IMES DISCUSSION PAPER SERIES

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）

Discussion Paper No. 2025-J-1

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

日本銀行金融研究所が刊行している論文等はホームページからダウンロードできます。
https://www.imes.boj.or.jp

IMES Discussion Paper Series 2025-J-1
2025 年 2 月

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へのリスクにどのように対処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、量子耐性を有する暗号（耐量子計算機暗号）への移行などに関する調査報告や提言が金融関連の団体や当局から最近相次いで発表されており、いずれも、リスク低減に向けた検討の早期着手が望ましいとの見方を示している。そのうえで、各金融機関のシステムにおける暗号の使用状況の調査・管理、長期間保護が必要な情報の特定とリスクの評価、量子耐性を有する暗号へ効率的に移行する仕組みの実装、金融業界としてのリスク低減計画の策定などが推奨されている。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、量子コンピュータ
JEL classification: G21、M15

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

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いただいた。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。

目　次

１．はじめに 1
２．金融分野における主な調査報告・提言 4
（１）ASC X9, Inc.による暗号メッセージ構文に関する報告 5
（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 .. 7
（３）UK Finance Limited による提言 9
（４）世界経済フォーラムによる提言 12
（５）シンガポール通貨庁による勧告 14
（６）G7 サイバー・エキスパート・グループによる提言 16
（７）FS-ISAC による暗号アジリティのガイダンス 17
（８）金融庁の検討会による報告 20
３．主な推奨事項のまとめ 21
４．おわりに 22
【参考文献】 24

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支える重要な要素技術として広く用いられている。暗号の用途として、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暗号が用いられている。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が採用されている。

こうした通信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[1]や楕円曲線暗号）には、量子コンピュータ[2]による解読のリスクがある（宇根・菅［2021］）[3]。大規模かつ実用的な量子コンピュータ（CRQC）[4]が実現して上記のリスクが顕在化するタイミングは明確になっていないものの、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[5]。したがって、こうした不正行為の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[6]に切り替えるなどのリスク低減策を事前に適用

---

1 RSA は RSA Security LLC.の登録商標である。

2 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（Willhelm *et al.* [2024]）。

3 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（quantum-vulnerable）を有する暗号アルゴリズムと呼ばれる。

4 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。

5 CRQC が実現する可能性のある時期に関して、2024 年にドイツのセキュリティ当局である BSI（Bundesamt für Sicherheit in der Informationstechnik）が発表した調査報告では、16 年後（2040 年）までに CRQC が実現する可能性を示唆している（Willhelm *et al.* [2024]）。

6 こうした暗号アルゴリズムは、量子耐性（quantum-resistant、quantum-safe など）を有する暗号アルゴリズム、または、耐量子計算機暗号と呼ぶケースが多い。アメリカでは、NIST（National Institute of Standards and Technology）が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。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国立研究機関であり、

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、量子耐性を有する暗号アルゴリズム（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公表している[7]。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（各国間で調整済みのもの）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 18 ヵ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、欧米の主要国は、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の一環として位置付けていると考えられる。今後こうした政策に沿って、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、こうした企業などと通信する必要がある日本の企業や組織も量子耐性を有する暗号を使用しなければならなくなる可能性がある。リスク対応の遅れは、CRQC によって暗号が解読されるというセキュリティ上の問題に加えて、欧米の企業など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 による暗号へのリスクにどのように対処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 PQC 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。

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）の策定などを担っている（https://www.nist.gov/about-nist）。

[7] 国家安全保障覚書“National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems”として公表されている（https://www.whitehouse.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）。

① 2019 年 1 月：ASC X9, Inc.（Accredited Standards Committee X9, Inc.）[8]が暗号メッセージ構文[9]（CMS：cryptographic message syntax）に関する報告書“Quantum Techniques in Cryptographic Message Syntax”を発表（Accredited Standards Committee X9, Inc. [2019]）。

② 2022 年 11 月：ASC X9, Inc.が報告書“Quantum Computing Risks to the Financial Services Industry”を発表（Accredited Standards Committee X9, Inc. [2022]）。

