様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月　 ４ 日現在

機関番号：１３９０１
研究種目：基盤研究(C)（一般）
研究期間：2019～2023
課題番号：１９Ｋ１１９６１

研究課題名（和文）機械学習を用いた標的型攻撃における侵入拡大経路推定に関する研究

研究課題名（英文）Research on intrusion expansion route estimation in targeted attacks using machine learning

研究代表者
山口　由紀子（YAMAGUCHI, Yukiko）

名古屋大学・情報基盤センター・協力研究員

研究者番号：９０２３９９２１

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：　組織を標的としたサイバー攻撃に対し、日々の活動の中で行われるインターネット／イントラネットの通信を監視して悪性通信を検出し通信データに潜む悪性通信の機械学習による検知手法に関する研究を行った。LightGBMを学習モデルとする悪性通信検知における特徴量の選択のための特徴量分析、追加学習時に受ける中毒攻撃検知手法、FPGAを組み合わせた高帯域通信に対する悪性通信検知システムなどの研究を行い、成果が得られた。
　また、バイナリデータを対象とした機械学習によるマルウェア検知、SNSなどの非公式な情報源を利用したWAFシグネチャのリアルタイム更新やナレッジベースの自動構成手法などの成果が得られた。

研究成果の学術的意義や社会的意義
　機械学習を用いたサイバーセキュリティの研究として、本研究課題で目的としている悪性通信検知とその派生である中毒攻撃検知ほか、バイナリデータを利用したマルウェア検知、GNNを用いた特徴量抽出など幅広い分野で検知技術の向上に貢献した。
　また、チャット系アプリのハイパーリンク生成機能における不具合を発見、開発元に連絡することで安全なアプリ利用に貢献した。

研究成果の概要（英文）：In order to counter cyber-attacks targeting organizations, we performed research on methods for detecting malicious communications hidden in communication data by monitoring Internet/intranet communications during daily activities. We conducted research on feature value analysis for selecting features in malicious communication detection using LightGBM, poisoning attack detection method for additional learning, and hybrid malicious communication detection system for high-bandwidth communication using FPGA.
In addition, we performed malware detection using machine learning targeting binary data, real-time updating of WAF signatures using unofficial information sources such as SNS, and automatic knowledge base configuration method.

研究分野：サイバーセキュリティ

キーワード：サイバーセキュリティ　悪性通信検知

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属します。

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

近年のサイバー攻撃は標的型攻撃と呼ばれる高度に制御された手法が用いられ、初期侵入の段階で検知することが難しい。インターネットとの接続点にファイアウォールや IDS（侵入検知システム）を設置するなどの対策をとっていても、結局情報窃取などの被害が発生して初めて発覚する場合もある。標的型攻撃では一般に、手順 1：計画立案、手順 2：攻撃準備、手順 3：初期潜入、手順 4：攻撃基盤構築、手順 5：内部調査侵入、手順 6：目的遂行の段階を踏んで実施される（参考文献[1]）。そのため、被害が発覚した時点ではすでに攻撃基盤が構築されており再発の危険性をはらんでいる。そのような状況での対応は組織の CSIRT（Computer Security Incident Response Team）およびネットワーク管理者にとって大きな負担となっている。事実 IPA（情報処理推進機構）が毎年発表している組織における情報セキュリティ 10 大脅威では、研究開始当初の 2018 年、2019 年は標的型攻撃が 1 位となっており（参考文献[2]）、CSIRT の活動を支援する研究が求められていた。

【参考文献】

[1] 独立行政法人情報処理推進機構、「高度標的型攻撃対策に向けたシステム設計ガイド」 https://www.ipa.go.jp/files/000052614.pdf

[2] 独立行政法人情報処理推進機構、情報セキュリティ 10 大脅威 https://www.ipa.go.jp/security/10threats/index.html

２．研究の目的

本研究は、組織を標的としたサイバー攻撃に対し、日々の活動の中で行われるインターネット／イントラネットの通信を監視して悪性通信を検出し、組織の CSIRT 活動を支援し、担当者の負担を軽すること減を目的としている。組織に対する標的型攻撃では、手順 4：攻撃基盤構築、手順 5：内部調査侵入の段階で攻撃活動による通信が発生する。そこで、本研究では通信データに潜む悪性通信の機械学習による検知手法の確立を目指す。機械学習を用いた識別器では、学習モデルと特徴量の選択も課題となる。また、機械学習による識別器は追加学習によって新しい攻撃パターンの検知も可能になるが、その一方で追加学習時の中毒攻撃を受ける可能性があり、その検知も課題である。なお、本研究課題では実験ネットワークを構築して擬似的な攻撃を行い、通信データを収集する計画であったが、コロナ禍などの影響があり、既存のデータセットを用いた研究を行うこととした。

