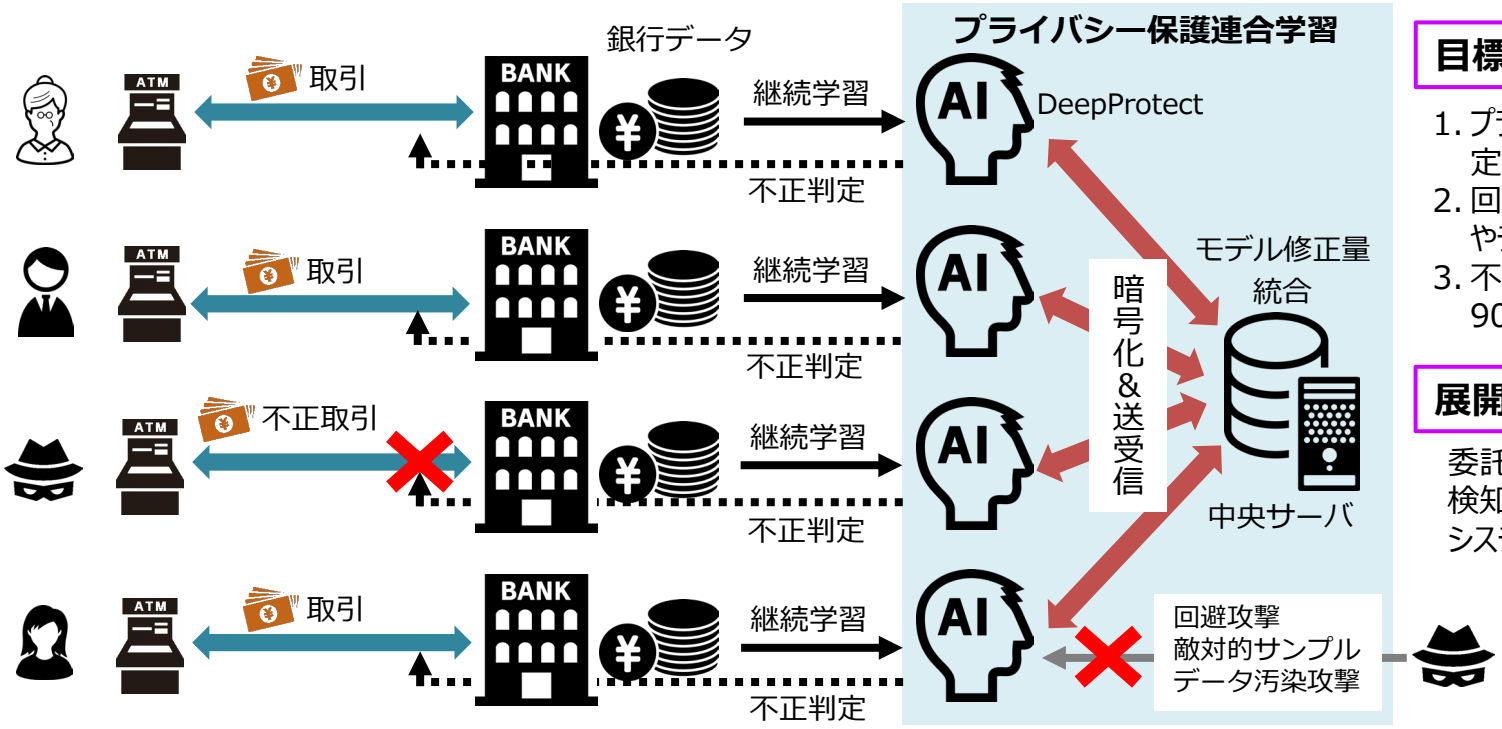
課題229
採択番号22901

プライバシー保護連合学習の高度化に関する研究開発

継続実運用に資する不正取引モニタリングに向けたプライバシー保護連合学習の高度化

研究概要：組織の機微なデータを他組織と共有しなくても、高度なAIを協調して構築できる連合学習は、プライバシー保護を重視する社会実装に不可欠な技術となりつつある。本研究では、現状の連合学習で実運用上解決すべき問題である安定した継続学習および回避攻撃を意図した敵対的サンプルやデータ汚染攻撃への耐性向上を実現し、DeepProtectの高度化を行うことを目的とする。また、本技術を喫緊の社会課題であるマネーロンダリング対策に導入し、４行以上の金融機関との連携を通して不正送金検知実証実験を実施し、不正取引の検知再現率が継続的に90%以上維持されることを目標とする。



目標

1. プライバシー保護連合学習における安定した継続学習の実現
2. 回避攻撃を意図した敵対的サンプル・やデータ汚染攻撃への耐性向上
3. 不正取引の検知再現率が継続的に90%以上を達成

展開・普及計画

委託研究の終了後において、不正取引検知プロトタイプの取引モニタリング共同システムへの採用を目指す

【研究開発期間】 令和４年度から令和５年度まで
【受託者】 国立大学法人神戸大学（代表研究者）、ＥＡＧＬＹＳ株式会社