2022 年度 委託研究

課題 229

プライバシー保護連合学習の高度化に関する研究開発

研究計画書

国立研究開発法人
情報通信研究機構

１．研究開発課題

プライバシー保護連合学習の高度化に関する研究開発

２．目的

国立研究開発法人情報通信研究機構(以下「機構」という。)は、社会の持続的発展において欠くことの出来ない情報のセキュリティやプライバシーの確保を確かなものとするため、プライバシー保護技術の研究開発を実施し、組織横断的な連携を含むデータ利活用を促進するとともに、国民生活を支える様々なシステムへの普及を図ることを目指している。

組織横断的な連携が求められている社会課題として金融分野における不正取引対策がある。特にマネーロンダリング・テロ資金供与対策については、我が国は、世界各国・地域のマネロン対策を調べる国際組織「金融活動作業部会」（FATF, Financial Action Task Force）の対日審査の結果を受け、国として早急な対応が迫られている。令和３年８月に財務省より発表された「マネロン・テロ資金供与・拡散金融対策に関する行動計画」［1］の「２．金融機関及び暗号資産交換業者によるマネロン・テロ資金供与・拡散金融対策及び監督」では、「令和６年春」を期限として「取引時確認、顧客管理の強化および平準化の観点から、取引スクリーニング、取引モニタリングの共同システムの実用化を図る」としている。現在すでに各銀行において個別に口座への入出金や顧客ごとの取引が監視されているが、今後は金融機関が協力して対策を講じることが重要であり、その際には、顧客情報等のプライバシーの保護をシステムの中に組み込み、その上で金融機関が組織横断的に連携し、データを連携・利活用していくことが極めて重要と考えられる。

機構は、データを外部に開示することなく、機密性を保ったまま連携して機械学習を行うプライバシー保護連合学習技術「DeepProtect」を開発し[２，３]、産学と連携し、複数の金融機関（５銀行）と不正送金検知に関する実証実験を行った。本実証実験では、DeepProtect を用いた連合学習を行い、複数銀行のデータをもとに学習した連合学習モデルで１銀行での学習モデルより高い不正送金の検知精度が出るケースを示した[４]。その結果、取引データを銀行間で互いに開示することなく不正送金の検知精度が向上できることが示され、取引モニタリング共同システムの実現のために、DeepProtect が中心的な役割を果たすことが示された。プライバシー保護連合学習技術を活用した実証実験の類似事例としては、連合学習に、準同型暗号ではなく秘密分散を適用した方式を活用した［５］がある。一方、取引モニタリングの現場で、持続的・長期的に高い検知精度を保つためには、共同システムへの参加銀行数の増減や利用できるデータの種別の変化、さらには金融犯罪手口の巧妙化等、データが日々変化していく実運用時の課題への対応が必要となる。これは機械学習分野における継続学習（Continual Learning）に関する課題であり、この課題を解決するため、DeepProtect の高度化が必要となる。

本委託研究では、持続的・長期的に運用可能な取引モニタリング共同システムの実現を目指し、機構が開発した DeepProtect を高度化し、さらなる検知精度の向上と日々巧妙化する金融犯罪に対応するためのプライバシー保護連合学習の継続学習に関する研究開発を行う。

３．内容

機構が開発した DeepProtect は、学習で利用するデータを組織外部に開示することなく、複数組

織で協調して機械学習を行うことを可能とする技術である。各組織から外部サーバーに送る情報は統計情報化されたパラメータの一部のみとし、さらに準同型暗号で暗号化して取り扱うことが可能であるため、データ漏洩のリスクが極めて低い。本委託研究では、DeepProtect を中核技術として、下記を実施する。なお、機構は、受託者に対し、本委託研究遂行に必要な範囲で、DeepProtect の無償での利用を許諾する。

1）DeepProtect の継続学習による不正取引検知精度向上のための研究開発および検証

これまで機構が実施してきた連合学習の実証実験では、学習で利用するデータは静的なものであり、複数の銀行から日々更新されるデータを用いたプライバシー保護連合学習の継続学習に関しては実施していない。取引モニタリングを複数の金融機関で行う共同システムを DeepProtect を用いて実現する場合、学習モデル構築後の参加銀行数や利用可能なデータの増減、金融犯罪手口の巧妙化等、日々更新されるデータに対応する必要がある。そのため、DeepProtect に継続学習を組み合わせて高度化することが重要となる。

