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　５ 年　 ６ 月 １３ 日現在

機関番号：１３９０１
研究種目：基盤研究(B)（一般）
研究期間：2019～2022
課題番号：１９Ｈ０４１０８

研究課題名（和文）機械/深層学習型検知への対抗能力を備えたマルウェア利用への対抗アルゴリズム研究

研究課題名（英文）Countermeasure for counter machine/deep learning based detection system types of malware exploitation

研究代表者
嶋田　創（Shimada, Hajime）

名古屋大学・情報基盤センター・准教授

研究者番号：６０３７７８５１

交付決定額（研究期間全体）：（直接経費）　　12,400,000円

研究成果の概要（和文）：機械学習応用のサイバーセキュリティ応用への広がりにより、事前に中毒攻撃用のマルウェアサンプルをばらまいて機械学習系検知の検知精度を下げる攻撃を懸念し、対抗研究を実施した。
特に、中毒攻撃データ生成とその検知に関する研究を推進し、マルウェアバイナリ特徴量をベースにSVMマルウェア識別器に対するSVM中毒攻撃において、学習前後におけるSVM識別器内の勾配係数ベクトルの変化量から検知する成果を得た。
他に、GNNによるマルウェア特徴量圧縮、検知のための損失関数のカスタマイズ、自動リンク処理時の悪性ハイパーリンク生成の可能性、オープンデータからのセキュリティナレッジ構築とWAFルール生成などの成果を得た。

研究成果の学術的意義や社会的意義
研究課題名に関する中毒攻撃用マルウェアサンプルの検知において、学習前後の識別器内の勾配情報を利用する方法を提案し、研究賞受賞などの評価を得た。
また、機械学習系マルウェア検知や悪性通信検知の向上に関する研究で検知技術の向上の研究で貢献した。
さらに、オープンデータのセキュリティナレッジ構築や偽無線LAN検知や悪性ハイパーリンク生成などのサイバーセキュリティ一般に関する研究で、サイバーセキュリティ一般に研究で貢献した。

研究成果の概要（英文）：Due to increase of Machine Learning (ML) application to cyber security area, we performed researches about countermeasure for attacks that distributes malware samples for poisoning attack to reduce detection accuracy of ML based classifier.
We mainly promoted poisoning attack data generation and their detection. We obtained good achievement by detecting poisoning attack data from evaluating gradient vector in SVM based malware classifier before and after relearning.
We also performed several cyber security area such as malware feature compression with GNN, log loss function customize for malware detection, malicious hyper-link generation possibility in auto-link feature, security knowledge or WAF rule construction from open data, and so on.

研究分野：サイバーセキュリティ、ネットワークセキュリティ、マルウェア検知

キーワード：サイバーセキュリティ　マルウェア検知　対・対・機械学習/深層学習　対標的型攻撃

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

近年では機械学習や深層学習を応用したマルウェア検出や悪性通信検出の研究が盛んであり、商用のセキュリティ機器においても、機械学習系の技術の活用をうたっている機材が多数出てきている状況にある。我々も過去研究において、自組織の過去の通信を学習して生成した識別器によるアノマリ型検知など、機械学習系を用いたしかしながら、近年では機械学習系に対して誤判定や誤検知をさせるための学習データを送りつける、敵対的学習という技術がある。現状のサイバーセキュリティ関係の敵対的学習の研究においては、全てのマルウェア等に関しての検知率を下げる話がほとんどである。たとえば、参考文献[1]では特徴空間での勾配方向を考慮した誤検知誘発について検討されており、また、参考文献[2]では Android マルウェア識別用の機械学習系の識別器に細工をしたマルウェアを学習用に送り込むことで検知精度を低下させることが行われている。この形では、セキュリティ対応側は過去から検知率が低下することで、敵対的学習が試みられていることに気づくことができる。しかしながら、いずれ攻撃者が、攻撃に用いる特定のマルウェアのみ検知率を下げ、他のマルウェアへの検知率は落とさない形での敵対的学習を実現する、いわば、対機械学習および深層学習検知のマルウェア送付手法を確立し、ブラックマーケットなどでマルウェア送付フレームワークとして販売されるようになることが懸念される。近年ではサイバー攻撃グループによる標的型攻撃も活発になっており、機械学習系の検知環境を持つ標的への標的型攻撃への有用性を考えると、標的型攻撃を実施するグループが、前述のような言わば「対機械学習系検知」のフレームワークを活用してくることが懸念される。

[1] H. S. Anderson, et. al., ``Evading Machine Learning Malware Detection,'' Black Hat USA 2017, Jul. 2017.

