量子コンピュータの特性を活用した新たな暗号機能

NTT 社会情報研究所　西巻　陵

2026年 2月27日

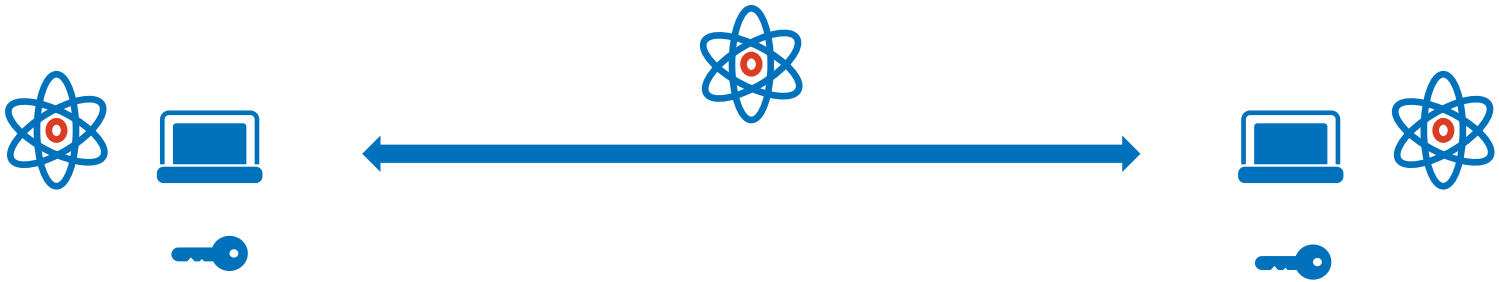
量子コンピュータと古典暗号の限界

量子コンピュータによる攻撃

- 量子コンピュータの登場によって既存の多くの暗号が破られる
- 量子コンピュータに対しても安全と期待される暗号（耐量子計算機暗号）への移行が必要
- 耐量子計算機暗号は古典コンピュータ上で動く
- 量子コンピュータによる防御は？

