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　 ５ 月 ３１ 日現在

機関番号：３４３１０
研究種目：基盤研究(B)（一般）
研究期間：2020～2022
課題番号：２０Ｈ０４１８４

研究課題名（和文）機械学習を悪用したサイバー攻撃に対抗するネットワークシステムの研究開発

研究課題名（英文）Research on network systems to counter cyber attacks using machine learning

研究代表者
木村　共孝（Kimura, Tomotaka）

同志社大学・理工学部・准教授

研究者番号：２０７５６３８２

交付決定額（研究期間全体）：（直接経費）　　13,800,000円

研究成果の概要（和文）：近い将来，機械学習を悪用したサイバー攻撃が出現し，その被害が爆発的に増加することが懸念されている．機械学習は日々急速に進歩しつづけており，機械学習を悪用したサイバー攻撃は計り知れない脅威になり得る．本研究では，進化するサイバー攻撃を数理モデル化し，サイバー攻撃がネットワーク性能にどのような影響を与えるかを明らかにした．さらに，この分析を踏まえた上で，ネットワークの内部での対抗策としてDoS攻撃を緩和するルーチング方式や，ネットワークエッジでの対抗策としてフィッシング検知手法，マルウェア検知手法，ウェブページの異常検知手法を提案した．

研究成果の学術的意義や社会的意義
本研究では，近い将来，出現し得る機械学習を悪用したサイバー攻撃への対抗策を検討した．IoT 環境の急速な発展など新しいネットワークサービスの普及が行われている現在の情報通信ネットワークにおいては，インフラやサービスを保護するために，進化するサイバー攻撃に対抗する手段を検討することは非常に重要な課題である．本研究では，数理モデル化によって今後出現し得るサイバー攻撃の特性を明らかにし，その上でネットワーク内部やネットワークエッジでの対抗策を検討しており，今後のインターネットセキュリティの強化に役立つ．

研究成果の概要（英文）：Cyber attacks using machine learning will appear in the near future, and the number of victims will increase exponentially. Machine learning is advancing rapidly day by day, and the cyber attacks would become an immeasurable threat. To counter such cyber attacks, this study clarified how cyber attacks affect network performance by modeling cyber attacks. As a countermeasure in the network, we proposed a routing scheme to mitigate DoS attacks. Furthermore, we proposed a phishing detection method, a malware detection method, and a web page anomaly detection method as network edge countermeasures.

研究分野：通信ネットワーク

キーワード：ネットワークセキュリティ　機械学習　サイバー攻撃

１．研究開始当初の背景

近年，パソコンやスマートフォンの普及に伴い，SNS，ブログ，電子商品取引など，さまざまなオンラインサービスが提供され，情報通信技術が社会経済活動に不可欠な基盤となっている．情報通信技術により利便性が大きく向上している一方で，情報セキュリティに対する脅威が高まっており，不正アクセスや機密情報の流出などの多くの被害が報告されている．さらに近い将来，機械学習を悪用したサイバー攻撃が出現し，その被害が爆発的に増加することが懸念されている．実際に機械学習を悪用した例としては，ネットワーク内でのユーザの動作を模倣することで検出を回避するサイバー攻撃が存在する．また，研究段階においては，Web カメラなどから取得したユーザの情報を用いて，標的かどうかを自動判定し，サイバー攻撃を仕掛けるような仕組みも考案されている．さらに，世間に知られていないゼロデイ脆弱性を機械学習により発見し，その脆弱性を突くことで感染を拡大させるマルウェアの出現も示唆されている．このように機械学習は日々急速に進歩しつづけており，機械学習を悪用したサイバー攻撃は計り知れない脅威になり得る．

IoT 環境の急速な発展や仮想通貨といった新しいネットワークサービスの普及が行われている現在の情報通信ネットワークにおいては，インフラやサービスを保護するために，このような機械学習を悪用したサイバー攻撃に対抗する手段を検討することは非常に重要な課題である．しかしながら，従来のサイバー攻撃よりも巧妙化・悪質化してきており，これまでの攻撃対策では不十分である．ウィルス対策ソフトを用いたユーザ端末での対抗策や侵入防御システムを用いたゲートウェイでの対抗策などにおける攻撃対策は限界に達しており，これらの従来の攻撃対策のみでは将来のサイバー攻撃の脅威を取り除くことができない．本研究では，このような研究背景のもと，機械学習を悪用したサイバー攻撃に対抗するネットワークシステムの研究を行ってきた．

