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

# 引数情報を用いたAPIコール列に基づくマルウェアのファミリ分類手法

# Malware Family Classification Method Based on API Call Sequences That Considering Argument Information

廣瀬 優希 * 花田 真樹 * 面 和成 † 折田 彰 ‡ 関谷 信吾 ‡
Yuuki Hirose Masaki Hanada Kazumasa Omote Akira Orita Shingo Sekiya
村上 洋一 * 早稲田 篤志 * 布広 永示 *
Yoichi Murakami Atsushi Waseda Eiji Nunohiro

**キーワード** マルウェア分類，動的解析，機械学習

## あらまし

近年，インターネットの普及に伴いマルウェアは増加の一途を辿っている．アンチウイルスソフトで用いられているパターンマッチング法は，マルウェアの特徴的なコードを定義したファイルをデータベースに蓄積し，検査対象のファイルと比較することで検知を行うため，既存のマルウェアに対しての検知は行えるが，定義ファイルが存在しない未知や亜種のマルウェアに対しての検知は困難である．そのため，検知回避などを目的とした亜種のマルウェアが自動作成ツールによって大量に作られている．膨大な数のマルウェアを解析するには多くの時間を要するため，マルウェアの亜種を短時間で正確に分類することができれば，その後の詳細な解析の手助けとなる．

マルウェア解析のために従来から用いられている手法には大きく分けて表層解析と静的解析，動的解析の3つが挙げられる．表層解析は，他の解析手法に比べ容易に行うことが可能だが，限られた情報しか得ることができない．静的解析は，マルウェアを実行せずに詳細な挙動について調査することが可能であるが，解析には専門的な知識や時間を必要とする．さらに，多くのマルウェアには難読化や暗号化といった解析を妨害するための処理が施されているため解析はより困難となる．動的解析は，静的解析より短い時間で解析が可能であり，マルウェアを動作させることから難読化や暗号化などの影響を受けずに解析を行うことができる．

このような背景のもと，動的解析によって得られる時系列順序のAPIコール列を用いたマルウェアのファミリ分類手法が多く提案されている．既に筆者らも，API間の依存関係を正確に捉えるために，APIのカテゴリ情報を用いたマルウェアのファミリ分類手法を提案している [1]．本研究では，更なるファミリ分類の精度向上を目指し，APIの引数情報を利用したマルウェアのファミリ分類手法を提案する．動的解析結果から得られる引数の重要度を考慮したN-gramのAPIコール列を特徴量として抽出し，マルウェアのファミリ分類の精度に関する評価実験を行い，本提案手法の有効性を示す．

## 参考文献

[1] 廣瀬優希，花田真樹，面和成，村上洋一，折田彰，関口竜也，布広永示, “APIのカテゴリ情報を用いたマルウェアのファミリ分類手法,” 2021年暗号と情報セキュリティシンポジウム，1C1-2 (2021).

* 東京情報大学
Tokyo University of Information Sciences
4-1 Onaridai, Wakaba-ku, Chiba-shi, Chiba 265-8501, Japan.
† 筑波大学
University of Tsukuba
1-1-1 Tennodai, Tsukuba-shi, Ibaraki 305-8572, Japan.
‡ 株式会社日立システムズ
Hitachi Systems, Ltd.
1-2-1 Osaki, Shinagawa-ku, Tokyo 141-8672, Japan.