③ 2023 年 3 月：FS-ISAC（Financial Services Information Sharing & Analysis Center）[10]が“Preparing for a Post-Quantum World by Managing Cryptographic Risk”と題するペーパーを 4 件の報告書のサマリーとして発表（Financial Services Information Sharing & 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アルゴリズムを実装・テストするプロジェクト Leap の概要を紹介するペーパーを発表（Bank for International Settlements, Banque de France, and Deutsche Bundesbank [2023]）。

⑤ 2023 年 11 月：UK Finance Limited[11]が“Minimising the Risks: Quantum Technology and Financial Services”と題するペーパーを発表（UK Finance Limited [2023]）。

⑥ 2024 年 1 月：世界経済フォーラム（World Economic Forum）[12]が“Quantum Security for the Financial Sector: Informing Global Regulatory Approaches”と題するホワイト・ペーパーを発表（World Economic Forum [2024]）。

---

8 ASC 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（https://x9.org/overview-of-x9/）。

9 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。インターネット上で使用される汎用的な暗号メッセージ構文の標準仕様としては、インターネット上の各種技術仕様を策定している IETF（Internet Engineering Task Force）の RFC 5652（Housley [2009]）が知られている。アメリカでは、金融取引に関する暗号メッセージ構文の国内標準規格として ANSI X9.73（Accredited Standards Committee, X9 Inc. [2023]）が存在する。

10 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（https://www.fsisac.com/who-we-are）。

11 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各種の規制や業界ルールの立案、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（https://www.ukfinace.org/about-us）。

12 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連携し課題解決に向けて協力するための枠組みを提供している（https://www.weforum.org.uk/about/world-economic-forum/）。

⑦ 2024 年 2 月：シンガポール通貨庁（Monetary Authority of Singapore）[13]が“Advisory on Addressing the Cybersecurity Risks Associated with Quantum”と題する金融機関向け勧告を発表（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（Cyber Expert Group）[14]が“Planning for the Opportunities and Risks of Quantum Computing”と題する提言を発表（G7 Cyber Expert Group [2024]、金融庁［2024］）。

⑨ 2024 年 10 月：FS-ISAC が“Building Cryptographic Agility in the Financial Sector”と題するガイダンス・ペーパーを発表（Financial Services Information Sharing & 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[15]が報告書を発表（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効率的に入れ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 による暗号へのリスクなどに適切に対処していく必要がある。

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・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について既に宇根［2023］で紹介していることからここでは割愛し、それら以外の調査報告・提言の内容を本節で紹介する。

---

13 シンガポール通貨庁は、シンガポールの中央銀行の機能および金融関連の規制の策定・遂行を担当する公的機関である（https://www.mas.gov.sg/who-we-are）。

14 G7 サイバー・エキスパート・グループは、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（https://home.treasury.gov/policy-issues/international/g-7-and-g-20/g7-cyber-expert-group）。

15 この検討会（事務局：金融庁）は、預金取扱金融機関が PQC のアルゴリズムへの移行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と検討するために開催された（https://www.fsa.go.jp/news/r6/singi/20240704.html）。法令に基づく審議会ではない。

（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.の分科委員会の 1 つである X9F（データと情報セキュリティ〈Data & Information Security〉を担当）は、量子コンピュータが暗号に及ぼす影響や金融業界での対応のあり方について検討を行っている。そうした成果の 1 つとして、暗号メッセージ構文において用いられる暗号アルゴリズムへの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、共通鍵暗号に焦点を当て、量子脆弱性を有する暗号アルゴリズムへの影響と対応方針を説明している。

イ．デジタル署名

デジタル署名をメッセージの一貫性確認や認証に使用している場合、そのアルゴリズムが量子脆弱性を有しているならば、CRQC が登場すると、署名検証鍵から署名生成鍵が推定されて署名が偽造され、メッセージの一貫性確認や認証が無効化される可能性があるとしている。また、量子脆弱性を有する署名デジタルによる署名が付与されている電子証明書についても偽造される可能性があると指摘している。

上記のリスクへの対応として、量子耐性を有するアルゴリズムを実装することを推奨している。そうした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みられるアルゴリズム（十分な信頼を得ているとはいえないもの）を既存の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[16]〈hybrid method〉）を推奨している**。双方の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、これらを検証して署名の正当性を判断する[17]。

その他の対応としては、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）を取得・保管する方法を紹介している[18]。