一方、通信データだけでなくマルウェア検体（バイナリデータ）分類の性能向上やインシデント情報・脆弱性情報をいち早く入手して対策をとるためのシステム作りも組織を守るために必要な要素であり、これらの研究も推進していく必要がある。

３．研究の方法

本研究課題では、通信データを利用したサイバーセキュリティに関する研究として主に以下の 3 テーマについて研究を行った。

(1) 機械学習による悪性通信検知に関する研究

本研究課題では実験ネットワークを構築して通信データを収集し、機械学習による悪性通信を検知の結果から感染経路を特定する計画であったが、コロナ禍や研究室移動などによる影響で通信データの収集が困難な状況となった。そのため、既存の通信データセットを利用して、機械学習による悪性通信の検知、およびその派生として検知システムへの中毒攻撃に関する研究を行った。

(2) 組織内通信の安全性を高める研究

本研究課題の目的としている組織内部で検出された感染端末の挙動を分析する研究として、SDN を利用して感染端末が行う通信のみを仮想環境に転送して分析することにより、攻撃のターゲットを分析するシステムを提案した。また、2020 年以後広く定着したリモートワーク環境からの組織へのアクセスの安全性を高めるシステムの提案も行った。

(3) 悪性通信検知の高速化に関する研究

標的型攻撃検知のためには組織内通信のモニタリングが必要になる。しかしながら組織内のイントラネット通信は、ISP などと契約するインターネット通信と比べて高帯域で行われるものが多く、費用の面から IDS などの検知システムを導入することが難しい。そこで、FPGA と組み合わせることで高速通信に対応可能な悪性通信検知に関する研究を行った。

４．研究成果

各研究テーマについて以下の研究成果が得られた。

(1) 機械学習による悪性通信検知

機械学習による悪性通信検知では、機械学習モデルと特徴量の選択が重要である。本研究では、Kyoto2016 データセットと国立情報学研究所の情報セキュリティ運用連携サービス（NII Security Operation Collaboration Services: NII-SOCS）のデータセットについて悪性通信検知システムを生成し分析を行った。Kyoto2016 はハニーポットの通信データを収集したもので広く

公開されている。一方、NII-SOCS データセットは参加機関の実際の通信を監視し検知処理実施時のトラフィックデータから生成されており利用にあたっても契約が必要となる。NII-SOCS データセットは Kyoto2016 に準拠した 20 個の特徴量で構成されており、双方の比較が容易である。機械学習モデルとして LightGBM を使用し、各特徴量の重要度を算出するゲイン(ジニ不純度の減少に関する評価値）を比較した（図 **1**)。

その結果、おおよその傾向は同じであったが、NII-SOCS では「受信バイト数(特徴量番号 3)」が最大のゲインとなっている一方、Kyoto2016 では「サブネット識別子が同じ過去のセッション数(特徴量番号 15)」「セッション終了時の接続状態(特徴量番号 18)」でゲインが大きく、データセットによる差が大きくなった。これは Ktoto2016 がハニーポットへの攻撃が多く含まれる通信データであることに起因していると考える。なお、これらのデータセットを利用した悪性通信検知に関する研究は今後も継続して行っていく予定である。

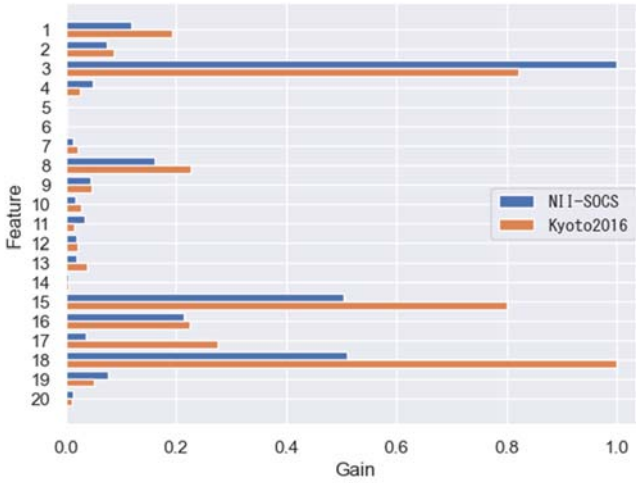

図 1　データセットによる特徴量のゲインの比較
[小川 2024]

