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　：　効果的・効率的なインシデントレスポンスの実現技術
申請者　：　羽田 大樹
審査委員会　：　主査　教授　後藤 厚宏
副査　教授　大久保 隆夫
副査　教授　松井 俊浩
副査　准教授　橋本 正樹

Ⅰ．論文内容の要旨

コンピューターが社会基盤として，さらには企業や組織の戦略を実現するための手段として当たり前に利用されている現代において，サイバーセキュリティへの対応は組織が持続的・発展的な活動を行うための重要な課題となっている．CSIRT は日々発生する組織内の大小様々なセキュリティインシデントをハンドリングすることで本業を支える重要な組織であるが，このインシデントレスポンスをいかに効率良く適切に行うかという課題を抱えている．本研究では，組織におけるマルウェア感染に対するリスクを最小化することを目標として，CSIRT おいて最も対応力が要求されるインシデントレスポンス業務における 2 つの課題についてフォーカスし，これを効率的・効果的に解決するための手法を提案した．

本論文は，「効果的・効率的なインシデントレスポンスの実現技術」と題し，6 章からなる．

第 1 章の「序論」では，本研究の背景として，経営課題として一般的に認識されるようになったサイバーセキュリティのリスクに備えるために設置された CSIRT（Computer Security Incident Response Team）の重要性を示した上で，CSIRT に求められる役割の中でも最も重要なインシデントレスポンス業務を効果的・効率的に行う研究の位置付けを明確にしている．

第 2 章では，CSIRT が抱える課題を広く調査して整理し，その中で本論文が対象とする課題を分析している．CSIRT 業務のインシデントレスポンスにおける「トリアージ」「事象の分析」「対応計画」「対応実施」のプロセスを分析し，それぞれが有する課題と関連研究を分析した上で，本研究で取り組む課題として，脅威情報の調査における課題と事象の分析における課題の二つを示している．

第 3 章では，脅威情報の調査における課題の解決に取り組んだ．インシデントレスポンスの「トリアージ」「対応実施」において対応の優先度や対応要否を決定するために必要となる Web ブラックリストの分類を提案している．Web サイトの脅威に対して CSIRT が抱えるブラックリストの課題を示した上で，CSIRT にとって有用な Web ブラックリストの 4 項目による分類を提案している．この分類について，公開されている 38 種類のブラックリストにはこの分類に相当する情報がほとんど含まれていないこと，また，100 組織において実際にインシデント判定を求められた 400 件の悪性情報について手動で調査を行い，提案する分類に妥当性があり，有用であることを示している．

第 4 章では，事象の分析における課題の解決に取り組んだ．制御フローグラフの比較を用いた関数の検索によるマルウェア解析の効率化のために，過去に解析したマルウェアの関数の制御フローグラフと命令列を用いて相当する関数を検索する新しい方式（BinGrep）を提案している．提案方式と BinDiff について正常プログラムを用いて比較評価するとともに，実際に APT 攻撃で使用された RAT である Emdivi と PlugX について評価を通して，提案方式がマルウェア解析において有効であることを示している．

第 5 章では，CSIRT に対する貢献と今後の展望について述べている．今後の展望においては，CSIRT におけるクラウドサービス利用の促進，および IT から OT へのスコープの拡大した場合でも提案技術が有用であることと，AI 主体の CSIRT への貢献の可能性について述べている．

第6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．

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，さらにマルウェ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．

本論文では，CSIRT に求められる役割の中でも最も重要なインシデントレスポンス業務に着目してこの行程を分析し，インシデントレスポンスを効果的・効率的に行うための 2 つの技術を提案している．Web ブラックリストに紐づいた分類を用いることで「トリアージ」における端末特定の要否，次の調査項目，優先度といった判断が，「対応実施」における通信の遮断の要否といった判断がマニュアルに基づいて合理的に行えることを示している．また，「事象の分析」において過去に解析したマルウェアの亜種を用いて解析すべき箇所を特定できるため，通信先や暗号処理の解析に速やかに取りかかることができるようになり，影響範囲の特定を効率化できるようになる．CSIRT のインシデントレスポンス業務における課題を解決する技術の提案により，組織の持続的・発展的な発展に貢献することができるものであり情報学の発展に大きく寄与する．

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 31 年 1 月 30 日に論文内容とこれに関連する事項について口述試問を行い、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。