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 １９ 日現在

機関番号：６２６１５
研究種目：若手研究
研究期間：2019～2023
課題番号：１９Ｋ２０２６８

研究課題名（和文）宛先の待受状態に着目した不正通信検出手法の開発とセキュアネットワーク構築への応用

研究課題名（英文）Development of a method for detecting suspicious communications based on the waiting state of the destination and its application to the construction of secure networks

研究代表者

長谷川　皓一（HASEGAWA, Hirokazu）

国立情報学研究所・ストラテジックサイバーレジリエンス研究開発センター・特任准教授

研究者番号：９０８０６０５１

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：昨今の深刻なサイバー攻撃に対し、組織のローカルネットワークにおいて効率的に不審通信を検出し、その対応、対策を行うための手法の研究を実施した。
ローカルネットワーク通信とその宛先端末の待機状態に着目し、不審な通信を検出、また、その結果を用いて、ローカルネットワーク内の不必要な通信を制限することにより、マルウェアの通信などを事前に抑制するセキュアなネットワーク構築可能となる成果を得た。
さらに、昨今の在宅勤務などを前提した社内ネットワークの利用形態を考慮し、VPN通信を実施するユーザの情報セキュリティ観点からの信頼度を評価し、個々人に応じて適切なアクセス制御構築を可能とする成果を得た。

研究成果の学術的意義や社会的意義
研究課題名にもしている、宛先の待機状態を活用することで組織内通信から不審な通信を検出する手法を提案し、これを発表した文献はBest Paper Awardの受賞などの評価を得た。
また、不正通信検出の新たな手法により、サイバー攻撃の検知向上の研究で貢献した。さらに、セキュリティレベルの高いネットワークの構築手法の実現により、サイバーセキュリティ一般に貢献した。
これらの成果は、社会問題となっているサイバー攻撃対策の一助となり得る成果である。

研究成果の概要（英文）：Due to the recent serious situation of cyber attacks, we researched methods for efficient detection, response, and countermeasures to suspicious communications in an organization's local network.
A method of detecting suspicious communication in local networks based on the state of the destination terminal of communication was proposed. In addition, by using the results of the method, we have achieved the construction of a secure network that can restrict malware communication in advance by restricting unnecessary communication within the local network.
Furthermore, considering the recent usage pattern of the company network based on the assumption of telecommuting, an access control construction method for VPN connection was proposed. It is based on the evaluation results about the information security perspective trust of each user, and we can obtain suitable access control for each user.

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

キーワード：サイバーセキュリティ　ネットワークセキュリティ　不正通信検知　マルウェア検知　SDN

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

近年、様々なサイバー攻撃が発生しており、巧妙な手法の攻撃により深刻な被害が発生する場合もある。これに対し、被害を防ぐための対策として、ネットワーク内の端末がマルウェアに感染した際に、迅速に感染端末を検出する必要がある。感染端末の検出手法は様々な研究開発が日々行われているが、攻撃者も検出を逃れる方法を探求しており、イタチごっこの状態である。

また、感染端末の検出後は、感染端末の隔離など速やかな対応の実施が求められる。しかしながら、検出した端末を単にネットワークから切り離した場合、当該の端末に関する業務継続は深刻な影響を被ることは自明であり、さらには、別の端末に感染が拡大していた場合、攻撃者に悟られ活動を隠蔽されるおそれがある。これらを考慮の上、ネットワーク管理者などは対応を決定する必要があり、大きな負担となっている。研究代表者らはこれまでにも、サイバー攻撃時の対応策を効果と業務継続性の観点から判断し管理者に推薦する手法を開発してきたが、最終的には管理者の判断に委ねるという点では、いまだ管理者の負担は大きいと言える。

２．研究の目的

昨今の巧妙なサイバー攻撃に対して、マルウェア感染が疑われる端末を検出し、対応、対策を速やかに実施する必要がある。本研究では、これらの活動を可能な限り効率的に実施し、管理者の負担を低減させるために、組織内部のローカルネットワークで行われる通信から不審なものを検出し、対応を行う手法を開発する。

