IMES DISCUSSION PAPER SERIES

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

宇根正志（うね まさし）

Discussion Paper No. 2023-J-13

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

IMES Discussion Paper Series 2023-J-13
2023 年 9 月

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

宇根正志（うねまさし）*

要　　旨

大規模かつ実用的な量子コンピュータが実現した場合、それを用いて主要な暗号アルゴリズム（公開鍵暗号）を効率的に解読することができるようになるとみられている。このリスクに対処するために、量子コンピュータを用いても解読が困難と評価されている暗号への移行に向けた検討が海外を中心に活発化している。アメリカ政府は、量子コンピュータに対して耐性を有するアルゴリズムとして 4 つのアルゴリズムを標準化する方針を 2022 年 7 月に発表した。また、ドイツ、フランス、オランダ、イギリス、カナダ、オーストラリアのセキュリティ当局は、IT システムの運営者に対し、量子コンピュータによる暗号解読に関するリスク評価や、アルゴリズム移行などの必要な対応の検討を推奨している。金融分野では、FS-ISAC が暗号の移行に関する検討を進めている。金融機関が量子コンピュータによる暗号解読のリスクに適切に対処していくうえで、こうした動向をタイムリーにフォローし、自社での検討に活かしていくことが重要であろう。

キーワード：暗号アルゴリズム、公開鍵暗号、リスク評価、量子コンピュータ
JEL classification: L86、L96

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

本稿は、2023 年 8 月 31 日時点の情報をもとに作成した。本稿の作成に当たっては、菅野哲氏（GMO サイバーセキュリティ by イエラエ株式会社）より有益なコメントを頂戴した。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

安全な金融取引を実行するうえで、暗号は欠かせない存在となっている。インターネットを介した金融サービスでは、顧客（スマートフォンやパソコン）と金融機関（サーバ）との間で通信されるデータを第三者から保護するために共通鍵暗号や公開鍵暗号が使用されているほか、アクセス先のサーバが実際に金融機関のサーバか否かを顧客が確認する際に、公開鍵暗号をベースとする電子証明書やその関連技術が用いられている（Seito [2017]）。こうした暗号を採用するにあたって、それがサービス内容に見合ったセキュリティを確保していることを確認するとともに、採用後も、そのセキュリティが著しく低下していないか（当該サービス提供に支障がないか）、また、その予兆がみられないかといった観点から暗号のセキュリティの動向を注視することが求められている。

暗号のセキュリティ動向に関して、近年、量子コンピュータが暗号に及ぼす影響に注目が集まっている（宇根・菅［2021］）。将来、大規模かつ実用的な量子コンピュータが実現すると、公開鍵暗号の主要なアルゴリズム（RSA 暗号[1]や楕円曲線暗号）が効率的に解読されるおそれがあると指摘されている（四方［2019］、CRYPTREC 暗号技術調査ワーキンググループ（耐量子計算機暗号）［2023a, b］）。こうした主要な公開鍵暗号を解読するのに十分な能力をもつ量子コンピュータは、暗号解読可能量子コンピュータ（CRQC：cryptographically relevant quantum computer）と呼ばれることが多い。

例えば、長期間秘密にしておく必要がある取引データ、または、それを（共通鍵暗号によって）暗号化する際に用いたセッション鍵を、公開鍵暗号によって暗号化したうえでインターネットを介して通信していたとしよう。取引データを解読したい攻撃者は、暗号化された取引データやセッション鍵を通信途上で取得・保管しておき、CRQC を使用できるようになったタイミングで解読を試みる（ハーベスト攻撃）可能性がある（Communications Security Establishment [2020]）。また、取引データの一貫性（integrity）を確保するために、当該データにデジタル署名が付与されていたとする。この場合、仮に CRQC が実現したとすると、取引データに付与されているデジタル署名やそれを検証するための電子証明書が信頼できないものとなり、取引データの改変の有無を確認することが困難となる可能性がある。

こうした CRQC による暗号解読のリスクに対処するために、海外のセキュリティ当局は、既存のコンピュータやネットワーク機器の使用を前提としつつ、CRQC を用いても解読が困難な暗号[2]を今後採用する方向で検討を進めている。

---

[1] RSA は米国 RSA Security LLC.の登録商標である。

[2] 今後採用の候補となる暗号として、既存のコンピュータやネットワーク機器の使用を前提とす

このような暗号は、英語では、「post-quantum cryptography」、「quantum-safe cryptography」、「quantum-resistant cryptography」などと呼ばれているが、本稿では、CRYPTREC[3]のガイドライン（CRYPTREC 暗号技術調査ワーキンググループ（耐量子計算機暗号）［2023a］）において使用されている「post-quantum cryptography（PQC と略す）」を用いることとする。また、PQC に対応する日本語についても、上記のガイドラインで耐量子計算機暗号と呼ばれていることから、この用語を使用する。

アメリカは、NIST（National Institute of Standards and Technology）[4]が連邦政府機関において使用される PQC のアルゴリズムの標準化を 2016 年から推進しており、4 つのアルゴリズムを標準化する方針を 2022 年 7 月に発表している。また、ドイツ、フランス、オランダ、イギリス、カナダ、オーストラリアは、セキュリティ当局が CRQC によるリスクへの対処について検討する際の留意事項やガイドラインをそれぞれ独自に公表し、PQC のアルゴリズムへの移行に向けた検討に着手することを推奨している。金融分野においても、FS-ISAC[5]が PQC のアルゴリズムへの移行に向けた検討を開始している。

この点、わが国では、CRYPTREC が、CRQC や PQC の研究動向を調査しており、その成果として PQC のガイドラインと技術報告書を 2023 年 3 月に公表し

る暗号のほかに、量子鍵配送（quantum-key distribution）と呼ばれる技術に基づく暗号が挙げられる（National Cyber Security Centre [2020]）。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。量子鍵配送に基づく暗号を使用するためには、専用のネットワーク機器を導入する必要があるなどの実装上の制約が存在することなどから、本稿で紹介する海外のセキュリティ当局のうち、本稿執筆時点で導入を推奨している先は筆者が知る限り存在していない。こうした点を踏まえ、本稿では、既存のコンピュータやネットワーク機器を使用できる暗号に焦点を当てることとする。

[3] CRYPTREC（Cryptography Research and Evaluation Committees）は、電子政府における調達のために参照すべき暗号の安全性を評価・監視し、それらの適切な実装・運用の方法を調査・検討するプロジェクトである（https://www.cryptrec.go.jp）。暗号技術検討会（事務局：総務省・経済産業省・デジタル庁。座長：横浜国立大学・松本勉教授）およびその下に設置された暗号技術評価委員会（委員長：東京大学・高木剛教授）と暗号技術活用委員会（委員長：横浜国立大学・松本勉教授）によって構成されている。なお、暗号技術調査ワーキンググループ（耐量子計算機暗号）は暗号技術評価委員会の下に設置されている。

[4] 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、連邦政府機関が使用する情報技術の標準規格（FIPS：Federal Information Processing Standards）の策定を担っている（https://www.nist.gov/about-nist）。

[5] FS-ISAC（The Financial Services Information Sharing & Analysis Center）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を提供している非営利団体である。アメリカに本部があり、75 ヵ国の金融機関がメンバーとして参画している（https://www.fsisac.com/who-we-are）。

ている（CRYPTREC 暗号技術調査ワーキンググループ（耐量子計算機暗号）［2023a, b］）。

金融機関は、将来の CRQC による暗号解読のリスクに適切に対処していくうえで、こうした文書やガイドライン、検討結果を自社での検討に活かしていくことが有用である。

本稿では、まず 2 節において、IT システムにおける暗号アルゴリズムの一般的な移行プロセスを示す。3 節で、海外の主なセキュリティ当局が公表している文書を参照し、CRQC による暗号アルゴリズムへの影響や対応に関する推奨事項を紹介する。4 節では、金融分野における取組みの事例として、FS-ISAC のペーパーの概要を紹介する。5 節では、3、4 節で取り上げた各種文書やガイドラインの内容を踏まえ、アルゴリズム移行に関する検討を行う際の留意事項や課題を考察する。

