金融庁
Financial Services Agency

資料７－１

金融分野におけるサイバーセキュリティに関する取組状況

2025年6月

金融庁総合政策局リスク分析総括課
ITサイバー・経済安全保障監理官室

耐量子計算機暗号（PQC）への移行対応

経緯	• 実用的な量子コンピュータ（量子計算機）の実現と普及は、**社会に恩恵をもたらす一方で、攻撃者が、量子コンピュータを既存の暗号化技術の解読（危殆化）のために使用するおそれ** • 耐量子計算機暗号（PQC：Post-Quantum Cryptography）への移行に向けた早期の準備が必要
概要	金融庁において、2024年7月から10月にかけて、「**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**」を開催（計3回）
目的	金融機関においてPQCへの移行を検討する際の**推奨事項、課題及び留意事項**について、**幅広い関係者と議論**を深めるため
参加者	預金取扱金融機関に係る**各業界団体の代表者や有識者**が参加 構成メンバー：3メガバンク、全銀協、地銀協、第二地銀協、全信協、全信中協、労金協、農林中金、日銀金融研究所、日本ネットワークセキュリティ協会の代表者 オブザーバー：金融ISAC、CRYPTREC事務局、FISC、日銀金融機構局、NISC
成果物（報告書）	• 金融機関の**経営層がリスクを正しく認識し、リスク低減策を適切に推進**できるようにすることを目的として、本検討会の議論を踏まえた**報告書を公表**（2024年11月） • 預金取扱金融機関のみならず、あらゆる業態の金融機関に参考となる

PQC検討会による報告書の主要メッセージ

量子コンピュータの実用化によって現在の暗号技術が破られることになれば、インターネットバンキングをはじめとする金融情報システムの安全性が根底から覆される。すべての金融機関は顧客や自身の情報・財産を守るため、規模・特性にかかわらず、直ちに耐量子計算機暗号（PQC）への移行に着手しなければならない

報告書の主要メッセージ

① 金融機関はまず、自らの情報資産を網羅的に把握した上で、それぞれの情報資産の重要性を評価し、どのような暗号が用いられているかをリスト化したインベントリー（台帳・目録）を作成すること

② その際、自らが運用するシステムだけではなく、サードパーティーに運用を委託している重要システムの情報資産と暗号に関するインベントリーも作成すること

③ インベントリーの作成作業にはかなりの労力を要するので、早い段階からITベンダーの協力を得ること

④ インベントリーに基づき、量子コンピューターが実現すると脆弱性にさらされる情報資産のうち、影響が大きいシステムから順にPQCへの移行を進めること

⑤ 検討の開始から移行までの一連の作業に関して、ロードマップを作成すること

⑥ 実務的には大規模システム更改などに合わせてPQCへの移行を進めることを踏まえると、量子コンピューターの実用化（2030年代半ば）までに残された時間は少ないため、速やかに移行への対応を開始すること

⑦ PQC自体も脆弱性が明らかとなる恐れがあるため、特定の暗号に固定することを前提とするのではなく、それが脆弱になった場合に暗号を差し替えやすいシステムにしておく、いわゆるクリプト・アジリティーを確保しておくこと

⑧ 移行には長い期間と多くの経営資源の投入が必要であるため、経営陣の強いコミットメントが求められること