政府機関等における耐量子計算機暗号（PQC）への移行について（中間とりまとめ）

令和７年 11 月

政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議

１．はじめに

量子計算機技術の進展に伴い、現在広く利用されている公開鍵暗号の安全性の低下・危殆化が予想されており、耐量子計算機暗号（PQC）への移行は急を要する課題である。そのため、令和７年６月 30 日に第１回「政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議」（以下「連絡会議」という。）を開催するとともに、その下に幹事会を設置し、具体的な検討を進めている。

今般、以下のとおり、政府機関等における耐量子計算機暗号（PQC）への移行の方向性を整理するため、第１回連絡会議における資料３の検討すべき論点について、中間とりまとめを行った。

本中間とりまとめを踏まえつつ、別紙の骨子を基に、引き続き、工程表（ロードマップ）の策定に向け、検討を進めていくこととする。

２．現状の整理（検討すべき論点１、２及び３）

（１）量子計算機の開発・普及状況及びそれに伴い安全性が低下・危殆化する暗号技術の特定とその時期について

ア　量子計算機の開発・普及状況

量子計算機の開発は、現在、NISQ（Noisy Intermediate-Scale Quantum）[1]段階から、FTQC（Fault-Tolerant Quantum Computer）[2]の実現に向けて、国内外の企業が競って技術開発を加速させている[3][4]。

一方で、現在、インターネット等の通信で使われている公開鍵暗号を現実的な時間で解くためには、FTQC の実現を前提とし、100 万物理量子ビット以上の量子計算機が必要とされている。こうした量子計算機の実現の時期については、諸説あるが、2039 年よりも前に RSA-2048[5]を解読できる量子計算機が実現する可能性は５%未満と推定する研究[6]等がある一方で、2024 年の時点で 15 年以内に実現する可能性が 39%から 62%程度であるとの分析[7]もあるなど、その開発時期を正確に予測することは困難であり、暗号技術に与える影響の将来予測を困難なものとしている。

---

[1] 小・中規模でノイズを含む量子計算機。

[2] ノイズ等の影響を低減し大規模・長時間の計算を可能とした量子計算機。

[3] https://www.meti.go.jp/shingikai/sankoshin/green_innovation/industrial_restructuring/pdf/034_09_00.pdf

[4] https://www.cas.go.jp/jp/seisaku/pqc/kanjikai/dai2/shiryou1.pdf

[5] 公開鍵暗号方式の一つで、暗号アルゴリズムを RSA、鍵の長さを 2048 ビットとしたもの。

[6] J. Sevilla and C. J. Riedel. Forecasting timelines of quantum computing. (2020). arXiv: 2009.05045.

[7] M. Mosca, M. Piani. 2024 Quantum Threat Timeline Report. https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/. 2024-12.

イ　安全性が低下・危殆化する暗号技術の特定とその時期

FTQC を実現した大規模な量子計算機が利用可能になった場合、Shor のアルゴリズムを量子計算機で実行することにより多項式時間で素因数分解問題や（楕円）離散対数問題が解けることが知られており、とりわけ CRYPTREC（Cryptography Research and Evaluation Committees）[8]の「電子政府における調達のために参照すべき暗号リスト（CRYPTREC 暗号リスト）」[9]（以下「CRYPTREC 暗号リスト」という。）の電子政府推奨暗号リストに掲載されている公開鍵暗号の暗号技術全てにとって理論的には大きな脅威になる。

しかしながら、現時点で実現されている量子計算機と実際の暗号解読に必要とされる量子計算機の性能に関しては、依然として大きな乖離がある。前述のとおり、公開鍵暗号を現実的な時間で解くための量子計算機について、その実現時期を正確に予測することは困難であることから、量子計算機によって公開鍵暗号の安全性が低下・危殆化する時期を現時点で予測することは困難である。ただし、革新的な技術の発展等により暗号解読が近い将来に実現する可能性は否定できない点に留意が必要である。

なお、共通鍵暗号やハッシュ関数については、公開鍵暗号のように量子計算機を用いた効率的なアルゴリズムは見つかっていないが、Grover のアルゴリズムや BHT のアルゴリズムにより、量子計算機を用いることで計算の一定の効率化が可能とされている。そのため、現在主に用いられている鍵長が 128 ビット相当の共通鍵暗号及びハッシュ関数については、よりセキュリティ強度の高い鍵長への変更検討が必要と考えられる。

