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

令和 6 年 11 月 26 日

目次

エグゼクティブサマリー

量子コンピュータの実現と普及に伴い、既存暗号技術の危殆化リスクが高まるため、耐量子計算機暗号への移行などのリスク低減策を講ずる必要があるが、その対応には長期にわたり多大なリソースを要するため、経営層がリスクや移行の期限などを正しく認識する必要がある。以下、本文書で記載した、金融機関が対策を適切に推進するうえで留意すべき事項のうち、特に経営層が認識または対処すべき事項の要点を記載する。

- 経営層が果たすべき役割
  - 預金取扱金融機関の経営層が全社(または全組織的)施策としてリーダーシップを発揮し、各システムで利用されている暗号状況や自組織データの重要性及び保存期間等を把握し、適切なリスク評価や優先順位付けした上で、移行方針を決定することが望ましい。(pp.42-43, p.54)
- 対応時期目安について
  - 暗号解読可能な量子コンピュータの登場時期予測は、専門家内でも意見が分かれており時間軸に幅がある一方で、アメリカ政府では 2035 年目途に移行推進している状況から、預金取扱金融機関を対象にした各種法令や海外規制動向に耐量子計算機暗号への移行対応が盛り込まれる可能性がある。(p.16, p.41)
  - 各組織内の優先度の高いシステムは、技術進展や海外規制動向を注視しつつ、2030 年代半ばを目安に耐量子計算機暗号のアルゴリズムを利用可能な状態にすることが望ましい。(p.9, p.48)
- 移行への事前準備
  - 移行に向けた事前準備として、暗号利用箇所やアルゴリズムの棚卸しを実施し、定期的に管理する仕組みが必要であり、そのような仕組みを構築・運用するのに相当の期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。(pp.43-46)
  - 耐量子計算機暗号のアルゴリズムであっても将来的に脆弱性やシステム実装時の課題が発見される可能性があり、段階的な移行や柔軟に暗号切り替え可能な技術の実装を考慮すること(クリプト・アジリティを向上させること)が重要である。(pp.46-48)
  - 具体的には、移行のための基本事項は以下のように整理できる。(p.42)
    - 暗号解読可能な量子コンピュータによる既存の暗号危殆化に関連するリスクに基づいて、移行対象の優先順位付けを行う。
    - 移行対象の詳細な把握のため、クリプト・インベントリを構築する。
    - 暗号危殆化状況に応じて安全かつ迅速に対応できるアーキテクチャを検

討する。

- 優先順位の高いものを中心に移行期限を設定し、期限超過の可能性も踏まえたリスク低減策も検討する。

- ステークホルダーとの連携

・ 移行対応は、自組織単独で完結するものではなく、ベンダーや金融インフラ提供事業者、Fintech 企業などと協働して検討することが重要である。(p.49, p.54)

・ 金融業界においては、政府等とも密に情報連携し、業界としてのロードマップを策定し、共通する課題については協力・分担して対応していくことが望ましい。(pp.50-54)

はじめに

量子コンピュータの実現と普及は、デジタル化された社会において革新的なブレイクスルーを生み出す可能性がある一方で、既存の公開鍵暗号技術を危殆化させ、金融システムへの攻撃リスクを増大させる可能性が指摘されている。そのリスクに対応するため、アメリカの国立標準技術研究所(以下、NIST)において、耐量子計算機暗号(Post-Quantum Cryptography、以下 PQC)に関する研究開発や標準化検討が進められ、2024 年 8 月に新たな暗号アルゴリズムに関する標準化文書が公表された。それにより、IT サービスを提供する事業会社やそれらを利用する事業会社において、既存暗号から PQC への移行に向けた検討が加速していくと考えられる。

このような環境下において、金融庁においても、金融分野について、従前から PQC へ移行する際の留意事項や課題について幅広い関係者と議論を実施してきたが、更に検討を深めるため、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」(以下「本検討会」)が開催された[1]。

本成果物は、2024 年 7 月の初回検討会開催以降、預金取扱金融機関や有識者等で組成された検討会及び作業部会メンバーにおける同年 10 月の第 3 回検討会までの検討結果やベンダーなどの有識者ヒアリング結果に基づき、金融業界にとって参考になるよう、取りまとめられたものである。

[1] 本検討会は行政運営上の意見交換の場として開催されたものであり、法令に基づく審議会等ではない。

1. 背景

預金取扱金融機関の情報システムは、社会生活を支える重要インフラであり、取り扱う情報の漏えい、改ざん等を防ぐための手段として、暗号技術が重要な役割を果たしている。一方、既存のコンピュータの性能向上や、さらには、量子コンピュータの登場により、既存暗号が危殆化するリスクが指摘されている。ただ、2022 年 3 月に公表された CRYPTREC による「暗号強度要件（暗号アルゴリズム及び鍵長選択）に関する設定基準」においては、セキュリティ強度要件強化が提言されているが、既存暗号に関しては、種類に応じて移行期限や設定基準が明示されている一方で、PQC 移行については明示的な期限設定がされていない[2]。また、技術動向や課題についてもベンダー発信による情報が多く、預金取扱金融機関を含む事業者観点で整理された情報が少ない状況である。

そのため、本成果物では、PQC 移行に焦点を絞った上で、預金取扱金融機関のシステムに関わる責任者や経営層が、PQC 全般に関する技術動向や量子コンピュータによるリスク、PQC 移行に関する推奨事項や課題等を正しく理解し、預金取扱金融機関内での移行推進を支援するための参考資料として公開する。また、本成果物は預金取扱金融機関に留まらず、業界横断で PQC に関する正しい情報の共有や理解の促進、リスクベースでの適切な移行等の支援に活用されることを期待する。

2. 耐量子計算機暗号対応について

(1) 量子コンピュータの発展と現在の暗号アルゴリズムへの影響

現代社会において、暗号技術は情報を保護するために広く利用されており、金融機関においても様々な形態で利用されている。しかしながら、将来、一定以上の能力をもつ量子コンピュータが登場した場合には、既存暗号の一部が解読されてしまう（破られる）という脅威が指摘されている[3,4,5]。本章では、暗号解読に利用可能な水準の量子コンピュータ（Cryptographically relevant quantum computer、以下 CRQC）が登場したときに、解読されてしまうおそれのある暗号アルゴリズムはどのようなものか、

---

[2] https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022r1.pdf

[3] https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2019.html

[4] National Security Agency, 'Announcing the commercial national security algorithm suite 2.0. ', U/OO/194427-22, 2022.

[5] Mark Pecen, 'Chairman's report for 2018: ETSI cyber working group for quantum safe cryptography', presentation at ETSI/IQC Quantum Safe Workshop, European Telecommunications Standards Institute, 2018.

またどのような対策をとりうるかについて概説する。

従来から、Shor のアルゴリズム(1994 年発表[6])を量子コンピュータで実行することにより、既存の公開鍵暗号が解読されうることは知られていた。しかし、当該アルゴリズムを実行するための量子コンピュータは存在しなかったため、量子コンピュータによる暗号解読は現実的な脅威としては考えられていなかった。

近年、量子コンピュータ関連技術の進展には目覚ましいものがあるが、現時点でも既存の公開鍵暗号の解読に現実的な脅威をもたらすほどの水準にはない。他方で、近年、ごく小さな特定の合成数に対して素因数分解を実行可能な量子コンピュータが登場したという事実もある[7]。今後、実際に CRQC が登場するに至った場合においては、現在広く利用されている暗号の安全性が低下するだけでなく、公開鍵暗号については現実的な時間で解読されうる[8,9]。

CRQC の登場までにどの程度の期間が必要かについては諸説あり、2030 年から 2050 年[10]くらいに登場するとするものから永遠に完成しないとするものまで存在するものの、CRQC が登場すれば多くの金融サービスに対しても大きな影響を及ぼすおそれが非常に高いと想定されており、また暗号の置き換えには長期間を要することを踏まえると、早急に検討を開始することが望ましいと考えられる。

現代の暗号技術の主要な構成要素として、ハッシュ関数、共通鍵暗号、公開鍵暗号が存在する。NIST の見解(表 2.1 参照)にもあるように、ハッシュ関数や共通鍵暗号においては、より大きな出力や鍵へと変更することにより、CRQC による攻撃に備えることができる。言い換えれば、これらの暗号は量子耐性をもつ暗号であり、所定の情報システムがハッシュ関数や共通鍵暗号のみを利用していた場合は、比較的軽微な変更により、その情報システムを量子耐性のあるものに変えることができる。

他方で、公開鍵暗号を含む情報システムにおいては事情が異なる。RSA、ECDSA、ECDH などに代表される公開鍵暗号は、CRQC の登場によって危殆化するおそれがあ

---

[6] Shor, Peter W., “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” Proceedings of IEEE Annual Symposium on Foundations of Computer Science (FOCS) 1994, IEEE, 1994, pp. 124-134.

[7] https://arxiv.org/abs/1903.00768

[8] Bennett, Charles Henry, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani, “Strengths and Weaknesses of Quantum Computing,” SIAM Journal on Computing, 26(5), Society for Industrial and Applied Mathematics, 1997, pp. 1510-1523.

[9] Brassard, Gilles, Peter HØyer, and Alain Tapp, “Quantum Cryptanalysis of Hash and Claw-Free Functions,” Proceedings of Latin American Symposium on Theoretical Informatics (LATIN) 1998, Lecture Notes in Computer Science, 1380, Springer Verlag, 1998, pp. 163-169.

[10] CRQC に必要な要素技術を実現する量子コンピュータを開発するプロジェクトとしては、JST ムーンショットプログラム「目標６　2050 年までに、経済・産業・安全保障を飛躍的に発展させる誤り耐性型汎用量子コンピュータを実現」が存在する。https://www.jst.go.jp/moonshot/program/goal6/index.html

る。言い換えると、これらの暗号アルゴリズムは CRQC に対して脆弱なものであり、「量子脆弱性をもつ」とも称される。また、危殆化した場合には、暗号鍵をより長いものに変更したとしても十分な安全性を確保できないとされている。公開鍵暗号は様々な情報システムにおいて広く利用されており、その保護対象には、利用者を認証する情報、ファームウェア、デジタルコンテンツ、デジタルコンテンツを暗号化するための鍵、デジタルコンテンツにデジタル署名を付与するための鍵、各種暗号鍵を計算するための情報、電子証明書等が含まれる。これらの情報システムの安全性を維持できなければ、金融サービスの運営に大きな影響を与えるおそれがある。

表 2.1 CRQC の攻撃対象となる暗号アルゴリズム(NISTIR8105 より)

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

(備考)Table 1 – Impact of Quantum Computing on Common Cryptographic Algorithms

一方で、CRQC による攻撃に対しても安全と評価されている PQC アルゴリズムも存在する。代表例は NIST によって 2024 年 8 月に公開された FIPS 203 ML-KEM[11]、FIPS 204 ML-DSA[12]、FIPS 205 SLH-DSA[13] 及び将来 FIPS 206 として公開される予定の FN-DSA[14]が挙げられる。

[11] Module-Lattice-Based Key-Encapsulation Mechanism Standard (nist.gov)

[12] Module-Lattice-Based Digital Signature Standard (nist.gov)

[13] Stateless Hash-Based Digital Signature Standard (nist.gov)

[14] NIST Releases First 3 Finalized Post-Quantum Encryption Standards | NIST

(2) 現在のセキュリティ対策への影響

i. 既存暗号アルゴリズムへの影響

CRYPTREC の 2022 年 3 月のレポートでは、「近い将来に CRYPTREC 暗号リスト記載の暗号技術が危殆化する可能性は低い」[15]とされており、差し迫った将来に CRQC による攻撃が行われることは見込まれていない。また、金融機関においては、様々なセキュリティ対策が多重防御として導入されており、仮に CRQC を用いた攻撃を行うことが可能となった場合であっても、情報システムへの影響が限定的となるシナリオも考えられる。

しかし、Michele Mosca[16]が指摘するように、暗号処理の実装の置き換えに要する期間(図 2-1 中の「暗号システムの移行期間」)をＸ年とし、各データに対する暗号による保護が期待される期間をＹ年としたとき、それらを足し合わせた期間が、CRQC 登場までの期間Ｚ年よりも長い場合(すなわち、Ｘ＋Ｙ＞Ｚ となる場合)は、後述の Harvest Now Decrypt Later (HNDL)[17]攻撃に備えるための検討が必要となる。

また、現在のセキュリティ対策への影響を検討する上では、公開鍵暗号によって直接保護されている情報以外の情報、すなわち、公開鍵暗号によって間接的に保護されている情報に対する影響も考慮する必要がある。

例えば、典型的な暗号通信においては、通信コンテンツは共通鍵暗号により暗号化され、共通鍵暗号の鍵が公開鍵暗号で保護される。ここで、CRQC をもつ攻撃者は、公開鍵暗号部分を攻撃して共通鍵暗号の鍵を得たのちに、その鍵を利用して通信コンテンツを復号するというアプローチをとることが考えられる。そのため、共通鍵暗号部分が量子耐性をもっていたとしても、公開鍵暗号部分が量子脆弱性をもつ場合には、その暗号通信は、全体としては量子脆弱性をもちうる。このような暗号通信を量子コンピュータに対して安全なものにするためには、公開鍵暗号部分を PQC に変更する、または公開鍵暗号に依存しない方法で保護することが必要となる。ただし、公開鍵暗号に依存しない方法を採用した場合、一般に拡張可能性(スケーラビリティ)が低下する点には注意が必要となる。

ii. HNDL 攻撃のメカニズム

HNDL 攻撃とは、事前に暗号技術で保護されたデータを集めておき、後からそのデータに対して攻撃を行うような行為を指す。PQC の文脈においては、CRQC が登場する前に、既存の暗号で保護されたデータを収集・保管しておき、CRQC が登場した後

---

15 https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2019.html

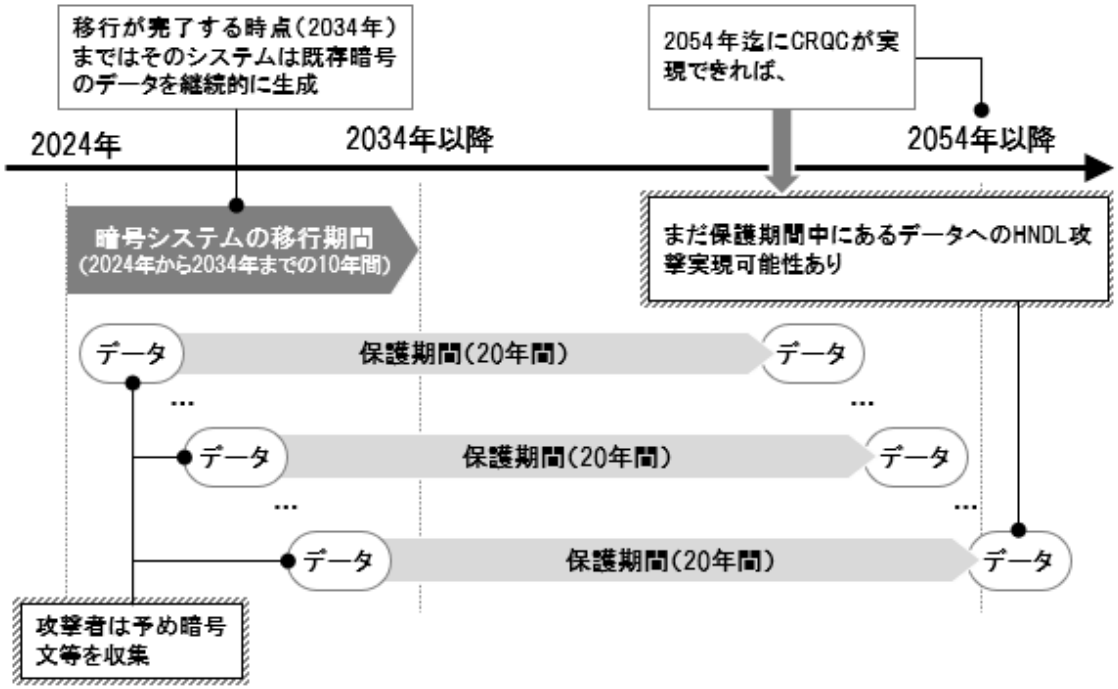
16 Michele Mosca, “Cybersecurity in a quantum world: will we be ready? workshop on cybersecurity in a post-quantum world, ”, workshop on cybersecurity in a post quantum world, Apr. 2015.

