

## 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

### 【ポイント】

- 金融犯罪（不正送金等）の自動検知をめざした実証実験において 5 行の銀行との連携を開始
- 委託を受け、プライバシー保護深層学習技術により金融取引データを安全に解析
- データの機密性を維持したまま、複数組織による協調学習を可能とするシステムの構築を目指す

国立研究開発法人情報通信研究機構（NICT、理事長：徳田 英幸）サイバーセキュリティ研究所セキュリティ基盤研究室は、独自に開発したプライバシー保護深層学習技術「DeepProtect」<sup>\*1</sup> を利用し、国立大学法人神戸大学、株式会社エルテスとともに、現在の大きな社会課題である不正送金<sup>\*2</sup> の自動検知をめざして、データの利活用とプライバシー保護を両立できるプライバシー保護深層学習技術の研究開発及び実用性検証に取り組んでいます。「DeepProtect」は、データそのものを外部に送ることなく、複数の組織内で学習した結果のみを暗号化して中央サーバに集め、中央サーバで暗号化したまま学習結果を更新できる技術です。このたび、不正送金の自動検知の精度向上に向けて、既に連携してデータ解析を進めてきた千葉銀行に加え、三菱 UFJ 銀行、中国銀行、三井住友信託銀行及び伊予銀行が実証実験に参加し、オープンイノベーションによる実施体制を構築しました。各組織のデータを互いに開示することなく、複数組織による協調学習が可能なシステムを目指します。

※本実証実験は、2019 年度から JST CREST「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」の加速フェーズ研究課題として採択された研究課題「プライバシー保護データ解析技術の社会実装」のもとで実施しています。

### 【背景及びこれまでの経緯】

近年の目覚ましいテクノロジーの進化や経済のグローバル化が進む一方で、マネー・ローンダリング、不正送金、振り込み詐欺などの金融犯罪手法は以前にも増して複雑化・巧妙化しており、それらの脅威に対する対策は、社会課題の一つとして、より重要性を増しています。中でも、振り込み詐欺等の特殊詐欺による 2019 年の全国の被害金額は 8 年連続で 300 億円を超え（警察庁発表）、依然として深刻な社会問題となっています。これら不正送金等の金融犯罪に対して、現状、多くの金融機関は、それぞれが保有する金融取引データに対し、ルールベースのモニタリングツール<sup>\*3</sup> を用いて、人手で不正取引を検出していますが、これには担当者の経験等への依存やコストの課題があります。そこで、機械学習技術を用いた不正取引の自動検知システム（AI システム）の導入検討

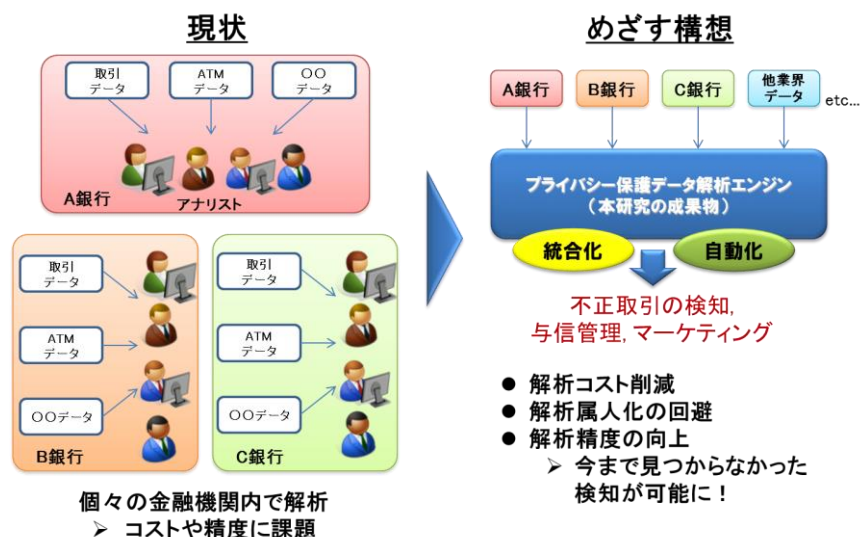


図 1 金融分野における課題と目指す構想

が進んでいますが、単独の金融機関では十分な量の学習データを用意することが難しく、また、個人情報を含む金融取引データを各金融機関外に持ち出すことができないため複数の金融機関で協力して学習することもできず、AI システムの普及は進んでいませんでした。

この社会問題を解決するため、NICT、神戸大学及びエルテスは、2019 年 2 月から、暗号技術と機械学習技術の融合により、データを外部に開示することなく機密性を保ったまま機械学習を行うことを可能とする NICT 独自開発のプライバシー保護深層学習技術「DeepProtect」を応用し、パーソナルデータの保護を図りつつ、複数の金融機関が協調して不正送金等を自動検知することが可能なシステムの実現を目指し、検知精度を向上させる実証実験に取り組んできました。

