講演番号：5

マルウェアの動的解析の可視化手法の検討

A-7　　Study of visualization method in malware dynamic analysis

長瀬　拓実†　　宮保　憲治†　　笠間　貴弘††

Takumi NAGASE†　　Noriharu MIYAHO†　　Takahiro KASAMA††

† 東京電機大学　情報環境学部　情報環境学科　　††国立研究開発法人情報通信研究機構

† School of Information Environment. Tokyo Denki University　　††National Institute of Information and Communications Technology

1.　はじめに

インターネットの急速な普及により，多種多様なマルウェアが蔓延し，その被害は年々増加傾向にある．これらマルウェアは日々，新種が検出され，対策の一手法として，解析対象の検体を解析環境（サンドボックス）内で実際に実行させ，その挙動を観測・分析する研究が進んでいる．

例えば，Cuckoo Sandbox 等の動的解析システムを利用することで，短時間で容易にマルウェアの挙動に関する情報やログをレポートで確認することができる．解析時に出力される膨大な情報量により，詳細な挙動を把握できる反面，専門的な知識や経験が欠けている場合には，解析結果を的確に判断できなかったり，重要な挙動を見逃す可能性がある．そこで本検討では，マルウェアの挙動を視覚的に分かり易くする方法を導入することで，解析結果を可視化することでマルウェアの動的解析の支援をする．

2.　提案手法

2.1 マルウェアタイプの統計表示　Cuckoo Sandbox の解析結果の中には，ファイルや web サイトのマルウェア検査を行う Virus Total によるアンチウイルスソフトの検査結果が含まれている場合がある．

```
"Kaspersky": {
  "detected": true,
  "version": "15.0.1.13",
  "result": "Virus.Win32.Nimnul.a",
```

図1　Virus Total の検査結果例

検査結果内の result 欄には，各アンチウイルスソフトが判断したマルウェアタイプ(Virus.Win32.Nimnul.a)が記述されているため，それを収集し統計を取ることにより，検査したマルウェアタイプの判別が可能であると考えた．

2.2 API カテゴリの統計表示　マルウェアが使用する API には，一定の類似性が存在する．例えば，ファイル操作では，CopyFile，CreateFile 等を使用する．本検討では，それらの判別にアナライジングマルウェア[1]に掲載されているマルウェア解析のための Win32API チート表を活用した．

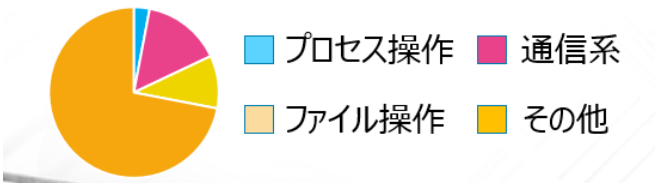

図2　マルウェアの挙動をグラフ化

図2のようにグラフで示すことで，解析中のマルウェアが，どういった系統の挙動をしているのか推測できる．また，前述したマルウェアタイプ予測と併用することで，さらなるマルウェア挙動の予測が可能であると考える．

2.3 プロセスツリーの表示　プロセスツリーは，プロセスの一覧とプロセスの親子関係を確認できる．プロセスツリーのイメージを図3に示す．

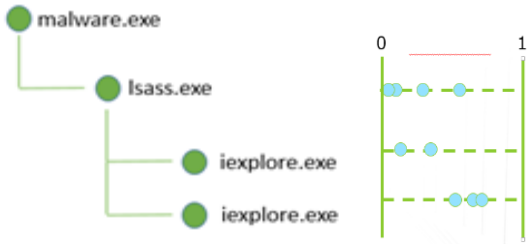

図3　プロセスツリーのイメージ図

図3は，iexplore.exe というプロセスは lsass.exe によって実行された子プロセスであることを表している．

また，Cuckoo Sandbox の解析結果には，プロセスごとのイベントが発生順にまとめられている．解析結果内のタイムスタンプを利用することで，指定時間内のイベントを棒状に点として表示することでタイムラインを表示した．点を選択するとイベントの詳細を確認できるようにすることで，どのプロセスが悪意のある挙動を行っているのか，より鮮明に明らかにできると考える．

3.　まとめ

本検討では，Cuckoo Sandbox の動的解析結果を用い，マルウェア解析をサポートする可視化手法を提案した．今後は，本検討で提案した可視化手法を実装したアプリケーションの，有効性を確認したい．

参考文献

[1]新井悠・岩村誠・川古谷裕平・青木一史・星澤裕二，『アナライジングマルウェア-フリーツールを使った感染事案対処』オライリージャパン，東京，2010 年

Copyright © 2019 IEICE