17 https://www.nist.gov/cybersecurity/what-post-quantum-cryptography

になって、それらのデータに対して攻撃することが考えられる。このような攻撃が見込まれる場合には、一部の情報システムにおいては、CRQC を利用した攻撃についての備えを相当な時間的猶予を確保して実施する必要がある。

例えば、公開鍵暗号によって保護される所定の情報システムにおいて、暗号アルゴリズム移行に少なくとも 10 年を要し、また公開鍵暗号によって保護される(すなわち、旧来の暗号で保護される)生成データは 20 年保護する必要があるものとする。その場合、その情報システムの公開鍵暗号を PQC へ移行する処理を現時点から行ったとすると、情報システムの移行が完了するのは 10 年後となり、また移行完了の直前に生成された(旧来の暗号で保護された)データを生成時点からさらに 20 年保護することになる。そのため、それらの保護対象のデータに対して特別な移行処理を行わない限り、旧来の暗号による保護を 30 年間維持しなければならないことになる。したがって、そのような旧来の暗号による保護がなされている 30 年のうちに CRQC が登場した場合には、それらのデータは HNDL 攻撃の脅威に晒されることになる(図 2-1 参照)。

図 2-1「配慮が必要」なシナリオ例



(備考)秘匿の必要性や有用性の観点からデータ保護期間が適切に設定されている前提

このように、暗号アルゴリズム移行に長い期間を要する暗号システムや、暗号化データを長期間保護する必要があるシステムでは、それらの期間が長ければ長いほど HNDL 攻撃の脅威に晒されることとなり、同時にそれら期間内に CRQC が登場する可

能性も上昇することになる。他方で、暗号アルゴリズム移行が短期間で完了する暗号システムや、生成される暗号化データの保護期間が短い場合は、そのような脅威は相対的に減少する。CRQC の登場に効率的に備えるためには、このような論点も考慮に入れることが望ましい。

(3) 対策の標準的アプローチ

HNDL 攻撃のリスクを踏まえると、長期間の保護が想定されうる暗号の用途では、以下のような対策に早急に着手することが望ましいケースも存在する。

- コード署名

  情報システムで利用されるハードウェアの中には、容易に入れ替えできないものが存在する。また、それらのハードウェアに対応するソフトウェアの中にも、容易に入れ替えられないものが存在する。ファームウェアに対するコード署名は、上記のような理由から入れ替えが困難となる事も考えられるため、その場合は公開鍵暗号以外の保護手段も視野に入れて対応を行うことが望ましい。
- TLS 通信におけるハンドシェイクの暗号化

  TLS 通信では、様々な暗号に利用され、その情報の中には保管期間が長いものと短いものが混在することも考えられる。ここで、特定の情報のみ異なる処理を行うことは容易ではないと考えられ、保存期間の長短や、情報の価値に関わらず、同じように処理されることも想定される。そのため、TLS 通信の鍵共有[18]に対しては優先して対応することが望ましい。

現状においては、量子コンピュータの開発の見通しに不透明な点も多く、革新的な技術発展が起こりうることも考慮すると、HNDL 攻撃が可能となる時期を推測することは困難である。そのため、CRQC の登場時期を予想した上でのリスク評価や、ある程度正確な費用対効果を計算した上での移行計画の立案は極めて困難となる。PQC を使用可能にするタイミングの設定においては、アメリカ連邦政府の PQC 移行のタイムラインで示されているように(第 3 章(2)i(ア)を参照)、各国の対応動向等の社会的動向を踏まえて 2030 年代半ばと設定するのが妥当と考えられる。

次に、対策手段について検討する。量子コンピュータによる暗号解読の脅威への対応はいくつか考えられるが、最も汎用的かつ根本的な対応は、既存の公開鍵暗号アルゴリズムを PQC に置き換えることである。代表的な PQC アルゴリズムとしては、

---

[18] HNDL 攻撃は TLS の鍵共有に対しては効果的であるが、認証に対してはほとんど影響がないと考えられる。

前述(1)でも挙げたように、ML-KEM、ML-DSA、SLH-DSA 及び FN-DSA がある。また、公開鍵暗号による鍵共有のかわりにインターネットではない別のチャネルによって乱数(共通鍵暗号の鍵)を配送するなどの方法が考えられる。ただし、既存の全ての鍵共有にこれを適用することは非現実的であり、事前に、HNDL 攻撃による許容できないリスクが存在する情報を見極めることが必要である。

i. 課題

PQC への暗号移行は根本的解決となるものの、いくつかの課題も存在する。以下、検討することが望ましい課題について列挙する。

- システムの暗号移行には長い期間を要する

  大規模システムにおける暗号移行は、一般に時間が掛かり、移行に要するコストも増加しがちである。これは、機器やソフトウェアを切り替えるには時間が掛かること、運用やデータ管理に係る様々な処理も併せて移行する必要があること、移行期間中に対象となる情報システムを停止することが出来ない場合においては旧来のシステムを運用しつつ、段階的に移行する必要があること等が影響するためである。ソフトウェアやシステム間に複雑な依存関係が存在する場合にはさらに長い時間を要することもある。

  仮に、暗号移行の対象となる情報システムが、他のシステムに与える影響の少ない独立したものであり、暗号アルゴリズムの切り替え中にシステムを停止しても問題がないようなものであれば、比較的短期間での暗号移行が可能となるかもしれない。しかしながら、そうではない多くの情報システムの暗号移行については、時間を掛けて実施する必要があり、多くの金融機関のシステムにおいても長期間を要すると考えられる。

  なお、情報システムに関連するステークホルダーが多い場合や、特定の国際標準等に準拠することが必要な場合は、それらの調整にも時間を要する場合がある。
- PQC は従来の暗号アルゴリズムに比べて、より多くのリソースを要求しうる

  PQC は従来の暗号アルゴリズムに比べて、通信量や計算量が増加することも移行における課題となる。PQC は、暗号鍵のデータ量、デジタル署名のデータ量、必要とする計算量のうち、少なくとも 1 つ以上で、既存の公開鍵暗号アルゴリズムに比べて多くのリソースを消費する。これに起因して、例えば現状の TLS 通信[19]の Server Hello においては、ペイロード[20]のデータ量の制限から、

[19] Eric Rescorla, “The transport layer security (TLS) protocol version 1.3, ”IETF RFC 8446, 2018.

[20] 当該メッセージにおける、コンテンツデータを積載可能な領域。

PQC 用のサーバ認証用証明書を単一のペイロードに格納できないという課題が指摘されている[21]。また、計算量の増加やハードウェアアクセラレーション回路の不備等に伴って、単一の Web サーバが同時に処理可能なコネクション数が減少するおそれがある。これらの課題に対応するためには、前者はプロトコル仕様の変更、後者はより性能の高いハードウェアへの置き換え等を行うことが考えられる。これらの置き換え処理は、一般にある程度の時間を要すると考えられる。

なお、情報システムが標準プロトコルを利用していない場合においては、プロトコル設計や相互運用性の確認等も自社で行うことになり、移行に要する時間はさらに長くなることには注意が必要となる。他方で、機器が暗号回路を含むファームウェアアップデートをオンラインで実施できる場合においては、移行に要する時間は比較的短くなることが期待される。

- PQC 移行中は、脆弱性等への対応が遅れる可能性がある

  PQC への移行の実施中に、別の課題が発生するおそれがある。PQC への移行の実施中に、例えば、何らかのセキュリティホールが発見されることが考えられるが、仮に PQC への移行が完了しない限りセキュリティパッチが適用できない状況であったとすると、PQC への移行が完了するまでは当該セキュリティホールを放置することを余儀なくされることになる。

- PQC 移行後または移行実施中に PQC 自身に問題が発生する可能性がある

  PQC への移行完了後または移行実施中に、PQC アルゴリズムが危殆化するおそれがある。ML-KEM、ML-DSA、SLH-DSA 及び FN-DSA は、NIST による慎重な選考プロセスの結果、標準化された暗号アルゴリズムであり、相当の信頼性をもつものと期待される。しかしながら、過去には、有望と期待されていた暗号アルゴリズムに深刻な脆弱性が発見されたこともある。上記の NIST によって標準化された PQC アルゴリズムが、RSA や ECDSA 等の既存暗号アルゴリズムよりも早く危殆化する可能性は否定できない。そのようなリスクも踏まえ、PQC 導入後の数年間は、いつでも既存のアルゴリズムに戻せる体制で運用を行うアプローチも考えられる。

ii. 標準的アプローチ

前述のような課題に対応するためには、暗号アルゴリズムの変更をより迅速にできる(すなわち、よりクリプト・アジリティの高い)情報システムにシフトさせていく施策が効果的であると考えられる。クリプト・アジリティを上昇させる方法は様々であるが、代表的なアプローチは、以下(全てもしくは一部を組み合わせたもの)となる。

---

[21] Mike Ounsworth, “PQC at the Internet Engineering Task Force (IETF), ” Post-Quantum Cryptography Conference, Ottawa, Canada, Mar. 2023.

- 暗号回路部分をモジュール化し、入れ替え可能なように設計しておく。
- 暗号をハードコードするのではなく、ソフトウェアで変更できるようにしておき、可能であればオンラインでファームウェアアップデートを行えるようにしておく。
- 多機能なモジュールは、個別にアップデート可能な単機能のモジュールに分離できるようにする(シンプルな機能のみをもつモジュールは、より多機能なモジュールより入れ替えやすい傾向にある)。異なる機能をもつモジュールが同じ暗号鍵を使いまわしており、それらのモジュールを分離することが難しい場合は、異なる暗号鍵を利用するようにする。
- 迅速な移行の阻害要素となる処理の自動化を行う。これは、人の介在を減らすことにより、より迅速な移行を行えるようになることを意図したものとなる。なお、法令や業界基準等により自動化できない処理も存在しうることには注意されたい。
- 情報システム内の機器やソフトウェアが利用中である暗号アルゴリズム及び利用可能な暗号アルゴリズムを整理しておく。所定のアルゴリズムの変更が必要となった際に、その暗号アルゴリズムを利用している機器やソフトウェアを検索できるようにしておく。
- 機器のライフサイクル管理を行う。所定の期間内にファームウェアアップデートを行う。ファームウェアアップデートを行わずに所定の期間が過ぎた機器は置き換える。
- データのライフサイクル管理を行い、所定の期間が過ぎた情報は公開/破棄/アーカイブ等を行う。
- 前述2つのケース(すなわち、機器及びデータのライフサイクル管理)において、「所定の期間」を短縮する。
- 電子証明書のライフサイクル一元管理や自動的な更新ができるように管理プラットフォームなどの活用を進める。

上記のような施策を事前に行うことで、より短期間で暗号移行を行うことが期待でき、それにより、移行に要する各種コストを削減することが可能となる。事前に十分に移行コストを削減させ、その後に必要な情報システムのみを PQC へ移行することで、費用対効果の高い対策の実施が可能になると考えられる。

また、優先順位を付けた上で対策を行うことも重要であると考えられる。多くの金融機関は、多様な情報システムを管理しており、全ての情報システムの暗号を移行するには、相当の期間とリソースを要する。優先順位の設定においては、以下のようなアプローチが存在する。

- 特に重要な情報を扱うシステムから優先して移行を行う。

- 重要かつある程度以上の期間、機密性あるいは完全性を保持する必要がある情報を扱うシステムから優先して移行を行う。
- 時間の経過とともに情報の価値が下がることも優先順位を決定する際の考慮に入れる(例えば、有効期間の短い認証情報に対する攻撃価値は、有効期間の長い認証情報に対する攻撃価値と比較して小さい。また、将来の事業戦略、価格設定等に関する情報の価値は時間の経過とともに相当程度陳腐化すると考えられる。他方で、本人と紐づけ可能な希少な遺伝子情報は、その人物の存命中のみならず、将来的に価値が上がることも考えられる。)
- 多重防御で既に保護されている情報よりも、不特定多数の利用者がアクセス可能となる情報の保護を優先する。

(4) 暗号移行に向けた事前準備

前章でも述べたが、CRQC への対策は相当の期間とリソースを掛けて行われることになる。そのため、暗号移行を行うに当たっては、その移行ができる限り短期間で実施可能となるような準備を整えた上で、適切な優先順位の下、管理を行うことが望ましい。

優先順位の管理の精度を上げ、より良い移行計画を立案するためにも、自社のもつ機器やソフトウェア等の IT 資産を棚卸しして検索可能な状態とすること、すなわちインベントリ管理が重要であると考えられる。情報システムをインベントリ管理する仕組みを既に保有している場合は、管理対象の情報に、利用する暗号アルゴリズム及び利用可能な暗号アルゴリズムを追加することでクリプト・インベントリを構築するアプローチも考えられる。

上記を踏まえて、CRQC 対策においては、全ての情報システムに単純に PQC への移行を実施するのではなく、実施対象とすべき情報システムを事前に洗い出した上で、移行の必要性が高いシステムを優先し、以下の項目について並行して対処することが効率的だと考えられる。

- 量子技術の発展状況の把握
- クリプト・インベントリ管理の構築・管理
- リスクアセスメント
- クリプト・アジリティの向上
- 優先順位の管理の検討
- 計画の立案

3. 国内外の対応状況

(1) 標準化動向

i. NIST(アメリカ)

NIST が 2016 年 2 月に PQC の標準化計画を発表して以来、数十件の PQC が標準暗号の候補として提出され、その中から4つの暗号アルゴリズムが選定された[22]。そのうち、FIPS 203 ML-KEM[23]、FIPS 204 ML-DSA[24]、FIPS 205 SLH-DSA[25]は 2024 年 8 月に公開され、FN-DSA も、FIPS 206 のドラフト版として近日中に公開予定である。これらの暗号アルゴリズムの提案者は、当該標準を実装する用途に関しての知的財産権の権利不行使等も要求されている。また、NIST は当該標準を実装する上での知財リスクの排除も標準化プロセスの過程で実施している[26]。これらの暗号アルゴリズムは十分な安全性をもつと期待されているものの、ML-DSA と FN-DSA は、いずれも格子に基づくデジタル署名となる。格子に基づくデジタル署名は比較的新しい暗号体系に属する技術であることから、それらが一斉に危殆化するリスクも考慮し、NIST は新たに PQC 署名アルゴリズムの選考を 2022 年に開始し[27]、2024 年 10 月、40 の候補アルゴリズムのなかから 14 のアルゴリズムに絞り込んだ旨を発表した[28]。なお、NIST は ML-KEM については代替となるアルゴリズムを追加募集する予定はなく、また SLH-DSA は性能面の制約から広く利用する署名アルゴリズムとみなされていない模様である[29]。

ii. CRYPTREC(日本)

CRYPTREC では、PQC について、2022 年度に「CRYPTREC 暗号技術ガイドライン(耐量子計算機暗号)[30]」及び「耐量子計算機暗号の研究動向調査報告書[31]」を発行している。いずれのドキュメントも PQC の代表的な候補である 5 種類の分類(すなわ

---

[22] https://csrc.nist.gov/PQC-standardization

[23] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

[24] https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.204.pdf

[25] https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.205.pdf

[26] NIST は、これらの暗号を使う上で障害となりうる関連特許の調査の実施及びアメリカ内での利用に関する調整を完了している。日本で使用する場合においても、当該標準の実装に関連する特許が存在する可能性があり、それによる知的財産権の侵害リスクが存在しうることは否定できない。

[27] NIST Announces Additional Digital Signature Candidates for the PQC Standardization Process | NIST

[28] https://csrc.nist.gov/pubs/ir/8528/final

[29] slides-120-pquip-nist-PQC-standards-00.pdf (ietf.org)

[30] https://www.cryptrec.go.jp/report/cryptrec-gl-2004-2022.pdf

[31] https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2022.pdf

ち、格子に基づく暗号技術、符号に基づく暗号技術、多変数多項式に基づく暗号技術、同種写像に基づく暗号技術、ハッシュ関数に基づく署名技術)について調査し、主に2022 年 9 月 30 日までの調査結果をまとめたものである。前者のガイドラインは暗号初学者を、後者の調査報告書は暗号についての知見のある技術者や専門家をそれぞれ対象とするなどの違いがある。

ガイドラインの第 1 章には PQC の必要性や標準化等の動向が、第 2 章には暗号初学者向けに PQC の活用方法に関する内容、特に守秘・鍵共有・署名のための PQC の利用などが記載されている。なお、PQC への移行方針などについての直接的な記載はなされていない[32]。

iii. IETF

Internet Engineering Task Force(IETF)では、暗号技術が組み込まれたインターネット上の様々な通信プロトコルなどの標準化が行われている。PQC への移行においては、こうした通信プロトコルを PQC に対応させて標準化することが必要になる。IETF では、複数のワーキンググループ(pquip wg, lamps wg, tls wg, ipsecme wg, cose wg 等)において、各種プロトコルなどにおける PQC を組み込んだ標準化が検討されている。中でも pquip(Post-Quantum Use in Protocols) wg は、様々な課題の交通整理を行う場としても機能している。

IETF における議論は、CMS(Cryptographic Message Syntax)で PQC を使うための準備、CMP(Certificate Management Protocol)にて PQC を使うための準備、TLS を CRQC に対して安全にする方法、PQC に関する用語整理等が含まれており、多数のインターネット標準(RFC)の整備も急速に進展しつつある。

(2) 政府・当局

各国・各地域における CRQC による公開鍵暗号アルゴリズムのリスクへの対応方針をみると、PQC のアルゴリズムへの移行を柱とするものが大勢である。具体的には以下のとおりである[33]。

---

[32] CRYPTREC シンポジウム 2024「暗号技術評価委員会活動報告（2023 年度～2024 年度)」(2024 年 9 月 2 日）に、「2024 年度までに新たな耐量子計算機暗号の調査報告書・ガイドラインを作成」(p24)