２．暗号アルゴリズムの移行プロセス

（１）５つのフェーズ

暗号アルゴリズムの移行プロセスは、一般に、次の 5 つのフェーズに分けることができる（図 1 を参照）。

① **【状況把握】**IT システムの運営者（以下、運営者）は、現在使用している暗号アルゴリズム（以下、現行アルゴリズム）の状況を把握する。
② **【影響・リスク評価】**運営者は、現行アルゴリズムが解読されたときにどのような影響やリスクが IT システムやそれを用いたサービスに及ぶかを評価する。
③ **【対象特定】**運営者は、上記の評価結果を踏まえ、移行の対象を特定する。
④ **【計画立案】**運営者は、暗号アルゴリズムの移行計画を立案する。
⑤ **【計画実行】**運営者は移行計画を実行する。現行アルゴリズムによって保護

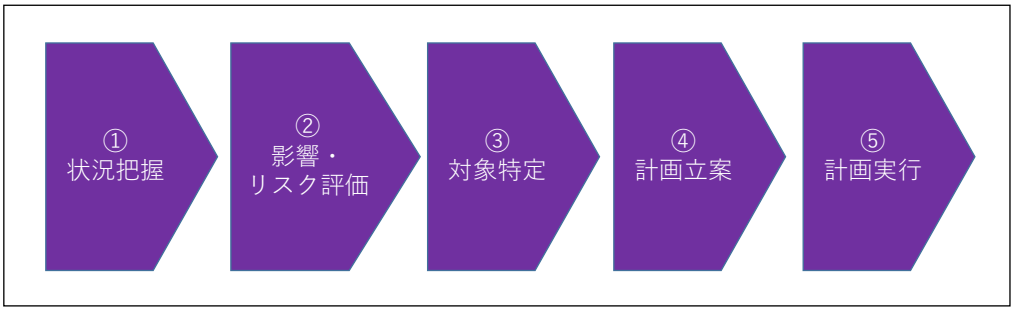

図 1 暗号アルゴリズムの移行プロセス

してきたすべてのデータの使用期限が到来するまで現行アルゴリズムの使用を継続する（使用期限が到来したタイミングで移行完了となる）。

（２）現行アルゴリズムの使用状況調査

状況把握のフェーズでは、現行アルゴリズムの使用状況を IT システムやサービスごとにそれぞれ調査し、使用状況に関する情報を収集する。そうした情報として、例えば以下が想定される。なお、それぞれの情報を整理・記述する方法にはさまざまな形態がありうる。

- 現行アルゴリズムを特定する情報（名称、用途、パラメータ〈例：鍵のサイズ、平文・暗号文のサイズ〉など）
- 暗号化の対象となるデータに関する情報（当該データの内容・用途・保存期間〈データが暗号化されてから破棄されるまでの期間〉、当該データの重要度、法律や規制によって保護が義務付けられている期間など）
- セキュリティ要件（達成すべきセキュリティ特性とそのレベルなど）
  —— セキュリティ要件は、暗号化もしくはデジタル署名の対象となるデータの特性に依存することから、当該特性と整合的しているかという観点から確認しておくことが有用である。
- 性能要件（暗号処理速度、通信速度など）
- 動作環境（現行アルゴリズムと連動して動作するソフトウェア、OS など）

運営者は、こうした情報を適宜アップデートすることが必要となる。暗号アルゴリズムの使用状況に関する情報を収録・管理する仕組みやその機構は「クリプト・インベントリ（crypto inventory）」と呼ばれることが多い。

（３）暗号アルゴリズムの移行計画の立案

計画立案のフェーズでは、運営者は、移行が必要と判断した現行アルゴリズムに関して、移行の優先順位付け、（現行アルゴリズムと組み合わせて運用する、あるいは、最終的な移行先となる）PQC のアルゴリズムの選定、それを動作させるソフトウェア（暗号ライブラリなど）やハードウェア（専用プロセッサなど）の選定を行うこととなる。

PQC のアルゴリズムを動作させるソフトウェアやハードウェアの選定では、運営者は、仕様書どおりに動作することや、期待どおりのセキュリティを確保し

ていることなどを確認する。公的機関が認定した試験機関によるテスト・評価[6]が実施されていれば、その結果を参照することが有用である。

３．海外のセキュリティ当局の動向

（１）NIST（アメリカ）における PQC のアルゴリズム標準化

NIST は、連邦政府機関が使用する現行アルゴリズムを PQC のアルゴリズムに移行するために、標準規格（FIPS）として採用する PQC のアルゴリズムの募集を 2016 年 12 月に開始した[7]。公募対象のアルゴリズムは、暗号化（public-key encryption）あるいは鍵カプセル化[8]（KEM: key encapsulation mechanism）のアルゴリズムと、デジタル署名のアルゴリズムである。

NIST は、3 つの評価フェーズ（第 1～3 ラウンド）を経て、4 つのアルゴリズムを標準する方針を 2022 年 7 月に発表した（Alagic *et al.* [2022]）。具体的には、暗号化あるいは KEM のアルゴリズムとして CRYSTALS-Kyber を選定したほか、デジタル署名用のアルゴリズムとして CRYSTALS-Dilithium、Falcon、SPHINCS+を選定した。NIST は、これらのアルゴリズムの詳細な仕様を決定したうえで、2024 年頃に標準規格文書を完成させる予定としている[9,10]。

また、NIST は、暗号化あるいは KEM のアルゴリズムに関して、別の 4 つのアルゴリズム（Classic McEliece、BIKE、HQC、SIKE）を継続して評価している（第 4 ラウンド）。今後、これらのなかから追加的に標準化されるアルゴリズムが選定される可能性がある。

デジタル署名のアルゴリズムについて、NIST は、選定した 3 つのアルゴリズムとは異なる数学問題の困難性に基づく方式を別途標準化する意向を示し、ア

---

[6] 代表的な例として、CMVP（Cryptographic Module Validation Program）が挙げられる。CMVP はアメリカ政府（NIST）とカナダ政府（Canadian Centre for Cyber Security）によって運営されている暗号モジュールのテスト・評価の枠組みである。詳細については、NIST のウェブサイト（https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program）や田村・宇根［2008］を参照されたい。

[7] NIST の PQC に関するウェブサイト（https://csrc.nist.gov/Projects/post-quantum-cryptography）において、PQC のアルゴリズム標準化に関する最新情報が公開されている。

[8] 鍵カプセル化のアルゴリズムは、共通鍵暗号用のセッション鍵などを通信当事者間で共有するためのアルゴリズムであり、公開鍵暗号の一種である。

[9] NIST は、標準化作業と並行して、PQC のアルゴリズムを導入する際のガイダンス（SP 1800-38A、Newhouse *et al.* [2023]）の作成をセキュリティ・ベンダーらと協力して進めている。

[10] NIST は、2023 年 8 月 24 日、CRYSTALS-Kyber、CRYSTALS-Dilithium、SPHINCS+の標準規格文書案（それぞれ FIPS 203、204、205）をウェブサイト（https://csrc.nist.gov/News/2023/three-draft-fips-for-post-quantum-cryptography）で公表し、パブリック・コメントを募集した。

ルゴリズムの募集を実施した。その結果、50 件のアルゴリズムが応募され、そのうち募集要件を満たした 40 件が標準化の対象とされた旨が 2023 年 7 月に発表された[11]。今後、デジタル署名のアルゴリズムの標準化が上記の第 4 ラウンドとは別に進められることになる。

PQC のアルゴリズムに関する標準規格が完成した後、各ベンダーは当該標準に準拠した暗号製品を製造し出荷するとみられる。その際、暗号製品を連邦政府の調達対象にするために、ベンダーが暗号製品を CMVP によるテスト・評価の対象とするケースが想定される。

（2）BSI（ドイツ）のガイドライン

ドイツの BSI（Bundesamt für Sicherheit in der Informationstechnik）[12]は、「Migration to Post Quantum Cryptography, Recommendations for Action by the BSI」と題するガイドラインを 2021 年 5 月に公表した（Bundesamt für Sicherheit in der Informationstechnik [2021]）。本ガイドラインは、長期的な視点でみると今後 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暗号アルゴリズムの移行の必要性や時期に関する検討に着手すべきとしている。主な推奨事項は以下のとおりである。

