

配信先: 総務省記者クラブ、テレコム記者会、文部科学記者会、
科学記者会、草津市政記者クラブ、長野市政記者クラブ、
松本市政記者クラブ、地方新聞記者会、
石川県文教記者クラブ、三重県政記者クラブ

プレスリリース
2025 年 7 月 1 日

国立研究開発法人情報通信研究機構
立 命 館 大 学
国 立 大 学 法 人 信 州 大 学
国 立 大 学 法 人 滋 賀 医 科 大 学
国 立 大 学 法 人 金 沢 大 学
国 立 大 学 法 人 三 重 大 学

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 ～プライバシー保護連合学習技術「DeepProtect」の医療応用～

【ポイント】

- 医療現場の課題解決を目指し、データサイエンス(高機能暗号)と医学(画像診断)の異分野融合研究を開始
- NICT・立命館大学が高機能暗号技術を応用し、連合学習技術の個人情報の保護とセキュリティの機能を強化
- 信州大学・滋賀医科大学・金沢大学・三重大学が放射線画像診断支援 AI の実現を目指し臨床研究を実施

国立研究開発法人情報通信研究機構(エヌアイシーティー、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プライバシー保護連合学習技術「DeepProtect」^{*1}を用いて、AI を活用した放射線画像診断業務の効率化・高度化を目指し、立命館大学(学長: 仲谷 善雄)、信州大学(学長: 中村 宗一郎)、滋賀医科大学(学長: 上本 伸二)、金沢大学(学長: 和田 隆志)及び三重大学(学長: 伊藤 正明)と共に、国立研究開発法人科学技術振興機構(JST)の K プログラム「セキュアなデータ流通を支える暗号関連技術(高機能暗号)」に、研究課題「高機能暗号を活用した連合学習技術の高度化と医療データへの応用」を共同提案し、採択されました。

これにより、高機能暗号技術^{*2}と連合学習技術に強みを持つ NICT 及び立命館大学が、医療向けに DeepProtect の個人情報の保護とセキュリティの機能を強化し、豊富な症例とデータを有する信州大学、滋賀医科大学、金沢大学及び三重大学は、DeepProtect を用いて放射線画像診断支援 AI を研究開発する異分野融合型の共同研究を開始します(図 1 参照)。

【背景】

近年、医療需要が高まり、診断業務のひっ迫が顕著となる一方で、医師の働き方改革が求められる医療現場において、AI を活用した診断の効率化・高度化が期待されています。医療現場での実用に耐え得る AI を実現するには、様々な属性を持つ患者の多様な症例を網羅する大量のデータを AI の学習に使う必要がありますが、単独の医療機関が網羅的なデータを確保することは困難です。一方、複数の医療機関のデータを連携させて網羅的で大規模なデータの確保を目指す場合、個人情報の保護とセキュリティの確保が課題となります。政府が次世代医療基盤法に基づく匿名加工医療情報による医療データの利活用活性化等の取組を進めているものの、匿名加工の困難さやデータ解析に及ぼす制約(匿名加工によってデータの粒度が落ちるため、AI の性能に悪影響を及ぼすことがある)等により、依然として医療機関間のデータ連携は難しいのが現状です。

近年、複数の機関が持つデータそのものを共有せずに共同で AI の学習を行うための有望な方法として、分散型機械学習技術の一種である連合学習技術が世界的に研究されています。しかし、現在の連合学習技術にはサイバー攻撃に対する脆弱性が指摘されており、要配慮個人情報を多く取り扱うため厳格なデータ保護が必要な医療データ解析に連合

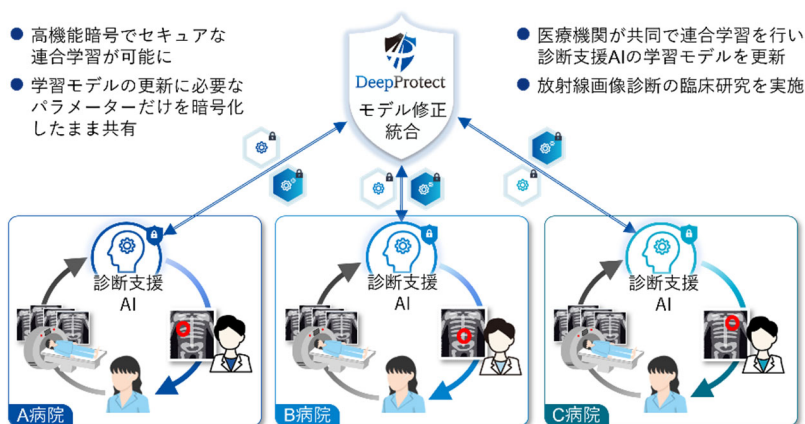


図 1 放射線画像診断支援 AI の実証実験のイメージ

学習技術に応用するには課題がありました。一方で、NICT ではこれまで、暗号技術と連合学習技術の融合により、個人情報の保護とセキュリティの機能を強化したプライバシー保護連合学習技術「DeepProtect」の研究開発に独自に取り組んできました。

