第25回情報セキュリティ・シンポジウム

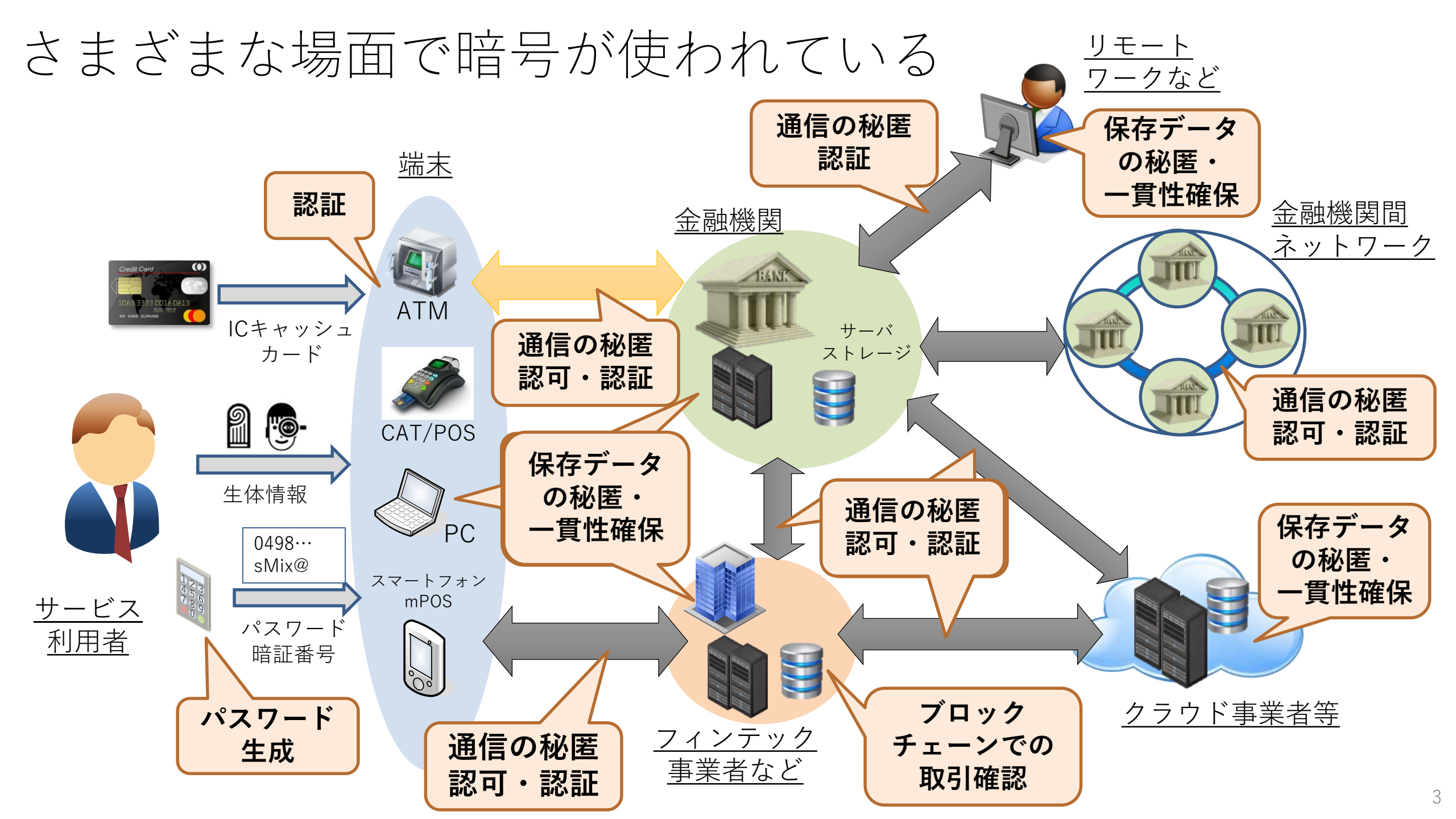
量子耐性を有するシステムの実現に向けた金融分野での取組み

2025年3月6日

日本銀行金融研究所 参事役
宇根正志

本講演における意見は講演者個人に属し、日本銀行の公式見解を示すものではありません。

さまざまな場面で暗号が使われている



暗号と量子コンピュータ

- 暗号：セキュアな金融サービスに欠かせない要素技術
  - 金融取引などにかかわる通信データの暗号化
  - 取引相手やデバイスの認証・認可
- 量子コンピュータによる暗号へのリスク
  - 量子コンピュータの研究開発の進展
  - 公開鍵暗号（RSA、楕円曲線暗号など）への影響
    - 暗号アルゴリズムの危殆化
    - 暗号化、認証、認可などが無効に