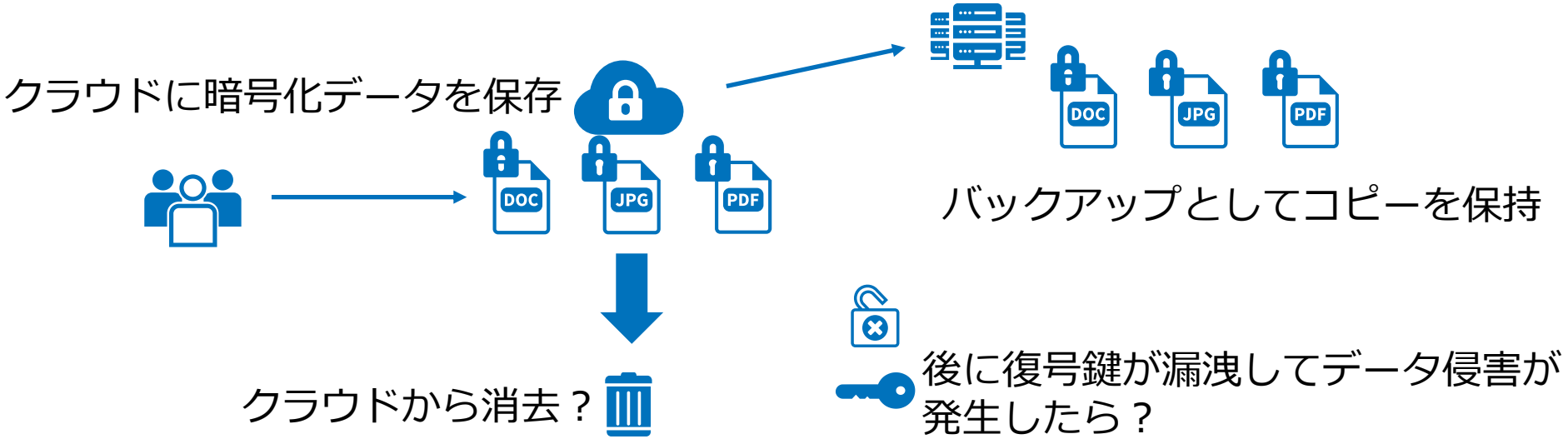
量子技術を利用した暗号

- 量子鍵配送（Quantum Key Distribution）
- 量子状態を利用することで安全に鍵共有を行う



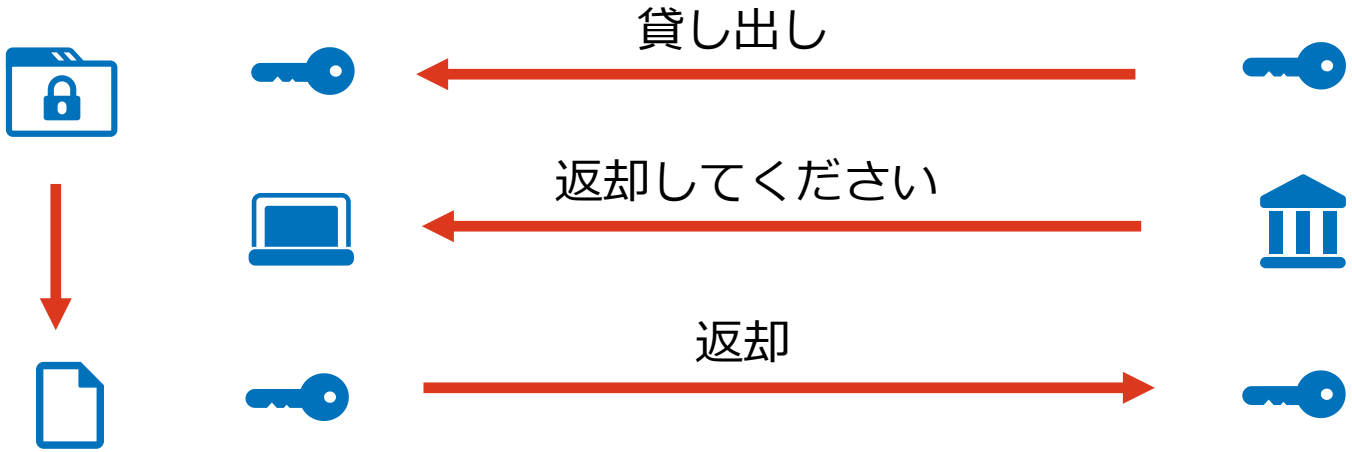
- 鍵共有という暗号機能自体は古典コンピュータでも実現可能
- 安全性が無条件であるか、計算が困難とされている問題に依拠しているかが違い
- さらに、信頼できる古典通信路が必要