さらに派生として機械学習による悪性通信検知システムへの中毒攻撃に関する研究を行った。

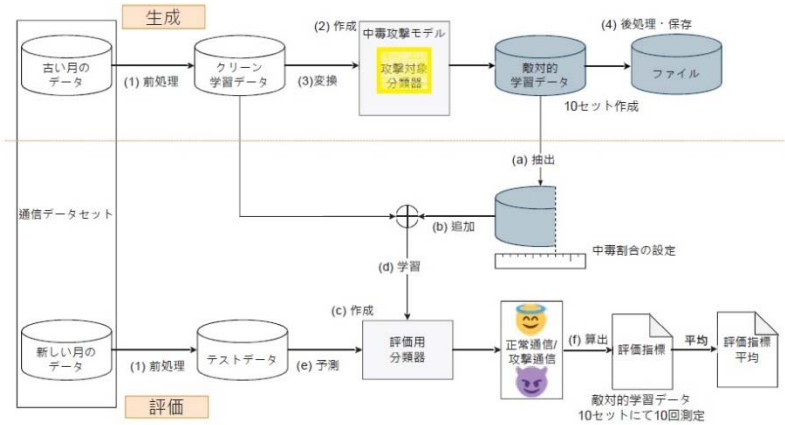

図 2　中毒攻撃検知評価実験の概要［桑山 2021］

インターネットにおけるサイバー攻撃は日々変化しているため、機械学習による検知システムでは最新の攻撃パターンに対応するための追加学習が必須となる。その過程において追加学習用のデータに攻撃用データを混入させる中毒攻撃を受ける危険性がある。そこで追加学習時の中毒攻撃の有無を判定する研究を行った。本研究では通信データとして Kyoto2016 データセット、機械学習モデルとして SVM を使用した。評価実験の概要を図 **2** に示す。あらかじめ作成した悪性通信を検知する分類器を対象として、まずは中毒攻撃用の敵対的学習データの生成を行う。本研究では scikit-learn と Adversarial Robustness Toolbox(ART)ライブラリを利用した実験環境を構築し、Kyoto2016 データセットについて特徴量の正規化とラベルの反転を行い敵対的学習データの生成を行った。評価段階においては混入させる敵対的学習データの割合を変化させて追加学習を行った識別器について識別性能の変化を分析し、中毒率 25%で正解率が大きく下がることを確認した。なお、敵対的学習データの公開を見据えた後処理も含めた生成手法を確立したことも本研究の成果である。

(2) 組織内通信の安全性を高める研究

本研究課題の目的としている組織内部におｋる感染端末の挙動を分析する研究として、SDN を利用して感染端末が組織内サーバ／端末に対して行う通信のみを仮想環境に転送して観測することにより、攻撃のターゲットを分析するシステムを提案した。標的型攻撃では、最初に感染した端末が攻撃の目的ではなく、組織内の重要なデータを窃取することを目的としており、感染端末は C&C サーバからの指令を受けて攻撃活動を行うことが一般的である。そこで、本研究では SDN と仮想環境を利用して感染挙動分析システムを構築した（図 **3**)。感染が検知された端末とインターネットとの通信（図 **3** の(1)）は制限せず、組織内の他の端末との通信(2)は仮想環境の解析端末へ転送することにより、参考文献[1]の標的型攻撃の手順 5 にあたるサーバ不正ログイン(3)／他端末への攻撃範囲拡大(4)の挙動を分析するものである。SDN スイッチとして Open vSwitch、仮想環境として VMware vSphere Hypervisor を利用してプロトタイプシステムを構築

し、インターネット側に設置した Kali Linux から攻撃するシナリオを実行してデータ収集を行い、本提案の有効性を検証した。

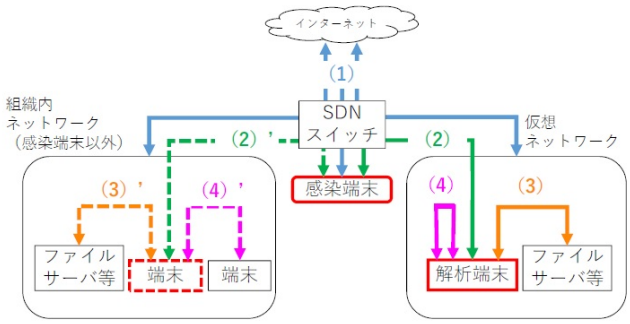

図 3　感染端末挙動分析システム　[大橋 2019]

