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 １９ 日現在

機関番号：１７１０２
研究種目：基盤研究(B)（特設分野研究）
研究期間：2019～2023
課題番号：１９ＫＴ００２０

研究課題名（和文）通信・電磁情報と行動認識に基づくIoT機器に対するトラストの実現

研究課題名（英文）Creating trust for IoT devices by analyzing the network and electromagnetic information, and activity recognition

研究代表者

荒川　豊（Arakawa, Yutaka）

九州大学・システム情報科学研究院・教授

研究者番号：３０４２４２０３

交付決定額（研究期間全体）：（直接経費）　　14,300,000円

研究成果の概要（和文）：本研究では、IoT機器から送出される通信情報や電磁情報を観測し、機器とその動作を識別する「IoT活動量計」を実現した。通信トラフィックの分析により、スマートスピーカーの機能を56.4%で推定可能であることを示した。電磁波から内部処理を推定する手法も開発し、機器の環境や配線状態が影響することを明らかにした。プライバシー保護のため、差分プライバシーを用いて匿名性を保ちつつ精度を改善する手法を提案した。連合学習においては、エッジデバイスの性能差に応じた最適化手法を開発し、IEEE IoT Journal (Impact Factor 11.1)に採択された。

研究成果の学術的意義や社会的意義
本研究では、IoT機器の安全な利用を促進するため、機器から送信されるデータを監視し、機器の動作を識別する「IoT活動量計」を開発した。通信トラフィックや電磁波の解析によって，機器の種類や実行中の機能を特定できることを実証した．また、見守り等，行動認識が必要な状況でもプライバシーを保護を両立する連合学習手法を確立した．提案システムは，世界最高水準の論文誌への採択など、研究の学術的価値も高く評価されている．これらの成果は，IoT機器の普及に伴うプライバシーリスクを低減する一助となり，安心して新技術を活用できる社会の実現に貢献する．

研究成果の概要（英文）：We realized an "IoT activity meter" that identifies IoT devices and their operations by observing communication traffic and electromagnetic emissions. Through traffic analysis, it was shown that smart speaker functions could be estimated with 56.4% accuracy. A method for inferring internal processing from electromagnetic waves was also developed, revealing the impact of the device's environment and wiring conditions. To protect privacy while improving accuracy, a differential privacy method was proposed to maintain anonymity. For federated learning, an optimization method was developed to adapt to varying edge device performance and was accepted by IEEE IoT Journal (Impact Factor 11.1).

研究分野：情報ネットワーク

キーワード：IoT (Internet of Things)　セキュリティ　トラスト　差分プライバシー　連合学習　行動認識　通信トラヒック分析

様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

Amazon Echo, Google Home などの音声認識型の IoT（Internet of Things）機器は, VoiceLabs の発表では，2017 年末には 3300 万台に達するとされており，一般家庭のスマートホーム化は今後ますます進展していくことが予想される．同時に，IoT テディベアを介した情報漏えいや性玩具メーカーによる秘密裏な情報収集など, 家庭に普及した IoT 機器がトロイの木馬となって，プライバシー情報を送出する事件が相次いでいる．スマートフォンの場合，過去に同様の問題が起きた結果，現在では，アプリケーション毎に，位置情報や連絡先などの情報，カメラ，マイクなどの入力装置に対するアクセス権を簡単に設定可能になっている．

情報機器に対して，モノとしての安全性や性能を担保する手段として，工業標準化法に基づく JIS マークや電気用品安全法に基づく PSE マークなどがある．しかしながら，こうした**機器から送出される情報に対する安全性**を担保するような法律や基準は不明確であり，ユーザが安全性を判断する仕組みがない．

２．研究の目的

本研究の目的は，急速に広がる IoT 機器を安心して利用するために，情報機器に対するトラストを構築する手段を提供することである．その実現のため, 機器からどのようなデータがクラウド上にアップされているかを誰もが簡単に検知，理解，遮断することを可能にするプラットフォームを実現することを目標とする．

