金融分野における耐量子計算機暗号の導入に関する動向

宇根 正志 [1,*]

概要：大規模かつ実用的な量子コンピュータが実現した場合，それを用いていくつかの主要な公開鍵暗号のアルゴリズム（RSA 暗号や楕円曲線暗号）を効率的に解読することができるとみられている．こうした暗号解読による将来のリスクに備えるために，耐量子計算機暗号の導入に関する検討が金融分野において活発に行われている．例えば，イギリスの UK Finance Limited は，2023 年 11 月，量子コンピュータによるリスクを類型化するとともに，リスク軽減の方針や主なタスクを示した．2024 年 1 月には，世界経済フォーラムが，リスク対応に際してグローバルな連携・調和の重要性を提言した．シンガポール金融管理局は，2024 年 2 月，耐量子計算機暗号の導入を促す勧告を金融機関に対して行った．2024 年 10 月には，FS-ISAC が暗号アジリティに関する指針を発表した．わが国では，2024 年 11 月，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（事務局：金融庁）の報告書が発表され，耐量子計算機暗号を導入する際の推奨事項や課題が示された．本稿では，こうした金融分野における耐量子計算機暗号の導入に向けた最近の検討状況を紹介する．

キーワード：暗号アジリティ，公開鍵暗号アルゴリズム，耐量子計算機暗号，リスク，量子コンピュータ

Recent Discussion on the Implementation of Post-Quantum Cryptography in the Financial Sector

Masashi Une[1,*]

Abstract: It is believed that, if a large-scale and practical quantum computer were realized, several conventional public-key cryptographic algorithms, e.g., RSA and elliptic-curve cryptography, would be compromised. In order to prepare the mitigation of an IT system risk posed by the vulnerable algorithms in the future, the implementation of the post-quantum cryptography has been actively discussed in the financial sector. For example, in November 2023, UK Finance Limited released a paper that classified risk scenarios caused by the quantum computer and proposed principles and tasks for addressing them. In January 2024, World Economic Forum published a white paper that emphasized the importance of the global harmonization and collaboration in addressing the risk. In February 2024, Monetary Authority of Singapore released the advisory on the implementation of the post-quantum cryptography to the financial institutions. In October 2024, FS-ISAC published a guidance paper on the improvement of the cryptographic agility. In Japan, a working group on the post-quantum cryptography in depository institutions, hosed by Financial Services Agency, published a report that clarified recommendations and future challenges on the implementation in November 2024. This paper will show recent discussion on the implementation of the post-quantum cryptography in the financial sector.

Keywords: Cryptographic Agility, Post-Quantum Cryptography, Public-Key Cryptography, Quantum Computer, Risk

1. はじめに

暗号は，金融サービスや金融業務のセキュリティを確保する重要な要素技術として普及している．例えば，ATM における IC キャッシュカードの認証，インターネット・バンキングやモバイル・バンキングにおける通信データの暗号化や認証，金融機関間や金融機関とフィンテック事業者との間の通信データの暗号化や認証が挙げられる．また，出張中や在宅勤務中の職員の端末と金融機関のシステムとの間の通信データを保護する手段としても暗号が利用されている．業務でクラウドを使用している場合も，クラウドと金融機関の端末・サーバとの間の通信データや，クラウドのデータを保護する手段として暗号が採用されている．

データの暗号化や認証において用いられている公開鍵暗号の代表的なアルゴリズム（RSA[a]や楕円曲線暗号）には量子コンピュータによって解読されるリスクがある[1]．暗号解読可能な量子コンピュータ（CRQC: cryptographically relevant quantum computer）が実現するタイミングは明確でないものの，仮に，攻撃者が CRQC を使用することができるようになれば，金融取引や顧客に関する情報（暗号化されていたもの）が盗取されたり，金融機関のシステムにアクセスする際の認証が破られて不正な処理が実行されたりする可能性がある．こうしたリスクが許容できないシステムでは，量子コンピュータでも解読困難な暗号アルゴリズムに切り替えるなどのリスク軽減策を適用する必要がある．

CRQC によるリスクに関して，海外の政府機関では，リスクの評価や対策に関するガイダンスを発表する動きがみられる[2]．例えば，アメリカでは，2035 年を目途に量子コ

