戦略的創造研究推進事業　CREST
研究領域「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」

研究課題「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」

研究終了報告書

研究期間　2016年12月～2019年3月

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）

§1 研究実施の概要

（1）実施概要

本研究課題では、複数組織間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技術、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った。一連の研究成果は 15 件以上の国際会議や論文誌で採択されたほか、特許出願も行った。特に、機密データを外部に開示することなく、複数組織で連携して深層学習を行うシステムを提案、プロトタイプを開発した。本技術を金融分野で社会問題となっている不正取引（振り込め詐欺等）の検知に適用し、2つの銀行と連携して顧客の口座取引明細データから不正取引の検知を行う実証実験を行った。銀行から提供された過去1年間の取引明細データを用いて、実際の不正取引のうち、約 70%を不正取引であると正しく判定できた。これを複数金融機関で連携し、不正取引の検知精度向上に向けた実証実験を加速フェーズで実施するため、参加機関募集の共同プレスリリースを NICT、神戸大、エルテスで行った。また、金融分野のみならず、プライバシーを保護したまま医療データを解析し、解析対象外データの混入を検知する実証実験を行い、JST CREST プロジェクト間連携として筑波大 佐久間淳教授及び JST と共同プレスリリースを行った。これらの研究成果は、プレスリリース、招待講演、CEATEC2018 展示等を通してアウトリーチ活動を行い、新聞・Web 等で 35 件以上報道された。また、フィンテックにおけるプライバシー保護データマイニング技術の活用とイノベーション創出に向けた公開シンポジウムを開催、本技術を社会実装する上で必要な課題や法制度について、金融庁、日本銀行金融研究所、Fintech 企業他、多くの分野からの参加者約 130 名と議論を行った。さらに、加速フェーズに向けて的確な課題設定を行うため、金融分野コンサルタントと連携し金融業界の将来像予測とその中で本技術が担うべき役割について調査を実施した。

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深層学習を行うシステム DeepProtect を提案した。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。さらに、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た。また、小澤グループ、菅原グループとともに、金融機関と連携し、実証実験を開始した。

神戸大学（小澤グループ）では、プライバシー保護機械学習手法として、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 とプライバシー保護指数型分布族ベイズ推定法を開発した。どちらも、学習・予測で必要な演算のうち加算項のみを加法準同型暗号で暗号化し、依頼計算サーバ上での秘匿計算が実現される。評価用ベンチマークデータを用いた評価実験で、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同等以上の精度をもつことを確認した。また、準同型加算の演算時間は数ミリ秒以下、暗号処理時間も数十～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示した。現在、完全準同型暗号を仮定したプライバシー保護フレームワークで ELM、ナイーブベイズ分類器、決定木分類器を開発中である。

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、ネットバンキング1行、地銀1行の金融機関の協力を得て、意見交換会を実施した。結果として、不正送金、振り込め詐欺などの検知を中心としたシーンを想定すると共に幅広い利用シーンに対応すべく、基本となるログデータの選定を行った。また、金融機関の特徴及び利用シーンに応じて、基本となるログデータに他のログデータを組み合わせ、検知を行う方針を構想した。さらに、加速フェーズでの実運用に向けて、盛合グループ及び小澤グループが開発したアルゴリズム及び分析手法を金融取引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練り、中央サーバと銀行2行のサーバからなる試験環境を構築した。