課題：量子耐性を有するシステムへの移行

リスクが顕在化する時期

- （実現するとすれば）暗号解読可能な量子コンピュータ（CRQC）の実現時期の見通しは**専門家によって区々**
- Global Risk Instituteのアンケート（2024年12月）[1]
  - 「鍵のサイズが2,048ビットのRSA暗号を1時間で解読できる量子コンピュータが**XX年後まで**に実現する可能性が5割以上」とみている有識者（32名）の割合は？
    - 15年後（2039年）まで：全体の約63%
    - 20年後（2044年）まで：全体の約91%
- BSIの調査報告（2024年8月）[2]
  - **2040年頃にCRQCが登場する可能性**を示唆

CRQC: cryptographically relevant quantum computer
BSI: Bundesamt für Sicherheit in der Informationstechnik
[1] Mosca, M., and M. Piani, “Quantum Threat Timeline Report 2024,” Global Risk Institute, 2024.
[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_1.html?nn=916616

今回の暗号移行対応の難しさ

- 対応すべき範囲：不透明
  - ➢ 対応方針や責任分担などの調整が必要な関係者も多い
  - ⇒ **対応に時間がかかる**
- 脅威が顕在化する時期：不透明
  - ➢ 暗号解読可能な量子コンピュータの実現時期が不透明
  - ⇒ **「いつまでに対応が必要か？」が未確定**
- 耐量子計算機暗号とその実装：未成熟
  - ➢ 移行対応後に脆弱性が新たにみつかるリスクに配慮
  - ⇒ **追加的なシステム対応の可能性**

早目の対応着手が大切

海外のセキュリティ当局の動き

- アメリカ
  - 2035年末までにリスクを最大限低減させる方針[1]
    - 2035年末で、既存の連邦政府標準暗号（公開鍵暗号）の使用を禁止する方針[2]
    - 耐量子計算機暗号（PQC: Post-Quantum Cryptography）の新アルゴリズムを標準化[3]
- EU
  - 欧州委員会：加盟国に対して、PQC移行のロードマップを策定する旨（2026年4月まで）を勧告[4]
  - 加盟18カ国：PQC移行に向けた検討への早期着手を推奨[5]

[1] https://irp.fas.org/offdocs/nsm/nsm-10.pdf
[2] https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf
[3] https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved
[4] https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography
[5] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.html

PQCの実装に向けた動き

- 実サービスでのPQC実装
  - ウェブブラウザ[1]
  - メッセージング・アプリ[2, 3]
  - テレビ会議[4]
- PQC実装のハードウェアの評価・認証
  - 暗号機能搭載ICのセキュリティ認証（BSI）[5, 6]
    - 枠組み：コモン・クライテリア
- セキュリティ・エレメントへのPQC組込み[7]

[1] https://blog.chromium.org/2024/05/advancing-our-amazing-bet-on-asymmetric.html
[2] https://signal.org/blog/pqxdh/
[3] https://security.apple.com/blog/imessage-pq3/
[4] https://www.zoom.com/en/blog/guide-to-post-quantum-end-to-end-encryption/
[5] https://www.infineon.com/cms/en/about-infineon/press/press-releases/2025/INFCSS202501-043.html
[6] https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/CC/SmartCards_IC_Cryptolib/1249.html?nn=520690
[7] https://globalplatform.org/moving-forward-with-confidence-preparing-for-a-phased-migration-to-post-quantum-cryptography/

金融分野における主な動き (1)

① 2022/11：ASC X9：量子コンピュータによるリスクの調査報告[1]

② 2023/3：FS-ISAC：リスク対策に関する調査報告[2]

③ 2023/6：BIS・仏中銀・独連銀：共同プロジェクト“Leap”の報告[3]

④ 2023/11：UK Finance：リスク・シナリオや対応方針に関する報告[4]

ASC X9: Accredited Standards Committee X9, Inc.
FS-ISAC: Financial Services Information Sharing and Analysis Center
[1] https://x9.org/wp-content/uploads/2022/11/X9F-Quantum-Computing-Risk-Study-Group-IR-F01-2022_20221129-Published-PDF.pdf
[2] https://www.fsisac.com/knowledge/pqc
[3] https://www.bis.org/about/bisih/topics/cyber_security/leap.htm
[4] https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/minimising-risks-quantum-technology-and-financial