1 日本銀行金融研究所
Institute for Monetary and Economic Studies, Bank of Japan
* masashi.une@boj.or.jp

a) RSA は RSA Security LLC.の登録商標である．

ンピュータによるリスクを可能な限り軽減する方針が2022年5月に国家安全保障覚書[b]によって表明され，次世代の暗号アルゴリズムとして「耐量子計算機暗号」（PQC: post-quantum cryptography）の標準化，脆弱化する暗号アルゴリズムの使用停止の検討などが進められている．欧州では，PQCを導入するためのロードマップの策定が欧州委員会において2024年4月に勧告され，2025年6月にロードマップ[c]が公開されている．このロードマップをみると，概ね2035年末までにPQCの導入を完了する見通しとなっている．

わが国では，サイバーセキュリティ戦略本部（事務局：国家サイバー統括室）の第43回会合（2025年5月開催）において，「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」の1つとして，政府機関等におけるPQC移行の方向性について次期サイバーセキュリティ戦略に盛り込むことが決定されている[d]．今後，PQC移行の方針が検討される見通しとなっている．

金融分野においても，海外の金融関連の団体や当局を中心にリスク対応に関する検討が活発化しており，提言や指針が発表されている[3]．わが国では，2024年11月，「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」（事務局：金融庁）から報告書が公表され，PQC導入に向けた課題が示されている[e]．

金融機関においては，こうした動向をタイムリーにフォローしつつ，CRQCによる暗号へのリスクに適切に対処していくことが求められている．

本稿では，金融関連の団体や当局による主な提言や指針を紹介する．なお，本稿の意見や内容は筆者本人に属し，日本銀行の公式見解を示すものではないことを予め断っておく．

2. 金融分野における主な提言・指針

PQC導入に関して大きな契機となっているのが，アメリカ国立標準技術研究所（NIST: National Institute of Standards and Technology）によるPQCの標準化プロジェクトである．NISTは，アメリカの連邦政府が調達するPQCのアルゴリズムを選定・標準化する役割を担っており，標準化の候補となったアルゴリズムの標準規格（3件）の草案を2023年8月に発表した．このタイミング以降，CRQCによる暗号へのリスクに関して金融分野において検討が活発化した．2023年8月以降の主な提言・指針を列挙すると以下のとおりである．

① 2023年11月：UK Finance Limitedが提言ペーパー“Minimising the Risks: Quantum Technology and Financial Services”を発表[f].
② 2024年1月：世界経済フォーラム（World Economic Forum）が提言ペーパー“Quantum Security for the Financial Sector: Informing Global Regulatory Approaches”を発表[g].
③ 2024年2月：シンガポール金融管理局（Monetary Authority of Singapore）が金融機関向けの勧告“Advisory on Addressing the Cybersecurity Risks Associated with Quantum”を発表[h].
④ 2024年9月：G7サイバー・エキスパート・グループ（Cyber Expert Group）が提言ペーパー“Planning for the Opportunities and Risks of Quantum Computing”を発表[i].
⑤ 2024年10月：FS-ISACが暗号アジリティ（暗号アルゴリズムの切替えへの対応能力）の向上に関する指針ペーパー“Building Cryptographic Agility in the Financial Sector”を発表[j].
⑥ 2024年11月：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が，PQC導入を検討する際の推奨事項・課題・留意点を取りまとめた報告書を発表．
⑦ 2025年7月：国際決済銀行のスタッフらがPQC移行のロードマップの提案ペーパー“Quantum-Readiness for the Financial System: A Roadmap”を発表[k].

以下では，これらの提言や指針の概要を紹介する．

2.1 UK Finance Limitedの提言

UK Finance Limitedは，イギリスにおける金融機関間の連携の支援，金融サービスに関連する各種の規制や業界内の取決めの立案，政府を含むステークホルダーとの調整などの役割を担っている業界団体である．2023年11月に，CRQCによるリスクへの対応に関する提言ペーパーを公表した．

2.1.1 主なリスク・シナリオ

提言では，CRQCによる主なリスク・シナリオを以下のとおり列挙している．

b) https://irp.fas.org/offdocs/nsm/nsm-10.pdf
c) https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
d) https://www.nisc.go.jp/pdf/policy/kihon-s/250529kikkin.pdf
e) https://www.fsa.go.jp/singi/pqc/houkokusyo.pdf
f) https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/minimising-risks-quantum-technology-and-financial
g) https://www3.weforum.org/docs/WEF_Quantum_Security_for_the_Financial_Sector_2024.pdf
h) https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/mas-quantum-advisory/mas-quantum-advisory.pdf
i) https://home.treasury.gov/system/files/136/G7-CYBER-EXPERT-GROUP-STATEMENT-PLANNING-OPPORTUNITIES-RISKS-QUANTUM-COMPUTING.pdf
j) https://www.fsisac.com/knowledge/pqc
k) https://www.bis.org/publ/bppdf/bispap158.pdf

