CRYPTRECシンポジウム2026
2026年7月31日

金融分野における耐量子計算機暗号への移行：これまでの取組みと課題

日本銀行金融研究所 参事役
宇根　正志

本発表における意見や解釈は、発表者個人に属し、日本銀行の公式見解を示すものではありません。

自己紹介

- 1971　広島県福山市生まれ
- 1994　筑波大学 社会工学類 卒、日本銀行入行（調査統計局）
- **1996　金融研究所（暗号の調査研究を担当）**
- 2003　横浜国立大学大学院 博士課程後期修了　博士（工学）
- 2006～2007　産業技術総合研究所 情報セキュリティ研究センター 招聘研究員
- 2010～2015　システム情報局（日銀のシステムの開発・管理、セキュリティ対策など）
- 2015～　金融研究所

- **2009, 2015～2021　暗号技術検討会 構成員**
- 2024　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 メンバー（金融庁）
- 2025～　一橋大学 非常勤講師

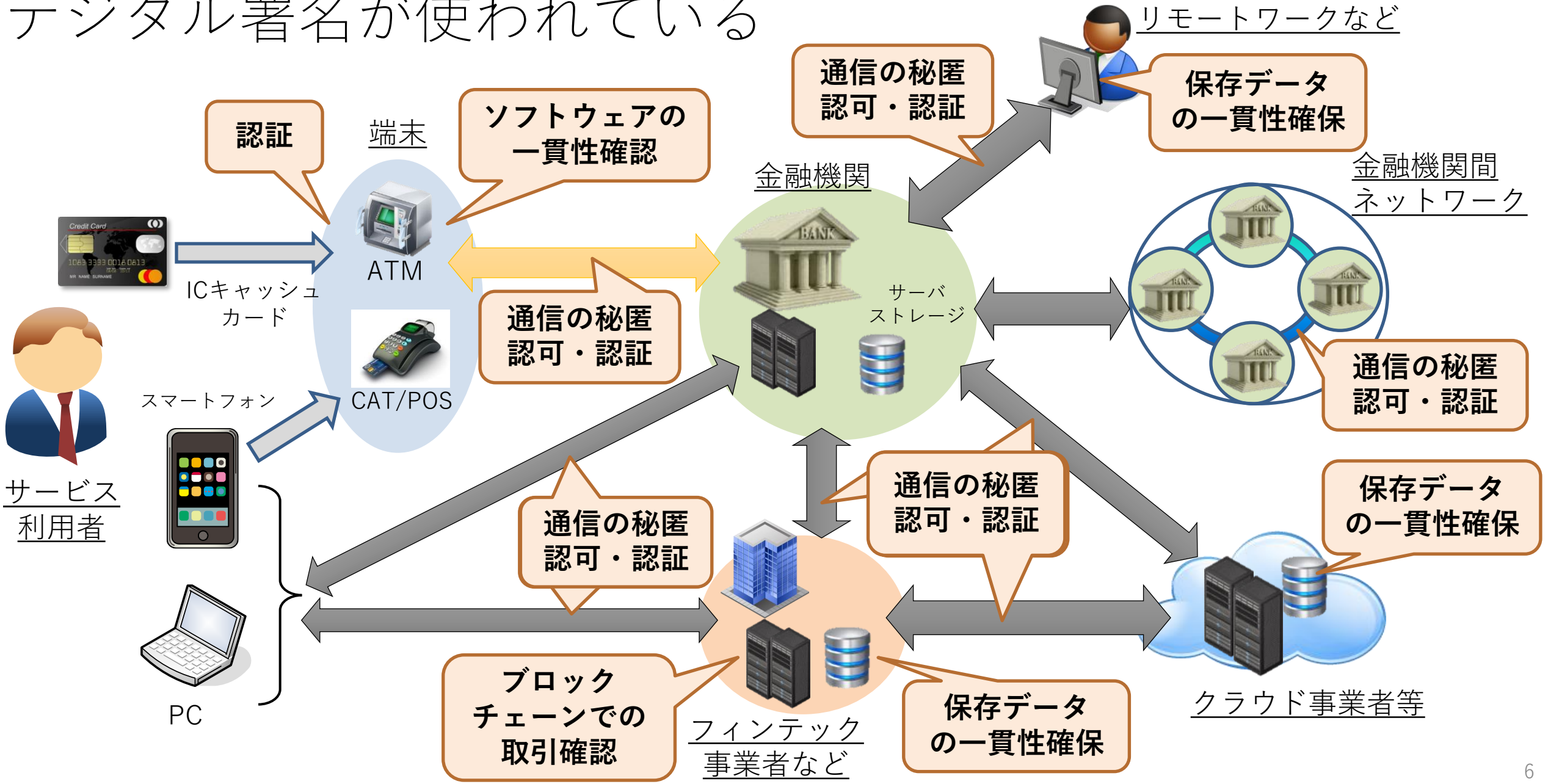
- 暗号、生体認証、AIセキュリティ、オープンAPI、暗号資産・ブロックチェーンなど
- 「AI・量子コンピュータにかかわるリスク管理」オーム社、2025年（坂本静生さんと共著）