[2] S. Chen, et. al. ``Automated Poisoning Attacks and Defenses in Malware Detection Systems: An Adversarial Machine Learning Approach,'' arXiv:1706.04146, Jun. 2017.

２．研究の目的

対機械学習系検知に対抗するため、言わば、「対・対機械学習系検知」の研究は重要となると考える。そこで、本研究では、特定のマルウェアをベースに、それを通過させることを志向した敵対的学習用データが送られている環境において、敵対的学習用データの存在可能性の推定アルゴリズム、および、そのような敵対的学習に対して補完する学習データを生成することによって、対機械学習および深層学習の機能を備えたマルウェア送付フレームワークに対抗する、対対機械学習系検知の研究を行う。また、補完用学習データの生成とその利用は、adversal examples 方式など他の機械学習系検知逃れに対する有用性もあると考え、その有用性を評価する。本研究課題では、特定のマルウェアに対する敵対的学習が可能となる将来を見据えた上で研究を行う。

機械学習系に誤判定をさせる研究は、特に、機械学習系の有用性が大いに評価されている画像処理や音声処理で活発であり、adversal examples のように、元画像や音声に計算して生成したノイズを乗せることで「人間には正常に見えるが、機械学習系では誤判定される」ものが話題となっている。将来的に攻撃者が adversal examples をマルウェアに応用してくることが考えられるが、本研究課題で「補完用学習データの生成」は adversal examples にも一定の有用性があると考え、マルウェアへの adversal examples 応用が活発になった時点で有効性を評価する形とする。また、本研究課題に対する攻撃者側のさらなる対抗手法の出現も考えたアルゴリズム作成を意識し、対抗手法の出現を困難とさせる。

３．研究の方法

研究推進は大きく分けて、以下の 3 種類に分けて実施した。

1) 研究課題名となっている、対・対機械学習系検知マルウェアや悪性通信の生成とその検知に関する研究。この研究で攻撃対象とする識別器は取り扱いの容易なシンプルな識別器(SVM など)として、対・対機械学習系検知マルウェアとその検知の概念実証を容易とした。

2) 機械学習系マルウェア検知や悪性通信検知の向上に関する研究。これは、検知技術の向上の研究で貢献するのと同時に、高度な識別器における概念実証への移行を容易とするためである。

3) オープンデータのセキュリティナレッジ構築や偽無線 LAN 検知や悪性ハイパーリンク生成などのサイバーセキュリティ一般に関する研究。これは、サイバーセキュリティ一般に研究で貢献するのと同時に、将来的に機械学習技術が応用される可能性の高いセキュリティ関連分野への中毒攻撃の可能性についての展開を容易とするためである。

４．研究成果

前節で説明した 1)から 3)の項目の研究成果において、各項目の主要な成果を 2 論文(予稿を含む)ずつ説明する。

前節 1)で説明した項目の主要な成果として、追加学習前後の識別器の内部係数の変化量から追加学習データへの中毒攻撃用マルウェア特徴量の混入の有無を検知する研究[1]、および、GAN と強化学習を組み合わせた偽学習データサンプル生成を試み[2]について述べる。

発表文献[1]については、SVM ベースのマルウェア識別器に対し、追加学習前後の SVM ベースのマルウェア識別器の勾配ベクトルの変化量をもとに、追加学習データに中毒攻撃用マルウェア由来のデータが含まれているか判別することを試みたものである。中毒攻撃用マルウェアは

識別器の内部状態である勾配ベクトルを大きく乱すような学習データになると想定し、再学習を行った後の識別器の勾配ベクトルが大きく変化した場合に追加した学習データは中毒攻撃由来であったと判別するものである。追加学習前後に図 1 に示す検知アルゴリズムで追加訓練データの評価を行い、閾値を超える勾配ベクトルの変化があった場合に中毒攻撃用データと判断するものである。なお、判別の閾値は、識別器生成者側で，既存の学習データから閾値決定用の中毒攻撃用データを生成し、学習した時の勾配ベクトルの変化量から決定する。評価は，新たにクリーンなデータと中毒攻撃用データをそれぞれ 300/150/75 ずつを追加して学習した識別器の勾配ベクトルとのユークリッド距離を変化量で行った。評価の結果，閾値の設定においてクリーンなデータの追加時の変化量の最大値と中毒攻撃用データの追加時の変化量の最小値を使うことになっても、その中間値を閾値として設定して判別可能なことを確認した。