本手法は、組織内部のネットワークにおいて行われる通信の宛先に着目し、宛先の端末の待受状態や応答通信を調べることにより、不審通信を検出するものである。さらに、この結果をもとに、不審と判定された通信を遮断することで、マルウェアの活動を抑制することを目指す。不審判定は、宛先の待受状態の結果、通信に対応するサービスを提供していない場合などが挙げられるが、これは、観測された通信がそもそも成立しないものであると考えられるため、当該の通信を遮断することによる業務継続への影響はわずか、もしくはないものと考えられる。また、これは、特定の不必要な通信をネットワーク内で禁止することとも同義であり、マルウェアに感染した際の不正な通信を未然に防ぐ効果があり、セキュアな内部ネットワークを構築することが可能となる。

３．研究の方法

本研究ではまず、組織内ネットワークにおける通信と宛先の待機状態を用いた不正通信検出手法を開発する。実際に業務で用いられるプロトコルや、それらの適切な待ち受け状態、通信が発生した際の適切なレスポンスを含めた正常挙動を分析し、その結果から外れたものを不正通信として検出可能かどうかを調査する。その結果を踏まえ、実際にシステム構築を行い、擬似的な攻撃通信を不正通信として検出可能かどうかなど、提案手法の制度や実現可能性を評価する。

その後、それまでに開発した不正通信検出手法をセキュアネットワーク構築へと応用する。実際にローカルネットワーク内において不正通信として検出された通信について、通信を行なった端末の特定を行い、SDN 技術などを用いて当該端末の通信を遮断するようにネットワークを動的に再構成する仕組みの構築を試みる。

４．研究成果

(I)宛先の待機状態を用いた不正通信検出手法の開発

組織内の通信をキャプチャし、通信の宛先と、ポートスキャンにより得られた宛先端末の待機状態を照合することにより、不正通信を検出する手法[1]を開発した。研究計画の段階においては、通信のレスポンスなど挙動の詳細分析をもとに構築する予定であったが、宛先の端末が通信に対応するサービスを待ち受けている状態であるか否かのみでも、一定の判定は可能であるという結果を実験から得たため、宛先の待機状態のみを活用し、不正通信の検出を行った。

この手法では、組織内の通信に対して宛先の状態との照合を行うが、全ての通信に対してこれを実施した場合システムに対して膨大な負荷となってしまう。そこで、研究代表者の過去の研究を活用し、事前にある程度のアクセス制御が構築されているネットワークを対象としている。その上で、アクセスが許可された用途と実際に行われている通信に差異がある場合などに、本手法を適用する形とすることで、負荷を軽減している。

10 台程度の小規模ではあるが、組織ネットワークを模した擬似環境を構築し、その環境下において擬似的な業務シナリオと擬似不正通信を混ぜた通信を行うことによる実験を実施した。その結果、正規通信は正しく判定できていた。一方で、一部の不正通信については、必要な正規通信であると誤判定する結果となった。これは、マルウェアに感染した端末がファイルを探索するような活動を模したシナリオを実施した際に、ファイル共有サーバにアクセス権限がない状態で通信を行った際などに発生した。原因は、宛先の待機状態との照合のみでは、有効なサービ

スを提供していることしか判定できないため、そのサービスに対する正当な権限を持つか否かまでは判定できないという点であった。これは、マルウェアによる活動に限らず、正規のユーザが意図せずに誤って行なってしまった通信なども含まれる。本研究では、このような意図しない不必要な通信も正規の通信以外と判定し遮断することでセキュアなネットワーク環境を構築することを目標としていたため、誤判定を可能な限り低減する仕組みが必要となった。