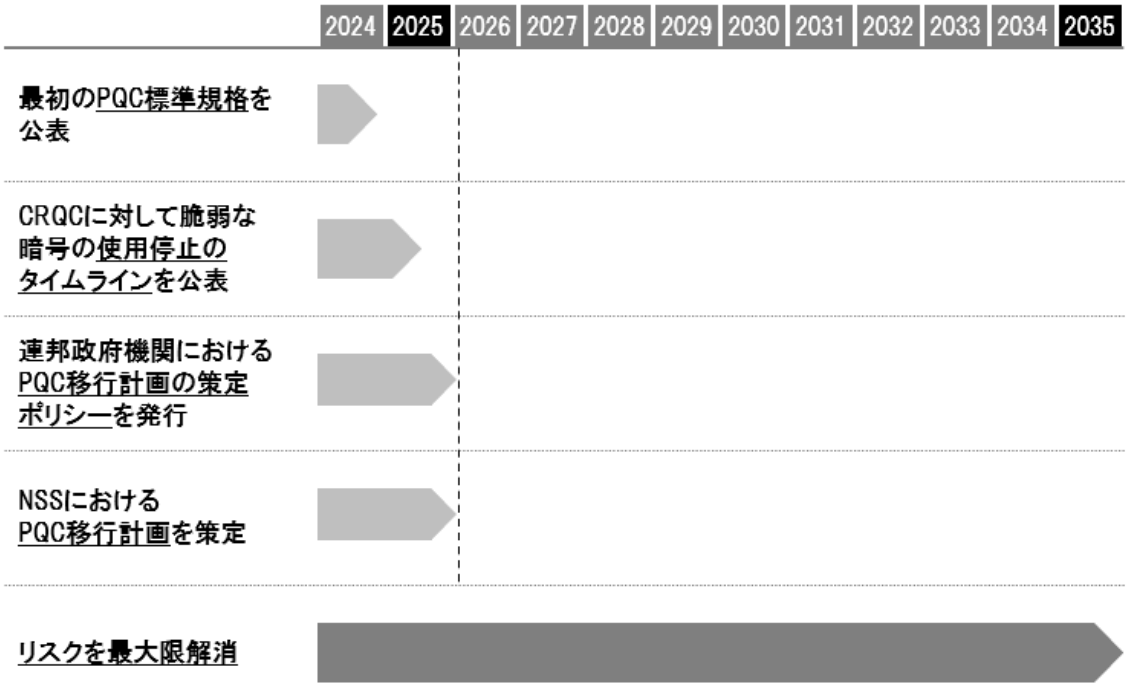
[33] 日本では、自由民主党政務調査会デジタル社会推進本部が 2024 年 5 月に「サイバーセキュリティ対策の更なる強化に向けた提言」(https://www.jimin.jp/news/policy/208287.html) を発表した。そのなかで、PQC 対応のための政策パッケージの策定を提言しており、「PQC 対応のための行動計画（仮称)」を策定することが含まれている。行動計画に織り込む項目としては、①わが国全体を視野に入れた「移行計画（ロードマップ)」、②企業向けの「PQC 対応ガイドライン」、③推進主体の明確化と必要な人員・権限の強化、④移行推進に当たって必要な支援策、⑤国際標準化・海外展開の支援が挙げられている。

i. アメリカ

(ア)連邦政府における PQC 移行の計画とタイムライン

アメリカ連邦政府は、量子コンピュータによる産業競争力向上とそれによる現在の暗号アルゴリズムのリスクをバランスさせるために、連邦政府機関における国家安全保障に関わるシステム(NSS: National Security Systems)などに PQC のアルゴリズムを導入して 2035 年までにリスクを最大限解消する方針とタイムライン(図 3.1 参照)を、2022 年 5 月に発表した[34]。これによれば、アメリカ連邦政府は、2025 年に、現在の暗号アルゴリズムの使用停止のタイムラインの公表、各システムにおける PQC のアルゴリズムへの移行の計画を策定する予定である[35]。

図 3.1 アメリカ連邦政府における PQC 対応のタイムライン



(備考) National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (May 2022) をもと

[34] 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

[35] NIST は、2024 年 11 月、量子脆弱性を有するアルゴリズムから PQC アルゴリズムへの移行の方針を示す技術文書のドラフト（NIST IR 8547 ipd）を発表した（https://csrc.nist.gov/pubs/ir/8547/ipd)。本技術文書は移行のタイムラインも示しており、RSA や楕円曲線暗号の使用期限を 2035 年末（disallowed after 2035）としている。

に作成。

PQC のアルゴリズムとして採用されるものについては、NSA（National Security Agency）が、2022 年 9 月、PQC のアルゴリズムを含む CNSA 2.0（Commercial National Security Algorithm version 2.0）を発表した（表 3.1 を参照）[36]。

CNSA は、国家安全保障に関わるシステムで使用される機器に搭載する暗号アルゴリズムの組合せであり、現在採用されているバージョン 1.0 からバージョン 2.0 に移行されることになる。CNSA 2.0 は、PQC のアルゴリズムとして、鍵共有アルゴリズムに CRYSTALS-Kyber（FIPS 203: ML-KEM）が採用されているほか、署名アルゴリズムには CRYSTALS-Dilithium（FIPS 204: ML-DSA）、ソフトウェアやファームウェア向けのコード署名のアルゴリズムとして、LMS あるいは XMSS（NIST SP 800-208）が採用されている。

表 3.1　NSA の CNSA 1.0 と 2.0

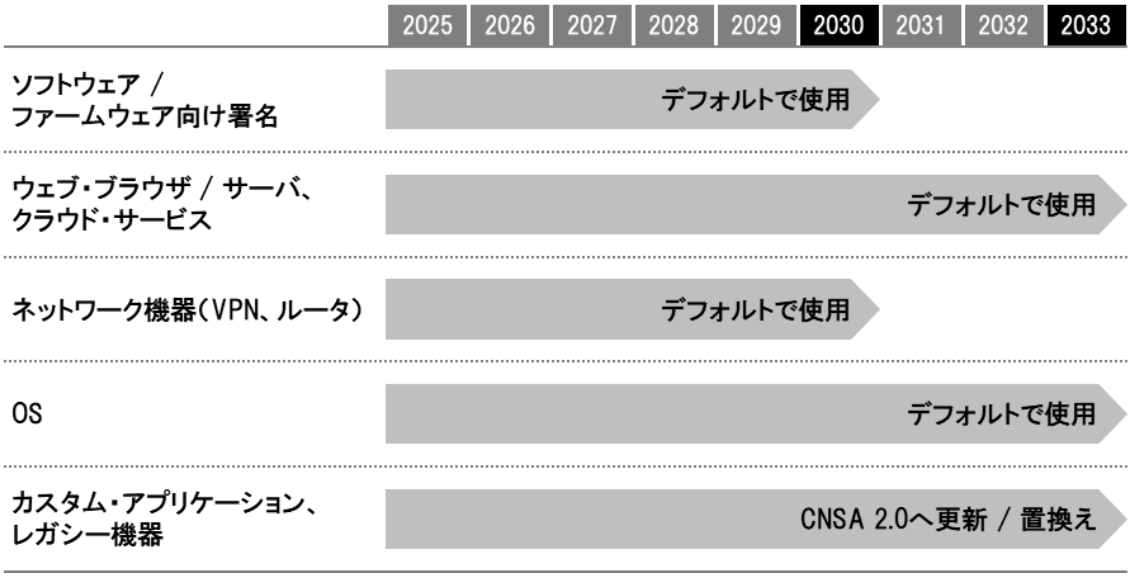
	CNSA 1.0	CNSA 2.0
ブロック暗号	AES-256	AES-256
ハッシュ関数	SHA-384	SHA-384 or SHA-512
鍵共有	RSA-3072 or ECDH P-384	*CRYSTALS-Kyber (level V)*
デジタル署名	RSA-3072 or ECDSA P-384	*CRYSTALS-Dilithium (level V)*
ソフトウェア / ファームウェア向けの署名		*LMS or XMSS (LMS: SHA-256/192 recommended)*

（備考）Announcing the Commercial National Security Algorithm Suite 2.0 (September 2022)をもとに作成。下線部が変更されたアルゴリズムであり、イタリックが PQC のアルゴリズム。

また、NSA は、CNSA 2.0 の発表と同時に、それを搭載する予定の各種暗号製品の調達可能時期についてもベンダーに向けてタイムライン（図 3.2 参照）も発表した。これによれば、概ね 2033 年までに、全ての（調達対象の）暗号製品においてデフォルトで CNSA 2.0 のアルゴリズムを搭載することを求めている。また、カスタマイズされたアプリケーションやレガシー機器についても、2033 年までに、それぞれのベンダーに対して CNSA 2.0 のアルゴリズムを搭載するよう求めている。

[36] https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.pdf

図 3.2　CNSA 2.0 搭載の暗号製品の調達可能時期に関するタイムライン



（備考）Announcing the Commercial National Security Algorithm Suite 2.0 (September 2022) をもとに作成。

（イ）NIST が標準化した PQC のアルゴリズムの性能及び相互運用性のテスト

NIST は、CRYSTALS-Kyber、CRYSTALS-Dilithium、Falcon、SPHINCS+などを実装している暗号製品を用いて、暗号プロトコルの性能や、異なる暗号製品間の相互運用性の評価をベンダーと連携して実施し、2023 年 12 月、結果を NIST SP 1800-38C として公表している[37]。対象となったのは、TLS 1.3、SSH、QUIC、X.509 証明書、ハードウェア・セキュリティ・モジュールであり、これらを実現する暗号製品をいくつかを選択してテストを実施した。

TLS のテストでは、IETF が TLS 1.2 のメンテナンスを実施しない（frozen）という方針を示していることなどに基づいて、TLS 1.3 のみを対象とした。テストはハンドシェイク[38]に関して実施された。鍵共有は、①PQC のアルゴリズム（CRYSTALS-Kyber）のみ使用する場合と、②PQC のアルゴリズムと ECDH を組み合わせて使用する場合（ハイブリッド方式）がそれぞれ対象となった。デジタル署名による認証は、③ECDSA を用いる場合と④PQC のアルゴリズム（CRYSTALS-Dilithium など）を用いる場合がそれぞれ対象となった。

---

[37] NIST SP 1800-38C (draft): Migration to Post-Quantum Cryptography Quantum Readiness: Testing Draft Standards, 2023 (https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf)

[38] 暗号通信を開始する準備として、通信当事者間で、使用する暗号アルゴリズムの決定、セッション鍵の共有、通信相手の認証などを実施する処理のこと。

性能に関しては、1 秒間に実行されたハンドシェイク数で比較したところ、CRYSTALS-Kyber が ECDH よりも高速であった(デジタル署名には ECDSA を使用)。また、ハイブリッド方式では、ECDH 単独の場合よりも低速であったほか、速度低下の度合いは暗号ライブラリによって区々であった。

相互運用性に関しては、通信当事者間で使用した暗号製品における TLS 1.3 の実装形態[39]が異なっている場合、通信できない場合があることが判明した。

(ウ)量子コンピュータの脅威が国家の重要な機能に及ぼす影響の分析

国土安全運用分析センター(HSOAC:Homeland Security Operational Analysis Center[40])は、2022 年、「国家の重要な機能における新たなリスクの分析(National Critical Function Emerging Risk Analysis: Assessments of Quantum Computing Vulnerabilities of National Critical Functions)」と題するプロジェクトの報告書を公表している[41]。このプロジェクトは、サイバーセキュリティ・社会基盤安全保障庁(CISA:Cybersecurity and Infrastructure Security Agency)を支援するために実施されたものであり、量子コンピュータが国家の重要な機能に与えうる影響やそれによる問題に関して、CISA が理解を深めることを支援するとともに、それらの機能の運営主体へのアメリカ連邦政府の支援に関して、CISA による優先順位付けの支援を行うことを主な目的としている。

報告書では、国家の重要な機能を 55 のカテゴリーに分けたうえで、量子コンピュータによる脅威、脆弱性の度合い、リスクの大きさ、それぞれのカテゴリーにおける脆弱性の度合いを分析した結果が示されている。分析結果は、主に、各機能の運営主体に求められる脆弱性対応の緊急度(urgency)、脆弱性対応に関わる組織の範囲の広さ(scope)、脆弱性対応に必要なコスト(cost)、連邦政府による支援の優先順位(priority for assistance)によって示されている。

報告書によれば、脆弱性対応の緊急度が高い(high)と評価されているのは以下のとおりである。

- インターネットベースのコンテンツ・情報通信(Provide Internet Based Content, Information, and Communication Services)
- 衛星による通信(Provide Satellite Access Network Services)
- 無線アクセス通信(Provide Wireless Access Network Services)

---

[39] アルゴリズム識別子、鍵シェア (key_share)、アルゴリズムの選択方法など。

[40] HSOAC は、国土安全法 (Homeland Security Act) に基づいて国土安全保障大臣によって認可・設置された連邦研究開発センター (federally funded research and development center) であり、国土安全に関する問題の調査・分析を担っている。

[41] https://www.rand.org/pubs/research_reports/RRA1367-6.html

- 法執行(Enforce Law)
- 医療記録へのアクセス(Maintain Access to Medical Records)
- 機密情報の保護(Protect Sensitive Information)
- 公衆衛生支援(Support community health)
- 情報技術製品・サービス(Provide Information Technology Products and Services)
- 防衛産業への物資・運用支援(Provide Material and Operational Support to Defense)

金融関連の機能に関しては以下が挙げられており、いずれも緊急度は中位(medium)または低い(low)と分析されている。

- 資本市場や投資行動(Provide Capital Markets and Investment Activities)
- 商業銀行(Provide Consumer and Commercial Banking Services)
- 資金提供・流動性供給(Provide Funding and Liquidity Services)
- 決済(Provide Payment, Clearing, and Settlement Services)
- 保険(Provide Insurance Services)
- 大口資金提供(Provide Wholesale Funding)

金融関連の機能における緊急性に関するこうした評価の背景として、報告書では、金融サービスが攻撃の対象となる可能性が高いとしつつも、金融業界が連邦政府による規制のもとでセキュリティ対策を既に講じており、具体的な攻撃手法が成功する可能性が比較的小さいと考えられることや、金融業界が PQC アルゴリズムの実装を促進するための活動を先行して進めていることを挙げている[42]。

ii. 欧州

(ア)欧州連合

A. 欧州委員会

---

[42] 金融分野と他の重要インフラ分野との間には相互に依存関係が存在し、PQC 対応を検討する上でその関係性を考慮することが重要である（第 5 章（5）i を参照)。例えば、金融機関は、業務遂行のために様々なステークホルダーや自組織内部で通信サービス（IPsec-VPN 等も含む）を利用しているが、これは前脚注の報告書において「緊急度が高い」と評価されている「インターネットベースのコンテンツ・情報通信」サービスに該当する。こうした他の重要インフラ分野の対応状況は金融分野における対応にも影響を与えかねないため、依存関係にある他の重要インフラ分野との間で情報共有等の連携を進めていくことが望ましい。

欧州委員会は、2024 年 4 月、各加盟国に対し、PQC のアルゴリズムへの移行の検討を促す勧告「Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography」を発した[43]。具体的には、PQC のアルゴリズムへの移行の戦略を立案することを求めており、2 年以内に、加盟国間で調整を行ったうえで移行のロードマップを完成させることを要請している。また、欧州域内の専門家や関係機関と連携し、PQC のアルゴリズムの評価や欧州標準仕様の策定を行うことも促している。

勧告では、PQC 移行のための戦略の検討に関して、各加盟国とそれらの公的部門において同期のとれた移行(synchronized transition)を実現する内容とするとともに、PQC 移行の中間目標やタイムラインを明確に設定することが望ましいとしている。こうした戦略の立案・調整を行う主体として、EU 域内のネットワークや情報システムにおけるセキュリティ対策の企画・調整を担当する NIS Cooperation Group 内にサブグループを新設し担当させることを推奨している。本サブグループでは、各加盟国のセキュリティ当局の代表者、サイバーセキュリティ分野の専門家がメンバーとして参画するとともに、行政やその他の重要インフラ(public administrations and other critical infrastructures)における PQC 移行関連の取組みについて情報共有や調整を促す観点から、ステークホルダーである公的組織や産業界の代表者も参画することが考えられるとしている。このほか、同様の検討を他の組織でも実施することを回避するために、Europol や NATO といった他の関連組織とも議論することを推奨している。

B. ENISA

欧州連合におけるサイバーセキュリティ政策の企画・実施を担当する ENISA (European Union Agency for Cybersecurity)は、2022 年 10 月、PQC のアルゴリズムに関する研究開発動向の調査報告書「Post-Quantum Cryptography: Integrated study」を公表した[44]。

この調査報告書では、PQC のアルゴリズムの分類、セキュリティや性能の評価結果、PQC のアルゴリズムを用いる暗号プロトコルや情報システムの研究開発の動向、暗号プロトコルの標準化動向などが紹介されている。

