プレスリリース
2025 年 7 月 22 日

国立研究開発法人情報通信研究機構
国立大学法人神戸大学
株式会社エルテス
株式会社テラアクソン

プライバシー保護連合学習技術「DeepProtect」「eFL-Boost」を活用した不正送金検知の実証実験を実施し、再現率向上を確認

【ポイント】

- 銀行 3 行と連携し、プライバシー保護連合学習技術「DeepProtect」と「eFL-Boost」を活用した不正送金検知の実証実験を実施
- 継続学習のシナリオを採用し、両連合学習技術で不正口座検知の再現率向上を確認
- 本研究で得た成果を基に他業種への展開を目指す

国立研究開発法人情報通信研究機構（ＮＩＣＴ（エヌアイシーティー）、理事長: 徳田 英幸）、国立大学法人神戸大学（学長: 藤澤 正人）及び株式会社エルテス（代表取締役: 菅原 貴弘）は、科学技術振興機構（JST） 戦略的創造研究推進事業の支援を受け、プライバシー保護連合学習技術「DeepProtect」[*1] 及び「eFL-Boost」[*2] を活用した安全な組織間データ連携技術の社会実装の研究を実施しました。本研究では千葉銀行、中国銀行及び三井住友信託銀行と連携し、銀行の実データを利用した不正送金検知の実証実験を行いました。

この実験では日々進化する犯罪手法に対応するため、新しいデータを追加で学習できる継続学習[*3] のシナリオを採用し、DeepProtect と eFL-Boost の双方で、3 銀行の個別学習で得られた AI モデルと、3 銀行の連合学習で得られた AI モデルの検知結果を比較しました。その結果、3 銀行の個別学習で得られた AI モデルよりも、連合学習で得られた AI モデルの方が、不正口座を見逃さず検知できた割合（再現率[*4]）で平均 18 ポイント程度の改善が得られました。併せて性能改善への取組として疑似取引データを生成し、そのデータを学習した場合の検知精度を検証した結果、1 銀行で適合率[*5] が改善しました。

さらに、実証実験の後続フェーズとして株式会社テラアクソン（代表取締役 経営責任者: 安田 鉄平）と共に協力銀行 1 行での行内実証実験を開始しています。今後は本研究で得た成果を基に他業種への展開も視野に入れ、引き続き研究を進めていきます。

【背景】

NICT、神戸大学及びエルテスは、かねてより複数の組織が有する膨大なデータを連携し、プライバシーを保護しつつ AI を活用して金融取引における異常・不正検知を行うセキュアなビッグデータ解析技術の研究開発に取り組んできました。2016 年には振り込め詐欺等の金融分野における不正取引の検知を実現するシステムの構築を目標に、JST から支援を受けて CREST スモールフェーズとして要素技術の開発を始め、2019 年より CREST 加速フェーズとして実証実験を含めた社会実装に向けた取組を研究開発と共に進めてきました。

2022 年にはプロジェクト継続に値するとして再度 JST より支援を受け、研究課題「組織間連合学習による不正送金検知システムの社会実装」に取り組み、DeepProtect（NICT が開発した深層学習ベースの技術）と eFL-Boost（神戸大学が開発した勾配ブースティング決定木[*6] ベースの技術）の二つのプライバシー保護連合学習技術を共同で研究開発すると共に、千葉銀行、中国銀行及び三井住友信託銀行の協力を得て今回の実証実験を行いました。

【今回の成果】

本研究では不正取引に使われている銀行口座を AI で検出する実証実験を行いました。3 銀行で互いにデータを直接提供することなしに、共同で AI（学習済みモデル）を構築し、データ解析を可能にする連合学習技術として、NICT は DeepProtect、神戸大学は eFL-Boost を用いました（図 1 参照）。双方の技術を比較することで、相対的な性能を

明らかにすると共に、課題の特性や用途に合わせてそれぞれを使い分けられるよう、実験を通じて得たデータを収集しました。また、日々巧妙化する犯罪手法の変化に対応するため、新しいデータを追加で学習できる継続学習が可能になるようにそれぞれの連合学習モデルを改良しました。

その結果、3 銀行の個別学習で得られた AI モデルよりも、連合学習で得られた AI モデルの方が、DeepProtect と eFL-Boost の双方に対して、再現率で平均 18 ポイント程度の改善が得られました（図 2 参照）。また、いずれの銀行においても、約 89%以上の再現率で検知可能であることが示されました。

