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　２ 年　 ６ 月　 ２ 日現在

機関番号：１４５０１
研究種目：基盤研究(B)（一般）
研究期間：2016～2019
課題番号：１６Ｈ０２８７４

研究課題名（和文）サイバー攻撃のリアルタイム検知・分類・可視化のためのオンライン学習方式

研究課題名（英文）Online Learning Algorithms for Real-time Detection, Classification, and Visualization of Cyberattacks

研究代表者
小澤　誠一（Ozawa, Seiichi）

神戸大学・数理・データサイエンスセンター・教授

研究者番号：７０２１４１２９

交付決定額（研究期間全体）：（直接経費）　　10,200,000円

研究成果の概要（和文）：本研究では，時々刻々と進化するサイバー攻撃に追従しながら，大規模ダークネット（未使用IPアドレス群）センサで観測される通信パケットから，サイバー攻撃の検知・分類・可視化を持続的に行えるオンライン学習方式と3種類の学習型攻撃監視システムを提案した．一つ目はDDoSバックスキャッタ監視システムであり，通信トラフィック特徴をサポートベクトルマシンや深層学習を組み合わせて適用し，97%以上の検知精度と高速学習特性を実現した．また，相関ルールマイニングやポート番号の埋込ベクトル学習によって，未知のサイバー脅威の検知やマルウェアの振る舞いの変化などを監視できる画期的なシステムを開発した．

研究成果の学術的意義や社会的意義
金融資産や知的財産などを狙ったサイバー攻撃の手口は年々巧妙化し，深刻な被害をもたらしている．新たなサイバー脅威の検出や分析を速やかに行い，損失を最小限に抑える仕組み作りが強く求められているが，サイバー攻撃に対する知識とスキルをもつ専門家は限られている．このような状況を打開するため，本研究では，機械学習を導入して，これまで専門家が担ってきたサイバー攻撃の監視や分析の一部を自動化することで，攻撃者に対抗する手段を提供する点で社会的意義の高い研究である．また，未知のサイバー攻撃に対して，持続的に性能改善できるよう，専門家を介在させたオンライン学習には，学術的に意義の高い研究である．

研究成果の概要（英文）：In this project, we have proposed several online learning algorithms to continuously perform the detection, classification, and visualization of cyberattacks by analyzing communication packets observed by a large-scale darknet (i.e., unused IP address range) sensor, while following the ever-evolving cyberattacks. In addition, we have developed three types of adaptive attack-monitoring systems. The first is a DDoS backscatter monitoring system, which applies communication traffic features in combination with support vector machines and deep neural networks to achieve detection accuracy of 97% or more and high-speed learning characteristics. Moreover, we have developed a new type of cyberattack monitoring systems that can detect unknown cyber-threats and monitor changing behaviors of malware by association rule mining and the representation learning of port-number embedding.

研究分野：知能情報学

キーワード：機械学習　サイバーセキュリティ　攻撃検知　攻撃分類　攻撃可視化　追加学習　相関ルールマイニング　深層学習

様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

(1) 金融資産や知的財産などを狙ったサイバー攻撃の手口は年々巧妙化し，深刻な被害をもたらしている．サイバー攻撃からユーザを守る手段としては，セキュリティ対策ソフトの導入や OS，アプリケーションソフトのアップデートが基本であるが，脆弱性を狙った新しいサイバー攻撃の出現に対策が追い付かないのが現状である．新たなサイバー脅威の検出や分析を速やかに行い，損失を最小限に抑える仕組み作りが強く求められているが，サイバー攻撃に対する知識とスキルをもつ専門家は限られている．そこで，機械学習を導入して，これまで専門家が担ってきたサイバー攻撃の監視や分析の一部を自動化する試みが注目されている．

(2)インターネット上のサイバー攻撃を広域監視する仕組みとして，「ダークネット」と呼ばれる未使用 IP アドレスの空間を利用する方法がある．ダークネットは応答を返さないパッシブなセンサネットで，取得できる情報は限られるが，攻撃者から見えないため，サイバー攻撃でやり取りされる通信トラフィックを持続的に収集できる．従来研究には，既知のスパムボットと同期して観測されるダークネットトラフィックに基づき，仕掛けたスパムトラップで受信されるパケット情報からスパムボットのタイプを判定する機械学習手法の提案や，ダークネット観測を通して，ワームの振る舞い（感染スピードや感染手順）を最尤推定法で予測する手法が提案されている．これら従来研究の多くは，ラベル付けされた訓練データを前提に識別器をバッチ学習し，判定や分類が行われる．よって，未知のマルウェアを検出したり，持続的に追従したりすることは難しい．また，一定期間の通信トラフィックを静的な空間パターンに変換して学習・判定するものがほとんどであり，通信トラフィックの時間構造を陽に学習するアプローチは限られている．トラフィックの時間構造には，攻撃プロセスを特徴づける情報が含まれているはずで，この特徴を陽に学習することで高精度な攻撃分類が可能になると考えられる．

