脅威情報とホワイトリストを用いたサイバー攻撃自動対処システムの研究

2020 年 1 月 21 日

「博士学位請求論文」審査報告書

審査委員（主査）　総合数理学部　専任教授

氏名　菊池　浩明　㊞

（副査）　総合数理学部　専任教授

氏名　斉藤　裕樹　㊞

（副査）　立命館大学 情報理工学部教授

氏名　毛利　公一　㊞

1　論文提出者　　氏名

重本　倫宏

2　論文題名

脅威情報とホワイトリストを用いたサイバー攻撃自動対処システムの研究

（欧文訳）　A Study on Automated Defense System based on Threat Intelligence and White List

3　論文の構成

本論文の構成は以下の通りである.

1 章　研究目的と背景
2 章　基本定義と従来研究
3 章　マルウェア解析高度化
4 章　脅威情報の収集
5 章　脅威度の推定
6 章　脅威情報を用いた自動対処
7 章　ホワイトリストを用いた自動対処
8 章　ホワイトリストの最適化
9 章　結論

4　論文の概要

本論文は，サイバー攻撃への自動対処に関する研究である.

重要インフラに標的を絞った独自のマルウェアによる高度サイバー攻撃に対して，従来型の既知パターンデータベースであるシグネチャー型の対策技術では間に合わない恐れが増している．脅威情報を基に攻撃元を遮断すると，無害の正規なサービスも道連れにされてしまい，業務に悪影響を与える問題も生じている．そこで，これらの課題に対して，本研究では，マルウェア解析を構造化して脅威情報を自動抽出し，脅威の度合いを判定し，最適化されたホワイトリストを導入して，業務への影響のない自動対策技術の構築を試みている．

5　論文の特質

1 章では，本論文の背景である重要インフラを狙ったサイバー攻撃の現状と高度な技術により解析を困難にするマルウェア動的解析と脅威情報の効率的な共有に関する課題を整理し，本研究の目的を明確に定義している．従来手法の多くは，マルウェアを特殊な環境で実行して振舞いを観測する動的解析手法を採っているが，それらを企業で導入すると過度な追加認証を求めることになり，業務作業の低減を招くことが考慮されていない．問題解決における本研究の手法の新規性と先行研究の流れの中での本研究の位置づけを明らかにしている．

2 章は，マルウェア解析研究における基本概念の定義と自動化対策技術に関する先行研究のサーベイを行っている．本分野の研究は，マルウェア解析に関する研究，脅威情報の収集に関する研究，ウェブサイトの脅威度推定に関する研究，自律型防御に関する研究などに大別することが示されている．

3 章では，多様な環境におけるマルウェアの振舞いの変動を観測し，いくつかのクラスタに自動分類する解析手法を提案している．TCP 通信先，DNS リクエスト先，API 呼び出し数などの 13 個の特徴量からマルウェアの類似度を算出し，約 8,000 の検体を 134 種類のファミリに約 64%の精度で分類できることを示している．

4 章では，非構造化された脅威情報を自動的に構造化する手法を提案している．マルウェアの脅威情報は独立した多数のセキュリティベンダーによりそれぞれ独自の表現で報告されており，新しいマルウェア名や脆弱性名などの未知語が頻出している．そこで，自然言語処理の手法を用いて固有表現を自動識別するインテリジェンス(脅威情報)構造化手法を提案している．

5 章は，ウェブサイトの脅威度を自動推定する方式を提案している．正規なサイトが混入した不正サイトの集合に対して，URL の文字列の特徴，ドメインの登録に関する情報，DNS 情報などから定められた 35 の特徴量と 3 つの機械学習による識別機を用いて脅威度を推定し，オープンデータを用いた評価結果を報告している．

6 章は，脅威情報に基づいて，マルウェアの動的解析と検出を自動化する基本動作の実装について述べている．マルウェアを多種環境で動的解析して脅威情報を自動抽出し，セキュリティベンダーの提供する外部データベース VirusTotal により確信度を算出し，業務影響度を考慮して自動対処する．34 名の評価者によるアクセス履歴を用いて提案方式の精度と影響度を評価している．

7 章では，6 章にて開発した方式を改良している．正規と分かったサイトをホワイトリストで与え，それ以外で危険性のあるサイトへの接続に対して追加認証を要求することで，業務に与える影響を低減している．ユーザ規模を変化させて可用性を評価し，追加認証要求率が十分に低減されて実用に耐えうる規模が 1000 人以上であることを確認している．

8 章は，誤検知と検知見逃しの二つの観点についてホワイトリストの最適化を試みている．相反する二つの指標を考慮した適応度関数を定め，遺伝的アルゴリズムにより問題を解いている．組織内の 26 台の PC の 2 カ月間活動ログを用いて評価を行い， 誤検知と検知見逃しの両方について 15%以上の改善を確認している．

9 章にて，本研究で提案した種々の手法が研究目的である即時性のある脅威情報の獲得と不確実な脅威情報に基づく業務影響の低減の二つの目的を達成していることを結論付けている．

6　論文の評価

マルウェアの動的解析を中心として，脅威情報を自動抽出して対処を行うための多くの試みを組合わせた実用性の高い研究である．次々に新種が現れ，人手で解析するには困難であったマルウェアからの脅威情報収集に対して，機械的に処理を行い，質の高い脅威情報の収集を実現した本研究が，サイバーセキュリティ対策に果たす役割は大きい．

脅威情報の自動抽出の精度を高めても，誤って正規サイトを検出してしまうリスクは避けられない．精度の向上だけではなく，業務への影響に焦点をおいて対処しているところに本研究の新規性はある．自動抽出された脅威情報の確信度を評価し，正規サイト情報から最適化されたホワイトリストと組み合わせることにより，追加認証による業務低下を引き起こすことなく，安全な企業活動を実現している．

提案された方式を，マルウェアデータセット，オープンデータなどの種々の情報を基に定量的に評価して，その安全性を立証している．特筆すべきは，データに基づく客観評価だけではなく，実組織における試験運用を行い，利便性などに関する主観評価を与えている点である．これらの多様な評価は，本研究の高い完成度を表している．

学位論文には，約 110 件の参考文献が挙げられており，本分野の最新の関連研究に対して十分な調査が行われていると言える．学位論文は研究成果を論理的に構成して，技術用語や数学的な表記についても不備なく適切に研究をまとめている． 研究成果は，情報処理学会や国際会議にて発表されており，本分野の複数の専門家による公平な査読が行われており，十分な信頼性を持っていることを裏付けている．

以上の点から，本論文は，サイバーセキュリティの研究として新規的かつ有益性の高いものであると評価する．

7　論文の判定

本学位請求論文は，先端数理科学研究科において必要な研究指導を受けたうえ提出されたものであり，本学学位規程の手続きに従い，審査委員全員による所定の審査及び最終試験に合格したので，博士（工学）の学位を授与するに値するものと判定する．

以　上