社会課題解決に向けた
パーソナルデータ活用機械学習モデルとプライバシ

所属：　電気通信大学　大学院情報理工学研究科　情報学専攻

助成対象者：清雄一

共同研究者：大須賀昭彦、田原康之

概要

長寿化や経済格差の拡大などの社会問題に対処するためには、生体情報や行動情報など、センサから得られる個人データを使用した統計解析や機械学習が有効である。この流れで、個人のデータを学習データとして使用した学習済みの機械学習モデルを公開するサービスが普及している。今後は、さまざまな場所で多種多様な学習済み機械学習モデルが生み出され公開される、ユビキタス機械学習社会の到来が予想される。様々な IoT システムから集められる個人データを保護する技術の開発が目標である。

abstract

To address societal issues such as increasing longevity and economic inequality, machine learning using personal data from sensors, including biometric and behavioral information, have proven effective. At the same time, there has been a proliferation of services that publish machine learning models trained on individuals' data. It is expected that a ubiquitous machine learning society will emerge, characterized by the generation and publication of a wide variety machine learning models in different domains. The development of technologies to protect personal data collected from various IoT systems is a critical goal.

研究内容

① 誤差・欠損値を含む個人データに対する連合学習手法の提案

連合学習は、分散された個人データに対してプライバシを保護しながら機械学習を行うフレームワークとして注目を集めている。たとえば、スマートフォン上でのコンバージョン履歴の予測や病院が持つ電子カルテを機械学習で利用するシナリオが考えられる。しかしこれまでの研究では、各組織が持つデータ属性の均一性を前提としており、データに欠損や誤差が多く含まれていることの考慮が不足している。この制限を克服するために本研究では、欠損・誤差が多く含まれる場合でも高い機械学習精度を実現する連合学習アルゴリズムを提案した。

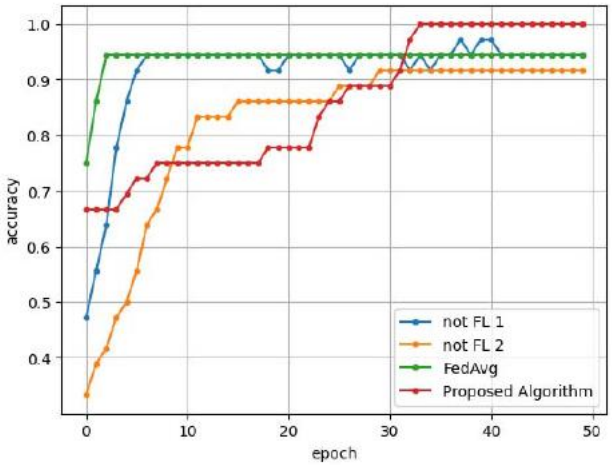

図 1. 連合学習で達成した精度

図 1 に示すとおり、ベースライン手法と比較して提案アルゴリズムが高い精度を実現する結果が得られた。

② 測定誤差を考慮したプライバシ保護フレームワークの提案

近年、「差分プライバシ」技術に基づくプライバシ保護手法が注目を集めている。保護すべき個人データが IoT 機器により測定された場合、その測定値に対してノイズを加えることで差分プライバシは達成される。しかしノイズの追加はデータの有用性を低下させる。本研究では、測定機器によって得られた値には誤差が含まれているという事実に着目し、目標するプライバシ保護レベルを一定に保ったままノイズの量を減らすアルゴリズムを提案した。図 2 に示すとおり、提案アルゴリズムである T-Geo-I はベースライン手法と比べてノイズ付与量を小さくすることを可能とした。

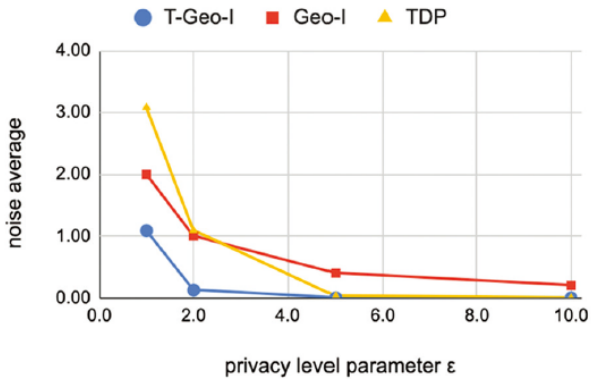

図 2. 目標とするプライバシ保護レベル（横軸）とノイズ負荷量（縦軸）

③ IoT 機器の脆弱性検出ミドルウェアの提案

IoT 機器の脆弱性を狙ったサイバー攻撃が年々増加しており、この攻撃を通じて個人情報が暴かれるリスクが増大している。既存の研究で提案されている IoT 機器の脆弱性検出ツールは分析カバレッジが低く、攻撃を見逃してしまうリスクがある。本研究では、この問題に対処するために IoT ファームウェアの静的分析を行うためのミドルウェアを提案・開発して公開した（図 3）。高速に脆弱性を検出し、また、様々な IoT 機器に対応できることが特徴である。さらに、一般ユーザが使いやすいインタフェースを有している。

