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

2019 年度
実績報告書

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

本研究においては、入出力情報を秘密に保ったままデータ処理を実行可能なプライバシー保護データ解析技術について、広範な適用範囲に対して誰でも利用可能な汎用的技術と金融データ解析を特に念頭においた専用的技術の双方に関して研究開発を行うことで、社会実装を推進していくことを目的としている(図1)。加速フェーズ初年度となる 2019 年度では、スモールフェーズにおいて開発されたコア技術をもとに、アルゴリズムの更なる高度化、応用手法技術の開発を中心に行った。

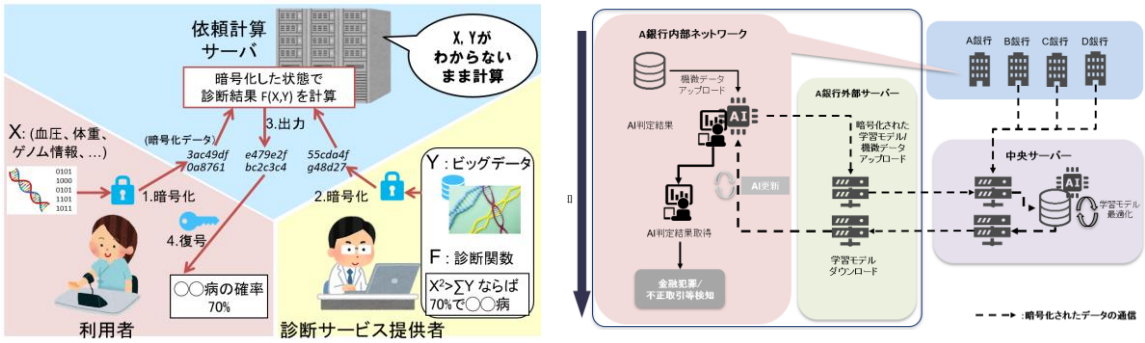

図 1　本研究において想定するプライバシー保護解析技術の利用形態

【花岡グループ】

スモールフェーズにおいて開発を行った汎用秘匿化依頼計算システム用ツール群について、理論レベルでの再設計を行い、大幅な高速化に成功した。また、これらの改良手法についても安全性について厳密に評価を行い、理論的にも安全であることを示した。さらに、これらの開発技術に基づき、専門的研究者でなくても容易に利用可能なライブラリの実装を行い、また、具体的なアプリケーションとして、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の開発を進め、CEATEC 2019 などにおいて出展を行った。

【盛合グループ】
共通鍵をベースとする秘匿深層学習の設計を行い、その高速性と安全性を示した。また、深層学習以外の機械学習についても、その秘匿版の研究開発を進めた。実証実験で利用するデータについては、実証実験への参加金融機関を 1 行から 5 行に増やすことにより、データの大幅拡充に成功した。さらに、これらデータを解析するために、提案方式のシステム化に着手した。
【浅井グループ】
すでに開発した、任意の1入力関数の秘匿計算が可能なプロトコルを用いて、文字列間の編集距離を求めるアルゴリズムを実装・公開した。また、すでに開発した MPC ライブラリを用いて、機械学習に必須な効率的な秘匿除算、およびゲノム解析に応用可能な高速秘匿全文検索のアルゴリズムを開発した。さらに、CPU のセキュリティ技術の一つである Intel SGX を用いて個人ゲノムデータを解析するシステムを開発した。
【小澤グループ】
プライバシー保護機械学習を金融データ解析への実装に適したものと、学術性が高く、将来的に実応用が見込めるものに分けて開発した。前者には、複数組織間で協調学習でき、説明可能性に優れた決定木アンサンブルであるプライバシー保護 XGBoost とデータ分布を可視化できるプライバシー保護 t-SNE を開発した。なお、XGBoost については、平文であるが 2 銀行のデータ解析に適用し、高い不正検知性能を有することを確認した。後者には、高速演算可能な決定木モデルや多層パーセプトロン、指数型分布族ベイズ推定法やナイーブベイズ分類器のプライバシー保護機械学習手法の開発を行った。
【菅原グループ】
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を取得した。その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なるネットワークの設計及びそのテストが完了し、安全に機密情報をやり取りする基盤が完成した。

【代表的な原著論文】
1. Satsuya Ohata and Koji Nuida, “Communication-Efficient (Client-Aided) Secure Two-Party Protocols and Its Application”, Proc. of Financial Cryptography 2020, to appear.
2. Le Trieu Phong and Tran Thi Phuong, ″Privacy-Preserving Deep Learning via Weight Transmission″ IEEE Transactions on Information Forensics and Security, vol. 14, no. 11, 2019
3. Keitaro Hiwatashi, Satsuya Ohata, and Koji Nuida, ″An Efficient Secure Division Protocol Using Approximate Multi-Bit Product and New Constant-Round Building Blocks″, Proc. of ACNS 2020, to appear.

§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)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