参考資料

（参考１）
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

（参考２）サイバーセキュリティ戦略（令和７年１２月２３日閣議決定）

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。