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

宇根正志（うねまさし）

要　旨

金融分野では、量子コンピュータ開発の今後の進展を展望し、量子コンピュータによる暗号アルゴリズムへのリスクにどのように対応していくかに関心が集まっている。大規模かつ実用的な量子コンピュータが実現すると、現在普及している公開鍵暗号のセキュリティが低下し、それによって保護されている情報が解読される可能性がある。こうしたリスクへの対応として、既存の公開鍵暗号を量子コンピュータでも解読困難な耐量子計算機暗号に移行させていくことが求められる。近年、暗号アルゴリズムの移行に関する調査報告や提言が金融関連の団体や当局から相次いで発表されており、いずれも、リスク低減に向けて暗号アルゴリズムの移行に関する検討の早期着手が望ましいとしている。そのうえで、各金融機関のシステムにおける暗号アルゴリズムの使用状況の調査・管理（暗号インベントリの整備）、長期間保護が必要な情報の特定とリスクの評価、対応すべきシステムの優先順位付け、暗号アルゴリズムを円滑に切り替える仕組みの実装（暗号アジリティの向上）を推奨事項として挙げている。また、金融機関が連携し、金融業界としてのリスク低減計画を策定することも推奨している。各金融機関においては、こうした推奨事項を踏まえつつ、量子耐性を有するシステムの実現に向けて適切に対応する必要がある。

キーワード：暗号アジリティ、暗号アルゴリズム移行、暗号インベントリ、公開鍵暗号、耐量子計算機暗号、リスク低減計画、量子コンピュータ

本稿は 2024 年 11 月 5 日時点の情報に基づいて作成した。本稿の作成に当たっては、松本泰フェロー（特定非営利活動法人日本ネットワークセキュリティ協会）から有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者個人に属する。

宇根正志　日本銀行金融研究所参事役（E-mail: masashi.une@boj.or.jp）

1. はじめに

暗号アルゴリズムは、金融サービスや金融業務のセキュリティを支える重要な要素技術として広く用いられている。暗号アルゴリズムの用途として、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用いられている。業務でクラウドを使用している場合には、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アルゴリズムが採用されている。

こうした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や楕円曲線暗号）には、量子コンピュータ[1]による解読のリスクがある（宇根・菅［2021］）[2]。RSAや楕円曲線暗号を効率的に解読することができるレベルの量子コンピュータ（CRQC）[3]が実現するタイミングは明確になっていない[4]。しかし、仮に、攻撃者がCRQCを用い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）が解読されたり、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。したがって、このようなリスクが許容できないと判断されるシステム（量子脆弱性を有するシステム）においては、量子コンピュータでも解読困難な暗号アルゴリズム[5]に切り替えるなどのリスク低減策を事前に適用し、CRQCに対しても十分なセキュリティを確保できるシステム（量子耐性を有するシステム）を実現する必要が

1 量子コンピュータは量子力学の原理を活用したコンピュータの総称であり、超伝導回路方式などさまざまな実現方式の量子コンピュータの研究開発が活発に進められている。

2 一定の規模や機能を有する量子コンピュータを用いて効率よく解読する方法が知られている暗号アルゴリズムは、量子脆弱性を有する（quantum-vulnerable）暗号アルゴリズムと呼ばれる。

3 量子脆弱性を有する暗号を現実的な時間と費用によって解読することが可能なレベルの量子コンピュータはCRQC（cryptographically relevant quantum computerまたはcryptanalytically relevant quantum computer）と呼ばれている。

4 CRQCが実現する可能性のある時期に関して、ドイツのセキュリティ当局であるBSI（Bundesamt für Sicherheit in der Informationstechnik）が2024年に発表した調査報告では、2040年頃までにCRQCが実現する可能性が示唆されている（Bundesamt für Sicherheit in der Informationstechnik 2025）。

5 こうした暗号アルゴリズムは、量子耐性を有する（quantum-resistant、quantum-safe、quantum-secureなど）暗号アルゴリズムと呼ばれている。アメリカのNIST（National Institute of Standards and Technology）は量子耐性を有する暗号アルゴリズム（群）を標準化しており、それらをPQC（post-quantum cryptography）と呼んでいる。PQCは耐量子計算機暗号と訳されるケースが多い。なお、NISTは、セキュリティ技術をはじめとする各種先端技術の研究開発や標準化を行う商務省傘下の研究機関であり、連邦政府機関が使用する情報技術の標準規格FIPS（Federal Information Processing Standards）の策定を担っている。

ある。

CRQC によるリスクへの対応は金融分野に限られるものではない。海外の主要な国の政府機関では、CRQC によるリスクの評価やリスク低減策に関するガイダンスやホワイト・ペーパーを発表する動きが 2020 年頃からみられている（宇根［2023］）。アメリカ連邦政府は、2035 年を目途に量子コンピュータによるリスクを可能な限り低減する方針を 2022 年 5 月に表明し、耐量子計算機暗号の標準化、量子脆弱性を有する暗号アルゴリズムの使用停止など、リスク低減に向けたロードマップを発表している（White House 2022）。欧州では、欧州委員会が欧州連合加盟各国に対して、量子耐性を有する暗号アルゴリズムの実装ロードマップを 2026 年 4 月までに策定することを、2024 年 4 月に勧告している（European Commission 2024）。また、欧州連合に加盟している 18 の国のセキュリティ当局は、各国の行政・産業界に向けて、リスク対応に関する検討への早期着手を促す声明を 2024 年 11 月に共同で発表している（Secure Information Technology Center Austria *et al.* 2024）。

このように、欧米では、CRQC が登場するタイミングが不透明ななかにあっても、なるべく早期にリスクを排除するという観点から、量子耐性を有するシステムの実現を政策として促進している。今後、欧米の企業や組織（日本企業の海外支店なども含む）が量子耐性を有するシステムに移行していくとすれば、欧米の企業や組織と通信する必要がある日本国内の企業や組織も量子耐性を有するシステムに移行しなければならなくなる可能性がある。こうした対応に遅れた場合、CRQC によるリスクにさらされるだけでなく、欧米の企業や組織と通信できなくなるというネットワークの接続性の問題にもつながりうることにも留意すべきであろう。