### 【今回開始した金融機関との連携と実験内容】

これまで、千葉銀行と進めてきたデータ解析において、個人を特定できないように加工された金融取引データ(取引明細情報及び口座情報)を用いて、特殊詐欺等の可能性が疑われる取引の検知を様々な機械学習手法を用いて試み、実際の不正送金のうち、70%以上を不正送金であると正しく判定できる例が出ています。しかし、個々の銀行で日々発生する不正送金の件数は、学習データとしては十分多いとはいえず、より多くの銀行のデータをもとに学習した結果を統合することで、不正送金の検知精度を 80%以上に向上させることを目指しています。

そこで、2019 年 2 月 1 日にプレスリリース<sup>\*4</sup>を行い、より多くの金融機関に対して実証実験への参加を呼び掛けたところ、新たに三菱 UFJ 銀行、中国銀行、三井住友信託銀行及び伊予銀行が実証実験に参加することになりました。

現在、NICT、神戸大学は各金融機関との業務委託契約の下、金融取引データ解析の委託を受け、個別の金融機関ごとの個人を特定できないように加工された金融取引データに対し機械学習技術を用いることで、不正取引の検知の実証実験を実施しています。今後、各金融機関の学習結果を統合し、協調して不正取引を検知するシステムの開発と社会実装を目指し、各金融機関との連携体制を深め、産学官連携体制の下、実証実験を進めてまいります。

### 【将来の展望】

NICT、神戸大学及びエルテスは、金融機関との連携の下、2021 年度末までに、プライバシー保護深層学習技術を活用し、各金融機関が持つ顧客データを互いに開示することなくプライバシーの保護を図りつつ、複数機関で連携した機械学習が可能なシステムを構築し、不正送金の高精度自動検知を実現することによって、特殊詐欺の検知精度向上に貢献していきます。

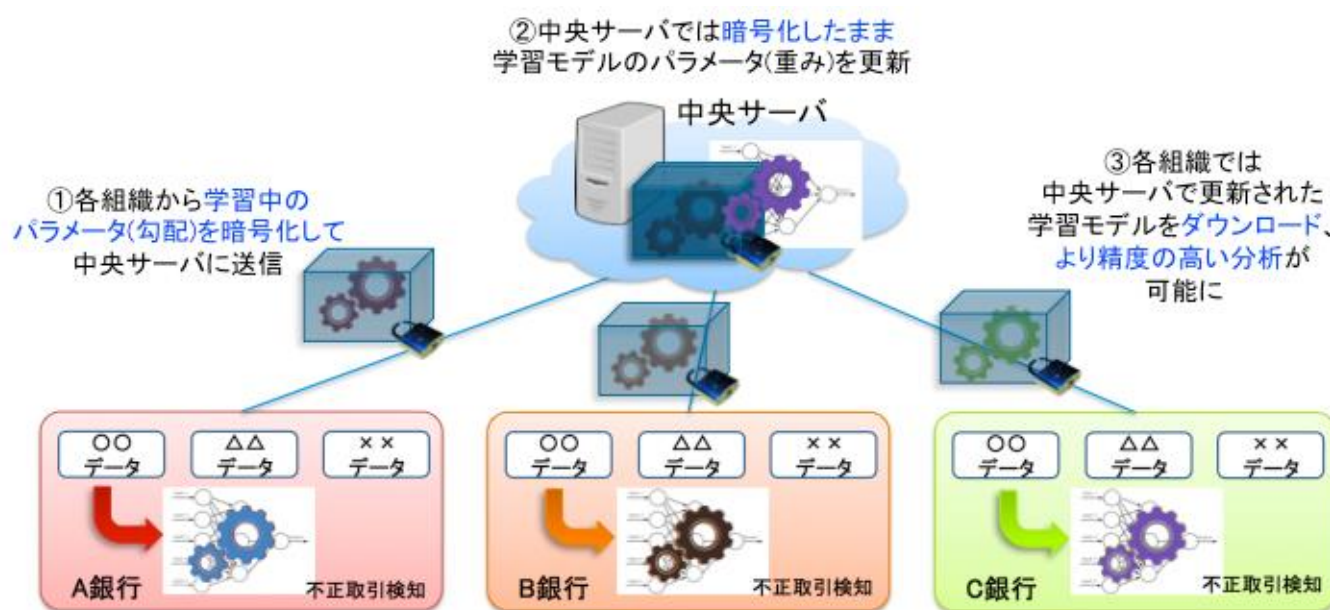


図 2 複数の組織が持つデータを外部に開示することなく協調して深層学習を行える  
プライバシー保護深層学習システム「DeepProtect」

## <用語解説>

### \*1 プライバシー保護深層学習技術「DeepProtect」

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)の更新を行うことができる。この更新処理は加算のみで行えるため、暗号化したまま加算が可能な「加法準同型暗号」を使うことで効率的に実現可能となっている。

複数の組織からの学習データを基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。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、各組織で持つ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.