① IT システムの新規開発あるいは既存システムの更改にあたっては、クリプト・アジリティ（cryptoagility）[13]を付与するよう考慮すべきである。
② 現行アルゴリズムと PQC のアルゴリズムを組み合わせて実装するハイブリッド方式（hybrid solution）を採用すべきである。PQC のアルゴリズムのみを使用することを推奨しない。また、高いレベルのセキュリティが求められるアプリケーション（high-security application）においては、ハイブリッド方式の使用を（「推奨」ではなく）要求する（require）。
③ アルゴリズム移行の過程で、暗号プロトコルの仕様変更が生じる可能性についても視野に入れておくべきである。
④ KEM のアルゴリズムとして、FrodoKEM または Classic McEliece を採用す

---

11 本件は https://csrc.nist.gov/news/2023/additional-pqc-digital-signature-candidates において発表された。

12 BSI（英語の名称は Federal Office for Information Security）は、ドイツにおけるサイバーセキュリティ対策を担当する政府機関（https://www.bsi.bund.de/EN/Das-BSI/Leitbild/leitbild_node.html）。

13 クリプト・アジリティは、用語の定義についてコンセンサスがまだ得られていないが、「IT システムにおいて使用されている暗号アルゴリズムを、円滑かつ最小限の負担で別のアルゴリズムに入れ替えることを可能にする IT システムの特性」という意味で用いられることが多い（Accredited Standards Committee X9, Inc. [2022]）。

ることを推奨する。

⑤ 共通鍵暗号で用いられるセッション鍵を配送するために公開鍵暗号のアルゴリズムを使用しているケース[14]において、短期間でセッション鍵を保護する必要がある（アルゴリズム移行の時間的余裕がない）場合には、セッション鍵を生成するためのマスター鍵（pre-distributed symmetric long-term key）を通信当事者間で（オフラインなどで）事前に共有するという方法を検討することを推奨している。

上記④に関して、本ガイドラインによって推奨されている KEM のアルゴリズムは NIST による標準化アルゴリズムとは異なっている。この点について、本ガイドラインは、作成時点（2021 年）においてデータの保護を早急に実現する必要があったため、NIST の標準化完了に先立ち、セキュリティの観点から相対的に望ましいと評価できるアルゴリズムを選定・推奨したと記述している。ただし、NIST の標準アルゴリズムが決定した後、その結果を考慮しつつ、当該アルゴリズムをドイツの暗号アルゴリズムのガイドラインに追加する可能性がある旨も記述している。

上記⑤に関して、本ガイドラインは、データの送信者と受信者が通信のセッションを開始する際にマスター鍵に一定の変換（key derivation process）を施して新しいセッション鍵を生成し、それを用いてデータ本体を暗号化・復号するという方法を紹介している。

（３）ANSSI（フランス）のポジション・ペーパー

フランスの ANSSI（Agence Nationale de la Sécurité des Systèmes d’Information）[15]は、「ANSSI views on the Post-Quantum Cryptography Transition」というタイトルのポジション・ペーパーを 2022 年 3 月に公表している（Agence Nationale de la Sécurité des Systèmes d’Information [2022]）。

本ポジション・ペーパーは、CRQC が現行アルゴリズムに及ぼす影響に関して、ハーベスト攻撃によるリスクを適切に評価し、そのリスクを許容できないと判断した場合には現行アルゴリズムから PQC のアルゴリズムへ可能な限り早期に（as soon as possible）移行することを推奨している。同時に、PQC のアルゴリ

---

14 ここでは、通信データ本体の暗号化を（CRQC による影響が比較的小さい）共通鍵暗号によって行い、その共通鍵暗号のアルゴリズムで使用される暗号鍵（セッション鍵）の共有を公開鍵暗号によって実施するケースが想定されている。このケースでは、CRQC によってセッション鍵が解読されたならば、そのセッション鍵によって通信データ本体も解読されることになる。

15 ANSSI（英語の名称は French National Cybersecurity Agency）は、フランスにおけるサイバーセキュリティ対策を担当する政府機関（https://www.ssi.gouv.fr/en/mission/what-we-do）。

ズムへの移行に際して、本ポジション・ペーパーは、以下の課題に直面しうると指摘している。

① PQC のアルゴリズムが依拠している数学問題の困難性を定量的に評価することは、現時点では容易とはいえない。
② PQC のアルゴリズムにはさまざまなセキュリティ・パラメータが設定されており、所要のセキュリティ・レベルに対応したパラメータ（の組合せ）を選択することは容易でない。
③ PQC のアルゴリズムのセキュリティを評価できたとしても、それを部品として用いる暗号プロトコルの評価を別途行う必要がある。
④ サイドチャネル攻撃[16]などの実装上の脆弱性を悪用する攻撃に関して、PQC のアルゴリズムを実装した暗号ハードウェアなどの評価や対策の手法が確立しているとはいえない。

こうした状況を踏まえ、本ポジション・ペーパーは、BSI のガイドラインと同様に、PQC のアルゴリズムを単独で使用することを当面推奨せず、ハイブリッド方式（hybrid mechanism）での実装を推奨している。ただし、PQC のアルゴリズムの標準化や学界における研究・評価の蓄積が今後進めば、PQC のアルゴリズムに対する信頼が徐々に高まり、PQC のアルゴリズムを単独で使用できる状況になるとの見方を示している。本ポジション・ペーパーは、こうした PQC のアルゴリズムを巡る状況の変化を次の 3 つのフェーズに分けて表現している。

- フェーズ 1（現在〈2022 年〉）: PQC のアルゴリズムの（実装を含めた）セキュリティを信頼することが難しく、「IT システムのセキュリティは現行アルゴリズムによって実現・維持する」というスタンスで臨む。PQC のアルゴリズムは多重防御（defense in depth）の手段の 1 つとしてハイブリッド方式で使用する。
- フェーズ 2（2025 年頃以降）: PQC のアルゴリズムに関する研究成果や評価結果が蓄積され、PQC のアルゴリズムのセキュリティに対する信頼が高まっていく。
- フェーズ 3（2030 年頃以降）: PQC のアルゴリズムのセキュリティに対する信頼が十分に醸成される。ハイブリッド方式から、PQC のアルゴリズム

16 サイドチャネル攻撃は、暗号アルゴリズムをパソコンや IC カードなどで動作させた際に予期せぬチャネル（サイドチャネル）から漏れる情報（消費電力パターン、処理時間パターン、漏洩電磁波パターンなど）を用いて秘密情報（パソコン等の内部に格納されている暗号鍵など）を効率的に推定するタイプの攻撃である。

を単独で使用する形態に移行する。

ハイブリッド方式で使用することができる PQC のアルゴリズムは、KEM のアルゴリズムとして CRYSTALS-Kyber と FrodoKEM、デジタル署名のアルゴリズムとして CRYSTALS-Dilithium と Falcon が推奨されている。また、本ポジション・ペーパーは、セキュリティ面で信頼できる PQC のアルゴリズムの基準を今後策定する予定であるとしている。

クリプト･アジリティに関しては､「暗号モジュール自体を交換することなく、当該モジュールに実装されている暗号アルゴリズムを更新することができる（という特性、機能）」と定義している。そのうえで、ベンダーに対して、今後開発する暗号モジュールでは可能な限りクリプト・アジリティを実現する方向で検討を開始することを推奨している。

（４）NBV（オランダ）のガイドライン

オランダの NBV（Nationaal Bureau voor Verbindingsbeveiliging）[17]は、CRQC が現行アルゴリズムに与える影響を説明するとともに、PQC のアルゴリズムへの移行に関する推奨事項を内容とするガイドラインを 2021 年 9 月公表した（Netherlands National Communications Security Agency [2021]）[18]。

