

## 標的型攻撃対策のための体験型学習システムの開発と評価

今村 彰吾† 平川 豊‡ 大関 和夫‡

† 芝浦工業大学大学院理工学研究科 ‡ 芝浦工業大学工学部

## 1. 研究背景

近年、詐称メールを見抜く技術の必要性が高まっている。独立行政本陣情報処理推進機構（IPA）のサイバーレスキュー隊（J-CRAT）の“2015年上半期活動報告”[1]によると、標的型サイバー攻撃特別相談窓口への相談件数は2014年4月から9月の間に41件であったが、2015年には246件にまで増加している。代表的な事例としては、2015年6月初めに発覚した日本年金機構の100万件規模の個人情報漏えい事件がある。サイバーセキュリティ戦略本部による“原因調査結果書”[2]によると、原因は不正なファイルが添付された攻撃メールであったと報告されている。このような攻撃を回避するためには、添付ファイルが不正なプログラム（マルウェア）であるかを判定できる技術が重要となる。

本稿ではマルウェア判定技術を学ぶための体験型学習システムを提案し、その有効性を評価する。

## 2. 既存技術

マルウェア判定にはウイルス対策ソフトがよく使われる。ウイルス対策ソフトは、既知の攻撃コードが含まれているかを調査するパターンマッチング機能と、振る舞い検知と呼ばれる機能でマルウェアを判定する。振る舞い検知とは「定期的にスクリーンキャプチャを行い、外部へ送信する」といった特徴的なマルウェアの挙動をまとめた定義ファイルに基づいて、対象プロセスの怪しさを点数化する。分析するポイントは数百種類以上あり、「キーボード入力を記録しているか」や「スクリーンキャプチャを行えるか」といったものがある。その中でも特徴的なマルウェアの挙動が現れやすい部分がプロセス、ファイルシステムへの書き込みや通信の3つの部分である[3]。そのため、マルウェアを判定する際にはこれら3つの部分を監視することが重要である。

Development and evaluation of an experience-based learning system for targeted attacks countermeasure

†Shogo Imamura, ‡Kazuo Ohzeki, ‡Yutaka Hirakawa

†Electrical Engineering and Computer Science, Shibaura Institute of Technology, Tokyo, Japan

‡Information Science and Engineering, Shibaura Institute of Technology, Tokyo, Japan

## 3. 提案手法

提案する内容は、学習する判定手法とマルウェア判定時に用いる判定手順書の2つである。体験型学習システムは、学習者がWebブラウザから接続できるように作成している。

## 3.1 学習する判定手法

学習者は以下の3つの着眼点を監視することでマルウェアの挙動を把握し、マルウェアか否かを判定する。

着眼点

- プロセス名
- 書き込まれたファイル名やプログラム名
- 通信先のドメイン名やIPアドレス

学習者はマルウェアの種類や解析の流れなどのマルウェア判定に必要な事前知識と、以下のツール群の使い方を学ぶ。

マルウェア判定に活用するツール

1. Sandboxie
2. Process Monitor
3. RegShot
4. ApateDNS

1のSandboxieはファイルシステムを仮想化するツールである。Sandboxie上でプログラムを実行するとファイルシステムへの書き込みはすべて“C:\¥Sandbox”配下に行われるようになる。

2のProcess Monitorは、子プロセスの生成や外部への通信などのプロセスが行った処理を記録し、表示できるツールである。

3のRegShotは2つのファイルシステムの状態を比較し、ファイルシステムへの変更を確認できるツールである。

4のApateDNSは偽装したDNSリクエストを返す擬似DNSサーバーである。自分のPC上から行われたDNSリクエストを簡単に確認することができる。

実際に攻撃に使われたMicrosoft Excelファイル(malware.xls)を例に挙げて、判定手法を具体的に説明する。

プロセス部分では、Excel型のファイルを開いた際、Process Monitorには通常“EXCEL.EXE”のようなExcel型のファイルを編集するためのプロセスだけが実行されている。しかしこのマルウェアを実行した際には、cmd.exeとfracmo.exeの2つの子プロセスが生成された。

cmd.exe はコマンドプロンプトと呼ばれる、Windows の操作や設定を行う Windows 標準のツールである。コマンドプロンプトを用いると、任意のプログラムを画面に表示させずに実行することができる。また fracmo.exe は Windows 標準や Excel 関連のものではなく、心当たりのないプロセス名である。そのため、攻撃者独自のプログラムが勝手に実行されている可能性が高い。任意のプログラムを実行できる cmd.exe や心当たりのない fracmo.exe などが実行されていることから、疑わしいと判断できる。