金融分野においても、CRQC によるリスクにどのように対応するかについて関心が高まっている。海外の金融関連の団体や当局から、リスク対応に関する調査報告や提言が最近相次いで発表されている。NIST が耐量子計算機暗号の標準化候補となる暗号アルゴリズムの募集を開始した 2016 年 12 月以降に絞ると、主な調査報告や提言として以下が挙げられる。

① 2019 年 1 月：ASC X9, Inc.[6] が暗号メッセージ構文[7]（CMS: cryptographic message syntax）に関する報告書を発表した（Accredited Standards Committee X9, Inc. 2019）。
② 2022 年 11 月：ASC X9, Inc. が CRQC によるリスクに関する報告書を発表した（Accredited Standards Committee X9, Inc. 2022）。
③ 2023 年 3 月：FS-ISAC[8] が CRQC によるリスクへの対応に関する提言を発表し

6 ASC X9, Inc.（Accredited Standards Committee X9, Inc.）はアメリカ国内における金融サービスに関連する標準規格を策定する非営利団体である。
7 暗号メッセージ構文とは、暗号アルゴリズムによる処理（デジタル署名生成、ハッシュ化、暗号化など）の対象となるメッセージの構成要素やフォーマットを指す。
8 FS-ISAC（Financial Services Information Sharing and Analysis Center）は、金融機関におけるサイバー

た（Financial Services Information Sharing and Analysis Center 2023）。

④ 2023 年 6 月：国際決済銀行・フランス銀行・ドイツ連邦銀行が量子耐性を有する暗号アルゴリズムを実装・テストするプロジェクト Leap の報告書を発表した（Bank for International Settlements, Banque de France, and Deutsche Bundesbank 2023）。

⑤ 2023 年 11 月：UK Finance Limited[9] が CRQC によるリスクへの対応に関する提言を発表した（UK Finance Limited 2023）。

⑥ 2024 年 1 月：世界経済フォーラム[10] が CRQC によるリスクに対応するための規制や国際協調に関する提言を発表した（World Economic Forum 2024）。

⑦ 2024 年 2 月：シンガポール金融管理局が CRQC によるリスクへの対応に関して金融機関向けの勧告を発表した（Monetary Authority of Singapore 2024）。

⑧ 2024 年 9 月：G7 サイバー・エキスパート・グループ[11] が CRQC によるリスクへの対応に関する提言を発表した（金融庁［2024］；G7 Cyber Expert Group 2024）。

⑨ 2024 年 10 月：FS-ISAC が暗号アルゴリズムを円滑に切り替える体制の整備に関するガイダンスを発表した（Financial Services Information Sharing and Analysis Center 2024）。

⑩ 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[12] が報告書を発表した（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［2024a］）。

上記の⑨は、システムにおいて使用する暗号アルゴリズムを円滑に切り替えることを可能にする性質である暗号アジリティ（cryptographic agility）をテーマとしているが、その他の調査報告においても暗号アジリティの重要性が指摘されている。

金融機関においては、こうした報告書などを参照しつつ、CRQC によるリスクに適切に対応していく必要がある。

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。

9 UK Finance Limited はイギリスにおける金融分野の業界団体であり、金融業界内での連携の支援、金融サービスに関連する規制や金融業界内のルールの立案、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。

10 世界経済フォーラム（World Economic Forum）は、社会の発展のために、政治、産業、学術などの各界のリーダーや有識者が課題解決に向けて協力するための枠組みを提供する国際的な非営利団体である。

11 G7 サイバー・エキスパート・グループ（G7 Cyber Expert Group）は、サイバーセキュリティに関するポリシーや戦略の調整、関連する情報の共有、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。

12 この検討会（事務局：金融庁）は、金融機関の実務者や有識者が預金取扱金融機関による耐量子計算機暗号への移行における推奨事項、課題、留意点を検討するために、2024 年 7 月から 10 月にかけて開催された。

本稿では、金融関連の団体や当局による調査報告や提言におけるリスク低減の方針や推奨事項を説明する。

2. 金融分野における主な調査報告・提言

1節で列挙した10件の調査報告・提言のうち、②と③は宇根［2023］で紹介されていることからここでは割愛し、残りの8件を紹介する。

(1) ASC X9, Inc. による暗号メッセージ構文に関する報告

ASC X9, Inc. は、暗号メッセージ構文の暗号アルゴリズムへの CRQC による影響と対応に関する報告書を 2019 年 1 月に発表している（Accredited Standards Committee X9, Inc. 2019）。報告書では、公開鍵暗号に基づくデジタル署名と鍵共有、共通鍵暗号を対象としている。

イ. デジタル署名

報告書では、署名アルゴリズムが量子脆弱性を有している場合、CRQC によって署名検証鍵から署名生成鍵が推定され、署名の偽造によって、メッセージの一貫性確認や認証が無効化されうるとしている。また、量子脆弱性を有する署名アルゴリズムが用いられている電子証明書も偽造されうると指摘している。

このようなリスクへの対応として、量子耐性を有していると十分信頼できる署名アルゴリズムを実装することを推奨している。そうした署名アルゴリズムを採用できない過渡期においては、量子耐性を有すると期待されている署名アルゴリズムを既存の署名アルゴリズムと組み合わせて用いる手法（ハイブリッド手法〈hybrid method〉[13]）を推奨している。双方の暗号アルゴリズムによってそれぞれ署名を生成し、署名検証時にはこれらの検証結果を用いて署名の正当性を判断する[14]。

また、別の対応として、物理的にアクセスを制御している場所に署名対象データを保管する方法や、特定の時点に署名対象データが存在していたことを第三者が認めた証となるデータ（タイムスタンプ[15]）を取得・保管する方法も紹介している。

13 ハイブリッド手法は、組み合わされた暗号アルゴリズムのうち、少なくとも1つが安全であれば、保護対象のデータの安全性を維持することができるように設計されている手法である。

14 例えば、双方の署名アルゴリズムのうち、署名検証時に危殆化していないものによって生成された署名に着目し、その検証が成功すれば署名を正当とみなすという方法が挙げられる。

15 タイムスタンプの各種手法については、宇根・松浦・田倉［2000］を参照されたい。

ロ. 鍵共有

報告書は、メッセージ本体の暗号化には共通鍵暗号を使用し、その暗号鍵（セッション鍵）を公開鍵暗号によって通信当事者間で共有する形態を前提としている。そのうえで、セッション鍵の共有方法として次の 3 つを説明している。