２．研究の目的

本研究では，国立研究開発法人 情報通信研究機構（以下，NICT）がもつ大規模ダークネットで観測された通信パケットを観測し，その通信トラフィックに基づいてサイバー攻撃の検知・分類・可視化を行い，新たな攻撃に追従できるオンライン学習方式の開発を行う．具体的には，次の 2 つの小課題に分け，機械学習とサイバーセキュリティの専門家が協同して研究を実施する．

(1)サイバー攻撃広域観測システムの構築

図 1 にダークネットを使ったサイバー攻撃の広域観測の様子を示す．ダークネットで観測可能な攻撃には，スキャン，DDoS，マルウェアによる感染行為などがあり，これまでスキャン攻撃と DDoS 攻撃に対してサポートベクターマシン(SVM)を導入した攻撃の検知・分類システムを開発し，t-Distributed Stochastic Neighbor Embedding (t-SNE)を用いた攻撃の可視化を行ってきた．しかし，スキャン攻撃か DDoS 攻撃かの判定しかできず，例えば SYN flood や DNS アンプといった攻撃タイプ別に分類できていない．また，スキャン攻撃についても，どのようなマルウェアがどのような脆弱性を探索しているかの傾向を捉えるには至っていない．そこで本研究では，機械学習を導入して，詳細な攻撃の分類や可視化を可能とする観測システムを構築する．

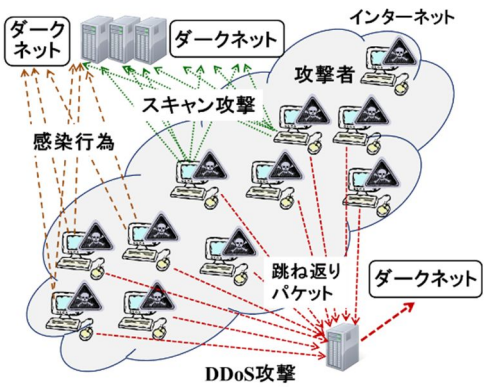

図1　ダークネットによるサイバー攻撃の監視

(2)オンライン学習を導入したサイバー攻撃の検知・分類・可視化手法の確立

(1)で構築される広域観測システムは，外れ値検出による新しい攻撃の検知，攻撃の分類，攻撃の可視化の 3 つのパートで構成される．これまで，外れ値検出には 1 クラス SVM，攻撃の分類と可視化には，それぞれ L2-SVM と t-SNE を用いてきた．しかし，いずれも一括学習型の識別器モデルであるため，膨大な通信パケットが観測されるダークネットに対して，実運用可能な時間で学習可能かどうかは自明でない．本研究では，上記 3 つのパートに対するオンライン学習アルゴリズムを開発し，その効果を実データで実証する．

３．研究の方法

(1) 追加学習型 DDoS バックスキャッタ監視システム

DDoS（Distributed Denial of Service）攻撃は特定ホストに一斉に大量のパケットを送りつけサービス停止に追い込むサイバー攻撃である．DDoS 攻撃を行うホストは IP を詐称してパケットを送るため，被害ホストは詐称された IP アドレスに返信を行い，その返信パケットの一部がダークネットで観測される．この返信パケットはバックスキャッタと呼ばれ，このトラフィックパターンに基づいて DDoS 攻撃のイベント検知が可能になる．図 2 に追加学習型 DDoS バックスキャッタ監視システムの検知フローを示す．

訓練フェーズでは，ダークネットで観測されたトラフィックデータをホストごとに整理し，設定した時間間隔内のパケットから，以下の 17 個の特徴を求める．

パケット総数，パケット間の時間間隔の平均・分散，送信元ポートの総数，
送信元ポートごとの送信されたパケット数の平均・分散，プロトコルの種類数，
送信先 IP アドレスの総数，送信先 IP アドレスごとの送信されたパケット数の平均・分散，
パケット間の送信先 IP アドレスの差分の平均・分散，送信先ポートの総数，
送信先ポートごとの送信されたパケット数の平均・分散，ペイロードの平均・分散

図 2 より，まずシグネチャーによる DDoS 判定が行われ，合致するルールがない場合のみ特徴ベクトルの作成が行われる．その後，1 クラス SVM により外れ値検出が行われ，外れ値と判定された場合は監視者の目視判定の結果をクラスラベルとして追加学習が行われる．一方，外れ値でない場合は SVM 識別器による DDoS 判定が行われ，判定の確信度が高いときは識別器の判定を採用し，低いときは監視者による目視判定が行わる．そして，この場合も監視者の判定結果をクラスラベルとして追加学習する．このように，機械学習による判定が難しい場合，セキュリティ専門家が検知フローに介在して正解を教示するオンライン学習を導入することで，信頼性の高い攻撃判定を持続的に実現する．

