研究計画・目的

個人情報保護とデータ利活用における先進的な欧州において，UNESCO Data Privacy Chair を始め多くのデータプライバシープロジェクトを主宰する Universitat Rovira i Virgili (URV)大学 Josep Domingo-Ferrer 特別教授 (Distinguished Full Professor of Computer Science) である研究室を訪問し，データプライバシーに関する共同研究を行うことを目的として，2022 年度の在外研究を実施した．当初の計画では，2020 年度に実施の予定であったが，新型コロナウィルスの世界的なパンデミックにより 2 年間延期し，更に 2023 年 2 月からのウクライナ情勢によりフライトのキャンセルが続き，ようやく出国できたのは 2 年 1 ヶ月後の 2022 年 5 月 14 日であった．

新特例措置を適用し，2022 年 5 月 14 日より 2023 年 2 月 28 日まで，URV のあるスペインカタルーニャ州 Tarragona に滞在し，研究活動を実施した．2023 年 3 月 1 日より 3 月 31 日までは，京都大学医学部付属病院の森由希子講師とヘルスケアデータのプライバシー強化に関する共同研究を行った．京都大学附属病院では，新型コロナ感染対策の為に学外者に対する制約が多く，ほとんどの活動は在宅にてオンラインで実施した．

研究活動

Domingo-Ferrer 教授の研究室には，データプライバシーを中心として，連携学習におけるバックグランド攻撃，機械学習における公平性検出，説明可能 AI，テキストデータ匿名化などの幅広いテーマについて探求を続けている．これらの中で，次のような共同研究を行った．

- 多次元データのランダマイズドレスポンス
  データを置換することによりプライバシーを保証するアルゴリズムを多次元データに適用する研究．変数間の相関に応じてクラスタリングンを行い，相関の強い変数間を統合して匿名化することで，データの利便性と安全性を両立させる方式を提案した．提案手法の評価を，CSS 2022 と IFIP SEC 2023(業績 5, 7)にて発表予定である．
- 人物識別カメラにおける説明可能性
  顔領域を匿名化しても，歩容特徴量から人物が識別可能であることを指摘している（業績 3)．博士課程大学院生 Rami Haffar 氏と，彼の行っている説明可能 AI との統合について検討を行った．人種や性別の異なるデータベースを準備中である．
- PSD2022 の参加
  Domingo-Ferrer 教授が UNESCO Data Privacy Chair とし 2004 年から主催している Privacy in statistical databases (PSD)を 2022 年 9 月に Paris のフランス国立工芸院(CNAM)にて開催した．本会議開催支援，および発表聴講を行った．個人データの新しい合成アルゴリズムなどに関して複数の分科会が設けられた．
- JST PREST-URV CRISES Research Group Workshop
  2023 年 2 月 16 日に，URV “Sala de Graus”セミナー室にて，報告者がアドバイザーを

務める JST さきがけ「社会変革における ICT 基盤強化」（東野輝夫研究総括）の採択研究者と Domingo-Ferre 教授が代表を務める URV の CRISES 研究グループとの合同ワークショップを開催した．本ワークショプには，Domingo-Ferrer 教授の分散コンピューティングにおけるセキュリティとプライバシー課題と題するキーノートを始め，日西の研究者による 8 件の研究発表がなされ，活発な質疑応答が交わされた．