本ガイドラインは､CRQC が実現し主要な公開鍵暗号が脆弱化する可能性について、ガイドライン公表時点では非常に小さいとしている。ただし、2030 年頃に実現する可能性を一部の専門家が指摘していることを紹介しつつ、2030 年以降も保護が必要なデータが存在する場合、ハーベスト攻撃による解読のリスクがあるとしている。そのうえで、このようなリスクの評価を行い、必要があれば対処の方法に関して検討に着手すべきであるとの見方を示している。

本ガイドラインは、上記のリスクへの対処方法として PQC のアルゴリズムへの移行を検討することを推奨している。その際にはハイブリッド方式（hybrid

---

[17] NBV（英語の名称は Netherlands National Communications Security Agency〈NLNCSA〉）は、オランダにおけるサイバーセキュリティ対策を担当する政府機関（https://english.aivd.nl/about-aivd/the-aivd-who-we-are）。

[18] オランダの研究機関である TNO（Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek。英語の名称は Netherlands Organisation for Applied Scientific Research）が、政府機関と共同で「The PQC Migration Handbook」を 2023 年 3 月に公表している（Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek, Centrum Wiskund & Informatica, and Algement Inlichtingen- en Veiligheidsdienst [2023]）。本ハンドブックは、NBV のガイドラインと整合的なスタンスで、インベントリの作成、リスク評価、アルゴリズム移行の計画の策定・実行の方法や推奨事項、留意点を示している。

construction）を採用するとともに、KEM のアルゴリズムとして Classic McEliece または FrodoKEM を使用することを推奨している。また、ハーベスト攻撃への早急な対処が必要であり、PQC のアルゴリズムへの移行の時間的余裕がない場合には、代替案として、公開鍵暗号で保護してきたデータを共通鍵暗号によって保護する[19]、あるいは、当該 IT システムをオフラインで運用する[20]といった対応を検討することを推奨している。

PQC のアルゴリズムへの移行の準備として、本ガイドラインは、以下の対応を実施することを推奨している。

- 保護すべきデータの内容、保護期間、現行アルゴリズムの種類など、保護対象データに関する情報を収集する（クリプト・インベントリの整備）。
- PQC のアルゴリズムに移行するために必要な時間、移行作業の対象となる暗号ソフトウェアや暗号装置を特定する。

また、IT システムの新設や改修のタイミングで新しい暗号モジュールを導入する場合、PQC のアルゴリズムへの移行が発生しうることを念頭において以下の対応を行うことを推奨している。

- 運営者は、ベンダーに対して、採用する候補となる暗号モジュールが PQC のアルゴリズムをサポートしているか否かを事前に問い合わせる。
- 採用する候補となる暗号モジュールのうち、クリプト・アジリティを有するものを選択して導入するよう努める。

（５）NCSC（イギリス）のホワイトペーパー

イギリスの NCSC（National Cyber Security Centre）[21]は、「Preparing for Quantum-Safe Cryptography」と題するホワイトペーパーを 2020 年 11 月に公表した（National Cyber Security Centre [2020]）[22]。

---

[19] 例えば、セッション鍵生成用のマスター鍵を（公開鍵暗号でなく）オフラインによって通信当事者間で事前に共有する、あるいは、デジタル署名の代わりに共通鍵暗号をベースとしたメッセージ認証子（message authentication code）を用いるなどの対応が挙げられる。

[20] 本ガイドラインは、IT システムをオフラインで運用することに伴うコストやサービス内容の低下による損失が CRQC によるリスク（を金銭換算した額）よりも少ないのであれば、オフラインでの運用も選択肢となりうるとしている。

[21] NCSC は、イギリスにおけるサイバーセキュリティ対策を担当する政府機関（https://www.ncsc.gov.uk/section/about-ncsc/what-we-do）。

[22] 本ホワイトペーパーは耐量子計算機暗号を「quantum-safe cryptography」と記載しているが、

本ホワイトペーパーは、暗号アルゴリズムによって長期間保護すべきデータを有する組織において、CRQC によるハーベスト攻撃に留意すべきであるとしたうえで、これに対処する方法として PQC のアルゴリズムへの移行が最も望ましいとの見方を示している[23]。

ただし、その際に採用する PQC のアルゴリズムについては、しかるべき標準化機関や公的機関による評価を経て標準化されたアルゴリズムに限定している。この点に関して、本ホワイトペーパーは、標準化されていないアルゴリズムを使用した製品を採用した場合、セキュリティが十分に検証されていない可能性があるほか、標準仕様に準拠した製品を新たに採用することになった際にアルゴリズムの違いなどによって追加的な作業（例えば、標準仕様に適合するようにシステムの構成を変更するなど）やコストが発生する可能性があると指摘している。

PQC のアルゴリズムへの移行を計画するに際して、本ホワイトペーパーは、以下の調査や検討を行うことを推奨している。

- IT システム／インフラにおいて暗号アルゴリズムを使用している部分や製品を特定する（クリプト・インベントリの構築）。
- 暗号アルゴリズムを使用している部分や製品などが複数存在する場合、それらの間の依存関係を明確にする。
- 暗号アルゴリズムを使用している部分や製品への対応（アルゴリズム移行を含む）に関して優先順位を決定する。例えば、個人に関するデータなどの高い機密性が要求されるデータを取り扱うシステム、有効期間が相対的に長い電子証明書を取り扱う PKI のシステムなどは、比較的早期にアルゴリズムの移行を実現することが求められる。

PQC のアルゴリズムの選定に関して、本ホワイトペーパーは、あらゆるアプリケーションに適用可能なアルゴリズムが提案されていないとしたうえで、本稿執筆時点では具体的なアルゴリズムを推奨していないものの、NIST による標準化の動向をフォローしつつ各アプリケーションに適したアルゴリズムを今後

ここでは読みやすさの観点から PQC に置き換えて記載する。

[23] セッション鍵の配送に関して、PQC のアルゴリズムを採用する代わりに、セッション鍵やそれを生成するためのマスター鍵を通信当事者間で事前に共有するという方法もある。これに関して、本ホワイトペーパーは、セッション鍵などの管理が煩雑となり、運営者やエンド・ユーザにとっての使い勝手がよいとはいえないことから望ましくないとの見方を示しているほか、通信相手が頻繁に変化するインターネット通信に適用することが実際上難しいといった問題があると指摘している。

特定・推奨していく方針を示している。

（６）CSE（カナダ）のガイダンス

カナダの CSE（Communications Security Establishment）[24]は、「Preparing Your Organization for the Quantum Threat to Cryptography」と題するガイダンスを 2021 年 2 月に公表している（Communications Security Establishment [2021]）。本ガイダンスは、IT システムにおいて中長期間使用する情報（any information with a medium or long lifespan）が CRQC によるリスクにさらされるおそれがあるとの見方を示したうえで、運営者に対して、CRQC に耐性をもつ暗号[25]への移行計画を検討するほか、標準化されたアルゴリズムが利用可能になったタイミングでそれを実装すべきであるとしている。

本ガイダンスは、CRQC によるリスクの管理や PQC への移行を、以下のステップで実施することを推奨している。

① 日々実施しているリスク・アセスメントの一貫として、組織内で使用する情報の重要性を評価するとともに、それらの機密性を保持する期間を決定し、CRQC によるリスクにさらされる可能性がある情報を特定する。
② IT システムのライフサイクル管理の見直しを行い、PQC のアルゴリズムへの移行計画の策定を速やかに開始する。
③ 重要なソフトウェアやハードウェアのアップデートに関して、その実施時期が近づいたところで予算やリソースを確保する。
④ CRQC によるリスクに対処するために必要な研修やトレーニングを（自分も含め）担当者に受講させる。
⑤ ベンダーに対して、PQC のアルゴリズムを実装するための計画に関して問い合わせる。例えば、将来のソフトウェア・アップデートに PQC のアルゴリズムの導入が含まれているか、または、PQC のアルゴリズムを使用可能にするためには新しいソフトウェアやハードウェアを購入する必要があるかといった質問が該当する。
⑥ ベンダーに対して、FIPS のように標準化された（PQC の）アルゴリズムを使用するように要請する。
⑦ IT システムのライフサイクル・プランにおいて、いつどのように PQC の