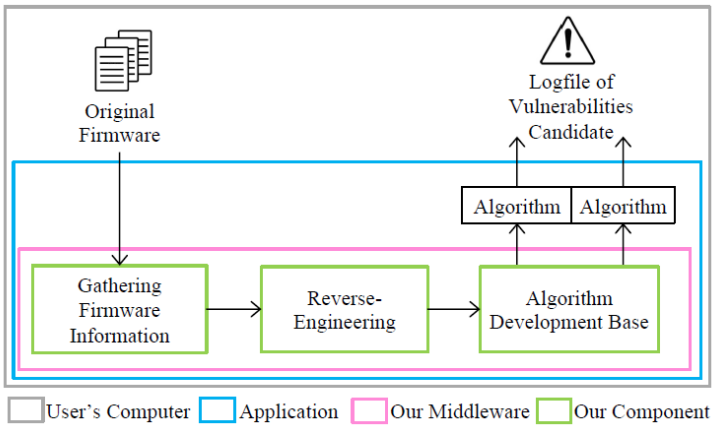

図 3. IoT 機器の脆弱性検出ミドルウェア

以上の研究のほか、ヘルスケア情報を対象としたブロックチェーン技術によりプライバシを保護するための調査を網羅的に行いサーベイ論文として公開した。睡眠状況、マスクに隠された部分の顔画像等の推測を行うアルゴリズムを開発し、プライバシ保護に関するリスクについての検討を行った。また、データ間の関係性を推測する技術を提案し、意図しない個人データの漏洩につながりうる関係性について考察を行った。

本助成に関わる成果物

［論文発表］

1. Keiichiro Oishi, Yuichi Sei, Andrew J, Yasuyuki Tahara, Akihiko Ohsuga: Algorithm to Satisfy l-diversity by Combining Dummy Records and Grouping, Security and Privacy, 2024
2. Riho Isawa, Yuicih Sei, Yasuyuki Tahara, Akihiko Ohsuga: Minimizing Noise in Location Privacy Protection Through Equipment Error Consideration, International Journal of Electrical and Computer Engineering Systems, Vol.15, No.3, pp.285-296, 2024
3. Takao Murakami, Yuichi Sei: Automatic Tuning of Privacy Budgets in Input-Discriminative Local Differential Privacy, IEEE Internet of Things Journal, Vol.10, No.18, pp.15990-16005, 2023
4. Andrew J, Deva Priya Isravel, K. Martin Sagayam, Bharat Bhushan, Yuichi Sei, Jennifer Eunice: Blockchain for Healthcare Systems: Architecture, Security Challenges, Trends and Future Directions, Journal of Network and Computer Applications, Vol.215, No.103633, pp.1-36, 2023

［口頭発表］

1. Yuichi Sei: Integrating Behavioral, Biometric, and Environmental Data for Health Insights, International Conference on Health Informatics, Intelligent Systems and Networking Technologies, 2024 (Invited)
2. Tetsumaru Akatsuka, Ryohei Orihara, Yuichi Sei, Yasuyuki Tahara and Akihiko Ohsuga: Reconstruction of Facial Geometry from Face-Masked Images Using Voice Cues, 16th International Conference on Agents and Artificial Intelligence (ICAART), 2024
3. Minami Yoda, Shigeo Nakamura, Yuichi Sei, Yasuyuki Tahara, Akihiko Ohsuga: A Scalable Middleware for IoT Vulnerability Detection, 26th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), "Studies in Computational Intelligence," Springer, 2024
4. Tetsumaru Akatsuka, Ryohei Orihara, Yuichi Sei, Yasuyuki Tahara and Akihiko Ohsuga: Estimation of Unmasked Face Images Based on Voice and 3DMM, 36th Australasian Joint Conference on Artificial Intelligence (AJCAI), pp.239-251, 2023