２．研究の目的

ネットワーク仮想化技術などの将来ネットワーキング技術や最適ネットワーク設計理論を用いて，機械学習を悪用したサイバー攻撃に対抗できるセキュアなネットワークシステムの確立を目指すことが本研究の目的である．多くの既存研究では，機械学習のポジティブな側面に光を当てた検討がされていたが，本研究では，機械学習のネガティブな側面に焦点をあてた研究である．機械学習を悪用したサイバー攻撃を想定した研究はこれまでほとんど考えられておらず，このような攻撃の発生がネットワーク性能にどのような影響を与えるかについてはわかっていない状況である．また，ネットワーク設計の観点から，サイバー攻撃の特性を理論解析によって分析した上で対抗策を考える必要がある．さらに，柔軟かつ堅牢性のあるネットワーク構築が可能な最新のネットワーク技術を用いて有効な対抗策を検討する必要がある．

３．研究の方法

本研究の目的を達成するためには，機械学習を悪用したサイバー攻撃の特性を明らかにした上で，対抗策を検討することが必要不可欠である（図 1）．そこで，本研究では，課題を(1) サイバー攻撃の数理モデル化，(2) ネットワーク内部での対抗策，(3) ネットワークエッジでの対抗策の小課題に分け，各々の小課題の解決に取り組んだ．

課題（1）では，機械学習を悪用したボットネットに着目し，このボットネットの挙動の数理モデル化に取り組んだ．さらに，ボットネットへの対抗策を検討し，ゲーム理論を用いた分析によって対抗策の有効性を示した．

課題（2）では，ネットワークの内部での対抗策では，DoS (Denial of Service)攻撃が仕掛けられている状況を想定し，トラヒックを分散できるルーチング方式について検討した．

課題 (3) では，ネットワークエッジ部での対抗策として機械学習を用いたフィッシング検知，マルウェア検知，ウェブページの異常検知に取り組んだ．

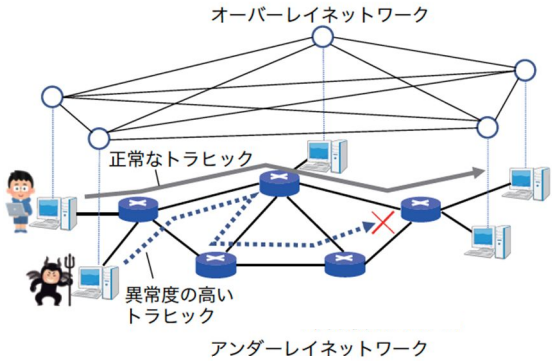


図 1 概要

４．研究成果

(1) サイバー攻撃の数理モデル化

近い将来，出現し得る機械学習を悪用した自律進化型ボトネットへの対抗策を検討した．自律進化型ボットネットは，ボットネットマルウェアに感染したゾンビコンピュータの計算資源を悪用し，分散型機械学習によって脆弱性マイニングを実行する．脆弱性マイニングによってボットネットマルウェアは未知の脆弱性を発見し，感染していないホストに対してゼロデイ攻撃を行い，発見した脆弱性を突き，新たな感染ホストを増加させることができる．

将来のインターネットを保護するには，このようなマルウェアの進化に対抗する対策を検討することが重要である．本研究では，ゲーム理論を用いたアプローチによって対抗策を検討した．自律進化型ボットネットに対抗するための対策グループでは，自律進化型ボットネットと同様に，対策グループに参加するホストの計算資源を利用して脆弱性マイニングを行う．自律進化型マルウェアを用いた攻撃者よりも，対策グループのマイニングによって未知の脆弱性を先に発見することができれば，マルウェアに感染しないように保護することができる．

本研究では，対策グループが存在する状況下におけるマルウェアの感染ダイナミクスを連続時間マルコフ連鎖によって定式化した．ホストの利己的な行動を表現するために，複雑ネットワーク上の進化ゲームの概念を流行モデルに適用した．具体的には，ホストが戦略のペイオフを用いた進化ゲームに基づいて戦略（対策グループへの参加や離脱）を変更する状況を考えた．さらに，マルウェアの進化に対抗するための対策モデルとして対策グループによって見つけた脆弱性の情報を対策グループ内でのみ共有する Ally モデルと対策グループ外のホストにも情報共有を行う Volunteer モデルの二つのモデルを検討した．図 2 は利得のパラメタ w に対する感染ホスト数（I）と対策グループに参加したホスト数（C）の変化を示している．図 2 から $0 \leq w \leq 0.4$ では，Volunteer モデルよりも Ally モデルが有効であることが確認できる．さらに，図 3 は経過時間に対する感染数の違いを示している．Ally モデルと Volunteer モデルのいずれの場合においてもわずかな報酬（$w > 0$）を与えるだけでマルウェアの拡散を大きく抑えられている．また，対策グループへの報酬が増加するにつれて感染ホスト数を削減する速度が向上することが確認できる．これらの結果より，本研究で提案した対策グループが将来のマルウェアの進化への対抗に有効であることが分かった．