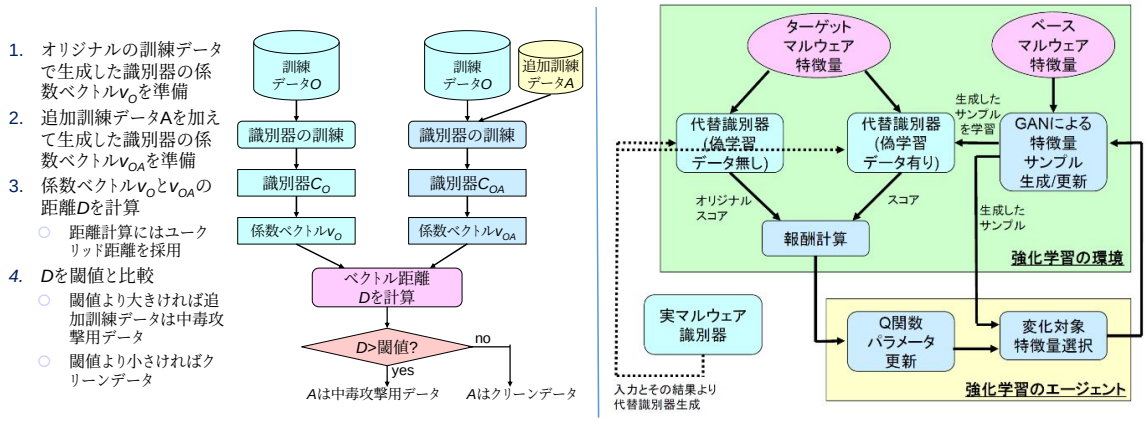

図 1(左): 学習前後の識別器の勾配ベクトル変化量からの中毒攻撃用データ検知
図 2(右): 敵対的生成ネットワークと強化学習を組み合わせた敵対的サンプル生成

発表文献[2]については、「マルウェアを用いてサイバー攻撃を行う者が、事前に偽学習データとなる偽マルウェアをばらまいた上で、偽学習データによる中毒攻撃が成功したタイミングで本命(ターゲット)マルウェアで攻撃」というシナリオが成立するかの検証を行った結果をまとめたものである。検証では、図 2 と以下の箇条書きで示した手順で、マルウェア識別器(代替識別器)、偽学習データを生成する GAN(Generative Adversarial Networks)、偽学習データの生成を誘導する Deep Q Network による強化学習を利用し、偽学習データの生成の検証を行った。

(1) 偽学習データ生成用としてベースとなるベースマルウェア特徴量を設定する。
(2) 強化学習のエージェント側からの変化対象特徴量選択を受け、偽学習データの特徴量を変化させる。
(3) 代替識別器に対して偽学習データをバッチサイズ分複製し学習させる。
(4) 検知を回避させたいターゲットマルウェア特徴量を偽データ学習後の代替識別器に識別させ、悪性度を出力させる。
(5) オリジナルの代替識別器が出力した悪性度と手順(4)で学習した識別器が出力した悪性度を比較し、どのくらい悪性度が低下したかを報酬として出力する。
(6) 強化学習のエージェント側は報酬を受け取り、最適な行動を選ぶための Q 関数のパラメータを更新して、より正確に最適な行動(より悪性度を低下させる特徴量変更)が選べるように学習する。
(7) エージェント側において、Q 関数の出力と前状態の偽学習データをもとに、次に変化させるべき特徴量を選択する。

評価結果は芳しくなかったが、これは、先行研究で利用されたデータセットに合わせたため、利用するバイナリ特徴量が 128 個の API の呼び出しの有無で表したシンプルなバイナリ特徴量であったため、特徴量空間の狭さによって強化学習によって出力されるサンプルの自由度の無さが影響したと推測した。

前節 2)の主要な成果として、カスタム損失関数を導入した識別器の学習によるマルウェア検知精度の向上[3]、および、Graph Isomorphism Network を用いたバイナリ特徴量圧縮によるマルウェア検知精度の向上[4]の成果について記す。