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、その暗号鍵を公

---

16 報告書は、ハイブリッド手法として、組み合わされたアルゴリズムのうち、少なくとも 1 つが安全であれば、その手法によって保護されているデータも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を指している。

17 例えば、いずれかの署名の検証が成功すればその署名を正当とみなす（すべての署名の検証に失敗した場合に限り、その署名を不当なものとみなす）という方法が考えられる。

18 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。

開鍵暗号によって通信当事者間で秘密に共有する形態を前提としている。暗号鍵の主な共有方法として、①通信当事者の一方が暗号鍵を生成し、それを公開鍵暗号アルゴリズムによって暗号化したうえで通信相手に配送する方法（key transport）、②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共通鍵暗号用の暗号鍵の元となるデータ（shared secret）をそれぞれ生成する方法（key agreement）、③鍵カプセル化メカニズム[19]を使用する方法があると説明している。

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、共通鍵暗号用の暗号鍵やその元となるデータが解読されてしまい、最終的に、保護対象のメッセージが盗取される可能性があるとしている。

対応の方針として、報告書は、デジタル署名の場合と同様にハイブリッド手法の採用を挙げている。特に、**HNDL 攻撃[20]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対応が間に合わないと判断される場合には、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、共通鍵暗号用の暗号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〉による手法）を紹介している。

また、報告書は、量子耐性を有するアルゴリズムの多くが鍵カプセル化メカニズムのアルゴリズムであり、NIST の標準化対象になっていることなどから、（上記の key transport、key agreement ではなく）鍵カプセル化メカニズムの採用を推奨している。

ハ．共通鍵暗号

共通鍵暗号への影響に関して、報告書は、公開鍵暗号への影響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現時点での約 2 倍に伸長することを推奨している。

---

19 鍵カプセル化メカニズム（KEM: key encapsulation mechanism）は、公開鍵暗号の使用形態の 1 つであり、送信者は受信者の公開鍵などから暗号文と（共通鍵暗号用の）暗号鍵を生成し、（送信者から暗号文を受信した）受信者は暗号文と自分のプライベート鍵から暗号鍵を生成するという方法で暗号鍵の共有を実現する。

20 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・保管してい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、または、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（イノベーションハブ・ユーロシステムセンター）、フランス銀行、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暗号通信ネットワークに実装・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 月に公表した（Bank for International Settlements, Banque de France, and Deutsche Bundesbank [2023]）。

イ．背景

報告書は、背景として、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の認識を示したうえで、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している。特に、**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、それらのなかでも特にクラウドなどのように金融機関の外部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との認識を示し、早急な対応が必要であるとしている**。このリスクへの対応として、報告書は、量子耐性を有するシステムやネットワークを実現するため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

報告書は、プロジェクト Leap 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上で動作させ、実装性を把握することを挙げている。この実装性は、①暗号アルゴリズムの切替えの容易性（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[21]を変化させた際の処理の可否（セキュリティ〈security〉）という 3 つの特性によって評価されるとしている。

プロジェクトでは、通信ネットワークとして、フランス銀行とドイツ連邦銀行を接続する暗号通信路[22]を使用している。通信当事者は、通信相手を相互に認証した後、公開鍵暗号によって共通鍵暗号（AES）用の暗号鍵を共有し、その暗号

---

21 NIST の標準化対象のアルゴリズムでは、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に必要なセキュリティ・パラメータが各アルゴリズムで決定されている。

22 暗号通信路には、一般に広く使用されている IPsec VPN が採用されている。IPsec VPN は、暗号通信プロトコル IPsec（IP Security）を用いて仮想的な専用通信網（virtual private network）を実現する技術である。IPsec は、通信当事者のそれぞれの通信機器間でデータの暗号化や認証を実現するプロトコルであり、その技術仕様（群）は IETF において標準化されている。

鍵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 の標準化対象のアルゴリズム（CRYSTALS-Kyber、CRYSTALS-Dilithium、SPHINCS+、Falcon）に加えて、ANSSI[23]や BSI[24]が推奨している鍵カプセル化メカニズムのアルゴリズム 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。