- 金融機関が管理している個人情報（personally identifiable information）が盗取される．
- ホールセール決済のシステムにおいて認証が破られ，なりすましによる不正送金が行われる．
- 金融機関が公開している API（application programming interface）における認証・認可プロトコルが不正に操作され，なりすましによる不正な金融取引が発生する．
- ブロックチェーンにおける初期ブロック（genesis block）が偽造され，それ以降のすべてのブロックの内容が信頼できないものとなる．
- 金融サービス向けのシステムやインフラの管理者権限が奪取され，システムが不正に操作される．
- リテール決済のシステムにおける認証が署名偽造などによって無効化され，不正な取引が実行される．
- ソフトウェアやファームウェアに付与される署名（コード署名）が偽造され，不正なソフトウェアがシステムに組み込まれて不正な動作を誘発する．
- 金融機関内部で管理されている各種データベースが改変される．
- 金融取引において参照される公的なデータベース（登記簿のデータベースなど）のデータが改変される．

2.1.2 リスク対応の方針や主なタスク

上記のリスクに対処するための方針として，提言では，業界横断的なタスクフォースをまず設置し，業界全体としての移行計画（quantum safe transition plan）を策定した後，それに基づいて各金融機関が自社の移行計画を策定するという対応が効率的であり望ましいとしている．タスクフォースにおける主なタスクとして以下を挙げている．

- タスクフォース内で知見を共有し，PQC の使用に関するガイドラインなどを策定する．
- 学会や研究機関と連携して量子計算技術（quantum computing）の動向をフォローするとともに，関連する技術のスキルをもつ金融機関スタッフを育成する．
- 政策立案者や当局と連携し，量子計算技術の適切な活用を促進しつつリスク軽減に資する政策や規制のフレームワークを検討する．

2.2 世界経済フォーラムの提言

世界経済フォーラムはスイスに本部を置く国際的な非営利団体であり，社会の発展を目指して，政治・産業・学術などの各界のリーダーや有識者が連携・協力するための枠組みを提供している．同フォーラム主催の国際会議における講演や議論，有識者へのインタビューの内容に基づき，CRQC によるリスク対応に関する提言ペーパーを 2024 年 1 月に公表した．

2.2.1 現状認識

提言では，現状に関して，各国政府におけるリスク対応方針の調和がとれていないとの認識を示している．そのうえで，グローバルにビジネスを展開している金融機関からみると，各国のリスク対応方針に沿った複雑な対応を強いられる可能性があるとの見方を示している．

また，提言では，金融機関のシステムが相互に接続されており，金融機関のネットワークのセキュリティは最も脆弱なポイントに依存しうるとしたうえで，相互に接続している金融機関全体が適切に対応する必要があるとしている．さらに，政府のリスク対応方針に不備があれば，ベンダーの対応（PQC を導入する暗号ソリューションの提供など）が遅れ，最終的には，金融機関による PQC 導入の遅れにつながる可能性があるとの見方を示している．

2.2.2 リスク対応における原則

提言では，金融当局と金融機関が連携し，以下の原則に沿ってリスク対応を進めることが有用であるとしている．

- 既存の手段や枠組みの活用（reuse and repurpose）：リスクに対処するうえで，既存の技術やベスト・プラクティスなどを活用することをまず検討する．
- 交渉不要な要求事項の設定（establish non-negotiables）：リスク対応の要求事項として，例えば，既存のベスト・プラクティスや国際標準仕様など，既に合意が得られているものを明確にしておく．
- 情報の開示と共有の促進（increase transparency）：ステークホルダー間でリスク対応の戦略やベスト・プラクティス，その他の関連する情報を可能な限り共有する．
- 分断の回避（avoid fragmentation）：リスク対応に関連する規制に関して各国や地域の金融当局間で連携・調整し，国や地域によって規制が異なる状況をなるべく回避する．