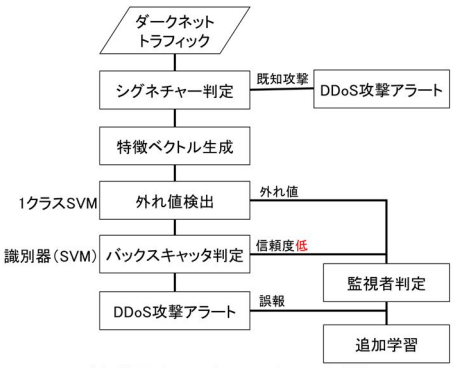

図2 追加学習型DDoSバックスキャッタ検知フロー

(2) 追加学習型 DDoS バックスキャッタ監視システムの高度化

(1)の監視システムでは，送信元ホストから送出されるパケットのトラフィック特徴に基づいて検知が行われるが、UDP 通信の場合など，これだけでは判定がむずかしい場合もある．そこで，従来の 17 個の通信トラフィック特徴に加えて、図 3 に示す「タイル」と呼ばれる通信トラフィックを可視化した画像特徴を追加する．具体的には，タイル画像を畳込みニューラルネットで学習し，最終特徴層 126 ユニットの内部表現を 17 個のトラフィック特徴に結合して 143 次元特徴ベクトルとし，これに最終結合層を与えて深層学習識別器を構成する．

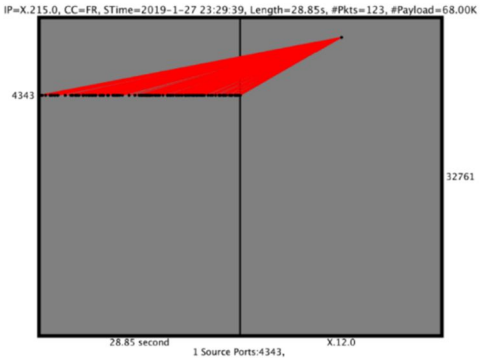

図3 タイルによる通信トラフィックの可視化

(3) 相関ルール解析を用いたネットワークスキャン観測の高度化

相関ルール解析システムにおける処理フローを図 4 に示す．提案システムは，相関ルール学習と詳細解析の 2 つのフェーズで構成され，相関ルール学習フェーズでは，スキャン活動の調査を行うため，ダークネットトラッフィックデータの TCP 制御フラグが SYN であるパケットを抽出する．そして，トランザクションを作成するが，まず得られたスキャンパケットを 24 時間ごとに分け，送信元 IP アドレスにしたがってトランザクション ID を与える．このトランザクションから FP-tree を作成し，FP-growth アルゴリズムを実行することで頻出パターンを抽出し，相関ルールの学習を行う．

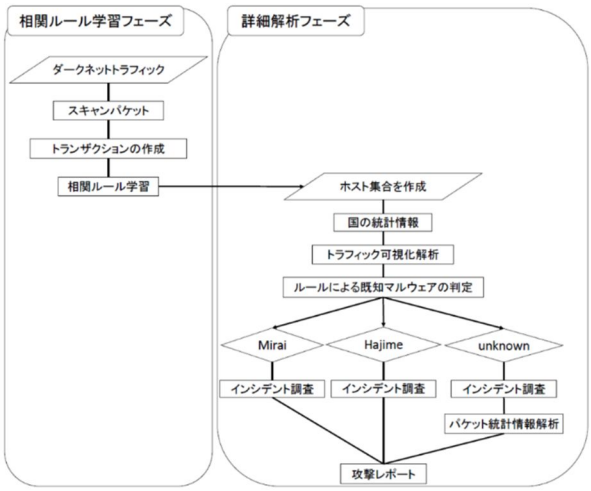

図4 相関ルール解析を用いたネットワークスキャン観測システム

詳細解析フェーズでは，まず相関ルール学習で得られたルールに適合するホスト集合を作成し，IP アドレスから WHOIS コマンドや GeoIP と呼ばれる検索ツールを利用して，送信元ホストの国や地域を調べる．そして，図 3 に示した「タイル」と呼ばれるトラフィックの可視化手法を用いて，スキャン活動の特徴を分析する．

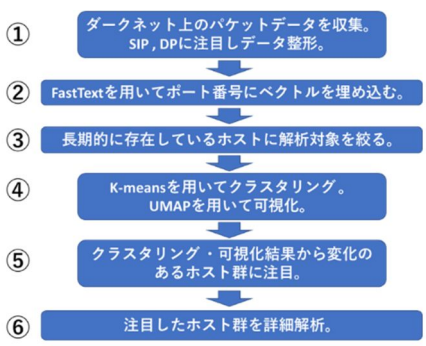

図5 Port Embeddingを用いたボットネット追跡

(4) スキャン攻撃分類に基づくボットネット検知

提案するスキャン攻撃分類に基づくボットネット追跡フローを図 5 に示す．まず，送信元ホストから送出される TCP SYN パケットから宛先ポート番号を抽出し、このポート番号の集合をドキュメントと捉えて、テキス

トマニングで使われる FastText による, 宛先ポートの共起性に基づいた Port 埋込ベクトルを得る．この埋込ベクトルを *k*-平均クラスタリングで分類し、類似したスキャン攻撃を行っているホスト群を特定して、それらを追跡しながらボットネットを可視化する．

