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 １８ 日現在

機関番号：１４４０１
研究種目：基盤研究(B)（一般）
研究期間：2021～2023
課題番号：２１Ｈ０３４４２

研究課題名（和文）AI時代の安全な計算プラットフォーム

研究課題名（英文）Secure Computing Platform in the AI Era

研究代表者
小泉　佑揮（Koizumi, Yuki）

大阪大学・大学院情報科学研究科・准教授

研究者番号：５０５５２０７２

交付決定額（研究期間全体）：（直接経費）　　13,000,000円

研究成果の概要（和文）：本研究プロジェクトでは、機械学習から漏洩するプライバシー情報の保護を目的とし、安全な分散型機械学習の処理プラットフォームを設計した。核となる開発技術は、モデルからの情報漏洩を防ぐために、ユーザーから出る機械学習モデルをマスクしたまま秘密裏に集約可能な安全なモデル集約法であり、これによりモデルから漏洩する情報の保護のみならず、モデルの改竄も防ぐことに成功した。さらに、匿名通信やTrusted Execution Environmentを併用することで、分散処理の安全性や入力の安全性を向上させることに成功した。

研究成果の学術的意義や社会的意義
学術的には、連合学習における安全なモデル集約法の実現により、機械学習におけるプライバシー保護の技術的限界を拡張した。社会的には、個人のデータを保護しながら集合知を活用する新しい形の機械学習の利用法を実現可能にした。医療、創薬や金融など、情報の秘匿性が重要な分野での安全なデータ利用を促進する利用シナリオへの適用が予想される。さらに、提案技術は、プロトコルにはしたがうものの秘匿された情報の奪取を試みる脅威の存在に対しても頑強であり、異なる、あるいは競合するビジネス主体間の安全な連合をも可能にする。このように、情報のプライバシーを守りつつ、社会全体の技術革新の促進に寄与した。

研究成果の概要（英文）：In this project, we developed a secure distributed machine learning processing platform, especially focusing on federated learning, designed to protect against the leakage of privacy information from machine learning models. The core technology is a secure model aggregation method that allows for the confidential aggregation of user-generated machine learning models while keeping them masked, that is, it aggregates the models confidentially to any other participants. This approach not only safeguards against information leakage from the models but also effectively prevents model tampering. Additionally, by integrating anonymous communication and trusted execution environments (TEEs), we significantly enhanced the security of distributed processing and the protection of input data.

研究分野：情報ネットワーク

キーワード：機械学習　プライバシー　セキュリティー　連合学習

１．研究開始当初の背景

機械学習を用いたシステム（AI システムと呼ぶ）の社会システムへの浸透と同時に、機械学習に対する脆弱性の指摘も増えている。その攻撃は多岐にわたり、機械学習のモデルの学習に用いられた元データの復元を試みる Model Inversion Attack（あるいは Data Reconstruction Attack）、入力データに対し人には判別ができないわずかなノイズを加えることでニューラルネットワークの推論結果を変更する Evasion Attack、特定の入力に対して誤った推論を導くように教師データを改竄する Data Poisoning Attack などが指摘されている。

いずれの攻撃も、AI システムの根幹をゆるがすものである。例えば、自動運転を想定した場合、Evasion Attack によるニューラルネットワークの認識結果に対する攻撃は自動車の誤操作を引き起こし、交通事故を誘発する恐れがある。Model Inversion Attack によりモデル学習に用いた入力データが漏洩すると、ニューラルネットワークに基づく認証が突破される。指紋や顔認証による AI システムに対して、Evasion Attack を用いて攻撃者を正規のユーザとして認証させる攻撃が実践されるなど、AI システムの社会への普及を鑑みると、ニューラルネットワークの脆弱性は社会安全に対する重大な懸念である。

２．研究の目的

前述の背景に対して、本課題の研究目的は、ニューラルネットワークが抱える脅威に総合的に対処し、入力から出力までの安全性が担保された AI システムのための安全な計算プラットフォームを実現することである。

AI システムに対する脅威を、モデルからの情報漏洩とモデルそのものに対する攻撃に分類して考える。現状では、それぞれの脅威に対して対処療法的に脆弱性を軽減する手法が開発されているものの、抜本的な解決策が存在しない。これに対して、本プロジェクトでは、計算プラットフォームの観点でこの脅威に抜本的に対応することを目的とする。