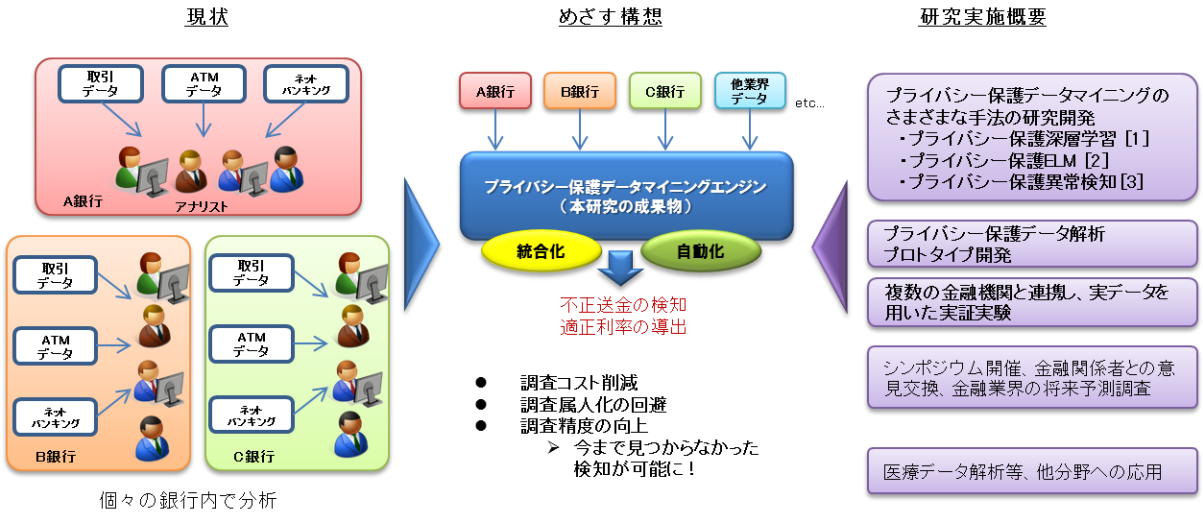

図 1 研究実施概要

(2)顕著な成果

＜優れた基礎研究としての成果＞

1. 複数の組織が持つデータを互いに秘匿したまま深層学習を行うシステムの提案

概要: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、複数の組織が持つデータセットを互いに秘匿したまま深層学習を行うことが可能なシステム DeepProtect を提案した[1]。また、本システムのプロトタイプ実装を行い、公開データセットを用いて実用性検証を行った。特に、Kaggle で公開されている 28 万件あまりの欧州クレジットカード取引レコード(うち 0.2%程度が不正利用)を秘匿分散協調学習し、不正利用 1 件あたり 1 ミリ秒で検出できることを確認した。

2. 多入力依頼計算型プライバシー保護機械学習の提案

概要:複数の組織が持つデータを加法準同型暗号で秘匿して依頼計算サーバで学習・予測が可能なプライバシー保護型の Extreme Learning Machine[2]と指数型分布族ベイズ推定を開発した。これらのモデルでは、データ提供者、分析者、依頼計算サーバの 3 者で学習・予測に必要な演算を分担し、プライバシーを保護しながら高速に学習・予測を行える。計算実験において、数十～数百ミリ秒の学習時間で平文モデルと同等の性能を有することを示した。

3. プライバシー保護異常検知フレームワークの提案

概要:個人情報を含むデータの収集を行う際に、異常データを提供しない限りデータ提供者の匿名性を担保しつつ、異常データ提供者のみを特定可能とするフレームワークを提案した[3]。国内最大級のコンピュータセキュリティシンポジウム CSS にて、プライバシー保護技術の発展等に貢献すると認められる論文 1 編に与えられる PWS2017 論文賞を受賞、さらにプライバシーに関する著名な国際ワークショップに採録された。

＜科学技術イノベーションに大きく寄与する成果＞

1. 銀行の実取引データを用いた不正取引検知の実証実験

概要:過去 12 ヶ月分の取引明細情報及び口座情報の中から約 170 万件のデータを用いて、

特殊詐欺などの金融犯罪の可能性が疑われる取引を様々な機械学習手法により検知する実証実験を開始した。取引データに事前処理を行い、有用と思われる特徴に変換した後、さまざまな機械学習手法で学習を行った。特徴抽出(40 分)後、約 10 秒で学習が完了、実際の不正取引のうち、約 70%を不正取引であると正しく判定できた。

2. プライバシーを保護したまま医療データを解析する暗号方式の実証実験

概要:暗号化した医療データの中身を見ることなく解析を行うと共に、解析対象外データの混入を防ぐ解析手法を開発、2017 年度情報処理学会山下記念研究賞を受賞した。本方式を実医療データに適用して「ある病気に罹患していること」と「ある遺伝的特徴を持つこと」との統計的な関連性を解析、4,500 名程度のデータに対し、1 分弱で暗号化及び解析が完了することを示し、筑波大学及び JST と共同でプレスリリースを行った。

3. プライバシー保護データマイニング技術の社会実装に向けた取り組み

概要:プライバシー保護データ解析技術を活用し、複数金融機関で連携して不正取引の検知精度向上をめざす実証実験を加速フェーズで実施するため、参加機関募集の共同プレスリリースを NICT、神戸大、エルテスで行った。また、フィンテックにおけるプライバシー保護データマイニング技術の活用とイノベーション創出に向けた公開シンポジウムを開催した。さらに、金融業界の将来像予測とその中で本技術が担うべき役割について有識者と連携した調査を実施した。

＜代表的な論文＞

[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.

§2 研究実施体制

(1)研究チームの体制について

① 盛合グループ
研究代表者:盛合 志帆 (情報通信研究機構セキュリティ基盤研究室 室長)
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
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)
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
主たる共同研究者:菅原 貴弘 ((株)エルテス 代表取締役)
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)国内外の研究者や産業界等との連携によるネットワーク形成の状況について

- 筑波大学システム情報系 佐久間 淳 教授
  JST CREST「ビッグデータ基盤」(喜連川総括)のもとで佐久間教授が進める研究課題「自己情報コントロール機構を持つプライバシ保護データ収集・解析基盤の構築と個別化医療・ゲノム疫学への展開」と連携し、共同開発した暗号化したまま演算が行える「準同型暗号」の演算を制御する方式を医療データに適用し、病気の罹患情報と遺伝子情報との関連性を暗号化したまま解析するχ^2独立性検定を行った。この成果を2018年7月18日にJST、筑波大と下記の共同プレスリリースで発表した。
  「プライバシーを保護したまま医療データを解析する暗号方式を実証
  ～中身を見なくても誤データ混入防止、医療ビッグデータの安全な利活用へ～」

- 産総研サイバーフィジカルセキュリティ研究センター 花岡 悟一郎 研究チーム長
  JST CREST「人工知能」(栄藤総括)のもとで花岡研究チーム長が進める研究課題「安全な秘匿化データ処理を実現する汎用依頼計算技術」と連携し、加速フェーズ研究提案を共同提案した。

- 現時点で公開できない産業界等の連携は§6(非公開)に記載