別紙様式第２号

学位論文及び審査結果の要旨

横浜国立大学

氏　　名	田辺 瑠偉
学位の種類	博士（情報学）
学位記番号	環情博甲第 1903 号
学位授与年月日	平成２９年３月２４日
学位授与の根拠	学位規則（昭和 28 年 4 月 1 日文部省令第 9 号）第４条第１項及び横浜国立大学学位規則第５条第１項
学府・専攻名	環境情報学府　情報メディア環境学専攻
学位論文題目	A Study on Malware Detection and Disinfection Based on Dynamic Analysis （動的解析を応用したマルウェアの検知と駆除に関する研究）
論文審査委員	主査　横浜国立大学　教　授　松本　勉 横浜国立大学　教　授　森　辰則 横浜国立大学　教　授　四方 順司 横浜国立大学　准教授　吉岡 克成 横浜国立大学　准教授　白川 真一

論文及び審査結果の要旨

昨今のサイバー攻撃では悪意のあるソフトウェア（マルウェア）により攻撃が実行されるため、マルウェアの動作を正確に把握することが防御において重要となる。マルウェアのコード自体を詳細に解析することはその動作を把握する上で有効であるが、これには専門的な技能が必要であり非常にコストが高い。そのため、専門的な技能を必要としない動的解析技術が特に注目されている。動的解析は、解析環境（サンドボックス）内でマルウェア検体を実行してその挙動を把握する技術であり、これまで多くの研究開発がなされると共に組織防御やマルウェア対策の現場でも基盤技術として利用されている。

本論文は、発展の著しい動的解析技術を、マルウェアの挙動把握だけでなく、直接的に組織ネットワークを防御する目的で応用する方法について論じている。ゲートウェイなど外部との境界におけるマルウェア検知、組織ネットワーク内のエンドホストにおけるマルウェア検知、組織ネットワーク内での感染拡大活動の検知と阻止という、組織ネットワーク防御の 3 つのフェーズにおいて、それぞれ動的解析技術を応用する方法について論じている。ゲートウェイなど外部との境界におけるマルウェア検知技術については、既に多くの手法が提案され、セキュリティアプライアンス製品として実用されているため、この検知能力の評価を実施している。

具体的には、これらの製品内で実装された解析環境の特徴に着目し、これを高い精度で検知し得ることを考察し、世界的に導入されているセキュリティアプライアンス製品による検知を回避して組織に侵入ができることを示し、そのような攻撃への対策方法を提案している。組織ネットワーク内のエンドホストにおけるマルウェア検知については、まだ十分に効果の高い手法が提案されていないことから、特に情報漏えい型のマルウェア検知を行う新たな手法を提案している。提案手法では、情報漏えい型マルウェアが侵入後のホストにおいて重要情報を探索する際のファイルアクセス失敗に着目し、マルウェア感染の事実を高い精度で検知できることを実験により示している。組織ネットワーク内での感染拡大活動の検知と阻止は、本論文においてはじめて提案される概念であり、組織ネットワークに侵入し、感染を広げようとする攻撃を検知する囮システムを用意し、攻撃検知時には逆に攻撃元に対してアクセスし、感染拡大活動を阻止する方法を示している。

本論文は全 7 章からなり、第 1 章の序論に続き、第 2 章で背景となるサイバー攻撃の現状と対策技術について述べている。3 章では動的解析技術を応用した組織ネットワーク防御の全体像を示し、提案する 3 つの技術の位置づけを示している。4 章では組織の入り口である

ゲートウェイにおける防御を担うセキュリティアプライアンスの評価を行い、最先端の製品であっても容易に検知を回避することができることを示し、対策方針を示している。5 章では、ゲートウェイでの防御を突破し、内部のホストに感染するマルウェアを想定し、感染時のファイル探索挙動を検知する手法を提案している。6 章では組織内ネットワークで感染の拡大を目指す攻撃を検知し、これを阻止する技術を提案しており、7 章で結論を述べている。

以上のように、本論文は、動的解析を応用した組織ネットワーク防御に関してゲートウェイ、内部ホスト、内部ネットワークの各位置において、既存の技術の問題点指摘と改善、新たな手法の提案を行っており、サイバーセキュリティ分野の研究に大きく貢献するものである。また本論文の内容は、査読付論文誌論文 2 篇、査読付き国際会議論文 1 篇、研究会論文 13 篇により公表されており、学会からも高い評価を得ている。

よって、本論文は博士（情報学）の学位論文として十分な価値を有すると論文審査委員全員一致で認め、平成 29 年 2 月 8 日 13 時から 14 時 20 分まで、環境情報 1 号棟 305 号室において博士論文発表会（公聴会）を開催した。博士論文発表会は 55 名の参加者を得て充実した質疑応答がなされた。同日 14 時 20 分から 14 時 35 分まで、同棟 304 号室において論文審査委員全員出席のもとで、田辺 瑠偉氏の最終試験を行った。審査委員からの博士論文に関する質問、セキュリティを中心とする専門分野および情報工学関連分野における口頭試問を行い、これらの専門知識に関する質問に対する応答から、専門知識、博士論文の内容の公表状況について十分であることを確認した。外国語については、英語による論文執筆ならびに発表があることをもって学力を確認した。また、履修単位が修了要件を満たすことを確認した。これらから、同氏は最終試験に合格であると、論文審査委員全員一致で判定した。

以上の論文審査委員会の結論に基づき、平成 29 年 2 月 13 日に開催した環境情報学府 情報メディア環境学専攻会議にて審議し、全員一致で本論文を博士（情報学）の学位論文としての価値があるものとして環境情報学府教授会に付議することを決定した。その後、環境情報学府学務委員会での確認を経て、平成 29 年 3 月 6 日に開催された環境情報学府教授会において審議を行い、無記名投票により、田辺瑠偉氏に博士（情報学）の学位を授与することを決定した。

注　論文及び審査結果の要旨欄に不足が生じる場合には、同欄の様式に準じ裏面又は別紙によること。