SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

# サイバー攻撃者のインテリジェンス収集のためのディープマルウェア解析
# Deep malware analysis for collecting intelligence of cyber attackers

村上　弘和 *　　西垣　正勝†
Hirokazu Murakami　　Masakatsu Nishigaki

**キーワード** サイバー攻撃，マルウェア解析，デジタルフォレンジック，インテリジェンス，プロファイリング

## あらまし

サイバー攻撃が年々拡大し、攻撃方法が巧妙化・複雑化するとともに、その被害や影響も大きくなってきた。それに伴うサイバー攻撃による被害の金額も年々大きくなってきており、経済的な影響が出てきている。また、社会インフラへの攻撃では、人々の生活にまで影響を及ぼすようになってきた。その結果、サイバー攻撃に関連する人間を調査､追跡する必要性が年々高くなっており、デジタルフォレンジックなどの調査技法が進歩してきた。

マルウェアの解析は、従来はマルウェアかどうかの判定や、特徴の発見による分類に重きが置かれてきた。しかし、マルウェアからもサイバー攻撃者よって作成、利用されているのであれば、マルウェアからサイバー攻撃者のインテリジェンスを抽出することは可能であり、このインテリジェンスはサイバー攻撃に対抗するための有用な手がかりの一つになる。そこで、サイバー攻撃者の情報を収集することを目的としてマルウェアの解析を進めた結果、４つの観点に着目して解析､分析することで、インテリジェンス情報を抽出することが可能であることを実証することができた。

本研究を行う目的として、以下が挙げられる。

- マルウェアを分析することにより、マルウェアの作成者やそれを利用した攻撃者についてより多くの情報を得て、それらの人物・組織像に迫る分析をできるようにする。
- 複数サイバー攻撃に用いられたマルウェアの分析結果を比較して類似性を判定し、それらの攻撃の中で同一のマルウェアの作成者やそれを利用した攻撃者がいた場合、それを発見することで、それらの人物、組織の繋がりを把握し、捜査や将来の行動・被害予測に利用する。
- 以上を達成するための分析手法を提案、試行し、有用性や問題点をあぶりだし、将来的に有効な分析手法を確立する。

これらの目的を達成するために、研究の目標を以下のものとする。

- マルウェアで使われている技法やプログラミングの実装方法の特徴を分析し、それらを総合的に判定することにより、マルウェア作成者または作成した組織に関する技術的な面からのプロファイルを作成できるようにする。
- 複数のマルウェアに対し同様の分析を行い、類似性を判定することにより、同じ作成者・組織かどうかを判定する「マルウェア作成者の筆跡鑑定」を行えるようにする。
- マルウェアの分析によりその能力を正しく把握することにより、マルウェアを使用した攻撃者の「攻撃の意図」を掴めるようにする。

## 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」, オライリー・ジャパン, 2013 年

[2] Itay Cohen, Eyal Itkin, “Graphology of an Exploit – Hunting for exploits by looking for the author’s fingerprints”, https://research.checkpoint.com/2020/graphology-of-an-exploit-volodya/, 2020 年

* 株式会社 CyCraft Japan, 〒100-0004 東京都千代田区大手町 1-9-2 大手町フィナンシャルシティ グランキューブ 3 階, CyCraft Japan, Financial City Grand Cube 3F 1-9-2 Ohtemachi Chiyoda Tokyo, 100-0004, Japan
†静岡大学創造科学技術大学院, 〒432-8011 静岡県浜松市中区城北 3-5-1, Graduate School of Science and Technology, Shizuoka University, 3-5-1 Johoku, Naka, Hamamatsu, 432-8011, Japan