- 通信当事者の一方がセッション鍵を生成し、それを通信相手の公開鍵によって暗号化したうえで通信相手に配送する（鍵配送〈key transport〉）。
- 通信当事者が（自分のプライベート鍵を用いて生成した）公開可能なデータをそれぞれ通信相手に送信し、受信したデータと自分のプライベート鍵からセッション鍵を生成する（鍵合意〈key agreement〉）。
- 鍵カプセル化メカニズム（KEM）[16] を使用する。

報告書は、いずれの方法においても、量子脆弱性を有する暗号アルゴリズムが使用されている場合、CRQC を用いる攻撃者によって公開鍵からプライベート鍵が推定され、保護対象のメッセージが盗取されうるとしている。

対応の方針として、報告書は、デジタル署名の場合と同じくハイブリッド手法の採用を挙げている。特に、**HNDL 攻撃 [17] による暗号解読のリスクが許容できない場合には、多重防御の観点からハイブリッド手法を可能な限り早期に採用することが望ましい**としている。ハイブリッド手法の採用が間に合わない場合には、インターネットとは別の物理的なチャネルなどを介して、セッション鍵の元となるデータを通信当事者間で共有する方法（事前共有鍵〈pre-shared key〉を用いる方法）を紹介している。

また、量子耐性を有する暗号アルゴリズムの多くが鍵カプセル化メカニズムであり、NIST の標準化対象になっていることなどから、鍵配送、鍵合意ではなく、鍵カプセル化メカニズムを推奨している。

ハ. 共通鍵暗号

報告書は、共通鍵暗号への影響が公開鍵暗号の場合ほど大きくないとしたうえで、セキュリティを維持するために暗号鍵のサイズを約 2 倍に伸長することを推奨している。

---

16 KEM（key encapsulation mechanism）は公開鍵暗号の使用形態の 1 つである。セッション鍵の共有の流れは、①まず、送信者が受信者の公開鍵を入手する、②送信者は公開鍵などから暗号文とセッション鍵を生成する、③送信者は暗号文を受信者に送信する、④受信者は暗号文と自分のプライベート鍵からセッション鍵を生成するというものである。

17 HNDL（harvest now, decrypt later）攻撃は、CRQC が登場する前から暗号文を収集しておき、CRQC が登場して使用可能になったタイミングで収集した暗号文を一気に解読するという攻撃である。SNDL（store now, decrypt later）攻撃、ハーベスト攻撃とも呼ばれる。

(2) 国際決済銀行・フランス銀行・ドイツ連邦銀行のプロジェクト報告

国際決済銀行、フランス銀行、および、ドイツ連邦銀行は、量子耐性を有する暗号アルゴリズムを中央銀行間の通信ネットワーク・システムに実装・テストするプロジェクト Leap の報告書（フェーズ 1）を 2023 年 6 月に発表した（Bank for International Settlements, Banque de France, and Deutsche Bundesbank 2023）。

イ. 背景

報告書では、金融機関の業務やサービスで用いられる通信データのセキュリティが暗号プロトコルに大きく依存しているとしたうえで、量子コンピュータを悪用するサイバー攻撃に暗号プロトコルがさらされる可能性があるとの認識を示している。10 年以上の長期間にわたって秘匿する必要があるデータ、特に金融機関以外の場所（クラウドなど）で保管されているものについて、HNDL 攻撃の脅威が既に存在しうることから早急な対応が必要であるとしている。対応として、報告書では、量子耐性を有するシステムを実現する必要があるとしている。また、そうしたシステム向けの新しい暗号プロトコルや暗号アルゴリズムの開発・標準化が NIST などによって進められていることを紹介している。

ロ. プロジェクトの概要

報告書では、プロジェクトのフェーズ 1 の目標として、量子耐性を有する主な暗号アルゴリズムを実際の通信ネットワーク・システムで動作させ、実装性を把握することを挙げている。具体的には、①暗号アルゴリズムの円滑な切替え（暗号アジリティ）、②処理の速度や安定性（性能〈performance〉）、③セキュリティ・パラメータ[18] を変化させた際の処理の可否（セキュリティ〈security〉）によって実装性を評価している。

プロジェクトでは、通信ネットワーク・システムとして、フランス銀行とドイツ連邦銀行を接続する暗号通信路[19] を使用している。通信当事者は、通信相手を認証した後、共通鍵暗号（AES）用のセッション鍵を公開鍵暗号によって共有し、それを用いてメッセージ（サイズは約 1 メガ・バイト）本体を暗号化して通信する。量子耐性を有する暗号アルゴリズムとして、NIST の標準化対象の暗号アルゴリズム（CRYSTALS-Kyber、CRYSTALS-Dilithium、SPHINCS+、Falcon）に加えて、ドイツ

18 NIST の標準化対象の暗号アルゴリズムでは、5 段階のセキュリティ・レベルが設定されており、それぞれのレベルを達成するためのセキュリティ・パラメータが定められている。

19 暗号通信路には、広く使用されている IPsec VPN が採用されている。IPsec VPN は、通信機器間での暗号化や認証を実現する標準プロトコル IPsec（IP Security）を用いて仮想的な専用の通信網 VPN（virtual private network）を実現する技術である。

のセキュリティ当局などが推奨している鍵カプセル化メカニズムの暗号アルゴリズム FrodoKEM を選択し、これらを市販の暗号ライブラリによって実装している。

上記の暗号アルゴリズムはハイブリッド手法で実装されている。セッション鍵の共有では、既存の暗号アルゴリズムとして RSA を使用し、量子耐性を有する暗号アルゴリズムとして CRYSTALS-Kyber と FrodoKEM を使用している。通信相手の認証に用いられるデジタル署名に関しては、既存の署名アルゴリズムとして RSA を使用し、量子耐性を有する署名アルゴリズムとして CRYSTALS-Dilithium、SPHINCS+、Falcon を使用している。

ハ. 結果

暗号アルゴリズムの切替えに関して、セッション鍵の共有では、通信当事者間で使用する暗号アルゴリズムを決定する機能が暗号ライブラリに設定されていたため、円滑に切り替えることができた。デジタル署名では、署名アルゴリズムを識別する機能が暗号ライブラリに設定されておらず、署名アルゴリズムを識別する機能を手動で設定した。