古典暗号の限界



デジタル情報はいくらでもコピー可能であり消去したことを証明する手段はない

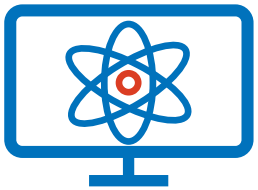
古典暗号の限界



コピーを保持可能
消去の保証がない

安全な貸与は古典暗号では実現不可能

量子情報の力を応用？



複製不可能定理：すべての未知の量子状態をコピーする一般的な方法はない

不確定性原理：ある情報量Aを高い精度で観測すると別の情報量Bは低い精度でしか観測できない

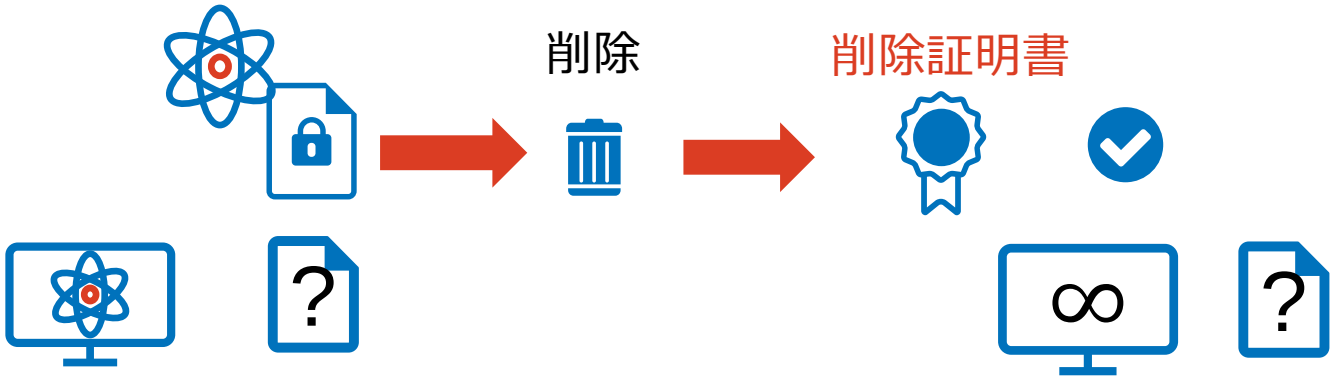
古典暗号の限界を量子情報の力で突破可能？
(古典暗号で実現不可能なことが実現できるか？)