2020 年から始まったコロナ禍の影響で多くの組織でリモートワークが導入され、コロナ禍が治まりつつある 2024 年においても継続して利用されている。リモートワークでは、家庭などの遠隔地から組織内部へ VPN 接続を利用してアクセスし就労することとなる。コロナ禍以前は、限定された社員が社外からのアクセス用にセットアップされた端末を利用する運用であったが、コロナ禍においては多くの従業員が VPN 接続することとなり、その安全性の担保が重要な課題となった。そこで、従業員の信頼度とリモートから利用する社内リソースの重要度に従ってアクセス制御を行うシステムを提案した（図 **4**）。従業員のセキュリティ研修、標的型メール訓練、過去のインシデント件数などから信頼度を算出し、VPN への接続要求時に社内リソースへのアクセス制御（ACL）を生成し、SDN（OpenFlow）でルータに自動的に反映することで、ネットワーク管理者の負担を権限できる。プロトタイプシステムを構築し、可用性を検証した。

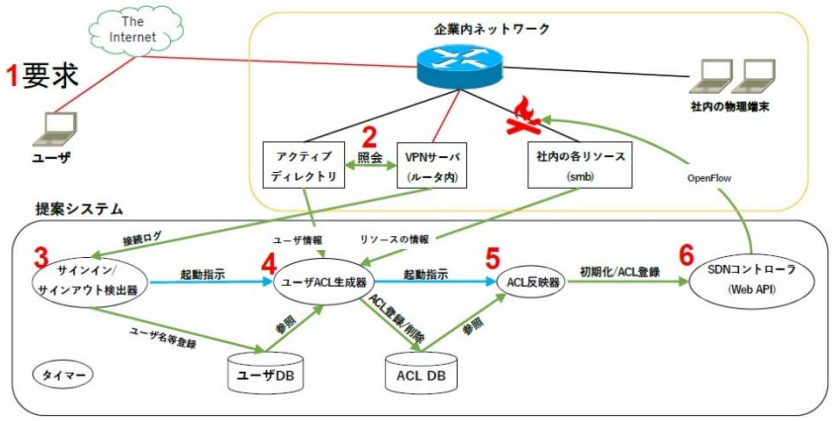

図 4　リモートワークに対応したアクセス制御システム　[篠田 2022]

(3) 悪性通信検知の高速化に関する研究

100Gbps などの高帯域の通信については、インターネット通信での導入は少ないが、イントラネットについては徐々に導入されつつある。しかしながら、高帯域対応な IDS は費用の面から導入することが難しい。そこで本研究では高帯域通信に対するリアルタイムでの悪性通信検知システムとして、FPGA による特徴抽出を行い、ホスト CPU で悪性検知を行うハイブリッドな悪性通信システムを構築した（図 **5**）。悪性通信検知時のリアルタイム性を確保するため、FPGA で抽出した特徴量をペイロードとして埋め込んだ UDP パケットを構築し、通信データと

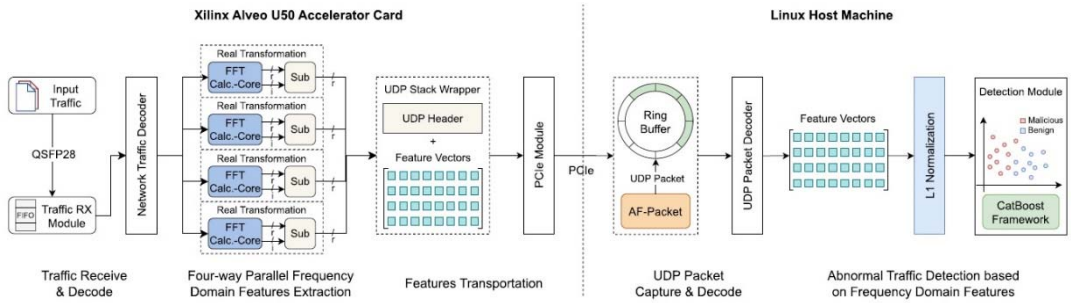

図 5　ハイブリッド構成による高速悪性通信検知システム　[Hu 2023]