３．研究の方法

本プロジェクトでは、安全に AI を計算するプラットフォームの実現を目指し、機械学習、とりわけ、分散機械学習の手法の中で有望な連合学習を対象とし、モデルからの情報漏洩とモデルに対する攻撃を防ぐため、モデルの保護技術と、それを支える匿名通信技術の研究に取り組んだ。これらの技術は、ユーザのデータを保護しながら高性能な機械学習モデルを構築し、安全な通信を提供するために不可欠である。

４．研究成果

上記の研究目的を達成するために、本プロジェクトでは以下の主要な成果を挙げた。

- 連合学習からの情報漏洩の分析
- 連合学習からの情報漏洩を防ぐモデル集約技術
- モデルに対する攻撃を防御する通信技術

本報告ではそれぞれの研究成果の概要を説明し、全体として成果を総括する。

(1) 連合学習からの情報漏洩の分析

この研究では、垂直連合学習におけるデータ漏洩の脆弱性を指摘し、新たな攻撃手法を提案した。垂直連合学習（Vertical Federated Learning）は、同一のサンプルで異なる特徴を持つデータを所有する参加者が、データを共有せずに協力してモデルを訓練する手法である。この手法は、参加者間でデータのプライバシーを保護するための重要な手段であるが、推論時に全ての参加者が関与する必要があり、効率性に課題があった。

Huang らが提案した Vertical Federated Knowledge Transfer（VFedTrans）は、Federated Singular Value Decomposition（FedSVD）を用いて参加者間でデータの潜在表現を生成し、それを基に知識蒸留を行う。この手法により、各参加者は他の参加者のデータに依存せずに独自に推論を行うことができ、既存のデータ漏洩攻撃を無効化するという利点がある。

本研究では、VFedTrans に対する新たなデータ漏洩攻撃手法を提案した。具体的には、セミオネストな参加者が潜在表現と元のデータの間の線形関係をニューラルネットワークを用いて推論し、他の参加者のデータを再構築する手法である。この攻撃手法により、潜在表現から元のデータを復元し、参加者間のデータプライバシーを侵害するリスクが高まる。

実験には、医療および金融に関する 2 つのデータセットを使用し、提案手法の有効性を評価した。結果として、提案手法は受動的参加者のデータの一部を再構築する能力を持つことを示した。

① 提案手法

本研究では、Vertical Federated Knowledge Transfer（VFedTrans）という手法を用いる。VFedTrans は、Federated Singular Value Decomposition（FedSVD）を用いて参加者間でデータの潜在表現を生成し、それを基に知識蒸留を行う手法である。これにより、各参加者は他の参加者のデータに依存せずに独自に推論を行うことができる。

提案手法では、以下のステップを通じてデータ漏洩攻撃を実行する。

1. 潜在表現の取得：攻撃者は、共有された潜在表現を取得する。
2. ニューラルネットワークの構築：攻撃者は、潜在表現と元のデータの間の線形関係を学習するためのニューラルネットワークを構築する。
3. データの復元：ニューラルネットワークを用いて、潜在表現から元のデータを復元する。

攻撃者は共有された潜在表現から元のデータを高い精度で復元することができる。

② 実験と評価

提案手法の有効性を評価するために、医療および金融に関する 2 つのデータセットを使用して実験を行った。評価項目は以下の通りである。

1. データ復元精度：提案手法を用いて潜在表現から元のデータを復元する精度を評価する。
2. モデル精度：垂直連合学習におけるモデルの精度を評価し、提案手法の適用による影響を確認する。
3. 計算コスト：提案手法を適用する際の計算コストを評価する。

実験結果から、提案手法は高い精度で元のデータを復元することができることを確認した。また、垂直連合学習におけるモデルの精度にも大きな影響を与えないことが示された。計算コストについても、提案手法は効率的にデータ復元を実行することができることが明らかにした。

③ まとめ

本研究では、垂直連合学習におけるデータ漏洩攻撃の新たな手法を提案し、その有効性を実験により評価した。提案手法は、共有された潜在表現から元のデータを高い精度で復元することができるため、垂直連合学習におけるプライバシー保護の脆弱性を明らかにした。