（２）諸外国の動向の把握について

諸外国の中には、耐量子計算機暗号（PQC）への移行の時期に係る方針を既に公表しているところがあるが、米国、欧州連合（EU）、英国、カナダ等、その多くが 2035 年までを期限としたスケジュールに基づいて移行を進めている。例えば、米国では、暗号システムを耐量子計算機暗号(PQC)へ移行し、2035 年までに量子リスクを最大限解消する方針とともに、国家安全保障システムかどうかに応じた移行の進め方やタイムラインも示されている。また、欧州連合（EU）、英国、カナダのように、2035 年までを期限としつつ、優先度等に応じた段階的な移行の時期を示している国もある。

耐量子計算機暗号（PQC）の国際的な標準化動向については、米国の NIST（National Institute of Standards and Technology）が FIPS（Federal Information Processing Standards）として複数の暗号方式の標準化を進めており、今後、標準化済みの FIPS の暗号方式を多くの国が用いることが想定される。一方で、こうした標準化プロセス

[8] 電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。

[9] 電子政府推奨暗号リスト（安全性及び実装性能が確認された暗号技術で、市場における利用実績が十分であるか今後の普及が見込まれ、利用を推奨するもののリスト）、推奨候補暗号リスト（安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト）及び運用監視暗号リスト（実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったと確認されたが、互換性維持のために継続利用を容認する暗号技術のリスト）で構成されている。

から外れた暗号方式や独自の暗号方式の標準化を進めている国もある。

（３）耐量子計算機暗号（PQC）の安全性等の評価・確認とその時期について

CRYPTREC において、CRYPTREC 暗号リストの更新が可能となるよう、耐量子計算機暗号（PQC）の安全性評価・実装性能評価に関する活動を開始している。具体的には、2024 年８月に NIST 標準として公開された FIPS 203(ML-KEM)、FIPS 204(ML-DSA)、FIPS 205(SLH-DSA)を対象として、順次、安全性評価・実装性能評価を実施中である。

３．現状の整理を踏まえた移行期限、支援策等（検討すべき論点４及び５）

（１）耐量子計算機暗号（PQC）への移行期限及び安全性が低下・危殆化した暗号技術の利用に係る停止の時期について

ア　耐量子計算機暗号（PQC）への移行期限

量子計算機により公開鍵暗号の安全性が低下・危殆化する時期を現時点で予測することは困難である。一方で、諸外国の状況を見ると、耐量子計算機暗号（PQC）への移行の時期に係る方針を既に公表している国のうち、米国、欧州連合（EU）等、2035 年までを移行期限として耐量子計算機暗号（PQC）への移行を進めている例が多い。

こうした諸外国に比べて我が国における耐量子計算機暗号（PQC）への移行が遅れることとなれば、諸外国との間で、安定的なネットワークの構築やサイバーセキュリティの確保、更には、防衛や外交といった安全保障上重要な情報のやり取りに支障が出ることも想定される。サイバー空間は、国際的なネットワークであるところ、国際連携等を鑑みれば、我が国も 2035 年を目標として耐量子計算機暗号（PQC）への移行を進めていくことが考えられる。

また、暗号方式の提案から社会的な普及までは RSA 等で 20 年ほどの期間が必要とされたことから、耐量子計算機暗号（PQC）の場合でも相当の期間が必要と想定されるため、長期間の移行スケジュールを策定し、準備を行う必要がある。

その際、情報の重要性や暗号技術の利用状況等を把握した上で、どのように移行を進めるかを情報システムごとに十分に検討し、適切に判断することが重要と考えられる。例えば、特に機微な情報や保護期間が非常に長期となることが想定されている情報等を扱う場合等においては、HNDL（Harvest Now, Decrypt Later）攻撃[10]といった現に直面しているリスクがあることにも留意し、上記の目標を踏まえつつ、より早期に耐量子計算機暗号（PQC）への移行を行うことも含め、適切に検討を進めることが重要と考えられる。

イ　安全性が低下・危殆化した暗号技術の利用に係る停止の時期

政府機関等は、政府機関等のサイバーセキュリティ対策のための統一基準群において、電子政府推奨暗号リストに基づき、情報システムで使用する暗号等を定めることとされているところ、電子政府推奨暗号リストに掲載された暗号技術について