[24] CSE は、カナダにおけるサイバーセキュリティ対策を担当する政府機関（https://www.cse-cst.gc.ca/en/corporate-information/mandate）。

[25] 本ガイダンスは「量子コンピュータに耐性をもつ暗号」を「quantum-resistant cryptography」あるいは「quantum-safe cryptography」と記載しているが、ここでは読みやすさの観点からいずれも PQC に置き換えて記載する。

アルゴリズムを実装するかを決定する。

⑧ PQC のアルゴリズムを導入するために IT システムのアップデートやパッチ適用を実施する。その後のアップデートやパッチ適用を適切に実施する。

PQC のアルゴリズムの推奨に関して、本ガイダンスには特定のアルゴリズムが記述されていない。もっとも、PQC のアルゴリズムの評価を NIST と協力しつつ進めている旨が本ガイダンスに記載されているほか、CSE が NIST と共同で CMVP を運営していることから、NIST によって標準化されたアルゴリズムを今後推奨する可能性が高いとみられる。

（7）ASD（オーストラリア）のガイダンス

オーストラリアの ASD（Australian Signals Directorate）[26]は、「Planning for Post-Quantum Cryptography」と題するガイダンスの改訂版を 2023 年 5 月に発表している（Australian Signals Directorate [2023]）。本ガイダンスは、PQC のアルゴリズムの採用を、CRQC が実現したとしても安全な通信を維持するための実用的な手段と位置付けている。

採用すべき PQC のアルゴリズムに関して、本ガイダンスは、特定の PQC のアルゴリズムを推奨する旨を記述しておらず、NIST によって標準化されるアルゴリズムを参考にしながら PQC のアルゴリズムを評価・選定するとしており、最終的にはそれらを ASD の承認暗号アルゴリズム（ASD-Approved Cryptographic Algorithms）のリストに追加する予定である旨を示している。

また、公開鍵暗号を使用している IT システムを有する組織が PQC のアルゴリズムへの移行計画を立案するに際し、本ガイダンスは以下の事項を推奨している。

- 公開鍵暗号を使用する環境において、すべてのアプリケーションと情報通信機器に関する暗号アルゴリズムの使用状況を調査してクリプト・インベントリを整備する。
- 公開鍵暗号によって現時点で保護されているすべてのデータの価値を特定する。
- PQC のアルゴリズムへの移行計画を策定する。移行計画には、PQC のアルゴリズムのテストや導入、現行アルゴリズムの使用停止などに関する事項が含まれる。

[26] ASD は、オーストラリアにおけるサイバーセキュリティ対策を担当する政府機関（https://www.asd.gov.au/about）。

- ベンダーや PQC の研究者の協力を得ながら、PQC のアルゴリズムへの要件を検討する。
- PQC のアルゴリズムへの移行作業に関わる（組織内の）スタッフに対して必要なトレーニングを実施する。

また、本ガイダンスは、PQC のアルゴリズムに関する調査研究、テスト、実証実験の実施も推奨している。

４．金融分野での検討状況

本節では、CRQC が現行アルゴリズムのセキュリティに及ぼす影響に対処するための金融分野における取組みとして、FS-ISAC の活動を紹介する。FS-ISAC は、Post-Quantum Cryptography Working Group を設置して、CRQC が金融サービスのセキュリティに及ぼしうる影響や対処方法について検討し、その成果を技術報告書（technical paper）として公表している[27]。ここでは、技術報告書の内容を要約したサマリー・ペーパー「Preparing for a Post-Quantum World by Managing Cryptographic Risk」から、CRQC によるリスクと対応のスタンス、アルゴリズム移行準備のロードマップについて紹介する（Post-Quantum Cryptography Working Group [2023a]）。

（１）量子コンピュータによるリスクと対応のスタンス

本サマリー・ペーパーは、CRQC によるハーベスト攻撃などの可能性を踏まえたうえで、CRQC の完成時期の予測可能性によらず、そのリスクに対抗することができるように情報セキュリティ・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）としている。

また、本サマリー・ペーパーは、従来型コンピュータ（classical computer）の性能向上によるリスクにも留意する必要があるとの見方も示している。CRQC の開発に関する研究が進展すると、その成果が従来型コンピュータの設計やアルゴリズムの研究にも活用され、結果として、その性能が予想以上に向上する可能性もあるとしている。

これらを踏まえ、本サマリー・ペーパーは、CRQC と従来型コンピュータの両方に対してセキュリティを確保し、さらに、既存の IT システムとの相互運用性が高いセキュリティ・プロトコルを PQC のアルゴリズムを用いて開発すること

[27] 4 つの技術報告書（technical paper）が公表されている。タイトルは、それぞれ、Risk Model Technical Paper、Infrastructure Inventory Technical Paper、Current State (Crypto Agility) Technical Paper、Future State Technical Paper である（Post-Quantum Cryptography Working Group [2023b, c, d, e]）。

が重要であるとしている。

（２）アルゴリズム移行準備のロードマップ

本サマリー・ペーパーは、PQC のアルゴリズムへの移行プロセスのうち、次の 6 つのフェーズに関して考察している。すなわち、①現行アルゴリズムによって保護されているデータに関する調査（inventory existing encryption assets）、②想定されるリスクの網羅的な洗出し（assess risk）、③ベンダーにおける対応の調査（assess vendors）、④リスク評価フレームワークの作成（create a risk assessment framework）、⑤リスク・モデルの適用（apply a risk model）、⑥リスク低減策の適用（remediation）である。

各フェーズの内容を要約すると以下のとおりである。

イ．現行アルゴリズムによって保護されているデータに関する調査

暗号アルゴリズムの使用状況（knowledge of all uses of cryptography）のみでなく、暗号による保護の対象となるデータや情報資産の種類や属性を網羅的に調査し、収集した情報を適切に管理することが求められる。本調査で得られた情報は、金融機関が、CRQC による影響やリスクを特定したり、暗号アルゴリズムの変更を容易にする体制を整備したりする際に役立つ[28]。

各種の情報収集を行う際に以下の点に留意すべきである。

A) アプリケーションに関する留意点
- 金融機関が開発したアプリケーション（in-house application）とベンダーが開発したアプリケーション（vendor application）を分けたうえで、それぞれに関して暗号アルゴリズムの使用状況を把握する。
- 重要度が高いアプリケーション、および、高い可用性が求められるアプリケーションに関してクリプト・インベントリを整備する。
- 金融機関の内部のアプリケーションと外部のアプリケーションとを接続するシステムに関してクリプト・インベントリを整備する。

B) ベンダー管理に関する留意点
- PQC を実装するためのベンダーのロードマップに関する情報を得る。
- PQC を実装する製品をベンダーから調達するうえで必要な検討を実施する。

C) 業務データなどに関する留意点

[28] こうしたインベントリに関する対応の推奨事項については、Infrastructure Inventory Technical Paper に検討結果がまとめられている（Post-Quantum Cryptography Working Group [2023c]）。

- 各データを保護すべき期間を明確にする。
- 最も高い機密度や重要度が求められるデータセット（most sensitive and critical datasets）についてインベントリを整備する。
- 各データがハーベスト攻撃の対象となるか否かをそれぞれ確認する。

D) 規制に関する留意点
- 規制当局（regulators）からの問合せに対応できるように準備する。

E) データ使用・保管場所に関する留意点
- 情報収集に関する対応で求められるタイムラインがデータを使用・保管している地域によって異なる場合がある。

ロ．想定されるリスクの網羅的な洗出し

本フェーズでは、どのようなリスクが存在するかを網羅的に洗い出す。そのうえで、既存のリスク軽減策を考慮しつつ、個々のリスクが顕在化する可能性やインパクトを把握する。その結果、既存のリスク軽減策では十分対応することができないリスク（残余リスク）が明らかとなる。

ハ．ベンダーにおける対応の調査

金融機関は、PQC のアルゴリズムに関するベンダーへの要求事項の検討、既存のリスク評価プロセスの見直し、PQC のアルゴリズムの導入に関する法律上あるいは契約上の要求事項の見直しなどを行う。その際、金融機関は、PQC のアルゴリズム移行への対応状況をベンダーに問い合わせることも有用である[29]。