【研究手法】

このような中で、NICT サイバーセキュリティ研究所と信州大学医学部は、2023 年に両機関の間で締結した包括連携協定書に基づき、2024 年に「医療・ヘルスケア分野のサイバーセキュリティ及びデータプライバシーの確保に関する研究に関する協定書」を締結し、医療現場の課題をデータサイエンスで解決するために協議を重ねた結果、今回、DeepProtect を放射線画像診断業務に応用することを目指すことになりました。

高機能暗号技術により、連合学習技術の個人情報の保護とセキュリティの機能を強化することで、複数の医療機関が安全に連携して画像診断支援 AI を実現する研究構想を策定し、共同研究機関を募った結果、信州大学医学部に加え、放射線画像診断において豊富な症例を有する滋賀医科大学医学部、金沢大学医薬保健研究域医学系及び三重大学医学部が参加することになりました。また、高機能暗号技術を用いた連合学習技術の研究開発には、NICT に加えて立命館大学情報理工学部が参加します。上記 6 機関は、JST の K プログラム「セキュアなデータ流通を支える暗号関連技術(高機能暗号)」に、NICT(研究代表者: 篠原 直行)を代表機関として、研究課題「高機能暗号を活用した連合学習技術の高度化と医療データへの応用」を共同提案し、採択されました。

本共同研究では、まず、NICT 及び立命館大学(主たる研究分担者: 野島 良)が DeepProtect を医療に応用することが可能となるように、個人情報の保護とセキュリティの機能を強化します。次に、信州大学(主たる研究分担者: 山田 哲)、滋賀医科大学(主たる研究分担者: 渡邊 嘉之)、金沢大学(主たる研究分担者: 小林 聡)及び三重大学(主たる研究分担者: 市川 泰崇)は、DeepProtect の提供を受け、それぞれの機関が長年にわたる診断(アノテーション)によって蓄積してきた大量のデータを教師データとして、放射線画像診断支援 AI のプロトタイプを開発し、標準治療として採用されることを目指して 2029 年まで臨床研究を行う計画です(図 2 参照)。



図 2 共同研究実施体制図

【波及効果・今後の予定】

プロトタイプの実証実験を通じて得られる DeepProtect の医療応用上の評価や課題は、NICT 及び立命館大学にフィードバックし、更なる技術向上のサイクルを回します。また、医療分野や ICT 分野の企業との連携を積極的に行い、個人情報の保護とセキュリティの機能の強化だけでなく、使いやすいユーザーインターフェースや保守可能なシステムの実現も含めた社会実装を目指すオープンイノベーション体制の構築を行います。

<関連する過去の NICT の報道発表>

- ・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 17 日 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～
<https://www.nict.go.jp/press/2022/03/17-1.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>
- ・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
～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>

本研究は、JST 経済安全保障重要技術育成プログラム【JPMJKP24U1】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
篠原 直行
E-mail: security@ml.nict.go.jp

立命館大学
情報理工学部 情報理工学科
野島 良
E-mail: ryo-no@fc.ritsumeit.ac.jp

信州大学
学術研究院(医学系)
山田 哲、山本 俊太郎
E-mail: flair-ml@shinshu-u.ac.jp

国立大学法人滋賀医科大学
放射線医学講座
渡邊 嘉之
E-mail: ywatanab@belle.shiga-med.ac.jp

国立大学法人金沢大学
医薬保健研究域医学系
小林 聡
E-mail: satoshik@staff.kanazawa-u.ac.jp

国立大学法人三重大学
附属病院放射線科
市川 泰崇
E-mail: yasutaka@med.mie-u.ac.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
E-mail: publicity@nict.go.jp

立命館大学
総合企画部広報課
Tel: 075-813-8300, Fax: 075-813-8147
E-mail: r-koho@st.ritsumeit.ac.jp

国立大学法人信州大学
総務部総務課広報室
Tel: 0263-37-3056, Fax: 0263-37-2182
E-mail: shinhp@shinshu-u.ac.jp

国立大学法人滋賀医科大学
総務企画課広報係
Tel: 077-548-2012, Fax: 077-543-8659
E-mail: hqkouhou@belle.shiga-med.ac.jp

国立大学法人金沢大学
医薬保健系事務部総務課総務係
Tel: 076-265-2109, Fax: 076-234-4202
E-mail: t-isomu@adm.kanazawa-u.ac.jp

国立大学法人三重大学
企画総務部総務チーム広報・渉外室
Tel: 059-231-9794, Fax: 059-231-9000
E-mail: koho@ab.mie-u.ac.jp

<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。

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 高機能暗号技術

従来の暗号技術に対して、機能が追加・向上される等の優位性を主張する暗号技術及び従来の暗号技術では困難であった事象を解決できる等の新規機能を有することを主張する暗号技術のこと。近年、従来の守秘、認証、署名の機能だけではなく、様々な機能を持つ「高機能暗号」(Advanced Cryptography)の研究開発が進んでおり、学会等で提案されている。高機能暗号は日本が強みを持つ分野であり、日本での研究開発が盛んで、日本発の高機能暗号が、多くの著名な国際会議で発表されている。また、ISO/IEC 等において標準化が進められている高機能暗号技術もある。