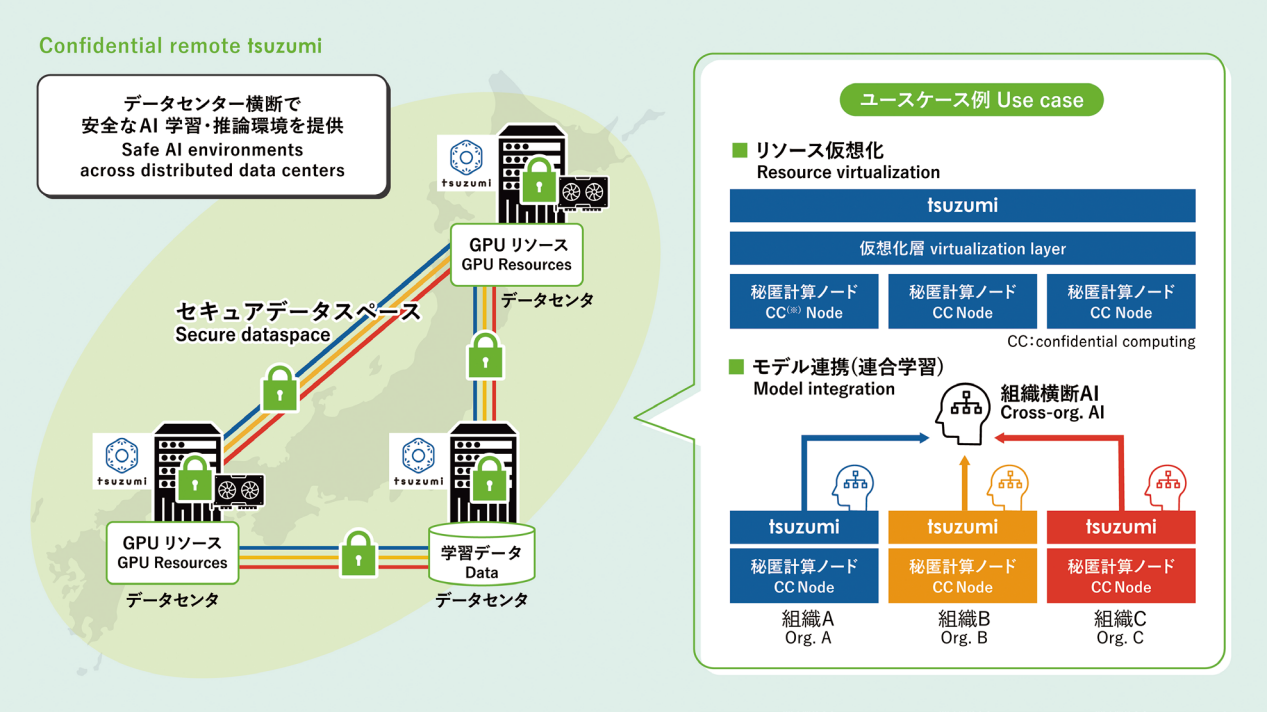
#Safety & Security #Data-Driven Insights #Risk Management

Enabling AI analytics through secure multi–data center collaboration, even in the era of quantum computing

Secure Data Space

Background and Technical Challenges

We aim to build a “Secure Data Space” by developing secure and trustworthy utilization of computing and network resources in distributed data centers. This requires post-quantum communication, computing resource protection like CPU memory protection and their verifiable implementation. In addition, such environments will also enable high-quality AI learning through data collaboration across organizations.



R&D Goals and Outcomes

We aim to realize secure and verifiable AI analytics and federated learning across distributed data centers by operating LLMs such as “tsuzumi” within Secure Data Space, established through the interconnection of secure and verifiable computing resources.

Key Technologies

01 Core Technologies

- A framework linking secure computing resources through quantum-safe networks, securing computing and connectivity as one trusted domain.
- A secure AI model integration mechanism based on Secure Federated Learning.

02 Key Differentiators

- A protocol for mutual verification of encryption across memory and communication domains.
- Implementation of Secure Federated Learning enhanced with Differential Privacy techniques.

Use Cases	Multi-industry	**R&D phase**	Research
Technology Schedule	FY25-26	**Commercialization Schedule**	FY27-29

【Exhibitors】
NTT Social Informatics Laboratories

【Co-exhibitors】
-

【問い合わせ先】
Social Information Sharing Research Project

【Related Links】
https://www.rd.ntt/e/sil/project/iown-pets/iown-pets.html