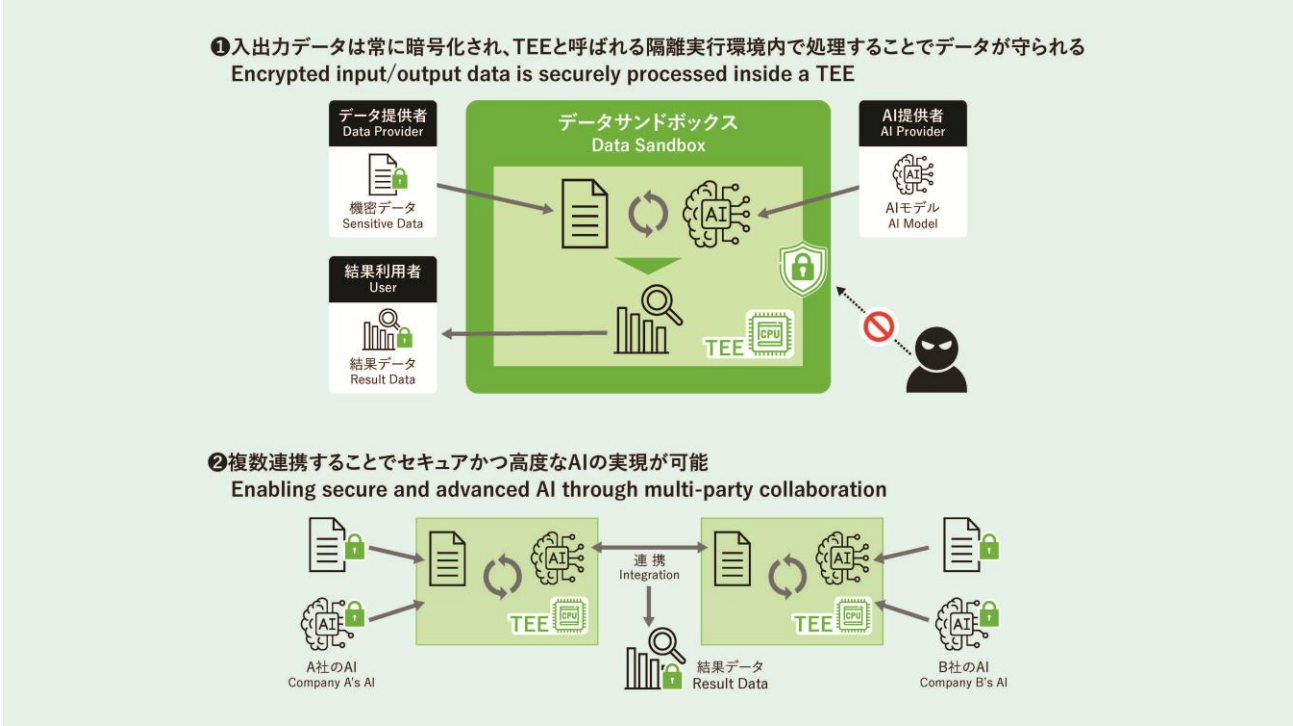
Enabling AI utilization while keeping data confidential across users

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.



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

【Co-exhibitors】
NTT DATA Group Corporation

【Contact】
Data Sharing Infrastructure Project

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