(イ)イギリス

イギリスのセキュリティ当局である NCSC(National Cyber Security Centre)は、PQC のアルゴリズムへの移行に関するガイダンス「Next Steps in Preparing for Post-

[43] https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography

[44] https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

Quantum Cryptography」(アップデート版)を 2024 年に公表した[45]。

ガイダンスでは、価値の高いデータを公開鍵暗号アルゴリズムによって長期間保護する場合、CRQC による HNDL 攻撃が現時点で大きな脅威になっているとの見方を示している。そのうえで、このリスクへの対応として、PQC のアルゴリズムへの移行が最も望ましいとしており、採用する PQC のアルゴリズムとして、NIST が標準化したアルゴリズムを推奨している。具体的には、鍵共有アルゴリズムとして ML-KEM、汎用目的の署名のアルゴリズムとして ML-DSA、ファームウェアやソフトウェアのコード署名用の署名アルゴリズムとして、SLH-DSA、LMS、XMSS を挙げている。

これらのアルゴリズムを使用する際の留意点として、ドラフト段階の仕様を実装する暗号製品ではなく、標準化が完了した仕様を実装しているもののみを採用することを推奨している。また、上記のアルゴリズムを使用する暗号プロトコルについても、IETF において標準化が完了した RFC を実装したものを採用することを推奨している。さらに、現在の暗号アルゴリズムと PQC のアルゴリズムを組み合わせるハイブリッド方式を採用する場合には、ハイブリッド方式の採用を過渡的なものとして位置付けたうえで、将来の PQC のアルゴリズムのみの実装への移行を速やかに実現できるようにしておくことを推奨している。

(ウ)ドイツ

ドイツのセキュリティ当局である BSI(Bundesamt für Sicherheit in der Informationstechnik)は、2021 年、PQC のアルゴリズムへの移行のガイドライン「Migration to Post Quantum Cryptography, Recommendations for action by the BSI」を公表した[46]。

ガイドラインでは、今後、長期的にみると、PQC のアルゴリズムが広く採用されるとの見方を示したうえで、適切なリスク管理手法に基づいて PQC のアルゴリズムへの移行の必要性や時期の検討に着手することを推奨している。また、ハイブリッド方式を採用することや、PQC のアルゴリズムへの移行を円滑に実施できるようにする(クリプト・アジリティの向上)ために情報システムの構成を見直すことを推奨している。

また、BSI は、2024 年、PQC の推奨アルゴリズムを公表した[47]。鍵共有アルゴリズムとして、CRYSTALS-Kyber、FrodoKEM、Classic McEliece を推奨しているほか、デジタ

---

[45] https://www.ncsc.gov.uk/pdfs/whitepaper/next-steps-preparing-for-post-quantum-cryptography.pdf

[46] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Migration_to_Post_Quantum_Cryptography.html?nn=916626

[47] BSI, "Cryptographic Mechanisms: Recommendations and Key Lengths," BSI TR-02102-1, Version 2024-1, 2024 (https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html)

ル署名のアルゴリズムとしては、CRYSTALS-Dilithium、SPHINCS+、LMS、XMSS などを推奨している。

（エ）フランス

フランスのセキュリティ当局である ANSSI（Agence Nationale de la Sécurité des Systèmes d'Information）は、2023 年、PQC のアルゴリズムへの移行に関するポジション・ペーパー「ANSSI views on the Post-Quantum Cryptography Transition (2023 follow up)」を発表した[48]。

ポジション・ペーパーでは、ベンダーに対して、CRQC による脅威を暗号製品のリスク分析に加えるとともに、PQC のアルゴリズムを実装するなど、必要なリスク低減策を検討することを推奨している。PQC のアルゴリズムの推奨に関しては、鍵共有アルゴリズムとして、CRYSTALS-Kyber と FrodoKEM を挙げているほか、デジタル署名のアルゴリズムとして、CRYSTALS-Dilithium、Falcon、SPHINCS+、LMS、XMSS を挙げている。また、PQC のアルゴリズムを実装する際には、当面、ハイブリッド方式を採用することを推奨している。

このほか、暗号製品の評価・認証（コモンクライテリアに基づく）に関して、ハイブリッド方式によって PQC のアルゴリズムを実装する暗号製品の認証を 2024 年～2025 年頃から開始するとの見通しも発表している。

iii. カナダ

（ア） CSE

カナダのセキュリティ当局である CSE（Communications Security Establishment）は、CRQC による公開鍵暗号アルゴリズムへのリスクに対処するためのガイダンス「Preparing Your Organization for the Quantum Threat to Cryptography」を 2021 年に公表している[49]。

ガイダンスでは、中長期間使用される（暗号化対象の）情報が HNDL 攻撃のリスクにさらされる可能性があるとしたうえで、リスク低減の必要がある場合、NIST が標準化した PQC のアルゴリズムへの移行を検討すべきであるとしている。主な対応として以下を推奨している。

① クリプト・インベントリを整備してリスクにさらされる情報を特定する。
② リスク低減策の一環として情報システムのライフサイクルを見直す。
③ PQC のアルゴリズムの導入に伴うソフトウェアやハードウェアの更新に必要な予

[48] https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf

[49] https://www.cyber.gc.ca/sites/default/files/cyber/publications/itsap00017-e.pdf

算を確保する。
④ PQC のアルゴリズムへの移行に必要なノウハウを習得するための研修を担当者に対して実施する。
⑤ ベンダーによる PQC のアルゴリズムの暗号製品への実装状況を把握し、実装が遅れている場合には PQC のアルゴリズムの実装をベンダーに要請する。

（イ）CFDIR

カナダにおける重要インフラの頑健性確保を目的とする産官連携フォーラムである CFDIR（Canadian Forum for Digital Infrastructure Resilience）は、Quantum-Readiness Working Group を設置し、PQC のアルゴリズムへの移行のガイドライン「Canadian National Quantum Readiness: Best Practices and Guidelines」（Version 3）を 2023 年に発表した[50]。

ガイドラインでは、PQC のアルゴリズムへの移行のフェーズとして、①準備、②調査、③リスクアセスメント、④リスク低減策の検討、⑤暗号アルゴリズムの移行、⑥リスク低減効果の検証が挙げられている。これらのうち、①～③のフェーズ（リスクアセスメントの完了まで）について、PQC のアルゴリズムの標準化が完了する前に着手するとともに、2024 年末までに完了させるように対応することを推奨している。また、④～⑥のフェーズに関しては、2025 年以降に着手し、2030 年末までに完了させるように対応することを推奨している。

iv. シンガポール

シンガポール金融管理局（Monetary Authority of Singapore）は、2024 年 2 月、金融機関向けの勧告「Advisory on Addressing the Cybersecurity Risks Associated with Quantum」を発表した[51]。

この勧告において、シンガポール金融管理局は、CRQC による暗号解読などのサイバーセキュリティのリスクが今後 10 年で顕在化する可能性があるとの専門家による見通しを紹介している。そのうえで、金融機関に対して、情報システムやインフラに大きな影響を与えることなく、量子脆弱性をもつ暗号アルゴリズムから PQC のアルゴリズムに効率的に移行するためにクリプト・アジリティを向上させる必要があるとしている。そのための準備として、金融機関に対して以下の検討の実施を求めている。

---

[50] https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2023/cfdir-quantum-readiness-best-practices-v03.pdf

[51] Monetary Authority of Singapore, “Advisory on Addressing the Cybersecurity Risks Associated with Quantum,” 2024 (https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/mas-quantum-advisory/mas-quantum-advisory.pdf)

① CRQC によるリスクへの認識を高める。具体的には、ベンダーやステークホルダーと連携しつつ、リスクの評価や経営層の啓発を行う。
② クリプト・インベントリを適切に管理しつつ、PQC のアルゴリズムへの移行に関する対応の優先順位を決定する。
③ PQC のアルゴリズムへの移行に向けた戦略を策定するとともに、戦略を適切に遂行する能力を高める。この戦略には、PQC のアルゴリズムへの移行に携わるスタッフのスキル向上、組織内部の方針・手続きの見直し、現在の暗号の危殆化時期前倒しの際の対応計画の策定、PQC のアルゴリズムを情報システムに導入する実験の実施といった項目が含まれる。

v. 韓国

韓国では、PQC のアルゴリズムを公募し、応募されたアルゴリズムを評価して国内標準を定めるプロジェクト「KpqC」が進められている[52]。2022 年 11 月より評価の第 1 ラウンドが開始され、暗号化・鍵共有アルゴリズム 7 件、デジタル署名のアルゴリズム 9 件が評価対象となった。その後、2023 年 12 月、評価の第 2 ラウンドの対象として、暗号化・鍵共有、デジタル署名それぞれ 4 件のアルゴリズムが選ばれた。2024 年 7 月末時点では、ラウンド 2 の評価が継続されており、2024 年中に最終的な標準化候補アルゴリズムが選定されるとみられている[53]。

vi. G7 サイバー専門家グループ

G7 サイバー専門家グループ(Cyber Expert Group)は、2024 年 9 月、「G7 Cyber Expert Group Statement on Planning for the Opportunities and Risks of Quantum Computing」と題する提言を発表した[54]。

提言では、今後 10 年以内に CRQC が実現する可能性が高まっており、HNDL 攻撃のリスクなど、CRQC による公開鍵暗号アルゴリズムへのリスクが高まっているとの見方が示されている。また、金融当局や金融機関が協調してリスクを低減させるには相応の時間とコストが必要となることから、可能な限り早期に対応に着手することが推奨されている。具体的な対応事項として次の点が挙げられている。

・ 専門家やベンダーと協力しつつ、量子コンピュータの開発状況をフォローする

---

[52] https://www.kpqc.or.kr/competition.html

[53] Kwon, Hyeokdong, Minjoo Sim, Gyeongju Song, Minwoo Lee, and Hwajeong Seo, "Evaluating KpqC Algorithm Submissions: Balanced and Clean Benchmarking Approach," IACR ePrint 2023/1163, 2023 (https://eprint.iacr.org/2023/1163.pdf)

[54] https://home.treasury.gov/system/files/136/G7-CYBER-EXPERT-GROUP-STATEMENT-PLANNING-OPPORTUNITIES-RISKS-QUANTUM-COMPUTING.pdf

とともに、CRQC とそれによるリスク、リスク低減策について理解を深める。
- 各金融機関においてクリプト・インベントリを整備するなどの活動を通じて、CRQC によるリスクを評価し、実施すべきリスク低減策を決定する。
- ステークホルダーとその役割・責任範囲の特定、リスク低減に向けた活動に関する目標の設定など、CRQC によるリスクを低減するための計画を立案する。

また、提言では、金融当局に対して、一連の活動の重要性を啓発するために関連する主体と密接に連携して対応することが推奨されている。

vii. BIS・フランス銀行・ドイツ連邦銀行

BIS 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、2023 年 6 月、中央銀行間における金融関連データの通信の保護に PQC のアルゴリズムを適用する際に課題となりうる事項の抽出を目的としたプロジェクト「Project Leap」の概要と成果の一部を発表した[55]。

本プロジェクトにおいて想定されている脅威は、通信路上で暗号化データが盗取・収集され、後日 CRQC によって解読されるタイプの攻撃（HNDL 攻撃の一種）である。保護対象は長期間秘密にしておく必要があるデータとなっている。こうしたデータを取り扱う情報システムに関して、「新しい暗号アルゴリズムの仕様発表から移行完了までに 10 年以上かかる場合もあることから、量子脆弱性を有する情報システムの特定やクリプト・インベントリの整備など、移行に向けた検討に着手することが望ましい」としている。

プロジェクトは 2 つのフェーズから構成されている。フェーズ1は、PQC のアルゴリズムを用いた暗号通信のテスト環境の構築や性能評価を目的とし、フェーズ2は、ネットワーク構成のさらなる検討、異なるタイプのハードウェアによる性能評価などを実施する予定としている。

2023 年 6 月に完了したフェーズ 1 では、テスト環境として、フランス銀行とドイツ連邦銀行を結ぶ IPsec-VPN の通信路が準備された。この通信路で使用される鍵共有アルゴリズムとして、RSA、CRYSTALS-Kyber、FrodoKEM が対象となったほか、署名アルゴリズムとして、RSA、CRYSTALS-Dilithium、SPHINCS+、Falcon が対象となった。そのうえで、決済データに模したデータ（XML メッセージ）を送信するケースを想定し、複数の暗号ライブラリによる暗号通信が試行された。その結果、鍵共有の処理はいずれの PQC のアルゴリズムにおいても成功したものの、署名による認証の処理に関

[55] BIS Innovation Hub, “Project Leap: Quantum-proofing the financial system,” June 2023 (https://www.bis.org/publ/othp67.pdf)

しては実施できないケースがあった旨が報告されている[56]。性能評価については、VPN のセットアップ(主に鍵共有と認証の処理)にかかる時間を測定したところ、鍵共有・認証ともに PQC のアルゴリズム(例えば、CRYSTALS-Kyber と CRYSTALS-Dilithium の組合せ)を用いる場合の時間が、RSA を用いる場合に比べて長くなるなど、現在の暗号アルゴリズムを用いる場合に比べて性能低下がみられた旨が報告されている[57]。

(3) 金融業界・民間団体全般

i. FS-ISAC

FS-ISAC は、金融機関の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、金融機関間における情報の共有や分析を実施する枠組みを提供する非営利団体である。FS-ISAC は、量子コンピュータが金融サービスに与える影響を検討するために、Post-Quantum Cryptography Working Group を設置し、金融サービスへのリスクと対処方針、今後の展望などに関する検討結果を 4 つの技術報告書(technical paper)として 2023 年に公表した[58]。これらの技術報告書のサマリーペーパー「Preparing for a Post-Quantum World by Managing Cryptographic Risk」は、HNDL 攻撃の可能性などを踏まえ、以下の見解を示している。

- **CRQC の登場時期の予測可否によらず、リスクに対処できる情報システムの準備を直ちに開始しなければならない(must immediately begin preparing)。**
- **古典コンピュータ(classical computer)の性能向上によるリスクにも留意する必要がある。CRQC の開発が進むと、その成果が古典コンピュータにも応用されて性能が向上する可能性がある。**
- **CRQC と古典コンピュータに対してセキュリティを確保しつつ、現在の情報システ**

---

[56] 一部の暗号ライブラリにおいて、署名用の PQC のアルゴリズムを識別する機能が設定されていなかった旨が報告されている。

[57] このほか、BIS のスタッフによる個人名ペーパー「Quantum Computing and the Financial System:Opportunities and Risks」(https://www.bis.org/publ/bppdf/bispap149.htm) が 2024 年に発表されている。このペーパーでは、量子コンピュータが金融サービスに今後もたらす可能性があるメリットやデメリットが紹介されており、デメリットに関して、公開鍵暗号アルゴリズムの安全性低下による金融サービスへの潜在的なインパクトが大きいとの見方が示されている。そのうえで、将来の金融システムへの信頼を維持する観点から、中央銀行は、リスク低減に向けて、専担チームの設置、重要な情報や取引を保護している暗号アルゴリズムのインベントリの整備、PQC への移行のロードマップの作成といった検討に着手することが望ましいとしている。また、そうした活動が一部の中央銀行で開始されているとしたうえで、その事例の 1 つとして Project Leap が紹介されている。

[58] https://www.fsisac.com/knowledge/pqc

ムとの相互運用性が高い暗号プロトコルをPQCのアルゴリズムによって開発することが重要である。

サマリーペーパーは、PQC のアルゴリズムへの移行のプロセスとして、①暗号アルゴリズムによって保護されている情報資産の棚卸しやクリプト・インベントリの整備、②リスクアセスメントの実施、③ベンダーの対応状況の調査、④リスク評価フレームワークの準備、⑤リスクモデルの適用、⑥リスク低減策の適用を挙げている。これらのうち、①～⑤の概要は以下のとおりである。

①情報資産の棚卸しやクリプト・インベントリの整備

まず、暗号アルゴリズムの使用状況、暗号アルゴリズムによる保護対象の情報資産やデータの種類・属性を網羅的に調査し、収集した情報をクリプト・インベントリとして適切に管理する。

②リスクアセスメント

リスクアセスメントでは、クリプト・インベントリに基づいてリスクを網羅的に抽出し、リスクの顕在化の可能性や業務への影響、対応の優先順位などを決定する。

③ベンダーにおける対応状況の調査

ベンダーにおけるPQCのアルゴリズムの導入に関する状況を把握する。そのうえで、ベンダーに対して、PQC のアルゴリズムの導入要請や、それに伴う契約上の要求事項の見直しを、必要に応じて行う。

④リスク評価フレームワークの準備

業務の目的に適合したリスク評価のフレームワークを決定する。

⑤リスクモデルの適用

リスクを低減する必要があると判断されたアプリケーションに対してリスクモデルを適用し、リスクを定量化する。

また、Post-Quantum Cryptography Working Group は、2024 年に「Building Cryptographic Agility in the Financial Sector: Effective, Efficient Change in a Post Quantum World」と題するペーパーを発表している[59]。このペーパーは、量子コンピュータが普及した世界(post-quantum world)の到来を展望し、システムやインフラにお