処理速度に関して、主に認証・鍵共有の処理と暗号化メッセージの通信にかかる時間をそれぞれ測定した。認証・鍵共有の時間は、既存の暗号アルゴリズム（鍵共有・署名ともに RSA）を使用する場合よりも、量子耐性を有する暗号アルゴリズムを用いる場合（例えば、鍵共有に CRYSTALS-Kyber、署名に CRYSTALS-Dilithium を使用）において長くなった[20]。暗号化メッセージの通信の時間は、いずれの場合も AES を使用したことからほぼ同じであった。

処理の安定性に関して、暗号通信路の機能が正常に維持されているか否かを 1 時間ごとに確認したところ、24 時間正常であった。

セキュリティ・パラメータを変化させた際の処理の可否に関して、量子耐性を有する暗号アルゴリズムを異なるセキュリティ・パラメータのもとでそれぞれ動作させた結果、いずれのパラメータでも正常に動作した。また、相対的に高いセキュリティ・レベルに対応するパラメータで動作させた場合、処理速度が低下した。これらを踏まえて、実装時にはセキュリティ・レベルと処理速度のトレードオフに留意する必要があるとしている。

ニ. 暗号アルゴリズム移行に向けた対応と今後のプロジェクト

報告書では、今後、中央銀行やその他の金融機関が暗号アルゴリズムの移行において直面する課題として、暗号アルゴリズムの使用状況の調査、量子脆弱性を有する暗号アルゴリズムの使用の特定、リスク評価などを挙げている。また、暗号アル

20 量子耐性を有する暗号アルゴリズムの処理速度に関しては、鍵共有では、CRYSTALS-Kyber が FrodoKEM よりも優れていた。署名では、CRYSTALS-Dilithium と Falcon が同程度であったほか、これらと比べると SPHINCS+ が劣っていた。

ゴリズムの移行が、今回のプロジェクトのような暗号通信路だけでなく、さまざまなシステムにおいて求められるとしたうえで、各種のシステムに対応する新しい暗号プロトコルの開発、それらを実現するハードウェアやソフトウェアの導入、量子耐性を有する暗号アルゴリズムに関する専門的なスキルをもつスタッフの育成・確保が必要であるとの見方を示している。そして、こうした取組みに要する時間を十分確保するという観点から、暗号アルゴリズム移行に向けた検討の早期着手が重要であるとしている。

本プロジェクトの今後について、報告書では、量子耐性を有する暗号アルゴリズムを複雑なシステム環境（例えば、中央銀行とその他の組織との間の通信ネットワーク・システム）において実装・テストすることが考えられるとしている。

(3) UK Finance Limited による提言

UK Finance Limited は、2023 年 11 月に発表した提言において、量子コンピュータが金融商品のポートフォリオの最適化などに貢献しうると期待されている一方で、金融サービスで使用されている暗号アルゴリズムに深刻な影響を与えるリスクがあるとしている（UK Finance Limited 2023）。そのうえで、量子コンピュータによるメリットを享受するためにも、金融業界全体としてリスクに対応する必要があるとしている。

イ. CRQC を用いる攻撃によって生じうる事象の例

提言では、金融機関が使用する暗号アルゴリズムが CRQC によって解読された場合、以下の事象が生じうるとしている。

① 金融機関が保持している個人情報（personally identifiable information）が盗取される。
② ホールセール決済に関連する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などが行われる。
③ 金融機関が公開している API（application programming interface）における認証や認可を実行する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実行されたり、暗号化されたデータが解読されたりする。
④ 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、それ以降に生成されたすべてのブロックの内容が信頼できないものとなる。
⑤ 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、システムなどが不正に操作される。
⑥ リテール決済のシステムにおける認証が無効化され、なりすましなどによって

不正な取引が実行される。

⑦ ソフトウェアやファームウェアの一貫性を確認することができなくなり、不正なソフトウェアなどが金融機関のシステムに組み込まれて不正な動作を引き起こす。

⑧ 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。

⑨ 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）が改変される。

ロ. 金融業界レベルでの検討

提言では、上記の事象への対策として、**金融業界のステークホルダーが連携して業界横断的なタスクフォースを設置し、金融業界レベルの移行計画（quantum safe transition plan）を策定する**ことを推奨している[21]。そして、**金融業界レベルの移行計画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る**としている。また、移行計画を策定する過程において想定される主な作業項目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、量子耐性を有する暗号アルゴリズムの使用に関するガイドラインなどを策定する。
- 学界や研究機関と連携し、量子計算技術（quantum computing）や暗号技術における最先端の動向をフォローするとともに、これらに関するスキルを有するスタッフを育成する。
- 政策立案者などと連携し、量子計算技術の適切な使用を促進しつつリスクを低減させるために望ましい政策や規制のフレームワークを検討する。

ハ. 個別の金融機関レベルでの検討

提言では、各金融機関が自社の移行計画を策定する際の検討項目として以下を挙げている。

- 自社のシステムにおける暗号アルゴリズムの使用状況、それに関連する業務プロセスや保護対象の情報などを調査して暗号インベントリを整備する。
- 想定される脆弱性の特定、各システムのリスク評価、保護すべき情報やシステムの優先順位付けなどを実施する。
- 量子計算技術の活用やリスク対応に関するロードマップを立案する。ロードマップには、量子耐性を有するシステムへの移行における中間目標、タイムライン、必要なリソースなどを盛り込む。

21 ここでの移行計画とは、量子耐性を有するシステムやインフラを実現するための活動内容やそのタイムラインを示すものである。提言では、移行計画を効率的に策定するために、業界団体、金融機関、その他のステークホルダーが連携する必要があるとしている。

- 移行計画を策定する際には、必要に応じて、他の金融機関、ベンダー、当局と情報を共有したり共同でプロジェクトを実施したりする。
- 量子耐性を高めるために有効な技術やソリューションの調査・研究・投資を実施する。
- 量子計算技術の動向をフォローし、リスク対応を必要に応じて強化する。
- 量子計算技術のスキルを有する人材を育成するための訓練・研修を実施する。
- 量子計算技術に関連する規制や政策の変更を注視し、必要に応じて、コンプライアンス対応や移行計画を遅滞なく変更する。