上記のアルゴリズムはハイブリッド手法（hybrid mode と呼称）で実装している。その理由として、ANSSI や BSI が、量子耐性を有する暗号アルゴリズムへの完全移行には相応の時間が必要であり、それまでの間はアルゴリズム移行の過渡期として、既存のアルゴリズムとの組合せを推奨していることを挙げている。暗号鍵の共有では、既存のアルゴリズムとして RSA を使用し、量子耐性を有する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、既存のアルゴリズムとして RSA を使用し、量子耐性を有する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は、暗号鍵の共有において、通信当事者間で使用するアルゴリズムを決定する機能が（今回使用した）暗号ライブラリにデフォルトで備わっており、切替えを円滑に実施することができたとして、暗号アジリティが高いと評価している。一方、デジタル署名については、アルゴリズムを識別する機能が暗号ライブラリにデフォルトで設定されておらず、そのままでは認証の処理を実行できないケースが生じ、アルゴリズムを識別する機能の設定を手動で実行する必要があったとしている。これらを踏まえ、手動で対応する場合も含め、暗号ライブラリを適切に設定・実装することによってアルゴリズムの円滑な切替えが可能であったとしている。

処理の速度に関して、暗号通信路のセットアップ（主に認証と鍵共有の処理）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。その結果、暗号通信路のセットアップにかかる時間は、鍵共有・署名ともに既存のアルゴリズム（鍵共有と署名ともに RSA）を使用する場合よりも、量子耐性を有する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としている[25]。暗号化メッセージの通信の

---

23 ANSSI（Agence Nationale de la Sécurité des Systèmes d'Information）は、フランスのサイバーセキュリティ対策を担当する政府機関である（https://www.ssi.gouv.fr/en/mission/what-we-do）。

24 BSI（Bundesamt für Sicherheit in der Informationstechnik）は、ドイツのサイバーセュリティ対策を担当する政府機関である（https://www.bsi.bund.de/EN/Das-BSI/Leitbild/leitbild_node.html）。

25 鍵共有のアルゴリズムに関しては、CRYSTALS-Kyber が FrodoKEM よりも処理速度の面で優

時間は、いずれのケースでも AES を共通に使用したことから、鍵共有や署名のアルゴリズムによらずほぼ一定であったとしている。

処理の安定性に関しては、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、丸一日正常であったとしている。

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ついては、量子耐性を有するアルゴリズムに関して異なるセキュリティ・パラメータのもとで動作させた結果、いずれのパラメータでも処理が適切に実行されたとしている。もっとも、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として、実装時にはセキュリティ・レベルと処理の速度のトレードオフ関係に留意する必要があると説明している。

ニ．アルゴリズム移行に向けた対応と今後のプロジェクト

報告書は、今後、中央銀行やその他の金融機関がアルゴリズムの移行に向けて直面する課題として、自組織における暗号アルゴリズムの使用状況の調査（暗号インベントリの整備）、量子脆弱性を有する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、アルゴリズムの移行が、今回のプロジェクトのような暗号通信路だけでなく、他のさまざまなシステムにおいても求められるとの見方を示したうえで、各種システム向けの新しい暗号プロトコルの開発、関連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している。そして、**こうした各種の取組みに要する時間を十分確保するという観点から、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、報告書は、量子耐性を有するとみられる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 が 2023 年 11 月にイギリスの金融機関向けに公表したペーパー“Minimising the Risks: Quantum Technology and Financial Services”は、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いくつかの用途において大きなメリットをもたらすと期待されている一方で、金融サービスのセキュリティを確保するうえで不可欠な暗号に深刻な影響を与えるリスク[26]があると

れていたとしている。署名のアルゴリズムに関しては、CRYSTALS-Dilithium と Falcon が同程度であったほか、これらと比べると SPHINCS+が劣っていたとしている。

[26] ペーパーは、暗号へのリスクに加えて、①量子コンピュータを使用できる市場参加者（競争上有利な立場を獲得）によって市場の競争が歪められ、市場が不安定化するリスク、②量子コン

指摘している（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こうしたリスクに適切に対処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

ペーパーは、金融機関が各種システムにおいて量子脆弱性を有する暗号アルゴリズムを使用していた場合に、それらが CRQC によって破られることによって生じうる主な事象として以下を列挙している。

① 金融サービスを提供するために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、暗号化された通信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 金融サービスなどで用いられる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署名の偽造などによって無効化され、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ための署名（コード署名）が偽造され、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）上のデータが改変される。