アジェンダ

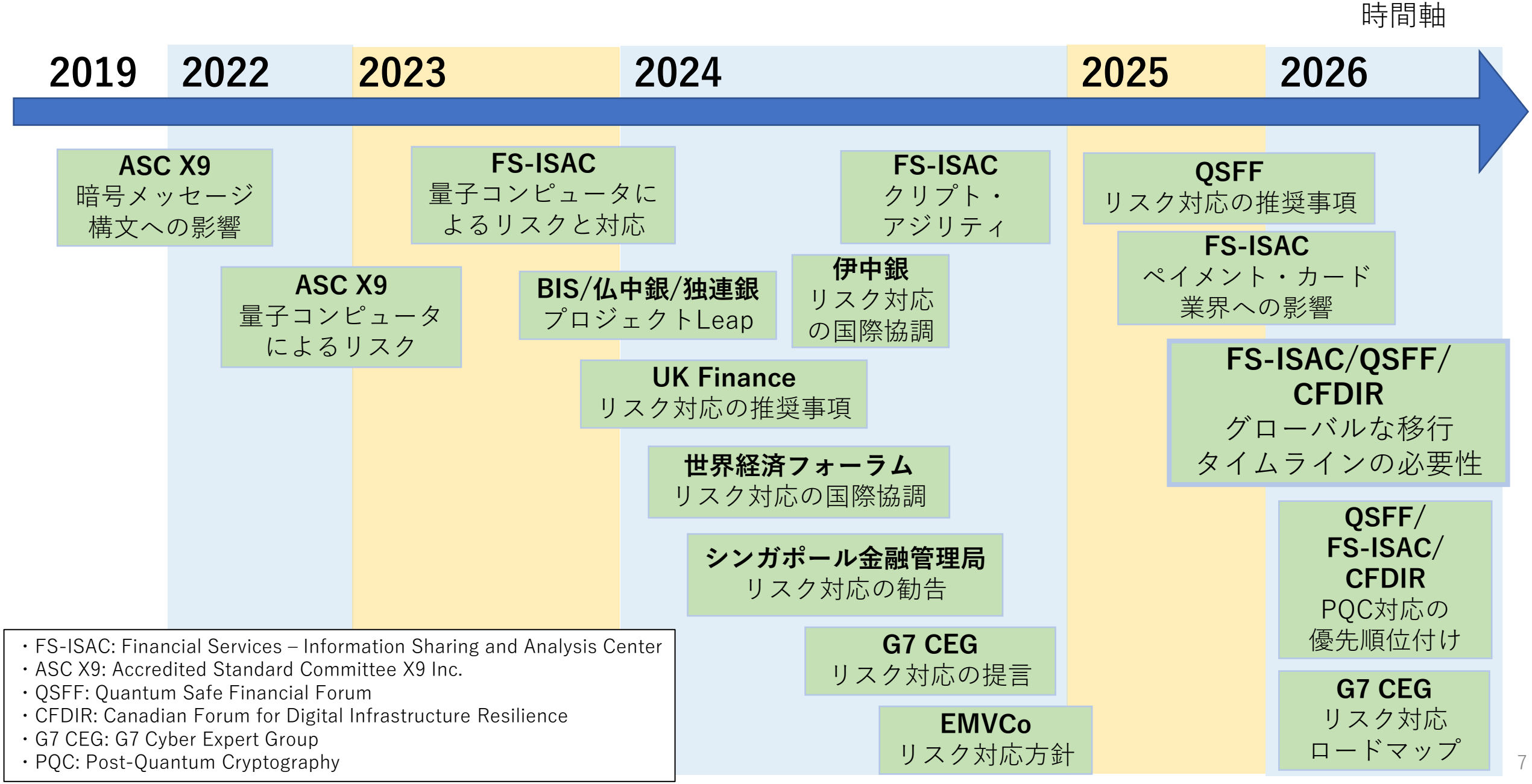
1. 海外金融業界における議論・検討
2. わが国の金融業界における検討
3. 今後の課題と期待