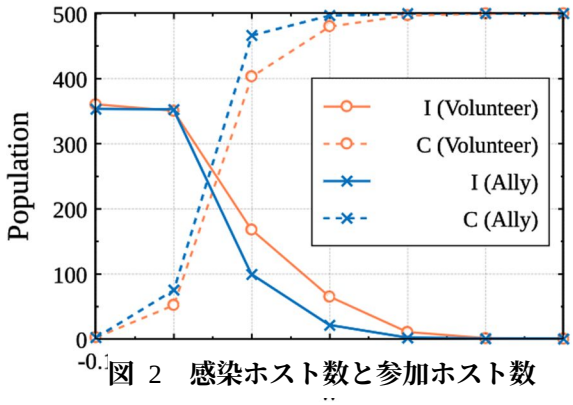
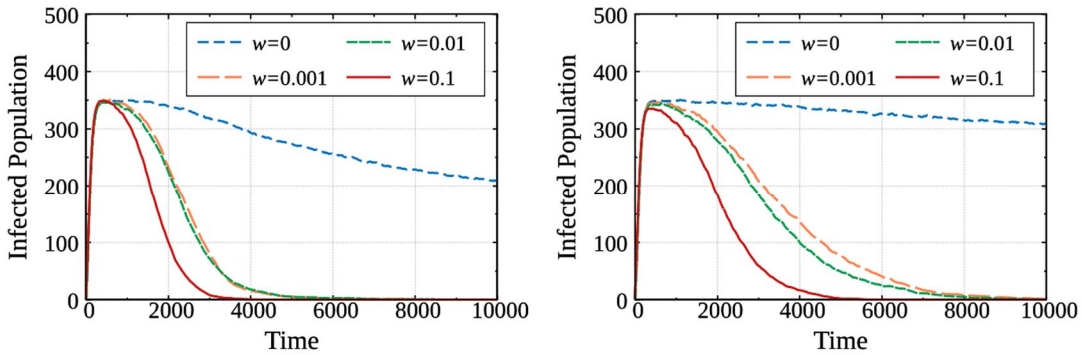


図 2　感染ホスト数と参加ホスト数



(a) Ally model scenario.　(b) Volunteer model scenario.

図 3 感染ホスト数の時間変化

(2) ネットワーク内部での対抗策

機械学習の悪用によって今後，増加が見込まれる DoS 攻撃への対抗策として ACO（Ant Colony Optimization）アルゴリズムを用いたマルチパスルーチング方式を提案した．通常は，ACO アルゴリズムは最短経路を求めるために利用するが，本研究ではホップ数の長い経路を求めるために利用する．ACO アルゴリズムによって得られた複数の経路のうち，これらを確率的に利用する（図 4）．こうすることで，DoS 攻撃を仕掛けられたとしても多くのトラヒックが迂回した経路を利用するようになるため，ネットワーク内の輻輳を分散させることができる．

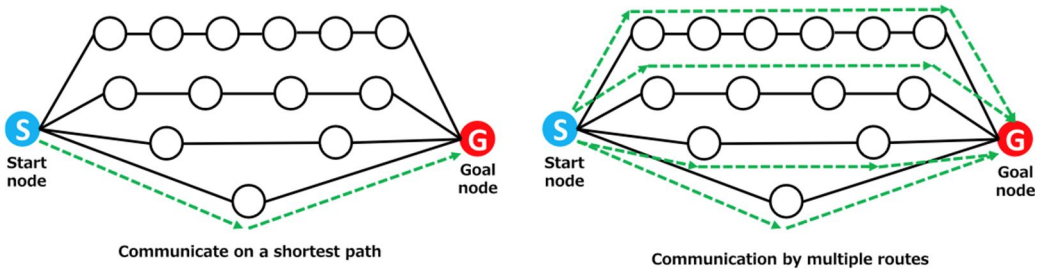


図 4 マルチパスの設定

図 5 と図 6 はそれぞれ BA（Barabási-Albert）モデルと WS （Watts-Strogatz） モデルにおいて提案手法を用いた場合の攻撃者以外のユーザのスループットの結果を示している．これらの図から DoS 攻撃が仕掛けられているにも関わらず，ユーザのスループットが減少しないことが確認できる．よって，提案手法を用いることで DoS 攻撃によるネットワーク負荷を分散させ，軽減できることが確認できた．

