博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目　：　未知マルウェア対策技術に関する研究
申請者　：　田中　恭之
審査委員会　：　主査　後藤 厚宏（教授）
副査　大久保　隆夫（教授）
副査　大塚　玲（教授）
副査　橋本　正樹（准教授）

Ⅰ．論文内容の要旨

近年，マルウェアは増加の一途をたどり，アンチウイルスソフトの検出を逃れる未知マルウェアも多く出現し大きな社会問題となっている．本研究では，直接的，準直接的，間接的の 3 つの異なるアプローチから未知マルウェア対策手法を提案・検証し，未知マルウェア感染を軽量な手法で未然に検出できる対策技術によって，実社会に貢献することを目指したものである．

本論文は，「未知マルウェア対策技術に関する研究」と題し，5 章と付録からなる．

第 1 章の「序論」では，本研究の背景として，マルウェアの爆発的な増加を受けたアンチウイルスソフトの検出の限界，標的型攻撃で用いられるようなゼロデイ脆弱性を含むようなマルウェアの存在，マルウェアが配布されるインターネット上の悪性サイトの多様化の問題を挙げている．次に，従来からのマルウェア対策技術分野を，マルウェア自体を検出する技術と，マルウェアの感染のプロセスの中で生じる通信を検出する対策技術に分類し，本研究で取り組んだ 3 つのアプローチの位置付けを明確にしている．

第 2 章では，マルウェアを内蔵するファイルの静的な特徴について，統計的手法を用いて直接的にマルウェア判定を行う手法を提案し，その有用性を定量的に示している．本手法は，インターネット上のマルウェアダウンロードサイトから配布されるような一般に広く流通する未知のマルウェア検出に有効である．評価実験では，パッキングの有無，アンチウイルスソフトの検知有無を考慮した複数の検証条件で，マルウェアダウンロードサイトから収集した未知マルウェアを含むデータセットで，マルウェアであるか正常ファイルであるかの識別精度評価を行っている．結果，従来手法に比べ識別性能が高いことを示している．さらに選定した変数モデルを，代表的な機械学習手法であるサポートベクターマシンに適用し，さらに高精度で識別できることを示している．

第 3 章では，　ROP(Return-Oriented Programming)と呼ばれる攻撃コードが，シェルコードの複合ルーチンの外側に配置されるという攻撃コードを構成する上での特徴を利用し

て，準直接的にマルウェア検出を行う手法を提案し，その有用性を定量的に示している．本手法は，第 2 章での検出対象である一般に広く用いられるマルウェアでなく，大きな社会問題となっている標的型攻撃において，未知のゼロデイ脆弱性とともにも用いられる特定のマルウェアに有効であることを示している．ROP コードは，ここ数年の脆弱性においてホスト側の防御機構を突破することを目的として，多くの攻撃コードに付加されるものである．この ROP コードを静的に検出することで，悪性文書ファイル判定を行う方式を提案し，実際の検体にて評価を行っている．さらに，各検体で共通に使われる ROP コードを分析し，一部の ROP コードは異なる脆弱性とともに汎用的に用いられることを示し，これらの ROP コードを検出することでゼロデイ脆弱性対策として有用であることを示している．

第 4 章では，第 2 章や第 3 章で示すマルウェア自体の特徴を捉えて検出する直接的（または準直接的な）手法ではなく，マルウェアのダウンロードサイトを効果的にブラックリスティングして未知マルウェア対策につなげるという間接的な手法を提案し，その有用性を定量的に示している．本手法は，マルウェア自体のハッシュ値等の特徴が変化して，未知マルウェアがダウンロードされた場合の検出に有効である．評価実験では，約 43,000 個のマルウェアダウンロードサイトを，Web クローラを用いて約 1.5 年にわたり長期観測を行い，幾つかのサイトはとても長い期間にわたりマルウェアダウンロードサイトとして生存を続けること，また幾つかのサイトは消滅と復活を繰り返しながらマルウェアダウンロードサイトとして活動を続けることなど，マルウェアダウンロードサイトの特徴を明らかにしている．

第 5 章では，結論として，本論文の提案についてまとめ，将来課題について展望を示している．今後の展望としては，応用が期待されるＡＩ技術とともに，セキュリティ分析官や研究者の育成が急務であるとしている．

Ⅱ．論文審査結果の要旨

本論文は，現代さらに将来の社会における未知マルウェア対策の課題を解決するために，直接的にマルウェアを特定する対策から，マルウェアを内蔵するファイルの特徴から準直接的に未知マルウェアを検出する手法，さらにマルウエアの配布サイトの特性を見つけ出す間接的な対策まで，3 レベルに渡る対策手法を提案し，十分な量の実データを用いた定量的評価を通して，提案手法の有効性を示しており，情報学への貢献は大きい．

よって，本論文は，博士（情報学）の論文として合格と認められる．

Ⅲ．審査経過

本審査委員会は，平成 30 年 2 月 2 日に論文内容について口述試問と最終試験審査を行ない，申請者が学位取得にふさわしい知見を持つものと判断した．