さらに、学習モデルの性能改善への取組として、不正取引は通常取引に比べて割合が極めて少なく、一般的に学習に使えるデータが少ない問題に着目し、実データに加えて凍結口座の疑似取引データを人工的に生成し、これを学習した AI モデルに対して、不正検知実験で性能評価を行いました。その結果、1 銀行で適合率が改善しました。

また、実証実験終了後に、本研究で開発した継続学習型の DeepProtect と eFL-Boost を AI エンジンとして組み込んだ AI 不正検知システムを、神戸大学発ベンチャーであるテラアクソンが協力銀行 1 行に提供し、不正モニタリング業務（加害口座と被害口座の検知など）を継続的に実施する、銀行の実環境下での実証実験を開始しています。今後の運用を通じて性能検証や問題点の洗い出し、システム改善を行っていきます。

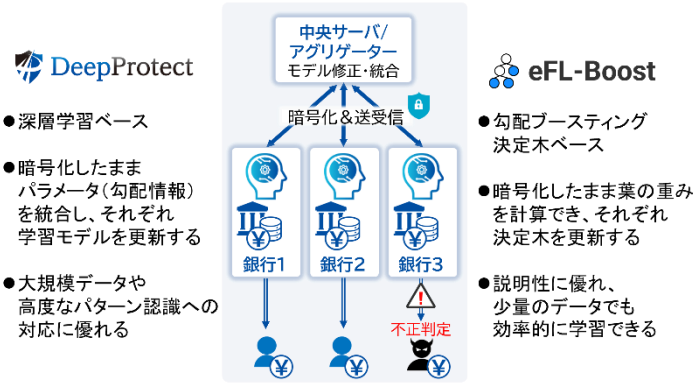

図 1. DeepProtect と eFL-Boost の比較と金融分野の適用例

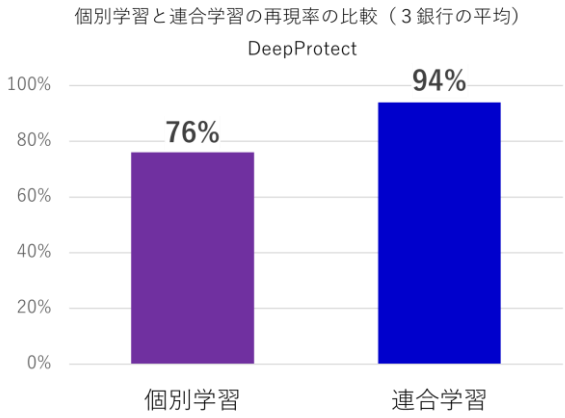

図 2. 個別学習と連合学習の再現率の比較

【今後の展望】

本研究で得た成果を基に、連合学習技術を金融の分野だけではなく、データのプライバシー保護を必要とする様々な業種（医療、健康、流通など）への展開を目指していきます。具体的には、これまでのプロジェクトで開発された DeepProtect や eFL-Boost に対し、本研究で開発した継続学習化機能や性能改善機能を活用し、社会課題の解決を目指して企業等との連携を進めていきます。さらに、当実証実験を通して得られたユーザーのニーズへの対応及び DeepProtect や eFL-Boost の機能拡張技術などへの応用を図るため、引き続き基礎研究を進めていきます。

＜各機関の役割分担＞

・NICT: DeepProtect の研究開発、実証実験計算基盤運用・保守、実証実験の運営・実施
・神戸大学: eFL-Boost の研究開発、実証実験の企画・実施、データ解析
・エルテス: 実証実験の運営
・テラアクソン: 実証実験の企画・実施支援、データ解析支援、行内実証実験用システムの導入・実施

＜関連する過去の NICT のプレスリリース＞

・2025 年 7 月 1 日 放射線画像診断支援 AI の実用化に向け高機能暗号を用いた異分野融合型の共同研究を開始
https://www.nict.go.jp/press/2025/07/01-1.html
・2025 年 6 月 10 日 プライバシー保護連合学習技術「DeepProtect」を活用した銀行の不正口座検知の実証実験を実施し、検知精度向上を確認
https://www.nict.go.jp/press/2025/06/10-1.html
・2022 年 3 月 10 日 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
https://www.nict.go.jp/press/2022/03/10-1.html
・2020 年 5 月 19 日 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において金融機関 5 行との連携を開始
https://www.nict.go.jp/press/2020/05/19-1.html
・2019 年 2 月 1 日 プライバシー保護深層学習技術で 不正送金の検知精度向上に向けた実証実験を開始
https://www.nict.go.jp/press/2019/02/01-2.html

