令和６年度 東京情報大学総合情報研究所プロジェクト研究
研究実績報告書

１．研究課題名
サイバー攻撃の分析・検知に関する多角的な開発研究

２．研究組織

区分	氏名	所属・職名
研究代表者	花田　真樹	総合情報学部 総合情報学科・教授
研究分担者	岸本　頼紀	総合情報学部 総合情報学科・准教授
	早稲田　篤志	総合情報学部 総合情報学科・助教
	石田　裕貴	大学院総合情報学研究科・博士後期課程 3 年
	青野　健	大学院総合情報学研究科・博士前期課程 2 年
	磯野　怜	大学院総合情報学研究科・博士前期課程 1 年
	谷屋　直樹	大学院総合情報学研究科・博士前期課程 1 年

３．研究期間
2024 年 4 月 1 日～2025 年 3 月 31 日

４．研究の目的
全世界におけるサイバー攻撃による 2025 年の被害額は 10.5 兆ドル（約 1575 兆円）に達すると推定されている。このような背景のもと、本研究では、サイバー攻撃による被害を最小限に留めるために、サイバー攻撃による、ネットワークへの不正侵入、マルウェア感染、フィッシング詐欺、情報漏洩を検知・分析する基盤技術の確立を目的とする。

５．研究報告
本研究では、サイバー攻撃による、ネットワークへの侵入、マルウェア感染、フィッシング詐欺、情報漏洩を検知・分析するための基盤技術として、①サイバー攻撃の分析・検知、②マルウェアの検知・解析、③フィッシングと悪性通信の分析・検知、④サイバー攻撃による情報漏洩の分析、に関する新たな手法の提案・評価を実施した。

① サイバー攻撃の分析・検知

本研究項目では、被害に遭ったシステムの各種ログを効率よく収集し（攻撃痕跡の自動収集）、収集したログにおいて攻撃者による不審な事象が発生した箇所（ログ異常箇所の調査支援）を明らかにする。

1 つ目の攻撃痕跡の自動収集の目的は、各種ログから JSON 形式ログを正確に収集することである。システム内の各ファイルの先頭から 1000 バイトを特徴量とし、fastText を

用いてテキスト形式ログと JSON 形式ログを分類する手法を提案し、評価した。テキスト形式ログに関しては 21.23%しか収集できなかったが、JSON 形式ログは 100%収集することができた。2 つ目のログ異常箇所の調査支援の目的は、被害に遭った Windows イベントログに対して攻撃者による不審な事象が発生した箇所を推定し、可視化することである。ログファイルのイベント ID を単語、一定区間のイベント ID の集合を文章として、これらの特徴量を Doc2Vec で算出し、PCA で圧縮して描画を行う手法を提案した。周期的に特徴量が変化する箇所（Windows アップデートなど）を削除したが、正常な箇所も異常と判断される場合があることが明らかになった。

② マルウェアの検知・解析

本研究項目の目的は、マルウェアの表層解析・動的解析により分析した情報をもとに、検査対象のプログラムが正規プログラムかマルウェアか及びマルウェアのどの種類かを高精度で判別・分類する新たな手法の確立である。加えて、解析者によるマルウェアの動的環境構築を容易にするために、サーバの導入や設定を自動化するシステムの構築を行う。本研究項目では、時系列の API コール列の特徴ベクトルに対して LSTM（長・短期記憶）機械学習アルゴリズムを適用したマルウェア判別手法の実装を行い、既存のマルウェア判別手法より高精度で判別可能であることを示した。また、動的解析環境自動構築システムの開発を行った。本システムは、Web 管理ツールを介して、Vagrant を使用して仮想環境の自動構築を行い、Ansible を使用してアプリケーションの導入・設定を行うシステムである。