(2) 連合学習からの情報漏洩を防ぐモデル集約技術

この研究では、連合学習におけるプライバシー保護のための新しい手法を提案した。従来の連合学習では、サーバが受け取る差分モデルからユーザのデータを推定するモデル反転攻撃のリスクがあった。差分プライバシーを用いる方法も提案されているが、それにはモデルの性能が低下するという弊害もある。本提案手法は、差分プライバシーベースの手法の限界を克服し、モデルの品質を保持しながらプライバシー保護を実現する新しい手法を開発した。

具体的には、各ユーザが生成した差分モデルを複数のフラグメントに分割し、他のユーザのフラグメントとシャッフルして集約することで、個々の差分モデルを攻撃者から隠蔽する。この手法により、共有モデルの品質を劣化させることなく、モデル反転攻撃に対する耐性を実現する。

提案手法の評価には、様々なシナリオでの実験を行い、その有効性を確認した。実験結果から、提案手法は従来の連合学習と同等の性能を持つ共有モデルを生成する一方で、モデル反転攻撃に対する強い耐性を示した。また、通信コストについても評価し、提案手法の総トラフィック量は従来の連合学習とほぼ同等であることが確認した。

①　提案手法

本研究では、差分モデルを複数のフラグメントに分割し、これらをシャッフルして集約する手法を提案する。この手法により、各ユーザが生成する差分モデルを攻撃者から隠蔽しつつ、モデルの品質を保つことができる。提案手法は以下のステップで構成される。

1. モデルの分割：各ユーザは、ローカルで計算した差分モデルを複数のフラグメントにランダムに分割する。
2. フラグメントのシャッフル：生成したフラグメントを他のユーザと交換する。交換するフラグメントはランダムに選ばれるため、各フラグメントの出所が特定されにくくなる。
3. フラグメントの集約：シャッフルされたフラグメントを集約し、共有モデルの更新に使用する。

これにより、個々の差分モデルは攻撃者から隠蔽され、モデル反転攻撃のリスクが低減される。

また、ノイズを加えることなくプライバシーを保護できるため、モデルの性能も維持される。

② 実験と評価

提案手法の有効性を評価するために、複数のデータセットを使用して実験を行った。評価項目は以下の通りである。

1. モデルの精度：提案手法を適用した場合と従来の差分プライバシーを適用した場合のモデル精度を比較する。
2. プライバシー保護効果：モデル反転攻撃に対する耐性を評価する。具体的には、攻撃者が差分モデルから元のトレーニングデータを推定する精度を測定する。
3. 通信コスト：提案手法を適用する際の通信コストを評価する。フラグメントの分割とシャッフルによる通信量が従来の連合学習と比較して増加するかどうかを確認する。

実験結果から、提案手法は従来の差分プライバシーを用いる方法と比較して、モデルの性能を劣化させることなくプライバシー保護を実現することが確認された。また、通信コストについても、提案手法の総トラフィック量は従来の連合学習とほぼ同等であることを明らかにした。

③ まとめ

本研究では、連合学習におけるモデル反転攻撃に対する新しいプライバシー保護手法を提案した。提案手法は、差分モデルを複数のフラグメントに分割し、これらをシャッフルして集約することで、モデルの品質を維持しながらプライバシーを保護するものである。実験により、提案手法は高いプライバシー保護効果とモデル性能を両立することを確認した。

(3) モデルに対する攻撃を防ぐ通信技術 - 匿名通信技術

インターネットにおける匿名通信は、ユーザのプライバシー保護において重要な役割を果たす。同時に、提案する AI システムのための計算プラットフォームに対しても重要な役割を果たす。しかし、オニオンルーティングに基づく匿名通信プロトコルは、複数のリレーを介して通信データを暗号化し、送信元と送信先の匿名性を確保するため、低スループットと高レイテンシの問題があり、連合学習などのリアプリケーションには適していない。

本研究では、ネットワーク層のルータに実装される軽量匿名通信プロトコル (gPHI) を設計し、パケットのヘッダのみを暗号化することで高速なパケット転送を実現した。しかし、既存のプロトコルは、悪意のあるノード間の結託を伴う攻撃や、IP ネットワークのトポロジやルーティング・ポリシーの情報を用いる攻撃に対して脆弱であることが指摘されている。gPHI では、経路の確立のためにガードと呼ばれる新たなサーバを導入し、経路設定フェーズにおけるプロトコルを拡張することで、これらの脆弱性に対する攻撃の影響を緩和した。実際のインターネット・トポロジに基づいたシミュレーションにより、gPHI が既存のプロトコルと比較してより強力な関係匿名性を実現することが確認した。

