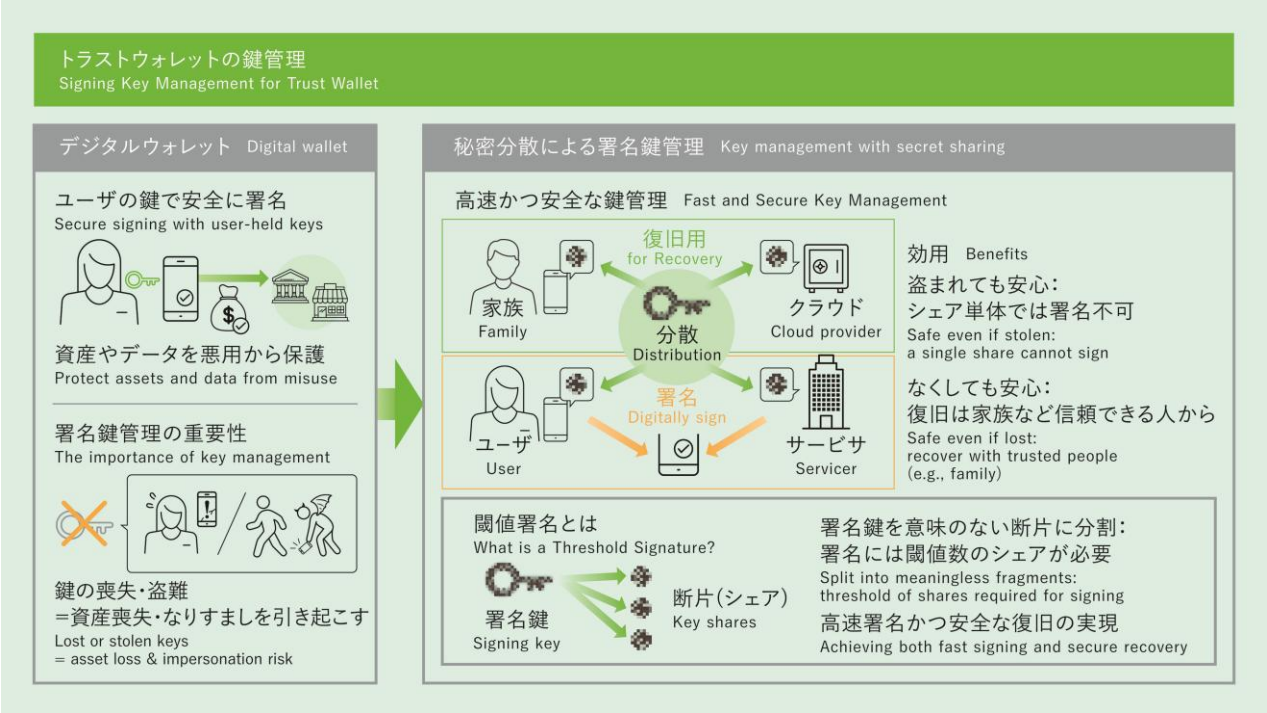
Distributed key management for flexible recovery from loss or leakage

Secret-sharing-based trust wallets

Background and Technical Challenges

Digital wallets, which store digital currency and certificates, have been attracting increasing attention. The security of the “signing key,” equivalent to a personal seal, is crucial. However, if the key is lost due to smartphone failure or loss, assets may become inaccessible. Therefore, a secure and user-friendly key management mechanism is required.



R&D Goals and Outcomes

To enable secure and flexible recovery of signing keys via secret sharing for trusted digital ID and payment platforms.

Key Technologies

01 Core Technologies

- Distributed key management using secret sharing
- Flexible key share recovery and access control
- Quick key share recovery from partial data loss

02 Key Differentiators

Conventional cloud- or device-based key management made recovery difficult. This technology splits a key into shares and enables secure recovery with trusted parties.

Use Cases	Public Services & Local Government	**R&D phase**	Development
Technology Schedule	FY25–26	**Commercialization Schedule**	FY27–29

【Exhibitors】
NTT Social Informatics Laboratories

【Co-exhibitors】
-

【Contact】
Social Information Sharing Research Project

【Related Links】
-