS 科研費 20K12078 の助成を受けたものです．

## 参考文献

[1] サイバー攻撃者が複雑な連携、偽装の手口を巧妙化–アクセンチュア調査. -ZDNet Japan https://japan.zdnet.com/article/35144890/.(参照 2020-08-02)

[2] 流行マルウェア「EMOTET」の内部構造を紐解く-三井物産セキュアディレクション https://www.mbsd.jp/blog/20181225_2.html.(参照 2020-08-17)

[3] 三村聡志, 佐々木良一ほか. プロセス情報と関連づけたパケットを利用した不正通信原因推定手法の提案. マルチメディア, 分散協調とモバイルシンポジウム 2014 pp. 1973-1980, 2014.

[4] 三村聡志, 佐々木良一ほか. 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.

[5] 中里純二, 津田侑, 高木彌一郎, 衛藤将史, 井上大介, 中尾康二ほか. ホスト型 ids を用いた標的型攻撃対策. コンピュータセキュリティシンポジウム 2014 pp. 466–473, 2014.