[59] https://www.fsisac.com/pqc-crypto-agility

けるクリプト・アジリティの実現が重要であることを指摘するとともに、クリプト・アジリティの実現に向けたプロセスを解説するものである。

本ペーパーでは、クリプト・アジリティについて検討するうえで、まずクリプト・アジリティの達成度の目標を設定し、その目標を達成するために必要なシステム開発・運用のプロセスを検討・決定することが重要であるとしている。

クリプト・アジリティの達成度の基準としてはさまざまなものが考えられるとしており、例えば、 暗号アルゴリズムの移行後のシステムの状態に着目すると、クリプト・アジリティ実現の対象となっているアーキテクチャが(いったん実装された後に)新しい暗号アルゴリズムを採用する際に(アーキテクチャに対して)大きな変更を要しない確からしさが基準となりうるとしている。また、暗号アルゴリズムの変更プロセスに着目すると、暗号アルゴリズムの移行作業時において稼働中のシステムが停止しない確率が基準となりうるとしている。

また、設定した目標を達成するためのシステム開発・運用のプロセスとして次の8つのフェーズが定義されている。

- インベントリ:暗号アルゴリズムによって保護される資産、それらの依存関係、リスクを明確化。
- 計画:暗号アルゴリズムの移行・統合計画を策定。PQC アルゴリズムを選定。
- テスト・正当性確認:選定した PQC アルゴリズムをシステムに実装した際の性能を分析。
- 実装:重要度の低いシステムから移行を開始。
- 切り替え:関連するシステムのコンポーネントを更新(例えば、TLS 1.2 から TLS 1.3 への更新)。
- 検証:PQC アルゴリズムの実装結果を組織の内部及び外部で検証(基準値の目標達成度合いの確認)。
- メンテナンス:実装した PQC アルゴリズムを取り巻く環境やリスクを監視。
- 再検討フェーズ:PQC アルゴリズムの実装に関連する事項の見直し・再実施(技術標準の見直しなど)。

このように、クリプト・アジリティに関する検討には、インベントリ管理や監視戦略なども含まれており、システム対応などの技術面だけでなく、それに関連する全ての運用・プロセスもスコープに含まれることが示されている。

ii. ASC X9

ASC X9(Accredited Standards Committee X9, Inc.)は、アメリカ国内における金融サービスに関する標準規格を策定する団体であり、金融サービスで使用される暗号

アルゴリズムに関する規格も策定している。

ASC X9 のうち、X9F Cybersecurity and Cryptographic Solutions Workgroup は、2019 年 1 月、「Quantum Techniques in Cryptographic Message Syntax (CMS)」と題する技術報告書を発表している[60]。この技術報告では、CRQC が現在の暗号アルゴリズム、暗号通信、公開鍵暗号基盤(public-key infrastructure)に与えうる影響、量子耐性を有する暗号アルゴリズム、暗号メッセージ構文(cryptographic message syntax)で使用されている暗号アルゴリズム(鍵共有アルゴリズム、署名アルゴリズムなど)への影響と推奨対応策が説明されている。特に、HNDL 攻撃による暗号化データの解読を防ぐために、現在の鍵共有アルゴリズムと量子耐性を有するとみられる鍵共有アルゴリズム(標準化されていないもの)を組み合わせて使用するハイブリッド方式(hybrid methods)が推奨されている。

また、ASC X9 は、X9F Quantum Computing Risk Study Group を設置して量子コンピュータの動向や金融サービスに与える影響を調査し、2022 年 11 月、調査報告書「Quantum Computing Risks to the Financial Services Industry」を発表している[61]。この報告書のエグゼクティブサマリーには、CRQC によるリスクとそれへの対処に関して以下の見解が示されている。

- 近年、CRQC に関する有識者の見方が変化している。従来は、「CRQC 登場の障害となっている課題や技術的障壁を克服することができるか？」という声が大半であった。最近では、「課題や技術的障壁がいつ克服できるか？」という、(登場することを前提に)登場の時期を問う声が多くなっている。
- CRQC の脅威にさらされる情報資産を特定し、それらをどう保護するかについて検討する必要性が高まっている。
- CRQC 登場の時期については、今後、5～30 年後(2027 年から 2052 年頃)とみられる。量子コンピュータ関連の研究開発投資や技術的課題の克服状況によって、実現のタイミングは変化する。
- 時間の経過とともに、CRQC 登場の時期をより正確に予測できるようになる反面、リスクに対処するための時間も減少することに留意すべきである。

こうした見解を踏まえ、調査報告書は、現在の暗号アルゴリズムから PQC のアルゴリズムに移行することが望ましく、以下の対応を実施すべきであるとしている。

- 量子コンピュータとその影響、脅威に対処するためのツール、技術、標準規格を

[60] https://x9.org/wp-content/uploads/2019/03/ASC-X9-TR-50-2019-Quantum-Techniques-in-Cryptographic-Message-Syntax-1.pdf

[61] https://x9.org/wp-content/uploads/2022/11/X9F-Quantum-Computing-Risk-Study-Group-IR-F01-2022_20221129-Published-PDF.pdf

理解する。
- 量子コンピュータの開発動向を注視する。
- 量子脆弱性を有する暗号アルゴリズムの使用状況を特定する(クリプト・インベントリの整備)。
- CRQC 登場が業務やサービスに及ぼす影響を評価する。
- CRQC によるリスクに対処するためのツールをどの情報システムのどの部分に適用するかを決める。
- サプライチェーン上の関連組織に対して、PQC のアルゴリズムへの移行の戦略立案を要請する。
- PQC のアルゴリズムを情報システムに導入する前に、テストを実施して対策の効果を検証する。

このほか、ASC X9 は、2023 年 6 月、「Post-Quantum Cryptography Assessment Guidelines」と題する技術報告書(technical report)の策定に着手する旨を発表している[62]。

iii. UK Finance

UK Finance は、2023 年 11 月、PQC 移行に関する提言ペーパー「Minimising the Risks – Quantum Technology and Financial Service」を公表した[63]。このペーパーは、量子コンピュータが金融サービスに及ぼす影響やリスクを説明するとともに、対処方針を示している。

CRQC によるリスクへの対処方針として、ステークホルダー間の協調(collaboration)が重要であり、当局を含む金融業界全体として対応していくという姿勢の必要性を強調している。まずは、PQC のアルゴリズムへの移行に関するワーキンググループを設置し、学術・研究機関とも連携しつつ、金融業界の行動計画を作成する必要があるとしている。同時に、円滑な移行を実現するための金融機関向け支援に関する政策や規制の枠組みについても検討することが考えられるとしている。

また提言ペーパーでは、金融業界の行動計画に基づいて、各金融機関がそれぞれ自社の行動計画を策定する必要があるとしている。行動計画に含めるべき事項として、①クリプト・インベントリの整備、②リスクの評価、③サイバーセキュリティ対策の強化、④量子コンピュータ活用の戦略とロードマップの作成、⑤量子コンピュータ活用やサイバーセキュリティ対策への投資の検討、⑥ステークホルダーとの協力、⑦量子技術に関する知見を備えた人材の育成強化、⑧PQC のアルゴリズムへの移行に伴っ

62 https://x9.org/wp-content/uploads/2023/06/X9-PQC-TR-6-23-FINAL.pdf

63 https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/minimising-risks-quantum-technology-and-financial

て生じうる規制の変更の監視とそれに伴うコンプライアンス・プロセスの見直しが挙げられている。

ⅳ. World Economic Forum

World Economic Forum は、2024 年 1 月、「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している[64]。このホワイトペーパーは、イギリス金融行為規制機構(Financial Conduct Authority)と連携して作成されている。

ホワイトペーパーは、現状として、CRQC によるリスクへのアプローチが国や地域によって異なっている点を指摘したうえで、金融機関のシステムが相互に接続され、それがグローバルに広がっている点を踏まえると、一部の金融機関の対応の遅れによる影響が他の国や地域の金融機関に及ぶ可能性があるとの見方を示している。そのため、CRQC へのリスクに対処する際には、統一的でグローバル、業界横断的なアプローチが必要であり、国際的な協力体制の強化、金融機関と当局との間の協力も不可欠であるとしている。

また、CRQC によるリスクへの対応ロードマップとして、①準備(prepare)、②明確化(clarify)、③ガイド(guide)、④移行と監視(transition and monitoring)の 4 つのフェーズを示している。それぞれの概要は以下のとおりである。

- 「準備」フェーズ： リスクに対するステークホルダーの意識向上、スタッフの啓発・スキルアップ、現状把握(クリプト・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。
- 「明確化」フェーズ： ステークホルダー間の連携・協力体制の確立、PQC のアルゴリズムへの移行に必要な作業・コスト・期間などの明確化、既存の規制の再評価など。
- 「ガイド」フェーズ： PQC のアルゴリズムへの移行戦略の検討、必要な規制の策定、ベストプラクティスの作成など。
- 「移行と監視」フェーズ： PQC のアルゴリズムへの移行戦略の実施、クリプト・アジリティや頑健性の確保・向上のための開発プロセスの適用(policy development process to ensure long-term agility and resilience)、脅威やリスクの状況の監視と先行きを見通した対処方法(forward-looking approach)の検討など。

ⅴ. DTCC(アメリカ)

証券決済・保管機関である DTCC は、2022 年 9 月、PQC のアルゴリズムへの移行

[64] https://www3.weforum.org/docs/WEF_Quantum_Security_for_the_Financial_Sector_2024.pdf

に関するホワイトペーパー「Post-Quantum Security Considerations for the Financial Industry」を公表した[65]。このホワイトペーパーは、金融機関に対して、CRQC による公開鍵暗号アルゴリズムへのリスクが足許のリスク(near-term risk)であることを認識してもらうとともに、PQC のアルゴリズムへの移行においてまず何をすればよいかを伝えることを目的としている。

ホワイトペーパーは、まず、現在の暗号アルゴリズムによって保護されているデータが CRQC 登場によって解読されたり改変されたりするリスクがあることを指摘したうえで、HNDL 攻撃を紹介しつつ、暗号解読の脅威が既に存在しうるとしている。そして、NIST による PQC のアルゴリズムの標準化が完了する前から、PQC のアルゴリズムへの移行に向けた準備を開始することが必要であるとしている。具体的な対応項目として以下が挙げられている。

- 重要な情報を処理・保管している情報システムやその部分、そうした情報システムにおいて用いられている暗号アルゴリズムを調査・把握する(クリプト・インベントリの整備)。
- PQC のアルゴリズムへの移行をなるべく円滑なものにする(クリプト・アジリティの向上)ために、暗号鍵や電子証明書の管理を一元化(centralizing)する、暗号アルゴリズムの使用方法として標準仕様に基づく方法を採用する、暗号製品の変更時にその内容を記録しておく、といった対応を実施する。
- 暗号製品を切り替えるために必要なステップを詳しく説明するプレイブックを準備する。また、プレイブックの内容を理解するための訓練や小規模な実験を実施する。
- リスク対応に関する組織のカルチャーやマインドセットを変更・強化する。例えば、リスクに関して顧客やベンダーと情報共有や対話を開始する、PQC のアルゴリズムへの移行の準備のためのチームを設置する、担当者を育成する、リスクやその対応について経営陣に報告するなどが挙げられる。

vi. QSFF

EC3(European Cybercrime Centre)[66]は、2024 年、欧州域内の金融業界における PQC のアルゴリズムへの移行を支援するために、QSFF(Quantum Safe Financial Forum)を設置した[67]。

---

[65] https://www.dtcc.com/-/media/Files/Downloads/WhitePapers/Quantum-Computing-WhitePaper-2022.pdf

[66] EC3 は、欧州域内のサイバー犯罪に対する法執行活動を強化するために欧州刑事警察機構（Europol）によって設置された組織である。

[67] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/qsff

QSFF には、欧州、イギリス、アメリカの主要な商業銀行や中央銀行のスタッフが参加しているほか、銀行協会やその他の金融サービス事業者のスタッフ、PQC のアルゴリズムや関連する分野の専門家も参画している。

QSFF の主な目標として、①金融業界における PQC のアルゴリズムへの移行の促進、②量子コンピュータによる脅威の評価と評価結果の金融業界内での共有、③課題の特定とベスト・プラクティスの確立、④金融業務向けのソリューションの検討、⑤他の地域における活動との連携、⑥知見の共有や訓練・学習の機会の提供が挙げられている。

(4) ベンダー

i. ウェブブラウザ

ウェブブラウザ Chrome(バージョン 124。デスクトップ向けに限定)において、TLS 1.3 及び QUIC の鍵共有のデフォルトのアルゴリズムとして CRYSTALS-Kyber が実装されている旨が Chromium Blog(2024 年 5 月 23 日付)で紹介されている[68]。鍵共有アルゴリズムの使用形態は、CRYSTALS-Kyber と ECDH によるハイブリッド方式(X25519Kyber768)[69]である。ただし、CRYSTALS-Kyber の暗号文のサイズ拡大による通信への影響を考慮し、本発表時点では、Android 向けの Chrome への搭載を行っていないとしている。

その後、Google Security Blog(2024 年 9 月 13 日付)において、Chrome バージョン 131 より、従来の CRYSTALS-Kyber(標準化される前の仕様)のサポートを停止して ML-KEM(標準化された仕様)をサポートする旨が発表されている[70]。

ii. スマートフォン・アプリ

メッセージング・アプリ Signal において、メッセージ暗号化用のセッション鍵(共通鍵暗号)を生成するための秘密情報の共有[71]に CRYSTALS-Kyber と ECDH を組み合わせて使用する方法が採用されている旨が、Signal Foundation のブログ(2023 年 9 月 19 日付)で紹介されている[72]。

---

[68] https://blog.chromium.org/2024/05/advancing-our-amazing-best-on-asymmetric.html

[69] Westerbaan, Bas, and Douglas Stebila, "X25519Kyber768Draft00 hybrid post-quantum key agreement," draft-tls-westerbaan-xyber768d00-03, IETF, 2023 (https://www.ietf.org/archive/id/draft-tls-westerbaan-xyber768d00-03.html)

[70] https://security.googleblog.com/2024/09/a-new-path-for-kyber-on-web.html

[71] Signal Foundation のブログでは、鍵共有プロトコルとして PQXDH (https://signal.org/docs/specifications/pqxdh/pqxdh.pdf) が採用されている旨も紹介されている。

[72] https://signal.org/blog/pqxdh/

また、メッセージング・アプリ iMessage においても、鍵共有に関して、CRYSTALS-Kyber と ECDH を組み合わせて使用する形態(hybrid design)が採用される予定が、Apple Security Research のブログ(2024 年 2 月 21 日付)において紹介されている[73]。

iii. Web 会議システム

Zoom のコラボレーション・プラットフォーム Zoom Workspace の一部において、エンドユーザー間でのデータの暗号化(end-to-end encryption)における鍵共有のために CRYSTALS-Kyber を使用することができる旨が、Zoom Blog(2024 年 5 月 24 日付、同年 7 月 15 日更新)で紹介されている[74]。

ⅳ. IC カード

凸版印刷と情報通信研究機構は、ISARA と連携し、CRYSTALS-Dilithium を搭載した IC カードを開発した旨を 2022 年 10 月に発表している[75]。この IC カードは、情報通信研究機構が運用するテストベッド「保健医療用の長期セキュアデータ保管・交換システム」における IC カード認証やアクセス制御に使用される旨が紹介されている。

また、凸版印刷と情報通信研究機構は、上記の IC カードに格納される電子証明書を発行するプライベート認証局を構築した旨を 2023 年 3 月に発表している[76]。プライベート認証局が発行する電子証明書に付与される署名アルゴリズムとして、CRYSTALS-Dilithium が使用されている。

ⅴ. 本邦におけるシステムインテグレータ

量子コンピュータの研究開発を推進している一部のシステムインテグレータ(以下、SIer)では、PQC 移行に向けたクリプト・インベントリ作成や移行優先度検討に関する支援サービスの提供を開始している。一方、一部の SIer では、研究部門においてサービス提供に向けた研究開発を進めているものの、事業部門での提供時期について明言しておらず、現状として国の動向を注視していると推測される。

4. 金融分野における耐量子計算機暗号対応の必要性

(1) 金融データの機密性と完全性

金融機関で取り扱うデータは、顧客データ、取引データ、財務データ、市場データ、

---

[73] https://security.apple.com/blog/imessage-pq3/

[74] https://www.zoom.com/en/blog/guide-to-post-quantum-end-to-end-encryption/

[75] https://www.holdings.toppan.com/ja/news/2022/10/newsrelease221024_1.html

[76] https://www.nict.go.jp/press/2023/03/14-1.html

内部データ、規制・コンプライアンスデータなど多岐にわたる。これらのデータを安全に取り扱うためには、高度な機密性と完全性の確保が重要になる。これを実現するためには、金融機関は適切なアクセス権の設定や通信ネットワークやシステムでの論理的または物理的な隔離といった対策を多重に実装する必要がある。暗号技術はその対策技術の 1 つであって、ユーザーの認証や盗聴防止などに幅広く利用されている。

