論 文 内 容 の 要 旨

博士論文題目　Towards Automated Malware Analysis for Understanding Characteristics in Malicious Capability Using Dynamic Analysis

氏　名　与那嶺 俊

（論文内容の要旨）

In this dissertation, we develop countermeasures against malware through automated malware analysis that extract information about the malware's capability. This research focuses on methods that can automatically characterize the malware behavior and be generalized to analyze malware that can target various internet-connected devices like IoT. Against the threat landscape brought by the innovation and sophistication of malware, this research aims to provide perspectives to keep adapting functionalities for analyzing malware that can target various devices like IoT.

First, we propose an analysis method that automatically identifies the kind of malicious capability that the malware can perform. In order to identify a specific malicious capability in malicious activity, we consider system calls executed by malware to perform data input from file/socket as malicious actions that may initiate malicious behavior. Our proposal leverages data flow tracking using taint analysis and virtual machine introspection in order to analyze malicious activity executed in the system in detail. The experimental evaluation has shown the feasibility of our proposal to identify various kinds of malicious capabilities from malware's activity in an automated manner. Furthermore, we have shown an advantage of our proposal that may work effectively for analyzing malware that uses multiple malware processes for evading dynamic analysis. Thus, this work also may provide a perspective that complements the traditional malware analysis method.

Second, we proposed a sandbox dedicated to extracting characteristics of the malicious behavior for analyzing IoT malware. Our proposed sandbox supports execution environments for binaries specific to architectures for IoT and aims to provide functionality for automating dynamic malware analysis for IoT malware. This work demonstrates the feasibility of our proposal that can perform dynamic malware analysis automatically against a number of malware samples in a dataset. Furthermore, this work combines methods for advanced dynamic malware analysis and verifies the benefits that can be brought by these efforts. The evaluation based on data analysis approaches has demonstrated an advantage that this approach may provide insights for under- standing the malicious behavior of IoT malware in detail.

氏　名	与那嶺 俊

（論文審査結果の要旨）

本研究はサイバーセキュリティの課題であるマルウェア対策におけるマルウェアの動的解析を通して有用な情報の抽出を自動化する方法に取り組んでいる。従来のマルウェア対策研究の多くは対象の検体が悪性であるかどうかに焦点を当てたものが多く、マルウェアの振る舞いについて詳細な理解を得るための解析技術については未だ十分に検討されていない。また、現代のマルウェアはPCやサーバーに限らずIoTや組み込み機器を標的としており、マルウェアの振る舞いも高機能化し検体の種類も多様化している。そこで本研究はマルウェアの悪意ある振る舞いの詳細な理解に繋げるための情報の抽出を目的とした解析を自動化するための方法を提案している。本論文の主な成果は次の通り。

まず初めに、動的解析を用いてマルウェアが感染端末上で実行した悪意ある機能の特定を自動化する方法を提案している。この手法では、マルウェアが行う不正活動の起点に使用される動作の呼び出しに着目し、悪意ある機能に関係する動作や痕跡をデータフロー追跡を用いて抽出した情報に基づき、機能の識別を行う。評価実験において、様々な機能を持った検体に対して提案手法を適用し、振る舞いの識別を自動的に行えることを示した。また、提案手法が複数の悪性プロセスを用いた解析妨害手法に対しても対処できるということを同等の機能を備えた擬似検体の解析を通して実証した。複数の悪性プロセスを用いた解析妨害手法については、従来の手法では考慮されていなかったことから、従来のマルウェア解析手法を補完できることを示した。

次の成果として、IoTマルウェアの解析に特化した解析環境を提案した。提案手法はIoTマルウェアの実行環境と動的解析を安全に実施するための隔離環境として設計されており、自動解析のための仕組みとマルウェアの振る舞いを引き出すための機能を備えている。実験的評価では大量のIoTマルウェア検体に対して提案手法が自動解析を効率的に行えることを示し、また発展的なバイナリ解析技法がマルウェア解析において有効に働くケースについても検討している。また、マルウェアの振る舞いを引き出すための仕組みを解析環境に導入することでIoTマルウェアの振る舞いについてより多くの情報を取り出すことができ、得られた特徴が分類においても寄与する点で提案手法の利点を示した。

以上のことから、本研究はマルウェアの挙動の解析手法と解析環境の提案という点から、大規模化し、多様化するマルウェアの脅威への対策技術の発展に寄与するものである。よって本論文は、博士（工学）の学位論文としての価値があるものと認める。