金融分野における主な動き (2)

⑤ 2024/1：世界経済フォーラム：リスク対応における連携（民間部門と当局、国家間）の重要性に関する提言[5]

⑥ 2024/2：MAS：リスク対応に関する金融機関への勧告[6]

⑦ 2024/9：EMVCo：リスク対応のポジション・ステートメント[7]

⑧ 2024/9：G7 CEG：リスク対応に関する提言[8]

MAS: Monetary Authority of Singapore
CEG: Cyber Expert Group
[5] https://www3.weforum.org/docs/WEF_Quantum_Security_for_the_Financial_Sector_2024.pdf
[6] https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/mas-quantum-advisory/mas-quantum-advisory.pdf
[7] https://www.emvco.com/resources/security-position-statement-quantum-computing-and-emv-chip-cryptography-2/
[8] https://home.treasury.gov/system/files/136/G7-CYBER-EXPERT-GROUP-STATEMENT-PLANNING-OPPORTUNITIES-RISKS-QUANTUM-COMPUTING.pdf

金融分野における主な動き(3)

⑨ 2024/10：FS-ISAC：暗号アジリティの重要性と方法論のガイダンス[9]

⑩ 2024/11：「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」：PQC移行対応に関する報告[10]

⑪ 2024/11：仏中銀・MAS：共同プロジェクト（メールへのPQC実装）の報告[11]

⑫ 2025/2：QSFF：リスク対応に向けた推奨事項[12]

QSFF: Quantum Safe Financial Forum
[9] https://www.fsisac.com/knowledge/pqc
[10] https://www.fsa.go.jp/singi/pqc/houkokusyo.pdf
[11] https://www.banque-france.fr/en/press-release/banque-de-france-and-monetary-authority-Singapore-conduct-groundbreaking-post-quantum-cryptography
[12] https://www.europol.europa.eu/publications-events/publications/quantum-safe-financial-forum-call-to-action

わが国における取組み

- 預金取扱金融機関の耐量子計算機暗号への対応に関する検討会 （PQC検討会）
- 2024年7月から3回開催
- 事務局：金融庁
- 議論・検討の内容を報告書[1]としてまとめ、11月に公表

[1] https://www.fsa.go.jp/singi/pqc/houkokusyo.pdf

「経営層が認識または対処すべき事項の要点」[1]

- **経営層が果たすべき役割**
  - **リーダーシップの発揮、全社施策として対応方針の決定**
- PQCを使用可能にするタイミングの目安
  - 優先度の高いシステム：2030年代半ば
  - 海外規制動向にも留意
- 移行への事前準備
  - 暗号利用箇所やアルゴリズムの棚卸し、リスク評価、優先順位付け
  - 早目に着手することが望ましい
- ステークホルダーとの連携
  - ベンダー、金融インフラ提供事業者、フィンテック企業、政府など

[1] https://www.fsa.go.jp/singi/pqc/houkokusyo.pdf

今後生じうる情勢の変化

- 量子コンピュータの開発進捗が前倒し？
- より強力な解読アルゴリズムの提案？
- 海外の規制が変更？
- PQCのソフトウェアやハードウェアに脆弱性？

検討項目

- PQC移行のための体制整備
  - ⇒　情報収集、ステークホルダー調整、啓発
  - ⇒　事前準備（暗号インベントリ整備、リスク評価）
  - ⇒　金融業界内、重要インフラ事業者間での連携体制
- PQC移行のためのロードマップづくり
  - ⇒　業界向け、個別金融機関向け
  - ⇒　課題の洗出しとステークホルダーへの働きかけ
- 長期的な視点からのシステム対応
  - ⇒　柔軟かつ効率的な暗号対応が可能なアーキテクチャ

おわりに

- 欧米では、業界団体やコミュニティによる検討や提言が活発化
- わが国の金融業界も、金融庁・PQC検討会の成果物などを活用。検討の活発化を期待
  - 金融ISACにおける検討
- 暗号アルゴリズムの経年劣化やリスク対応は今後も続く。こうした変化を想定したシステム・アーキテクチャやエコシステムを目指すべき

関連する内容はこちら（↓）

宇根正志、「量子耐性を有するシステムの実現に向けて：
金融分野における取組みと対応の推奨事項」、
金融研究所ディスカッションペーパー No. 2025-J-1、
日本銀行金融研究所、2025年2月

https://www.imes.boj.or.jp/research/abstracts/japanese/25-J-01.html