基礎理論とシステム基盤技術の融合による Society 5.0 のための基盤ソフトウェアの創出　　2022 年度年次報告書

2021 年度採択研究代表者

山口 弘純

大阪大学 大学院情報科学研究科
教授

地域を支える知のデジタライゼーションと共有基盤

主たる共同研究者:

新井 圭太（近畿大学 経済学部 准教授）
稲場 圭信（大阪大学 大学院人間科学研究科 教授）
矢内 直人（大阪大学 大学院情報科学研究科 准教授）
矢野 健太郎（讀賣テレビ放送(株) 編成局 チーフ・エキスパート）

研究成果の概要

本研究の主テーマである， (1) 地域データやAIのプライバシ保護技術，(2)車や人のモビリティデータ生成技術，に関連する論文発表を実現した．(1)については，GAN などの生成 AI により地域データを安全化する新しいアイディアに基づく技術を開発し，論文がモバイルデータ管理の著名国際会議に採択され，研究開発に従事した学生が地理空間データに関する著名国際会議の学生コンペティションに入賞したりしている．また，秘密計算を用いた AI モデルの秘匿化技術を提案した論文が国際ワークショップで採択され，さらに，AI のなかでも高品質な画像を生成できるとして近年注目を集めている拡散モデルについてのプライバシ漏洩リスクを評価した最新の成果も深層学習のセキュリティ・プライバシワークショップで発表している． (2)については，映像や距離センサからのスポット観測に基づき，地域課題解決に不可欠なモビリティデータを生成する方法を確立しつつある．限られた車両映像から対象地域全体の車両モビリティを生成する技術については，駐車場などの PoI における滞留行動をモデルに組み込んだモビリティ生成方法を開発した．人流モビリティを再現する技術については，モバイルとパーベイシブコンピューティング分野のフラグシップ会議 IEEE PerCom2023 にフルペーパーが採択されている．地域を支える知のデジタライゼーションに求められる技術について成果発表を積極的に行っている．

また，本研究開発のテーマについて，代表者の山口は2022年度中に，国際会議での基調講演，国際ワークショップでの基調講演，ならびに 1 件の招待講演を実施し，デジタライゼーションコンセプトの啓蒙活動を実施した．主たる研究者の矢内は，2022 年度第 3 回デバイス・ハードウェアセキュリティ技術分科会 (2022-09) において AI セキュリティに関する招待講演を行っている．関連する研究者へのプロジェクト広報に努めている．

自治体や企業とのデータ連携・活用も進めている．協同関係にある市町村とはワークショップや議論を実施し，一部地域については前述のモビリティ生成手法で交通データを生成し一般公開している．また，モビリティデマンドレスポンスに関する交通ビッグデータを入手・加工し活用している．防災・減災に関連しても鹿屋市など多くの自治体との連携体制を確認・構築し，危機管理・防災担当者等への災害時の避難所情報システムなどのヒアリング、避難所および避難場所の実態調査を行っている．デジタルテレビ活用についてはテレビ活用シナリオとシステム設計を行っている．

【代表的な原著論文情報】

1. Ren Ozeki, Haruki Yonekura, Hamada Rizk, and Hirozumi Yamaguchi, Balancing Privacy and Utility of Spatio-Temporal Data for Taxi-Demand Prediction, Proceedings of the IEEE International Conference on Mobile Data Management (MDM2023), 6 pages, 2023 (in press)
2. Yumeki Goto, Tomoya Matsumoto, Hamada Rizk, Naoto Yanai, Hirozumi Yamaguchi, Privacy-Preserving Taxi-Demand Prediction Using Federated Learning, Proceedings of the 9th IEEE International Workshop on Sensors and Smart Cities (SSC2023), 2023 (in press)
3. Hiromasa Kitai, Naoto Yanai, Kazuki Iwahana, Masataka Tatsumi and Jason Paul Cruz, "MOTUS: How Quantized Parameters Improve Protection of Models and Their Inference Inputs," The 15th International Conference on Security for Information Technology and

Communications (SECITC 2022), Springer, LNCS 13809, pp 184–202 (2022-12).
4. Tomoya Matsumoto, Takayuki Miura, and Naoto Yanai, "Membership Inference Attacks against Diffusion Models," The 6th Deep Learning Security and Privacy Workshop (DLSP 2023), IEEE (2023-05)
5. Masakazu Ohno, Riki Ukyo, Tatsuya Amano, Hamada Rizk and Hirozumi Yamaguchi, Privacy-preserving Pedestrian Tracking using Distributed 3D LiDARs, Proceedings of the 21st Annual IEEE International Conference on Pervasive Computing and Communications (PerCom2023), pp. 43-52, 2023