イノベーション創発に資する人工知能基盤技術の創出と統合化
2019 年度採択研究代表者

2020 年度
年次報告書

花岡 悟一郎

産業技術総合研究所 サイバーフィジカルセキュリティ研究センター
研究チーム長

プライバシー保護データ解析技術の社会実装

§1. 研究成果の概要

花岡グループでは、前年度に開発を行った、データを秘匿したままでデータベース上の操作を実行可能なシステムについて、連携先となる企業へのヒアリング等を通じて実用化に向けて必要となる機能を明らかにし、それに応じた拡張を行った。特に、テーブル結合機能や整列機能の実現や、秘密計算に必要となる乱数生成の外部サーバへの委託機能の追加を行った。

盛合グループでは、小澤グループ、菅原グループとともに、金融機関 5 行と連携し、プライバシー保護深層学習技術を活用した不正送金検知の実証実験を進め、複数組織による協調学習で高い精度を達成できるよう、銀行間で特徴量やラベルの整理等を行った。また、小澤グループとともにアンサンブル決定木をベースとしたプライバシー保護協調学習方式を提案した。

浅井グループでは、索引構造を用いた高速秘匿全文検索、秘匿木構造検索を開発した。また、秘密分散による効率的な浮動小数点数演算・シャフル演算を開発し、実アプリケーション開発に提供した。さらに、大規模個人ゲノム情報を実用的な速度で解析できるプライバシー保護解析システムを、Intel SGX を用いて開発した。

小澤グループでは、前年度に開発を行った、協調学習型決定木アンサンブル FL-XGBoost に対し、組織間の通信回数を減らして学習を高速化した。また、組織間協調学習が可能な異常検知モデルである pp-iForest を提案した。不正送金検知については、フェーズ 0 の実証実験を 2 銀行に対して実施し、どちらも検知率で 85%以上を達成した。

菅原グループでは、金融機関等の取引先の協力を得ながら目的とする検知対象事象に適したログデータから得られた研究結果に対するデータ提供元のフィードバックを解析手法や結果の改善に役立て、そこで獲得した技術・知見をもとに実社会で有効活用できるシステムの基盤と統合アプリケーションの開発を行った。

§2. 研究実施体制

(1)花岡グループ

① 研究代表者:花岡 悟一郎 (産業技術総合研究所 サイバーフィジカルセキュリティ研究センター 研究チーム長)

② 研究項目

・プライバシー保護データ解析技術の社会実装

(2)盛合グループ

① 主たる共同研究者:盛合 志帆 (情報通信研究機構 サイバーセキュリティ研究所 上席研究員)

② 研究項目

・プライバシー保護データ解析技術の高度化と社会実装

(3)浅井グループ

① 主たる共同研究者:浅井 潔 (東京大学 新領域創成科学研究科 教授)

② 研究項目

・プライバシー保護情報処理の高度化と汎用化

(4)小澤グループ

① 主たる共同研究者:小澤 誠一 (神戸大学 数理・データサイエンスセンター 教授)

② 研究項目

・プライバシー保護機械学習の開発と社会実装

(5)菅原グループ

① 主たる共同研究者:菅原 貴弘 (株式会社エルテス 代表取締役)

② 研究項目

・プライバシー保護データマイニング手法の事業化及び社会実装

【代表的な原著論文情報】

1) Shweta Agrawal and Shota Yamada, "Optimal Broadcast Encryption from Pairings and LWE," Proc. of EUROCRYPT 2020, pp.13-43, 2020.

2) Fuki Yamamoto, Lihua Wang, Seiichi Ozawa, "New Approaches to Federated XGBoost Learning for Privacy-Preserving Data Analysis," Proc. of ICONIP 2020, pp. 558-569, 2020.