C 03

サイバーセキュリティ

DeepProtect: 暗号化された情報で深層学習！

～ 組織間で生データを共有せず連合学習技術でデータ保護を実現 ～

外部連携可

基礎研究 応用研究 技術実証 社会実証

概要

DeepProtectは、連合学習という機械学習の手法に暗号技術を融合したNICT独自のプライバシー保護技術です。複数の組織が持つデータセットを互いに秘匿し、プライバシーや機密性を保ったまま共同で深層学習を実行します。

DeepProtect の仕組み

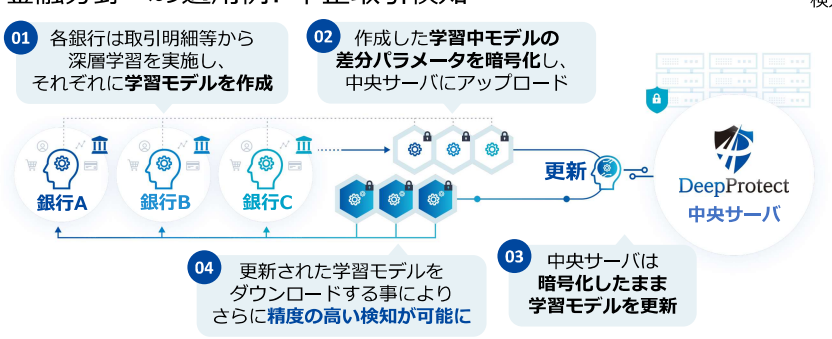
原論文が受賞

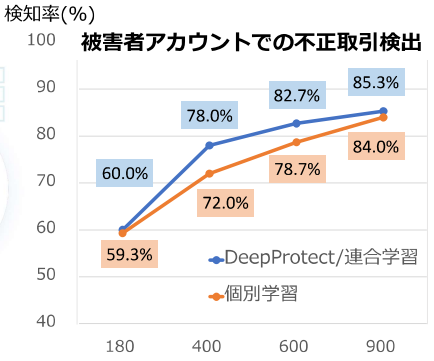
＼ 2023 IEEE SPS Best Paper Award ／

- 暗号化された情報だけが各組織の外で使用され、**各組織のデータは公開されない**
- 準同型暗号を連合学習に応用して、**プライバシー保護と実用性を両立**する

DeepProtect Webサイト

金融分野への適用例: 不正取引検知





- 銀行データを用いた不正検知の実証実験によって実用性を立証
- 各銀行が自分のデータだけで個別に学習した場合よりもDeepProtectで他銀行と協力した場合の方が不正利用を多く検知できる

特徴

- 連合学習と準同型暗号の融合
- データセットは非公開のまま深層学習
- 個々のデータセットだけでの学習よりも性能向上

ユースケース

- 銀行間で不正送金の検出のために協力
- クレジットカードの不正利用検知のために協力
- 複数の病院の電子カルテから病気発見の可能性

今後の展開

- ビジネス展開を見込んでいる企業への技術移転
- 更なる社会実装の促進
- 金融、医療に限らず様々な分野での活用の可能性を探索

【お問合せ先】
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 : security@ml.nict.go.jp

NICTオープンハウス2024