「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」
平成 28 年度採択研究代表者

H29 年度
実績報告書

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
室長

複数組織データ利活用を促進するプライバシー保護データマイニング

§1. 研究実施体制

(1)盛合グループ
① 研究代表者: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 セキュリティ基盤研究室 室長)
② 研究項目
・プライバシー保護データマイニング手法の開発

(2)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
・機械学習を用いた大規模データからの知識獲得

(3)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
・リスク検知に特化したビッグデータ解析ビジネス

§2. 研究実施の概要

本研究課題では、複数組織での横断的データ利活用を促進するためのプライバシー保護データマイニング、具体的には暗号技術や人工知能技術を活用し、プライバシーやセキュリティを保護した状態で高速にデータ分析や異常検知を行う技術の研究開発を行う。この技術を活用し、金融分野における不正送金検知や顧客に合わせた金利決定の支援といった課題の解決を目指す。

平成 29 年度は、国立研究開発法人情報通信研究機構(NICT)、国立大学法人神戸大学、及び株式会社エルテスの 3 研究グループで連携し、プライバシー保護データマイニングのさまざまな手法の開発を行い、実装を行って公開データセットを用いた実用性検証を行った。さらに金融取引データ等をセキュアに保管・解析するデータ管理サーバを構築し、金融機関が抱えている課題解決に適用できるよう、協議を行った。平成 29 年度に実施した研究概要は以下の通りである。

NICT(盛合グループ)では、プライバシー保護データマイニング手法の開発を推進し、プライバシーを保護したまま機械学習可能なアルゴリズムの拡充を行った。具体的には、準同型暗号技術と分散コンピューティング技術の組み合わせにより、多数の参加者(組織)が持つデータセットを互いに秘匿したままディープラーニング(深層学習)を行うシステム「DeepProtect」を提案した[1]。また、個人情報を含むデータの収集およびその分析を行う上で、データ提供者が異常データを提供しない限り匿名性が担保される汎用的なプライバシー保護フレームワークを提案した[3]。さらに、神戸大(小澤グループ)とも連携して暗号化データの分類・予測を行う機械学習アルゴリズムの研究開発を行っている[2](後述)。また、エルテス(菅原グループ)、神戸大(小澤グループ)とともに、本研究成果を活用し、具体的な社会問題の解決に取り組むため、実データ提供にご協力頂ける金融機関等と意見交換を行った。さらに、金融機関から提供された金融取引データ等をセキュアに保管・解析を行うデータ管理サーバを構築した。

神戸大学(小澤グループ)では、プライバシー保護型代理計算モデルのパターン識別スキームとして、加法準同型暗号を用いて実時間で学習と予測が可能なプライバシー保護 Extreme Learning Machine (PP-ELM)を開発した[2]。提案した PP-ELM では、ネットワークの順方向計算において必要となる積和計算のうち、乗算部分をデータ提供者で計算して暗号化してもらうことで、代理計算サーバ上では、複数のデータ提供者から送られたデータの加算のみで済むようにしている。これにより、分析者は大規模なデータであっても、安全かつ高速に予測値および結合荷重を求めることが可能となる。4 種類の公開データセットを用いた計算実験を行い、従来のプライバシー保護ロジスティック回帰モデルと比較して精度が向上していることを確認した。また、準同型加算の計算は 1 ミリ秒以下、暗号処理に要する時間も数十〜数百ミリ秒程度であり、十分に実用に耐えうる高速計算性を有することを実証した。また、加法準同型暗号を仮定したときにデータ分析者に復号権限を与える必要がある点を解決するため、現在、ELM、ナイーブベイズ分類器、Binary Weight Network に完全準同型暗号を導入したプライバシー保護型代理計算モデルを開発中である。

エルテス(菅原グループ)では、利用シーンの想定および、収集するログの種類の選定として、複数の金融機関の協力を得て、意見交換会を実施した。また、NICT 及び神戸大学が開発したアルゴリズム及び分析手法の実データへ適用するにあたっての実験環境の条件、データ移管方法について構想を立てた。

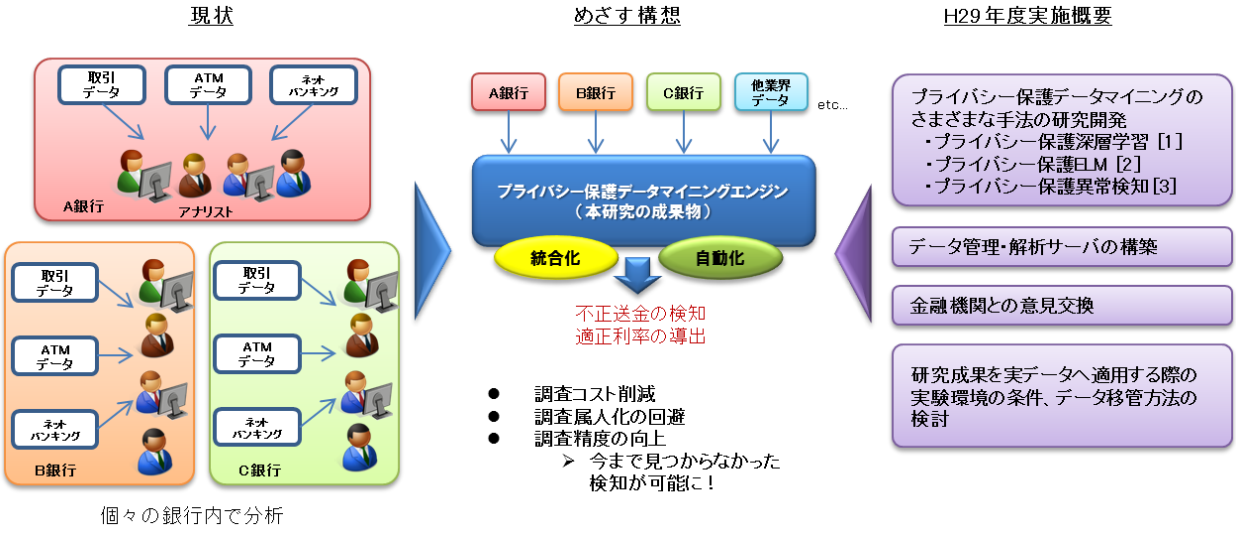

図 1 H29 年度のチーム全体の研究実施概要

[1] L. T. Phong, Y. Aono, T. Hayashi, L. Wang, and S. Moriai, "Privacy-Preserving Deep Learning via Additively Homomorphic Encryption", IEEE Transactions on Information Forensics and Security, Vol.13, No.5, pp.1333-1345, 2018.

[2] S. Kuri, T. Hayashi, T. Omori, S. Ozawa, Y. Aono, L. T. Phong, L. Wang, S. Moriai, "Privacy Preserving Extreme Learning Machine Using Additively Homomorphic Encryption," Proc. of 2017 IEEE Symposium Series on Computational Intelligence, pp. 1350-1357, 2017.

[3] H. Arai, K. Emura, and T. Hayashi, "A Framework of Privacy Preserving Anomaly Detection: Providing Traceability without Big Brother", Proc. of Workshop on Privacy in the Electronic Society (WPES 2017), pp.111-122, ACM, 2017.