5. Minami Yoda, Shigeo Nakamura, Yuichi Sei, Yasuyuki Tahara, Akihiko Ohsuga: A Middleware to Improve Analysis Coverage in IoT Vulnerability Detection, 6th IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), pp.103-107, 2023
6. Keiichiro Oishi, Yuichi Sei, Yasuyuki Tahara, Akihiko Ohsuga: Federated Learning Algorithm Handling Missing Attributes, 6th IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), pp.146-151, 2023
7. 赤塚哲丸，折原良平，清雄一，田原康之，大須賀昭彦：音声と 3DMM に基づくマスクを除去した顔画像の推定，合同エージェントワークショップ＆シンポジウム (JAWS)，信学技報，Vol.123，No.190，pp.187-193，2023
8. 石禾里帆，清雄一，田原康之，大須賀昭彦：測定機器の誤差を利用した効果的な位置情報プライバシ保護手法の提案，合同エージェントワークショップ＆シンポジウム (JAWS)，信学技報，Vol.123，No.190，pp.77-82，2023
9. Atsuya Tsuda, Kazutaka Matsuzaki, Yuichi Sei：Developing REM Sleep Prediction Models Using Smart Home Sensor Data, 2nd IEEE World Conference on Applied Intelligence and Computing (AIC), pp.851-856, 2023

[ポスター発表]

1. Riho Isawa, Yuicih Sei, Yasuyuki Tahara, Akihiko Ohsuga: Enhance Data Usefulness in Privacy Protection Under Considering IoT Measurement Error, 16th International Conference on Agents and Artificial Intelligence (ICAART), 2024

[その他]

〈受賞〉

1. IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS) Best Paper Award, 2023
2. IEEE Computer Society Japan Chapter JAWS Young Researcher Award, 2023
3. 電気通信普及財団賞テレコム学際研究賞，2024
4. 日本冷凍空調学会 学術賞，2023

〈書籍〉

1. Yuichi Sei, Keiichiro Oishi, Yasuyuki Tahara, Akihiko Ohsuga, Agbotiname Lucky Imoize: Differentially Private Human Interactions for the Real World and the

Metaverse, chapter in book ″Advanced Metaverse Wireless Communication Systems″, 2024

2. Yuichi Sei, Keiichiro Oishi, Yasuyuki Tahara, Akihiko Ohsuga, Agbotiname Lucky Imoize: Enhancing Machine Learning Accuracy in the Metaverse: Overcoming Noise and Error in Object Counting Systems, chapter in book ″Advanced Metaverse Wireless Communication Systems″, 2024
3. Yuichi Sei: Privacy-Preserving Data Collection and Analysis for Smart Cities, chapter in book ″Human-Centered Services Computing for Smart Cities″, IEICE Monograph, Springer, 2024
4. Riho Isawa, Yuicih Sei, Yasuyuki Tahara, Akihiko Ohsuga, Agbotiname Lucky Imoize: Location Information Privacy Protection Method Considering Human Presence Probability, chapter in book ″Artificial Intelligence and Blockchain Technology in Modern Telehealth Systems″, The Institution of Engineering and Technology (IET), Chapter 17, pp.497 -521, 2023
5. Yuichi Sei, Akihiko Ohsuga, J. Andrew Onesimu, Agbotiname Lucky Imoize: Local Differential Privacy for Artificial Intelligence of Medical Things, chapter in book ″Handbook of Security and Privacy of AI Enabled Healthcare Systems and Internet of Medical Things″, CRC Press (Taylor & Francis), Chapter 10, pp.241-270, 2023
6. Yuichi Sei, Akihiko Ohsuga, Agbotiname Lucky Imoize: A Lightweight Algorithm for Detection of Fake Incident Reports in Wireless Communication Systems, chapter in book ″Security and Privacy Schemes for Dense 6G Wireless Communication″, The Institution of Engineering and Technology (IET), Chapter 11, pp.235-260, 2023

〈メディア掲載〉

「マスクに隠れた顔を AI で再現」日本経済新聞朝刊 16 面, 2024

「マスクで隠れた部分を AI が予測…“声”で精度 UP？」ABEMA ヒルズ, 2024

「AI・ゲノムで個人特定、犯罪捜査に道 情報保護が課題」日本経済新聞, 2024

「Enhance data usefulness in privacy protection under considering IoT measurement error」EurekAlert, 2024

「Study addresses privacy-preserving collaborative data collection and analysis with many missing values」, 2023