なお、本研究は、JST、AIP 加速課題（AIP Accelerated Program）、JPMJCR22U5 の支援を受けたものです。

＜ 本件に関する問合せ先 ＞

国立研究開発法人情報通信研究機構
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 小川 一人
E-mail: security@ml.nict.go.jp

国立大学法人神戸大学
数理・データサイエンスセンター
教授 小澤 誠一
E-mail: ozawasei@kobe-u.ac.jp

株式会社エルテス
IRI 事業本部
リスクインテリジェンス部 基盤グループ
森 大樹
E-mail: eltes-aip-ml@eltes.co.jp

株式会社テラアクソン
代表取締役 研究責任者
小澤 誠一
Email : seiichi.ozawa@telaaxon.com

＜ 広報 （取材受付）＞

国立研究開発法人情報通信研究機構
広報部 報道室
E-mail: publicity@nict.go.jp

国立大学法人神戸大学
総務部 広報課
E-mail: ppr-kouhoushitsu@office.kobe-u.ac.jp

株式会社エルテス
経営企画グループ 広報担当
E-mail: pr@eltes.co.jp

株式会社テラアクソン
代表取締役 経営責任者
安田 鉄平
Email : teppei.yasuda@telaaxon.com

＜用語解説＞

*1 プライバシー保護連合学習技術「DeepProtect」

連合学習技術に暗号技術を融合することによって、NICT が独自に開発したプライバシー保護連合学習技術のこと。まず、各組織で持つデータを基に深層学習を行う際に、学習中のパラメータ（勾配情報）を暗号化して中央サーバに送り、中央サーバでは、暗号化したまま学習モデルのパラメータ（重み）の更新を行う。次に、更新されたこの学習モデルのパラメータを各組織においてダウンロードすることで、より精度の高い分析が可能になる。DeepProtect は、各組織から中央サーバにデータそのものを送ることなく、学習中のパラメータのみを暗号化して送信するが、このパラメータは、複数のデータを集計した統計情報とすることによって個人を識別できない状態にすることが可能であり、さらに、暗号化を施すため、データの外部への漏えいを防ぐことができる。
本技術により、パーソナルデータのような機密性の高いデータを外部に開示することなく、複数組織で連携して多くのデータを基にした深層学習が可能となる。eFL-Boost と比較して、大規模データや高度なパターン認識への対応に優れる。
本技術は、複数のジャーナルに採択・掲載されている[1,2]。また、動画による紹介を行っている[3]。

[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] L. T. Phong and 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.
[3]『NICT ステーション ～DeepProtect～』
https://youtu.be/CpA9OD5vUIM

*2 決定木ベースのプライバシー保護連合学習「eFL-Boost」

神戸大学と NICT はプライバシー保護に配慮した勾配ブースティング決定木の連合学習方式である eFL-Boost（Efficient Federated Learning for Gradient Boosting Decision Trees）を開発した[1]。eFL-Boost は、異なる組織が互いにデータを開示することなく、一つの勾配ブースティング決定木モデルを組織間で協調して学習する組織間連合学習スキームである。学習過程では、木構造の決定を特定の組織がローカルで行い、葉の重みを全組織で連携して計算することで、自組織のデータで学習した決定木構造を他組織に明かさないでプライバシー保護を実現しつつ、実用的な組織間通信量で高速かつ高精度と評価される XGBoost と同等の性能を達成することに成功した。組織間で共有されるのは、プライバシーリスクの低い統計情報のみであり、準同型暗号で暗号化したまま、葉の重みを計算できる[2]。eFL-Boost は、深層学習と比較して各特徴量の解析結果への寄与率を出力できるため説明性に優れ、少量のデータでも効率的に学習できる手法であり、非数値データを取り扱う必要性のあるケースなど、DeepProtect とうまく使い分けていくことが望まれる。
なお、本成果については国際特許出願（PCT）を行い、日本国内への移行手続きおよび米国への移行出願も完了している[3,4]。