本章の前半では、暗号技術によって保護するデータや情報システムについて代表例を示し、後半では、データの安全な利用に必要となる二つの特性、すなわち、機密性と完全性について述べる。

i. 暗号技術によって保護する対象

(ア)代表的なデータ

金融機関では、顧客に応じたきめ細やかな金融サービスを実現するために、個人や法人に関する様々な情報を取り扱っている(表 4.1 参照)。また、円滑な決済を行うための金融取引に関するデータや市場に関するデータを取り扱っている。コンプライアンス対応の観点から、これらの情報は金融取引発生後 7 年間保管することが法令[77]によって定められている。また、金融機関が行う融資業務の一部には 7 年を超えた貸付期間をもつ商品もあるので、金融サービスを実現するために用いるデータの使用方法や保存期間は様々である。加えて、自行を運営していくための機密度の高い行内情報の他、漏洩するとレピュテーションへの深刻な影響があり、かつ容易に変更できないため長期にわたる保護が必要になる情報、取引の内容や事実そのものが重要な情報となり得るもの(例えば、防衛産業企業との取引情報や M&A に関する情報)は優先して保護すべきデータと言える。

また、金融機関が取り扱うデータには、金融機関特有のデータ以外にも、例えば、インターネットに接続する Web システムの通信データ、IC キャッシュカードなどの IC カードのチップ内に保存される認証情報、利用するソフトウェアの改ざん防止のための署名情報などの、情報システムを構成するときに用いるデータがある。

金融機関特有のデータ以外については、今後、他業界における PQC への移行が急速に進むとすれば、それらのノウハウを金融業界でも活用することが期待できる可能性がある。もっとも、金融機関特有のデータについては、用途、保存環境、保存期間などが異なる可能性があるので、金融機関が主体的に検討していくことが望ましい。

---

[77] 犯罪による収益の移転防止に関する法律

表 4.1 代表的データ例

データ例	概要	公開鍵暗号以外の対策例
インターネットバンキングの認証情報、取引情報	インターネットを介して、口座残高の照会や送金取引などの各種金融取引を行うときに必要なデータ	多要素認証、リスクベース認証、モニタリング、アクセス制御
キャッシュカードのICチップ内の認証情報	ATMやICカードリーダーを取り付けたPC端末などで認証を行うときに利用するデータ	ハードウェア保護、多要素認証
行内の事務データ	顧客の金融取引や自行内の業務を行うために利用するデータ	物理制御、行内アクセス権設定、改ざん検知
電子メール・SMSメッセージ	顧客との連絡やお知らせについてインターネットを使って送信するデータのうち、改ざん対策や暗号化を施す必要があるデータ	送信元制御、ブランド保護(BIMI)

(イ)代表的な情報システム

前述したデータを取り扱う情報システムには、自行内で開発・運用していくものと、ベンダーが運用する共同センターや業界として開発・運用していくものとがある(表 4.2 参照)。それぞれの情報システムでは、データを安全に取り扱うために、暗号技術を含む多種多様なセキュリティ対策を講じられている。また、それらは、外部環境の変化の内容に応じながら、年々強化が図られている。業界として開発・運用していくシステムについては、多数の機関が利用しているので、セキュリティ対策の変更に関する計画策定では合意形成に一定の時間がかかるものと予想される。そのため、外部環境の変化の内容については、業界内で定期的に認識共有をすることが望ましい。

表 4.2 金融機関が共同で利用する情報システムの例

名称	概要
全銀システム[78]	全国銀行内国為替制度に加盟する銀行間の内国為替取引に関する通知の送受信、及び当該取引によって生じる銀行間の為替決済額の算出・清算などを集中的に行うオンラインシステム
日銀ネット[79]	日本銀行とその取引先金融機関との間の資金や国債の決済をオンライン処理により効率的かつ安全に行うことを目的として構築されたシステム
統合ATM[80]	金融機関が保有するCD(現金自動支払機)/ATM(現金自動預払機)の相互利用取引電文を中継するサービス
ANSER[81]	金融機関の窓口やATMで行っていた金融取引(残高照会や入出金明細の連絡、顧客の口座からの振込・振替など)を、オンラインを介して行うサービス
でんさいネット[82]	手形・指名債権(売掛債権等)を電子記録として扱うシステム。オンライン上で債権の保管や支払・受取などができる
CAFIS[83]	クレジットカードやデビットカードなどを使った決済情報を加盟店と金融機関との間で授受するオンラインシステム
SWIFT	銀行間の国際金融取引に係る事務処理の機械化、合理化及び自動処理化を推進するため、参加銀行間の国際金融取引に関するメッセージをコンピュータと通信回線を利用して伝送するネットワークシステム

[78] https://www.zengin-net.jp/zengin_system/

[79] 日本銀行金融ネットワークシステム, https://www.boj.or.jp/paym/bojnet/index.htm

[80] 統合 ATM スイッチングサービス, https://www.nttdata.com/jp/ja/lineup/integration_atm_switching/

[81] Automatic answer Network System for Electronic Request, https://www.nttdata.com/jp/ja/lineup/anser/

[82] https://www.densai.net/about/

[83] https://www.nttdata.com/jp/ja/lineup/cafis/

ii.　暗号技術によって保護する特性

情報セキュリティは、機密性、完全性、可用性の三つの性質を確保することである。この中で、暗号技術は、主に機密性と完全性の二つの性質を確保するために、多重防御の一つとして用いられる。

(ア)機密性

機密性とは、情報に関して、アクセスを認められた者だけがこれにアクセスできる状態のことをいう。暗号化された情報(暗号文)を読むためには、その暗号文に対応した暗号鍵を用いる必要があって、この暗号鍵が安全に管理されている限り、暗号化される前の情報を盗聴する事は非常に困難である。例えば、情報窃取の手口の 1 つに、有線・無線の各通信ネットワークで授受されるデータの盗聴がある。これを防ぐために、送受信者しかデータの内容が分からないように、双方だけがもつ暗号鍵でデータを暗号化することで、仮に盗聴されたとしてもデータの内容は分からないようにしている。

(イ)完全性

完全性とは、情報が原本のままで、破壊、改ざん、又は意図しない変更などが起きていない状態のことをいう。公開鍵暗号アルゴリズムを応用したデジタル署名を使うことで、情報作成者の証明や、情報が改ざんされていないことを検証することが可能である。機密性の脅威について例示した不正アクセスの手口の 1 つに、正規ユーザーへのなりすましがある。これを防ぐために、電子証明書を使った認証が有用である。

(2) 金融機関に対して起こり得る脅威シナリオ

機密性について、CRQC の開発が進むと、既存の公開鍵暗号によって暗号化されているデータでは、Shor のアルゴリズムの適用によって HNDL 攻撃のリスクが表面化する懸念がある。しかし、昨今、多重防御やリスクベースでの対策実施の考え方が浸透してきており、重要なシステムにおいて公開鍵暗号だけでセキュリティを確保しているケースは少ないとも考えられ、公開鍵暗号への依存度合いやその危殆化によるリスクを個々のシステムに関して評価して判断することが望ましい。

完全性については、CRQC の実現以後でしか侵害が発生しないので、HNDL 攻撃によって侵害される機密性よりも優先度を下げて考えることができる。ただし、CRQC の実現以前にデジタル署名されたデータは、CRQC の実現後、完全性が担保されなくなるので、データアーカイブやタイムスタンプなど、完全性を検証するための仕組みを検討することが望ましい。

本章では預金取扱金融機関のリスクシナリオとして、UK Finance の Minimising the

Risks: Quantum Technology and Financial Services 中で例示してあるリスク(pp.21-25)の中から特に金融分野にフォーカスしたものを引用した(Cryptographic Risk 2,3,4,7,8,9)[84] 。

- ホールセール決済システムの認証の脆弱化(Risk 2)
  ホールセール決済システムの認証は、公開鍵暗号に強く依存しているため、CRQC の攻撃で合法的な取引を模倣した不正決済を実行される可能性がある。

- 銀行間システムのインターフェースの侵害(Risk 3)
  オープンバンキングや相互接続された金融システムの普及により、利便性が向上する一方、 CRQC による攻撃と同時にインターフェースの脆弱性が悪用される対象になる可能性が高まっており、複数銀行の機密性の高い金融データや顧客情報、取引記録に不正アクセスされる可能性がある。

- 分散型台帳技術(DLT)を基にした金融商品の侵害(Risk 4)
  DLT の固有のセキュリティも脆弱性をもつ。CRQC によって、基盤である初期のブロック(ジェネシスブロック)の内容が後から変更されると、その後のブロックの完全性が崩れ、 DLT の不変性と透明性を損なう可能性がある。

- ソフトウェアの完全性における脆弱化(Risk 7)
  デジタル署名はソフトウェアとファームウェアの正当性の検証の基盤となっている。これらの署名は、公開鍵暗号アルゴリズムに依存しており、脆弱性を突いた攻撃によりソフトウェアやファームウェアが改変され、それが組み込まれた重要なシステムに混乱をもたらす可能性がある(例: SolarWinds 事件。 IT 管理及び監視ツールであるソフトウェアを侵害し、政府 民間を含む多数の組織のネットワークに侵入[85])

- 金融取引記録の改ざん(Risk 8 企業固有の台帳)
  企業の内部情報システムに保存されているデジタル署名付与済の金融取引記録は、CRQC によるデータの改ざんにより、資産所有権の書き換え、不正な取引の実行、取引履歴の変更等、取引記録(台帳)が保証する正確性と透明性を損なう可能性がある。

---

[84] https://www.ukfinance.org.uk/system/files/2023-11/Minimising%20the%20risks%20-%20quantum%20technology%20and%20financial%20services.pdf

[85] https://cloud.google.com/blog/topics/threat-intelligence/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor/?hl=enckdoor/?hl=en"

- 金融取引記録の改ざん(Risk 9 公的な台帳)

  土地登記などの台帳に保存される公共資産記録は、不動産の所有権、住宅ローン、及び関連する証券の基礎として機能しており改ざんのリスクをもち、所有権や法的権利、公開企業の記録、規制当局への提出書類、及びその他のデータソースも改ざんされる可能性がある。

上記のような金融分野で考慮する必要のリスクがある一方で、直ちに CRQC の完成が見込まれるわけではなく、現実的なリスクの表面化は相当の時間を要すると思われる。ただし、国内外の各種法令または規制に PQC への対応等が盛り込まれる可能性が否定できないほか、次章で述べるようなクリプト・インベントリの構築や更新については相当の時間を要することに留意が必要である。一般的なリスクベースの考え方では、組織の所有している情報資産の中で優先順位付けを行うが、これと同様に脆弱性対応や Hardening(ハードニング) と同じような形で検討を進めていくことが望ましいと考えられる。また、自組織環境だけではなく、利害関係者とのインターネット等を介したデータ授受や相手方に管理されている公開鍵や暗号文などを狙った HNDL 攻撃リスクを想定する必要があると考えられる。

5. 金融分野における耐量子計算機暗号対応に向けた推奨事項

(1) 耐量子計算機暗号対応の特徴(対応計画の前提事項)

既存の量子脆弱性をもつ暗号方式を PQC に置き換えること(=暗号移行すること)については、一般的な暗号移行よりも移行期間が長期化することが見込まれている。加えて PQC 暗号移行固有の特徴として、CRQC の登場時期及び実装を含めた PQC 関連技術の動向や製品供給に関する不確実性が大きい。移行期間が長期化しやすい理由については以下のようなものが挙げられる。

- 量子脆弱性をもつといわれる公開鍵暗号方式は様々な箇所で利用されており(TLS1.3 のような HTTPS 通信、電子文書への署名や IC カード、アプリケーション独自で利用されている暗号化等)、金融機関内で網羅的に把握しようとすると非常に時間がかかるため。
- 移行対象のシステムを取り巻くステークホルダーも多様であり、開発委託先ベンダーや製品調達先ベンダー、接続先システムの管理部門、ユーザー等、金融機関側の調整負荷が大きいため。
- 2024 年 8 月に NIST にて ML-KEM、ML-DSA、SLH-DSA の標準化仕様が決定し

たが、世の中への PQC の普及が進むには IETF をはじめとする標準化団体による暗号技術を利用したプロトコル仕様の標準化や暗号技術を実装したソフトウェア・ハードウェアの展開が求められるが、現在はその途上にあるため。

また、PQC に関する不確実性については以下のようなものが挙げられる。

- CRQC の登場時期が現在のところ未確定である(量子コンピュータそのものがハード面・ソフト面双方で実験段階の技術)。
- 早期に PQC への移行が可能であるにしても、PQC が比較的新しい技術である以上、採用した暗号方式の脆弱性が将来的に発見される可能性は否定できない[86]。(現代暗号のような長期にわたる実社会での評価を受けていない)

以上のように、移行期間の長期化の可能性や移行スケジュールの不確実性を考慮しながら対応方針を策定することになると考えられる。なお、10 年を超えるような長期間にわたって秘匿する必要がある情報の保護に量子脆弱性をもつ暗号を使用している場合、HNDL 攻撃の対象になる可能性がある。こうした情報に関しては、CRQC 実現前から、第 4 章 表 4.1 に記載のとおり、公開鍵暗号とそれ以外の各種対策を組み合わせて多重防御を講じる等、別途データを保護するための対応を検討することが考えられる。

(2) 耐量子計算機暗号対応の基本事項整理

前章の特徴を踏まえて、移行のための基本事項を整理する。詳細は(3)をご覧いただきたい。

- CRQC による既存の暗号危殆化に関連するリスクに基づいて、移行対象の優先順位付けを行う。
- 移行対象の詳細な把握のため、クリプト・インベントリを構築する。
- 暗号危殆化状況に応じて安全かつ迅速に対応できるアーキテクチャを検討する。
- 優先順位の高いものを中心に移行期限を設定し、期限超過の可能性も踏まえたリスク低減策も検討する。

[86] 実際に、NIST による Post-Quantum Cryptography Standardization の第 4 ラウンドに進んだ SIKE については解読手法が発見されてしまっている(W. Castryck , T. Decru, “An Efficient Key Recovery Atttack on SIDH,” Advances in Cryptology -- EUROCRYPT 2023, pp. 423-447, 2023.)

(3) 移行に向けた推奨事項

i. 耐量子計算機暗号対応の優先度・リスクの考え方整理

前述の通り、移行スケジュールの不確実性に鑑み、重要度が高く量子脆弱性をもつもので、悪用される可能性が比較的高いシステムから対応するのが基本的な考え方となる。その際にどのように対象システムを選定するか、その考え方の一例を以下に示すが、いずれもリスクベースでの選定軸である。

考え方:「以下の項目のいずれにも該当するものを優先的に対応する」

- 重要度が高いシステム
  - 業務重要性が高い(例えばFISC安全対策基準における「特定システム」のような社会的な影響が大きいシステム)
  - システムで扱うデータに、保護期間が長期に設定されているもの、もしくは漏えい時に影響が極めて大きいものが含まれている
  - 海外規制の影響を受ける
- 量子脆弱性をもつシステム
  - 公開鍵暗号や鍵長の短い共通鍵暗号を利用している
  - ソフトウェア/ファームウェア署名等、量子脆弱性のある暗号アルゴリズムによる対象の保護が比較的長期にわたる
  - 第4章(2)の脅威シナリオに記載の暗号利用と同等の利用がある
- 悪用される可能性が比較的高いシステム
  - インターネット経由で、保護すべき情報の通信が行われている
  - 金融機関がリスク管理の状況を直接把握していない外部のシステムと接続され、保護すべき情報がそのシステム上で取り扱われる
  - 暗号化以外の対策がほどこされていない(多重防御が講じられていない)

ii. クリプト・インベントリの構築・更新

第3章(国内外の対応状況)で述べたとおり、既存の量子脆弱性をもつ暗号からPQCへの移行を組織内で行うにあたり、移行の対象となる公開鍵暗号アルゴリズムによって保護されている資産を把握しておく必要がある。そのためにクリプト・インベントリを作成し、量子脆弱性をもつ暗号が現時点においてどこで使用されているかを特定する。複数の既存のガイダンスでもPQC移行の早期の段階でクリプト・インベントリの作成が推奨されているが、インベントリに含める情報や収集方法についてはガイダンス毎に様々である。