### \*2 社会課題となっている不正送金

被害者に電話をかけるなどして対面することなく信頼させ、指定した預貯金口座への振込みその他の方法により、不特定多数の者から現金等をだまし取る犯罪(総称して「特殊詐欺」という)の全国での被害金額が 8 年連続で 300 億円を超える(警察庁調べ)など社会課題となっています。

### \*3 ルールベースのモニタリングツール

個人口座から 1 日に一定額(例えば、100 万円)以上の高額の送金が行われた場合にその口座を検出するなど、予め決められた条件(ルール)に合致した場合にアラートを出すようなモニタリングツール。

### \*4 2019 年 2 月 1 日のプレスリリース

「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～」(NICT、神戸大学、エルテス)

<https://www.nict.go.jp/press/2019/02/01-2.html>

## 研究支援

本研究の一部は、国立研究開発法人科学技術振興機構(JST)CREST「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」(研究総括: 栄藤 稔)における 2016 年度採択の研究課題「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(課題番号 JPMJCR168A、研究代表者: NICT 盛合 志帆)」及び 2019 年度加速フェーズ採択の研究課題「プライバシー保護データ解析技術の社会実装(課題番号 JPMJCR19F6、研究代表者: 国立研究開発法人産業技術総合研究所 花岡 悟一郎)」の下で行われています。

「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」プロジェクト Web サイト:

<https://crest.ppdm.jp/research-groups/group-moriai/>

#### < 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  
野島 良  
Tel: 042-327-5345  
E-mail: crest-ppdm-info@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  
大学院 工学研究科 電気電子工学専攻  
教授 小澤 誠一  
Tel: 078-803-6466  
E-mail: ozawasei@kobe-u.ac.jp

株式会社エルテス  
新規事業室  
宮宗 唯  
Tel: 03-6550-9280  
E-mail: miyaso@eltes.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  
廣田 幸子  
E-mail: publicity@nict.go.jp

国立大学法人神戸大学  
総務部 広報課  
Tel: 078-803-6678  
E-mail: ppr-kouhoushitsu@office.kobe-u.ac.jp

株式会社エルテス  
コーポレート部  
藤田 朱夏  
Tel: 03-6550-9280  
E-mail: pr@eltes.co.jp

## 金融分野における課題と目指す構想

現在、多くの金融機関では、個々の金融機関内で人手によるデータ解析を行っており、コストの高さや精度に課題があります。この課題を、我々が取り組むプライバシー保護深層学習技術を用いることで、複数の金融機関からのデータ統合解析及び自動化を実現し、調査コストの削減、調査精度の向上、属人化（本業務を特定の人が担当し、その人にしかやり方が分からない状態になること）の回避につなげることを構想しています。

金融分野には、不正送金検知のみならず、決済、融資、保険、マーケティング等の各分野で種々のロジックを用いた分析が行われており、複数金融機関でのデータ統合解析はまだ限定的であることから、本技術により、各種分析の精度の向上を期待できる領域が多く存在していると思われます。

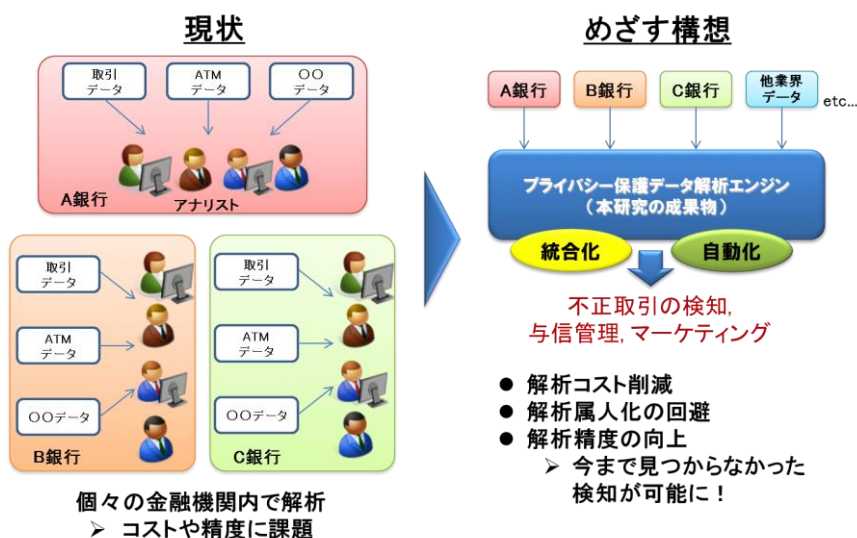


図 1 金融分野における課題と目指す構想(再掲)