[10] 暗号化データを保存しておき、量子計算機での暗号解読が可能となった後に解読を行う攻撃。

は、安全性維持が困難と判断された場合、CRYPTREC において、運用監視暗号リストに当該暗号技術を移行することとなっている。また、互換性維持の継続利用として使うにしても安全性維持が極めて困難で、互換性維持の継続利用が容認できないと CRYPTREC が判断した場合等には、運用監視暗号リストから当該暗号技術を削除するといった運用が行われている。

上記の運用における暗号技術の利用に係る停止の時期については、量子計算機技術の進展状況を踏まえた暗号技術の安全性評価、政府機関等における耐量子計算機暗号（PQC）への移行等の状況、諸外国の状況等を十分に踏まえながら、CRYPTREC 暗号リストの取扱い等について、具体的方策の検討を進める。

（２）政府機関等の移行への対応に必要な支援策等について

政府機関等の耐量子計算機暗号（PQC）への移行に必要な支援策等については、対応製品の動向や政府機関等における暗号技術の利用状況等も踏まえ、今後作成する工程表（ロードマップ）に盛り込めるよう、引き続き、検討していくこととする。

４．政府機関等の移行に向けた工程表（ロードマップ）の策定について（検討すべき論点６）

（１）工程表（ロードマップ）の方向性

量子計算機技術については、その進展に伴い、現在広く使われている公開鍵暗号の安全性の低下・危殆化が懸念されている。このような中で、米国や欧州連合（EU）等の諸外国においては耐量子計算機暗号（PQC）への移行についての方針をそれぞれ公表しており、その多くが 2035 年までを期限として進めている。サイバー空間の安全性・信頼性は、情報の秘匿や改ざんの防止、認証等のために用いられる暗号技術の基盤の上で成立しており、国際連携等の観点を踏まえれば、我が国における移行が遅れた場合、サイバーセキュリティや安全保障上の支障も懸念される。

我が国のサイバーセキュリティの確保等のため、政府機関等における耐量子計算機暗号（PQC）への移行について、原則として、2035 年までに行うことを目指し、政府機関等における暗号技術の利用状況等も踏まえ、関係府省庁の連携の下、2026 年度に工程表（ロードマップ）を策定し、我が国における円滑な移行を推進していく。

（２）工程表（ロードマップ）に盛り込むべき事項等

上記（１）の方向性を踏まえ、別紙の骨子を基に、今後作成する工程表（ロードマップ）に盛り込むべき事項等を引き続き検討していくこととする。

なお、別紙の骨子については、必要に応じて見直しを行う。

５．その他（検討すべき論点７）

現在の電子政府推奨暗号リストに掲載されている公開鍵暗号の鍵長と耐量子計算機暗号（PQC）の鍵長とでは大きくサイズが異なること等もあり、移行に当たってアプリケーションやインタフェース、データフォーマット、プロトコル等に大幅な変更が必要となる可能性が高い。その場合、移行のための準備や開発コスト、実際の移行に必要な期間等が従来以上に大きく膨らむ可能性があることに留意する必要がある。移行において

は、CRYPTREC が公表しているガイドライン[11]等も参考に、情報システムによって、必要とする保護期間や移行作業量が異なることを踏まえ、その優先度等に応じて対応を行ったり、移行対象の詳細な把握のためにクリプト・インベントリ[12]を構築したりするなど、移行の必要性や方法等について検討を進める必要がある。

また、現在主流の暗号技術とは違い、耐量子計算機暗号（PQC）に特化した暗号解読手法や安全性評価の蓄積、実装脆弱性を回避するための耐量子計算機暗号（PQC）を実装する際のセキュリティ対策（例えば、サイドチャネル攻撃対策）の蓄積といったものが十分に進んでいるとはいえない状況である点にも留意する必要がある。

こうした状況も踏まえ、暗号部分を迅速に切り替えられる情報システムを構築すること（クリプト・アジリティ）のほか、利用環境によっては、耐量子計算機暗号（PQC）への完全な移行ではなく、耐量子計算機暗号（PQC）と現在主流の暗号技術との併用を採用することや、量子計算機でも解読されない技術として量子暗号通信（QKD）[13]の導入等を視野に入れることも考えられる。

加えて、耐量子計算機暗号（PQC）の実装を進めていくに当たっては、量子計算機技術による検証等も考えられ、こうした技術開発を進めることも重要である。

なお、本とりまとめは政府機関等の耐量子計算機暗号（PQC）への移行を念頭にしたものであるが、耐量子計算機暗号（PQC）への移行については、政府機関等に限るものではなく、重要インフラ事業者等や民間事業者等においても考慮しなければならない課題であるため、関係府省庁の連携の下、必要な対応について検討を進め、円滑な移行を後押ししていく。