発表文献[3]については、勾配ブースティング型決定木による識別アルゴリズムの 1 種である LightGBM の学習時に用いられる損失関数に対し、False Negative 判定を減らす方向に学習を強める係数 α と False Positive を許容する方向に学習を強める係数 β を導入することにより、単独の識別器の検知精度と複数の識別器を複合させた場合の検知精度の双方について改善したものである。これは、一般提供されている識別アルゴリズムの学習は広く汎用的な識別に向けた学習に使えることを目指して設定されているため、マルウェア検知の学習に特化した物を作成することにより、マルウェア検知精度を向上させることができるのではという発想からの研究になる。評価は、特に、無害なバイナリサンプルとマルウェアサンプルの比率を偏らせた(マルウェアの数が少ない現実的な環境)で良い結果を示した。

発表文献[4]については、マルウェアバイナリからの特徴量抽出において Graph Isomorphism Network(GIN)を使った基本ブロックレベルの特徴量の抽出を実現し、マルウェア検知精度を向

上させた研究である。検知は図 3 の流れで行われ、バイナリの基本ブロック構造を抽出し(Graph Feature Extraction)、各基本ブロックの情報をグラフの節に埋め込んで各バイナリに対するグラフデータを生成し(Graph Data Generation)、生成したグラフデータを GIN によって 64 次元の特徴量ベクトルに圧縮する(Graph Classification)。最後に、得られた特徴量ベクトルを、多層パーセプトロン(MLP)によって識別する。

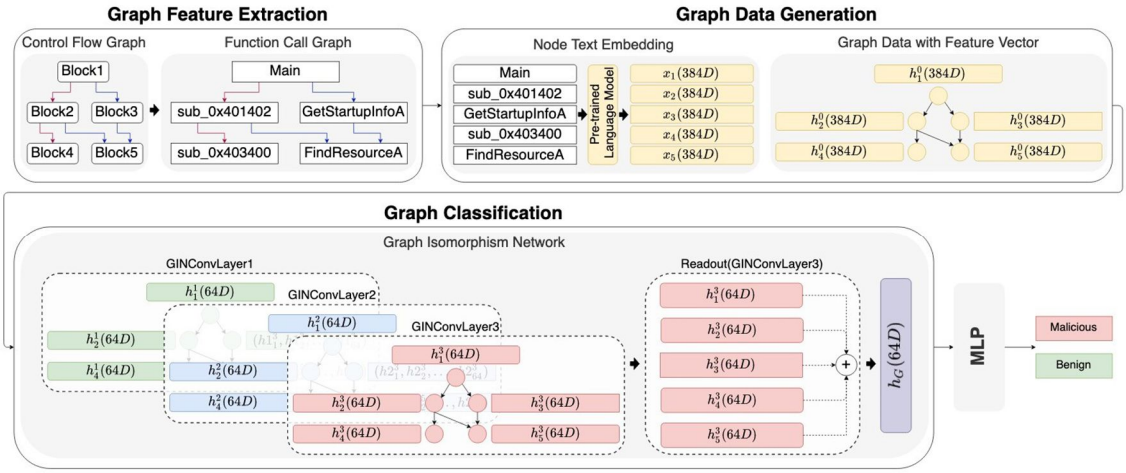

図 3: GIN を用いた基本ブロックレベル特徴量の圧縮とマルウェア識別への利用

前節 3)の主要な成果として、SNS 上などのオープンな情報からの新規脅威情報を抽出しての新規 Web Application Firewall のルール設定[5]、および、近年のチャット機能を備えるアプリにおける URL らしき文字列に自動的にハイパーリンクを付与する処理における悪性ハイパーリンク生成のリスクと対策[6]について記す。

発表文献[5]については、近年のゼロデイ脆弱性について、公式の脆弱性情報が出る前に SNS や議論系掲示板で話題になった段階で対策を取ることを半自動化することを目的とした研究である。図 4 に示すように、提案システムは SNS や議論系掲示板からのリアルタイムなオープンデータを取得し、ノイズの除去(Cleansing)、過去の脆弱性との比較からの Web Application Firewall (WAF)シグネチャ生成、システム管理者への脆弱性情報と生成された WAF シグネチャについての通知を行う。これにより、システム管理者はゼロデイ脆弱性に対し、公式の脆弱性情報や更新パッチが出る前に WAF による一時しのぎの対策を取ることができるようになる。