本委託研究では、複数の銀行から日々更新されるデータを用いてプライバシー保護連合学習の継続学習を行い、高い検知精度を維持するための研究開発とその効果についての検証を行う。一般に継続学習モデルは、機械学習で新たな知識を学習する際に、過去に学習・習得した知識を再利用することでより効率的で精度の高い学習を可能にするモデルであるが、新たなデータを用いて学習することにより、過去に学習したタスクに対する性能が著しく低下する破滅的忘却（catastrophic forgetting）という弱点が知られており、この課題を克服する必要がある。そのため、継続的に入力される銀行取引データを用いて、不正送金シナリオや出入金パターンの変化に対するロバスト性等を検証し、必要に応じて改良を行う。改良として個別学習や他の連合学習とのアンサンブル学習なども考えられる。

2）不正取引検知精度向上のためのデータ共通化の検討

プライバシー保護連合学習の継続学習による不正検知精度向上のため、機構が指定する 4 行以上の銀行よりデータ提供を受け、不正取引検知のための共通特徴量、特徴量抽出方法の検討や、不正取引検知 AI モデルの教師データ共通化に必要な犯罪フラグの共通化等に関する検討を行う。

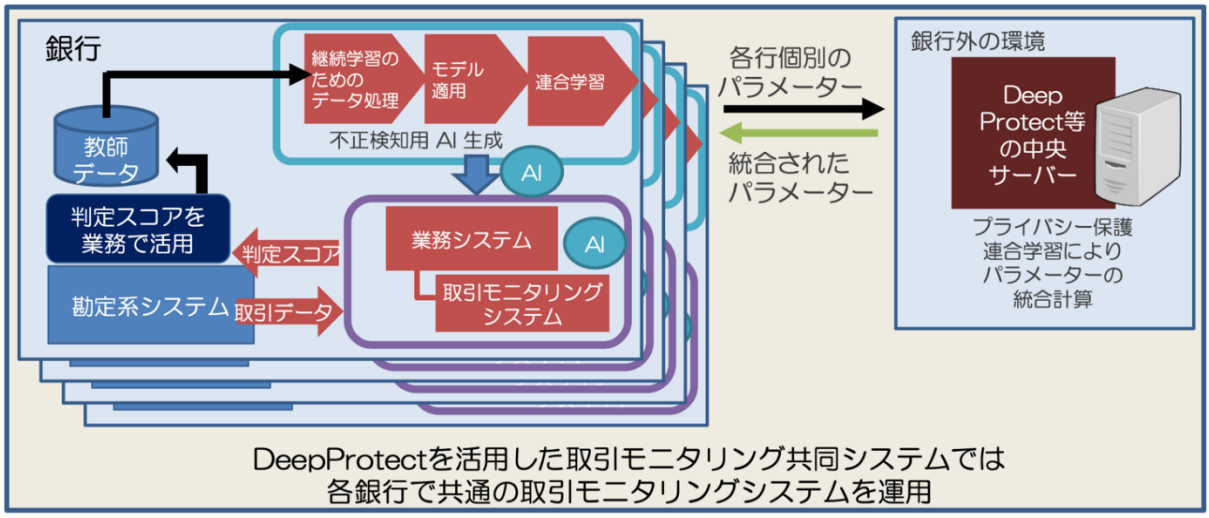

図１：DeepProtect を活用した取引モニタリング共同システムにおける継続学習のイメージ

4．アウトプット目標

- 銀行業務に導入可能な DeepProtect を活用したプライバシー保護連合学習の継続学習を実現する。目標とする検知精度は、４行以上の銀行から提供されるデータを用いて検知漏れの少なさを表す指標である再現率で 90%以上とする。
- ４行以上の銀行に適用可能な共通特徴量と犯罪フラグの提案を行うことを目標する。

5．アウトカム目標

本委託研究で得られた成果の社会実装に向けて、研究開発期間終了後に達成すべきマイルストーン等を具体的に記載。

- 2024 年：取引モニタリング共同システムへの組み込みに向けた不正取引検知エンジンのプロトタイプシステムの開発を行う。
- 2025 年：継続学習可能なプライバシー保護連合学習を用いた不正取引検知モデル更新機能の検証／ブラッシュアップ／試験運用を行う。
- 2026 年：継続学習可能なプライバシー保護連合学習の取引モニタリング共同システムへの導入を行い、他銀行にも横展開をはかる。

6．採択件数、研究開発期間及び研究開発予算等

採択件数　　：１件
研究開発期間：2022 年度（契約締結日）から 2023 年度
研究開発予算：各年度、30 百万円（税込）を上限とする。
（提案の予算額の調整を行った上で採択する提案を決定する場合がある。）
研究開発体制：単独の提案も可能であるが、産学官連携等による複数の実施主体からなる体制とすることを推奨する。その際、社会実装を考慮した体制とすること。