ニ．リスク評価フレームワークの作成

リスク評価フレームワークは上記ロで明らかにした残余リスクをより詳細に分析するためのツールである。フレームワークによる分析結果は、リスクへの対処の方法を検討するに活用することができる。金融機関は、そうしたリスク評価フレームワークを作成することが求められる。その際に参考になる代表的なフレームワークとして、Quantum Risk Assessment（QRA）と Crypto Agility Risk Assessment Framework（CARAF）が挙げられる。QRA は、端的にいえば、PQC のアルゴリズムへの移行が CRQC 実現のタイミングよりも後になる可能性が高いならば、保護対象のデータが漏洩するリスクが大きい（当該タイミングよりも前ならばリスクが小さい）との考え方に基づく[30]。CARAF は、アルゴリズム移

---

[29] ベンダーへの質問事項案が Risk Model Technical Paper（Post-Quantum Cryptography Working Group [2023b]）に記載されている。

[30] QRA は、①保護対象のデータを使用・保存する期間（X）、②現時点でのシステム運営計画に沿って暗号アルゴリズムの移行を実施する場合に移行完了までにかかる時間（Y）、③CRQC の

行にかかる時間が長い、あるいは、移行にかかるコストが大きいならば、保護対象のデータが漏洩するリスクが大きいとの考え方に基づく[31]。

ホ．リスク・モデルの適用

金融機関は、作成したリスク評価フレームワークを用いる、あるいは、独自にリスクのモデルを構築する[32]ことによって、残余リスクの定量的な評価を行う。例えば、各リスクに関して、一定の前提[33]を置いたうえで金銭的損害額（の期待値）を算出し、算出結果が特定の対策（例えば、現行アルゴリズムの入替え）の実施にかかるコストを上回る場合、当該対策を採用する根拠となる。

ヘ．リスク低減策の実施

金融機関は、PQC のアルゴリズムが搭載された製品を IT システムに導入する。その際、単に新しいアルゴリズムを実装するだけでなく、当該システムにおけるクリプト・アジリティを向上させるように新たな機能を追加するなどの方策を検討することが望ましい。今後も、暗号アルゴリズムや暗号プロトコルは、絶え間なく高度化していくと予想されるが、そうした変化に迅速に対応できるようにしておくことも重要である。

実現までに今後必要な時間（Z）を見積もり、「X + Y > Z」という関係が成立すると見込まれるアプリケーションを「リスクが大きいため、リスク軽減策が必要」と判断する。また、リスクが顕在化する時期（Z）などに関して一定の見通しを得るとともに、データの使用・保存期間（X）の見直しや移行完了までの時間（Y）の短縮化など、リスク軽減に必要な対応の手掛りを得ることもできる。QRA の詳細については、Mosca and Mulholland [2017]を参照されたい。

31 CARAF は、IT システムにおけるクリプト・アジリティの欠如を保護対象のデータに関するリスクとして捉えるフレームワークである。まず、保護対象のデータやアプリケーションごとに、新しい暗号アルゴリズムへの移行に必要な時間（T）とコスト（C）を見積もる（T と C は、それぞれ、値の多寡に応じて 4 段階の値〈1～4〉のいずれかを割り当てる）。「アルゴリズム移行が長期化するほど、あるいは、より多くのコストを必要とするほど、リスクは大きい」との考え方に基づき、リスクを「T×C」として算出する。すべての保護対象のデータやアプリケーションに関してリスクの算出を行うことによって、対応の優先順位、着手の時期、具体的な対応内容などを検討することが可能となる。CARAF の詳細については Ma *et al.* [2021]を参照されたい。

32 既存のフレームワークを選択するほかに、自社でリスク評価の方法を開発するというケースもある。本サマリー・ペーパーは、ウェルズ・ファーゴ（Wells Fargo & Company）がリスク評価の方法を独自に開発した事例を紹介している（Post-Quantum Cryptography Working Group [2023b]）。

33 例えば、CRQC が特定のタイミングで実現する確率、攻撃者が CRQC を使用する確率、攻撃者がデータの解読に成功する確率、当該データが悪用された場合に金融機関が被る損害額などが挙げられる。

５．考察

本節では、3、4 節の内容を踏まえて、CRQC によるリスクに対する各国のセキュリティ当局のスタンスを整理する。そのうえで、各文書において、PQC のアルゴリズムへの移行を検討するうえで重要な論点として挙げられているクリプト・インベントリの整備、ハイブリッド方式、クリプト・アジリティについてそれぞれ考察する。

（１）量子コンピュータによるリスクに対するスタンス

いずれの文書も、ハーベスト攻撃などによるリスクの存在を指摘したうえで、当該リスクの評価を実施することを推奨している。また、いくつかの先は対応の緊要性を強調するスタンスを示している。

例えば、ANSSI のポジション・ペーパーは、ハーベスト攻撃によるリスクを評価したうえで対応が必要と判断した場合には可能な限り早期に PQC へ移行すべきであるとしている。CSE のガイダンスも、CRQC によるリスクにさらされる可能性がある情報を特定し、PQC のアルゴリズムへの移行計画の策定を速やかに開始すべきとしている。

FS-ISAC のペーパーにおいては、リスクに対抗することができるよう情報セキュリティ・システムの準備を直ちに開始しなければならないとしている。リスクへの対処を準備するためには、クリプト・インベントリを整備したうえでリスク評価を実施することになる。したがって、これは ANSSI や CSE に近いスタンスであると考えられる。

（２）クリプト・インベントリ

NBV、NCSC、ASD のそれぞれの文書には、クリプト・インベントリの整備の必要性が示されている。そこで課題となるのは、クリプト・インベントリをどのように整備するかである。この点に関連して、以下では、クリプト・インベントリの対象と収録する情報の調査・収集方法を考察する。

イ．クリプト・インベントリの対象

まず、クリプト・インベントリで記録・管理する情報に関して、どの IT システムをインベントリの対象とするかを決める必要がある。ASD のガイドラインにあるように、CRQC による影響を受ける公開鍵暗号が使用されている環境において、すべてのアプリケーションと情報通信機器を調査する必要がある。さらに、自社の業務やサービスが、自社の IT システムだけでなく他社の IT システム（クラウドも含まれる）と連動して動作している場合には、他社の当該 IT シス

テムも調査対象となると考えられる。自社システムと連動するシステムを運営する他の企業やクラウド事業者などに協力を呼び掛けるなどの対応が求められる。

クリプト・インベントリの対象となるITシステム（やその一部）は、暗号アルゴリズムの移行などの対策を実施する対象となりうる。逆にいえば、クリプト・インベントリの対象とならなかったITシステムは対策実施の対象外となりうる。自社の業務やサービスに内在するリスクに適切に対処するためには、クリプト・インベントリの対象をもれなく設定する必要があり、クリプト・インベントリの対象の検討は慎重に行うべきであると考えられる。

ロ．クリプト・インベントリに収録する情報の調査・収集

クリプト・インベントリの対象となるITシステムを設定した後、実際に暗号アルゴリズムの使用状況に関する情報をどのように収集するかを決める必要がある。ITシステムを開発したシステム・インテグレータや個々のIT製品のベンダーに問い合わせたり、製品のカタログを参照したりする方法がまず挙げられる。

この方法によって、対象となっているITシステムの調査を網羅的に実施できるのであれば、クリプト・インベントリを整備する側としては手間も少なく望ましい。ただし、問合せやカタログの参照によってすべての情報を収集できない、あるいは、収集した情報に誤りがある（古い情報のみ参照可能であり最新の情報を入手できないなど）といったケースもありうる。クリプト・インベントリの情報を正確かつ網羅的に調査・収集することの重要性を踏まえたうえで、問合せやカタログ参照に加えて、別の手段で調査することも視野に入れておくべきであると考えられる。