発表文献[6]については、近年のチャット機能を備えるアプリにおける URL らしき文字列に自動的にハイパーリンクを付与する処理(自動リンク処理)におけるセキュリティリスクを低減する研究である。近年のアプリのチャット機能では、URL と判断できる文字列に対して自動的にハイパーリンクを付与する機能を備えているものが多いが、このハイパーリンク付与に失敗している事例は多くの利用者が目にしている。単純なハイパーリンク付与の失敗ならば良いが、本研究において、想定外の URL の分割により悪性 URL への誘導ができる可能性が示されたため、自動リンク処理が呼ばれた時に分割などの想定外の動作を起こす URL の無害化処理を行うラッパーを開発した(図 5)。

主要な成果として 6 つの成果とその概要を記したが、他にも、以下のような研究を実施した。

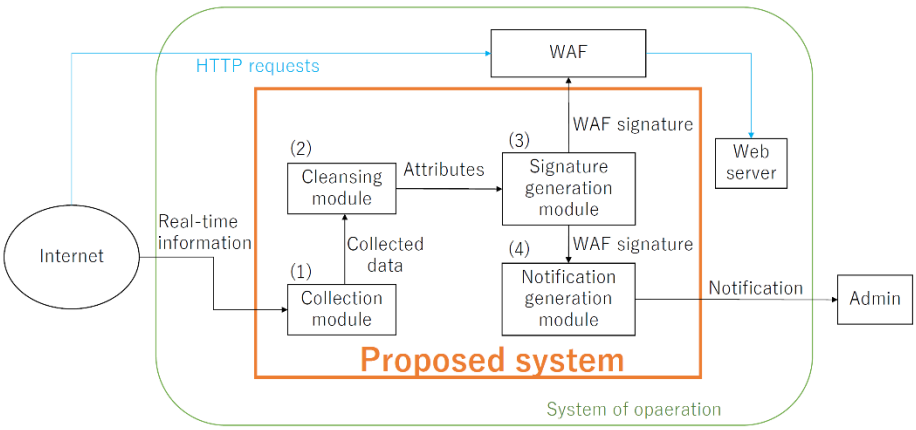

図 4: SNS 等の脆弱性話題からの WAF シグネチャ自動生成

発表文献[6]については、近年のチャット機能を備えるアプリにおける URL らしき文字列に自動的にハイパーリンクを付与する処理(自動リンク処理)におけるセキュリティリスクを低減する研究である。近年のアプリのチャット機能では、URL と判断できる文字列に対して自動的にハイパーリンクを付与する機能を備えているものが多いが、このハイパーリンク付与に失敗している事例は多くの利用者が目にしている。単純なハイパーリンク付与の失敗ならば良いが、本研

究において、想定外の URL の分割により悪性 URL への誘導ができる可能性が示されたため、自動リンク処理が呼ばれた時に分割などの想定外の動作を起こす URL の無害化処理を行うラッパーを開発した(図 5)。