2.2.3 リスク対応のロードマップ

提言では，リスク対応の手順として，①準備（prepare），②明確化（clarify），③ガイド（guide），④移行・監視（transition and monitor）というロードマップを示している．

① 準備：リスクに関するステークホルダーの認識レベルの向上，スタッフの啓発・スキルアップ，暗号の使用状況の把握，リスク評価，対応の優先順位付けなどを行う．
② 明確化：ステークホルダー間の連携・協力体制の確立，必要な作業・コスト・期間などの明確化，既存の規制の再評価などを行う．
③ ガイド：リスク対応に関する戦略の検討，必要な規制やベスト・プラクティスの策定などを行う．

④ 移行・監視：リスク対応に関する作業の実行，暗号の管理方法やシステムの開発プロセスの見直し（暗号アルゴリズムを円滑に変更する仕組みの検討など），脅威やリスクの監視などを行う．

2.3 シンガポール金融管理局の勧告

シンガポールにおける金融当局であるシンガポール金融管理局は，2024 年 2 月，金融機関に対して，CRQC によるリスクへの対応として PQC 導入の検討を促す勧告を行った．具体的には，リスク対応に関連する作業として，技術動向の把握とリスクの啓発，暗号インベントリ（暗号の使用状況に関する情報を管理する仕組み）と対応の優先順位付け，リスク対応の戦略の立案と遂行能力の向上を挙げている．

2.3.1 技術動向の把握とリスクの啓発

技術動向の把握とリスクの啓発に関して，以下のタスクを挙げている．

- 量子コンピュータの開発状況やリスクを監視する．
- 経営層や取引先ベンダーに対して，CRQC の潜在的な脅威や対策を説明し理解を得る．
- ベンダーと協力して CRQC によるサプライチェーン・リスクを評価するとともに，PQC を実装した暗号製品などの提供を依頼する．
- 依存関係にある他の産業分野と連携し，他の産業分野で発生しうるインシデントが金融分野に及ぼす影響やリスク（systemic quantum risk）を洗い出すとともに，リスク軽減策を検討する．

2.3.2 暗号インベントリと対応の優先順位付け

暗号インベントリと対応の優先順位付けとして，以下のタスクを挙げている．

- 暗号インベントリを整備・管理し，リスクが存在するシステムやインフラを特定する．暗号インベントリには，①使用中の暗号アルゴリズムの名称・鍵サイズ，②暗号アルゴリズムが組み込まれているシステムやアプリケーションの名称，③暗号アルゴリズムによって保護されている情報，④各情報の管理責任者の名称などを保持することが望ましい．
- CRQC に対して脆弱な暗号アルゴリズムが使用されているシステムやデータを特定・分類する．
- リスク対応の優先順位付けを行う．優先順位は，データの機密度・重要度・保護期間・リスクの大きさなどを考慮して決定することが望ましい．
- システムやインフラにおける暗号アジリティを評価する．PQC の導入を妨げる要素（計算処理能力の限界，インフラの仕様，ベンダーのサポート切れなど）を特定し，改善を検討する．

2.3.3 戦略の立案と遂行能力の向上

リスク対応に関する戦略の立案と遂行能力の向上に関して，以下のタスクを挙げている．

- リスク対応に携わるスタッフに対して，量子計算技術や暗号技術などの必要なスキルを身につけさせる．
- リスク対応の内容を，金融機関内部のポリシー，技術標準，各種手続きに反映させる．
- PQC 導入が困難なシステムやインフラがあれば，それに対するリスク軽減の戦略を立案する．
- 想定したタイムラインよりも早期にリスクが顕在化した場合を想定し，対処方法やシナリオを立案する．
- 可能であれば，量子耐性を有するシステムの概念実験（proof-of-concept trial）を行い，それを導入した際の業務への影響を評価する．

2.4 G7 サイバー・エキスパート・グループによる提言

G7 サイバー・エキスパート・グループは，G7 各国のサイバーセキュリティに関する対応方針や戦略の調整，情報の共有，インシデント対応などを担当する G7 のワーキング・グループである．2024 年 9 月，G7 各国の財務大臣と中央銀行総裁に向けて，CRQC による暗号へのリスクと対応に関して提言を公表した．