研究成果

本在外研究期間で発表した論文（発表予定含む）は以下の通りである．

1. Horigome, H., Kikuchi, H., " Improvement of Estimate Distribution with Local Differential Privacy", Modeling Decisions for Artificial Intelligence. MDAI 2022, Lecture Notes in Computer Science, vol 13408. Springer, Cham, 2022.
2. Hiroaki Kikuchi, Satoshi Ito, Kazuki Ikegami, and Shota Shindo, "Diseases Prediction from Officially Anonymized Medical and Healthcare Big Data", 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan, pp. 1-11, 2022.
3. H. Kikuchi, S. Miyoshi, T. Mori and A. Hernandez-Matamoros, "A Vulnerability in Video Anonymization – Privacy Disclosure from Face-obfuscated video", 2022 19th Annual International Conference on Privacy, Security & Trust (PST), Fredericton, NB, Canada, pp. 1-10, 2022.
4. Horigome, H., Kikuchi, H., Yu, CM., "Expectation-Maximization Estimation for Key-Value Data Randomized with Local Differential Privacy", Advanced Information Networking and Applications. AINA 2023. Lecture Notes in Networks and Systems, vol 654. Springer, Cham, pp. 502-512, 2023.
5. H. Kikuchi, J. Domingo-Ferrer, "Estimating Joint Probability of Independently Randomized Multi-dimensional Data",IPSJ Computer Security Symposium 2022, pp. 456-463, 2022.
6. Hikaru Horigome, Hiroaki Kikuchi, and Chia-Mu Yu, "Local Differential Privacy Protocol for Making Key–Value Data Robust Against Poisoning Attacks", Modeling Decisions for Artificial Intelligence. MDAI 2023, Lecture Notes in Computer Science, Springer, Cham, 2023.
7. Hiroaki Kikuchi, "Privacy-Preserving Clustering for Multi-Dimensional Data Randomization under LDP", 38th International Conference on ICT Systems Security and Privacy Protection (SEC 2023), 2023.
8. 堀込 光, 菊池 浩明, Chia-Mu Yu,key-value データにおける局所差分プライバシーア

ルゴリズム PrivKV の改良マルチメディア，分散，協調とモバイルシンポジウム (DICOMO 2022)，情報処理学会， pp. 1209-1216, 2022. (優秀論文賞受賞)

9. Andres Hernandez-Matamoros, Hiroaki Kikuchi Risk Evaluation of LDP scheme LoPub against Variational Autoencoder,コンピュータセキュリティシンポジウム 2022 論文集, pp. 289-296, 2022.
10. 堀込 光, 菊池 浩明, Chia-Mu Yu,ポイズニング攻撃に対してロバストな EM アルゴリズムを用いた key-value データにおける LDP プロトコルコンピュータセキュリティシンポジウム 2022 論文集, pp. 129-136, 2022.
11. 中川 裕志, 菊池 浩明, 個人データの利用に対する許容度に関する社会調査, コンピュータセキュリティシンポジウム 2022 論文集, pp. 1222-1229, 2022. （CSS 2022 奨励賞）

今後の展望

この在外研究をきっかけに, Domingo-Ferrer 教授と Najeeb Jebreel 博士課程大学院生, Alberto Blanco-Justicia 助教と共にデータプライバシー国際コンテスト international Privacy Workshop on Security, iPWS Cup 2023(仮称)の 2023 年 8 月に横浜で開催する計画を進めている．多次元データの差分プライバシー保護に関する共同研究の成果を今後論文にまとめ，国際会議などに投稿予定である．

教育への効果

Domingo-Ferrer 教授の研究室の研究指導は，週一回のオンライン会議を中心として，個別指導を丁寧に重なることに寄って進められていた．8 名の博士課程大学院生の指導をするのは大きな負担であるが，研究グループの David Sanchez 教授，Maria Bras-Amodos 教授，Oriol Farras 准教授，Alberto Blanco-Justicia 助教と協力して分担しながら研究を進めている．更に数名のポストドクター研究者を加えており，セキュリティプライバシーに関しては極めて大きく全方位的に強力な研究体制を有している．欧州圏の多くの競争的研究資金を獲得しており，フランス，イタリア，ベルギー，スウェーデン，フィンランドなどの共同研究者との間で頻繁に大学院生のショートビジットを含む協力体制を敷いている．

近隣の国との間での交流は学生指導においても大変効果的である．本学においてもアジアの近隣国との間での研究教育協力に活かしたいと考えている．