３．研究の方法

本研究では，図１に示すように，IoT 機器から送出される通信情報および電磁情報に基づいた，機器とその動作識別技術を開発し, **IoT 活動量計**としてユーザに提示することで，購入した機器に対するトラストを形成する．各種 IoT 機器は有線 LAN および無線 LAN を介してインターネットに接続されるものとし, IoT 機器から発信される通信情報と電力情報は，無線ルータおよび配電盤で収集するものとする．ルータ内の提案システムは，暗号化されている通信内容には触れず，宛先 IP アドレスやパケットサイズなど，通信情報だけを観測する．配電盤内の提案システムは，消費電力量や電磁ノイズ情報を観測する．どちらのシステムも，クラウド上のデータベースと定期的に情報を交換しており，観測した通信情報や MAC アドレス, 消費電力情報や電磁情報などから機器とその動作を識別する．新たに接続された機器である場合は，ユーザのスマートフォンに通知し，その機器が何であるか，心当たりがあるかを確認し，登録する．登録後は, **IoT 活動量計**と呼ぶ機能を介して, IoT 機器の動作状況をいつでも確認することができる．さらに，発展的な研究として，このような行動識別に利用できる家庭内のデータを安全に共有する差分プライバシー手法や, 複数家庭で機械学習のモデルを安全に共有する連合学習（Federated Learning）に関する研究も実施する．

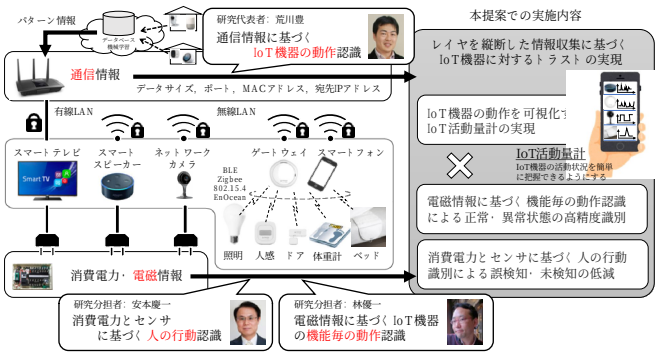

図１　研究概要

４．研究成果

2019 年度は，さまざまな IoT 機器を購入・設置し, 動作と機能を確認するとともに, 機能が発動した際に, IoT 機器から送出される通信パケットや電磁波を観測するシステムを構築し，発動される機能による違いを観察できるようにした. 電磁波観測システムは, 奈良先端大で開発しており，実験室内で IoT 機器からの電磁波を計測できるようになっている. 一方, 通信パケットの観測システムは, 九州大学で開発しており，大学内の住宅模擬設備(2DK)に IoT 機器とともに設置されているため，実環境に近い状態でデータを観測できるようになっている．

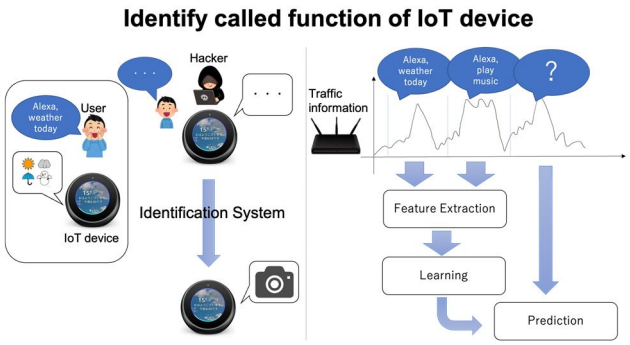

図２　IoT 機器の発動機能推定

2020 年度は，IoT 機器の中でもスマートスピーカーに焦点を当て，これまでに構築した観測システムを用いて，通信トラヒック分析に基づく発動機能推定に関する研究（図２）を進め，国内

会議 DICOMO2020 および国際会議 SAC2021 で発表した．さらに，漏えいする電磁波の計測に基づく内部処理推定に関する研究や精度改善のための行動認識に関する研究やプライバシーを保護するアップロード頻度調整手法について研究を進めた．スマートスピーカーの動作に関しては，通信トラヒックを機械学習によって学習することで，Amazon Echo Spot の 8 種類の機能を 56.4%で推定可能であることがわかった．一方，電磁波に基づく内部処理推定については，スマートスピーカーが設置される環境や給電線の接続状態が影響を与えることが明らかになった．また，行動計測では，消費電力センサ，人感センサ，環境センサを組み合わせ，リアルタイムに行動認識を行うシステムを構築した．さらに，プライバシーを保護する通信手法として，通信トラヒックから行動がわかってしまうという問題への対処策を検討し，トラヒックパターンを意図的に変化させてクラウドにアップロードする手法を提案した．