(4) 世界経済フォーラムによる提言

世界経済フォーラムは、CRQC によるリスクへの対応のあり方に関して、金融当局のスタッフや産業界の有識者による会議を主催しているほか、各国の金融当局に対してサーベイやインタビューを実施している[22、23]。2024 年 1 月発表の提言では、こうした会議での講演や議論、サーベイやインタビューの結果を紹介しつつ、リスク対応を進める際には金融当局と金融業界の連携や国際協調が重要であるとしている（World Economic Forum 2024）。

イ. 政府や金融業界におけるリスク対応の現状

提言では、政府のリスク対応方針や関連する規制が国によって異なっており、国際的な調和がとれていないほか、一部の国ではリスク対応方針が明確に示されていないとしている。そのうえで、複数の国でビジネスを展開している金融機関は、各国のリスク対応方針や規制に沿った対応を実施する必要があり、複雑な対応を強いられる可能性があるとしている。また、金融機関のシステムが相互に接続され、そのネットワークがグローバルに広がっている点を踏まえると、金融機関のネットワークのセキュリティはその中で最も脆弱なポイントに依存することになると説明している。さらに、政府のリスク対応方針や規制の不備は、ベンダーにおける対応（量子耐性を有する暗号ソリューションの提供）の遅れにつながり、金融機関の対応にも影響が及ぶ可能性があるとしている。

22 これらの活動は FCA（Financial Conduct Authority）との連携によって実施されている。FCA は、イギリスにおける金融市場の機能の維持・向上や消費者の保護を目的として、金融取引に関する規制やガイダンスの策定、金融市場における不正行為の検知・対応、金融機関の認可・検査などを行う公的機関である。

23 会議やサーベイ、インタビューに協力した有識者（43 名）の名前と組織（22 件）の名称がそれぞれ提言ペーパーの謝辞に記載されている。

ロ．リスク対応における 4 つの原則

提言では、今後、金融当局が金融機関と連携してリスク対応を進める必要があるとしたうえで、以下の 4 つの原則を示している。

- 既存の手段や枠組みの活用（reuse and repurpose）：CRQC によるリスクに対応するうえで、既存の技術、ベスト・プラクティス、規制など、既に存在する手段や枠組みを活用することをまず検討する。既存の手段などでは不十分な場合、新しい手段を開発するなどの対応を行う必要がある。
- 交渉不要な要求事項の設定（establish non-negotiables）：金融当局と金融機関は、リスク対応の際のベースラインとして共に認識している要求事項を明確化する。例えば、リスク対応に関する既存のベスト・プラクティスや国際標準などに規定されている事項などが挙げられる。
- 情報の開示と共有（increase transparency）：金融当局と金融機関は、それぞれの戦略やベスト・プラクティス、その他の関連する情報を可能な限り関係者に開示・共有する。
- 分断の回避（avoid fragmentation）：リスク対応に関連する規制について金融当局間で調整を行い、国や地域によって規制の内容が異なるといった事態をなるべく回避する。

ハ．リスク対応のロードマップ

提言では、①準備（prepare）、②明確化（clarify）、③ガイド（guide）、④移行・監視（transition and monitor）からなるリスク対応のロードマップの骨子を示している。

① 準備：リスクに対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、現状把握（暗号インベントリの整備）、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協力体制の確立、リスク対応に必要な作業・費用・期間などの見積り、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、必要な規制の検討やベスト・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戦略の実行、暗号アルゴリズムの管理方法やシステムの開発プロセスの見直し、脅威やリスクの状況の監視、先行きを見通した対応や規制の検討などを実施する。

ニ．暗号アジリティ

提言では、移行・監視フェーズにおける暗号アルゴリズムの管理方法の見直しに関して、先行きの潜在的なリスク（例えば、新しく実装した暗号アルゴリズムが危殆化する）に対応できるように準備することが重要であるとしている。そのうえで、

実装する暗号アルゴリズムに合わせてシステムの各要素を最適化する（one-size-fits-all approach）のではなく、暗号アジリティを実現する（cryptographic agile approach）という方針を採用することを推奨している。

(5) シンガポール金融管理局による勧告

シンガポール金融管理局は、2024 年 2 月発表の勧告において、金融機関が取り扱う重要な情報が今後 10 年で CRQC による脅威にさらされる可能性があるとしている。そのうえで、システムやインフラに大きな影響を与えることなく量子耐性を有するシステムへ移行するために、金融機関のシステムやインフラにおける暗号アジリティの向上が必要であるとしている（Monetary Authority of Singapore 2024）[24]。

勧告では、金融機関が CRQC によるリスクへの対応として、①量子計算技術の動向の把握とリスク対応の啓発、②暗号インベントリの管理とリスク対応の優先順位付け、③リスク対応の戦略の立案と実行能力の向上を挙げている。

イ. 量子計算技術の動向の把握とリスク対応の啓発

- 量子コンピュータの開発状況やそれに伴うリスクを監視するとともに、量子耐性を有する暗号アルゴリズムの適用などを検討する。
- 自社の経営層やベンダーに対して、潜在的な脅威やそれへの対応に必要なサポートを説明し理解を得る。
- ベンダーと協力して量子コンピュータによるサプライチェーン・リスク[25]を評価するとともに、量子耐性を有するシステムの実現に資する暗号製品の提供を依頼する。
- 相互依存関係にある他の産業分野においてリスクが顕在化し、それが金融分野に波及して悪影響を被るリスク（systemic quantum risk）を低減させるために、関連する産業分野などと連携して対応する。

24 勧告では、リスク低減策の選択肢として、量子鍵配送（quantum key distribution）などの検討も示唆している。量子鍵配送は、専用の通信機器を用いて暗号化や復号のための鍵を通信当事者間で共有する技術であり、データ本体は共通鍵暗号などによって暗号化することを想定している（菅・佐々木［2024］）。

25 金融機関が使用しているシステムの構成要素が複数のベンダーによるサプライ・チェーンのもとで開発・提供されるケースで生じるリスクとみられる。サプライ・チェーンの上流に位置するベンダーが量子脆弱性を有する暗号アルゴリズムを組み込んだソフトウェアを開発し、下流のベンダーに提供していた場合、金融機関は上流のベンダーが組み込んだ暗号アルゴリズムを把握できず、暗号アルゴリズムを切り替えることができないというリスクが想定される。

ロ．暗号インベントリの管理とリスク対応の優先順位付け

- 金融機関における暗号インベントリを管理するとともに、量子脆弱性を有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おける管理対象に以下を含めることが望ましい。

