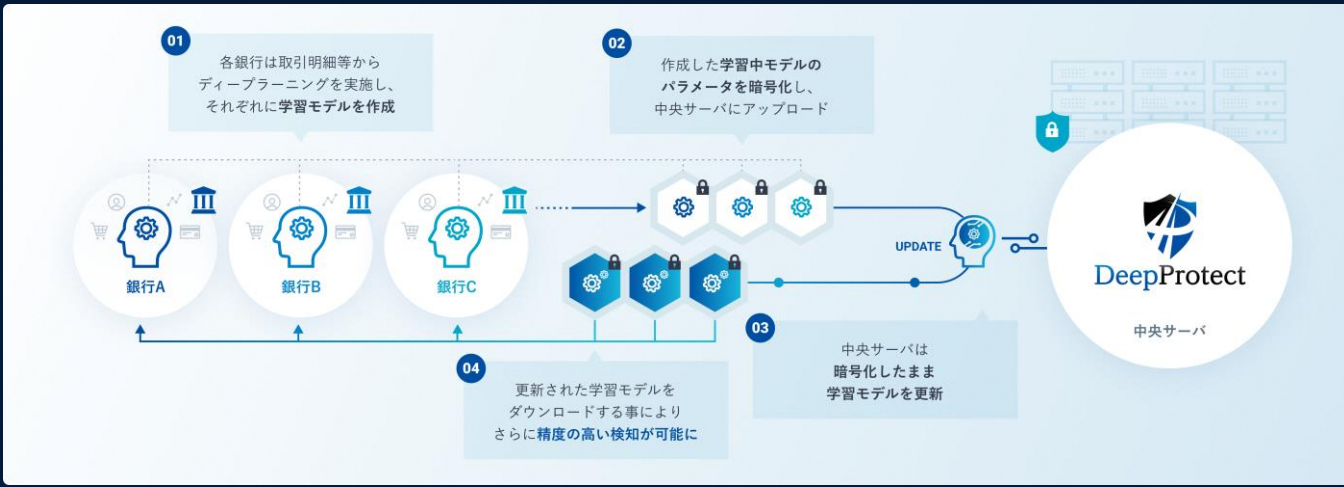
DeepProtect

個人情報など機密性の高いデータを開示せずに

複数組織で共同のデータ解析が可能に

DeepProtectの仕組み

～ 金融機関の不正取引検知の例 ～



DeepProtectは、連合学習（Federated Learning）という機械学習の手法に暗号技術を融合して実現した国立研究開発法人情報通信研究機構（NICT）独自のプライバシー保護技術です。

① まず、各組織は各自のデータをディープラーニングによって学習し、それぞれ学習モデルを作成していきます。
② 次に、各組織内で更新された学習モデルの差分パラメータ（勾配情報）を暗号化した上でそれぞれアップロードし、DeepProtectサーバに集約します。DeepProtectサーバに送られるのは差分のパラメータのみであり、各組織内のデータはアップロードされず、それぞれの組織内に留まります。
③ さらに、各組織からDeepProtectサーバにアップロードされたそれぞれの差分のパラメータは、秘密計算技術（準同型暗号技術）によって復号されずに暗号化されたまま統合・更新されます。
④ 各組織はこの更新された学習モデルをダウンロードし、各自の学習モデルを更新していきます。

このサイクルを繰り返すことで、精度の高い学習モデルを共同で構築し、各組織内のデータ解析に適用することができます。

一連の流れの中で各組織のデータは外部に送信されず、唯一外部に送信されるパラメータは暗号化されたまま処理されるため、データの機密性やプライバシーを保ちつつ、複数機関が共同して学習モデルを構築することが可能となります。

ユースケース

～ DeepProtect の活用先として考えられるユースケースをご紹介します ～

金融

マネー・ローンダリング、不正送金、振り込め詐欺などの金融犯罪手法は複雑化・巧妙化しており、早急な対策が求められています。DeepProtect を活用して複数の銀行にまたがるデータの解析を行うことで、単独の銀行では難しかったこれらの犯罪の検知が可能になります。

医療・ライフサイエンス

ウェアラブルデバイスの普及によるバイタルデータの観測や電子カルテシステム基盤などの環境整備が進み、医療やヘルスケア分野においても大量のデータの収集が行われています。DeepProtectを活用することで、このような機密性の高いデータのセキュアな統合分析が可能になります。

マーケティング

マーケティングデータの分析においても、DeepProtectを使うことでより精度の高い分析の実現が期待できます。単独の企業内のデータにとどまらず、グループ企業や販売パートナー企業、あるいは業界内を横断した豊富なデータをベースとした学習モデルの構築がその可能性を広げます。

製造

製造現場へのIoT技術の導入とともに、AIを使ったデータ分析の取り組みも始まっています。設備等の故障予知保全、部品の品質管理や製品の異常検知などさまざまな活用が期待される一方で、１社単独ではデータが足りず精度の高い検知が難しい場合もあります。DeepProtectはこの課題の解決を支援します。

サービス

電力やガスなどの公益サービスにおける需給バランスの最適化、あるいは自動翻訳やスパムメールの検出、カスタマーサービスのチャットボット、バーチャルアシスタントサービス、自律走行を制御する車両運転システムなど、高い機密性が求められるデータの分析を行う民間サービスについても広くDeepProtectの活用が期待できます。

～ DeepProtectを動画とサイトでご欄いただけます ～

[動画]
DeepProtectでの金融機関の不正検知

[サイト]
DeepProtectについて

お問い合わせ

DeepProtect全般についてのお問い合せは、こちらにお願いいたします。

〒184-8795
東京都小金井市貫井北町4-2-1

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

Mail：crest-ppdm-info@ml.nict.go.jp

〒150-8512
東京都渋谷区桜丘町26番1号

ＧＭＯサイバーセキュリティ ｂｙイエラエ株式会社
AI開発部

Mail：deepprotect@gmo-cybersecurity.com