2.4.1 検討の早期着手の推奨

提言では，将来 CRQC が悪用された場合，既存の暗号アルゴリズムによって保護されていた情報が解読される可能性があるとしている．その結果，金融機関が管理しているデータが盗取され，関係する組織のレピュテーションや顧客のプライバシーが損なわれるおそれがあるとの見方を示している．特に，長期間秘密に管理しておく必要があるデータに関しては，CRQC が実現する前から（既存の暗号アルゴリズムによって暗号化されている）暗号化データを収集・保存しておき，CRQC が実現した後に一気に解読するという攻撃（HNDL: Harvest Now, Decrypt Later）に留意する必要があるとしている．

また，提言では，金融分野の関係者（当局も含む）の間でリスクへの対処方法を検討・調整するためには相当の時間と経済的負担が必要となりうるとの見通しを示したうえで，関係者による準備をできるだけ早期に整えることを推奨している．

2.4.2 リスク対応の 3 つのステップ

提言では，金融機関におけるリスク対応のステップとして次の 3 つを挙げている．

① リスクと対処方法に関する理解深耕：ベンダーや専門家の協力を得ながら，量子コンピュータ，暗号へのリスク，対策技術について理解を深める．量子コンピュータの開発スケジュール，脅威となる事象，今後有望とみられる対策技術やアプローチについてもフォローすることが望ましい．

② リスク評価：暗号インベントリを整備するとともに，リスク対応に必要なリソースを見積もるために，自組織に関係するリスクを適切に評価する．

③ リスク軽減計画の立案：リスクを把握・管理するプロセスの検討，主なステークホルダーとその責任範囲の明確化，リスク対応の優先順位付けなどを行い，検討結果を盛り込んだリスク軽減計画（a plan for mitigating quantum technology risks）を立案する．

このほか，金融当局に対して，金融機関と協力し，CRQCによる攻撃への対策に資する技術（quantum resilient technologies）の重要性を広く情宣することも推奨している．

2.5 FS-ISACによる暗号アジリティに関する指針

FS-ISACは，金融機関におけるサイバーセキュリティや各種インシデントへの対応力の向上を目的として，関連する情報を金融機関間で共有する枠組みなどを提供する国際的な非営利団体である．FS-ISACは，2024年10月，暗号アジリティの重要性や導入に関する指針を公表した．

指針は2部構成となっており，第1部では，経営層に向けて暗号アジリティとその重要性，暗号アジリティを向上させるプロセスなどを説明している．第2部では，実務者や技術者向けに暗号アジリティに関連する技術的な検討課題や留意点を説明している．

2.5.1 暗号アジリティとは

指針では，暗号アジリティを次のとおり定義している．

暗号解読手法の向上，新しい脅威の出現，技術革新，脆弱性の発見などに応じて，迅速かつ効率的に，暗号アルゴリズム（パラメータや鍵を含む）や暗号ソリューションを適応させる組織の能力の度合い（a measure of an organization's ability）

このように，暗号アジリティを，暗号アルゴリズムの切替えの実現可能性という技術的な対応能力だけでなく，切替えにおける組織の対応能力（既存の業務や管理のプロセスでどれだけ対応できるか）として捉えている．

2.5.2 暗号アジリティの重要性

指針では，暗号アジリティを重視する背景として，今後，暗号アルゴリズムの切替えが複数回必要になる可能性があることと，対応が必要なシステムの範囲が広がっており切替えの負担が大きくなっていることを挙げている．

1つ目の点については，PQCのアルゴリズムのセキュリティに対する信頼が十分に醸成されているとは現時点ではいえないとの見方を示しており，今後，新たな脆弱性が指摘され，別のアルゴリズムに切り替える必要が生じうるとしている．

2つ目の点に関しては，さまざまな金融サービスにおいてデータのセキュリティの確保が必要となったことから，暗号アルゴリズムが使用される場面が増えたとしている．そのうえで，現在普及している暗号アルゴリズム（RSA，楕円曲線暗号）が長期間にわたって十分なセキュリティを維持できるであろうと見込まれていたため，暗号アルゴリズムの切替えに関してそれほど意識されることなく，さまざまなインフラやアプリケーションに暗号アルゴリズムが組み込まれることになったという経緯があるとしている．

指針では，金融機関がアルゴリズムの切替えの対応能力を向上させない場合，将来のアルゴリズムの切替え時に，今回よりも複雑かつ負担の大きな対応を強いられる可能性があると指摘している．

