

令和7年度 東京情報大学総合研究所プロジェクト研究
研究実績報告書

1. 研究課題名

インターネット上の攻撃に対する安全性向上とインターネットの快適性向上に関する
研究開発

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
	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・准教授
	石田 裕貴	総合情報学研究科・大学院生
	松本 遥也	総合情報学研究科・大学院生
	磯野 怜	総合情報学研究科・大学院生
	谷屋 直樹	総合情報学研究科・大学院生
	黒石 花恋	総合情報学研究科・大学院生
	齋藤 日華理	総合情報学研究科・大学院生
	高山 立磨	総合情報学研究科・大学院生
	小暮 秀明	総合情報学研究科・大学院生
	森川 天斗	総合情報学研究科・大学院生

3. 研究期間

2025 年 4 月 1 日～2026 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、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、DoS 攻撃を検知・分析する基盤技術の確立を行うとともに、攻撃やシステム異常に耐性のある新しいインターネット技術を確認する。

5. 研究報告

本研究では、サイバー攻撃による、ネットワークへの不正侵入、マルウェア感染、フィッシング詐欺、DoS 攻撃を検知・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マルウェア検知・解析、③フィッシングサイト分析・検知、④DoS 攻撃の分析・検知

に関する新たな手法の研究開発を実施した。加えて、現在のインターネット技術の問題を抜本的に解決するために、⑤新世代インターネットのキャッシングと経路制御に関する新しい手法の研究開発を実施した。

① サイバー攻撃の分析・検知

本研究項目の目的は、攻撃者がネットワークへの侵入後の行動（何をしたのか）について各種ログ（攻撃者の痕跡情報）を効率よく収集して分析し、その攻撃者の行動特性について可視化技術を用いて明らかにすることである。

本研究項目の1つ目として、各種ログに対して攻撃者の痕跡情報を残しながら、それ以外の情報を圧縮して表示することにより、攻撃者の痕跡情報の可視化における視認性の向上を図った。具体的には、最長共通部分文字列アルゴリズムにより定常ログを固定の文字に置換して圧縮し、攻撃者の痕跡情報のみを強調して可視化する。評価実験では、圧縮率が14%から90%となり、Pass-the-Hash 攻撃に関しては十分な痕跡情報を可視化できることが明らかとなった。本研究項目の2つ目として、各種ログに対して攻撃者の痕跡情報のグラフや図による可視化の視認性の向上を図った。これに関しては複数の提案・評価を実施した。1つ目の提案として、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、その第一主成分と第二主成分を2次元のグラフ上に可視化した。可視化では、重心からの距離による表示により、視認性が向上することが明らかとなった。その他の提案として、イベントIDをノード、イベント間の関係をリンクとしたネットワーク図による可視化、イベントIDに対する出現頻度の逆数の2次元グラフ上の可視化、イベントIDが付与されていないログのメッセージに対して、メッセージの類似性を利用したイベントIDの生成と可視化を実施した。いずれの提案においても可視化に関する一定の有効性が確認された。

② マルウェア検知・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を確立することである。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。

本研究項目の1つ目として、次の2つを提案し、追加実装した。(1)N-gramのAPIコール列の出現頻度の特徴ベクトルに対して機械学習アルゴリズム XGBoost を適用した手法、(2)時系列のAPIコール列の特徴ベクトルに対してTransformerを適用した手法の2つである。XGBoostに関しては精度向上が見られなかったが、Transformerに関しては大幅な精度向上が確認できた。今後は、この2つの手法を、マルウェア分類・判別システムに拡張実装する予定である。本研究項目の2つ目として、動的解析環境自動構築システムの解析に必要なアプリケーションやソフトウェアに関する検討を行った。本システムによるマルウェア解析環境の構築を自動化するにあたっては、実際にマルウェア検体を動

作させ、解析に必要なアプリケーションやソフトウェアを整理する必要がある。そこで、振る舞いの明らかになっている点（GitHub でソースコード公開）と汎用性のある点に着目し、マルウェア検体の選定を行った。その結果、リモートアクセス型のトロイの木馬である AsyncRAT を対象とすることにした。今後は、実際にマルウェア検体（AsyncRAT）を動作させ、解析に必要なアプリケーションやソフトウェアの整理を行い、どこまで環境構築を自動化できるかの検討と実装を実施する。

③ フィッシングサイト分析・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を確立することである。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、正規表現を用いたパターンマッチによりフィッシングサイトを検知する手法を提案し、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、高い適合率と低い再現率を実現できており、既存手法の結果より良好な結果が得られた。

④ DoS 攻撃の分析・検知

本研究項目の目的は、正常通信と判別が付きにくい低レート DoS 攻撃を対象として、その特徴を明らかにし、正常通信か低レート DoS 攻撃かを高精度で判別する新たな手法を確立することである。本研究項目では、通信回数および通信容量の PSD（Power Spectral Density）エントロピー、通信の統計量を特徴量とした機械学習アルゴリズム LightGBM による分類器の作成を提案し、評価した。研究成果として、先行研究の PSD エントロピーによるフィルタリングを用いた機械学習アルゴリズム SVM と NN による DoS 攻撃検出方式と比較して、F1 スコアが向上しており、提案方式の有効性が確認された。