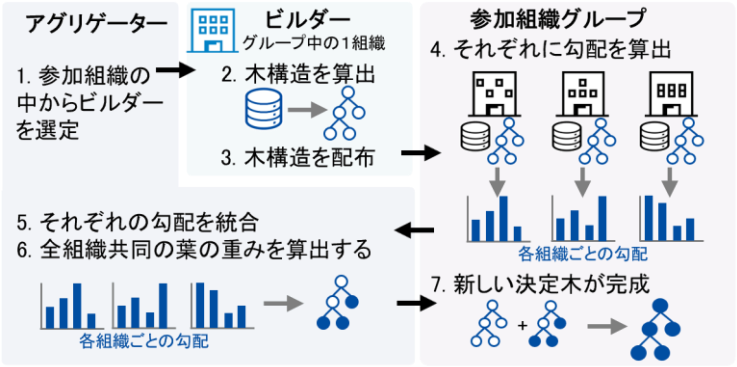

図 3. 勾配ブースティング決定木に基づく連合学習

[1] F. Yamamoto, S. Ozawa, L. Wang, “eFL-Boost: Efficient Federated Learning for Gradient Boosting Decision Trees,” IEEE Access, vol.10, pp.43954-43963, 2022. https://ieeexplore.ieee.org/document/9761890
[2] Le Trieu PHONG, Tran Thi PHUONG, Lihua WANG, Seiichi OZAWA, Privacy-Preserving Federated Learning with Neural-Network-Based and Decision-Tree-Based Approaches, IEICE TRANS. INF. & SYST., VOL.E107–D, NO.1 JANUARY 2024.【Invited Paper】
[3] 国際出願 PCT/JP2021/48383「協調学習システム及び協調学習方法」（国内移行出願 2023 年 5 月 12 日完了）、発明者：王立華、山本楓己、小澤誠一
[4] 出願番号：18/269747「Federated Learning System and Federated Learning Method”」（2023 年 6 月 26 日出願）、発明者：Lihua Wang, Fuki Yamamoto, Seiichi Ozawa,

***3 継続学習**

継続学習（Continual Learning） とは、機械学習モデルが新たなデータやタスクを継続的に学習しながら、既存のデータやタスクから得た情報・知識を保持したモデルを生成することを目的とした手法である。従来の機械学習では、全てのデータを一括して学習する「一括学習（batch learning）」が一般的であったが、実世界の多くの応用では、データが逐次的に到着するため、モデルが新規のデータの到着に順応し続けることが求められる。例えば、金融取引情報のように時系列で更新されるデータや、ユーザーの行動履歴が常に変化する状況においては、モデルが変化に即応して学習内容を更新する必要がある。継続学習は、こうした状況において忘却（catastrophic forgetting）を抑制しつつ、過去の知識を活かしながら新たな知識を蓄積することを可能にし、長期的な適応力を持つモデルの構築を支援する。

***4 再現率**

実際に「不正」なデータの中で、モデルが「不正」と正しく予想できた割合を示す指標。再現率が高いほど、取りこぼしなく正しく検知できていることを意味する。再現率は、不正検出など「取りこぼしを減らすことが重要なケース」で重視される。

***5 適合率**

モデルが「不正」と予測したデータの中で、実際に「不正」なデータである割合を示す指標。適合率が高いほど、誤検出が少なく、正確に予想できていることを意味する。適合率は、スパムメールの検出など「誤検出を減らすことが重要なケース」で重視される。

***6 勾配ブースティング決定木**

勾配ブースティング決定木（Gradient Boosting Decision Trees, GBDT）は、複数の決定木モデルを逐次的に構築・統合することで、高精度な予測を実現する機械学習手法である。単一の決定木では予測精度に限界があるが、GBDT では各決定木が直前のモデルで生じた誤差を補うように設計されており、これを繰り返すことで予測誤差を徐々に修正し、モデル全体の性能を高めていく。GBDT は決定木を基盤としており、各木の貢献度や特徴量の重要度が明示的に計算できるという特徴がある。これは深層学習にはない特徴であり、深層学習と比較して出力結果の解釈がしやすいという利点を持つ。決定木は、「どの特徴量がどのような条件で予測に影響したのか」を分岐のルールとして明示的に示すため、人間にも直感的に理解しやすい構造になっている。また、GBDT は浅い決定木を繰り返し組み合わせて誤差を修正しながら学習を進める手法であるため、外れ値に対し頑強であり、大量のデータがなくても過学習を抑えつつ効率的に高い予測性能を発揮することができる。さらに、数値データに限らず、「はい／いいえ」やカテゴリ名といった非数値データを直接扱える実装が多く、実用性に優れた汎用的なアルゴリズムとして広く活用されている。