してホストに送信し、ホスト側では UDP パケットから特徴量を抽出して、CatBoost による悪性通信検知を行う。本研究では、FPGA として QSFP28 ポートを持つ Xilinx Alveo U50 を利用して特徴抽出機能を実装した。データセットとして MAWI WIDE と USTC-TFC2016 を利用し、Mellanox ConnectX-5 NIC を装着した Cisco TRex から PCAP データを送信して、検知性能および遅延を評価した。その結果、検知性能として 0.98 の精度が得られ、1〜3Gbps のスループットで悪性通信検知が可能であることが確認できた。

また、本研究課題が対象としている通信データを用いた研究以外にもサイバーセキュリティに関する様々な研究を行い、以下の成果が得られた。

(4) バイナリデータを対象とするマルウェア検知

バイナリデータから CFG（Control Flow Graph）を抽出し、機械学習モデルとして GIN（Graph Isomorphism Network）を利用した識別器を構築した。生成された CFG について関数名やアドレスを特徴量に変換してノードへ埋め込み、さらにエッジの集約を行って GIN への入力とする。GIN による畳み込み後、最終的に得られたグラフのノードに埋め込まれた特徴量を抽出して MLP により分類する。評価実験の結果、0.98 の識別精度が得られた。

一般に機械学習を用いたマルウェア検知システムでは、最新のマルウェアに対応するため、追加学習を行うことで性能を維持している。このような検知システムについて、検知を逃れたい特定のマルウェアについて検知システムを混乱させる偽学習データを強化学習を用いて生成する手法を示した。機械学習モデルで利用した特徴量の次元が足りなかったため、期待した性能は得られなかった。

SVM によるマルウェア検知システム対する中毒攻撃について、追加学習用データの中毒検知に関する研究を行った。学習済みモデルの内部パラメータは正常な学習データでの追加学習では変動が少なく中毒データでは変動が大きいことを利用して、追加学習時の内部パラメータの学習前のものとの差分で閾値判定するものである。評価実験により差分の最大値と最小値の中間値を閾値とすることで判別可能であることを示した。

(5) 組織のセキュリティを守る研究

複数事業所から構成される大規模組織では、セキュリティ対応が手薄な小規模事業所を入口として標的型攻撃を受け、本体事業所に影響が及ぶ場合がある。そこで、各事業所で発生したインシデントを統合して CSIRT 活動を支援するシステムを提案した。本提案では、検出したインシデントを一定期間内に発生したインシデントとの相関関係を算出することにより、攻撃の意図を推測し、未然の対策実施を可能とする。

また、一般に公式な脆弱性情報は公開が遅いため、公開された時点ではすでに被害が発生している恐れがある。そこで、SNS などの非公式な情報源からセキュリティ情報を抽出し、WAF（Web Application Filter）シグネチャのリアルタイム更新やナレッジベースの自動構成を行う手法を確立した。しかしながら、X（旧 Twitter）など、SNS を運営する組織のポリシー変更により情報の入手が困難となった。

(6) サイバーセキュリティ一般

チャット系アプリではメッセージ内の URL に付加されたハイパーリンクが大変便利で多用されている。このようなアプリは Web 用、スマホアプリ用などの実装が提供されているが、Android アプリ版において、多言語 URL のハイパーリンク処理で分割が発生するなどの不具合があることを発見した。この不具合は単に URL にアクセスできないだけでなく悪性 URL への誘導を可能とする脆弱性を含んでいる。そのため、アプリ開発元へ連絡するとともに、対応策としてハイパーリンク処理の際に URL 境界に関する前処理を行うラッパーの開発を行った。

【発表文献（抜粋）】

[小川 2024] 小川剛史, 長谷川皓一, 山口由紀子, 嶋田創, "プライバシーに配慮した悪性通信検出手法の NII-SOCS ベンチマークデータを用いた検討," 電子情報通信学会研究報告, Vol. 123, No. 448, ICSS2023-80, pp. 79-84, 2024 年 3 月

[桑山 2021] 桑山拓也, 嶋田創, 山口由紀子, 長谷川皓一, "既存通信データセットに対する中毒攻撃を想定した敵対的学習データ生成の試行," 情報処理学会研究報告, Vol. 2021-CSEC-95, No. 9, pp. 1-8, 2021 年 11 月

[大橋 2019] 大橋宗治, 長谷川皓一, 山口由紀子, 嶋田創, "組織内部での攻撃行動を仮想環境へ誘導する挙動分析システム," 電子情報通信学会研究報告, Vol. 119, No. 288, ICSS2019-65, pp. 31-36, 2019 年 11 月.