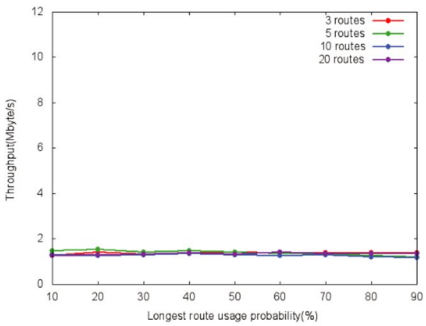


図 5 スループット（BA モデル）

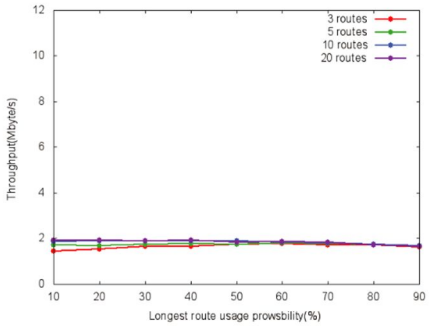


図 6 スループット(WS モデル)

(3)ネットワークエッジでの対抗策

ネットワークエッジでの対抗策としてフィッシング検知手法，マルウェア検知手法，ウェブページの異常検知手法について検討を行った．フィッシング検知手法では，従来の複数の特徴量（URL や DNS 情報）を同時に入力せずに，これらの特徴量を逐次的に利用する逐次型フィッシング検知手法を提案した．具体的には，一段階目に用いる URL 分析フェーズでは URL の情報を CNN-BiLSTM へ入力し，判定の確度が高い場合にはこの時点で正常か，フィッシングであるかを判定する．判定の確度が低い場合には，二段階目に用いるドメイン分析フェーズへ移行し，ドメインの情報を CNN-BiLSTM へ入力する．一段階目と同様に，判定の確度が高い場合には正常かフィッシングであるかを判定する．判定の確度が低い場合には，三段回目として HTML 分析フェーズへ移行する．図 7 は URL 分析フェーズからドメイン分析フェーズへの移行割合を制御するパラメタ α に対する Accuracy の変化を示している．パラメタ α を適切に設定することで HTML 分析フェーズを単独で行う場合と同程度の性能を達成できている．また，図 8 はパラメタ α に対する判定までに要する時間の変化を示している．HTTP 分析フェーズを単独で行う場合や既存方式である Web2Vec を用いる場合よりも，提案手法は短い時間で判定を行えていることが分かる．

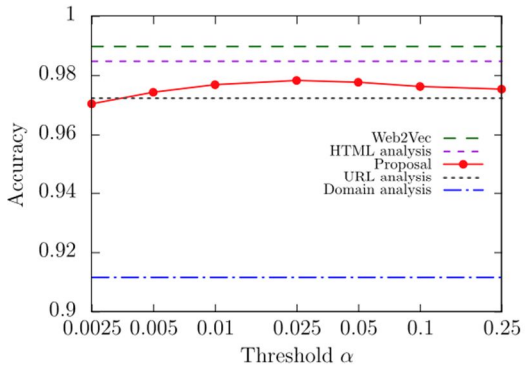


図 7 Accuracy（フィッシング検知）

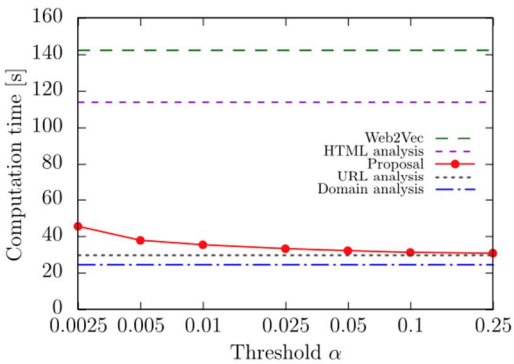


図 8 計算時間（フィッシング検知）

マルウェアを検知するために，API（Application Programming Interface）シーケンスを入力としたマルウェア検知器を検討した．本研究では，API シーケンス全体を判別に用いる検知器と API シーケンスを細かく分割した上で入力する検知器を組み合わせて利用する．このようにすることで API 全体の特徴だけではなく，API 列の局所的な特徴も学習できるため，マルウェアの検知率の向上が見込める．図 9 は提案手法である二段階検知器の Accuracy の結果を示している．図 9 から閾値α = 0のとき一段階だけの検知器を用いるよりも Accuracy を向上でき，マルウェアの検知性能を向上できることを示した．

