IoT が拓く未来
2019 年度採択研究者

2021 年度
年次報告書

清　雄一

電気通信大学　大学院情報理工学研究科
准教授

Web/IoT 横断的プライバシ保護データ解析基盤

§1. 研究成果の概要

様々な人や組織がIoTデータ及びWeb上のデータを横断的に活用した新たなサービスの構築・普及を考えており、今後これらのデータを流通させ、組み合せて活用していく制度やインフラが整っていくことが予想される。しかしながら、どこから個人のプライバシ情報が漏洩するかを予想することが困難になり、プライバシを保護する共通的で強固な枠組みの構築が重要な課題となる。

2021年度は主に、誤差・欠損を含むデータに対するプライバシ保護、組合せデータに対するプライバシ保護、プライバシ保護機械学習および機械学習への毒データ攻撃への対応、IoTデータ収集の各テーマに取り組んだ。各テーマの主な成果として、まずIoTの観測誤差が大きい場合に目標となるプライバシ保護レベルを維持したまま差分プライバシに基づくノイズの量を減らすことができるアルゴリズムを提案した。観測誤差を数学的に厳密に取り扱い、プライバシ保護レベルを維持できることを証明した上で、データの有用性を向上できることを、実データを用いたシミュレーションにより示した。また、データ間の隠れた関係を導出する手法および欠損しているデータの値を高精度に推測する手法を開発しており、個人に関する属性値の推測精度を向上させることができた。また同じ属性値をもつほかのユーザ数の推定値に基づいて動的にプライバシ保護レベルを決定する手法を開発、23人の被験者におけるIoTデータの公開を行った。さらに、IoTデータ機器への攻撃によるプライバシ情報漏洩を防ぐため、IoT機器のバックドア攻撃の検知手法を開発した。ユーザからのインプットに着目し、これまでよりも擬陽性の割合を大幅に減らすことが可能となった。

【代表的な原著論文情報】

1) Privacy-Preserving Collaborative Data Collection and Analysis with Many Missing Values, IEEE Transactions on Dependable and Secure Computing, 2022
2) Differential Privacy Featuring Errors to Deal with Internet-of-Things Data, IEEE Access, Vol.10, pp.8738-8757, 2022
3) Detecting Hardcoded Login Information from User Input, 40th IEEE International Conference on Consumer Electronics (ICCE), pp.104-105, 2022
4) A Countermeasure Method Using Poisonous Data Against Poisoning Attacks on IoT Machine Learning, International Journal of Semantic Computing, Vol.15, No.2, pp.215-240, 2021
5) Improvement of Legitimate Mail Server Detection Method using Sender Authentication, 18th IEEE/ACIS International Conference on Software Engineering, Management and Applications (SERA), pp.10-14, 2021