この課題を解決するために、新たに通信の統計情報を判定に加え、不正通信の判定精度を向上させた手法[2]を開発した。この手法は、先述した課題である、マルウェアによる不正通信や、正規ユーザによる意図しない通信を検出するため、これらの通信は正規の通信に比べて接続試行の量に有意な差があるという点に着目したものである。

この手法では、宛先 IP アドレス、ポート番号と送信元 IP アドレスの組みについて、通信を収集した期間においてどの程度の通信が発生したかを集計する。その上で、四分位範囲を用いた外れ値判定により極端に通信が少ない組みを導出し、それを不正通信として扱うものとしている。

30 台程度の規模に拡張した擬似環境において行った実験では、統計データを取得するために 30 分程度の通信を行った状態で提案手法による通信の判定を行ったところ、課題となっていた誤検知を回避し、適切な判定が行えることを確認した。

(II) VPN 接続ユーザに対する適切なアクセス制御適用手法の開発

VPN で組織内ネットワークに接続したユーザに対して、通常の組織内の通信よりも厳しいアクセス制限を行い、組織ネットワークのセキュリティを担保するための手法[3]を提案した。これは、COVID-19 の世界的な流行の影響から、在宅勤務などの遠隔地から組織ネットワークに接続して通信を行うという業務形態が爆発的に普及し、本研究課題の着手時とは組織ネットワークを取り巻く状況が異なるものとなったという背景によるものである。

VPN などの遠隔接続は、企業の管理部門によるシステム管理や監督がしづらくなり、セキュリティレベルが低下する恐れがある。一方で、在宅勤務を円滑に実施するためには、やみくもなセキュリティ強化で利便性を低下することは避ける必要がある。そこで本手法では、セキュリティ強化を行いつつ業務効率を可能な限り維持するアクセス制御を探求した。

本手法では、セキュリティの維持は、システムを扱う「人」に依存するという前提のもと、ユーザごとに「セキュリティの観点において，どれほど安全な対応ができているか」をスコア化した信用度を用いてアクセス制御を行った。これには、組織内で実施されるセキュリティ研修の受講状況、理解度テストの結果、Web フィルタリングの検知回数、管理端末のアップデート状況など、複数の指標を用いて定式化を行った。さらに、通信の宛先となるリソースの重要度（リソース自体がいかに重要なデータであるか、機密性などに応じて設定する）を用い、ユーザがあるリソースにアクセスする際に、ユーザの信頼度と宛先リソースの重要度からアクセス許可を判断する手法とした。なお、本報告書では詳細を省略するが、リソースの重要度をシステムが自動判定する手法の研究や、リソースに対するアクセス権限付与の判断に関する研究なども別途実施した。

提案手法に関して、クライアント数 11 台程度の擬似環境において、それぞれが外部の別クライアントから組織ネットワークに VPN 接続し、リモートデスクトップにより組織内リソースにアクセスするというシナリオの元で、接続が完了するまでの速度計測による実運用性の検証を行った。この実験では、アクセス制御に SDN スイッチを用いたため、クライアントが 1 台ずつ順に接続していく順次型、すべてが同時に接続する同時型のそれぞれにおいて、組織内ネットワークで特段通信が発生していない低負荷状態と異常に大きなトラフィックを発生させた状態の高負荷状態を試した。結果、表 1 に示すとおり、低負荷時については数秒以内に接続が完了しており、これは提案システムを用いない場合と大差ない値である。高負荷時においては、接続の所要時間が増大しており、業務効率への影響が懸念された。しかしながら、プログラムの実装方法によってはこれらの数値は著しく改善可能であることは確認できており、実運用性も問題ないと考えられる。

表 1. SMB 接続所要時間

複数接続	順次接続		同時接続	
対象	低負荷	高負荷	低負荷	高負荷
User 0	3.093	17.192	6.460	28.613
…	…	…	…	…
User 11	3.332	17.291	6.211	28.641
平均	3.186	17.214	5.966	26.622

主要な成果として上記の 2 項目について成果とその概要を示したが、本研究課題においては、様々な観点からの不正通信の検出やセキュアネットワークの構築のための技術として以下のような研究を実施した。

