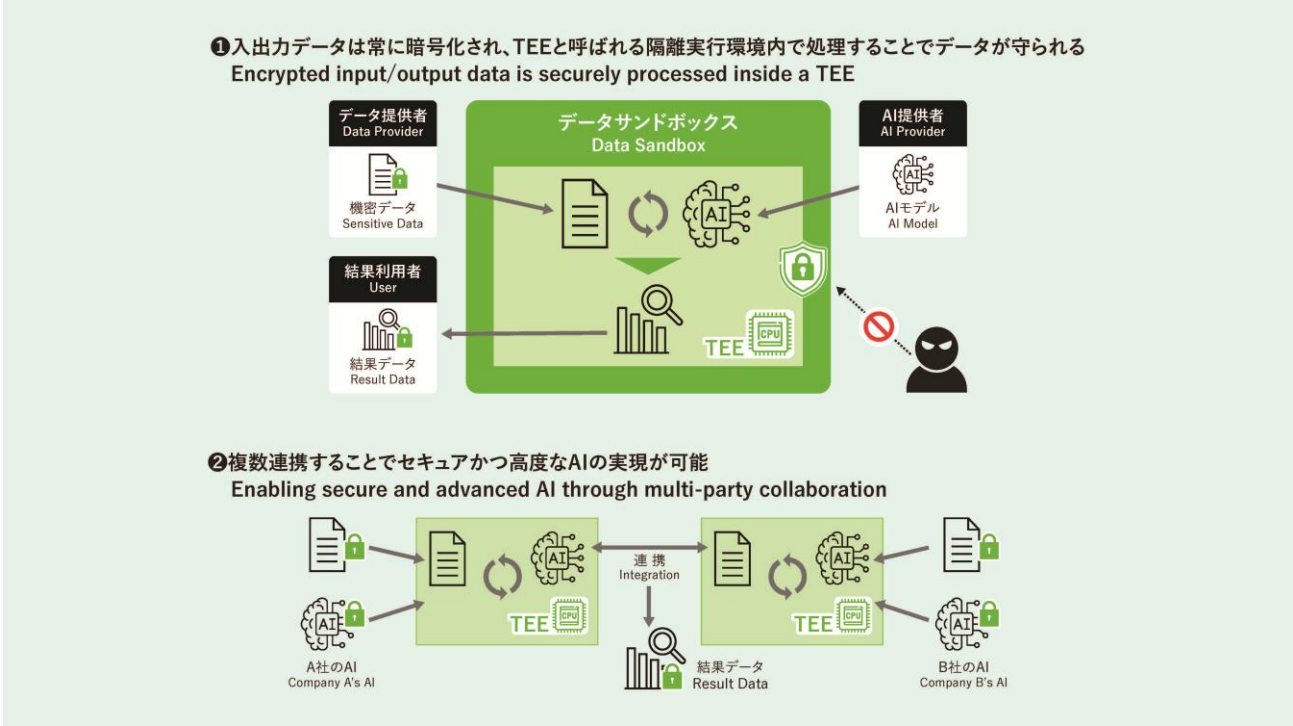
複数企業のデータを相互に秘匿したまま、AIでの活用を実現します

安全なAI活用を実現する秘匿処理技術

背 景 – 技術課題

企業のデータ活用において、複数のAIが連携して業務を支援するニーズが高まっています。また、安全性確保のためTEE（安全性が担保された計算処理空間-）の活用が進んでいます。しかし、TEEは利用範囲が単一組織内に限られ、悪意あるAIモデルやプログラムへの対策も不十分です。



研 究 目 標 – 成果

複数の組織が持つデータやプログラムを秘匿したままでの、データのAI活用を実現します。

技 術 ポ イ ン ト

01 要素技術

- データやプログラムを計算中も秘匿する秘匿処理技術
- 悪意のあるプログラムによるデータの漏洩を防ぐ要塞化技術

02 市中技術差異点

- 複数企業でのデータの共同利用が可能
- ユーザやAIプログラム経由でのデータ流出・窃取を防止

利用シーン	金融／ヘルスケア／宇宙・防衛	**R&Dフェーズ**	研究
技術確立予定時期	FY25-FY26	**ビジネス化予定時期**	FY27-FY29

【出展企業】
NTT株式会社 ソフトウェアイノベーションセンタ

【問い合わせ先】
データ基盤プロジェクト

【共同出展社/社外連携先】
株式会社NTTデータグループ

【関連Link】
https://www.rd.ntt/iown_tech/post_61-2.html