  ➢ 使用している暗号アルゴリズムの名称と鍵サイズ
  ➢ 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
  ➢ 暗号アルゴリズムによって保護されている情報、および、その情報を保管・管理する責任を負っている主体の名称

- 量子脆弱性を有する暗号アルゴリズムによって保護されているシステムや情報を特定・分類する。
- 上記の分類に基づいて、リスク対応の優先順位付けを行う。優先順位は、システムや情報に求められる機密度、重要度、保護期間、リスクの大きさなどを考慮しつつ決定することが望ましい。
- 既存の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。暗号アルゴリズムの移行を妨げる制約（例えば、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）がある場合には、そのシステムやインフラをアップグレードして暗号アジリティを高めることを検討する。

ハ．リスク対応の戦略の立案と実行能力の向上

- リスク対応に携わるスタッフに、量子耐性を有するシステムの実現に資するスキルを身につけさせる。
- リスク対応の内容との整合性を保つように、金融機関内部のポリシー、技術標準、各種手続きを見直す。
- 量子耐性を有する暗号アルゴリズムへ移行することが困難なシステムなどがあれば、それに対するリスク低減策を立案する。
- 想定よりも早期にリスクが顕在化した場合における対応の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。

(6) 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、2024 年 9 月発表の提言において、CRQC によるリスクに対応するための検討に着手することを推奨している（金融庁［2024］；G7 Cyber Expert Group 2024）。

提言では、CRQC が登場した場合、それが HNDL 攻撃に悪用され、量子脆弱性

を有する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。そのうえで、金融機関の顧客情報などが盗取され、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。また、こうしたリスクへの対応に関してステークホルダー間での調整には相当の時間と経済的負担が必要となる可能性があることから、可能な限り早期に対応に着手することが望ましいとしている。

提言では、リスク対応の 3 つのステップを挙げている。

① リスクと対応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、量子コンピュータとそれによるリスク、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し、リスクを適切に評価する。
③ リスク低減計画立案：リスクを把握・管理するプロセス、ステークホルダーの責任範囲、リスクの把握・管理のための作業と実施時期、リスク対応の優先順位などを検討し、検討結果を盛り込んだリスク低減計画を立案する。

金融当局に対しては、金融機関などと協力し、量子耐性を向上させる技術（quantum resilient technologies）の重要性を広く知らしめることを推奨している。

(7) FS-ISAC による暗号アジリティのガイダンス

FS-ISAC は、2024 年 10 月に暗号アジリティに関するガイダンスを発表している（Financial Services Information Sharing and Analysis Center 2024）。ガイダンスでは、経営層に対し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するとともに、実務者や技術者に対して暗号アジリティに関連する技術的な課題や留意点を説明している。

イ. 暗号アジリティとは

ガイダンスでは、冒頭で暗号アジリティを以下のとおり説明している。

> 【暗号アジリティ】
> 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、技術的な対応だけでなく組織としての対応を含む概念として記述している。したがって、暗号アジリティを高めるためには、暗号アルゴリズムを切り替える際に必要となる業務・管理プロセスも整備することが求められる。

ロ. 暗号アジリティがなぜ重要か

ガイダンスでは、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となりうる**ことと、**対応が求められる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、量子耐性を有すると期待されている暗号アルゴリズムの多くが不安定な開発のサイクル[26]にあることから、そうした暗号アルゴリズムの切替えの頻度が今後高まりうるとしている。そのうえで、今回の暗号アルゴリズムの切替えにおいて暗号アジリティを考慮しなかった場合、将来さらなる切替えが必要になった際に、対応の時間を確保できない可能性があるとの見方を示している。

2つ目の点については、金融機関が既存の暗号アルゴリズムの安全性を信頼し、暗号アルゴリズムの切替えを考慮しないで、さまざまなインフラやアプリケーションに組み込んできたとしている。その結果、暗号アルゴリズムの切替えが必要なインフラやアプリケーションの範囲が拡大したとしている。

こうした点を踏まえ、ガイダンスでは、**暗号アジリティを考慮しないで暗号アルゴリズムを切り替えることは長期的には金融業界の安全性（safety）にとって望ましくない**との認識を示している。

ハ. 暗号アジリティの度合いをどう把握するか

ガイダンスでは、暗号アジリティの度合いを表現する具体的な指標を示していない。その代わりに、指標を検討するうえで参考になる視点として次の3つを挙げている。

- システム設計の段階における暗号アジリティの考慮の度合い：暗号アルゴリズムの実装・切替えなどの機能がシステムの構成要素（ソフトウェア、ハードウェ

26 ガイダンスでは、不安定な開発のサイクルにあると判断した根拠を明確に示しておらず、NISTのウェブサイト（National Institute of Standards and Technology 2022）を引用している。このウェブサイトは、NISTが標準化対象とした暗号アルゴリズムと継続評価対象とした暗号アルゴリズムをそれぞれ発表するものである。NISTの標準化プロジェクトでは、量子耐性を有する暗号アルゴリズムの評価と改良、標準化が同時並行で進められているほか、将来の脆弱性発見の可能性を想定し（実際に、標準化候補の暗号アルゴリズムのいくつかは脆弱性が発見されて標準化対象外となっている）、さまざまなタイプの暗号アルゴリズムを標準化する方針が示されている。これらを踏まえると、標準化された暗号アルゴリズムであったとしてもセキュリティに対する信頼が十分に醸成されていないとの見方もできる。ガイダンスは、こうした状況を不安定な開発のサイクルと表現したと解釈することができる。

ア、関連するインフラ）や運用プロセスの設計にどの程度組み込まれているか。
- アーキテクチャにおける変更の度合い：新しい暗号アルゴリズムの導入の前後で、システムのアーキテクチャにどの程度の変更が生じるか。
- 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、稼働中のシステムを停止せずに対応できる可能性はどの程度あるか。