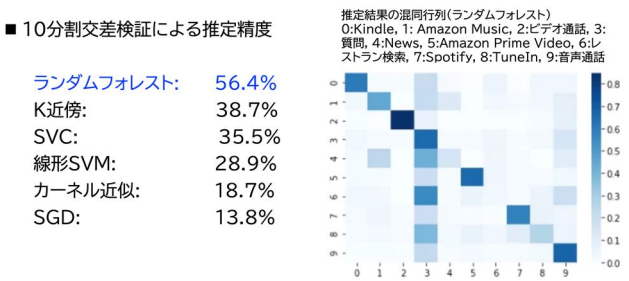

図３　発動機能の認識結果

2021 年度は，これまでに構築してきた通信トラヒックの収集と機械学習による機器および発動機能推定システムに，ユーザ側からの制御を行う部分を追加し，「IoT 活動量計」のプロトタイプを完成させた（図４）．プロトタイプでは，ソフトウェアルータ向けオープンソース OS である VyOS を用いて無線ルータを構築し，その内部機能として，トラヒック分析による機器および発動機能推定，ユーザ向けの制御インターフェースを実装している．

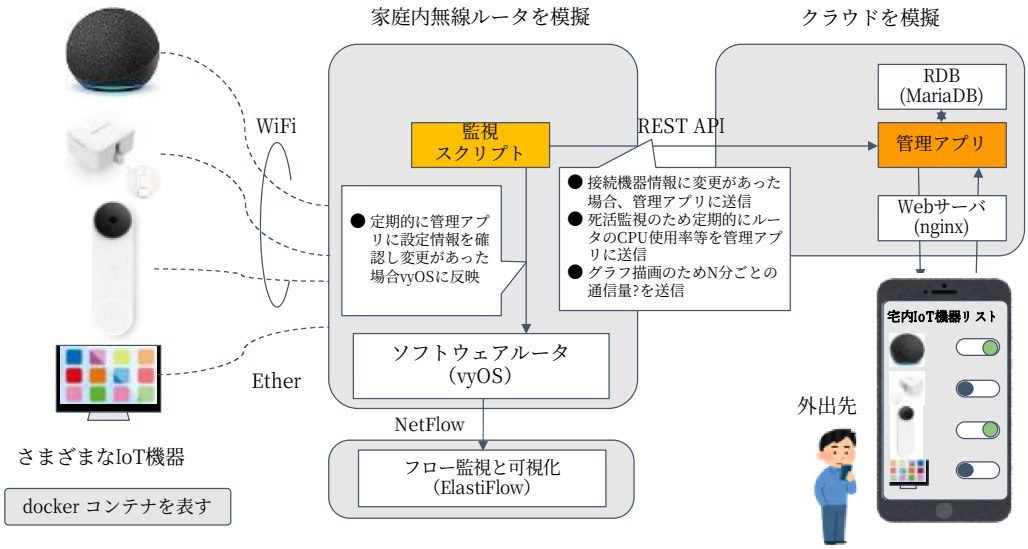

図４　開発した IoT 活動量計の構成図

さらに，IoT 機器への攻撃の一例として，非可聴域の音波を利用したドルフィンアタックへの対処を検証するための日常生活中のシナリオ 4 つを検討し，スマートホーム内に実験環境を設定した．また，IoT 機器から漏えいする電磁情報から機器の内部情報を推定する手法の高精度化にも取り組んだ．具体的には，複数の IoT 機器が宅内に存在する環境において，配電盤に伝搬する電磁情報を時間および周波数領域で計測し，計測情報からターゲットとする機器の内部情報を推定する手法を開発した．