インベントリに含める情報として既存のガイダンスではどのように言及しているかを述べる。

- オーストラリア信号局（ASD）では公開鍵暗号を使用する環境内の全てのアプリケーションや IT 機器を特定してインベントリを作成することが推奨されている[87]。
- オランダ総合情報保安局（AIVD）はソフトウェア・ハードウェアに関わらず組織で使用されている全ての暗号の網羅的なリストを作成することを求めている。さらに大抵の組織では公開鍵暗号アルゴリズムによって保護されている資産の大部分は外部ベンダーから提供されていることを踏まえて、AIVD はベンダーが量子耐性のあるソリューションに移行しているか、それらを提供できるかどうかを確認し、新しいベンダーを選択することも考慮に入れている[88]。
- シンガポール金融管理局（MAS）はクリプト・インベントリに使用されている暗号アルゴリズムとその鍵長、暗号資産の所有者及び管理責任者、暗号アルゴリズムが組み込まれた、または使用されているシステム及びアプリケーションの情報を含むことを求めている[89]。
- FS-ISAC は第 3 章で挙げたように、重要度が高い、または高可用性が求められるアプリケーションや組織内部のアプリケーションと外部のアプリケーションを接続するシステムに関するクリプト・インベントリを整備することを求めている。
- 欧州電気通信標準化機構（European Telecommunications Standards Institute, ETSI）ではクリプト・インベントリの収集及び準備のため、リスク評価・データ取扱方針・暗号学的特性・暗号用途・サプライチェーンに関与する資産の 5 つのカテゴリーを考慮してインベントリを作成することを求めている[90]。

インベントリ作成に必要な情報収集方法としては、一般的には暗号利用システムを構築した担当者（開発ベンダー含む）に問い合わせることが考えられるが、より正確かつ網羅的に調査するために例えばコード解析用のツールを使用してアプリケーションで利用されている暗号を把握するという方法も存在する[91]。FS-ISAC では収集方法について手作業やスキャンツール利用を含めて複数提示している[92]。上記を踏まえ、

---

[87]Planning for Post-Quantum Cryptography (https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/planning-post-quantum-cryptography)

[88] The PQC Migration Handbook (https://english.aivd.nl/publications/publications/2023/04/04/the-pqc-migration-handbook)

[89]Advisory on Addressing the Cybersecurity Risks Associated with Quantum (https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/mas-quantum-advisory/mas-quantum-advisory.pdf)

[90]TR 103 619 (https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf)

[91]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 (https://www.imes.boj.or.jp/research/papers/japanese/23-J-13.pdf)

[92] Infrastructure Inventory Technical Paper(https://www.fsisac.com/hubfs/Knowledge/PQC/InfrastructureInventory.pdf)

クリプト・インベントリ構築時に収集する情報の例を表 5.1 に記載する。

表 5.1 クリプト・インベントリの構成例

スコープ	自組織で利用される暗号機能をもつシステムで、以下も対象に含んだ上で優先度が高いシステムから構築する。 ● 自組織開発のシステム ● 自組織外から提供されたシステム及び製品
収集する情報	以下の情報を含めることが想定される。 ● 暗号利用場面：例えば以下のような情報が想定される – ユーザーとの通信 – インターネットVPNによるリモートアクセス – 電子文書や電子メールへの署名 – サーバ証明書による認証 – データベースの暗号化 ● 暗号用途：例えば以下のような情報が想定される – 通信内容を保護するため – お客さま情報を安全に保存するため – 文書の改ざんを防ぐため – サーバのなりすましを防ぐため ● 暗号実装箇所：例えば以下のような情報が想定される – 自組織開発のアプリケーションへの独自実装 – 自組織外から提供された製品（ハードウェア/ソフトウェア/アプリケーション） ● 利用アルゴリズム：例えば以下のような情報が想定される – RSA-OAEP – ECDH – RSA-PSS – ECDSA ● 利用している暗号鍵長 ● 利用している暗号鍵の更新頻度 ● 暗号鍵管理方法：例えば以下のような情報が想定される – 自組織所有のHSMにて管理 – クラウドサービスで管理 ● 長期間保護が必要なデータとの接点有無：例えば以下のようなケースが想定される – インターネット経由での当該データ送受信 – 対象システムと接続する外部委託先のシステム上での当該データの保管

	● 利用システムの担当者
収集方法	以下のとおり複数の手段が考えられる。 ● システム担当者へのヒアリング ● 開発ベンダーや製品ベンダーへのヒアリング ● ネットワークスキャンツールによる発見 ● アプリケーションコード解析による発見

クリプト・インベントリは一度作成しておけば良いものではなく、定期的に更新すること、並びに、対象システムの更改等の変更があったときに都度更新することが、適切な PQC 対応の実現の前提となる。

iii. アーキテクチャの構築・更新

量子脆弱性をもつ暗号を使用しているシステムから量子耐性のあるシステムへの移行においては、一般的には単に量子脆弱性をもつ暗号から PQC に置き換えることを短期間で完了させることができるとは断言しがたい。理由としては以下のとおりである。

- アプリケーションの実装が利用している暗号方式に強く依存している場合、PQC への移行時に暗号機能以外の改修も必要になり、移行開始から完了まで相応の期間を要する可能性がある。
- PQC は既存の暗号と比べて新しい技術であるため、将来的に効率の良い解読法が発見される可能性も少なくない。そのため、PQC に単一的に移行することについて利用者から十分な信頼を得られないことが考えられる。

上記の暗号移行の長期化や安全性に対する懸念への対策として、クリプト・アジリティ(暗号の俊敏性)の組み込みやハイブリッド方式の利用が考えられる。

クリプト・アジリティとはシステムで利用されている暗号方式から別の暗号方式への移行をスムーズかつ影響を最小限にしながら実施できるように実装するシステムの特性を指す[93]。2024 年 10 月に FS-ISAC より公表されたクリプト・アジリティ構築に関するガイダンスでもクリプト・アジリティについては同様の考え方である[94]。クリプト・ア

[93] Quantum Computing Risks to the Financial Services Industry(https://x9.org/download-qc-ir/)

[94] Building Cryptographic Agility in the Financial Sector(https://www.fsisac.com/hubfs/Knowledge/PQC/BuildingCryptographicAgilityInTheFinancialSecto

ジリティを付与するタイミングとしては、システムの開発・改修に歩調を合わせる形が効率的であり、例えば PQC を動作可能にする以前にシステム更改が行われる場合、そのタイミングで付与するのが望ましいと考えられる[95]。具体的なクリプト・アジリティの付与方法の例として以下のような対応が挙げられる。

- アプリケーションで暗号を利用する場合、メインルーチンでは抽象化した暗号機能の呼び出しに留め、具体的なアルゴリズム・パラメータによる処理を分離しておく。
- 標準化された PQC アルゴリズム及びパラメータを選択可能な製品や標準化されたプロトコル仕様にしたがって実装された製品を導入する。
- 電子証明書や IC カード等、暗号機能の一部となるものまたは暗号処理そのものを実施するもので第三者に配布するようなものの場合、有効期限を比較的短いものに設定する。
- PQC の適用がされない可能性があるプロトコル及びそのバージョンについてはアップグレードを図る。具体的には TLS1.2 から TLS1.3 の移行が挙げられる[96]。

クリプト・アジリティは量子脆弱性をもつ暗号から PQC への 1 回のみの移行だけでなく、複数回の暗号移行も考慮することが望ましい。PQC に移行後、利用している暗号アルゴリズムもしくはその実装に対して安全性低下に繋がる可能性のある攻撃方法が新たに発見された場合、直ちに別の PQC に切り替えられるようにするようなケースが想定されるからである。

ハイブリッド方式は PQC 移行の文脈において 1 つの暗号機能に対して既存の暗号方式と PQC 方式を組み合わせて用いる方法である。既存の量子脆弱性をもつ暗号から比較的新しい PQC に単一的に移行することについて十分な信頼を得られない可能性を考慮して両方を組み合わせて用いることで、どちらか一方のアルゴリズムが危殆化しても安全性が維持できることを目指しているものである。ハイブリッド方式は主に PQC への完全移行までの移行期間中に利用されるものと考えられ、早期の段階で量子耐性を確保できることからクリプト・アジリティ付与方法の 1 つでもあると考えられる。

ハイブリッド方式をアプリケーションで独自に実装する際には注意が必要である。

---

r.pdf)

[95] 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 (https://www.imes.boj.or.jp/research/papers/japanese/23-J-13.pdf)

[96] IETF が TLS1.2 のメンテナンスを実施しないという方針を提示 https://datatracker.ietf.org/doc/draft-ietf-tls-tls12-frozen/

異なる安全性をもつ暗号方式を複数組み合わせて使うため、実装ロジックによってはハイブリッド方式の系全体の安全性が一番弱い安全性の暗号方式に依存してしまうことになる可能性がある[97]。そのことが思いもよらない攻撃法が発見されることに繋がってしまうリスクになる。英国 NCSC では、ハイブリッド方式利用に限らず標準化されていない PQC を早期導入することは推奨していない[98]。インターネット VPN の実現手段の 1 つである IPsec で使われている鍵交換技術である IKEv2 のハイブリッド方式が RFC 9370 として公開されているほか[99]、TLS については執筆時点で IETF にてハイブリッド方式のドラフトが作成されている[100]。ハイブリッド方式はこのような完了済み・検討中の標準化方式にしたがって利用するのが望ましいと考えられる。

なお、PQC 移行に相応の時間がかかり、その間、通信相手のなかには PQC やそれを用いたハイブリッド方式の実装に対応できない場合も想定される。こうした場合でもサービス提供を継続するために、既存の通信方式も維持するためのシステムを準備することも必要に応じて検討することが望ましい。

iv. 耐量子計算機暗号対応の期限の考え方整理

CRQC の登場時期が不明ながらも、世の中の PQC のアルゴリズムへの移行の流れから外れてしまうことによるビジネスリスクを考慮すると、優先度が高いシステムについては 2030 年代前半から半ばまでを目安に PQC のアルゴリズムを利用可能な状態にしておくことが推奨される。当然、現在時点で設定した期限は固定ではなく、PQC のアルゴリズムへの移行に関わる法令・規制や CRQC の進展状況をフォローしながら柔軟に見直すことになると考えられる。

なお、上記の考えに基づいて定めた対応期限までに優先度が高いシステムに対する PQC のアルゴリズムへの移行が完了しない場合を不測の事態と捉えて、CRQC を用いた暗号危殆化リスクを低減させるための代替の対策を検討しておくことが望ましい。ASC X9 や AIVD によれば PQC に依存しないリスク低減策として以下のようなものがあるとされる[101,102]。

---

97 The PQC Migration Handbook(https://english.aivd.nl/publications/publications/2023/04/04/the-pqc-migration-handbook)

98 Preparing for Quantum-Safe Cryptography (https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography)

99 Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)(https://datatracker.ietf.org/doc/rfc9370/)

100 Hybrid key exchange in TLS 1.3(https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/)

101 Quantum Computing Risks to the Financial Services Industry(https://x9.org/download-qc-ir/)

102 The PQC Migration Handbook(https://english.aivd.nl/publications/publications/2023/04/04/the-pqc-migration-handbook)

- 事前共有鍵(Pre-Shared Key)による通信の秘匿化[103]。
- 暗号化通信の利用もしくは適用箇所を必要最低限にするようなポリシーを定め、それに従う。
- 保護が必要な文書のうち、特に重要な文書へのデジタル署名については、物理的な原本を厳重に保管しておく。

(4) IT ベンダーとの連携

PQC への移行は組織単独で完結するものではなく、IT ベンダーとの連携は欠かせないと考えられる。NIST を始めとする既存のガイダンスにおいても、システムで利用されている製品のベンダーにおいて PQC への移行を計画しているのか、PQC アルゴリズムをいつごろ製品に組み込もうとしているのか等、ベンダーにて着実に PQC への移行を進めようとしていることを確認しておくことが望ましいとされている[104,105]。対応状況によっては新しいベンダーに切り替えることも考えられる。FS-ISAC では組織がベンダーの PQC 移行のステータスをよりよく理解するための複数の質問例を与えている[106]。ベンダーのトップマネジメントが PQC 対応に向けて外部有識者と連携できているか、クリプト・インベントリを整備できているか、移行の優先順位付けの方針が存在するか等、踏み込んだ質問となっていて、実際のベンダーヒアリングに活用することが可能であると考えられる。

また、自組織から IT ベンダーへの一方的な状況確認だけでなく、IT ベンダーに対して自組織における現状や課題認識を伝えることも行い、どのような対応が双方で可能かを議論する場を設けるなど、必要に応じて積極的に検討することでより移行対応が進みやすくなると考えられる。

上記のベンダーとの移行に向けた連携を組織全体としてどこまでの範囲で実施するかも検討しておくことが望ましい。1 つのシステム開発においても複数のベンダーが関与するため、組織全体で見たときにそれらベンダーとの連携状況を網羅的かつ正確に把握することは難しいとも考えられる。組織において PQC 移行を優先的に実施すべきシステムに関与するベンダーや、組織に関する重要情報・機密情報を扱うベ

---

[103] ただしこの方法は公開鍵暗号を使わずに通信を確立する方法のため、事前共有鍵を物理的な方法で共有することが必要。これが適用できる環境は極めて限定的であると考えられる。この方法を適用可能な条件としては AIVD による The PQC Migration Handbook4 章を参照されたい。

[104] Quantum-Readiness: Migration to Post-Quantum Cryptography(https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography)

[105] The PQC Migration Handbook(https://english.aivd.nl/publications/publications/2023/04/04/the-pqc-migration-handbook)

[106] Risk Model Technical Paper(https://www.fsisac.com/hubfs/Knowledge/PQC/RiskModel.pdf)

ンダーを中心に移行に向けた検討をしていくことが現実的であると考えられる。

PQC 移行の進捗状況だけでなく、組織で利用されている暗号技術を把握し、クリプト・インベントリとして管理する場合にも IT ベンダーとの連携は必要である。クリプト・インベントリの対象となるシステムを開発した IT ベンダーや、そのシステムで使われる製品ベンダーに問い合わせることで、暗号技術の利用状況をより正確に把握することができると考えられる[107]。

(5) 政府、監督当局、業界団体等に期待される取組み

i. 本邦サイバーセキュリティ政策における政府、監督当局、業界団体等の関係性

預金取扱金融機関は、本邦「サイバーセキュリティ基本法」[108]の趣旨に鑑み政府のサイバーセキュリティ戦略本部（事務局：内閣官房内閣サイバーセキュリティセンター、以下「NISC」）により策定・決定される「重要インフラのサイバーセキュリティに係る行動計画」[109]（以下「行動計画」という。概要は図 5.1 参照）において特定される重要インフラのうち、「金融」分野の重要インフラ事業者に該当する。

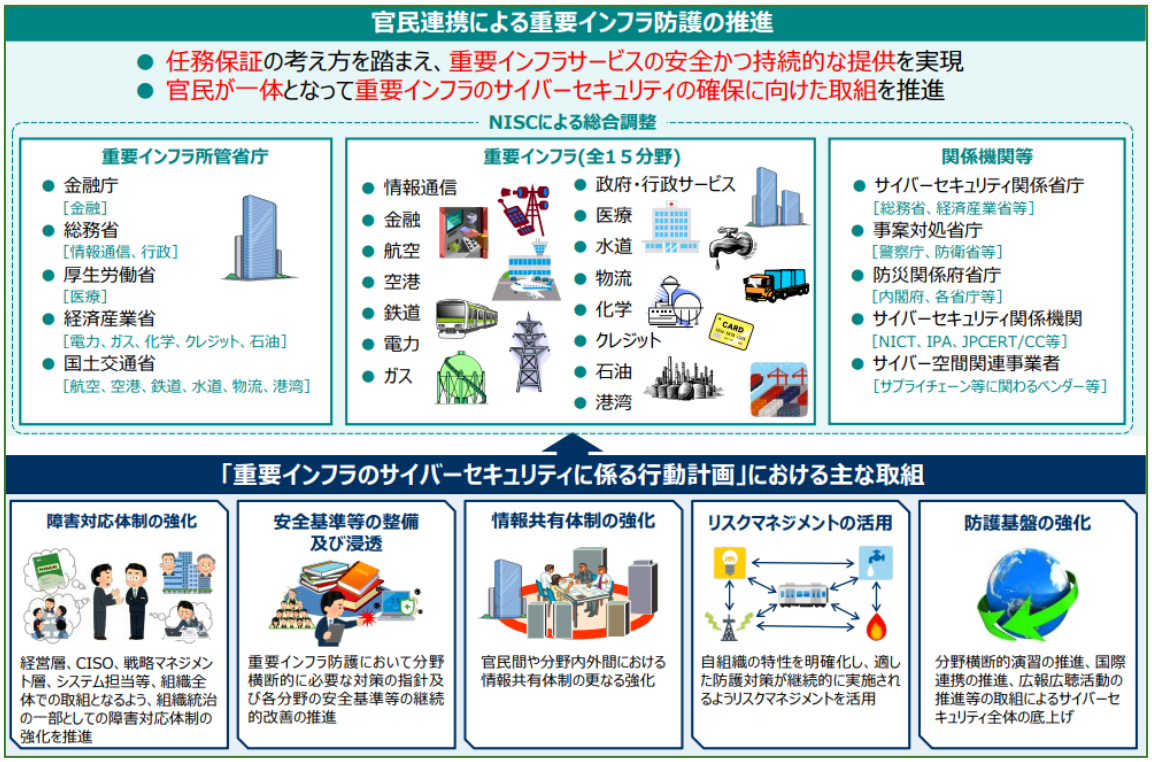
---

107 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 (https://www.imes.boj.or.jp/research/papers/japanese/23-J-13.pdf)

