資料６

技術・脅威の動向等を踏まえた対策（関連取組）

令和８年５月15日
内閣官房国家サイバー統括室

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）の概要①

✓ 第２回 関係府省庁連絡会議（令和７年11月19日）において、政府機関等におけるPQCへの移行に係る**検討すべき論点について、中間とりまとめを実施**

中間とりまとめの主な項目

○ 現状の整理（検討すべき論点１、２及び３）

- 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
- 諸外国の動向の把握
- 耐量子計算機暗号（PQC）の安全性等の評価・確認とその時期

○ 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）

- 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
- 政府機関等の移行への対応に必要な支援策等

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

- 工程表（ロードマップ）の方向性
- 工程表（ロードマップ）に盛り込むべき事項等

○ その他（検討すべき論点７）

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）の概要②

✓ 中間とりまとめにおいては、政府機関等のPQCへの移行に向けた**工程表（ロードマップ）の骨子も策定**

工程表(ロードマップ)の骨子（概要）

移行対象	• **「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 • **移行対象とする暗号技術は主に「公開鍵暗号」**。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
移行期限等	• 原則として、**2035年を目処**に移行。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 • **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 • **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PQCへの移行等の状況、諸外国の状況等を十分に踏まえる**
移行に向けた取組	• 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 • **政府機関等は、今後策定する工程表（ロードマップ）を踏まえ、移行に向けた計画を策定し、移行期限までにPQCへ移行**を行う

III. 目的達成のための施策

３．我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

（３）先端技術に対する対応・取組

② 量子技術の進展に伴う対応・取組

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**[55]、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**。

その上で、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。

量子暗号通信（QKD）について、諸外国における社会実装に向けた取組が加速していることを踏まえ、我が国においても、サイバーセキュリティ確保、国際競争力の強化等のため、テストベッド（実証基盤）の広域化・高度化、ユースケースやビジネスモデルの創出・実証等、2030年頃のQKDの社会実装に向けた取組を加速する。

---

55 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。

（参考１）政府統一基準における暗号利用に関する記載

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 （令和７年度版）＜抜粋＞

7.1.5 暗号・電子署名

目的・趣旨

情報システムで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、暗号と電子署名は有効であり、情報システムにおける機能として適切に実装することが求められる。

暗号化機能及び電子署名機能を導入する際は、使用する暗号アルゴリズム及び鍵長に加え、それを用いた暗号プロトコルが適切であること、運用時に当該アルゴリズム又は鍵長が危殆化した場合や当該プロトコルに脆弱性が確認された場合等の対処方法及び関連する鍵情報の適切な管理等を併せて考慮することが必要となる。

遵守事項

(1)暗号化機能・電子署名機能の導入

(a) 情報システムセキュリティ責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の全ての措置を講ずること。

一 要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。

二 要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。

(b) 情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された**「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及び電子署名の**アルゴリズム及び鍵長**並びにそれらを利用した安全なプロトコルを定めること。また、その運用方法について実施手順を定めること。

(c) 情報システムセキュリティ責任者は、機関等における暗号化及び電子署名のアルゴリズム、鍵長及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な**公的な公開鍵基盤が存在する場合はそれを使用する**など、目的に応じた適切な公開鍵基盤を使用するように定めること。

政府機関等の対策基準策定のためのガイドライン （令和７年度版）＜抜粋＞

【 基本対策事項 】

＜7.1.5(1)(b)関連＞

7.1.5(1)-2 情報システムセキュリティ責任者は、職員等が暗号や電子署名を利用する場合、あるいは情報システムの新規構築や更新に伴い、暗号化又は電子署名を導入する場合において、情報システムで使用するアルゴリズム及び鍵長並びにそれらを利用した安全なプロトコルを、「電子政府推奨暗号リスト」に基づき定めること。

7.1.5(1)-3 情報システムセキュリティ責任者は、基本対策事項7.1.5(1)-2で定めた事項の運用方法について、以下を全て含めて実施手順として定めること。

a) 暗号化及び電子署名に使用する**アルゴリズム又は鍵長が危殆化**した場合又はそれらを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること。

b) 暗号化された情報の復号又は電子署名の付与に用いる鍵について、**管理手順を定めること**。

（解説）

遵守事項7.1.5(1)(b)「「電子政府推奨暗号リスト」に基づき」について

職員等が暗号や電子署名を利用する場合、あるいは情報システムの新規構築や更新に伴い、暗号化又は電子署名を導入する場合においては、「電子政府推奨暗号リスト」に記載されたアルゴリズム及び鍵長を定めることが原則である。

しかし、職員等が利用するソフトウェアや連携する他の情報システム側が「電子政府推奨暗号リスト」に記載されたアルゴリズム又は鍵長に対応していない等の場合は、利用実績が不十分であること、また、今後の普及が見込めない可能性があることによる影響を踏まえた上で、「推奨候補暗号リスト」に記載されたアルゴリズム及び鍵長を利用するとよい。

なお、「運用監視暗号リスト」に記載されたアルゴリズム及び鍵長は互換性維持以外の目的での利用をしてはならない。また、互換性維持の目的であったとしても、暗号が解読される等のリスクが考えられるため、「電子政府推奨暗号リスト」に記載されたアルゴリズム及び鍵長への移行を検討する必要がある。