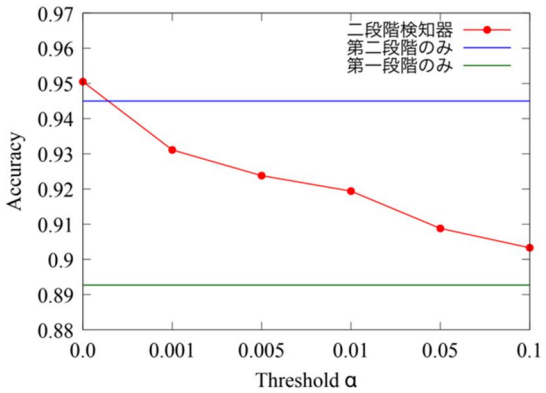


図 9　Accuracy (マルウェア検知)

ウェブページの異常検知手法として，HDBSCAN (Hierarchical Density-Based Spatial Clustering of Applications with Noise)と Deep SVDD (Support Vector Data Description)を用いた異常検知手法を検討した．提案手法では，まず，学習データに対して密度に基づくクラスタリングである HDBSCAN を使用し，クラスタ化されたデータを抽出する．次に，このデータを外れ値検知手法の一つである Deep SVDD の新たな学習データとして入力し，分類境界を求める．この分類境界によってデータを分類し，分類結果に基づきラベルを推定する．推定されたラベルは教師あり異常検知モデルの構築に使用する．構築された異常検知モデルを使用して異常の検知を行う．図 10 はウェブページのデータセットを用いた実験における F 値の値を示している．提案手法では，90%を超える F 値を達成できている．さらに，既存方式である OCSVM や Deep SVDD よりも高い F 値を達成できており，ウェブページの異常検知に有効であることを示した．

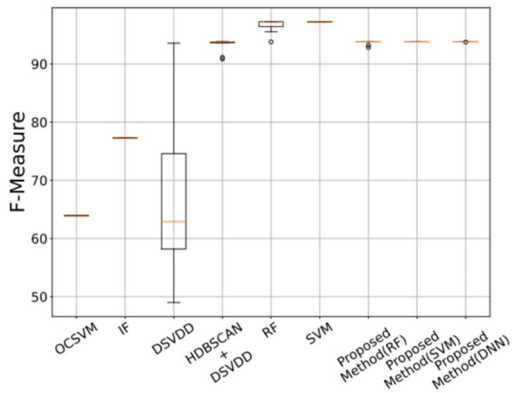


図 10 F 値（ウェブページの異常検知）

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　0件）

１．著者名 Ogawa Yuji、Kimura Tomotaka、Cheng Jun	４．巻 11
２．論文標題 Deep-learning-based sequential phishing detection	５．発行年 2022年
３．雑誌名 IEICE Communications Express	６．最初と最後の頁 171～175
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/comex.2021XBL0212	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 SHIMIZU Yuki、KIMURA Tomotaka、CHENG Jun	４．巻 E105.B
２．論文標題 Performance Evaluation of a Hash-Based Countermeasure against Fake Message Attacks in Sparse Mobile Ad Hoc Networks	５．発行年 2022年
３．雑誌名 IEICE Transactions on Communications	６．最初と最後の頁 833～847
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transcom.2021EBP3103	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 山中 啓太、阿萬 裕久、川原 稔	４．巻 38
２．論文標題 プログラムスライスとDoc2Vecを用いた変数名評価法の提案	５．発行年 2021年
３．雑誌名 コンピュータ ソフトウェア	６．最初と最後の頁 4_9～4_15
掲載論文のDOI（デジタルオブジェクト識別子） 10.11309/jssst.38.4_9	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 Miura Hideyoshi、Kimura Tomotaka、Hirata Kouji	４．巻 10
２．論文標題 Deterministic epidemic modeling of future botnet malware with a contact process	５．発行年 2021年
３．雑誌名 IEICE Communications Express	６．最初と最後の頁 295～300
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/comex.2021XBL0036	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 Shindo Takuya、Kimura Tomotaka、Hiraguri Takefumi	4．巻 10
2．論文標題 Defense against DoS attacks by multipath routing using the ACO algorithm	5．発行年 2021年
3．雑誌名 IEICE Communications Express	6．最初と最後の頁 973～978
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/comex.2021COL0018	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 宮本 敦哉、阿萬 裕久、川原 稔	4．巻 37
2．論文標題 バグ混入予測の精度向上に向けた個人化予測モデルの組合せ手法とその評価	5．発行年 2020年
3．雑誌名 コンピュータ ソフトウェア	6．最初と最後の頁 4_38～4_49
掲載論文のDOI（デジタルオブジェクト識別子） 10.11309/jssst.37.4_38	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55件（うち招待講演　1件／うち国際学会　13件）