⑤ 新世代インターネットの経路制御とキャッシング

本研究項目の目的は、有線・無線ネットワークにおける通信性能を向上させるために、MANET における新世代インターネットのアーキテクチャを対象とし、経路制御とキャッシングに関する新たな手法を確立することである。本研究項目の 1 つ目として、新世代インターネットの 1 つのアーキテクチャであるコンテンツ指向ネットワークを導入し、データの返送経路を制御することにより、データの取得を効率的に行う手法を提案した。要求パケットの経路の逆経路を利用して、返送パケットの効率的な返送経路を提案し、評価した。従来方式と比較して、コンテンツダウンロード時間が十分に短縮されており、提案方式の有効性が確認された。本研究項目の 2 つ目として、1 つ目と同様にコンテンツ指向ネットワークを導入し、データのキャッシュ位置を制御することにより、データの取得を効率的に行う手法を提案した。要求パケットの経路として頻繁に利用されるノードに積極的にキャッシュする方式を提案し、評価した。従来方式と比較して、キャッシュヒット率が向上しコンテンツダウンロード時間が十分に短縮されており、提案方式の有効性が

確認された。

6. 成果の公表

【研究会、シンポジウム、大会（査読なし）】

(① サイバー攻撃の分析・検知)

- [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, “ログ調査のための LCS を用いたログイベント圧縮表現方法の提案,” 情報処理学会 コンピュータセキュリティシンポジウム 2025 (CSS2025), 3F3-1, 2025 年 10 月.
- [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, “ログ解析のための Doc2Vec を用いた区間特徴量の 2 次元表現の一考察,” 情報処理学会 コンピュータセキュリティシンポジウム 2025 (CSS2025), 3F3-2, 2025 年 10 月.
- [3] 高山 立磨, 中野 心太, 関谷 信吾, 折田 彰, 岸本 頼紀, 早稲田 篤志, 花田 真樹, “ログ解析支援のための文書類似度に基づくイベント ID 割り当て手法の提案,” 情報処理学会 コンピュータセキュリティシンポジウム 2025 (CSS2025), 3F3-3, 2025 年 10 月.
- [4] 黒石 花恋, 中野 心太, 関谷 信吾, 折田 彰, 岸本 頼紀, 早稲田 篤志, 花田 真樹, “ログ調査のためのネットワーク図を用いたイベント出現関係可視化の提案,” 情報処理学会 コンピュータセキュリティシンポジウム 2025 (CSS2025), 3F3-4, 2025 年 10 月.
- [5] 齋藤 日華里, 中野 心太, 関谷 信吾, 折田 彰, 岸本 頼紀, 早稲田 篤志, 花田 真樹, “ログ調査のためのイベントログの矩形波表現を用いた可視化の提案,” 情報処理学会 コンピュータセキュリティシンポジウム 2025 (CSS2025), 3F3-5, 2025 年 10 月.

(② マルウェア検知・解析)

- [6] 甘利 涼, 石田 裕貴, 花田 真樹, “API コール情報を用いたマルウェア分類・判別システムの試作,” 第 28 回 日本情報ディレクトリ学会全国大会 研究報告予稿集, pp. 17-20, 2025 年 9 月.

(④ DoS 攻撃の分析・検知)

- [7] 東 勇樹, 花田 真樹, “PSD エントロピーと機械学習を用いた複数 DoS 攻撃検出方式,” 令和 8 年電気学会全国大会, L719-C3, 2026 年 3 月.

(⑤ 新世代インターネットの経路制御とキャッシング)

- [8] 小暮 秀明, 松本 遥也, 金光 永煥, 花田 真樹, “CCN ベースの MANET における再送を考慮したダウンロード時間を最小化する転送待機時間の提案,” 電子情報通信学会 コミュニケーションシステム研究会, 2026 年 3 月.

- [9] 松本 遥也, 金光 永煥, 花田 真樹, “CCN ベースの MANET におけるインタレストパケットの転送状況を用いたキャッシュ判断方式,” 電子情報通信学会 コミュニケーションシステム研究会, 2026 年 3 月.

【国際会議、学術論文誌（査読あり）】

(③ フィッシングサイト分析・検知)

- [1] 石田 裕貴, 早稲田 篤志, 金 武完, 花田 真樹, “DNS グラフを用いたフィッシングサイト検知手法,” 情報処理学会 論文誌 Vol. 66, NO. 8, pp. 1029–1045, 2025 年 9 月.

(⑤ 新世代インターネットの経路制御とキャッシング)

- [2] Haruya Matsumoto, Hidehiro Kanemitsu, Masaki Hanada, “‘ Cache Decision Policy Using Interest Packet Forwarding Information in CCN-based MANET ,’” Proc. of the 30th Asia-Pacific Conference on Communications (APCC2025) , T3-3.3, 2025 年 11 月.
- [3] 松本 遥也, 金光 永煥, 花田 真樹, “‘CCN ベースの MANET におけるインタレストパケットの転送経路を用いたデータパケットの転送方式 ,’ ” 電子情報通信学会 論文誌 (B) Vol. J108-B NO. 5, pp. 254–272, 2025 年 5 月.