１．海外金融業界における議論・検討

さまざまな場面で公開鍵暗号・デジタル署名が使われている



2010年代後半から議論・検討が開始された



- FS-ISAC: Financial Services – Information Sharing and Analysis Center
- ASC X9: Accredited Standard Committee X9 Inc.
- QSFF: Quantum Safe Financial Forum
- CFDIR: Canadian Forum for Digital Infrastructure Resilience
- G7 CEG: G7 Cyber Expert Group
- PQC: Post-Quantum Cryptography

提言・ガイダンスの主なポイント

- **業界としての取組み**を重視（UK Finance）
- **グローバルな相互運用性、国際協調**を重視
  （世界経済フォーラムほか）
- **既存暗号とPQCのハイブリッド**を推奨（ASC X9ほか）
- **クリプト・アジリティ**を重視（FS ISACほか）
- **長期的な計画と対応**を重視（FS ISACほか）

FS-ISAC/QSFF/CFDIRのポジションペーパー
“The Timeline for Post-Quantum Cryptographic Migration”（2025年9月）

- 参加者が所属する金融機関・団体
  - Banco Santander, CIBC, Wells Fargo, European Investment Bank, TD Bank, Dutch Banking Association, National Bank of Canada, Allianz SE, Bank of Montreal, Scotiabank, Bank of Spain, Mizuho Americas
- **PQC対応の難しさ（時間がかかる）**を再認識すべき
  - 金融サービスの複雑な依存関係がハードルに
- **グローバルな移行タイムラインの策定**が重要
- **ステークホルダー**との調整が必須
  - 金融サービスを提供する事業者・団体、ベンダー、標準化機関、当局

・https://www.fsisac.com/the-timeline-for-post-quantum-cryptographic-migration

マスターカードの調査研究レポート

“Migration to Post-Quantum Cryptography” （2025年10月）

- 著者：
  - マスターカード、シンガポール南洋理工大学、PQStation のスタッフ
- **Quantum Key Distribution：広く展開・使用するには高価**
  - PQCにアド・オンして使用
  - 特に高いセキュリティが必要なケースでの補完的手段
- **ペイメントカードへのPQC実装（署名）**に課題
  - 処理時間・メモリの制約
  - 共通鍵暗号の活用も視野に
- TLSにおける鍵共有では**ハイブリッド**で実装
  - 楕円曲線暗号とML-KEMの組合せ

・https://www.mastercard.com/global/en/news-and-trends/Insights/2025/post-quantum-cryptography-white-paper.html

Citiの調査研究レポート

“Quantum Threat: The Trillion-Dollar Security Race Is On”（2026年1月）[1]

- 著者：Citiの研究スタッフ
- **政府の規制を強く受ける業界：PQCへの移行はオプションではなく必須**
  - 規制当局はPQC移行の計画策定・リスク管理を強力に推進
  - 量子計算技術：科学研究上の話題から、経営課題へ
- **機密情報が流出した場合の被害は非常に大きい**
  - サイバー攻撃による被害額（2025年）は平均で数百万ドルに達するとの試算[2]も
- **金融機関に求められる対応**
  - 新システム開発時に、可能であれば、PQCを採用
  - クリプト・アジリティの機能を実装
  - PQCを実装済みのクラウドサービスの活用も視野に
  - カスタマイズして使用継続してきたレガシーシステムの見直し

1) https://www.citigroup.com/rcs/citigpa/storage/public/Citi_Institute_Quantum_Threat.pdf
2) https://www.ibm.com/reports/data-breach