現実的な方法として、例えば、コード解析用のツールを使用して暗号アルゴリズムの使用に関する情報を収集・分析するという方法が挙げられる（Post-Quantum Cryptography Working Group [2023c]）。もっとも、ツールによって収集することができる情報の種類が異なる可能性があり、必要な情報をすべて収集するためには複数のツールを組み合わせて使用することが必要となりうる。使用するツールの機能や収集可能な情報などを詳しく分析・特定するなどの対応を事前に実施しておくことが求められる。

（３）ハイブリッド方式

ハイブリッド方式に関する論点として、複数のアルゴリズムの組合せ方（ハイブリッド方式の具体的な構成）について考察する。

本稿では、ハイブリッド方式という用語を「現行アルゴリズムと PQC のアルゴリズムを組み合わせて実装するもの」として使用し、アルゴリズムの具体的な構成については言及しなかった。3 節で紹介した各文書も、ハイブリッド方式のアイデアを、「hybrid solution」、「hybrid mechanism」、「hybrid construction」などの異なる表現で説明しているほか、具体的な構成方法を記述していない。PQC のアルゴリズムへの移行の文脈でハイブリッド方式やそれに類する用語が頻繁に使用されるようになってきているが、用語の定義やハイブリッド方式の具体的な構成は自明ではなく、文書によって異なる内容を指している場合がある。このため、用語や概念を統一する試みが始まっている（Driscoll [2023]、Banerjee *et al.* [2023]）。

例えば、Driscoll [2023]は、複数の種類の暗号アルゴリズムを組み合わせて用いる暗号プロトコルに関連する用語を整理している。まず、「PQ/T Hybrid Protocol」と呼ばれる暗号プロトコルを、「同一の暗号機能を実現するアルゴリズムとして、伝統的なアルゴリズム（traditional algorithm）と PQC のアルゴリズムをそれぞれ少なくとも 1 つずつ用いる暗号プロトコル」と定義している。そのうえで、PQ/T Hybrid Protocol のバリエーションとして、「Composite PQ/T Hybrid Protocol」と「Non-composite PQ/T Hybrid Protocol」を紹介している [34]。

このように、ハイブリッド方式の構成についてはさまざまな形態が存在しうる。構成方法が異なると、達成されるセキュリティも変化する可能性がある。ハイブリッド方式を採用する際には、その形態にいくつかのバリエーションが存在しうるとともに、構成方法によってセキュリティやシステム改修の内容が左右される可能性がある点に留意する必要がある。

今後、ハイブリッド方式の構成のバリエーションやそれらのセキュリティに関する分析や評価が実施されると考えられる。こうした分析・評価結果についてもフォローしておくことが有用であろう。

---

34 Composite PQ/T Hybrid Protocol は、プロトコルのメッセージ・フローやデータ領域が、単一のアルゴリズムで実現する場合と同一となるプロトコルである。アルゴリズムの使用を単体から複数に変更する際に、プロトコルの仕様自体への影響をなるべく小さくすることに主眼を置いている。そのため、プロトコルの仕様に合致するように、暗号アルゴリズムのライブラリを改修することが必要となる。Non-composite PQ/T Hybrid Protocol は、使用するアルゴリズムにおける暗号要素（鍵、平文、暗号文など）のデータ・フォーマットが、単一のアルゴリズムで実現する場合と同一となるプロトコルであり、暗号アルゴリズムのライブラリの仕様への影響をなるべく小さくすることに主眼を置き、それに合致するようにプロトコルの仕様を改修することが求められる。

（4）クリプト・アジリティ

クリプト・アジリティに関して、その定義と対応時期について考察する。

イ．クリプト・アジリティの定義

クリプト・アジリティは、BSI、ANSSI、NBV のそれぞれの文書において、今後の暗号アルゴリズム移行を予定している IT システムに付与すべき重要な機能・特性として説明されている。もっとも、この用語は、ハイブリッド方式と同様に、統一的な定義が存在しておらず、各文書において特定の手法や技術仕様が示されているわけでもない。したがって、クリプト・アジリティによって何を達成するか、すなわち、クリプト・アジリティに関するシステム要件を明確にしておく必要がある。

まず、暗号アルゴリズムに関するどの処理を円滑に入れ替えるようにするかを決定することが求められる。一般に、暗号アルゴリズムは、暗号鍵やその他のパラメータの生成、暗号化、復号といった複数の処理から構成される。また、実際に暗号アルゴリズムを使用するためには、暗号鍵の保管・廃棄といった暗号鍵管理の処理が必要となるほか、公開鍵暗号の場合には、電子証明書の発行・保管・廃棄・失効情報管理といった処理も必要となる。これらのうち、どの処理に対してクリプト・アジリティを付与するのが適当かを検討しなければならない。

また、「円滑に入れ替える」とはシステム要件としてどのように記述するかについても検討することとなる。例えば、「入替えに要する時間やリソースを一定の範囲内とすること」をクリプト・アジリティのシステム要件の 1 つとすることが考えられるが、「一定の範囲」をどのように設定するかが課題となる。より短い時間の入替えが望ましいが、短時間での入替えを実現するためには相応のシステム対応やベンダーによるサポートが必要となる可能性がある。暗号アルゴリズム移行に充てられる費用やリソース、移行の緊要性などを考慮しつつ検討することが求められると考えられる。

ロ．クリプト・アジリティ対応の時期

クリプト・アジリティを IT システムに付与することを決定した場合、どのタイミングで IT システムに付与するかも重要な論点となる。

クリプト・アジリティに関する検討の流れとして想定されるのは以下のとおりである。

① クリプト・インベントリを整備する。
② リスク評価を実施する。
③ アルゴリズムの移行を実施する対象（IT システムやその部位）を特定する。

④ アルゴリズム移行の計画立案の検討項目の 1 つとして、クリプト・アジリティを付与すべき対象や具体的なシステム要件を設定する。
⑤ 上記④のシステム要件に合致したソリューションやサービスを調査・選定する。
⑥ クリプト・アジリティを付与するためのシステム改修を実施する。

クリプト・アジリティの付与を現行アルゴリズムの移行作業と同時に実施するケースでは、上記①～④は、2 節（1）で示した移行プロセスのフェーズ（状況把握、影響・リスク評価、対象特定、計画立案）にそれぞれ対応し、各フェーズの検討項目の一部として実施することが想定される。そのうえで、上記⑤と⑥を、実際のアルゴリズム移行（計画実行フェーズ）の前、あるいは、その一部として実施することとなる。

実施のタイミングについては、IT システムの既存の開発・改修計画と整合性をとる形で決定することが効率的であると考えられる。すなわち、既に予定されているシステム改修案件があれば、現行アルゴリズムの移行作業よりも前に、クリプト・アジリティを付与するための改修を当該改修案件に含める形で実施するというものである。また、複数の IT システムにおいて同様の対応を行うケースでは優先順位を決定する必要がある。IT システムの重要度、改修にかかる時間、他のシステムとの依存関係などを考慮して、どのシステムから改修を行うかを検討することになると考えられる。

６．おわりに

本稿では、海外のセキュリティ当局などが公表している文書を参照し、CRQC による暗号アルゴリズムのリスクへの対処方針や主な推奨事項を紹介したほか、アルゴリズム移行において主な論点となりうるクリプト・インベントリ、ハイブリッド方式、クリプト・アジリティについて考察し、検討時の留意点や課題を示した。

暗号アルゴリズムの移行を適切に実施するためには、クリプト・インベントリの整備、リスク評価、検討対象となる IT システムの特定、移行計画の立案・実施など、さまざまな課題を検討する必要がある。暗号アルゴリズム、とりわけ、公開鍵暗号は既にさまざまな IT システムで使用されていることから、インベントリの整備やリスク評価を、公開鍵暗号を使用している可能性のあるすべてのシステムに対して実施することになるかもしれない。また、対象となる IT システムのステークホルダーが複数存在する場合、ステークホルダー間でのスケジュール、作業分担、責任範囲、費用負担などの各種調整に相応の時間や費用が必

要になると想定される。このように考えると、海外のセキュリティ当局が推奨しているように、クリプト・インベントリの整備に向けた検討を早めに開始することが望ましいと考えられる。

