プレスリリース
2022 年 3 月 17 日

国立研究開発法人情報通信研究機構
株式会社イエラエセキュリティ

プライバシー保護連合学習技術「DeepProtect」を技術移転

～複数組織の機密性の高いデータ解析が必要なビジネス分野への活用に期待～

【ポイント】

- プライバシー保護連合学習技術「DeepProtect」を株式会社イエラエセキュリティに技術移転
- データの機密性やプライバシーを保護しつつ、安全に複数組織間で連合学習による解析を実現
- 複数組織の機密性の高いデータ解析が必要なビジネス分野への活用に期待

国立研究開発法人情報通信研究機構（ＮＩＣＴ、理事長：徳田　英幸）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において開発した、パーソナルデータなど機密性の高いデータを複数組織間で互いに開示することなく安全に解析することができるプライバシー保護連合学習技術「DeepProtect」[*1] を、株式会社イエラエセキュリティ※（代表取締役社長：牧田　誠）に技術移転しました。

複数組織が協力してデータを利活用するためには、機密性の確保やプライバシーの保護といった課題があり、プライバシー保護データ解析技術[*2] に対する期待が高まっています。しかし、プライバシー保護データ解析技術を利用するには、AI やセキュリティに関する高度な技術や知見が必要とされます。

今回、「DeepProtect」をサイバーセキュリティ・暗号・機械学習に関する高い技術力を持つイエラエセキュリティに技術移転したことによって、同社の環境構築や技術支援の下で、データの機密性やプライバシーの確保に課題を抱えてきた様々なビジネス分野（医療、マーケティング等）において、複数組織で協力したデータ解析が可能になりました。

今後、NICT は、引き続き、秘密計算技術や連合学習技術等のプライバシー保護データ解析の基盤技術の研究開発を進め、イエラエセキュリティは、プライバシー保護連合学習技術のビジネス化を推進していきます。

※「株式会社イエラエセキュリティ」は、2022 年 4 月 1 日に「GMO サイバーセキュリティ by イエラエ株式会社」へ社名を変更いたします。

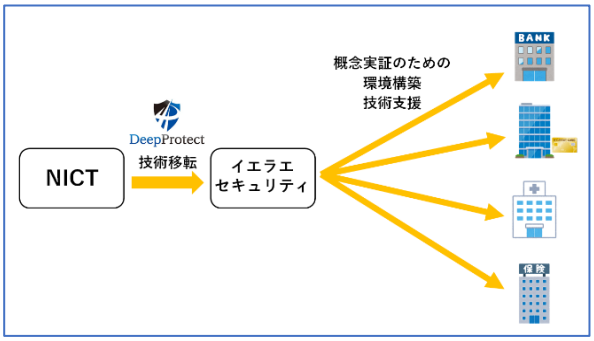
【背景】

様々な産業分野において AI の活用が普及し DX（デジタルトランスフォーメーション）が進展する中で、AI の性能を向上させるためには、多くの学習用データを集める必要があります。しかし、単一組織で十分な量のデータを確保することは難しく、また、複数組織間でデータを共有することについては、プライバシーの保護や情報漏えいに対する懸念があります。

このような中で、NICT はフェデレーテッドラーニング（連合学習）[*3] という技術に独自の暗号技術を融合し、パーソナルデータなど機密性の高いデータを互いに開示することなく安全に深層学習を用いて解析することができるプライバシー保護連合学習技術「DeepProtect」を開発しました。「DeepProtect」は、複数組織間で連合して深層学習を行う際に、組織外部に送信する情報（深層学習のパラメータ）を統計情報化し、かつ、暗号化することによって個人識別ができない状況で統合し、各組織の学習モデルを更新することが可能です。現在、NICT は、「DeepProtect」を活用して金融分野における不正送金の自動検知システムの実現に向けた実証実験を進めており（2022 年 3 月 10 日の報道発表を参照）、一方で、他の分野にも広く応用するため、本技術の社会実装を行うためのパートナーを探していました。

【今回の技術移転について】

今回 NICT は、サイバーセキュリティ・暗号・機械学習に関する高い技術力を持ち、実社会における社会課題解決に先端技術を適用する際の UX/UI デザインに強みを持つイエラエセキュリティとパートナーシップを構築し、同社に対し、「DeepProtect」に関する知的財産権をライセンスし技術移転を行いました。



NICT の「DeepProtect」をイエラエセキュリティに技術移転

これにより、イエラエセキュリティがプライバシー保護連合学習技術のビジネス利用に向けて環境構築・技術支援を実施する体制が整い、多様な業種（医療、マーケティング等）の企業等が、データの安全性を確保しつつ複数組織間で連合して深層学習を活用し、様々な社会課題を解決することが容易になると考えられます。

【今後の展望】

プライバシーの保護や情報漏えいに対する懸念に対処しつつ、複数組織間で連合して安全にデータを利活用することを可能とするために、NICT は、プライバシー保護データ解析技術の社会実装を目指し、引き続き、秘密計算技術や連合学習技術等の基盤技術の研究開発を進め、技術移転を推進していきます。また、イエラエセキュリティは、スマート社会実現に向け、複数組織間でのデータ利活用のユースケースに応じた最適なソリューションを様々な企業に提供し、プライバシー保護連合学習技術のビジネス化を推進していきます。

＜関連する過去のプレスリリース＞

・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
～実証実験に参加の金融機関を募集～
https://www.nict.go.jp/press/2019/02/01-2.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

・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
～被害取引の検知精度向上や不正口座の早期検知を確認～
https://www.nict.go.jp/press/2022/03/10-1.html

＜用語解説＞

***1 プライバシー保護連合学習技術「DeepProtect」**

DeepProtect は、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である。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。

本技術は、下記ジャーナルに採択・掲載されている。
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.
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

***2 プライバシー保護データ解析技術**

プライバシーの保護や漏洩の防止とデータ解析を両立する技術。パーソナルデータを複数組織間で共有することは、個人情報保護法上、個人情報の第三者提供にあたり、原則としてデータに係る個人の同意を要する。近年注目を集める秘密計算技術（データを暗号化などにより秘匿したまま計算を行い、各種解析を行う技術）を利用したとしても、現在の個人情報保護法上、個人情報は暗号化されていても個人情報として扱われるため、パーソナルデータの利活用上、課題があった。

***3 フェデレーテッドラーニング（連合学習）**

連合学習（Federated learning）とは、Google 社が提唱した、データ自体を一か所に集約せず分散した状態で連合して機械学習を行う技術であり、データを持つ複数の法人や個人がそれぞれ独自に機械学習を行い、学習結果の一部の情報のみを集約することによって学習済みモデルを更新することができる。あたかもデータを一か所に集約して機械学習を適用したような効果を安全に得られる技術として期待が集まっている。

＜ 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 総合企画室
山本 俊太郎
E-mail: crest-ppdm-info@ml.nict.go.jp

株式会社イエラエセキュリティ
取締役 CTO of Development
菅野 哲
E-mail: deepprotect@ierae.co.jp

＜ 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
Tel: 042-327-6923
E-mail: publicity@nict.go.jp

株式会社イエラエセキュリティ
事業推進部 事業推進課
E-mail: info@ierae.co.jp