４．研究成果

(1)サイバー攻撃広域観測システムの構築

NICT が所有する/16 ダークネットセンサによって，2016 年 1 月 1 日から 12 月 31 日までの 1 年間に観測された通信パケットを使用した．3-(1)で述べた 17 個の特徴量を送信元ホストごとに求めるが，その際に対象とするパケット列の長さは 30 秒～3600 秒の範囲で 30 秒間隔ごとに異なる時間ウィンドウを設定し，時間ウィンドウ内で 20 パケット以上を観測したものすべてとした．これによって，持続時間の短い攻撃からゆっくり持続する攻撃までを検知対象とすることができる．なお，図 2 の DDoS シグネチャーとして，送信元ホストからのパケットが TCP/80, UDP/53，TCP SYN，UDP Bit Torrent Protocol のいずれかのみで構成されるケースを考え，このケースでは，特徴ベクトルの生成を行わず DDoS バックスキャッタと判定する．よって，このケースを除いて実際に生成された特徴ベクトルを検知対象として性能評価を行った．性能評価に使用した特徴データセット数を表 1 に示す．

1 年間にわたって DDoS バックスキャッタ判定を行い，その平均検知精度を表 2 に示す．適合率（判定が正しい割合），再現率（DDoS を見逃さない割合）ともに高い精度を維持できており，外れ値や識別信頼度が低いケースで監視者による教示を与えることで安定した性能が得られることが実証された．また，監視者が目視確認した一日当たりの平均回数は，TCP と UDP それぞれで 46.7 回，17.2 回であった．これは，表 1 の 1 日平均データ数と比べれば，TCP で約 6%，UDP で約 0.3%と非常に少なく，提案システムを導入することで監視者の労力がかなり軽減されることがわかる．また，追加学習に要する時間も 1 日当たり 12 分程度であり，汎用のデスクトップパソコンで十分に運用可能である．

以上より，開発したサイバー攻撃広域観測システムは実用に耐え得るシステムと言える．

表１ 性能評価実験に用いたダークネットトラフィックデータ

データセット		データ数	1 日平均
TCP	バックスキャッタ	161,090	497.2
	非バックスキャッタ	94,527	291.8
UDP	バックスキャッタ	8,140	25.1
	非バックスキャッタ	1,776,531	5483.1

表 2　DDoS バックスキャッタ判定の年間平均検知精度．監視者データ数と計算時間は 1 日当たりの平均値

	適合率	再現率	F 値	確認回数	学習時間(秒)
TCP	0.974	0.980	0.977	46.7	209.9
UDP	0.927	0.808	0.904	17.2	502.4

(2) 追加学習型 DDoS バックスキャッタ監視システムの高度化

/16 ダークネットセンサにおいて，2019 年 1 月 1 日から 1 月 15 日までに観測された UDP パケットを学習し、その後、2 月 28 日までバックスキャッタ判定と低信頼度判定に対する追加学習を行ったときの性能評価を行った．その結果、表 3 に示す検知性能が得られた．これからわかるように，17 個のトラフィック特徴量のみで検知する場合に比べ，タイル画像特徴を加えることで，0.052 ポイントの性能改善が得られ、F 値は 0.976 となり、UDP 通信に対する DDoS バックスキャッタ検知も，ほぼ実用レベルに達したと言える．

表 3　深層学習を導入した追加学習型 DDoS バックスキャッタ監視システムの UDP 通信に対する性能評価

	適合率	再現率	F 値
トラフィック特徴	0.938	0.818	0.924
タイル画像特徴	0.783	0.981	0.869
ﾄﾗﾌｨｯｸ＋ﾀｲﾙ画像特徴	0.976	0.976	0.976

(3) 相関ルール解析を用いたネットワークスキャン観測の高度化

NICT の/16 ダークネットセンサで観測された 2016 年 7 月 1 日から 2018 年 12 月 31 日までの 30 ヶ月間，1 億以上のホスト IP アドレス から送信された 32,341,827,204 個の TCP/SYN パケットを解析した．これらのパケットを 1 日単位でホストごとに分割し，IP と TCP のヘッダに対してトランザクションを作成し，最低支持数 1000（最低ホスト数 1000），最低確信度 90%の条件で相関ルール解析を行った．その結果，TCP ヘッダ領域の送信先ポート番号，TCP ウィンドウサイズ，IP ヘッダ領域のパケット優先度を表す Type of Service (ToS)の 3 つのヘッダ情報について，IoT マルウェアである Mirai に関連した興味深い相関ルールが出現した．