G7 Cyber Expert Groupのステートメント

“Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector” （2026年1月）

- **PQCへの移行などの実現に向けた協調的なアプローチを後押し**
- **想定されるタイムライン**
  - 各国政府、標準化団体のガイダンス：**2035年が目標**
  - 最重要のシステム：2030～2032年を移行時期の目標に設定することも
- **協調のためのハイレベルな（幅のある）ロードマップ**
  - 準備（～2027年）
  - インベントリ（～2028年）
  - リスク評価・計画（～2029年）
  - 移行実施（～2034年）
  - 移行検証、モニタリング（～2035年）

  ⇒　金融機関がリスクに応じて対応の優先順位をそれぞれ決定

・https://home.treasury.gov/system/files/136/G7-CEG-Quantum-Roadmap.pdf

２．わが国の金融業界における検討

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

- 2024年7月～11月に実施（事務局：金融庁）
- **経営層が認識または対処すべき事項の要点**
  - 経営層が果たすべき役割：リーダーシップ、全社施策としての対応
  - 対応時期の目安：優先度の高いシステムは2030年代半ば
  - 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
  - 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
- 後続の検討：金融ISACによる**ロードマップひな形**の検討

・ https://www.fsa.go.jp/singi/pqc/houkokusyo.pdf

金融ISACにおける検討

- **本邦金融機関向けのPQCへの移行のガイダンスの作成**
  - 海外の金融当局や金融機関の対応に関する情報収集
  - システムインテグレータ、クラウドベンダーなどへのヒアリング
  - 関連業界団体への問題意識の共有や情報共有
  - 国内金融機関の対応状況のフォロー　など

  ⇒　個々の金融機関が対応するよりも業界として効率的に検討を推進
- PQC移行ロードマップ例
  - 優先度の高いシステムの移行：2030年代前半の早い時期を完了目標に
- 移行における主なタスク
  - 推進体制の整備、予算確保
  - 移行対象の範囲と優先順位
  - 移行フレームワークの策定
  - 各システムの移行計画の立案・推進

各システムの移行計画における主なポイント

- PQCとして採用するアルゴリズム・パラメータ
  - NIST、IETFなどで標準化されたものを推奨
- PQCの実装方法：PQ/T Compositeのハイブリッド
- クリプト・アジリティ確保のための対応
- 電子証明書の一元管理に向けた対応
- ソフトウェアやハードウェアの選定
- PQC移行によるシステムやサービスへの影響の見極め
- ユースケースごとの考慮点
  - 暗号化、署名・認証
  - オンプレミス、クラウド
  - FMI（Financial Market Infrastructure）
- ステークホルダーと責任範囲
- 移行計画のガバナンス

３．今後の課題と期待

移行ガイダンスに沿った対応に期待。
だが、課題は山積

- 効率的な情報収集
- 「情報収集」から「具体的なアクション」への後押し
- 移行検討のためのリソースの確保
- 個人の顧客や取引先への説明
- 金融業界として歩調を揃えた対応　など

ステークホルダーとの連携が必須

ステークホルダーとの連携

- ハードウェア／ソフトウェア提供者
- システム開発ベンダー、インテグレーター
- クラウドサービス事業者
- 認証局事業者
- 決済ネットワーク運営者（業界内、対顧客）
- 共同システム運営者
- API接続先（フィンテック事業者など）
- 重要インフラ事業者　など

ステークホルダーへの期待

- 技術やサービスの動向に関する情報の提供
  - 標準化動向（特に署名、証明書関連）
  - 製品／ソリューション、（インベントリ向けの）各種ツール、移行支援のサービス
  - 先行事例、教訓　など
- PQC移行に向けたサービスや体制の拡充
- 各ステークホルダーにおける取組み状況の共有
  - 電力・水道・交通・ICTなどの重要インフラでの対応も

CRYPTRECへの期待

- CRYPTREC暗号リストにおけるPQCアルゴリズムの早期拡充
  - 署名アルゴリズムの追加　など
- クリプト・アジリティ実現のための方法論やそのガイダンスの作成
  - 具体的な事例・ソリューションの紹介も

政府への期待

- 国全体としてPQC移行を効率的に進めるうえで、海外の動向、国内での取組み状況、参考になるガイダンスなどの情報をタイムリーに集約し、分野横断的に発信する役割が必要
- 情報の集約・流通の体制整備

End of Talk