【 3 】

氏　　名	ﾄﾗﾝ ｺﾝ ﾏﾝ
学位の種類	博　士（工学）
学位記番号	第　５５７　号
認定課程名	防衛大学校理工学研究科後期課程
学位授与年月日	平成 29 年 8 月 18 日
論文題目	A Research on Detection and Classification of Automated HTTP Communication（HTTP 自動通信の検出と分類に関する研究）
審査担当専門委員	（主査）九州大学教授　櫻井　幸一
	電気通信大学教授　阪口　豊
	早稲田大学教授　菅原　俊治

審　査　の　結　果　の　要　旨

我々が利用するウェブサービスの実装基盤である HTTP は、不正なアドウェアやボットを拡散させるための通信媒体として、サイバー犯罪者も悪用している状況にある。これに対抗するアンチウィルス製品が採用している、コンテンツおよびシグネチャベースの技術では、検出できないマルウェアが 30%以上を占め、本研究では、この対策のための新たな手法を提案している。著者は、HTTP 環境でのマルウェア検出のために、自動通信の挙動特徴を観測し、分類するネットワークベースとホストベースの２つの手法を提案し、さらに、実環境に適用するためのアプリケーションモデルも設計した。

ホストベースの検出手法では、正当なクライアントの周期的アクセス挙動とクライアントからサーバへのアクセス頻度の特性とを解析するアルゴリズムを設計し、実装実験によりその効果を明らかにしている。しかし、このホストベース手法では、すべてのクライアントが、このアプリケーションプログラムを実装する必要がある。著者は、この課題を解決するもう一つの、ネットワークベース手法の実現として、特定の URL ではなく，特定の目的 のための URL 群を解析するクラスター分類法を設計し、その効果を実験的に評価し、市販のアンチウイルスソフトでは特定できなかったマルウェア通信の特定に成功している。さらに著者は、提案した２つの手法を実働システムとして実現するための実装についても研究し、大規模データ環境に適用できる応用システムの設計を行い、それに適合するデータベースの特性を明らかにしている。

以上、本研究は、実ネットワークに混在する正当な通信とマルウェアによる通信とを識別

する手法を提案し、その有効性を実装実験により評価し、今後の課題まで論じた。これは、サイバーセキュリティ確保に対する情報工学的手法の有効性を示した結果であり、今後の安全・安心なサイバー社会の構築へ向けて大きな意義を有するものである。よって、学術的価値は高く博士(工学)として合格と判断した。