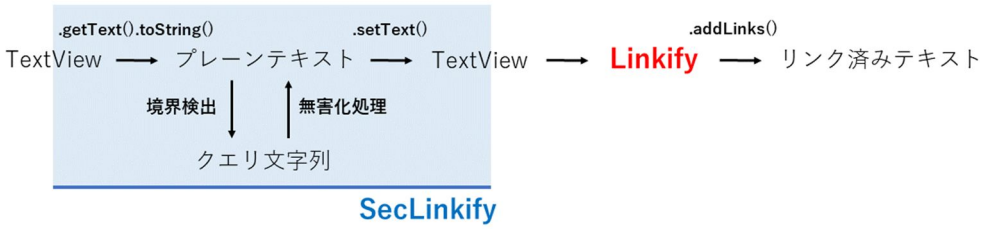

図 5: ラッパーによる悪性ハイパーリンク生成の可能性のある文字列への無害化処理

主要な成果として 6 つの成果とその概要を記したが、他にも、以下のような研究を実施した。

- 標的型攻撃検知応用のための研究として、組織内に侵入したマルウェアの最終目的を、OpenFlow を用いて極少数の仮想サーバ内で偽の拡散を許容しての追跡
- SNS や議論系ウェブページからの組織内情報機器に関するセキュリティ情報の自動収集とランク付けしての提示、および、オープンアクセス情報から収集した情報と既存の別種の脆弱性情報との類似性による関連付け
- メモリフットプリントプリントを利用したマルウェア検知
- 遅延ヒストグラムを特徴量とした不正無線 LAN の検知
- 組織内ネットワークの特徴量の継続的な採取とそれを利用した動的な侵入検知システムの識別器のアップデート
- 本店と支店をまたがる複数拠点間をまたぐ標的型攻撃攻撃対策の研究に関して、拠点間の類似インシデントの確認を利用した攻撃可能性の検知と情報流出の可能性の評価
- 国際化ドメイン名の自動リンク処理を悪用して悪性 URL へのリンクが生成される可能性について調査
- 既存通信データセットに対する敵対的学習データ生成
- サイバー攻撃内容の残存ログからの標的型攻撃内容の推定手法
- VR 可視化システムを利用した標的型攻撃対応のための通信遮断による影響範囲提示
- プライバシーに配慮した悪性通信検知手法
- テレワーク経路を利用する標的型攻撃を想定したネットワーク運用
- SRv6 を用いた攻撃由来通信の隔離ネットワーク誘導
- HBM 付き FPGA を利用した高スループット悪性通信検知システム

発表文献(主要成果として上記で詳細を報告した物のみ)

[1] 嶋田創, 蘇思遠, 長谷川皓一, 山口由紀子, "勾配情報変化量を利用した SVM ベースのマルウェア検知を標的にする中毒攻撃データの検知," 情報処理学会研究報告, Vol. 2022-CSEC-98, No. 19, pp. 1-8, 2022 年 7 月.

[2] 高木聖也, 長谷川皓一, 山口由紀子, 嶋田創, "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," 電子情報通信学会研究報告, Vol. 119, No. 288, ICSS2019-62, pp. 13-18, 2019 年 11 月.

[3] Yun Gao, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada, "Malware Detection using LightGBM with a Custom Logistic Loss Function," IEEE Access, pp. 47792-47804, DOI: 10.1109/ACCESS.2022.3171912, May 2022.

[4] Yun Gao, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada, "Malware Detection by Control-Flow Graph Level Representation Learning with Graph Isomorphism Network," IEEE Access, Vol. 10, pp. 111830-111841, DOI: 10.1109/ACCESS.2022.3215267, October 2022.

[5] Masahito Kumazaki, Yukiko Yamaguchi, Hajime Shimada, and Hirokazu Hasegawa, "WAF Signature Generation from Real-Time Information on the Web using Similarity to CVE," International Journal on Advances in Security, ISSN 1942-2636, Vol. 14, No. 1 and 2, pp. 26-36, December 2021.

[6] 辻知希, 嶋田創, 山口由紀子, 長谷川皓一, "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," 情報処理学会論文誌 Journal of Information Processing. Vol. 64, No. 5, pp. 1041-1052, 2023 年 5 月.

５．主な発表論文等

〔雑誌論文〕　計9件（うち査読付論文　9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 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 IPSJ 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 －

１．著者名 Shun Tobiyama, Yukiko Yamaguchi, Hirokazu Hasegawa, Hajime Shimada, Mitsuaki Akiyama, and Takeshi Yagi	４．巻 60
２．論文標題 Using Seq2Seq Model to Detect Infection Focusing on Behavioral Features of Processes	５．発行年 2019年
３．雑誌名 IPSJ Journal of Information Processing	６．最初と最後の頁 545-554
掲載論文のDOI（デジタルオブジェクト識別子） 10.2197/ipsjjip.27.545	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 辻知希，嶋田創，山口由紀子，長谷川皓一	４．巻 64
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 IPSJ Journal of Information Processing	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 Yun Gao, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada	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 EEE 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 Yun Gao, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada	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 WAF Signature Generation from Real-Time Information on the Web using Similarity to CVE	4．巻 14
2．論文標題 Masahito Kumazaki, Yukiko Yamaguchi, Hajime Shimada, and Hirokazu Hasegawa	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 14
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 Kazuki Koike, Ryotaro Kobayashi, Masahiko Katoh	4．巻 1
2．論文標題 IoT-Oriented High-Efficient Anti-Malware Hardware Focusing on Time Series Metadata Extractable from inside a Processor Core	5．発行年 2022年
3．雑誌名 International Journal of Information Security	6．最初と最後の頁 1-19
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10207-021-00577-0	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36件（うち招待講演　0件／うち国際学会　12件）