2.5.3 組織の対応能力の度合いの把握

暗号アジリティの度合いを把握する方法として，指針では，次の3つの観点から対応能力を評価できるとしている．

- システムの設計段階での考慮の度合い：暗号アルゴリズムの導入・更新・切替えなどの機能がシステムの設計段階でどの程度考慮されているか．
- アーキテクチャにおいて生じる変更の度合い：新しい暗号アルゴリズムを導入する前後で，システムのアーキテクチャにどの程度の変更が必要となるか．
- 稼働中のシステムへの影響の度合い：新しい暗号アルゴリズムの導入に際して，現時点で稼働しているシステムを停止させずに対応できる可能性はどの程度か．

2.5.4 暗号アルゴリズムの切替えを円滑に実施する手法

指針では，暗号アルゴリズムを円滑に切り替えるアプローチとして抽象化（abstraction）の手法を紹介している．

抽象化について，指針では，暗号に関する処理を個々のアプリケーションの一部としてそれぞれ導入するのではなく，アプリケーションとは別のシステムとして導入するという設計方針であると説明されている．

具体的には，メッセージの暗号化やデジタル署名の生成などを，暗号の処理に特化した別のシステムの機能によって実行するという方法が挙げられている．例えば，各アプリケーションが暗号処理に特化したシステムのAPIを読み出すなどの方法がある．アルゴリズムの切替えに際しては，

当該システムのみに新しいアルゴリズムを導入し，各アプリケーションでの対応はAPIによる処理の実行命令を変更するなどの軽微な対応に止めることができる．ただし，暗号の処理に特化したシステムとの間で通信が発生するなど，暗号の処理にかかる時間が長くなる場合があるほか，個々のアプリケーションの事情に応じて暗号の処理をカスタマイズすることが難しくなるという留意点がある旨が説明されている．

抽象化に基づく別の方法として，クリプト・アズ・ア・サービス（crypto-as-a-service），暗号ライブラリ，自動化されたPKI・認証局（automated PKI and CA），通信データ暗号化のためのサービス・メッシュ（service mesh for encryption in transit）を紹介している．

- クリプト・アズ・ア・サービス：暗号に関する処理をクラウド上で実現・提供するサービス．各アプリケーションは，ネットワーク経由でクラウドにアクセスして暗号に関する処理を依頼し，その結果を受信する．
- 自組織内の暗号ライブラリ：暗号ライブラリは暗号アルゴリズム（群）を実行するソフトウェアである．アプリケーションとは別に暗号ライブラリを自組織の内部システムとして準備し，各アプリケーションは暗号に関する処理を暗号ライブラリに依頼し処理結果を受け取る．自組織内で構築することから，クリプト・アズ・ア・サービスと比べて，暗号に関する処理のメンテナンスを柔軟に実行できる反面，メンテナンスを自前で行う必要がある．
- 自動化されたPKI・認証局：電子証明書の管理を実施するシステムを活用する．暗号アルゴリズムの切替えの際に，既存の電子証明書の失効や新しい電子証明書の発行を効率的に実施することができる．
- 通信データ暗号化のためのサービス・メッシュ：データの暗号化や認証の機能を有する機器（VPN 装置など）を介してアプリケーション間の通信が行われ，各アプリケーションが暗号化や認証に関する処理を実行する必要がないアーキテクチャ．暗号アルゴリズムの切替えの対応は，データの暗号化や認証の機能を有する機器でのみ行われる．

2.6 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の報告書

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は，預金取扱金融機関がPQCの導入を検討する際の推奨事項・課題・留意点について，金融機関の実務者や有識者が議論・検討するために2024年7～10月に開催された．議論や検討の内容は報告書としてまとめられ，2024年11月に公表された．

2.6.1 リスク対応のポイント

報告書では，エグゼクティブ・サマリーにおいて，CRQCによる暗号へのリスクに対応するためには長期間にわたって多くのリソースを必要とすることから，経営層がリスクやその対応の期限を正しく認識する必要があるとしている．そのうえで，リスク対応を適切に進めるためのポイントとして以下の点を示している．