まずは、既存のガイドラインや検討資料を参照し、具体的にどのような検討を行うことになるのかを確認する必要があろう。金融分野においても、FS-ISAC が既に検討を開始しており、成果物を公表している。これらを参照することが有用であろう。また、検討項目の洗出しやリスク評価の方法などの金融機関共通の課題に関して、金融機関間で連携して取り組み成果を共有することも業界全体のリソースの有効活用という観点から望ましい。今後、どのような体制で検討を進めるのが適切かも含めて、CRQC によるリスクへの対処に関する議論・検討をより深めていくことが肝要である。

以　上

【参考文献】

宇根正志・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 1 号、日本銀行金融研究所、2021 年、55～96 頁

四方順司、「量子コンピュータの脅威を考慮した高機能暗号：格子問題に基づく準同型暗号とその応用」、『金融研究』第 38 巻第 1 号、日本銀行金融研究所、2019 年、73～96 頁

田村裕子・宇根正志、「情報セキュリティ製品・システムの第三者評価・認証制度について：金融分野において利用していくために」、『金融研究』第 27 巻別冊第 1 号、日本銀行金融研究所、2008 年、79～114 頁

CRYPTREC 暗号技術調査ワーキンググループ（耐量子計算機暗号）、「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）」、CRYPTREC GL-2004-2022、CRYPTREC、2023 年 a（https://www.cryptrec.go.jp/report/cryptrec-gl-2004-2022.pdf、2023 年 8 月 31 日）

————、「CRYPTREC 耐量子計算機暗号の研究動向調査報告書」、CRYPTREC TR-2001-2022、CRYPTREC、2023 年 b（https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2022.pdf、2023 年 8 月 31 日）

Accredited Standards Committee X9, Inc., “Quantum Computing Risks to the Financial Services Industry,” ASC X9 IR-F01-2022, Accredited Standards Committee X9, Inc., 2022 (available at https://x9.org/download-qc-ir, 2023 年 8 月 31 日).

Agence Nationale de la Sécurité des Systèmes d’Information, “ANSSI views on the Post-Quantum Cryptography Transition,” Agence Nationale de la Sécurité des Systèmes d’Information, 2022 (available at https://www.ssi.gouv.fr/uploads/2022/01/anssi-technical_position_papers-post_quantum_cryptography_transition.pdf, 2023 年 8 月 31 日).

Alagic, Gorjan, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, and Daniel Smith-Tone, “Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process,” NIST IR 8413-upd1, National Institute of Standards and Technology, 2022 (available at https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf, 2023 年 8 月 31 日).

Australian Signals Directorate, “Planning for Post-Quantum Cryptography,” Australian Signal Directorate, 2023 (available at https://www.cyber.gov.au/sites/default/files/2023-05/PROTECT%20-%20Planning%20for%20Post-Quantum%20Cryptography%20%28May%202023%29.pdf, 2023 年 8 月 31 日).

Banerjee, Aritra, Tirumaleswar Reddy, Dimitrios Schoinianakis, and Timothy Hollebeek, “Post-Quantum Cryptography for Engineering,” draft-ar-pquip-pqc-engineers-00, Internet Engineer Task Force, 2023 (available at https://www.ietf.org/archive/id/draft-ar-pquip-pqc-engineers-01.html, 2023 年 8 月 31 日).

Bundesamt für Sicherheit in der Informationstechnik, “Migration to Post Quantum Cryptography, Recommendations for action by the BSI,” Bundesamt für Sicherheit in der Informationstechnik, 2021 (available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Migration_to_Post_Quantum_Cryptography.pdf, 2023 年 8 月 31 日).

Communications Security Establishment, “Addressing the Quantum Computing Threat to Cryptography,” ITSE.00.017, Communications Security Establishment, 2020 (available at https://www.cyber.gc.ca/sites/default/files/cyber/publications/ITSE.00.017.pdf, 2023 年 8 月 31 日).

————, “Preparing your organization for the Quantum Threat to Cryptography,”

ITSAP.00.017, Communications Security Establishment, 2021 (available at https://www.cyber.gc.ca/sites/default/files/cyber/publications/itsap00017-e.pdf, 2023 年 8 月 31 日).

Driscoll, Florence, “Terminology for Post-Quantum Traditional Hybrid Schemes,” draft-ietf-pquip-pqt-hybrid-terminology, Internet Engineering Task Force, 2023 (available at https://www.ietf.org/archive/id/draft-ietf-pquip-pqt-hybrid-terminology-00.html, 2023 年 8 月 31 日).

Ma, Chujiao, Luis Colon, Joe Dera, Bahman Rashidi, and Vaibhav Garg, “CARAF: Crypto Agility Risk Assessment Framework,” *Journal of Cybersecurity*, 7(1), Oxford University Press, 2021, pp. 1-11.

Mosca, Michele, and John Mulholland, “A Methodology for Quantum Risk Assessment,” Global Risk Institute, 2017 (available at https://uploads-ssl.webflow.com/63ef0996726f31b9968ba679/648c8e28cfee25748915738f_a-methodology-for-quantum-risk-assessment-pdf.pdf, 2023 年 8 月 31 日).

National Cyber Security Centre, “Preparing for Quantum-Safe Cryptography, An NCSC Whitepaper about Mitigating the Threat to Cryptography from Development in Quantum Computing,” National Cyber Security Centre, 2020 (available at https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography, 2023 年 8 月 31 日).

Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek, Centrum Wiskund & Informatica, and Algement Inlichtingen- en Veiligheidsdienst, “The PQC Migration Handbook, Guidelines for Migrating to Post-Quantum Cryptography,” 2023 (available at https://www.tno.nl/en/newsroom/2023/04-0/pqc-migration-handbook/, 2023 年 8 月 31 日).

Netherlands National Communications Security Agency, “Prepare for the threat of quantum computers,” General Intelligence and Security Service, 2021 (available at https://english.aivd.nl/binaries/aivd-en/documenten/publications/2022/01/18/prepare-for-the-threat-of-quantumcomputers/Prepare+for+the+threat+of+quantumcomputers.pdf, 2023 年 8 月 31 日).

Newhouse, William, Murugiah Souppaya,William Barker, and Chris Brown, “NIST Special Publication 1800-38A, Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography,” Preliminary Draft, National Cybersecurity Center of Excellence, National Institute of Standards and Technology, 2023 (available at https://www.nccoe.nist.gov/sites/default/files/2023-04/pqc-migration-nist-sp-1800-38a-preliminary-draft.pdf, 2023 年 8 月 31 日).

Post-Quantum Cryptography Working Group, “Preparing for a Post-Quantum World by Managing Cryptographic Risk,” FS-ISAC, 2023a (available at https://www.fsisac.com/hubfs/Knowledge/PQC/PreparingForAPostQuantumWorldByManagingCryptographicRisk.pdf?hsLang=en, 2023 月 8 年 31 日).

————, “Risk Model Technical Paper,” FS-ISAC, 2023b (available at https://www.fsisac.com/hubfs/Knowledge/PQC/RiskModel.pdf?hsLang=en, 2023 月 8 年 31 日).

————, “Infrastructure Inventory Technical Paper,” FS-ISAC, 2023c (available at https://www.fsisac.com/hubfs/Knowledge/PQC/InfrastructureInventory.pdf?hsLang=en, 2023 月 8 年 31 日).

————, “Current State (Crypto Agility) Technical Paper,” FS-ISAC, 2023d (available at https://www.fsisac.com/hubfs/Knowledge/PQC/CurrentState.pdf?hsLang=en, 2023 月 8 年 31 日).

————, “Future State Technical Paper,” FS-ISAC, 2023e (available at https://www.fsisac.com/hubfs/Knowledge/PQC/FutureState.pdf?hsLang=en, 2023 月 8 年 31 日).

Seito, Takenobu, “Cryptography and Financial Industry,” in B. Anderssen et al., eds. *The Role and Importance of Mathematics in Innovation*, Mathematics for Industry, Vol.25, Springer, Singapore, 2017, pp. 107-115.