1．発表者名 Yun Gao, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada
2．発表標題 Malware Detection Using Gradient Boosting Decision Trees with Customized Log Loss Function
3．学会等名 In Proceedings of the 35th International Conference on Information Networking (ICOIN2021), pp. 273-278, January 2021,（国際学会）
4．発表年 2021年

1．発表者名 Masahito Kumazaki, Yukiko Yamaguchi, Hajime Shimada, and Hirokazu Hasegawa
2．発表標題 WAF Signature Generation with Real-Time Information on the Web
3．学会等名 In Proceeings of the 14th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2020), ISBN: 978-1-61208-821-1, pp. 40-45, November 2020.（国際学会）
4．発表年 2020年

1．発表者名 Otgonpurev Mendsaikhan, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada
2．発表標題 Automatic Mapping of Vulnerability Information to Adversary Techniques
3．学会等名 In Proceeings of the 14th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2020), ISBN: 978-1-61208-821-1, pp. 53-59, November 2020.（国際学会）
4．発表年 2020年

１．発表者名
Yun Gao, Hirokazu Hasegawa, Yukiko Yamaguchi, and 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，pp. 589-595，2020年10月

４．発表年
2020年

１．発表者名
白倉大河，長谷川皓一，山口由紀子，嶋田創

２．発表標題
国際化ドメイン名の自動リンク処理等におけるセキュリティリスクの検討

３．学会等名
コンピュータセキュリティシンポジウム2020，pp.29-36，2020年10月

４．発表年
2020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，L-001，pp. 131-132，2021年9月．

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
電子情報通信学会研究報告，Vol. 120，No. 384，ICSS2020-31，pp. 31-36，2021年3月．

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
電子情報通信学会研究報告，Vol．120，No．384，ICSS2020-32，pp．37-42，2021年3月．

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
電子情報通信学会研究報告，Vol．120，No．264，ICSS2020-22，pp．17-20，2020年11月．

４．発表年
2020年

１．発表者名
佐藤秀哉，林はるか，小林良太郎，

２．発表標題
組織内で学習データを採取し定期的に判別器を更新する機械学習ベースのNIDS，

３．学会等名
情報処理学会研究報告 Vol.2021-CSEC-92，No.58，pp.1-8，2021年3月

４．発表年
2020年

１．発表者名
林はるか，佐藤秀哉，小林良太郎，

２．発表標題
機械学習ベースのNIDSにおける動的な判別器生成に関する検討と予備評価，

３．学会等名
情報処理学会研究報告 Vol.2020-CSEC-91，No.21，pp.1-8，2020年11月

４．発表年
2020年

１．発表者名
佐藤秀哉，林はるか，小林良太郎，

２．発表標題
組織内ネットワークにおけるハニーポットを備えた動的な機械学習ベースのNIDSの作成と予備的評価，

３．学会等名
コンピュータセキュリティシンポジウム2020(CSS2020)，pp.88-93，2020年10月

４．発表年
2020年

１．発表者名
Ziwei Zhang, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada

２．発表標題
Rogue Wireless AP Detection using Delay Fluctuation in Backbone Network

３．学会等名
The 43rd Annual International Computers, Software and Applications Conference (COMPSAC 2019)(Fast Abstract)（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
Identification of Cybersecurity Specific Content Using the Doc2Vec Language Model

３．学会等名
The 43rd Annual International Computers, Software and Applications Conference (COMPSAC 2019)（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

４．発表年
2019年

１．発表者名
永井雄也，小林良太郎，加藤雅彦，嶋田創

２．発表標題
プロセッサ情報によるマルウェア検知機構における特徴量のビット数削減手法の検討

３．学会等名
コンピュータセキュリティシンポジウム2019

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
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
石川亮太，小林良太郎，加藤雅彦，嶋田創

２．発表標題
画像処理ベースのプログラム識別を目的としたプログラムの挙動の可視化に関する検討

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
2019年

１．発表者名
Ziwei Zhang, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada

２．発表標題
Rogue AP Detection using Similarity of Backbone Delay Fluctuation Histogram

３．学会等名
The 34th International Conference on Information Networking (ICOIN2020)（国際学会）