ピュータを適切に活用するために必要なスキルを有する人材が不足し、必要な対応が実施できなくなるリスク、③量子コンピュータに関連する技術に向き合わず場当たり的な対応を継続した結果、最終的に対応を余儀なくされた際に（当初から計画的に対応を進めてきた場合に比べて）大きなコストを負担せざるをえなくなるリスク、④量子コンピュータが不適切な行為のために使用されたり（量子コンピュータによって動作する AI が偏った推論・判定を行うなど）、必要以上に莫大な電力が消費されたりするリスクを挙げている。本稿では、暗号へのリスクに焦点を当てるため、これらについては割愛する。

ロ．金融業界レベルでの検討

上記のリスクに対処するうえで、ペーパーは、**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、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[27]。そして、**こ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。
- 学会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、量子計算技術や暗号技術に関する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

ペーパーは、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、対処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（quantum-safe system）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織り込む。
- 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・投資を必要に応じて実施する。
- 量子計算技術の動向をフォローし、サイバーセキュリティ対策を必要に応じて強化する。

---

[27] 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。移行計画を効率的に策定するために、業界団体、各企業、当局、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。

・　量子計算技術のスキルを有する人材の育成のための訓練・研修のプログラムを実施する。
・　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が 2024 年 1 月に公表したホワイト・ペーパー“Quantum Security for the Financial Sector: Informing Global Regulatory Approaches”は、量子コンピュータによる暗号へのリスクにどのように対処するかについて、当局と産業界の連携や国際協調の重要性を強調しつつ提言している。内容は、金融当局のスタッフや産業界の有識者による会議（世界経済フォーラム主催）での講演や議論の内容、各国の金融当局へのサーベイやインタビューの内容に基づいている[28, 29]（World Economic Forum [2024]）。

イ．政府や産業界におけるリスク対応の現状

ホワイト・ペーパーは、現状について、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の認識を示している。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など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も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）の遅れにつながる可能性があるとしたうえで、それが金融機関のシステム対応に影響を及ぼす可能性を示唆している。

ロ．リスク対応における 4 つの原則

ホワイト・ペーパーは、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。

28　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・対処、金融機関の認可・検査などを行う公的機関である（https://www.fca.org.uk/about/what-we-do/the-fca）。

29　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）の名称がそれぞれホワイト・ペーパーの謝辞に記載されている。

・ 既存の手段や枠組みの活用（reuse and repurpose）：量子コンピュータによる暗号へのリスクに対処するうえで、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。そのうえで、既存の手段や枠組みでは不十分な場合には、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なる要求事項として共に認識している事項を明確化する。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連携・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

ホワイト・ペーパーは、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 4 つのフェーズ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連携・協力体制の確立、リスク対応に必要な作業・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：リスク対応の戦略の実行、暗号の管理方法やシステムの開発プロセスの見直し、脅威やリスクの状況の監視、先行きを見通した対処方法や規制の検討などを実施。

ニ．暗号敏捷アプローチ

ホワイト・ペーパーは、移行・監視フェーズにおける暗号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）に柔軟に対処できるように準備しておく（システムの頑健性を向上させる）ことが重要であるとして、**実装する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従来型のアプローチ（one-size-fits-all approach）ではなく、暗号敏捷アプローチ（cryptographic agile approach）を採用する**ことを推奨している。

暗号敏捷アプローチは、既存の暗号アルゴリズムや暗号ソリューションに問題が発生した場合に備えて、それらを（より高いセキュリティを実現する）別のものに早急に切り替えることができるようにしておくアプローチである。

（５）シンガポール通貨庁による勧告

2024 年 2 月にシンガポール通貨庁が発表した勧告“Advisory on Addressing the Cybersecurity Risks Associated with Quantum”は、金融機関が取り扱う重要なデータが今後 10 年で CRQC による脅威にさらされる可能性があるとしたうえで、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効率的に移行するために、**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]）[30]。

勧告は、金融機関が量子コンピュータによる暗号へのリスクに対処する手段として、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必要性の啓発

- 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。
- 自社の経営層や関係のあるベンダーに対して、潜在的な脅威やそれに対処するうえで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[31]を

---

30 勧告では、リスク低減策の一部として、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、専用のネットワーク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されることを想定している（菅・佐々木［2024］）。

