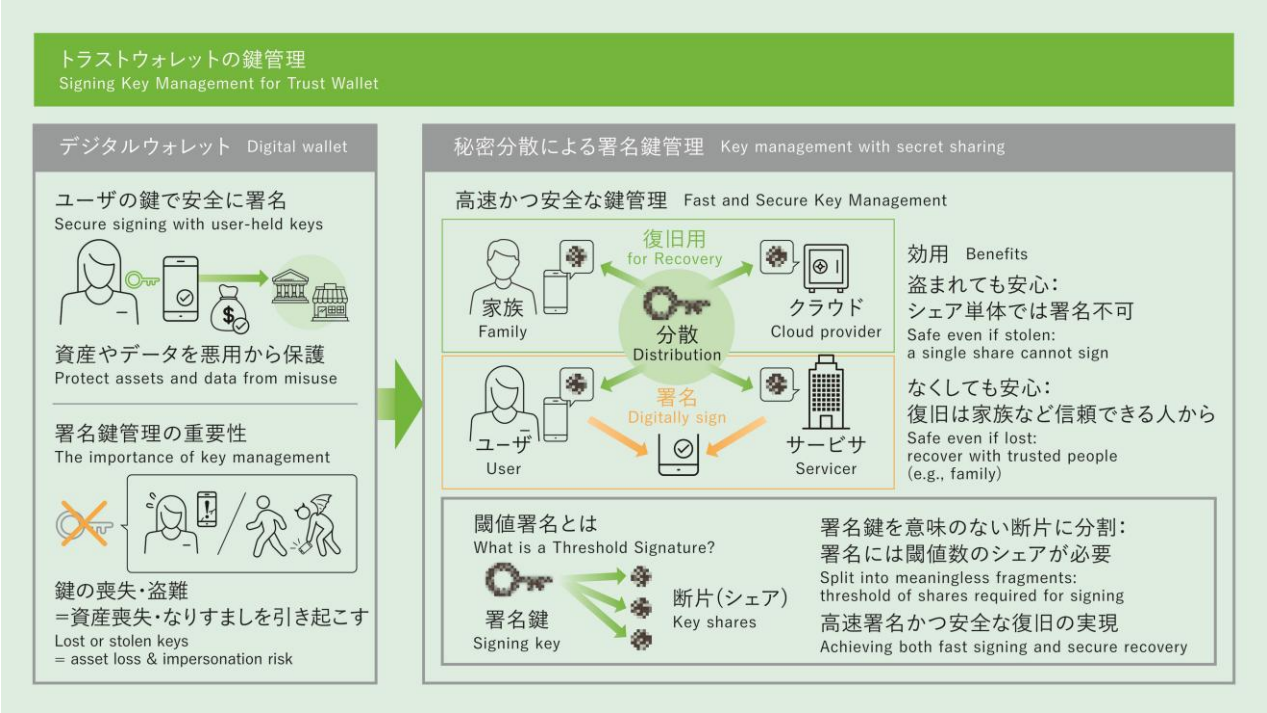
ウォレットの鍵を分散管理し、漏洩・紛失時も柔軟かつ安全な復旧を実現します

# 秘密分散型トラストウォレット

## 背 景 – 技術課題

電子現金や証明書を保管する「デジタルウォレット」は、近年ますます注目を集めています。デジタルウォレットにおいては、実印に相当する「署名鍵」の安全性が極めて重要です。しかし、スマートフォンの故障や紛失などによって鍵を失ってしまうと、資産が利用できなくなるリスクがあります。このため、安全性を確保しつつ利便性も損なわない鍵管理の仕組みが求められます。




## 研 究 目 標 – 成果

秘密分散技術により鍵の漏洩や紛失時でも柔軟かつ安全に復旧可能な管理を実現し、信頼性あるデジタルIDや決済基盤への応用をめざします。

## 技 術 ポ イ ン ト

### 01 要素技術

- 秘密鍵を安全に分散管理する、閾値秘密分散技術の適用
- 信頼レベルや利用環境に応じた鍵シェア構成の柔軟な制御
- 一部の鍵シェアが失われても復旧可能とする部分復元プロトコルの実装

### 02 市中技術差異点

従来のクラウドや端末単体での鍵管理では、紛失時の復旧が困難でした。本技術では、鍵を意味のない断片（シェア）に分割し、家族など信頼できる相手と協調して復旧できる、柔軟かつ安全な仕組みを実現します。

| | | | |
|---|---|---|---|
| **利用シーン** | 公共サービス・自治体 | **R&Dフェーズ** | 開発 |
| **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】**
–