2016 年 7 月 1 日から 2016 年 10 月 30 日までの期間に注目する．セキュリティレポートによると，この時期に Mirai が初めて出現したとされ，Mirai のシグネチャーをもつ通信の送信先ポート，TCP ウィンドウサイズ，ToS に相関ルールが出現した．図 6 は，それらの 3 つの相関ルールをもつホスト数の推移を示している．これらの中で最も興味深いのは， TCP ウィンドウサイズに関して得られた (1320, 2376→792) のルールであり，このルールは 8/2 に出現し，コミュニティフォーラムで Mirai ソースコードが公開されたとされる 9/4 までの間，約 37,000 ホストからの通信がこのルールに適合した．一方，送信先ポート番号と ToS に関するルールは，それぞれ 9 月初旬に出現し，このルールが出現したホストの振舞いは GitHub で公開された Mirai のシグネチャーに一致していた．このことから，. 8 月中に Mirai 開発者がプロトタイプを試行的に運用した後，TCP ウィンドウサイズのランダム化と TCP/2323 の送信先ポートへの追加を行って，ダークウェブのフォーラムにソースコードを投稿したのではないかと推測される．この裏付けは取れていないが，重要なことは，開発した相関ルール解析によって，一世を風靡した最強の IoT マルウェアの出現を予測できたかもしれないことである．

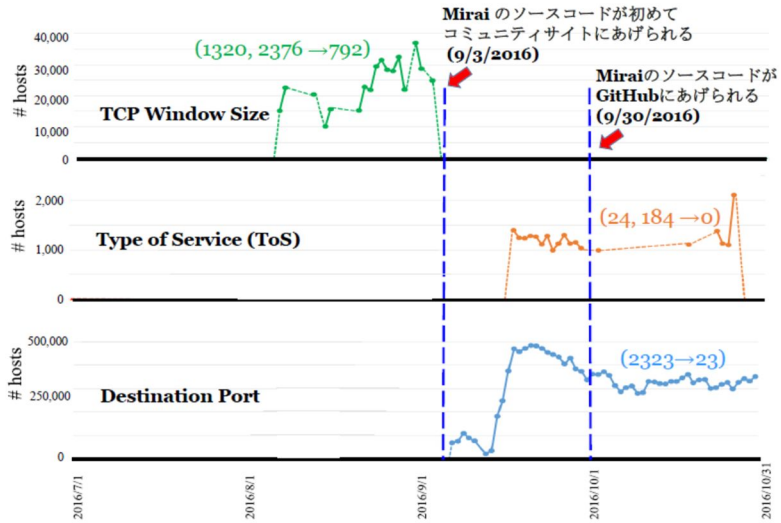

図 6　Mirai 出現期に現れた相関ルールの推移

また，この相関ルール解析により，Mirai やその亜種，さらに Hajime と呼ばれる新しい IoT マルウェアのスキャン行為を相関ルールのかたちで抽出し，その推移を観測することができる．図 7 にその結果を示す．

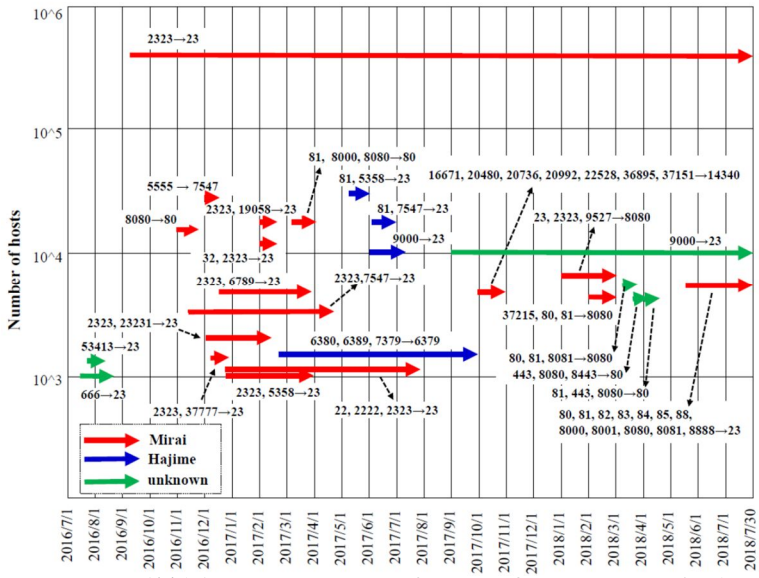

図 7　送信先ポートに関して出現した相関ルールの変遷

(4) スキャン攻撃分類に基づくボットネット検知

2020 年 1 月 30 日から 2 月 1 日の 3 日間において NICT /16 ダークネットセンサで観測された約 50 万ホストの TCP SYN パケットに対し，宛先ポートの共起性に基づいた Port 埋込ベクトルを求め, 類似したスキャン攻撃を行っているホスト群を k-平均クラスタリングで分類した．そして，これらクラスターで表されるホスト群の IP から WHOIS 情報などを用いて、国情報や組織情報，使用ポートセットなどを調べたところ共通点が見られ，さらに IoT マルウェアである Mirai への感染が疑われるホスト群（ボットネット）を確認した．