- 経営層のイニシアティブ：経営層はPQC導入の対応を全社施策として取り扱い，リーダーシップを発揮して方針を決定することが望ましい．
- PQCのアルゴリズムの導入時期：アメリカ連邦政府が2035年を目途にPQC移行を推進していることなどを踏まえ，重要度の高いシステムでは，2030年代半ばを目安にPQCを使用可能な状態にすることが望ましい．
- 暗号インベントリ：対応の事前準備として暗号インベントリの整備・管理が必要であるが，そのような仕組みの構築・運用に相当の時間とリソースを要するため，早期に着手することが望ましい．
- 暗号アジリティ：導入後のアルゴリズムにおいて脆弱性が発見される可能性があるため，アルゴリズムを柔軟に切り替えることを可能にする技術の導入を考慮すること（暗号アジリティを向上させること）が重要である．
- ステークホルダーとの連携：アルゴリズムの導入・移行は，ベンダー，金融インフラ提供事業者，フィンテック企業などと協力して検討することが重要である．
- 金融業界としてのロードマップ策定：政府とも密に連携しつつ金融業界としてのロードマップを策定するとともに，各金融機関に共通する課題に協力・分担して対応していくことが望ましい．

2.6.2 技術面での課題・留意点

技術面での課題や留意点を要約すると以下のとおりである．

- 暗号アジリティをどのように実現するかが重要な課題である．暗号処理を疎結合とするアーキテクチャの策定・適用，電子証明書や暗号鍵管理の機能の集約，暗号インベントリの整備・更新，暗号の利用状況を監視するための管理プロセスやツールの整備などが挙げられる．
- PQCのソリューションの適用に際して，標準化動向や技術の成熟度の把握が重要である．個々の金融機関での把握は困難なことも見込まれるため，政府・監督当局・業界団体と連携して情報の提供を受けることが望ましい．
- PQCへの移行の過渡期において，PQCのアルゴリズ

ムに対応していないシステムからの接続と対応済みのシステムからの接続が混在する場合が想定されるため，両方の接続を実現する機能を考慮することが望ましい．

- PQC 対応はシステムの大規模な更改･改修のタイミングに合わせて実施することを基本とし，時間に余裕を持って検討することが重要である．

2.7 国際決済銀行スタッフらによる PQC 導入ロードマップの提案

2025 年 7 月，国際決済銀行のスタッフらが，金融分野における PQC 導入を巡る最近の動向を紹介するとともに，PQC 導入のロードマップ（implementation roadmap）を提案する内容の個人名ペーパーを発表した．

2.7.1 概要

ペーパーでは，CRQC による暗号へのリスクを軽減するための検討を早期に開始することが望ましい（“The time to act is now.”）としたうえで，リスク軽減策として PQC の導入が最も現実的かつ効果的であるとの見方を示している．また，単に既存のアルゴリズムを PQC のアルゴリズムに切り替えるだけでなく，長期的な視点から，(切替え後の)PQC のアルゴリズムに問題が生じる可能性を考慮することが望ましいとしている．具体的には，既存のアルゴリズムと PQC のアルゴリズムを組み合わせるハイブリッド方式や，導入する暗号アルゴリズムを別のアルゴリズムに変更しやすいシステム・アーキテクチャ（暗号アジリティの向上）の採用を挙げている．

2.7.2 金融業界としてのロードマップ

PQC 導入のロードマップとして，ペーパーでは，金融業界としてのロードマップと各金融機関におけるロードマップをそれぞれ提案している．このうち，金融業界としてのロードマップは，金融当局や中央銀行も関与して検討・調整する事項を含んでおり，①合意形成（obtaining engagement），②計画（plan），③監視（monitor）3 つのフェーズから構成されている．

① 合意形成フェーズ : 金融業界として，ステークホルダーの啓発，リスク評価，対応の優先順位付けなどを実施する．
② 計画フェーズ : PQC のアルゴリズムの選定，PQC 導入の要件やタイミングの決定（国際間での調整を含む），導入計画の策定を行う．
③ 監視フェーズ : 各システムの PQC 導入の進捗状況を監視する．また，導入中または導入完了後に，性能評価やセキュリティ評価を実施し，計画通りに導入されているか否かを検証する．導入後は，CRQC によるリスクを通常のサイバーセキュリティ・リスク管理の枠組みのなかで継続的に監視する体制を実現する．

2.7.3 各金融機関におけるロードマップ

ペーパーでは，各金融機関が，金融業界としてのロードマップを参照しつつ整合性を保つように自社のロードマップを作成することが望ましいとしている．内容は，①啓発（awareness），②計画立案（planning），③実行（executing）の 3 つのステップで構成されている．

