

2023 年度年次報告書

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

2021 年度採択研究代表者

菊池 浩明

明治大学 総合数理学部

専任教授

安全性と有用性の保証のあるヘルスケア匿名コホート基盤

主たる共同研究者:

荒井 ひろみ (理化学研究所 革新知能統合研究センター ユニットリーダー)

金森 祥子 (情報通信研究機構 サイバーセキュリティ研究所 主任研究技術員)

野島 良 (立命館大学 情報理工学部 教授)

森 由希子 (京都大学 医学部附属病院 講師)

研究成果の概要

課題 1 (個人情報の同意取得)に関しては, 利用者の技術用語や個人情報保護法に対する理解の度合い, また、プライバシーポリシーにおける技術用語の利用が同意取得に与える影響について, 362 名の利用者に対して大規模な調査をおこなった(業績 1). 本発表は, CSS2023 優秀論文賞, UWS 優秀論文賞を受賞している.

課題 2 (匿名化ベンチマーク)に関して, 公開データを用いた匿名化コンテスト PWS Cup で用いた有用性と安全性指標を提案した. 本論文(業績 2)は, 情報処理学会論文誌ジャーナル特選論文を受賞し, 高く評価されている.

課題 3 (差分プライバシー匿名化)では, 列独立の摂動化データに対する秘匿クラスタリング技術を適用し, 相関の強さに応じた同時確率推定を行う多次元データの局所差分プライバシー方式を提案している(業績 3). また, 決定木学習において枝刈りの匿名化への効果に着目し, 属するデータ数が少なく識別リスクが高くなる葉を剪定することで, 差分プライバシーを満たすことができることを示した(業績 4). 業績 5)のジャーナル論文では, 局所差分プライバシーにおける潜在的な脅威である悪意を持つ加工者によるポイズニング攻撃に着目し, 暗号プロトコルと EM アルゴリズムを適用して安全性を向上できることを報告した. 業績 6)のジャーナル論文は, 課題 3.3 の連携学習に関する成果であり, 当初 2024 年度から着工の予定だったが, 前倒しで成果を出している.

【代表的な原著論文情報】

- 1) 金森祥子, 池田美穂, 亀石久美子, 長谷川彩子, プライバシーポリシーに使用される技術用語および個人情報保護法に対するユーザの理解度の調査, コンピュータセキュリティシンポジウム 2023 (CSS2023), 3D3-5, 2023. (CSS2023 優秀論文賞, UWS 優秀論文賞).
- 2) 千田 浩司, 荒井 ひろみ, 井口 誠, 小栗 秀暢, 菊池 浩明, 黒政 敦史, 中川 裕志, 中村 優一, 西山 賢志郎, 野島 良, 長谷川 聡, 波多野 卓磨, 濱田 浩気, 古川 諒, 山田 明, 渡辺 知恵美, AMIC:メンバーシップ推定を防ぐ匿名化技術コンテスト, 情報処理学会論文誌, Vol. 64, No.9, pp.1317-1329, 2023. (情報処理学会論文誌ジャーナル特選論文)
- 3) Hiroaki Kikuchi, Privacy-Preserving Clustering for Multi-Dimensional Data Randomization under LDP, 38th IFIP TC 11 International Conference, SEC 2023, 2023.
- 4) Ryo Nojima, Lihua Wang, "Differential Private (Random) Decision Tree Without Adding Noise", ICONIP (9) 2023, Vol. CCIS 1963, pp.162-174.
- 5) 堀込 光, 菊池 浩明, ジャミュー ユー, "Key-Value データの局所差分プライバシープロトコルにおける EM アルゴリズムを用いたロバストな分布推定手法の提案", 情報処理学会論文誌, Vol. 64, No.9, pp.1227-1240, 2023.
- 6) Tran Thi Phuong, Le Trieu Phong, Kazuhide Fukushima, "Distributed Stochastic Gradient Descent With Compressed and Skipped Communication", IEEE Access 11: 99836-99846 (2023)