③ フィッシングと悪性通信の分析・検知

本研究項目の目的は、フィッシングサイト URL の文字列の特徴や生成される時間的な特徴を明らかにし、検査対象のフィッシングサイト URL が正規サイトかフィッシングサイトかを高精度で判別する新たな手法の確立である。加えて、高精度で悪性通信を検知する新たな手法を確立する。本研究項目では、DNS グラフのサブグラフ単位でフィッシングドメインから正規表現を生成し、フィッシングサイトを検知する手法（正規表現を用いたパターンマッチによる手法）を提案し、評価した。研究成果として、フィッシングサイト検知において、適合率 98.063%、再現率 8.636%となっており、既存手法の結果より良好な結果が得られた。また、ラテラルムーブメントを行うマルウェア 3 検体の通信について調査を行い、攻撃段階に移行する前のスキャン活動などの感染初期段階を含めた検知ルールを提案し、評価した。研究成果として、調査に使用したマルウェア 3 検体に加えて、ラテラルムーブメントを行う別種のマルウェア 2 検体に対しても検知が可能であることを示した。

④ サイバー攻撃による情報漏洩分析

本研究項目の目的は、パーソナルデータや機密データから個人を特定する情報を含まないデータに加工し、個人情報や機密情報の漏洩を防止する新たな手法の確立である。本研究項目では、機械学習による学習済みデータからの情報漏洩の状況と防ぐ方法を提案

し、評価した。研究成果として、機械学習法の一つ決定木において木の深さを深くするほどデータの漏洩が生じることを示した。加えて、乱択決定木について次のように作成することで差分プライバシーを満たすことを示した。各葉に割り当てられるすべてのラベルの要素数がk以下になるように枝刈りを行い、学習に使用するデータを木ごとに確率βでサンプリングをする。

６．成果の公表

①サイバー攻撃の分析・検知の研究成果は[1]～[5]、③フィッシングと悪性通信の分析・検知の研究成果は[6]、④サイバー攻撃による情報漏洩の分析の研究成果は[7]において報告を実施した。

[1] 谷屋 直樹, 中野 心太, 関谷 信吾, 折田 彰, 岸本 頼紀, 早稲田 篤志, 花田 真樹, “ログ収集のための機械学習を用いた JSON 形式ログファイル判別の検討,” 情報処理学会 コンピュータセキュリティシンポジウム 2024 (CSS2024) , pp. 1880-1883, 2024 年 10 月 15 日.

[2] 磯野 怜, 中野 心太, 関谷 信吾, 折田 彰, 岸本 頼紀, 早稲田 篤志, 花田 真樹, “機械学習を用いた異常ログ可視化のための誤検知された正常ログ対策の検討,”情報処理学会 コンピュータセキュリティシンポジウム 2024 (CSS2024) , pp. 1884-1887, 2024 年 10 月 15 日.

[3] 谷屋 直樹, 中野 心太, 関谷 信吾, 折田 彰, 岸本 頼紀, 早稲田 篤志, 花田 真樹, “ファストフォレンジックのための機械学習を用いたユーザアプリケーションログ収集システム,” 情報処理学会 2025 全国大会論文集, 2025 年 3 月 15 日.

[4] 磯野 怜, 中野 心太, 関谷 信吾, 折田 彰, 岸本 頼紀, 早稲田 篤志, 花田 真樹, “Doc2Vec を用いた特徴量差分に基づくログ調査支援システムの試作,” 情報処理学会 2025 全国大会論文集, 2025 年 3 月 15 日.

[5] 岸本 頼紀, 中野 心太, 関谷 信吾, 折田 彰, 花田 真樹, “デジタルフォレンジックのための Doc2vec を用いたインシデント日時可視化システムの検討,” 東京情報大学研究論集, 巻 28, 号 1, p. 29-38, 2024 年 9 年 30 日.

[6] 青野 健, 石田 裕貴, 早稲田 篤志, 花田真樹, “感染拡大を行うマルウェアの悪性通信特徴に基づく検知手法,”電子情報通信学会 暗号と情報セキュリティシンポジウム (SCIS2025) , 3F1, 2025 年 1 月 30 日.

[7] A.Waseda, R. Nojima, L. Wang, ″A Differentially Private (Random) Decision Tree without Noise from k-Anonymity,″ Appl. Sci. 2024, 14(17), 7625, 2024.