・プライバシーの配慮した悪性通信検知手法

・e-learning 習熟度を活用したセキュリティ対策構築手法
・社会情勢分析によるサイバーリスク推定手法
・複数拠点にまたがる組織における、拠点間の類似インシデントログを活用した攻撃検知手法
・検知したマルウェアの通信先を SDN により仮装環境へ誘導、分析対応する手法
・FPGA を用いた高スループットな不審通信検知手法
・AI を活用したアクセス制御構築手法

上記で詳細を報告した主要な発表文献

[1] Yuya Sato, Hirokazu Hasegawa, Hiroki Takakura, “An Evaluation on Feasibility of a Communication Classifying System,” The Thirteenth International Conference on Emerging Security Information, Systems and Technologies, pp.9-15, 2019.
[2] Hirokazu Hasegawa, Yuya Sato, Hiroki Takakura, “Construction of Secure Internal Network with Communication Classifying System Using Multiple Judgment Methods,” International Journal On Advances in Telecommunications, Vol.13, No.3&4, pp.21-32, 2020.
[3] Atsushi Shinoda, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada, Hiroki Takakura, “Feasibility Verification of Access Control System for Telecommuting by Users Reliability Calculation,” The 18th International Conference on Systems and Networks Communications, pp.16-22, 2023.

５．主な発表論文等

〔雑誌論文〕　計6件（うち査読付論文　6件／うち国際共著　0件／うちオープンアクセス　5件）

１．著者名 Zhenguo Hu, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada	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 16
２．論文標題 Malware 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 オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Zhenguo Hu, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada	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 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 Yun Gao, Hirokazu Hasegawa, Yukiko Yamaguchi, 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 Hirokazu Hasegawa, Yuya Sato, Hiroki Takakura	４．巻 13-3&4
２．論文標題 Construction of Secure Internal Network with Communication Classifying System Using Multiple Judgment Methods	５．発行年 2020年
３．雑誌名 The International Journal on Advances in Telecommunications	６．最初と最後の頁 21-32
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 －

〔学会発表〕　計37件（うち招待講演　0件／うち国際学会　19件）

１．発表者名 Justus von der Beek, Atsushi Shinoda, Hajime Shimada, Hirokazu Hasegawa
２．発表標題 On-Demand Clock Boosting for Secure Remote Work System
３．学会等名 In Proceedings of the 12th International Conference on Communications, Computation, Networks and Technologies (INNOV 2023), pp. 8-13（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 Verification of Access Control System for Telecommuting by Users Reliability Calculation
３．学会等名 In Proceedings of the Eighteenth International Conference on Systems and Networks Communications (ICSNC 2023), pp. 16-22（国際学会）
４．発表年 2023年

１．発表者名
Yuki Kodaka, Hirokazu Hasegawa, Hiroki Takakura

２．発表標題
Design and Implementation of Access Control Method Based on Correlation Among Files

３．学会等名
In proceedings of the 16th International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services (CENTRIC 2023), pp. 44-51 (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
In proceedings of the 17th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2023), pp. 27-32 (国際学会)

４．発表年
2023年

１．発表者名
Nader Shahata, Hirokazu Hasegawa, Hiroki Takakura

２．発表標題
AI-driven Approach for Access Control List Management

３．学会等名
In proceedings of the 17th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2023), pp. 52-58 (国際学会)

４．発表年
2023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
電子情報通信学会研究報告, Vol. 123, No. 448, pp. 153-159

４．発表年
2024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
電子情報通信学会研究報告，Vol．123，No．448，pp．79-84

４．発表年
2024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），pp．101-108

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．157-162，2023年3月．

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 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），Abstract Session，February 2023.（国際学会）

４．発表年
2023年

１．発表者名
Yuki Kodaka, Hirokazu Hasegawa, Hiroki Takakura

２．発表標題
Proposal for a Granular Access Control Method Based on Similarity of File Accesses Behavior Among Users