[篠田 2022] 篠田優, 長谷川皓一, 山口由紀子, 嶋田創, 高倉弘喜, "ユーザの信用度を考慮したテレワーク通信へのアクセス制御手法の実装," コンピュータセキュリティシンポジウム 2022 (CSS2022), pp. 840-847, 2022 年 10 月.

[Hu 2023] Zhenguo Hu, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada, "Realtime Malicious Traffic Detection targeted for TCP Out-of-Order Packets based on FPGA," IEEE Access, Vol. 11, pp. 112212-112222, October 2023.

５．主な発表論文等

〔雑誌論文〕　計10件（うち査読付論文　10件／うち国際共著　0件／うちオープンアクセス　6件）

１．著者名 辻知希，嶋田創，山口由紀子，長谷川皓一	４．巻 Vol. 64, No. 5
２．論文標題 Androidアプリの自動リンクにおける悪意のあるリンク生成リスクの検討	５．発行年 2023年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 1041-1052
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Hu Zhenguo、Hasegawa Hirokazu、Yamaguchi Yukiko、Shimada Hajime	４．巻 11
２．論文標題 Realtime Malicious Traffic Detection Targeted for TCP Out-of-Order Packets Based on FPGA	５．発行年 2023年
３．雑誌名 IEEE Access	６．最初と最後の頁 112212～112222
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2023.3323853	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Yun Gao, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada	４．巻 Vol. 16, No. 3
２．論文標題 alware Self-Supervised Graph Contrastive Learning with Data Augmentation	５．発行年 2023年
３．雑誌名 International Journal On Advances in Security	６．最初と最後の頁 116-125
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Hu Zhenguo、Hasegawa Hirokazu、Yamaguchi Yukiko、Shimada Hajime	４．巻 12
２．論文標題 Enhancing Detection of Malicious Traffic Through FPGA-Based Frequency Transformation and Machine Learning	５．発行年 2024年
３．雑誌名 IEEE Access	６．最初と最後の頁 2648～2659
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2023.3348234	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Gao Yun、Hasegawa Hirokazu、Yamaguchi Yukiko、Shimada Hajime	4．巻 10
2．論文標題 Malware Detection Using LightGBM With a Custom Logistic Loss Function	5．発行年 2022年
3．雑誌名 IEEE Access	6．最初と最後の頁 47792～47804
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2022.3171912	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Gao Yun、Hasegawa Hirokazu、Yamaguchi Yukiko、Shimada Hajime	4．巻 10
2．論文標題 Malware Detection by Control-Flow Graph Level Representation Learning With Graph Isomorphism Network	5．発行年 2022年
3．雑誌名 IEEE Access	6．最初と最後の頁 111830～111841
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2022.3215267	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Masahito Kumazaki, Yukiko Yamaguchi, Hajime Shimada, and Hirokazu Hasegawa	4．巻 Vol. 14, No. 1&2
2．論文標題 WAF Signature Generation from Real-Time Information on the Web using Similarity to CVE	5．発行年 2021年
3．雑誌名 International Journal On Advances in Security	6．最初と最後の頁 26-36
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Otgonpurev Mendsaikhan, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada	4．巻 Vol. 14, No. 1&2
2．論文標題 Automatic Mapping of Threat Information to Adversary Techniques Using Different Datasets	5．発行年 2021年
3．雑誌名 International Journal On Advances in Security	6．最初と最後の頁 37-47
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Mendsaikhan Otgonpurev、Hasegawa Hirokazu、Yamaguchi Yukiko、Shimada Hajime、Bataa Enkhbold	４．巻 28
２．論文標題 Identification of Cybersecurity Specific Content Using Different Language Models	５．発行年 2020年
３．雑誌名 Journal of Information Processing	６．最初と最後の頁 623～632
掲載論文のDOI（デジタルオブジェクト識別子） 10.2197/ipsjjip.28.623	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Mendsaikhan Otgonpurev、Hasegawa Hirokazu、Yamaguchi Yukiko、Shimada Hajime	４．巻 8
２．論文標題 Quantifying the Significance and Relevance of Cyber-Security Text Through Textual Similarity and Cyber-Security Knowledge Graph	５．発行年 2020年
３．雑誌名 IEEE Access	６．最初と最後の頁 177041～177052
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2020.3027321	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計29件（うち招待講演　0件／うち国際学会　12件）