---

[11] CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）2024 年度版（2025 年 3 月 CRYPTREC 暗号技術調査ワーキンググループ（耐量子計算機暗号））。

[12] 利用している暗号モジュールや暗号方式のリストのこと。

[13] 量子鍵配送（Quantum Key Distribution）。量子力学の原理（物理法則）に基づき、盗聴が不可能な方法により鍵共有が可能。

（別紙）

政府機関等の耐量子計算機暗号(PQC)への移行に向けた工程表(ロードマップ)(骨子)

１．対象組織

「政府機関等のサイバーセキュリティ対策のための統一規範」の適用対象となる組織とする。

２．対象システム

「政府機関等のサイバーセキュリティ対策のための統一基準」の適用対象となる情報システムとする。

３．移行すべき暗号技術※について

（１）安全性の低下・危殆化が懸念される暗号技術

量子計算機技術の進展に伴い、将来的に安全性の低下・危殆化が懸念される暗号技術として、移行対象とする暗号技術は主に「公開鍵暗号」とする。なお、「共通鍵暗号」や「ハッシュ関数」についてもセキュリティ強度の高い鍵長への変更検討を行うこととする。

（２）耐量子計算機暗号（PQC）の安全性確認

移行すべき耐量子計算機暗号（PQC）の安全性評価等が行われ、安全性及び実装性能が確認された耐量子計算機暗号（PQC）について、CRYPTREC 暗号リストに反映されるよう、その掲載方法も含め、CRYPTREC において必要な検討を行うこととする。

また、政府機関等については、政府機関等のサイバーセキュリティ対策のための統一基準群において、電子政府推奨暗号リストに基づき、情報システムで使用する暗号等を定めることが現状規定されているため、上記の状況も踏まえて必要な検討を行うこととする。

４．耐量子計算機暗号（PQC）への移行期限及び暗号技術の利用に係る停止の時期

（１）耐量子計算機暗号（PQC）への移行期限

原則として、2035 年を目処に、耐量子計算機暗号（PQC）へ移行を行うこととする。

ただし、情報の重要性や暗号技術の利用状況等を把握した上で、どのように移行を進めるかを検討し、適切に判断する必要がある。例えば、特に機微な情報や保護期間が非常に長期となることが想定されている情報等を扱う場合等においては、より早期に移行を行うことも含め、情報システムごとに適切に検討を行うこととする。

※ 政府機関等が使用する暗号技術の技術分類としては、公開鍵暗号、共通鍵暗号、ハッシュ関数等があり、具体的な暗号アルゴリズムは「電子政府における調達のために参照すべき暗号リスト（CRYPTREC 暗号リスト）」を参照のこと。

（２）暗号技術の利用に係る停止の時期

暗号技術の安全性が低下・危殆化した場合の利用に係る停止の時期は、今後の量子計算機技術の進展を踏まえた暗号技術の安全性評価、政府機関等における耐量子計算機暗号（PQC）への移行等の状況、諸外国の状況等を十分に踏まえながら、CRYPTREC 暗号リストの取扱い等について、具体的方策の検討を進めていくこととする。

５．移行に向けた取組

（１）移行に向けた計画に盛り込むべき事項

今後策定する工程表（ロードマップ）において、政府機関等が移行に向けた計画を策定できるよう、移行に向けた計画に盛り込むべき基本的事項や留意すべき事項を示すこととする。

（２）政府機関等の取組

各政府機関等は、今後策定する上記５（１）の工程表（ロードマップ）を踏まえ、移行に向けた計画を策定し、上記４の移行期限までに、耐量子計算機暗号（PQC）へ移行を行うこととする。

（参考）

第１回政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議（資料３）

検討すべき論点

１．量子計算機の開発・普及状況及びそれに伴い危殆化する公開鍵暗号等の特定とその時期について

２．諸外国の動向の把握について

３．耐量子計算機暗号（PQC）の安全性等の評価・確認とその時期について

４．耐量子計算機暗号（PQC）への移行期限及び危殆化した公開鍵暗号等の利用に係る停止の時期について

５．政府機関等の移行への対応に必要な支援策等について

６．政府機関等の移行に向けた工程表（ロードマップ）の策定について

７．その他