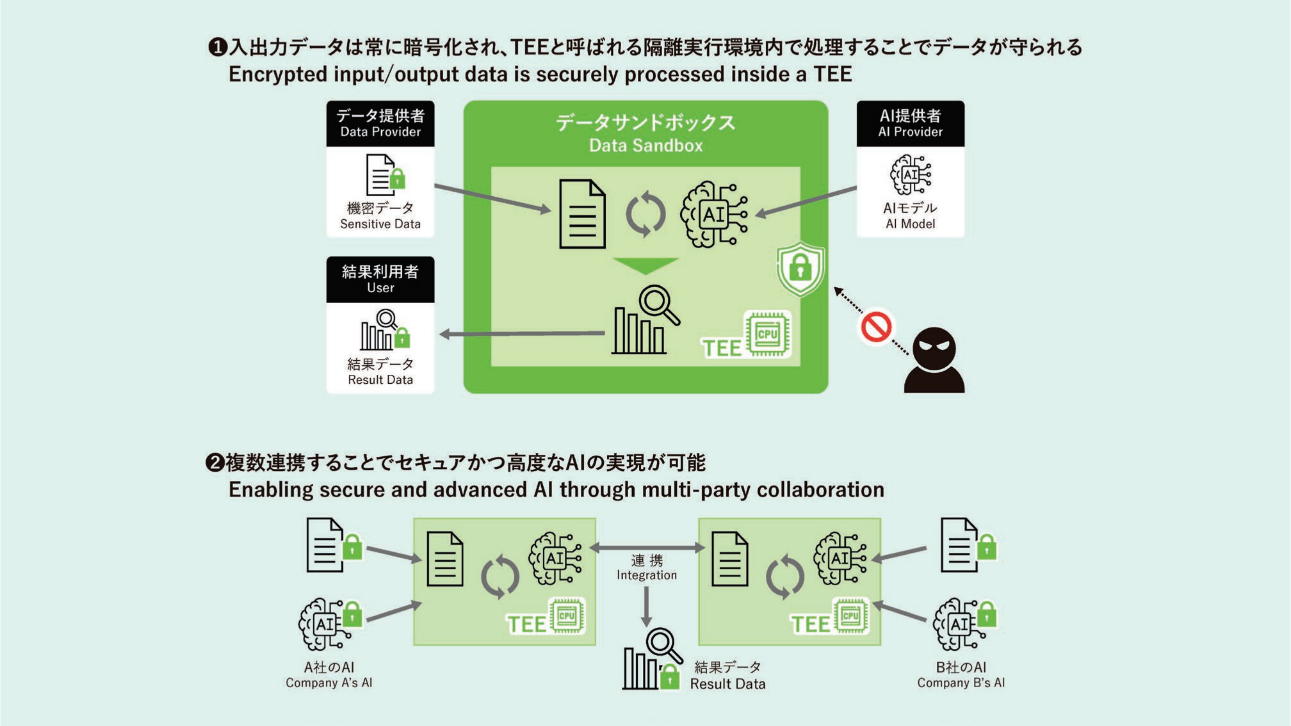
Enabling AI utilization while keeping data confidential across users

Data Sandbox for safe AI utilization

Background and Technical Challenges

In enterprise data utilization, the need for collaboration among multiple AIs to support operations is increasing. To ensure security, the use of TEE is expanding, but its scope is limited to single organizations and lacks measures against malicious AI models or programs.


❶入出力データは常に暗号化され、TEEと呼ばれる隔離実行環境内で処理することでデータが守られる
Encrypted input/output data is securely processed inside a TEE
データ提供者
Data Provider
機密データ
Sensitive Data
データサンドボックス
Data Sandbox
AI提供者
AI Provider
AIモデル
AI Model
AI
結果利用者
User
結果データ
Result Data
TEE
CPU
❷複数連携することでセキュアかつ高度なAIの実現が可能
Enabling secure and advanced AI through multi-party collaboration
連 携
Integration
A社のAI
Company A's AI
結果データ
Result Data
B社のAI
Company B's AI

R&D Goals and Outcomes

Enables AI utilization of data and programs from multiple organizations without disclosing them.

Key Technologies

01 Core Technologies

- Confidential computing technology that keeps data and programs secure even during processing
- Fortification technology that prevents data leakage by malicious programs

02 Key Differentiators

- Enables collaborative data utilization across multiple companies
- Prevents data leakage and theft through users or AI programs

Use Cases	Financial Services/Healthcare/ Aerospace & Defense	**R&D phase**	Research
Technology Schedule	FY25-FY26	**Commercialization Schedule**	FY27-FY29

【Exhibitors】
NTT Software Innovation Center

【Contact】
Data Sharing Infrastructure Project

【Co-exhibitors】
NTT DATA Group Corporation

【Related Links】
https://www.rd.ntt/iown_tech/post_61-2.html