1．発表者名 K. Tsunewaki, T. Kimura, J. Cheng
2．発表標題 LSTM-Based Ransomware Detection Using API Call Information
3．学会等名 IEEE International Conference on Consumer Electronics - Taiwan (IEEE ICCE-TW 2022)（国際学会）
4．発表年 2022年

1．発表者名 H. Miura, S. Abukawa, T. Kimura, K. Hirata
2．発表標題 Modeling of Malware Diffusion With Mobile Devices in Intermittently Connected Networks
3．学会等名 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2022)（国際学会）
4．発表年 2022年

１．発表者名
安井淳，木村共孝，程俊

２．発表標題
MPEG-DASHストリーミング配信におけるDQNを用いたサーバ選択法

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
小川侑治，木村共孝，程俊

２．発表標題
CNN-BiLSTM を用いた逐次型フィッシング検知

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
西浦幸来，小川侑治，木村共孝，程俊

２．発表標題
深層学習を用いたフィッシング検知手法における敵対的 URL に対する脆弱性の評価

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
常脇航平，小川侑治，木村共孝，程俊

２．発表標題
LSTMを用いた呼び出しAPI情報に基づくランサムウェア検知

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
奥嵩史，木村共孝，程俊

２．発表標題
マルコフ解析を用いたエネルギーハーベスト型センサネットワークのAoI評価

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
伊藤有輝，木村共孝，程俊

２．発表標題
再感染率の異なる複数の回復状態を持つマルウェア伝播モデルの分析

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
虻川翔哉，木村共孝，平田孝志

２．発表標題
劣通信環境下におけるマルウェア拡散挙動解析の検討

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
野地勇佑，木村共孝，程俊

２．発表標題
分散ファイルシステムにおけるHDBSCANを用いたインシデント発生間隔に基づく異常検知

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
狭間雄斗，三浦秀芳，木村共孝，平田 孝志

２．発表標題
ホストの獲得利得を考慮したマルウェア感染拡散対策モデルの考察

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
石川祥吾，三浦秀芳，木村共孝，平田孝志

２．発表標題
ハニーポットを用いたマルウェア感染拡散対策モデルの検討

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
伊藤有輝，三浦秀芳，木村共孝，平田孝志，程俊

２．発表標題
自律進化型ボットネットに対抗する複数対策グループモデルの分析

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
佐藤克樹，程俊，木村共孝

２．発表標題
センサの情報発生間隔を考慮したUAVの飛行経路計画

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
永井崚，木村共孝，程俊

２．発表標題
DQNを用いたアダプティブストリーミングにおけるダウンロード一時停止の検討

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
三浦秀芳，虻川翔哉，木村共孝，平田孝志

２．発表標題
劣通信環境におけるモビリティを考慮したマルウェア感染拡散モデルの考察

３．学会等名
電子情報通信学会 ネットワークシステム研究会

４．発表年
2022年

１．発表者名
西浦幸来，木村共孝，程俊

２．発表標題
［ポスター講演］深層学習を用いたフィッシング対策に対するバックドア攻撃の検知

３．学会等名
電子情報通信学会 革新的無線通信技術に関する横断型研究会（MIKA2022）

４．発表年
2022年

１．発表者名
船越宝，木村共孝，程俊，平栗健史

２．発表標題
［ポスター講演］疎密度モバイルアドホック網における端末密度を考慮した無線電力伝送

３．学会等名
電子情報通信学会 革新的無線通信技術に関する横断型研究会（MIKA2022）

４．発表年
2022年

１．発表者名
野地勇佑，木村共孝，程俊

２．発表標題
HDBSCANとDeep SVDDを用いたWebページの異常検知

３．学会等名
電子情報通信学会 コミュニケーションクオリティ研究会

４．発表年
2022年

１．発表者名
大隅博文，木村共孝， 平田孝志，程俊

２．発表標題
ドローンネットワークにおける連結性とエネルギー消費を考慮したドローン配置

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
向山知花，木村共孝，程俊

２．発表標題
物資運搬における強化学習を用いたUAVの飛行タイミングの決定法

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
虻川翔哉，三浦秀芳，木村共孝，平田孝志

２．発表標題
劣通信環境下における区画を考慮した微分方程式によるマルウェア拡散挙動解析の検討

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
細川雄河，木村共孝，程俊

２．発表標題
深層強化学習を用いたPost-Exploitationを抑制する動的ネットワーク構成変更法

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
大貫和基，常脇航平，木村共孝，程俊

２．発表標題
BERTを用いた呼び出しAPI情報に基づくランサムウェア検知

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
狭間雄斗，三浦秀芳，木村共孝，平田孝志

２．発表標題
ホストの隣接関係を考慮したマルウェア感染拡散対策モデルの考察

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
船越 宝，木村共孝，程俊

２．発表標題
