量子コンピュータは暗号社会に何をもたらすか？

金融研究所　情報技術研究センター
主査　清藤武暢

- 本講演に示されている意見は、発表者個人に属し、日本銀行の公式見解を示すものではない。

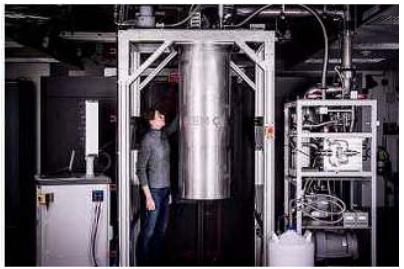
量子コンピュータとは？

■ 既存のコンピュータよりも**極めて高速な**演算処理が可能

量子コンピュータ

- **量子ゲート型**
  - ✓目的：任意の問題を解く
- 量子アニーリング型
  - ✓目的：特定の組合せ最適化問題を解く

IBM Q[1]



D-Wave2000[2]

[1] IBM News Release(2017/5/17), “IBM Builds Its Most Powerful Universal Quantum Computing Processors, 2017.
[2] D-Wave Systems inc., “The D-Wave 2000Q System,” 2016.

メリット

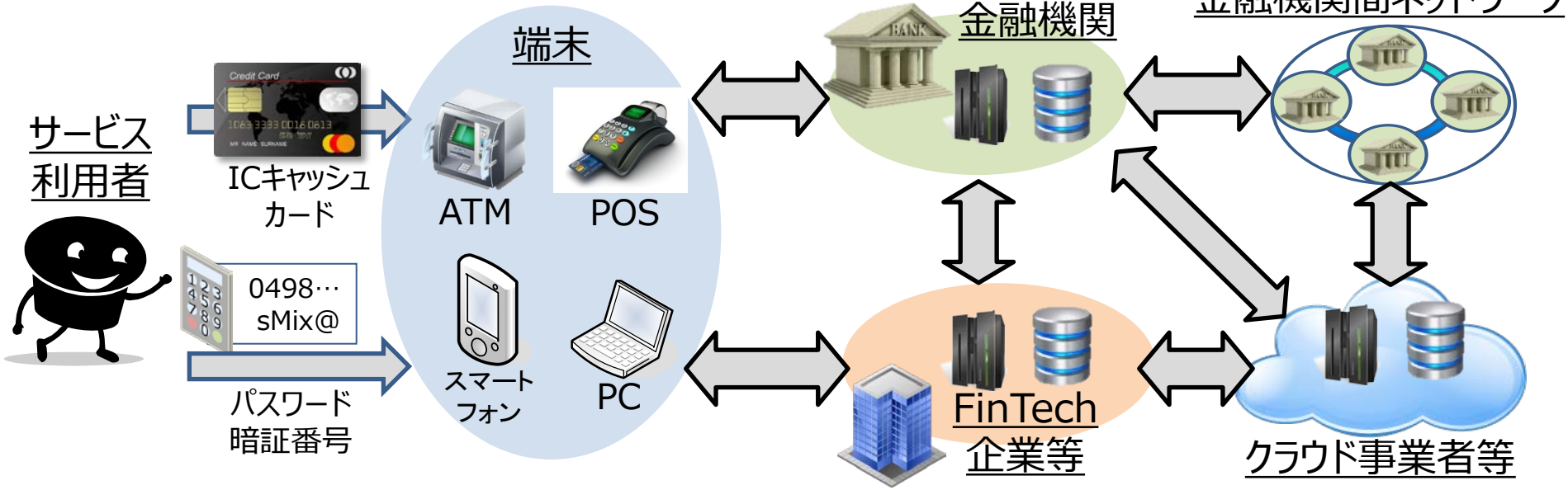
- 資産運用の最適化
- マーケット分析
- プライバシー保護を考慮したビッグデータ解析

既存のコンピュータより高い精度・効率を実現

金融サービスと暗号

■ 基礎技術として暗号が広く利用されている

暗号の主な機能	✓ データの盗聴・漏洩防止 ✓ データの改ざん検知 ✓ 他のサービス利用者や組織へのなりすまし防止



デメリット：暗号のセキュリティ低下

種類	現在主流の方式	脅威	対策
共通鍵暗号	AES	解読の手間が削減	暗号鍵の伸長（２～3倍程）
公開鍵暗号	RSA暗号 楕円曲線暗号	**数時間で解読**	**耐量子計算機暗号**への移行

金融機関は、余裕をもって検討する必要