2022 年度は，昨年度に VyOS をベースに構築した IoT 機器の通信監視および作動アプリケーション認識システムについて評価を行い，その内容をジャーナル論文にまとめ，採択された．また，その内容を国際会議および国内会議でも発表し，国際会議 ABC2022 においては，Excellent Paper Award を受賞した．IoT 機器のトラヒックから機能を推定できることから，悪意のある使い方をすれば，家庭内の IoT センサの情報から個人の行動が透けて見える可能性がある．そこで，このようなプライバシー上の問題を解決することを目的として，差分プライバシーに関する研究に取り組んだ．プライバシー保護と行動認識精度はトレードオフの関係にあるため，精度を可能な限り維持しつつ，個人を特定されないようにする手法を検討した．その結果，行動認識に用いる機械学習における特徴量寄与度に重みを変更した差分プライバシー手法を提案（図４）し，国内および国際会議で発表した．提案手法は，ユーザ認識モデルと行動認識モデル，それぞれにおける特徴量の寄与度を算出し，ユーザ認識モデルに対して寄与度の大きな特徴量にはより多くのノイズを加算することで，匿名性を向上させるものである．２つの行動認識用データセットを用いて評価した結果，従来の Laplace メカニズムと同等の匿名性を保ちながら，行動認識精度を