ニ．暗号アルゴリズムを円滑に切り替える手法

ガイダンスでは、暗号アルゴリズムの切替えを円滑に実施するアプローチとして抽象化（abstraction）を紹介している。

抽象化は、暗号アルゴリズムの処理に関する機能を個々のアプリケーションの一部としてそれぞれ実装するのではなく、アプリケーションとは別のシステムとして実装するという設計方針である。各アプリケーションは、メッセージの暗号化やデジタル署名の生成などを、暗号アルゴリズムの処理に特化したシステムの API を呼び出して実行する。暗号アルゴリズムの切替えに際しては、暗号アルゴリズムの処理に特化したシステムのみに新しい暗号アルゴリズムを組み込むなどの変更を実施し、各アプリケーションでは、API による処理の実行命令を変更するなどの軽微な対応とすることができる[27]。ただし、暗号アルゴリズムの処理に特化したシステムとの間で通信が発生するため、通常よりも暗号アルゴリズムの処理に時間がかかるほか、個々のアプリケーションの事情に応じて暗号アルゴリズムの処理をカスタマイズできなくなるといった留意点がある。

ガイダンスでは、抽象化に基づく手法の例として、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）を説明している。

- クリプト・アズ・ア・サービス：暗号アルゴリズムの処理をクラウドで実現・提供するサービス。アプリケーションはクラウドにアクセスして処理を依頼し、その結果を受信する形態を主に想定している。
- 暗号ライブラリ：暗号アルゴリズム（群）を実行するソフトウェア。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、アプリケーションは暗号アルゴリズムの処理を暗号ライブラリに依頼して処理結果を受け取る形態を主に想定している。自組織内で構築することから、クリプト・

27 API を使用する場合について、ガイダンスでは、API の名称や引数が暗号アルゴリズムの識別情報と独立か否かなどによって暗号アジリティのレベルが異なる旨を説明している。例えば、API の名称や引数がアルゴリズムの識別情報と独立であれば、暗号アルゴリズムの切替えに際して API の名称などを変更する必要がなく、暗号アジリティが相対的に高いといえる。また、暗号アルゴリズムの処理を実行する機器において、暗号アルゴリズムの切替えの際にユーザやその他のシステムとのインタフェースに変更を加える必要がない場合、暗号アジリティが相対的に高いといえる。

アズ・ア・サービスと比べて、暗号アルゴリズムの処理のメンテナンスを柔軟に実行することができる。

- 自動化された PKI・認証局：電子証明書を管理するシステム。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 の装置など）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のみで行われ、アプリケーションへの影響が少ない。

(8) 金融庁の検討会による報告

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、2024 年 11 月発表の報告書において、金融機関の経営層に対して耐量子計算機暗号への移行に関する対応の重要性、留意点や課題などを説明している（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［2024a］）。

イ．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、経営層がリスクや対応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。

- 経営層は暗号アルゴリズム移行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移行方針を決定することが望ましい。
- アメリカ連邦政府が 2035 年を目途にアルゴリズムの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 年代半ばを目安に量子耐性を有する暗号アルゴリズムを利用可能な状態にすることが望ましい。
- 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、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。
- 移行後の暗号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、暗号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実装を考慮すること（暗号アジリティを向上させること）が重要である。
- 暗号アルゴリズムの移行の検討を、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進めることが重要である。

- 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・分担して対応することが望ましい。

ロ. 技術面での課題・留意点

報告書では、技術面での課題や留意点を説明している。ポイント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。暗号アルゴリズムの処理を疎結合とするアーキテクチャの適用、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、暗号アルゴリズム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。
- 量子耐性を有する暗号アルゴリズム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。個々の金融機関では把握が困難であることも見込まれるため、金融当局、業界団体などと連携して情報の提供を受けることが望ましい。
- 暗号アルゴリズムの移行の過渡期において、新しい暗号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。
- 量子耐性を有する暗号アルゴリズムへの対応はシステムの大規模更改・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。

3. 主な推奨事項のまとめ

2節で紹介した調査報告や提言は、いずれも、CRQCによるリスクに関する検討に早期に着手することが望ましいとしている。今後、金融機関による取組みが推奨されている主な事項を要約する[28]と以下のとおりである。

- 金融業界としてのリスク低減計画の策定：金融業界の関係者（当局を含む）が連携し、関連する情報を共有しつつ、金融業界としてのリスク低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：リスクを見極めるためには、暗号アルゴリズムの使用状況を明確にする必要があることから、事前準備として、暗号インベントリ

28 リスク対応方針などの国際的な調和についても、世界経済フォーラムの提言において重要な推奨事項とされている。これは、主として各国の政府や金融当局への推奨事項であることからここでは割愛する。

を整備することが必要である。

- HNDL 攻撃対応：長期間（例えば 10 年以上）保護する必要がある情報を取り扱っているシステムでは、HNDL 攻撃が既に脅威となっている可能性がある。そのため、リスク評価を早期に実施し、リスク低減の必要性を明らかにすることが望ましい。
- 暗号アジリティに配慮したシステムの実現：今後、暗号アルゴリズムの切替えを複数回実施することになる可能性があり、切替えを円滑に実施するための技術的な仕組みや体制を整備することが望ましい。
- ハイブリッド手法の採用：量子耐性を有する暗号アルゴリズムへの移行の過渡期において、それを既存の暗号アルゴリズムと組み合わせて実装することが望ましい。

4. おわりに

本稿では、CRQC による暗号アルゴリズムへのリスクに関して、金融関連の各種組織による最近の主な調査報告や提言のポイントを紹介した。共通する推奨事項として、暗号インベントリの整備などの事前準備に早急に着手することが挙げられている。また、将来、暗号アルゴリズムの切替えが複数回必要となるケースを想定し、暗号アジリティに配慮したシステムの実現も推奨されている。

金融業界として足並みを揃えてリスク対応を進めるという観点からは、金融機関が連携して業界としてのリスク低減計画をまず策定し、それと整合的なリスク低減計画を各金融機関が策定するという対応が推奨されている。こうした対応は、各金融機関がリスク低減計画をそれぞれ独自に策定する場合と比べて、各金融機関における負担の低減につながる。また、一部の金融機関のリスク対応が遅れる可能性も低くなり、金融業界全体としてのセキュリティ・レベルの維持・向上に資すると期待することができる。

金融業界としてのリスク低減計画の策定には、各金融機関が CRQC によるリスクと対応の必要性を認識することが不可欠である。しかし、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におけるメンバーの発言で示されているように、リスク認識が金融業界に広く浸透しているとはいえない（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［2024b］）。各金融機関の経営層に対して暗号アルゴリズム移行への対応の必要性や緊要性をどのように説明し理解を得ていくかが重要な課題である。アプローチの 1 つとして、金融機関における暗号アルゴリズムの代表的なユースケースを洗い出し、それぞれのユースケースにおいて暗号解読などのリスクを明確化することが考えられる。リスク低減に必要な作業