① 提案手法

本研究では、ネットワーク層のルータに実装される軽量匿名通信プロトコルを設計する。提案手法は以下のステップで構成される。

1. ガードの導入：経路の確立のためにガードと呼ばれる新たなサーバを導入する。ガードは、経路設定フェーズにおいて信頼できる中継ノードとして機能する。
2. ヘッダの暗号化：パケットのヘッダのみを暗号化する。これにより、パケットのペイロードはそのまま転送されるため、低レイテンシで高速な通信が可能となる。
3. 経路設定：ガードを介して経路を設定し、各パケットが複数のリレーを経由して目的地に到達するようにする。

この手法により、パケット全体を暗号化する必要がないため、通信のオーバーヘッドが大幅に削減される。また、ガードの導入により、悪意のあるノード間の結託を伴う攻撃や、IP ネットワークのトポロジやルーティング・ポリシーの情報を用いる攻撃に対しても耐性を持つ。

② 評価結果

提案手法の有効性を評価するために、実際のインターネット・トポロジに基づいたシミュレーションを行った。評価項目は以下の通りである。

1. 匿名性の評価：提案手法が送信元と送信先の匿名性をどの程度確保できるかを評価する。
2. 通信速度：提案手法の通信速度を評価し、従来のオニオンルーティングに基づくプロトコルと比較する。

3. レイテンシ：提案手法のレイテンシを評価し、リアルタイム性が求められるアプリケーションに適しているかを確認する。

シミュレーション結果から、gPHI は既存のオニオンルーティングに基づくプロトコルと比較して、より高速で低レイテンシな通信が実現できることを確認した。

② まとめ

本研究では、高速かつ匿名性の高い通信を実現する軽量匿名通信プロトコル（gPHI）を提案し、その有効性を実験により評価した。提案手法は、パケットのヘッダのみを暗号化することで通信のオーバーヘッドを削減し、ガードの導入により匿名性を強化するものである。

(3) モデルに対する攻撃を防ぐ通信技術 - 匿名名前解決技術

この研究では、従来の DNS（Domain Name System）の設計には、基本的なセキュリティおよびプライバシー機能が欠けている問題を指摘し、複数のリレーを使用してユーザーの匿名性を確保する新しいアプローチである μODNS（Mutualized Oblivious DNS）を提案している。従来のリレーベースの匿名化スキームは、リレーとフルサービスリゾルバ間の共謀に対して脆弱であり、ユーザーの身元を隠すことができない。

μODNS は、ユーザーがネットワーク内に少なくとも 1 つの信頼できるリレーを持ち、そのリレーを他のユーザーと共有するという合理的な仮定に基づいている。ユーザーは、信頼できるリレーを次のホップリレーとして設定し、そのリレーを介してクエリをリゾルバに伝達し、他のエンティティと共有されるリレーをランダムに選択する。これにより、ユーザーのアイデンティティは、リレーがリゾルバと共謀しても隠されたままである。

さらに、PoC（Proof-of-Concept）実装を作成し、オープンソースソフトウェア化した。インターネット上での DNS メッセージの往復時間の測定により、プライバシー強化による性能低下を最小限に抑えることができることを実証した。また、これらのサービスは大阪大学と兵庫県立大学においてデプロイし、公開サービスとしても提供している。

① 提案手法

μODNS は、ユーザーがネットワーク内に少なくとも 1 つの信頼できるリレーを持ち、そのリレーを他のユーザーと共有するという合理的な仮定に基づいている。提案手法は以下のステップで構成される。

1. リレーの選択：ユーザーは信頼できるリレーを次のホップリレーとして設定する。また、このリレーを他のユーザーと共有する。
2. クエリの転送：ユーザーの DNS クエリは、選択されたリレーを介してリゾルバに転送される。この際、クエリは他のエンティティと共有されるリレーをランダムに選択して転送される。
3. 共謀耐性：複数のリレーとリゾルバが共謀しても、ユーザーのアイデンティティは隠されたままである。リレー間の情報交換がランダムに行われるため、特定のリレーとリゾルバ間での共謀が困難になる。