31 提言では明記されていないものの、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・提供されていた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（システムに組み込まれるもの）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、量子耐性を有する暗号アルゴリズムへの切替えができないというリスクにつながる。

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する。

ロ．暗号インベントリの管理と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は、以下の情報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を維持・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データを特定・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。優先順位付けは、システムやデータ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。量子耐性を有する暗号アルゴリズムへの移行などを妨げる制約（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．リスク対応の戦略立案と戦略遂行能力の向上

・ 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情報資産があれば、それに対するリスク低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た対処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・グループが 2024 年 9 月に公表した提言“G7 Cyber Expert Group Statement on Planning for the Opportunities and Risks of Quantum Computing”は、G7 各国の財務大臣と中央銀行総裁に向けて、**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対処するための検討に着手することを推奨している**（G7 Cyber Expert Group [2024]、金融庁［2024］）。

提言は、**大規模な量子コンピュータが登場した場合、それが HNDL 攻撃に悪用され、既存の（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、顧客情報を含む金融機関のデータが盗取され、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。

また、提言は、こうした脆弱性をどのようにして排除するかについて金融業界の関係者（当局も含む）の間で調整するため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としたうえで、**関係者が量子コンピュータによる脅威に対処するための準備をできるだけ早期に整えることが望ましい**との見方を示している。

提言は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、それによる暗号へのリスク、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**：リスク対応に必要なリソースを見積もるために、それぞれ自組織に関係するリスクを適切に評価する。まずは、重要なデータとそれを保護するために使用されている暗号技術に関するインベントリ（暗号インベントリ）を整備する。暗号インベントリの整備やリスクの評価の実施方法に関して、ベンダーと相談するという対応も考えられる。

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、リスクの把握・管理のプロセスにおける主な活動（暗号インベントリの整備など）とそれらの実施時期の検討、リスク対応の優先順位付けなどを行い、それらを盛り込んだリスク低減計画（a plan for mitigating quantum technology risks）を立案する。

提言は、金融当局に対して、金融機関などと協力し、量子コンピュータを用い

た攻撃への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 が 2024 年 10 月に発表した暗号アジリティに関するガイダンス・ペーパー“Building Cryptographic Agility in the Financial Sector”は 2 部構成となっている（Financial Services Information Sharing & Analysis Center [2024]）。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、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。

イ．暗号アジリティとは

ガイダンスは、冒頭で暗号アジリティを次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、ガイダンスは、暗号アジリティを「組織の能力の度合い」として捉えており、**暗号アルゴリズムの切替えという技術的な対応だけでなく、切替えなどを円滑に実現するための組織としての対応も含む概念**として位置付けている。すなわち、暗号アジリティを高めるためには、暗号アルゴリズムの切替えなどに際して実施すべき組織の業務・管理プロセスも整備する必要があるとの考え方を示しているといえる。

ロ．暗号アジリティがなぜ重要か

ガイダンスは、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、ガイダンスは、量子耐性を有するとみられる暗号アルゴリズムの多くが不安定な開発のサイクルにある[32]との見方を示したうえで、（新

[32] ガイダンスは、「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 のウェブサイトのリンク（https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-

しいアルゴリズムのセキュリティに対する信頼が醸成されておらず、）そうしたアルゴリズムの移行の頻度が今後高まる可能性があるとしている。ガイダンスは、従来、「一度移行したらそれでおしまい（once and done）」というスタンスで金融機関は対応してきたが、今後も同様のスタンスで臨んだ場合、移行に必要な時間を十分に確保できない可能性があるとしている。

2 つ目の点に関しては、現在普及している暗号アルゴリズムが長期間にわたって十分なセキュリティを維持するであろうと評価されてきたため、それらがさまざまなインフラやアプリケーションに組み込まれることになったとしている。その結果、暗号アルゴリズム移行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。

ガイダンスは、**暗号アジリティを考慮しないで暗号アルゴリズムの移行を実施することは可能であるものの、そうした対応は、長期的にみて金融業界の安全性（safety）にとって望ましくない**との認識を示している。

ハ.「組織の能力の度合い」をどう把握するか

ガイダンスは暗号アジリティを「組織の能力の度合い」として捉えているものの、「度合い」を表現する具体的な指標は示されていない。「度合い」をどう表現するかを考える際に参考になる視点として次の 3 つを挙げている。