５．主な発表論文等

〔雑誌論文〕　計14件（うち査読付論文　14件／うち国際共著　4件／うちオープンアクセス　6件）

１．著者名 Kim Sangwook、Omori Masahiro、Hayashi Takuya、Omori Toshiaki、Wang Lihua、Ozawa Seiichi	４．巻 11304
２．論文標題 Privacy-Preserving Naive Bayes Classification Using Fully Homomorphic Encryption	５．発行年 2018年
３．雑誌名 Neural Information Processing. ICONIP 2018. Lecture Notes in Computer Science	６．最初と最後の頁 349～358
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-030-04212-7_30	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 Ndichu Samuel、Ozawa Seiichi、Misu Takeshi、Okada Kouichirou	４．巻 1
２．論文標題 A Machine Learning Approach to Malicious JavaScript Detection using Fixed Length Vector Representation	５．発行年 2018年
３．雑誌名 Proc. of 2018 International Joint Conference on Neural Networks	６．最初と最後の頁 1-7
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/IJCNN.2018.8489414	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 Hashimoto Naoki、Ozawa Seiichi、Ban Tao、Nakazato Junji、Shimamura Jumpei	４．巻 144
２．論文標題 A Darknet Traffic Analysis for IoT Malwares Using Association Rule Learning	５．発行年 2018年
３．雑誌名 Procedia Computer Science	６．最初と最後の頁 118～123
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1016/j.procs.2018.10.511	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 Skrjanc Igor、Ozawa Seiichi、Ban Tao、Dovzan Dejan	４．巻 62
２．論文標題 Large-scale Cyber Attacks Monitoring Using Evolving Cauchy Possibilistic Clustering	５．発行年 2018年
３．雑誌名 Applied Soft Computing	６．最初と最後の頁 592～601
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.asoc.2017.11.008	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 該当する

1．著者名 Kawaguchi Yuki、Yamada Akira、Ozawa Seiichi	4．巻 1
2．論文標題 AI Web-Contents Analyzer for Monitoring Underground Marketplace	5．発行年 2017年
3．雑誌名 ICONIP 2017: Neural Information Processing	6．最初と最後の頁 888～896
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-70139-4_90	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 Kuri Shohei、Hayashi Takuya、Omori Toshiaki、Ozawa Seiichi、Aono Yoshinori、Phong Le Trieu、Wang Lihua、Moriai Shiho	4．巻 1
2．論文標題 Privacy preserving extreme learning machine using additively homomorphic encryption	5．発行年 2017年
3．雑誌名 Proc. of The 2017 IEEE Symposium Series on Computational Intelligence	6．最初と最後の頁 1350～1357
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/SSCI.2017.8285190	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 Skrjanc Igor、Ozawa Seiichi、Dovzan Dejan、Tao Ban、Nakazato Junji、Shimamura Jumpei	4．巻 1
2．論文標題 Evolving cauchy possibilistic clustering and its application to large-scale cyberattack monitoring	5．発行年 2017年
3．雑誌名 Proc. of The 2017 IEEE Symposium Series on Computational Intelligence	6．最初と最後の頁 2833～2839
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/SSCI.2017.8285203	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 該当する

1．著者名 Rogovschi Nicoleta、Kitazono Jun、Grozavu Nistor、Omori Toshiaki、Ozawa Seiichi	4．巻 1
2．論文標題 t-Distributed stochastic neighbor embedding spectral clustering	5．発行年 2017年
3．雑誌名 Proc. of 2017 International Joint Conference on Neural Networks	6．最初と最後の頁 1628～1632
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/IJCNN.2017.7966046	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 該当する

1．著者名	4．巻
S. H. A. Ali, S. Ozawa, T. Ban, J. Nakazato and J. Shimamura	1
2．論文標題	5．発行年
A neural network model for detecting DDoS attacks using darknet traffic features	2016年
3．雑誌名	6．最初と最後の頁
2016 International Joint Conference on Neural Networks	2979-2985
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1109/IJCNN.2016.7727577	有
オープンアクセス	国際共著
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	－

1．著者名	4．巻
Siti Hajar Aminah Ali, Kiminori Fukase, Seiichi Ozawa	7
2．論文標題	5．発行年
A Fast Online Learning Algorithm of Radial Basis Function Network with Locality Sensitive Hashing	2016年
3．雑誌名	6．最初と最後の頁
Evolving Systems	173-186
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1007/s12530-015-9141-5	有
オープンアクセス	国際共著
オープンアクセスとしている（また、その予定である）	－

1．著者名	4．巻
Murata Naoki、Kitazono Jun、Ozawa Seiichi	1
2．論文標題	5．発行年
Multidimensional Unfolding Based on Stochastic Neighbor Relationship	2017年
3．雑誌名	6．最初と最後の頁
Proceedings of the 9th International Conference on Machine Learning and Computing	248-252
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
https://doi.org/10.1145/3055635.3056586	有
オープンアクセス	国際共著
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	－

1．著者名	4．巻
Jun Kitazono, Nistor Grozavu, Nicoleta Rogovschi, Toshiaki Omori, Seiichi Ozawa	3
2．論文標題	5．発行年
t-Distributed Stochastic Neighbor Embedding with Inhomogeneous Degrees of Freedom	2016年
3．雑誌名	6．最初と最後の頁
ICONIP 2016: Neural Information Processing	119-128
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1007/978-3-319-46675-0_14	有
オープンアクセス	国際共著
オープンアクセスとしている（また、その予定である）	該当する