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

１．発表者名
金子尚史，嶋田創

２．発表標題
標的型攻撃演習シナリオの組み換えによる新規シナリオの機械生成の初期検討

３．学会等名
情報処理学会第82回全国大会

４．発表年
2020年

１．発表者名
篠田優，嶋田創，長谷川皓一，山口由紀子

２．発表標題
潜在表現の時系列差分を用いた亜種マルウェア検知精度向上の検討

３．学会等名
電子情報通信学会研究報告，Vol. 122，No. 86，ICSS2022-4，pp. 19-24

４．発表年
2022年

１．発表者名
嶋田創，蘇思遠，長谷川皓一，山口由紀子

２．発表標題
勾配情報変化量を利用したSVMベースのマルウェア検知を標的にする中毒攻撃データの検知

３．学会等名
情報処理学会研究報告，Vol．2022-CSEC-98，No．19，pp．1-8

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，pp．840-847

４．発表年
2022年

１．発表者名
辻知希，嶋田創，山口由紀子，長谷川皓一

２．発表標題
AndroidアプリのURL自動リンクにおけるフィッシングリスクの分析と対策の実装

３．学会等名
コンピュータセキュリティシンポジウム2022，pp．1194-1201

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
ユーザ信用度を考慮した動的アクセス制御遅延の環境差検証

３．学会等名
電子情報通信学会技術報告，Vol．122，No．306，IA2022-66，pp．91-98

４．発表年
2022年

１．発表者名
坂尾優斗，嶋田創

２．発表標題
SRv6による組織内ネットワークにおける攻撃由来通信の隔離ネットワーク誘導

３．学会等名
情報処理学会第85回全国大会予稿集，1ZA-03，pp．177-178

４．発表年
2023年

１．発表者名
熊谷僚太，嶋田創

２．発表標題
異種無線LAN構成におけるバックボーン遅延利用Rogue AP検出の追跡調査

３．学会等名
情報処理学会第85回全国大会予稿集，1ZA-06，pp．183-184

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
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
電子情報通信学会研究報告，Vol．122，No．422，ICSS2022-74，pp．157-162

４．発表年
2023年

１．発表者名
Zhenguo Hu, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada

２．発表標題
Towards Network-Wide Malicious Traffic Detection with Power-Effective Hardware NIDS Design

３．学会等名
In Proceedings of the 25th IEEE Symposium on Low-Power and High-Speed Chips (COOLChips 25), Poster 6, pp. 313-314（国際学会）

４．発表年
2022年

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

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
In Proceedings of the 12th IEEE International Workshop on Network Technologies for Security, Administration and Protection (NETSAP 2022), pp. 1495-1501, DOI: 10.1109/COMPSAC54236.2022.00237（国際学会）

４．発表年
2022年

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

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

３．学会等名
In Proceeings of the 16th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2022), ISBN: 978-1-68558-007-0, pp. 41-47（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
In Book of Abstract of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023), p. 25（国際学会）

４．発表年
2023年

１．発表者名
長谷川智祐，小林良太郎

２．発表標題
NIDSに対する中毒攻撃に関する調査及び詳細把握のための評価指標の導入

３．学会等名
コンピュータセキュリティシンポジウム2022，pp. 30-35

４．発表年
2022年

１．発表者名
Hideya Sato, Ryotaro Kobayashi

２．発表標題
Koga2022 Dataset: Dataset with Detailed Classification for Network Intrusion Detection Systems

３．学会等名
In Proceedings of the 9th International Workshop on Information and Communication Security (WICS 2022), pp. 351-357（国際学会）

４．発表年
2022年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
ネットワークセキュリティ関係の研究
https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/network_security.html
サイバーセキュリティ関係の研究
https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/cyber_security.html
ネットワーク関係の研究(攻撃検知用特徴量抽出話あり)
https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/network.html

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
研究分担者	小林　良太郎 (Kobayashi Ryotaro) (40324454)	工学院大学・情報学部（情報工学部）・教授 (32613)	
研究分担者	山口　由紀子 (Yamaguchi Yukiko) (90239921)	名古屋大学・情報基盤センター・助教 (13901)	
研究分担者	長谷川　皓一 (Hasegaw Hirokazu) (90806051)	国立情報学研究所・サイバーセキュリティ研究開発センター・特任准教授 (62615)	

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