- システムやその構成要素の設計段階での考慮の度合い：暗号アルゴリズムの実装・更新・切替えなどの機能がシステムの構成要素（ソフトウェア、ハードウェア、関連するインフラ）や運用プロセスの設計においてどの程度組み込まれているか。
- 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組み込む前後で、システムのアーキテクチャにどの程度の変更を生じるか。
- 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組込みに際して、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。

---

and-round-4）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アルゴリズムと継続評価対象としたアルゴリズムをそれぞれ発表する内容である。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、標準化がほぼ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。

ニ．暗号アルゴリズムの切替えを円滑に実施する手法

ガイダンスは、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、ガイダンスでは、暗号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と位置付けられている。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、暗号の処理に特化したシステムのみに新しい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においては、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と期待される[33]。ただし、暗号の処理に特化したシステムとの間での通信が発生するなどによって暗号の処理にかかる時間が長くなるほか、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困難になるといった留意点がある。

ガイダンスは、抽象化に基づく個別の手法として、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）、通信路上の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：暗号に関する処理をクラウド上で実現・提供するサービス。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ケースを主に想定。
- 自組織内の暗号ライブラリ：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に関する処理を暗号ライブラリに依頼して処理結果を受け取るケースを主に想定。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。暗号ア

[33] APIを使用するケースにおいて、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考えることができるとしている。また、暗号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、暗号アジリティが高いと考えることができるとしている。

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うえで役立つ。

- 通信路上の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。

（８）金融庁の検討会による報告

2024 年 11 月に公表された「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報告書」は、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．リスクへの対応のポイント

報告書は、エグゼクティブ・サマリーにおいて、量子コンピュータ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。
- PQC のアルゴリズムの実装時期：アメリカ政府が 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。
- 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：移行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**。
- ステークホルダーとの連携：アルゴリズム移行は、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</u>ことが望ましい。

ロ．技術面での課題・留意点

報告書は、技術面での課題や留意点を説明している（報告書の第 6 章）。ポイントを要約すると以下のとおりである。

- <u>暗号アジリティをどのように実現するかが重要な課題</u>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。
- <u>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</u>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、業界団体などと連携して情報の提供を受けることが望ましい。
- 量子耐性を有する暗号アルゴリズムへの移行の過渡期において、<u>移行後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</u>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。
- <u>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</u>ことを基本とし、<u>時間に余裕を持って検討することが重要</u>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、量子コンピュータによる暗号へのリスクに関する検討になるべく早期に着手することが望ましい旨を示している点で共通している。また、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して列挙する[34]と以下のとおりである。

- <u>業界としてのリスク低減計画の策定</u>：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。

[34] 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当局への推奨事項であることからここでは割愛する。

- **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においては、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。
- **暗号アジリティが高いシステムの実現**：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、切替えを円滑かつ効率的に実施するための仕組みや体制を整備しておくことが望ましい。アルゴリズムの切替えが円滑に実施できない場合、金融機関は、移行後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の両方に対応することを比較的長期間余儀なくされる可能性がある。
- **ハイブリッド方式の採用**：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、量子コンピュータによる暗号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。

概ね共通している推奨事項として、量子耐性を有する暗号アルゴリズムへの移行など、リスク低減策の実現には相応の時間とコストが必要になるため、余裕をもって対応するという観点で、暗号インベントリの整備などの事前準備に早目に着手することが挙げられている。特に、長期間保護が必要な情報を取り扱うケースにおいては、HNDL 攻撃への対応の必要性を見極めることが重要であり、リスク評価を早期に実施することが推奨されている。

また、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、その計画と整合的なリスク低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、各金融機関がリスク低減計画をそれぞれフルスクラッチで策定する場合に比べて、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できる。

ただし、日本では、リスク低減計画の策定のための金融機関の連携体制はまだ整備されていない。連携体制の整備には、各金融機関が量子コンピュータによる

暗号へのリスクと対応の必要性を認識することが必要であるが、金融庁の PQC 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 PQC 対応の重要性や緊要性に関してどのように理解を得ていくかが重要な課題である。そのためには、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たうえで、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とともに、対応に必要な作業項目や課題、それらに対処するためにかかる負担や時間を精緻に見積もるなどして、ユースケースに応じた「手触り感」のある分析結果に基づく説明を行うことができるか否かがポイントとなろう。