1．著者名 Narutaka Awaya, Jun Kitazono, Toshiaki Omori, Seiichi Ozawa	4．巻 1
2．論文標題 Stochastic Collapsed Variational Bayesian Inference for Biterm Topic Model	5．発行年 2016年
3．雑誌名 2016 International Joint Conference on Neural Networks	6．最初と最後の頁 3364-3370
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/IJCNN.2016.7727629	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 Seiichi Ozawa, Shun Yoshida, Jun Kitazono, Takahiro Sugawara and Tatsuya Haga	4．巻 1
2．論文標題 A Sentiment Polarity Prediction Model Using Transfer Learning and Its Application to SNS Flaming Event Detection	5．発行年 2016年
3．雑誌名 2016 IEEE Symposium Series on Computational Intelligence	6．最初と最後の頁 1-7
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/SSCI.2016.7849868	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33件（うち招待講演　23件／うち国際学会　11件）

1．発表者名 Sangwook Kim, Toshiaki Omori, Masahiro Omori, Takuya Hayashi, Lihua Wang, Seiichi Ozawa
2．発表標題 Privacy-Preserving Naive Bayes Classifier based on Homomorphic Encryption
3．学会等名 The 13th International Workshop on Security（国際学会）
4．発表年 2018年

1．発表者名 Samuel Ndichu, Sangwook Kim, Seiichi Ozawa, Misu Takeshi, Kazuo Makishima
2．発表標題 Detection of JavaScript-based Attacks Using Doc2Vec Feature Learning
3．学会等名 The 13th International Workshop on Security（国際学会）
4．発表年 2018年

１．発表者名
小澤誠一

２．発表標題
AI×セキュリティの現状と期待

３．学会等名
SICE 第6回制御部門マルチシンポジウム（招待講演）

４．発表年
2019年

１．発表者名
小澤誠一

２．発表標題
セキュリティ分野におけるAI活用の現状と期待

３．学会等名
第30回AIセミナー，産総研人工知能研究センター（招待講演）

４．発表年
2019年

１．発表者名
Seiichi Ozawa

２．発表標題
Challenges and Expectations against AI in Security

３．学会等名
2018 Artificial Intelligence and Cloud Computing Conference（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
小澤誠一

２．発表標題
AIのAIによるAIのためのセキュリティ：セキュリティ×AIの現状と期待

３．学会等名
SICE 制御技術部会研究会講演（招待講演）

４．発表年
2018年

１．発表者名
小澤誠一

２．発表標題
セキュリティ分野におけるAIへの期待と現状

３．学会等名
AC・Net研究会（招待講演）

４．発表年
2018年

１．発表者名
小澤誠一

２．発表標題
AIの躍進の背景と最新技術動向

３．学会等名
兵庫エレクトロニクス研究会（招待講演）

４．発表年
2018年

１．発表者名
Seiichi Ozawa

２．発表標題
"A New Direction of Machine Learning: Privacy-Preserving Data Mining (PPDM)

３．学会等名
BESK Workshop（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
Seiichi Ozawa

２．発表標題
A Machine Learning Approach to Privacy-Preserving Data Mining Using Homomorphic Encryption

３．学会等名
AI Flagship Project Workshop（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
小澤誠一

２．発表標題
AI・機械学習の基礎と広がるAI応用

３．学会等名
2018年AI・機械学習シンポジウム（招待講演）

４．発表年
2018年

１．発表者名
小澤誠一

２．発表標題
サイバー攻撃対策としてのAIへの期待と現状

３．学会等名
SCSK講演（招待講演）

４．発表年
2018年

１．発表者名
小澤誠一

２．発表標題
人工知能技術の基礎と応用

３．学会等名
KansAI0.6 事業開発講座（招待講演）

４．発表年
2018年

１．発表者名
小澤誠一

２．発表標題
AI・機械学習における 各種手法・技術と適用の ポイント・事例

３．学会等名
日本テクノセンターセミナー（招待講演）

４．発表年
2017年

１．発表者名
川口雄已，山田明，小澤誠一

２．発表標題
匿名ネットワークTorにおけるマーケット商品とセキュリティ事件との関連性に関する考察

３．学会等名
情報処理学会コンピュータセキュリティシンポジウム 2017

４．発表年
2017年

１．発表者名
橋本直輝，小澤 誠一，班涛，中里純二，島村隼平

２．発表標題
ダークネットトラフィックデータの頻出パターン解析

３．学会等名
情報処理学会コンピュータセキュリティシンポジウム 2017

４．発表年
2017年

１．発表者名
Seiichi Ozawa

２．発表標題
A Brief Introduction to Data Science Center and Research Topics on Machine Learning for Big Data

３．学会等名
2nd Bilateral Workshop on Research Exchange between National Taiwan University and Kobe University（招待講演）（国際学会）

４．発表年
2017年

１．発表者名
Seiichi Ozawa

２．発表標題
Recent Challenges to Cybersecurity and Privacy-Preserving Data Mining Using Machine Learning