② 評価結果

提案手法の有効性を評価するために、インターネット上での DNS メッセージの往復時間の測定を行った。評価項目は以下の通りである。

1. 匿名性の評価：提案手法がユーザーのアイデンティティをどの程度保護できるかを評価する。
2. 通信速度：提案手法の通信速度を評価し、従来の DNS プロトコルと比較する。
3. レイテンシ：提案手法のレイテンシを評価し、プライバシー強化による性能低下が最小限に抑えられるかを確認する。

実験結果から、μODNS は従来の DNS プロトコルと比較して、ユーザーの匿名性を高いレベルで保護することを確認した。また、通信速度およびレイテンシにおいても、プライバシー強化による性能低下が最小限に抑えられることを示した。

③ まとめ

本研究では、従来の DNS のセキュリティおよびプライバシー機能の欠如を克服するために、μODNS という新しいアプローチを提案し、その有効性を実験により評価した。提案手法は、複数のリレーを使用してユーザーの匿名性を確保し、リレーとリゾルバ間の共謀に対する耐性を持つ。

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Masuda Hiroki、Kita Kentaro、Koizumi Yuki、Takemasa Junji、Hasegawa Toru	４．巻 11
２．論文標題 Byzantine-Resilient Secure Federated Learning on Low-Bandwidth Networks	５．発行年 2023年
３．雑誌名 IEEE Access	６．最初と最後の頁 51754～51766
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2023.3277858	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 Kurihara Jun、Tanaka Toshiaki、Kubo Takeshi	４．巻 237
２．論文標題 μODNS: A Distributed Approach to DNS Anonymization with Collusion Resistance	５．発行年 2023年
３．雑誌名 Computer Networks	６．最初と最後の頁 110078～110078
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.comnet.2023.110078	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23件（うち招待講演　0件／うち国際学会　6件）

１．発表者名 北 健太朗，武政 淳二，小泉 佑揮，長谷川 亨
２．発表標題 ネットワーク層匿名化プロトコルにおいて匿名性と責任追跡性を両立する手法の設計に関する一考察
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 2023年

１．発表者名 増田 大輝，北 健太朗，武政 淳二，小泉 佑揮，長谷川 亨
２．発表標題 ユニキャストに基づく分散システム上のビザンチン耐性を持つ安全な連合学習の設計に関する一考察
３．学会等名 第194回マルチメディア通信と分散処理・第100回コンピュータセキュリティ合同研究発表会
４．発表年 2023年

１．発表者名
渡辺 龍，窪田 歩，栗原 淳

２．発表標題
エッジコンピューティング環境へのデータ圧縮手法の適用

３．学会等名
コンピュータセキュリティシンポジウム

４．発表年
2022年

１．発表者名
R. Watanabe, A. Kubota, J. Kurihara

２．発表標題
Application of Generalized Deduplication Techniques in Edge Computing Environments

３．学会等名
International Conference on Advanced Information Networking and Applications（国際学会）

４．発表年
2023年

１．発表者名
栗原 頂，栗原 淳，田中 俊昭

２．発表標題
ランプ型しきい値法のIndividual Insecurity

３．学会等名
電子情報通信学会 総合大会

４．発表年
2023年

１．発表者名
竹内廉，三橋力麻，西垣正勝，大木哲史

２．発表標題
セクション情報を考慮したアンサンブル型マルウェア分類器の提案

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2023年

１．発表者名
鈴木伶哉，竹内廉，柳生航平，西垣正勝，大木哲史

２．発表標題
感情を考慮した異常ログ生成手法についての検討

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2023年

１．発表者名
赤阪夢久，佐藤佑哉，前田壮志，西垣正勝，大木哲史

２．発表標題
特徴量変換器を用いたテンプレート復元攻撃の提案

３．学会等名
バイオメトリクスと認識・認証シンポジウム

４．発表年
2022年

１．発表者名
Muku Akasaka, Soshi Maeda, Yuya Sato, Masakatsu Nishigaki, Tetsushi Ohki

２．発表標題
Model-Free Template Reconstruction Attack with Feature Converter

３．学会等名
International Conference of the Biometrics Special Interest Group（国際学会）

４．発表年
2022年

１．発表者名
竹内廉, Vo Ngoc Khoi Nguyen, 西垣正勝, 大木哲史

２．発表標題
画像ベースマルウェア分類器に対するセクション情報が与える影響

３．学会等名
コンピュータセキュリティ研究会

４．発表年
2022年

１．発表者名
Hiroki Masuda, Kentaro Kita, Yuki Koizumi, Junji Takemasa, Toru Hasegawa

２．発表標題
Model Fragmentation, Shuffle and Aggregation to Mitigate Model Inversion in Federated Learning

