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



# 対話的に通信制御が可能なマルウェア解析システム
# SWAN: Sandbox with traffic Whitelisting for ANalyzing malware

濱島 圭佑 * 小谷 大祐 * 岡部 寿男 *
Keisuke HAMAJIMA Daisuke KOTANI Yasuo OKABE

**キーワード** マルウェア解析, サンドボックス, C2 サーバ

## あらまし

マルウェアを解析する手法の一つに，サンドボックス上で実行してその動作を分析する動的解析というものがある．サンドボックスとはあらかじめ用意された隔離実行環境のことで，その環境上でマルウェアを実行することによって外部のシステムに影響を与えることなく動作を確認することができる．

しかし，サンドボックス上での解析において，そのインターネットへの接続方法には課題がある．マルウェアの中には外部から別のマルウェアをダウンロードするものや，C2 サーバ (Command and Control Server) というマルウェアに感染したシステムに対して命令を出して制御しようとするサーバとやり取りするようなものが存在しており，そのようなマルウェアの解析を完全に行うためにはインターネットへの接続が不可欠である．一方，マルウェアを解析するためにインターネットへ接続した結果，外部へ感染を広げてしまうようなことは避けなければならない．よってサンドボックス上でより安全にマルウェアを解析するためには，必要な通信のみを外部へ通し，感染を広げるような通信は遮断する必要がある．

そこで，本研究では外部へ接続する通信を制御しながらサンドボックス上で動的解析を行う仕組みとして，SWAN(Sandbox with traffic Whitelisting for ANalyzing malware) システムを提案する．従来の研究では，ポリシーベースで通信を制御する方法 [1] や C2 通信のみを通すようなシステム [2]，ダウンローダを検知してマルウェアのダウンロードを別で行うシステム [3] などが提案されているが，マルウェアの通信は多種多様で，その解析にはより柔軟な通信制御方法が必要であると考えられる．また，近年 C2 サーバとの通信に TLS を用いるものも増えてきている[1]ので，平文のリクエストを読み解いて通信を制御していく従来の手法を適用するのが難しい．提案手法では，サンドボックス上の通信を全てインターネットシミュレータへリダイレクトする状態で解析を開始して，マルウェアが送信するリクエストを復号，確認し，無害であると推定されるものについて外部への通信を順番に許可しながら対話的にマルウェア解析を繰り返し実行することで，安全に外部への接続を試みる．

以上のような解析が可能になるようなシステムを設計して，そのアーキテクチャについて述べる．また，実際に SWAN システムを実装した後，いくつかのマルウェアに対して解析を行なって評価，考察を行った．その結果，提案手法がマルウェアの解析においてある程度有効であることを確認し，いくつかのマルウェアを想定して更なる改良が必要であることがわかった．

## 参考文献

[1] Yoshioka, K., & Matsumoto, T., “Multi-Pass Malware Sandbox Analysis with Controlled Internet Connection,” IEICE Trans. Fundamentals，Vol. 93, No. 1, pp. 210–218, 2010.

[2] Kreibich, C., Weaver, N., Kanich, C., Cui, W., & Paxson, V., “GQ: practical containment for measuring modern malware systems,” ACM IMC 2011, pp. 397–412, 2011.

[3] Shigemoto, T., Tokuyama, K., Shimotsuma, N., Hayashi, N., Kito, T., & Nakakoji, H., “マルウェア解析向け通信制御システムの開発,” IPSJ SIG Technical Report，Vol. 2015-IOT-29(3), 1-6, 2015.

* 京都大学, 〒 606-8501 京都府京都市左京区吉田本町, Kyoto University, Yoshida-honmachi, Sakyo-ku, Kyoto 606-8501 JAPAN

[1] https://www.zscaler.com/blogs/security-research/ssltls-based-malware-attacks