３．学会等名
Nanyang Technological University and Kobe University Workshop on Data Science（招待講演）（国際学会）

４．発表年
2017年

１．発表者名
小澤誠一

２．発表標題
AI・機械学習の観点からの 次世代セキュリティ

３．学会等名
第4回ASF次世代セキュリティシンポジウム（招待講演）

４．発表年
2017年

１．発表者名
小澤誠一

２．発表標題
機械学習によるサイバーセキュリティとプライバシー保護データマイニングへの取組み

３．学会等名
NICT サイバーセキュリティシンポジウム（招待講演）

４．発表年
2018年

１．発表者名
小澤誠一

２．発表標題
人工知能分野における最新の研究・技術動向

３．学会等名
データサイエンスセミナー（招待講演）

４．発表年
2018年

１．発表者名
小澤誠一

２．発表標題
なぜ『セキュリティ×機械学習』？

３．学会等名
第45回　SICE知能システムシンポジウム（招待講演）

４．発表年
2018年

１．発表者名
Seiichi Ozawa

２．発表標題
Collecting Cybersecurity-related Contents in Dark Web

３．学会等名
The 2nd Nanyang Technological University and Kobe University Workshop on Data Science and Artificail Intelligence（国際学会）

４．発表年
2018年

１．発表者名
小澤誠一

２．発表標題
万能でないAIのサイバーセキュリティでの活かし方

３．学会等名
AIセキュリティ最前線2018（招待講演）

４．発表年
2018年

１．発表者名
Seiichi Ozawa

２．発表標題
SNS Flaming Event Detection Based on Sentiment Polarity Prediction with Transfer Learning

３．学会等名
IEEE/INNS 2017 International Joint Conference on Neural Networks（招待講演）（国際学会）

４．発表年
2017年

１．発表者名
Nicoleta Rogovschi, Nistor Grozavu,Youn`es Bennani, Seiichi Ozawa

２．発表標題
t-Distributed Stochastic Neighbor Embedding based Self Organizing Maps

３．学会等名
61st ISI World Statistics Congress（国際学会）

４．発表年
2017年

１．発表者名
小澤誠一

２．発表標題
IoTとサイバーフィジカルシステムを知能化するAI技術の動向

３．学会等名
M2M・IoT研究会 関西部会第4回 技術研究講演会（招待講演）

４．発表年
2017年

１．発表者名
Sammie Ndichu Wangar、小澤誠一、三須剛史、岡田晃市郎

２．発表標題
Detection of Malicious JavaScript Contents Using Doc2vec Feature Learning

３．学会等名
2018年暗号と情報セキュリティシンポジウム

４．発表年
2018年

１．発表者名
Seiichi Ozawa

２．発表標題
Online Learning of Unstructured Data in Cybersecurity

３．学会等名
2016 IEEE World Congress on Computational Intelligence（招待講演）（国際学会）

４．発表年
2016年

１．発表者名
村田直紀，北園 淳，小澤誠一

２．発表標題
確率的近傍関係を用いた多次元展開法の開発

３．学会等名
システム制御情報学会

４．発表年
2016年

１．発表者名
粟屋成崇，北園 淳，大森敏明，小澤誠一

２．発表標題
Biterm Topic Modelの確率的崩壊型変分ベイズ推論

３．学会等名
システム制御情報学会

４．発表年
2016年

１．発表者名
小澤誠一

２．発表標題
機械学習によるダークネット /ダークウェッブ解析と可視化

３．学会等名
NICT Nicterワークショップ（招待講演）

４．発表年
2016年

１．発表者名
畑中拓哉，北園 淳，小澤誠一，班 涛，中里純二，島村隼平

２．発表標題
ダークネットトラフィックの可視化とオンライン更新によるモニタリング

３．学会等名
コンピュータセキュリティシンポジウム2016

４．発表年
2016年

〔図書〕　計2件

１．著者名	４．発行年
Cesare Alippi, Seiichi Ozawa	2018年
２．出版社	５．総ページ数
Accademic Press	19
３．書名	
Artificial Intelligence in the Age of Neural Networks and Brain Computing (Chap. 12)	

1．著者名 Akira Hirose, Seiichi Ozawa, Kenji Doya, Kazushi Ikeda, Minho Lee, Derong Liu	4．発行年 2016年
2．出版社 Springer	5．総ページ数 2660
3．書名 Neural Information Processing	

〔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
研究分担者	金　相旭 (Kim Sangwook) (00826878)	神戸大学・工学研究科・助教 (14501)	
研究分担者	北園　淳 (Kitazono Jun) (00733677)	神戸大学・工学研究科・工学研究科研究員 (14501)	
研究分担者	大森　敏明 (Omori Toshiaki) (10391898)	神戸大学・工学研究科・准教授 (14501)	
研究協力者	班　涛 (Ban Tao) (80462878)	国立研究開発法人情報通信研究機構・サイバーセキュリティ研究所・主任研究員 (82636)	