疎密度モバイルアドホック網における遭遇間隔を考慮した給電制御

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
長久保智子，木村共孝，程俊

２．発表標題
疎密度モバイルアドホック網におけるグループ検知を用いた連合学習法

３．学会等名
電気学会通信研究会

４．発表年
2022年

１．発表者名
H. Aman, S. Amasaki, T. Yokogawa, M. Kawahara

２．発表標題
An Investigation of Compound Variable Names Toward Automated Detection of Confusing Variable Pairs

３．学会等名
36th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW)（国際学会）

４．発表年
2021年

１．発表者名
H. Aman, S. Amasaki, T. Yokogawa, M. Kawahara

２．発表標題
A Large-Scale Investigation of Local Variable Names in Java Programs: Is Longer Name Better for Broader Scope Variable?

３．学会等名
Book cover Book cover International Conference on the Quality of Information and Communications Technology（国際学会）

４．発表年
2021年

１．発表者名
T. Minehisa, H. Aman, T. Yokogawa, M. Kawahara

２．発表標題
A Comparative Study of Vectorization Approaches for Detecting Inconsistent Method Names

３．学会等名
International Conference on Intelligence Science（国際学会）

４．発表年
2021年

１．発表者名
H. Miura, T. Kimura, K. Hirata

２．発表標題
Modeling of malware diffusion with the FLIPIT game

３．学会等名
IEEE International Conference on Consumer Electronics - Taiwan (IEEE ICCE-TW 2020)（国際学会）

４．発表年
2020年

１．発表者名
K. Uno, T. Kimura, K. Hirata

２．発表標題
Estimation method of malware infection spreading with graph convolutional networks

３．学会等名
IEEE International Conference on Consumer Electronics - Taiwan (IEEE ICCE-TW 2020)（国際学会）

４．発表年
2020年

１．発表者名
Y. Ogawa, T. Kimura, J. Cheng

２．発表標題
Vulnerability Assessment for Machine Learning Based Network Anomaly Detection System

３．学会等名
IEEE International Conference on Consumer Electronics - Taiwan (IEEE ICCE-TW 2020)（国際学会）

４．発表年
2020年

１．発表者名
Y. Nagasawa, K. Kishioka, T. Kimura, K. Hirata

２．発表標題
Prediction method of malware infection spreading considering network scale

３．学会等名
Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2020)（国際学会）

４．発表年
2020年

１．発表者名
Hirohisa Aman, Sousuke Amasaki, Tomoyuki Yokogawa, Minoru Kawahara

２．発表標題
A Comparative Study of Vectorization-Based Static Test Case Prioritization Methods

３．学会等名
46th Euromicro Conference on Software Engineering and Advanced Applications（国際学会）

４．発表年
2020年

１．発表者名
Asato Masanao, Aman Hirohisa, Amasaki Sousuke, Yokogawa Tomoyuki, Kawahara Minoru

２．発表標題
A Mahalanobis Distance-Based Integration of Suspicious Scores For Bug Localization

３．学会等名
27th Asia-Pacific Software Engineering Conference（国際学会）

４．発表年
2020年

１．発表者名
山中 啓太, 阿萬 裕久, 川原 稔

２．発表標題
Doc2Vec を活用した変数名の自動評価法の提案

３．学会等名
第27回 ソフトウェア工学の基礎ワークショップ

４．発表年
2020年

１．発表者名
木村共孝

２．発表標題
［依頼講演］Delay Tolerant NetworksにおけるAoIの分析

３．学会等名
電子情報通信学会CQ研専設立30周年に向けた特別企画ワークショップ

４．発表年
2021年

１．発表者名
長久保智子，木村共孝，程俊

２．発表標題
疎密度モバイルアドホック網における正常転送回数を用いたフェイクメッセージ攻撃の対策

３．学会等名
電気学会通信研究会

４．発表年
2021年

１．発表者名
宇野克紀，木村共孝，平田孝志

２．発表標題
GCNを使用したリスク推定によるマルウェア感染拡大の予測法

３．学会等名
電気学会通信研究会

４．発表年
2021年

１．発表者名
三浦秀芳，木村共孝，平田 孝志

２．発表標題
ネットワーク上の進化ゲームを用いたマルウェア感染拡散対策モデルの検討

３．学会等名
電気学会通信研究会

４．発表年
2021年

１．発表者名
清水浩毅，木村共孝，平田孝志

２．発表標題
脆弱性情報共有による進化型マルウェア感染抑制の考察

３．学会等名
電子情報通信学会 ネットワークシステム研究会

４．発表年
2021年

１．発表者名
Y. Ogawa, T. Kimura, J. Cheng

２．発表標題
Vulnerability Assessment for Deep Learning Based Phishing Detection System