１．発表者名 Zhenguo Hu, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada
２．発表標題 A Prototype Design of Real-Time Encrypted Malicious Traffic Detection based on Hardware Implementation
３．学会等名 the 26th IEEE Symposium on Low-Power and High-Speed Chips (COOLChips 26)（国際学会）
４．発表年 2023年

１．発表者名 Zhenguo Hu, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada
２．発表標題 Heterogeneous Network Inspection in IoT Environment with FPGA based Pre-Filter and CPU based LightGBM
３．学会等名 the 17th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2023)（国際学会）
４．発表年 2023年

１．発表者名
Atsushi Shinoda, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada, Hiroki Takakura

２．発表標題
Feasibility Verifcation of Access Control System for Telecommuting by Users Reliability Calculation

３．学会等名
the Eighteenth International Conference on Systems and Networks Communications (ICSNC 2023)（国際学会）

４．発表年
2023年

１．発表者名
小川剛史，長谷川皓一，山口由紀子，嶋田創

２．発表標題
プライバシーと悪性通信検知精度の両立を目指した通信ログ匿名加工の検討

３．学会等名
コンピュータセキュリティシンポジウム2023 (CSS2023)

４．発表年
2023年

１．発表者名
小川剛史，長谷川皓一，山口由紀子，嶋田創

２．発表標題
プライバシーに配慮した悪性通信検出手法のNII-SOCSベンチマークデータを用いた検討

３．学会等名
電子情報通信学会 情報通信システムセキュリティ研究会

４．発表年
2024年

１．発表者名
松波旭，長谷川皓一，山口由紀子，嶋田創

２．発表標題
機械学習を用いた悪性URLクエリ検知に対するラベル反転攻撃の攻撃耐性評価

３．学会等名
電子情報通信学会 情報通信システムセキュリティ研究会

４．発表年
2024年

１．発表者名
Yun Gao, Hasegawa Hirokazu, Yamaguchi Yukiko, Shimada Hajime

２．発表標題
Malware Detection using Attributed CFG Generated by Pre-trained Language Model with Graph Isomorphism Network

３．学会等名
the 12th IEEE International Workshop on Network Technologies for Security, Administration and Protection (NETSAP 2022)（国際学会）

４．発表年
2022年

１．発表者名
Yun Gao, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada

２．発表標題
Unsupervised Graph Contrastive Learning with Data Augmentation for Malware Classification

３．学会等名
the 16th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2022)（国際学会）

４．発表年
2022年

１．発表者名
Atsushi Shinoda, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada, and Hiroki Takakura

２．発表標題
Feasibility Verification on Impact of Frequently Access Control Update based on User Reliability

３．学会等名
the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023)（国際学会）

４．発表年
2022年

１．発表者名
篠田優，長谷川皓一，山口由紀子，嶋田創，高倉弘喜

２．発表標題
ユーザの信用度を考慮したテレワーク通信へのアクセス制御手法の実装

３．学会等名
コンピュータセキュリティシンポジウム2022 (CSS2022)

４．発表年
2022年

１．発表者名
小川剛史，長谷川皓一，山口由紀子，嶋田創

２．発表標題
悪性通信検知のためのプライバシーに配慮した通信ログ匿名加工の検討

３．学会等名
電子情報通信学会ICSS研究会

４．発表年
2023年

１．発表者名
蘇思遠，長谷川皓一，山口由紀子，嶋田創

２．発表標題
機械学習系マルウェア検知システムへの中毒攻撃データ生成の特徴量空間拡大検討

３．学会等名
情報科学技術フォーラム FIT 2021

４．発表年
2021年

１．発表者名
桑山拓也，嶋田創，山口由紀子，長谷川皓一

２．発表標題
既存通信データセットに対する中毒攻撃を想定した敵対的学習データ生成の試行

３．学会等名
情報処理学会　コンピュータセキュリティ研究会

４．発表年
2021年

１．発表者名
熊崎真仁，長谷川皓一，山口由紀子，嶋田創，高倉弘喜

２．発表標題
正常ログ残存を前提とするサイバー攻撃推定手法の性能評価

３．学会等名
情報処理学会第84回全国大会

４．発表年
2022年

１．発表者名
Masahito Kumazaki, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada, and Hiroki Takakura