や課題、費用負担や移行にかかる時間を見積もり、ユースケースに応じた「手触り感」のある説明を行うことが有用であろう。

当面、リスク低減に向けた検討は金融 ISAC において進められるとみられる。各金融機関においては、こうした活動に積極的に参加して金融機関間の連携を一段と強化するとともに、リスクやその対応に関する理解を深めることを期待したい。

参考文献

宇根正志、「量子コンピュータが暗号に及ぼす影響にどう対処するか：海外における取組み」、金融研究所ディスカッション・ペーパー、No. 2023-J-13、日本銀行金融研究所、2023 年

――――・菅　和聖、「量子コンピュータ開発の進展と次世代暗号」、『金融研究』第 40 巻第 4 号、日本銀行金融研究所、2021 年、55～96 頁

――――・松浦幹太・田倉　昭、「デジタルタイムスタンプ技術の現状と課題」、『金融研究』第 19 巻別冊第 1 号、日本銀行金融研究所、2000 年、105～154 頁

菅　和聖・佐々木寿彦、「量子鍵配送の安全性証明の進展と普及に向けた課題」、『金融研究』第 43 巻第 4 号、日本銀行金融研究所、2024 年、123～156 頁

金融庁、「『量子コンピュータの登場に伴う機会とリスクに備えた計画に関する G7 サイバー・エキスパート・グループによるステートメント』の仮訳」、金融庁、2024 年（https://www.fsa.go.jp/inter/etc/20240926/quantum_kariyaku.pdf、2025 年 12 月 10 日）

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、「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報告書」、金融庁、2024 年 a（https://www.fsa.go.jp/singi/pqc/houkokusyo.pdf、2025 年 12 月 10 日）

――――、「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（第 3 回）議事要旨」、金融庁、2024 年 b（https://www.fsa.go.jp/singi/pqc/gijiyousi/20241018.html、2025 年 12 月 10 日）

Accredited Standards Committee X9, Inc. 2019. “Quantum Techniques in Cryptographic Message Syntax (CMS).” Accredited Standards Committee X9, Inc. Accessed December 10, 2025. https://x9.org/wp-content/uploads/2019/03/ASC-X9-TR-50-2019-Quantum-Techniques-in-Cryptographic-Message-Syntax-1.pdf.

――――. 2022. “Quantum Computing Risks to the Financial Services Industry.” Accredited Standards Committee X9, Inc. Accessed December 10, 2025. https://x9.org/wp-content/uploads/2022/11/X9F-Quantum-Computing-Risk-Study-Group-IR-F01-2022_20221129-Published-PDF.pdf.

Bank for International Settlements, Banque de France, and Deutsche Bundesbank. 2023. “Project Leap: Quantum-Proofing the Financial System.” Bank for International Settlements. Accessed December 10, 2025. https://www.bis.org/about/bisih/topics/cyber_security/leap.htm.

Bundesamt für Sicherheit in der Informationstechnik. 2025. “Status of Quantum Computer Development.” Bundesamt für Sicherheit in der Informationstechnik. Accessed December 10, 2025. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_1.html?nn=916616.

European Commission. 2024. “Recommendation on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography.” European Commission. Accessed December 10, 2025. https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography.

Financial Services Information Sharing and Analysis Center. 2023. “Preparing for a Post-Quantum World by Managing Cryptographic Risk.” Financial Services Information Sharing and Analysis Center. Accessed December 10, 2025. https://www.fsisac.com/knowledge/pqc.

———. 2024. “Building Cryptographic Agility in the Financial Sector: Effective, Efficient Change in a Post Quantum World.” Financial Services Information Sharing and Analysis Center. Accessed December 10, 2025. https://www.fsisac.com/knowledge/pqc.

G7 Cyber Expert Group. 2024. “G7 Cyber Expert Group Statement on Planning for the Opportunities and Risks of Quantum Computing.” U.S. Department of the Treasury. Accessed December 10, 2025. https://home.treasury.gov/system/files/136/G7-CYBER-EXPERT-GROUP-STATEMENT-PLANNING-OPPORTUNITIES-RISKS-QUANTUM-COMPUTING.pdf.

Monetary Authority of Singapore. 2024. “Advisory on Addressing the Cybersecurity Risks Associated with Quantum.” Monetary Authority of Singapore. Accessed December 10, 2025. https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/mas-quantum-advisory/mas-quantum-advisory.pdf.

National Institute of Standards and Technology. 2022. “PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates.” National Institute of Standards and Technology. Accessed December 10, 2025. https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4.

Secure Information Technology Center Austria, Centre for Cybersecurity Belgium, National Cyber and Information Security Agency Czech Republic, Centre for Cyber Security Denmark, Information System Authority Estonia, Finnish Transport and Communication Agency, French National Agency for the Security of Information Systems, Federal Office for Information Security Germany, National Cyber Security Authority Hellenic Republic, National Cyber Security Centre Ireland, National Cybersecurity Agency Italy, Ministry of Defense Latvia, National Cyber Security Centre Ministry of Defense Lithuania, High Commission for National Protection Luxemburg, Netherlands National Communication Security Agency, Ministry of Interior and Kingdom Relations Netherlands, National Cyber Security Centre Ministry of Security and Justice Netherlands, Research and Academic Research Center Poland, Government Information Security Office Slovenia, and National Cryptologic Center Spain. 2024. “Securing Tomorrow, Today:

Transitioning to Post-Quantum Cryptography." Bundesamt für Sicherheit in der Informationstechnik. Accessed December 10, 2025. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.html.

UK Finance Limited. 2023. "Minimising the Risks: Quantum Technology and Financial Services." UK Finance Limited. Accessed December 10, 2025. https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/minimising-risks-quantum-technology-and-financial.

White House. 2022. "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems." White House. Accessed December 10, 2025. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems.

World Economic Forum. 2024. "Quantum Security for the Financial Sector: Informing Global Regulatory Approaches." World Economic Forum. Accessed December 10, 2025. https://www3.weforum.org/docs/WEF_Quantum_Security_for_the_Financial_Sector_2024.pdf.