３．学会等名
IEEE International Conference on Consumer Electronics - Taiwan (IEEE ICCE-TW 2021)（国際学会）

４．発表年
2021年

１．発表者名
H. Miura, T. Kimura, K. Hirata

２．発表標題
Inhibition modeling of future malware diffusion with an evolutionary game theory

３．学会等名
IEEE International Conference on Consumer Electronics - Taiwan (IEEE ICCE-TW 2021)（国際学会）

４．発表年
2021年

１．発表者名
小川侑治，木村共孝，程俊

２．発表標題
［ポスター講演］深層学習を用いたフィッシング検知システムの脆弱性の評価

３．学会等名
電子情報通信学会 コミュニケーションクオリティ研究会

４．発表年
2021年

１．発表者名
小川侑治，木村共孝，程俊

２．発表標題
深層学習を用いたフィッシング検知手法における多数決判別器によるAdversarial Examplesの対策

３．学会等名
電子情報通信学会 コミュニケーションシステム研究会

４．発表年
2021年

１．発表者名
三浦秀芳，木村共孝，平田孝志

２．発表標題
進化ゲーム理論を適用したマルウェア感染拡散対策モデルの考察

３．学会等名
電気学会通信研究会

４．発表年
2021年

１．発表者名
船越宝，木村共孝，程俊

２．発表標題
ホスト保護による自律進化型ボットネットの抑制

３．学会等名
電気学会通信研究会

４．発表年
2021年

１．発表者名
宇野克紀，木村共孝，平田孝志

２．発表標題
STGCNを用いたマルウェア感染源予測方法の検討

３．学会等名
電気学会通信研究会

４．発表年
2021年

１．発表者名
長江優輝，木村共孝，程俊

２．発表標題
主成分分析を用いた短期間ポートスキャン活動のON/OFFパターン分析

３．学会等名
電気学会通信研究会

４．発表年
2021年

１．発表者名
池田茜，木村共孝，程俊

２．発表標題
疎密度モバイルアドホック網におけるSpray and Wait方式のAoI評価

３．学会等名
電気学会通信研究会

４．発表年
2021年

１．発表者名
細川雄河，木村共孝，程俊

２．発表標題
強化学習を用いたペネトレーションテスト自動化ツールの性能評価

３．学会等名
電気学会通信研究会

４．発表年
2021年

１．発表者名
木村共孝，平田孝志

２．発表標題
［招待講演］機械学習を悪用したサイバー攻撃に対抗するネットワークシステムの検討

３．学会等名
電子情報通信学会 コミュニケーションシステム研究会（招待講演）

４．発表年
2021年

１．発表者名
西浦幸来，小川侑治，木村共孝，程俊

２．発表標題
［ポスター講演］深層学習を用いたネットワーク異常検知システムにおける多数決判定法の検討

３．学会等名
電子情報通信学会 革新的無線通信技術に関する横断型研究会（MIKA2021）

４．発表年
2021年

１．発表者名
小川侑治，木村共孝，程俊

２．発表標題
［ポスター講演］深層学習を用いた逐次型フィッシング検知手法の検討

３．学会等名
電子情報通信学会 革新的無線通信技術に関する横断型研究会（MIKA2021）

４．発表年
2021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
研究分担者	平田　孝志 (Hirata Kouji) (10510472)	関西大学・システム理工学部・准教授 (34416)	
研究分担者	井上　文彰 (Inoue Yoshiaki) (40779914)	大阪大学・工学研究科・助教 (14401)	
研究分担者	阿萬　裕久 (Aman Hirohisa) (50333513)	愛媛大学・総合情報メディアセンター・特任教授 (16301)	
研究分担者	桂井　麻里衣 (Katsurai Marie) (70744952)	同志社大学・理工学部・准教授 (34310)	
研究分担者	平栗　健史 (Hiraguri Takefumi) (90582817)	日本工業大学・基幹工学部・教授 (32407)	

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