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が、各金融機関においては、こうした活動に積極的に参加し、リスク対応に関する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。

以　上

【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、2024 年 11 月 14 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、2024 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、2024 年 12 月 10 日）

Accredited Standards Committee X9, Inc., “Quantum Techniques in Cryptographic Message Syntax (CMS), ASC X9 TR 50-2019, Accredited Standards Committee X9, Inc., 2019 (available at https://x9.org/wp-content/uploads/2019/03/ASC-X9-TR-50-2019-Quantum-Techniques-in-Cryptographic-Message-Syntax-1.pdf、2024 年 11 月 5 日).

――――, “Quantum Computing Risks to the Financial Services Industry,” ASC X9 IR-F01-2022, Accredited Standards Committee X9, Inc., 2022 (available at https://x9.org/wp-content/uploads/2022/11/X9F-Quantum-Computing-Risk-Study-Group-IR-F01-2022_20221129-Published-PDF.pdf、2024 年 11 月 5 日).

――――, “Cryptographic Message Syntax (CMS),” ANSI X9.73 – 2023, American National Standards Institute, 2023 (available at https://webstore.ansi.org/standards/ascx9/ansix9732023、2024 年 11 月 5 日).

Bank for International Settlements, Banque de France, and Deutsche Bundesbank, “Project Leap: Quantum-Proofing the Financial System,” Bank for International Settlements, 2023 (available at https://www.bis.org/about/bisih/topics/cyber_security/leap.htm、2024 年 11 月 5 日).

European Commission, “Commission Recommendation of 11.4.2024 on a Coordinated

Implementation Roadmap for the Transition to Post-Quantum Cryptography," European Commission, 2024 (available at https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography、2024 年 12 月 12 日).

Financial Services Information Sharing & Analysis Center, "Preparing for a Post-Quantum World by Managing Cryptographic Risk," Financial Services Information Sharing & Analysis Center, 2023 (available at https://www.fsisac.com/knowledge/pqc、2024 年 11 月 5 日).

————, "Building Cryptographic Agility in the Financial Sector: Effective, Efficient Change in a Post Quantum World," Financial Services Information Sharing & Analysis Center, 2024 (available at https://www.fsisac.com/knowledge/pqc、2024 年 11 月 18 日).

G7 Cyber Expert Group, "G7 Cyber Expert Group Statement on Planning for the Opportunities and Risks of Quantum Computing," U.S. Department of the Treasury, 2024 (available at https://home.treasury.gov/system/files/136/G7-CYBER-EXPERT-GROUP-STATEMENT-PLANNING-OPPORTUNITIES-RISKS-QUANTUM-COMPUTING.pdf、2024 年 11 月 5 日).

Housley, Russell, "Cryptographic Message Syntax (CMS)," RFC 5652, IETF, 2009 (available at https://www.rfc-editor.org/rfc/pdfrfc/rfc5652.txt.pdf、2024 年 11 月 5 日).

Monetary Authority of Singapore, "Advisory on Addressing the Cybersecurity Risks Associated with Quantum," Monetary Authority of Singapore, 2024 (available at https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/mas-quantum-advisory/mas-quantum-advisory.pdf、2024 年 11 月 5 日).

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, "Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography," a Joint Statement from Partners from 18 EU Member States, Bundesamt für Sicherheit in der Informationstechnik, 2024 (available at

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.html、2024 年 12 月 10 日)

UK Finance Limited, “Minimising the Risks: Quantum Technology and Financial Services,” UK Finance Limited, 2023 (available at https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/minimising-risks-quantum-technology-and-financial、2024 年 11 月 5 日).

Wilhelm, Frank K., Rainer Steinwandt, Daniel Zeuch, Paul Lageyre, and Susanna Kirchhoff, “Status of Quantum Computer Development,” Bundesamt für Sicherheit in der Informationstechnik, 2024 (available at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_1.html?nn=916616、2025 年 1 月 16 日).

World Economic Forum, “Quantum Security for the Financial Sector: Informing Global Regulatory Approaches,” World Economic Forum, 2024 (available at https://www3.weforum.org/docs/WEF_Quantum_Security_for_the_Financial_Sector_2024.pdf、2024 年 11 月 5 日).