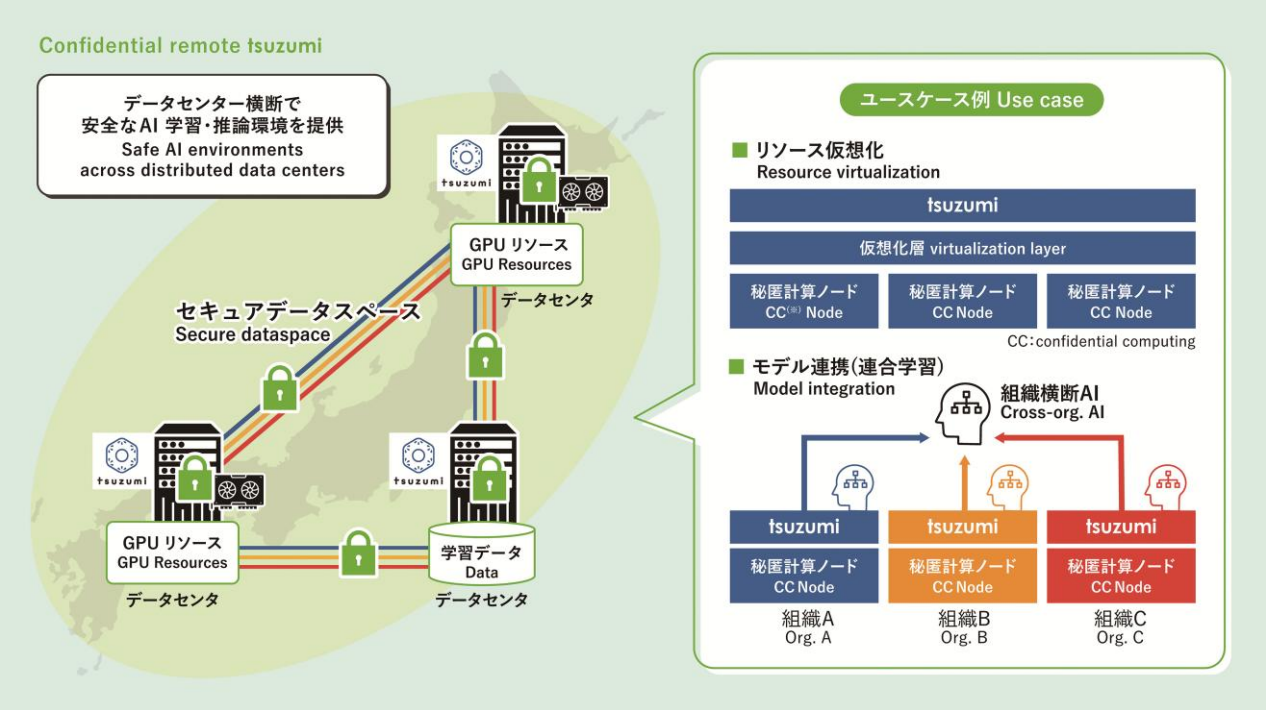
安心・安全 # データ活用 # リスクマネジメント

量子コンピュータ時代でも、安全な複数データセンタ連携によるAI分析を実現します

セキュアデータスペース

背 景 – 技術課題

AI駆動型社会の実現に向け、分散データセンタを活用した安全かつ高信頼の計算環境の実現をめざします。これには、量子計算機時代の安全な通信方式、CPUメモリ保護に代表されるハードウェアレベルの計算空間の安全性確保方式などに加えて、こうした機能が正しく実施されていることの検証可能性が重要です。また、こうした大規模かつ高信頼な計算環境により実現する、複数事業者のデータ連携によるAI学習モデルの品質向上が期待されています。



研 究 目 標 – 成果

安全性が確保され、相互に正当性が検証可能なセキュア計算空間を多数接続し実現する「セキュアデータスペース」上でtsuzumiなどのLLMを動作させることにより、分散データセンタ上での安全なAI活用、連合学習を実現します。

技 術 ポ イ ン ト

01 要素技術

- 多数のセキュア計算空間を耐量子ネットワークで相互接続し、これらを包括して保護する、リソース連携方式
- セキュア連合学習によるAIモデルの安全な統合方式

02 市中技術差異点

- セキュア計算空間、通信経路などシステム全体の暗号化状態を相互検証可能とする新たなプロトコルの確立
- 差分プライバシを適用した安全な連合学習の実現

利用シーン	マルチインダストリー	**R&Dフェーズ**	研究
技術確立予定時期	FY25-26	**ビジネス化予定時期**	FY27-29

【出展企業】
NTT株式会社 社会情報研究所

【問い合わせ先】
社会情報流通研究プロジェクト

【共同出展社/社外連携先】
–

【関連Link】
https://www.rd.ntt/sil/project/iown-pets/iown-pets.html