① 啓発ステップ : 各金融機関は，リスクや対応の必要性に関する認識を社内の関係部署およびステークホルダーと共有する．また，経営層のリーダーシップのもとで，リスク対応方針の決定，検討･推進体制の整備，予算の確保などを行う．
② 計画立案ステップ : 暗号インベントリの構築，リスク評価，対応の優先順位付け，システム要件の検討を行う．技術仕様の標準化や他の金融機関における検討状況を調査する．これらを踏まえ，ステークホルダーと連携しつつ，採用する PQC の仕様（アルゴリズム，暗号鍵のサイズ，ハイブリッド方式の有無など）やシステム対応の実施時期を決定し，各システムへの PQC の導入計画を立案する．
③ 実行ステップ : 導入計画に沿ってシステム更改作業を進め，システムレベルでの性能試験（暗号処理速度などを測定しシステム要件との整合性を確認）を実施する．導入完了後，当該システムの性能やリスクの状況を継続して監視・確認する．

3. 主な推奨事項のまとめ

2 節で紹介した提言や指針は，リスク対応の検討になるべく早期に着手することが望ましいとしている点で共通しているといえる．また，金融機関のリスク対応における推奨事項については，概ね次のようにまとめることができる．

- 金融業界としてのリスク軽減計画の策定 : 金融業界の関係者（当局を含む）が連携して情報を共有しつつ，業界全体としてリスク軽減に向けた計画を策定することが望ましい．
- 暗号インベントリの整備 : リスクを評価するためには，暗号アルゴリズムの使用状況を明確にする必要がある．そのための事前準備として暗号インベントリを早期に整備することが望ましい．
- HNDL 攻撃対応 : 長期間保護する必要がある情報を取り扱っているシステムにおいては，HNDL 攻撃が現時点で既に脅威となっている可能性がある．リスク評価を早期に実施し、HNDL 攻撃の標的となっている可能

性があるケースにおいては優先的に対応することが望ましい.

- 暗号アジリティの向上 : 今後，暗号アルゴリズムの切替えが複数回必要となる可能性がある. そうした事態に備えて, アルゴリズムの切替えを円滑に実施する仕組みや体制について検討することが望ましい.
- ハイブリッド方式の採用 : PQC への移行の過渡期において，既存のアルゴリズムには（CRQC による攻撃以外には）脆弱性が報告されていないにもかかわらず，PQC のアルゴリズムに新たな脆弱性が発見される可能性がある. こうした事態に対処するために，PQC のアルゴリズムと既存のアルゴリズムを組み合わせて導入することが望ましい.

4. おわりに

本稿では，量子コンピュータによる暗号へのリスクに関して, 金融分野における最近の主な提言や指針を紹介した。

PQC の導入を金融分野として完了させるためには，相応の時間とコストが必要になると見込まれる. 本稿で取り上げた提言や指針においても,「余裕をもって対応する」という観点から，暗号インベントリの整備などに早目に着手することが推奨されている.

また，金融機関が足並みを揃えてリスク対応を進めるという観点から，金融業界としてのリスク軽減計画をまず策定し，その計画と整合的なリスク軽減計画を各金融機関がそれぞれ策定するという対応が推奨されている. こうした対応は，各金融機関が自社のリスク軽減計画をそれぞれ独自に策定する場合に比べて，各金融機関における負担の軽減につながるほか，一部の金融機関においてリスク対応が遅れる可能性も低くなるというメリットも期待できる. わが国では，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での議論を受けて，PQC 導入のロードマップのひな形が金融 ISAC において検討されている[4].

各金融機関においては，こうした活動に積極的に参加することを通じて，金融機関間の連携の強化やリスク対応に関する理解の深耕を期待したい.

金融機関のシステムに関係するベンダーにおいては，金融機関との連携や情報共有を通じて, 円滑な PQC 導入に資する対応を期待したい.

参考文献

[1] 高木剛. 暗号と量子コンピュータ. オーム社, 2019, 215p.

[2] 坂本静生, 宇根正志. AI･量子コンピュータにかかわるリスク管理. オーム社, 2025, 349p.

[3] 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. 日本銀行金融研究所ディスカッションペーパー, 2025, No. 25-J-1, 26p.

[4] 屋敷利紀. すべての金融機関が直ちに着手すべき耐量子計算機暗号への移行：サイバー攻撃の標的とならないようシステム更改時期も見据えた対応を. 金融財政事情, 2025, 2025 年 4 月 15 日号, p. 38-41.