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	笠間貴弘
学位の種類	博士（工学）
学位記番号	環情博甲第 331 号
学位授与年月日	平成 26 年 3 月 26 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 Analysis Leveraging Sandbox Evasive Behaviors （マルウェアの回避挙動を利用した動的解析に関する研究）
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　長尾智晴 横浜国立大学　教　授　森　辰則 横浜国立大学　准教授　四方順司 横浜国立大学　准教授　吉岡克成

論文及び審査結果の要旨

近年多発しているセキュリティインシデントには、高度に機能化された悪意のあるソフトウェア（マルウェア）が関わることが多い。本論文はマルウェア解析技術の高度化に関する研究をまとめたものである。セキュリティインシデントに対する効果的な対策にあたり、マルウェアの持つ機能や特徴を明らかにすることが重要であるが、リバースエンジニアリング等の技術を駆使した熟練技術者による人手の解析では、極めて多数のマルウェアへの対応が事実上不可能であるため、解析環境（サンドボックス）内で実際にマルウェアを実行し、その挙動（ファイルアクセスやネットワークアクセスなど）を利用した「動的解析」が利用される。しかしマルウェア作成者は解析を妨害・回避するための機能をマルウェアに搭載するようになっている。本論文は、このような解析回避を試みるマルウェアを、その特徴を逆手にとって解析する、といった方法による、動的解析の高度化を目指している。

本論文は 7 章からなり、第 1 章の序論に続き、第 2 章で背景となるマルウェアとマルウェア解析手法の関連研究について整理している。

3 章では、本論文を貫く方法論を示している。新たなマルウェア対策技術が研究され広く用いられるようになると、マルウェア作成者はその対策技術を回避するための仕組みを開発するという、防御側と攻撃側のやり取りが長きに渡って続けられている。そのため、効果的な対策技術の研究開発のためには、いかにその対策をマルウェア作成者によって回避しづらいものにできるかという視点での検討が重要となる。本論文では、マルウェアが解析や検知の回避を試みることによって生じる正規プログラムとの挙動の差異を対策技術に利用するという方針を提案している。すなわち、解析手法を提案する際には、提案した解析手法を回避する挙動を用いた検知手法をも組み合わせて提案することにより、マルウェア作成者がとれる選択肢を狭めることができるという方法論である。なお 3 章では動的解析回避が「挙動把握の困難化」と「解析環境の検知」の二つに大別できることも示している。

4 章では疑似クライアントを用いたマルウェア解析手法を提案している。挙動把握を困難化にさせる手法を用いるマルウェアの中でも、大きな脅威となっているボットのような攻撃者の指令によって制御されるマルウェアに対して詳細かつ効率的な解析を可能とする新たな動的解析手法を提案した。提案手法では、まずマルウェアを解析環境内で一度実行し、マルウェアの行う通信挙動を把握する。その後、マルウェアの行った通信ログから感染活動などの危険性の高い通信を除外し、それ以外の通信を基にダミークライアントと呼ぶ簡易なスクリプトを用いることでマルウェアの通信挙動を模擬することで、指令サーバ等からマルウェアに対する応答を継続的に収集する。収集された応答は解析環境内で蓄積し、新たな応答が収集された際は再度マルウェアを実行し、マルウェアからのアクセスに対して解析環境内の

疑似サーバから収集した応答を送信することで、指令に対応したマルウェアの挙動を解析可能になる。またこの手法をインターネット上で収集したマルウェア検体に適用し、指令に応じた挙動を効果的に解析できることを確認している。

5 章では公開型マルウェア動的解析システムのデコイ挿入攻撃に対する脆弱性の検証を行っている。公開型マルウェア動的解析システムは、インターネット上で任意のユーザから検体投稿を受け付け、自動的に動的解析を行い、その挙動を解析して結果を投稿者に提供するシステムであり、その利用の簡易さから多くのユーザが怪しいファイル等の検査に利用している。しかし、攻撃者が特別に設計された検体（デコイ）をシステムに提出することで、サンドボックスの情報を収集し、その情報をもとに当該システムの検知を行う「デコイ挿入攻撃」が先行研究において提案され、実在するシステムが当該攻撃に対して脆弱であることが指摘されている。本論文では、当該脆弱性を正確に把握し適切な対策の導出へと繋げるために、検知に用いるサンドボックス情報に要求される 3 つの性質を定義し、16 種類のサンドボックス情報に着目して、これらが上記 3 つの性質を有しているかを評価実験によって明らかにした。評価実験の結果、先行研究で指摘された IP アドレス以外にも Windows プロダクトキーや MAC アドレス、OS インストール日時等のサンドボックス情報を用いた検知に対して既存のシステムが脆弱であることが判り、それらのサンドボックス情報については解析毎に値を変更するなど攻撃者に特定されないための対策が必要であることを明らかにしている。

6 章では、解析や検知の回避によって生じる正規プログラムとの差異を用いた対策技術の実現例として、新たなマルウェア検知手法を提案している。マルウェアの中にはシグネチャマッチングによる検知の回避や解析の妨害を目的として、実行毎に挙動を変化させるものが多く存在する。このようなマルウェアの挙動は実際に特定の解析や検知の回避に効果的である一方で、多くの正規プログラムでは見られない挙動であるため、このような回避挙動をマルウェアの特徴的な動作とみなし検知に活用できる可能性がある。提案手法では検査対象のプログラムに対して複数回動的解析を行い、それぞれの解析結果を比較することで実行毎の挙動の差異を判断することによりマルウェアの判定を行う。インターネット上で収集した正規プログラムとマルウェア検体を用いた評価実験を行い、提案手法では正規ソフトウェアの誤検知率を 1%程度に抑えながら 70%近くのマルウェアを検知でき、既存のアンチウイルスソフトが検知できないマルウェア検体の 50%近くを検知できることを確認している。

最後に 7 章で本論文のまとめと今後の展望について述べている。

以上のように、本論文は、解析回避を試みるマルウェアへの対策技術の確立を目指した新規性の高い研究結果を示したものであり情報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、本論文の研究内容は、3 篇の査読付論文誌論文、3 篇の査読付国際会議論文、6 篇の研究会・シンポジウム論文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（工学）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 26 年 2 月 12 日（水）14 時から 15 時 30 分まで、環境情報 1 号棟 515 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 44 名の参加者を得て、活発な質疑応答がなされた。同日 15 時 30 分より 16 時まで、環境情報 1 号棟 7 階ゼミ室において論文審査委員全員出席のもと、笠間貴弘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、情報セキュリティを中心とする専門分野および工学分野における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国際会議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、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 26 年 2 月 14 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（工学）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 26 年 3 月 3 日（月）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、笠間貴弘氏に博士（工学）の学位を授与することを決定した。