7．提案に当たっての留意点

- 機構が開発した DeepProtect の詳細については、参考文献[2,3,6]を参照すること。
- 具体的目標に関しては、定量的に提案書に記載すること。
- 本研究開発成果の情報発信を積極的に行うこと。
- 本委託研究の遂行過程で得られる科学的なデータがあれば、広くオープンにするのが望ましい。公開可能と想定される科学的なデータの有無と、有る場合には公開計画（例：公開するデータの種類、公開先、公開方法）を提案書に記載すること。
- 実施体制については、本研究開発の目的に則した実施体制を構築することとし、それぞれの役割を明記すること。
- 本研究開発成果の社会実装に向けて、到達目標の項目に記載したマイルストーンを意識しつつ、具体的な時期（目標）、体制、方策等を記載すること。その際、持続的に自走するための計画等についても記載すること。
- 本研究開発成果が円滑に社会実装されるように、複数の実施主体からなる研究開発体制

で実施する場合は、成果に係る知的財産（データ・学習モデル含む）の帰属や取扱いについて実施主体間で事前に協議・合意すること。

- 銀行から提供されるデータは機構が管理し、受託者は機構が指示する方法によりそのデータにアクセスし本委託研究を実施することを予定している。機構が銀行と協議し、データ管理とそのアクセス方法を変更する場合がある。データ利用に関した契約締結が必要な場合があるので応じること。また、銀行が求めるデータの安全管理と各種報告の提出等に機構と協力して対応すること。
- データ提供を受けた銀行に対し、継続学習の学習結果等（継続学習により構築された学習モデルで不正取引検知精度がどのように変化したか等）について定期的に報告を行うこと。

８．運営管理

- 機構と受託者の連携を図るため、代表提案者は、プロジェクトオフィサーの指示に基づき定期的に連絡調整会議を開催すること。
- 複数の機関が共同で受託する場合には、代表提案者が受託者間の連携等の運営管理を行い、受託者間調整会議を定期的に開催すること。
- 社会情勢や研究環境の変化等、必要に応じて、プロジェクトオフィサーが研究計画書を変更する場合があるので、留意すること。

９．評価

- 機構は、契約期間の終了年度に終了評価を実施する。また、機構は、本委託研究終了後に成果展開等状況調査を行い、追跡評価を行う場合がある。
- 機構は、上記以外にも本委託研究の進捗状況等を踏まえて、臨時にヒアリングを実施することがある。

１０．成果の社会実装等に向けた取組

- 本委託研究終了後には、DeepProtect 等の機構のプライバシー保護連合学習技術に係る知的財産権の実施の許諾を受け、実用化・事業化する計画であること。
- 上記の出口戦略を実現するため、本委託研究で得られた成果のオープン化（例えば、成果発表やそれに留まらずコミュニティ先導のための国際ワークショップや国内特別セッション主催、展示、標準化、オープンソース化等）を行う等、成果の社会実装等に向けて必要な取組を行うこと。
- 産学官連携体制の構築、研究開発の成果を参加企業等が実用化・事業化につなげる仕組みをビルトインし、委託研究実施時には、参加機関の間で共同研究契約等を締結すること。

１１．プロジェクトオフィサー

サイバーセキュリティ研究所セキュリティ基盤研究室　野島 良

参考

[1]「マネロン・テロ資金供与・拡散金融対策に関する行動計画」，財務省（2021 年 8 月 30 日）
https://www.mof.go.jp/policy/international_policy/councils/aml_cft_policy/20210830_2.pdf

[2] 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.

[3] L. T. Phong, T. T. Phuong, Privacy-Preserving Deep Learning via Weight Transmission, IEEE Transactions on Information Forensics and Security, Vol.14, No.11, pp.3003-3015, 2019.

[4]「プライバシー保護連合学習技術を活用した不正送金検知の実証実験を実施 ～被害取引の検知精度向上や不正口座の早期検知を確認～」，国立研究開発法人情報通信研究機構他（2022 年 3 月 10 日プレスリリース） https://www.nict.go.jp/press/2022/03/10-1.html

[5]「NEC、連合学習技術と秘密計算技術を用いた創薬における予測モデル構築に関する実証実験を実施」，日本電気株式会社（2022 年 3 月 11 日プレスリリース）
https://jpn.nec.com/press/202203/20220311_01.html

[6] DeepProtect 説明書（要求に応じて、秘密保持契約を結んだ上で提供するため、必要な場合はサイバーセキュリティ研究所 セキュリティ基盤研究室（E-mail: dp-itaku@ml.nict.go.jp ）に連絡すること。）