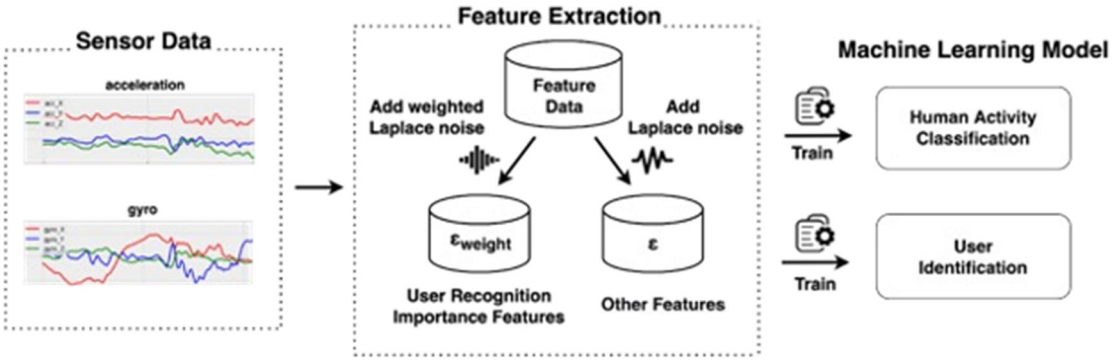

図４　重み付きε-差分プライバシーによる学習モデル

10%以上改善できることを示した．

2023 年度は，これまで開発してきた通信トラヒック観測に基づき，IoT 機器ならびにその機器

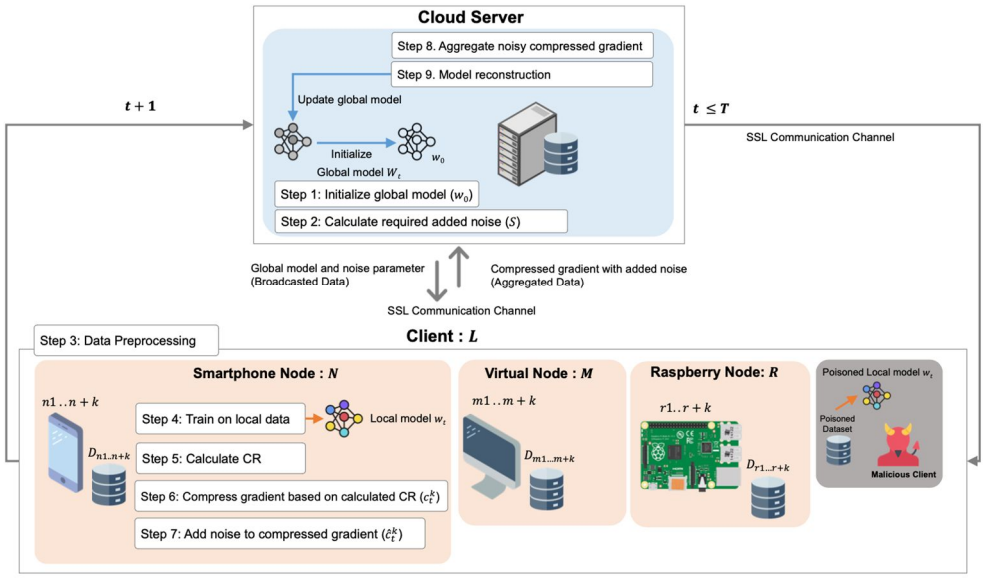

図５　不均一なエッジを対象とした連合学習のアーキテクチャ

上で発動している機能を認識するシステムを進化させ，数秒の短い通信トラヒック観測だけでもそれらを判別可能にするアルゴリズムを提案し，国際会議 ABC2023 で発表した．また，行動認識についてはスマートウォッチを用いたタイピング文字推定に関する研究を進め，タイピング中の加速度やタイピング音からユーザが何をタイプしているか盗聴可能であることを示し，国際会議 ICMU2023 で発表した．さらに，発展的な研究として，データのプライバシーを守りながら行動認識などに利用する仕組みとして，差分プライバシーや連合学習についても研究を進めた．その成果として，ハードウェアの性能が低く，さらにその性能が不均一な環境において，離散コサイン変換による重みつきプルーニングによるマスキングと適用ガウシアンクリッピングによる差分プライバシーを組み合わせることで，各エッジサーバの残リソースに応じて，高い性能を達成可能な連合学習手法は，国際会議 MDM2023 において最優秀デモンストレーション賞を受賞するとともに，インパクトファクター11 を超えるトップジャーナル IEEE IoT Journal に採択されるなど，想定を超える成果が得られた．

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 Hattori Yuichi、Arakawa Yutaka、Koike Daichi、Ishida Shigemi、Inoue Sozo	４．巻 34
２．論文標題 Function-level Access Control System for Home IoT Devices	５．発行年 2022年
３．雑誌名 Sensors and Materials	６．最初と最後の頁 2125～2125
掲載論文のDOI（デジタルオブジェクト識別子） 10.18494/SAM3901	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 Hidayat Muhammad Ayat、Nakamura Yugo、Arakawa Yutaka	４．巻 11
２．論文標題 Privacy-Preserving Federated Learning With Resource-Adaptive Compression for Edge Devices	５．発行年 2024年
３．雑誌名 IEEE Internet of Things Journal	６．最初と最後の頁 13180～13198
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/JIOT.2023.3347552	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19件（うち招待講演　0件／うち国際学会　9件）

１．発表者名 Ryusei Fujimoto, Yugo Nakamura, Yutaka Arakawa
２．発表標題 Differential Privacy with Weighted e for Privacy-Preservation in Human Activity Recognition
３．学会等名 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops, PrivaCom 2023)（国際学会）
４．発表年 2023年

１．発表者名 Yuichi Hattori, Yutaka Arakawa, Sozo Inoue
２．発表標題 Function Estimation of Multiple IoT Devices by Communication Traffic Analysis
３．学会等名 The 4th International Conference on Activity and Behavior Computing (ABC2022)（国際学会）
４．発表年 2022年

１．発表者名
藤本 隆晟，中村 優吾，荒川 豊

２．発表標題
行動変容支援サービスにおけるユーザ保護と有用性を両立する重み付きe-差分プライバシーの提案

３．学会等名
情報処理学会IoT行動変容学研究グループ 第2回研究会（IPSJ BTI2）

４．発表年
2022年

１．発表者名
服部 祐一，荒川 豊，井上 創造

２．発表標題
通信トラヒック分析による複数のIoTデバイスにおける機能推定手法の評価

３．学会等名
情報処理学会DICOMOシンポジウム 2022

４．発表年
2022年

１．発表者名
Research Dawadi, Teruhiro Mizumoto, Yuki Matsuda, Keiichi Yasumoto

２．発表標題
PATROL: Participatory Activity Tracking and Risk Assessment for Anonymous Elderly Monitoring