３．学会等名
The 9th International Conference on Information Systems Security and Privacy (ICISSP 2023), Abstract Session, February 2023.（国際学会）

４．発表年
2023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．91-98，2022年12月．

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．1194-1201，2022年10月．

４．発表年
2022年

１．発表者名
長谷川皓一，高倉弘喜

２．発表標題
e-learning習熟度を活用したセキュリティ対策強化の推薦手法に関する検討

３．学会等名
コンピュータセキュリティシンポジウム2022，pp．1093-1098，2022年10月．

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. 840-847，2022年10月.

４．発表年
2022年

１．発表者名
長谷川皓一，平井健士，高倉弘喜

２．発表標題
社会情勢分析によるサイバーリスク推定および防御構築支援

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. 92-96，2022年10月.

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
In Proceedings of the 16th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2022), ISBN: 978-1-68558-007-0, pp. 41-47, October 2022.（国際学会）

４．発表年
2022年

１．発表者名
Yingtao Zhou, Hirokazu Hasegawa, Hiroki Takakura

２．発表標題
A Resource Importance Estimation Method Based on Proximity of Hierarchical Position

３．学会等名
In Proceedings of the 5th International Conference on Information Science and Systems (ICISS2022), pp. 83-89, August 2022.（国際学会）

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. 1-8，2022年7月.

４．発表年
2022年

１．発表者名
Yun Gao，Hirokazu Hasegawa，Yukiko Yamaguchi，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，June 2022.（国際学会）

４．発表年
2022年

１．発表者名
篠田優，嶋田創，山口由紀子，長谷川皓一

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. 19-24，2022年6月.

４．発表年
2022年

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

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

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，April 2022.（国際学会）

４．発表年
2022年

１．発表者名
Yingtao Zhou, Hirokazu Hasegawa, Hiroki Takakura

２．発表標題
An Importance Estimation Method Based on Resource Lineage

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
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
小森工，嶋田創，長谷川皓一

２．発表標題
通信遮断による標的型攻撃対応のための影響範囲VR可視化システムの開発

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
Zhenguo Hu, Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada

２．発表標題
High-Performance Distributed NIDS Cluster Based on Hybrid Detection Platform

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
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
Proceedings of the 4th International Conference on Information Science and Systems (ICISS2021)（国際学会）

４．発表年
2021年

１．発表者名
Tomohiro Noda, Hirokazu Hasegawa, Hiroki Takakura

２．発表標題
Assessment System for Residual Risks of Information Leakage in Incident Countermeasures

３．学会等名
Proceedings of the 4th International Conference on Information Science and Systems (ICISS2021)（国際学会）

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
Proceedings of the 35th International Conference on Information Networking (ICOIN2021)（国際学会）

４．発表年
2021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
Proceedings of 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
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 第50回情報通信システムセキュリティ研究会（ICSS）

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 AP Detection using Similarity of Backbone Delay Fluctuation Histogram

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

４．発表年
2020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 第49回情報通信システムセキュリティ研究会（ICSS）

４．発表年
2019年

１．発表者名
Hajime Shimada, Katsutaka Ito, Hirokazu Hasegawa, Yukiko Yamaguchi

２．発表標題
Implementation of MQTT/CoAP Honeypots and Analysis of Observed Data

３．学会等名
Proceedings of the Thirteenth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2019)（国際学会）

４．発表年
2019年

１．発表者名
Yuya Sato, Hirokazu Hasegawa, Hiroki Takakura

２．発表標題
An Evaluation on Feasibility of a Communication Classifying System

３．学会等名
Proceedings of the Thirteenth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2019)（国際学会）

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 Wireless AP Detection using Delay Fluctuation in Backbone Network

３．学会等名
Proceedings of the 43rd Annual International Computers, Software and Applications Conference (COMPSAC 2019)（国際学会）

４．発表年
2019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