SEEDS

情報・通信

寺田（テラダ） 雅之（マサユキ） 教授

工学部 情報工学科

■ 研究業績等

【著書】
・著書 『Advances in Information and Computer Security: 8th International Workshop on Security, IWSEC 2013 Okinawa, Japan, November 18-20, 2013, Proceedings』Springer（共編）: 2013/11

【論文】
・学術論文 「Detection of Non-designated Evacuation Shelters from Real-time Population Dynamics using Autoencoder-based Anomaly Detection」ACM Trans. Spatial Algorithms and Systems（TSAS）（共著）: 2024/10
・学術論文 「圧縮メカニズム再考：スパースな観測行列を用いた圧縮センシングによる差分プライバシーの実現」情報処理学会論文誌（共著）: 2024/9
・学術論文 「公的統計に対する差分プライバシーの適用と有効性の評価に関する検討―国勢調査を例に―」統計研究彙報（共著）: 2024/3

【学会発表】
・「End-to-End Privacy-Preserving Vertical Federated Learning using Private Cross-Organizational Data Collaboration（Poster）」ACM Conf. Computer and Communications Security 2024（ACM CCS 2024）（査読付）: 2024/10
・「大規模集計データへのzCDPの適用」コンピュータセキュリティシンポジウム 2024（CSS2024）: 2024/10
・「秘匿クロス統計技術を用いたデータ入出力のプライバシを保護した垂直連合学習」マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2024）: 2024/6

キーワード　プライバシー保護　データ活用　差分プライバシー

対応可能なもの ■講演 □研修 ■研究相談（学術指導） □学術調査 □コメンテーター ■共同研究・受託研究

「健全なデータ活用」を普及・発展させるための差分プライバシー保証技術

研究の概要

「DX の時代」や「AI の時代」などのキーワードが象徴するように、これからの時代における社会や産業の発展や競争力の確保には、経済や社会、人々の行動などに関するさまざまなデータを活用していくことが不可欠となりつつあります。

しかし、それらのデータは社会に役立つ示唆を与える一方で、個人のプライバシーに関する情報を含むことも多く、いくら役に立つからと言っても、その活用にあたってそれらを暴露するようなことがあってはなりません。

そこで、このようなプライバシーの暴露を起こすことなく、安全にデータを活用するための技術、すなわち「プライバシー保護技術」が、今後の健全なデータ活用の普及や発展のためには極めて重要になってきます。

その実現に向け、差分プライバシー（Differential Privacy）と呼ばれる技術に着目し、さまざまな実社会の大規模データに対し、数理的に安全性が保証されたプライバシー保護を、実用的な精度や効率で実現するための技術の実現に取り組んでいます。

研究の詳細

□研究・技術のプロセス □研究事例 ■研究成果 ■使用用途・応用例 ■今後の展開

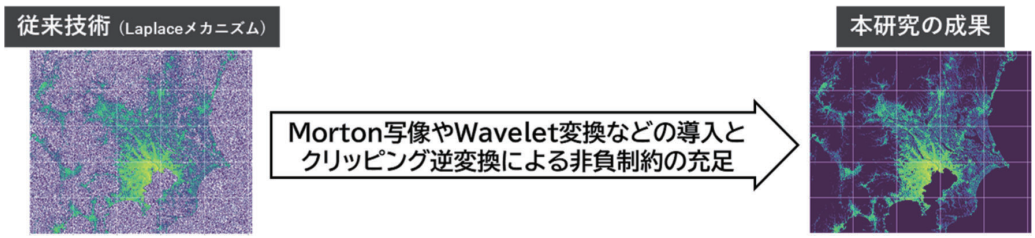
差分プライバシーは、（たとえば k- 匿名性などの）旧来のプライバシー保護手法とは異なり、どのような攻撃に対しても、データに含まれる誰一人として決定的にプライバシーが暴露されることはない、という強力な安全性保証を与えます。

その一方で、差分プライバシーを実用的な形で適用することは簡単ではなく、単純な形で適用しようとするとノイズが大きくなりすぎたり、現実の統計としては「ありえない」値が出力されたりするなどの課題がありました。

この問題に対し、局所性保存写像や Wavelet 変換の導入によるノイズ影響の緩和や非負制約の充足などを通じ、高次元の大規模データに対して実用的に差分プライバシーを適用する技術を開発しました。

この研究成果は、携帯電話基地局の運用データに基づくリアルタイム人口統計におけるプライバシー安全性を実現する礎となり、新型コロナウイルスの感染対策や高速道路の渋滞予測などの実社会における課題解決に貢献するとともに、科学技術分野における文部科学大臣表彰（科学技術賞）をはじめとする数々の表彰を受賞するなどの評価を受けています。

さらに、この技術に対してレニー情報量に基づくプライバシー計量などの、プライバシー保護に関する最新の理論発展の成果を組み合わせることなどにより、その適用領域をさらに拡大し、実用性を高める研究を進めています。



産学官連携先に向けたアピールポイント

・EU をはじめとする世界的なプライバシー保護の重視や法制度等の厳格化の潮流において、数理的なプライバシー安全性の保証を通じてデータの「健全な活用」を推進する技術です

ご連絡窓口　京都橘大学リエゾンオフィス（学術振興課）　TEL：075-574-4186　E-mail：aca-ext@tachibana-u.ac.jp