３．学会等名
Sensors 22(18): 6965, 2022.（国際学会）

４．発表年
2022年

１．発表者名
張志華，松井智一，上田浩行，高野誠也，藤本大介，林優一，安本慶一 ，荒川豊

２．発表標題
電磁・通信・家電情報に基づくIoT活動量計の検討

３．学会等名
第29回マルチメディア通信と分散処理ワークショップ（DPSWS2021）

４．発表年
2021年

１．発表者名
上田浩行，高野誠也，藤本大介，林優一

２．発表標題
音声の周波数スペクトルに着目したスピーカーフォンからの電磁的情報漏えい評価法

３．学会等名
電子情報通信学会ハードウェアセキュリティ研究会（HWS）

４．発表年
2022年

１．発表者名
小池 大地， 石田 繁巳， 荒川 豊

２．発表標題
通信トラヒック分析に基づくIoTデバイスの発動機能推定手法の検討

３．学会等名
マルチメディア，分散，協調とモバイル(DICOMO2020)シンポジウム

４．発表年
2020年

１．発表者名
Daichi Koike, Shigemi Ishida, Yutaka Arakawa

２．発表標題
Called Function Identification of IoT Devices by Network Traffic Analysis

３．学会等名
The 36th ACM/SIGAPP Symposium On Applied Computing (SAC2021)（国際学会）

４．発表年
2021年

１．発表者名
佐藤 佑磨，大山 航平，立花 巧樹，林 涼弥，宮地 篤士，松井 智一，中村 優吾，諏訪 博彦，安本 慶一

２．発表標題
スマートホームにおけるナッジを用いたオンライン行動認識システムの検討

３．学会等名
第40回社会システムと知能合同研究会（SIG-SAI）/ 社会システムと情報技術研究ウィーク（RST ’21）

４．発表年
2021年

１．発表者名
Sopicha Stirapongsasuti, Yugo Nakamura, Keiichi Yasumoto

２．発表標題
Privacy-Aware Sensor Data Upload Management for Securely Receiving Smart Home Services

３．学会等名
IEEE SMARTCOMP 2020（国際学会）

４．発表年
2020年

１．発表者名
福嶋 章悟, 藤本 大介, 林 優一

２．発表標題
設置環境の異なるスマートスピーカーからの電磁的情報漏えい評価と対策

３．学会等名
ハードウェアセキュリティ研究会(HWS)

４．発表年
2021年

１．発表者名
荒川豊

２．発表標題
IoT機器に対するトラストの実現

３．学会等名
東北大学 電気通信研究所共同プロジェクト20 周年記念研究会

４．発表年
2019年

１．発表者名
Gangkai Li, Yutaka Arakawa, Yugo Nakamura, Hyuckjin Choi, Shogo Fukushima, Wei Wang

２．発表標題
WatchLogger: Keyboard Typing Words Recognition Based on Smartwatch

３．学会等名
The 14th International Conference on Mobile Computing and Ubiquitous Networking (ICMU2023)（国際学会）

４．発表年
2023年

１．発表者名
Yuichi Hattori , Yutaka Arakawa, Sozo Inoue

２．発表標題
Evaluation of Functional Estimation Methods in IoT Devices at Intervals of a Few Seconds by Communication Traffic Analysis

３．学会等名
The 5th International Conference on Activity and Behavior Computing (ABC2023)（国際学会）

４．発表年
2023年

１．発表者名
Muhammad Ayat Hidayat, Yugo Nakamura, Billy Dawton, Yutaka Arakawa

２．発表標題
AGC-DP:Differential Privacy with Adaptive Gaussian Clipping for Federated Learning

３．学会等名
The 24th IEEE International Conference on Mobile Data Management (MDM 2023)（国際学会）

４．発表年
2023年

１．発表者名
Muhammad Ayat Hidayat, Yugo Nakamura, Yutaka Arakawa

２．発表標題
Efficient and Secure: Privacy-Preserving Federated Learning for Resource-Constrained Devices

３．学会等名
The 24th IEEE International Conference on Mobile Data Management (MDM 2023): Demo Paper（国際学会）

４．発表年
2023年

１．発表者名
服部 祐一, 荒川 豊, 井上 創造

２．発表標題
通信トラヒック分析に基づく数秒間隔でのIoTデバイスの機能判定手法

３．学会等名
マルチメディア、分散、協調とモバイル (DICOMO2023) シンポジウム

４．発表年
2023年

１．発表者名 藤本 隆晟，中村 優吾，荒川 豊
２．発表標題 時系列心拍データを用いたサービスにおけるユーザ保護と有用性を両立する差分プライバシー手法の検討
３．学会等名 第37回 人工知能学会全国大会（企画セッション:生体信号を活用した医療・ヘルスケアAI）
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	安本　慶一 (Yasumoto Keiichi) (40273396)	奈良先端科学技術大学院大学・先端科学技術研究科・教授 (14603)	
研究分担者	林　優一 (Hayashi Yuichi) (60551918)	奈良先端科学技術大学院大学・先端科学技術研究科・教授 (14603)	

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