できる！

量子性を使って初めて実現可能な暗号

削除証明可能暗号

量子状態の暗号文

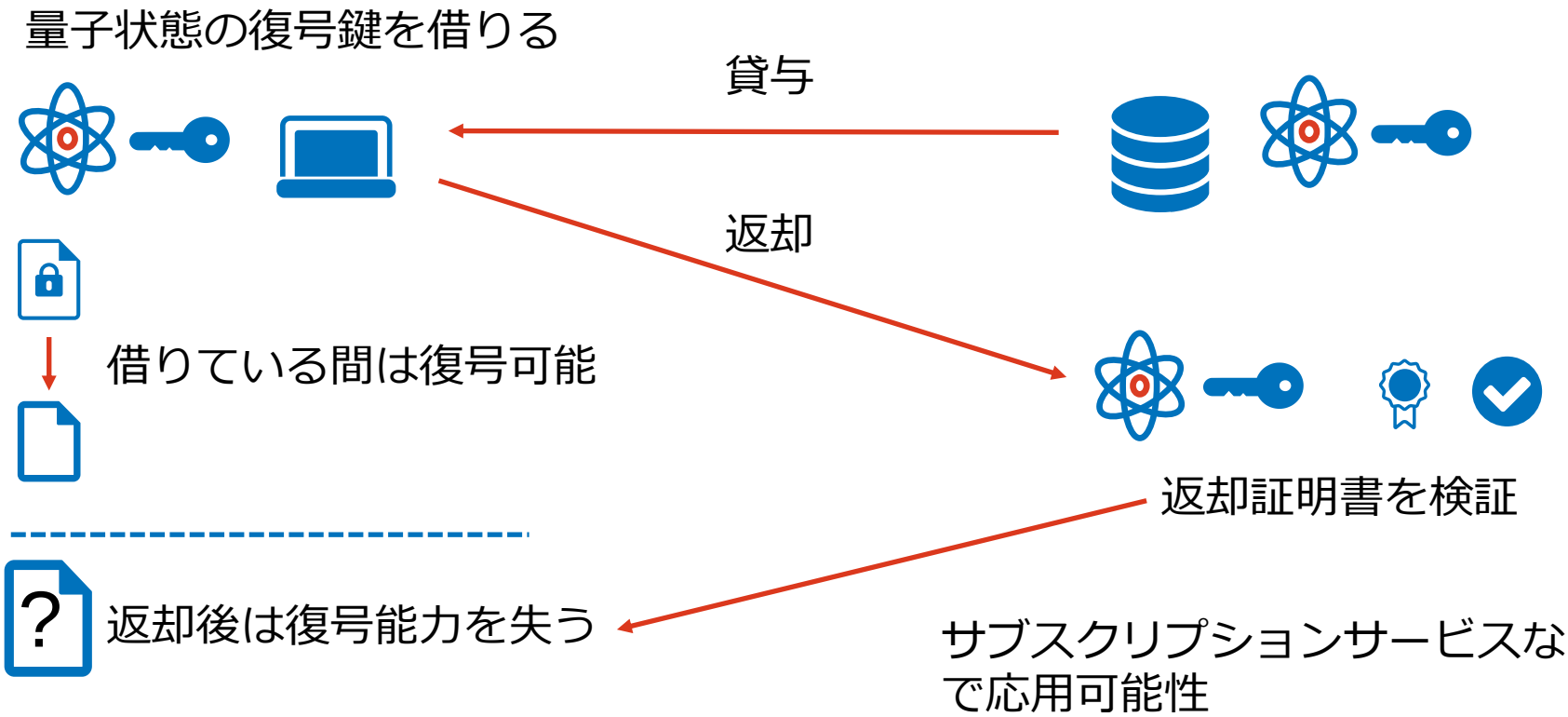


量子コンピュータでも
平文の内容はわからない

削除後は無限大の計算能力があっても
平文の内容はわからない

暗号文を一度外部に預けても削除すれば安全

安全な鍵貸与

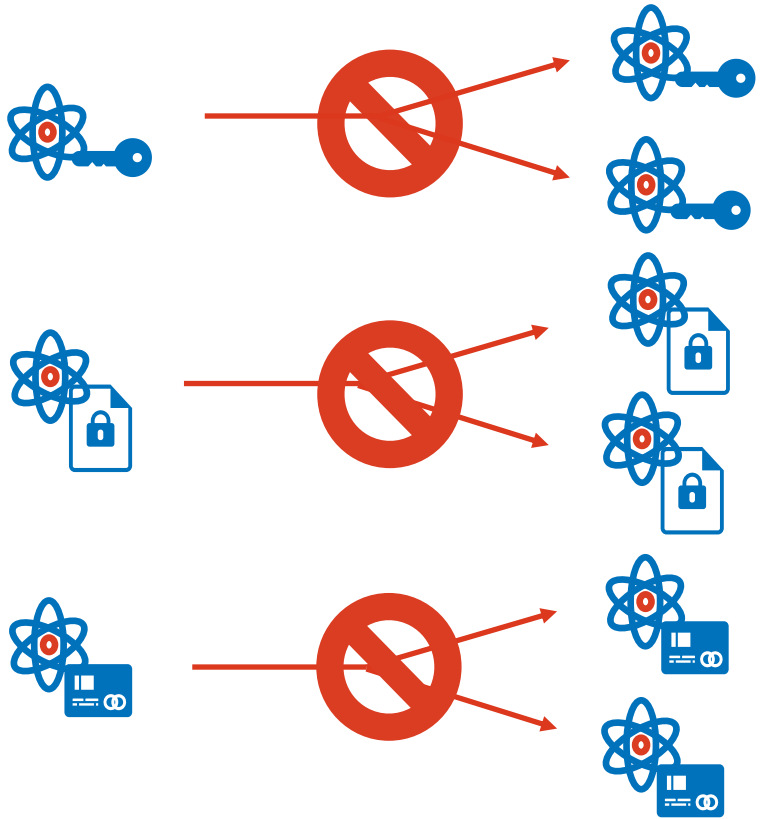


複製不可能暗号

量子秘密鍵

量子暗号文

量子プログラム



コピーを作成不可能

消去や返却といった
操作は不要

消去証明や安全な貸与
よりも達成が困難

まとめ

- 量子コンピュータを攻撃ではなくより高度な防御に利用
- 量子情報に固有の性質を使って古典コンピュータでは絶対に実現不可能な暗号機能を実現できる可能性
- 最新の研究で理論的には消去証明可能暗号や安全な鍵貸与は実現可能であることがわかってきている
- 複製不可能暗号の実現については未解明な点がまだ多い

Innovating a Sustainable Future for People and Planet


NTT