108 https://laws.e-gov.go.jp/law/426AC1000000104

109 https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2024.pdf

図 5.1 「重要インフラのサイバーセキュリティに係る行動計画」の概要



(備考)https://www.nisc.go.jp/pdf/policy/infra/cip_policy_abst_2024.pdf より引用

現行の行動計画において、重要インフラは、金融分野のほか情報通信分野や電力分野、鉄道分野等が具体的に特定されている。重要インフラは、そのサービス提供に当たり相互に依存関係が存在し、一例を挙げれば、預金取扱金融機関が顧客にサービス提供するにあたっては、それがインターネットバンキングである場合には、情報通信分野及び電力分野のサービス、営業店による場合には、情報通信・電力両分野に加えて、従業員が営業店に参集するにあたり利用される鉄道分野のサービスの提供が維持されることも必要不可欠と考えられる。他方で、サービスを提供する側の立場からは、預金取扱金融機関のサービス停止が、他分野におけるサービス提供に影響を及ぼし得る可能性を無視することもまた困難であろう。

重要インフラサービスの継続的提供を確かなものとするためには、こうした相互依存性にも目を向けながら、NISC による総合調整のもとで、重要インフラ所管省庁(監督当局)、重要インフラ(全 15 分野の業界団体・中央組織、預金取扱金融機関等の重要インフラ事業者)及び関係機関等が一体となりサイバーセキュリティの確保に向けて取り組むことが肝要であろう。

ⅱ. 政府、監督当局、業界団体等に期待される取組み

前述のとおり、重要インフラには相互に依存関係が存在するものの、その所管省庁

(監督当局)は 5 省庁、重要インフラ分野は 15 分野にわたり、また、分野によっては規模や業容が異なる複数の業界・業態の事業者や業界団体等から構成される状況にある。こうした重要インフラの防護の当事者のほか、直接関与する関係機関(NICT、IPA、JPCERT/CC 等)における取組みや、関連事業者(IT ベンダー等)における対応も重要となることも踏まえれば、本邦全体での対応を推進する“旗振り役”の存在は必要不可欠であると考えられる。

この“旗振り役”をいかなる組織が担うべきかについては、本邦全体としての PQC 対応の「方針」にも記載されるかたちで明確化され、政府により公表されることが望ましい。本項においては、今後の PQC 対応のなかで政府の“旗振り役”に期待される取組みを述べる。

（ア） 政府による重要インフラ分野横断的な議論等

具体的な取組事項として、PQC に係るリスク等が、本邦の重要インフラサービス提供にどの様に影響するかに係る分野横断的な議論が、重要インフラ相互間の依存関係を踏まえながら、政府において行われることが期待される。

第 3 章で述べたとおり、外国政府・当局においては、量子コンピュータがもたらす脅威から重要インフラ及び行政各部等を防護する観点での議論や、一部では既に具体的な対応が開始されている。それら具体的な対応のうち、本邦において議論を開始するにあたっての出発点として、アメリカにおける取組み（第 3 章 (2) ⅰ (ウ) 参照）も参考に、重要インフラや行政各部等、国民生活・経済社会活動にとって必要不可欠なサービス毎に、量子コンピュータによる脅威、脆弱性の度合い、リスクの大きさ等を分析・評価し、まずは対応の緊急度等を可視化する対応が一案として考えられる。

また、国民生活・経済社会活動への影響も考えれば、重要インフラや行政各部等だけでなく、関係機関(NICT、IPA、JPCERT/CC 等)や、産業界を含めた民間セクターにも検討や対応への参画を促していくことも有効と考えられる。先行事例として、欧州連合域内における PQC 移行のための戦略立案にあたり欧州委員会がとる考え方（第 3 章 (2) ⅱ (ア) A 参照)が参考になろう。

そうした取組みを通じて、本邦においても重要インフラ相互間における分野横断的なリスク等が確認された場合には、「暗号アルゴリズムの 2010 年問題」の際における取組み[110]も参考にしながら、NISC や重要インフラ所管省庁（監督当局）、関係機関等が、民間セクターや行政各部に対し、PQC 対応を促すことや、注意喚起を行うことが考えられる。

---

110 「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」https://www.nisc.go.jp/pdf/policy/general/angou_ikoushishin.pdf

（イ） 海外規制動向に係る情報収集・提供

また、本成果物の第 3 章に記載のとおり、PQC 対応については海外における取組みが先行している。そのなかで、米欧においては、政府と密接な関係にある専門機関（NIST 等）が中心となり、行政機関や各産業界を対象として、PQC 対応を求める要請等がされているところである。

米欧における今後の規制シナリオは様々想定されるものの、影響や対応負荷が大きいと考えられるシナリオとして、「自国内（アメリカ内・欧領域内等）でのサービス提供や、行政機関・企業・消費者等との取引において、PQC 対応未了の企業等との取引を規制すること」が懸念される。

こうした規制に係る情報については、基本的には、海外取引に参入している個々の預金取扱金融機関が自ら収集するべきであるものの、規制の対象が、当該国の行政機関や金融機関等になる以上、当該国の政府からみて外国企業となる本邦預金取扱金融機関に対する情報提供が充分にされないことも想定しておく必要がある。

かかる事態への予防的対応として、本邦関係省庁と業界団体等が連携しての情報収集が行われることや、収集された情報のうち、関係者で共有されるべきものについては、省庁間や分野・業界間といった垣根を越え、民間セクターを含めて共有されることが期待される。

（ウ） 移行ロードマップの策定等

PQC 対応をより促進する観点では、移行ロードマップを策定し、社会全体で共有する取組みや、移行状況の実態を把握する取組みも有効と考えられる。

ロードマップを策定する際の粒度や単位（所管省庁毎や分野毎等）は、重要インフラ所管省庁（監督当局）における規制の在り方や、個々の重要インフラ分野の特性に加え、重要インフラ分野横断的なリスク等も参考にしながら検討、決定されると考えられるものの、他の重要インフラとの依存関係が比較的強いと評価されるであろう分野が複数存在することも踏まえれば、総合調整の機能を担う NISC や、重要インフラ各分野の規制を担う重要インフラ所管省庁（監督当局）との連携が重要と考えられる。

以上のほか、個々の監督当局・業界団体等として取り組むべき施策の掘り起こしを行い、実施に向けた検討を行うことも期待される。一案として、社会全体に対する PQC 対応の必要性の広報や、個別の預金取扱金融機関が顧客に対して PQC 対応を求める際の周知ツール（チラシの調製等）の作成が考えられる。

ⅲ． 重要インフラの防護に関与する全ての組織に対する期待

上記のとおり、本章においては、金融分野の PQC 対応がより促進されるために必要と考えられる、国や監督当局、業界団体等における取組みについての一案を提示した。今後、NISC、重要インフラ所管省庁、重要インフラ（全15分野）及び関係機関等

においても、各々PQC 対応に係る検討がされると思われるが、当検討会としては、この際、個々の組織内部における PQC 対応に留まらず、社会全体での PQC 対応についても意識され、議論が興されることに期待する。

6. 耐量子計算機暗号対応に向けた課題・留意事項

(1) 戦略・態勢面

i. 経営陣の理解

PQC 対応は自社のリスクマネジメントにおける重要課題であり、経営層が全社施策としてリーダーシップを発揮して企画・推進することが望ましい。また、各システムの責任者も、リスクの大きさを把握した上で対応方針の意思決定をし、責任をもって対応することが望ましい。

一般的に、本邦金融機関はシステム開発・運用における外部委託先への依存度が高い。そのため、PQC 対応に向けたクリプト・インベントリの作成・更新やリスクアセスメント、移行・運用対応においては外部委託先との連携が欠かせない。一方、システムの単位でもマルチベンダー体制がとられることも珍しくない中、ベンダーの PQC 対応に向けた準備・対策状況にばらつきがあり、ベンダーにおける対応に完全に依拠する対応では限界があるため自社でオーナーシップをもって取り組むことが望ましい。

ii. 関係者の役割・責任の明確化

PQC 対応においては組織内外における多岐にわたるステークホルダーとコミュニケーションを取りながら推進することが望ましい。特に、組織内においてはビジネス部門、サイバー部門、IT部門、リスク管理部門、内部監査部門、広報部門等で役割・責任を明確にしながら推進することが肝要である。

ICT 業界、製品調達先・開発先のベンダーが対応しないと PQC 対応が出来ないおそれがあるため、他業界の動きを注視しながら連携・働きかけをすることが望ましい。ただし、ステークホルダーが多様であるため、各金融機関から個別に連携・働きかけをするとともに、業界団体や当局との連携も重要である。

金融機関で協力できる部分は協力する体制を作り、各金融機関が個別に検討するのではなく、共通する課題は協力・分担して進めていくという体制が、効率的な対応の推進、業界としての対応の共通化、ステークホルダーへの説明の共通化といった点でメリットがある。

また、第 5 章(金融分野における耐量子計算機暗号対応に向けた推奨事項)で述べている通り PQC 対応をより促進する観点から金融分野として移行ロードマップを策定し、社会全体で共有することで、移行状況の実態を把握する取組みは有効である

と考えられ、今後、当局や業界団体を含め、業界として協力して取り組む課題を抽出し、検討する枠組みの構築等が課題である。

iii. リソース(ヒト・カネ)の確保

PQC 対応においては、対象となる範囲が広く活動が長期にわたるため、活動の全体ロードマップと活動計画を策定し、計画的にリソース(ヒト・カネ)を確保して推進することが肝要である。特に、初期の活動として定義されるグランドデザイン/ロードマップの策定やクリプト・インベントリの作成といった活動により施策全体として必要となるリソースが見積れるようになり、ライフサイクルに合わせた対応等を検討することにより効率的に実施できることから、早めに取り組むことが肝要である。

金融機関のサイバー部門では、暗号に特化した部門・人材が十分に確保されていないことも想定され、既存のサイバー部門の役割・機能・体制の延長では PQC 対応の企画・管理・推進ができないことも視野にいれることが重要である。暗号領域は専門人材が不足しており、外部パートナーを含めてリソース確保に取り組む等の検討が期待される。

(2) 法令・規制面

2024 年 8 月に NIST は標準化した PQC のアルゴリズムの初版として 3 方式をリリースしたが、第 3 章で述べた通り、各国の政府・省庁はこの動きに先駆けて PQC 対応の移行計画と指針を整備している。現状では、法令・規制として制定されているものは少ないが、金融インフラに対する法令・規制の整備状況を継続的に注視することが重要である。

グローバルビジネスを展開している金融機関及び海外の企業や金融機関との間で暗号通信を実施している金融機関等では、相手国の組織が PQC 対応を先行させる可能性があり、自社でも PQC 対応を余儀なくされる可能性もある。また、海外当局との折衝、及び海外の法令・規制を遵守する必要性が出てくるため、こうした観点からも、海外の法令・規制を継続的に注視することが重要である。

(3) 技術面

i. 技術・運用面の課題

第 5 章で述べられているように、クリプト・アジリティは重要であり、どのように実現するかが重要な課題である。クリプト・アジリティの実現に向けた課題としては、暗号処理を疎結合とするアーキテクチャの策定・適用、証明書や暗号鍵管理の集約、使用されている暗号処理を把握するためのクリプト・インベントリの作成・更新、利用状況の監視を行えるような組織・プロセス・ツールの整備等があり、設計・実装上だけで

なく運用上の課題にも留意することが望ましい。

クリプト・インベントリの作成・更新や PQC 対応ソリューションの適用に際しては、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、業界団体等が情報を収集し、共有されることが望ましい。標準化技術に基づくソリューションを採用することにより、クリプト・インベントリの構築における精度・拡張性・柔軟性・スピードの確保や銀行間接続システム等の共通技術の利用が求められるシステムの移行の効率的・効果的な推進等が可能となる。本稿執筆時点で PQC 対応アーキテクチャやソリューションは開発中のものが多く、採用技術を見通すことが困難であることから継続的なモニタリングが必要であるが、クリプト・インベントリに関しては Ecma 国際標準（旧 CycloneDX v1.6）[111]にて定義されるフォーマット[112]の利用なども有効な選択肢となる。

ii. システム互換性の課題

顧客システム等ステークホルダーが多岐にわたるシステムでは PQC のアルゴリズムへの移行対応を一度・同時に完了させることは現実的ではない。そのため、移行の過渡期においては 1 つのシステム内に PQC 未対応のシステムと PQC 対応システムからの接続が混在することも見据え、両方の接続を実現する機能を考慮することが望ましい。その際、PQC 自体に加え、両方の接続を実現する機能についても新規技術が採用される可能性があるため、ソリューションの技術的アセスメント（自社システムに適用する際の非機能要件を含む）も重要である。

iii. 長期的なセキュリティ戦略との整合

PQC 対応はリソースの最適化の観点からシステムの大規模更改・改修タイミングに合わせたライフサイクルでの実施を基本として時間に余裕をもって検討することが重要である。ライフサイクルでの実施が難しいものは別途実施することになるが、個別対応が必要となるシステムにおいても、既存の施策への組み込みやシステム横断での推進等により効率的に実施することが望ましい。

---

111 「Ecma 国際標準に Cyclone DX v1.6 採択」 https://cyclonedx.org/news/cyclonedx-v1.6-now-an-ecma-international-standard/

112 「Cyclone DX v1.6 のフォーマット」 https://cyclonedx.org/guides/OWASP_CycloneDX-Authoritative-Guide-to-CBOM-en.pdf

（参考資料） 用語集

用語	用語意味
CRQC (Cryptographically relevant quantum computer / Cryptanalytically relevant quantum computer)	量子脆弱性をもつ暗号を現実的なリソースを用いて現実的な時間内で解読することが可能な量子コンピュータ
量子コンピュータ/量子計算機	量子力学の特性を用いて計算を行うコンピュータ
HNDL攻撃 (Harvest now, decrypt later / Store now, decrypt later / Retrospective decryption / Retrospective attack)	CRQCが実用化されていない現在においては暗号化データを収集し、CRQCが実用化された後にそれらを解読する攻撃
耐量子計算機暗号 / PQC(Post-Quantum Cryptography)	量子コンピュータが実用化されても、（現在のところ）効率的な攻撃方法が知られていない暗号
量子脆弱性をもつ暗号	量子コンピュータを用いて効率よく解読する方法が存在する暗号
量子耐性のあるシステム	量子コンピュータによる暗号解読に対して受ける影響が無視可能なシステム
量子脆弱性があるシステム	量子コンピュータによる暗号解読に対して受ける影響が無視できないシステム
クリプト・インベントリ/暗号インベントリ/暗号棚卸	各システムの暗号利用箇所や利用アルゴリズムなどの情報を一覧化した資料
クリプト・アジリティ/暗号アジリティ	システムで利用されている暗号アルゴリズムから別の暗号アルゴリズムへ、スムーズかつ影響を最小限にしながら、移行可能にするシステム特性

「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」
検討会メンバー名簿（敬称略、五十音順）

座長	寺井 理	株式会社みずほフィナンシャルグループ グループ執行役員・情報セキュリティ担当（グループ CISO） 金融 ISAC FinTech セキュリティワーキンググループ座長
メンバー	安藤 彰英	株式会社名古屋銀行 執行役員 業務部長
	岩崎 三郎	株式会社静岡銀行 リスク統括部長
	宇根 正志	日本銀行 金融研究所 参事役
	大城 徹	株式会社しんきん情報システムセンター 上席執行役員
	菅野 洋平	労働金庫連合会 情報システム部 副部長
	白井 大輔	株式会社三井住友フィナンシャルグループ グループ CISO サイバーセキュリティ統括部長
	高瀬 徹	農林中央金庫 IT 統括部長（システムリスク管理担当）
	松本 泰	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 フェロー
	峰 匡親	株式会社三菱 UFJ フィナンシャルグループ グループ CISO サイバーセキュリティ推進部 部長
	村山 朋彦	信組情報サービス株式会社 常勤取締役
オブザーバー	一般社団法人金融 ISAC、CRYPTREC 事務局、公益財団法人金融 情報システム センター、日本銀行 金融機構局、 内閣サイバーセキュリティセンター	
事務局	金融庁	

「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」
作業部会メンバー名簿（敬称略、五十音順）

部会長	福田 健太	株式会社三井住友フィナンシャルグループ 部長代理
メンバー	伊藤 彰志	株式会社みずほフィナンシャルグループ 次長
	伊藤 忠彦	独立行政法人情報処理推進機構 研究員
	宇根 正志	日本銀行 金融研究所 参事役
	岡野 裕樹	株式会社三菱 UFJ フィナンシャル・グループ 調査役
	長田 繁幸	株式会社日本総合研究所 シニアエキスパート
	唐沢 勇輔	Japan Digital Design 株式会社 Head of TDD
	神田 雅透	独立行政法人情報処理推進機構 部長
	設楽 佑一郎	株式会社三菱 UFJ フィナンシャル・グループ 上席調査役
	中山 雄司	株式会社みずほフィナンシャルグループ 調査役
	森 雄喜	株式会社三井住友フィナンシャルグループ 部長代理