３．学会等名
IEEE International Symposium on Local and Metropolitan Area Networks（国際学会）

４．発表年
2021年

１．発表者名
増田 大輝，北 健太朗，小泉 佑揮，武政 淳二，長谷川 亨

２．発表標題
連合学習における教師データのプライバシー保護のための学習プロトコルの設計に関する一考察

３．学会等名
電子情報通信学会ソサイエティ大会講演論文集

４．発表年
2021年

１．発表者名
増田 大輝，北 健太朗，小泉 佑揮，武政 淳二，長谷川 亨

２．発表標題
連合学習のためのモデル分割，シャッフル，集約によるモデル漏洩の防止に関する一考察

３．学会等名
コンピュータセキュリティシンポジウム

４．発表年
2021年

１．発表者名
Ngoc Khoi Nguyen Vo, Takamichi Terada, Masakatsu Nishigaki, Tetsushi Ohki

２．発表標題
EXAMINING OF SHALLOW AUTOENCODER ON BLACK-BOX ATTACK AGAINST FACE RECOGNITION

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

４．発表年
2021年

１．発表者名
井田 天星，竹内 廉，ヴォ ゴック コイ グエン，西垣 正勝，大木 哲史

２．発表標題
ブラックボックス型モデル反転攻撃におけるユーザ類似性を考慮した生成モデルの検討

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2022年

１．発表者名
Ryu Watanabe, Ayumu Kubota, and Jun Kurihara

２．発表標題
Resource Authorization Methods for Edge Computing

３．学会等名
International Conference on Advanced Information Networking and Applications（国際学会）

４．発表年
2022年

１．発表者名
Yutaro Yoshinaka, Junji Takemasa, Yuki Koizumi, and Toru Hasegawa

２．発表標題
gPHI: Lightweight Anonymity Protocol for Anonymity at Host and AS Levels

３．学会等名
IFIP Networking（国際学会）

４．発表年
2022年

１．発表者名
水門 巧実，小泉 佑揮，武政 淳二，長谷川 亨

２．発表標題
知識蒸留を用いた垂直連合学習におけるデータ漏洩攻撃の提案

３．学会等名
電子情報通信学会技術研究報告

４．発表年
2024年

１．発表者名
水門 巧実，小泉 佑揮，武政 淳二，長谷川 亨

２．発表標題
知識蒸留を用いた垂直連合学習におけるデータ漏洩攻撃に関する一考察

３．学会等名
電子情報通信学会総合大会講演論文集

４．発表年
2024年

１．発表者名
渡辺龍，窪田歩，栗原淳，櫻井幸一

２．発表標題
エッジコンピューティングにおけるリソース認可への自己主権型アイデンティティの適用

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
2024年

１．発表者名
R. Watanabe, A. Kubota, J. Kurihara, and K. Sakurai

２．発表標題
Extension of Resource Authorization Method with SSI in Edge Computing

３．学会等名
International Conference on Advanced Information Networking and Applications

４．発表年
2023年

１．発表者名
金山知美，田中俊昭，栗原 淳

２．発表標題
プライバシ保護を考慮したフィッシングサイト検知システム

３．学会等名
電子情報通信学会 総合大会

４．発表年
2024年

１．発表者名 栗原頂，栗原淳，田中俊昭
２．発表標題 線形秘密分散法とセキュアネットワーク符号化における新たな安全性尺度
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
４．発表年 2023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	栗原　淳 (Kurihara Jun) (10577399)	兵庫県立大学・情報科学研究科・准教授 (24506)	
研究分担者	大木　哲史 (Ohki Tetsushi) (80537407)	静岡大学・情報学部・准教授 (13801)	

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