２．発表標題
Cyber Attack Stage Tracing System Based on Attack Scenario Comparison

３．学会等名
the 8th International Conference on Information Systems Security and Privacy

４．発表年
2022年

１．発表者名
Masahito Kumazaki, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada, Hiroki Takakura

２．発表標題
Incident Response Support System for Multi-Located Network by Correlation Analysis of Individual Events

３．学会等名
the 4th International Conference on Information Science and Systems (ICISS 2021)（国際学会）

４．発表年
2021年

１．発表者名
熊崎真仁，長谷川皓一，山口由紀子，嶋田創，高倉弘喜

２．発表標題
複数拠点ネットワークにおける類似インシデント評価手法の検討

３．学会等名
電子情報通信学会情報通信システムセキュリティ研究会

４．発表年
2021年

１．発表者名
野田朋宏，長谷川皓一，嶋田創，山口由紀子，高倉弘喜

２．発表標題
インシデント対応策に残存する情報漏洩リスク評価システムの実装

３．学会等名
電子情報通信学会情報通信システムセキュリティ研究会

４．発表年
2021年

１．発表者名
Yun Gao, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada

２．発表標題
Malware Detection Using Gradient Boosting Decision Trees with Customized Log Loss Function

３．学会等名
the 35th International Conference on Information Networking (ICOIN2021)（国際学会）

４．発表年
2021年

１．発表者名
熊崎真仁，長谷川皓一，山口由紀子，嶋田創，高倉弘喜

２．発表標題
複数拠点におけるインシデント対応支援システムの初期検討

３．学会等名
電子情報通信学会情報通信システムセキュリティ研究会

４．発表年
2020年

１．発表者名
Otgonpurev Mendsaikhan, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada

２．発表標題
Automatic Mapping of Vulnerability Information to Adversary Techniques

３．学会等名
the 14th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2020),（国際学会）

４．発表年
2020年

１．発表者名
Masahito Kumazaki, Yukiko Yamaguchi, Hajime Shimada, Hirokazu Hasegawa

２．発表標題
WAF Signature Generation with Real-Time Information on the Web

３．学会等名
the 14th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2020),（国際学会）

４．発表年
2020年

１．発表者名
Yun Gao, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada

２．発表標題
Gradient Boosting Decision Tree Ensemble Learning for Malware Binary Classification

３．学会等名
コンピュータセキュリティシンポジウム2020

４．発表年
2020年

１．発表者名
Otgonpurev Mendsaikhan, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada

２．発表標題
Identification of Cybersecurity Specific Content Using the Doc2Vec Language Model

３．学会等名
The 43rd Annual International Computers, Software and Applications Conference（国際学会）

４．発表年
2019年

１．発表者名
Otgonpurev Mendsaikhan, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada

２．発表標題
Quantifying the Significance of Cybersecurity Related Text Documents by Analyzing IoC and Named Entities

３．学会等名
コンピュータセキュリティシンポジウム2019予稿集

４．発表年
2019年

１．発表者名
高木聖也，長谷川皓一，山口由紀子，嶋田創

２．発表標題
機械学習を用いたマルウェア検知システムに対する強化学習による敵対的サンプル生成の課題

３．学会等名
電子情報通信学会情報通信システムセキュリティ研究会

４．発表年
2019年

１．発表者名
大橋宗治，長谷川皓一，山口由紀子，嶋田創

２．発表標題
組織内部での攻撃行動を仮想環境へ誘導する挙動分析システム

３．学会等名
電子情報通信学会情報通信システムセキュリティ研究会

４．発表年
2019年

１．発表者名
熊崎真仁，長谷川皓一，山口由紀子，嶋田創

２．発表標題
Web上のリアルタイム情報を利用したWAFシグネチャ生成の初期検討

３．学会等名
電子情報通信学会情報通信システムセキュリティ研究会

４．発表年
2020年

１．発表者名
Otgonpurev Mendsaikhan, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada

２．発表標題
Quantifying the Significance of Cybersecurity Text through Semantic Similarity and Named Entity Recognition

３．学会等名
The 6th International Conference on Information Systems Security and Privacy（国際学会）

４．発表年
2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関