一方、通信部分の記録を見ると、malware.xls は kunie.it というドメインへ接続を試みていた。このドメイン名を Google でキーワード検索してみると、誰が管理しているサイトであるかが判明しなかった。不明な相手との通信が勝手に行われていることから、怪しい挙動であるとわかる。

このようにマルウェアを実行した際のプロセス名、通信を試みたドメイン名や書き込まれたファイル名などを確認し、疑わしい挙動を調べ、マルウェアか否かを判定する。

### 3.2 判定手順書

判定手順書は以下の流れになっている。

1. ファイルタイプ確認
2. 記録開始
3. マルウェアを実行
4. 記録を止め、以下の記録を順に調べる
  - 4.1. プロセス
  - 4.2. 通信先
  - 4.3. ファイルシステム

マルウェア判定をする際は、判定を目的とした手順に沿うべきである。マルウェア解析の流れに沿うと、より詳しくマルウェアの機能や目的を調べることができる。しかし、マルウェア判定を目的とする場合、詳細に調べる必要はない。不明な相手との通信が勝手に行われ、マルウェアであると判断した時点で、目的は達成している。そのため、より早く効率的にマルウェア判定をするためには、解析の手順ではなく、判定を目的とした手順に沿うべきである。

### 4. 評価

学習させた判定手法と判定手順書の効果を評価する。マルウェアに触れたことがない 6 人の大学生を対象に 1 時間程の体験学習の後で、判定手順書に沿って判定を行うグループ（判定手順書あり）と被験者の自由に判定させるグループ（判定手順書なし）に分けて評価を行った。VirusTotal というセキュリティサービスへ報告されたばかりの疑わしいファイル 15 個を被験者に一つずつ判定してもらった。疑わしいフ

イルとは、VirusTotal に登録されている 54 個のウイルス対策ソフトの中で 1 つだけがマルウェアと判定したファイルである。

実験から一週間後に、Symantec や TrendMicro などの有名なウイルス対策ソフト 10 個の判定結果と被験者の判定結果を照らし合わせた。

表 1 評価結果

	判定手順書なし	判定手順書あり
判定精度	91.1%	93.3%
判定時間 (ファイル毎)	6分11秒	3分02秒
操作数 (ファイル毎)	38	20

実験で初めてマルウェアに触れた被験者が 10 個のウイルス対策ソフトと 9 割以上同じ判定をする結果となった。これより、ウイルス対策ソフトをすり抜けたマルウェアであっても、学んだ手法によって判定できるようになったと考えられる。

一つのファイルを判定するまでの判定時間は、判定手順書ありグループの方が手順書なしグループの約 50%の短い時間で判定できた。また、操作回数も判定手順書ありグループの方が判定手順書なしグループの約 52%の少ない回数で行えた。これらの結果から、判定手順書に沿う方がより早く効率的にマルウェア判定できるようになったと言える。

### 5. まとめと今後の課題

詐称メール対策であるマルウェア判定技術を学べる体験型学習システムを開発した。このシステムにより、学習者がウイルス対策ソフトをすり抜けたマルウェアであっても、短時間で判定できるようになった。

今後の課題としては、学習効率を高めるための学習コンテンツの改良やうっかり不審なファイルを開いてしまった場合の初動対応等が挙げられる。

### 参考文献

- [1] J-CRAT, “サイバーレスキュー隊活動状況”, <https://www.ipa.go.jp/files/000048385.pdf>, 2015-10
- [2] NISC, “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”, [http://www.nisc.go.jp/active/kihon/pdf/incident\\_report.pdf](http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf), 2015-08
- [3] 藤野朗稚, 森達哉. “自動化されたマルウェア動的解析システムで収集した大量 API コールログの分析”, コンピュータセキュリティシンポジウム 2013 論文集, pp618-625. 2013-04