（参考２）政府統一基準に係る法令等

サイバーセキュリティ基本法（平成26年法律第104号）＜抜粋＞

（国の行政機関等におけるサイバーセキュリティの確保）

第十三条　国は、国の行政機関、独立行政法人（独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する独立行政法人をいう。以下同じ。）及び特殊法人（法律により直接に設立された法人又　は特別の法律により特別の設立行為をもって設立された法人であって、総務省設置法（平成十一年法律第九十一号）第四条第一項第八号の規定の適用を受けるものをいう。以下同じ。）等におけるサイバーセキュリティに関し、国の行政機関、独立行政法人及び指定法人（特殊法人及び認可法人（特別の法律により設立され、かつ、その設立等に関し行政官庁の認可を要する法人をいう。第三十三条第一項において同じ。）のうち、当該法人におけるサイバーセキュリティが確保されない場合に生ずる国民生活又は経済活動への影響を勘案して、国が当該法人におけるサイバーセキュリティの確保のために講ずる施策の一層の充実を図る必要があるものとしてサイバーセキュリティ戦略本部が指定するものをいう。以下同じ。）におけるサイバーセキュリティに関する統一的な基準の策定、国の行政機関における情報システムの共同化、情報通信ネットワーク又は電磁的記録媒体を通じた国の行政機関、独立行政法人又は指定法人の情報システムに対する不正な活動の監視及び分析、国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する演習及び訓練並びに国内外の関係機関との連携及び連絡調整によるサイバーセキュリティに対する脅威への対応、国の行政機関、独立行政法人及び特殊法人等の間におけるサイバーセキュリティに関する情報の共有その他の必要な施策を講ずるものとする。

（設置）

第二十五条　サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、内閣に、サイバーセキュリティ戦略本部（以下「本部」という。）を置く。

（所掌事務等）

第二十六条　本部は、次に掲げる事務をつかさどる。

一　サイバーセキュリティ戦略の案の作成及び実施の推進に関すること。

二　国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること。

三　～　六　（略）

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（令和７年６月27日サイバーセキュリティ戦略本部決定）＜抜粋＞

（目的）

第一条　本規範は、サイバーセキュリティ基本法（平成二十六年法律第百四号。以下「法」という。）第二十六条第一項第二号に定める国の行政機関、独立行政法人及び指定法人（以下「機関等」という。）におけるサイバーセキュリティに関する対策の基準として、機関等がとるべき対策の統一的な枠組みを定め、機関等に自らの責任において対策を図らしめることにより、もって機関等全体のサイバーセキュリティ対策を含む情報セキュリティ対策の強化・拡充を図ることを目的とする。

（適用対象）

第二条　本規範の適用対象とする組織は、次の各号に掲げるとおりとする。

一　国の行政機関 法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項若しくは第二項に規定する機関、国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関又はこれらに置かれる機関

二　独立行政法人 独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する法人

三　指定法人 法第十三条に規定する指定法人

２　本規範の適用対象とする者は、国の行政機関において行政事務に従事している国家公務員、独立行政法人及び指定法人において当該法人の業務に従事している役職員その他機関等の指揮命令に服している者であって、次項に規定する情報を取り扱う者（以下「職員等」という。）とする。

３　本規範の適用対象とする情報は、職員等が職務上取り扱う情報であって、情報処理若しくは通信の用に供するシステム（以下「情報システム」という。）又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び情報システムに入力された書面に記載された情報を含む。）及び情報システムの設計又は運用管理に関する情報とする。

（統一基準への委任）

第二十三条 本規範に定めるもののほか、本規範の実施のため必要な要件は、統一基準で定める。

（参考３）重要インフラの安全基準等策定指針における暗号利用に関する記載

重要インフラのサイバーセキュリティに係る安全基準等策定指針＜抜粋＞

5.4.3. 暗号を活用した情報管理

・ 暗号の利用方針や暗号鍵の管理方針を策定する。

5.4.4. 通信のセキュリティ

・ 情報の機密性や完全性等を保護する観点から、専用線や暗号技術の活用、IPv6 に関するセキュリティ対策の実施、ネットワークの分離、ログ取得及び監視によるサイバー攻撃の検知等によってネットワークのセキュリティを確保する。

・ 重要な情報を通信手段により転送するにあたり、セキュリティ確保に係る取組方針や手順を整理し、転送相手と合意する。

重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書＜抜粋＞

11.4.4. 暗号化を活用した情報管理

11.4.4.1. 機微なデータの取り扱い

・ 個人情報及び認証情報を含む機微なデータは、暗号化して保存され、許可された管理者のみがアクセスできるようにする。

11.4.4.2. 暗号化通信及び電子署名

・ 転送中のデータを保護するために、適切な TLS 暗号化を導入する。

＊ 非推奨や、脆弱な暗号化が使用されている資産を特定し、強度な暗号に更新する計画を立てて実施する。

＊ 制御システムについては、遅延と可用性への影響を最小限にするため、通常はリモートや外部資産との通信について、可能であれば暗号化を行う。

＊ **暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照**する。なお、暗号技術に係る国内外の法令及び規制の存在について留意する。

＊ 完全性が求められる情報を取り扱う情報システムについては、STARTTLS 等の通信経路の暗号化機能や、DMARC 等の電子署名の付与及び検証を行う機能を設ける必要性の有無を検討する。