諸外国における耐量子計算機暗号（PQC）移行の状況

令和７年７月31日　国家サイバー統括室

諸外国における耐量子計算機暗号（PQC）移行の状況

＜米国＞

脆弱な暗号システムへのリスクを緩和しながら量子コンピューティングにおける米国のリーダーシップを促進する国家安全保障覚書（2022年5月4日）

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

○ 暗号システムを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及びタイムラインを提示。
○ 国家安全保障システムかどうかに応じた役割分担や移行の進め方も提示。

商用国家安全保障アルゴリズムスイート2.0の発表（2022年9月7日）

Announcing the Commercial National Security Algorithm Suite 2.0

○ 国家安全保障システムの量子耐性アルゴリズムへの移行が2035年までに完了される前提で、機器等の移行の想定タイムラインを提示。

PQCのための3つのFIPS承認の発表（2024年8月13日）

Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography

○ 標準化を進めていた3つの方式を連邦処理標準のFIPS203、204、205として決定。
(※)FIPS206等の別の方式についても引き続き標準化が進められている。

国家のサイバーセキュリティを強化するための特定の取組を継続し、大統領令14144号等を改正する大統領令（2025年6月6日）

Sustaining Select Efforts To Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144

○ 2025年12月1日までに、PQCをサポートする製品が広く入手可能な製品カテゴリーのリストを公表し、定期的に更新することを要請。

＜欧州（EU）＞

耐量子計算機暗号(PQC) 移行に向けた協調実施ロードマップに関する欧州委員会勧告（2024年4月11日）

COMMISSION RECOMMENDATION of 11.4.2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

○ 本勧告の公表後2年以内にPQC移行に向けたロードマップの公表を要請。
○ 加盟国は、当該ロードマップを踏まえて移行計画を策定。

耐量子計算機暗号(PQC)移行に向けた協調実施ロードマップ（2025年6月11日）

A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography Part 1, Version: 1.1（EU PQC Workstream）

○ 2026年12月末まで
・すべての加盟国は、初期のPQC移行計画を策定。
・高・中リスクのケースのPQC移行について検討に着手。
○ 2030年12月末まで
・高リスクのケースについて、PQC移行を完了。
・中リスクのケースについて、PQC移行計画の策定を完了。
○ 2035年12月末まで
・中リスクのケースについて、PQC移行を完了。
・低リスクのシステムについては、可能な限りPQC移行を完了。

(※)PQC移行の完了に関して、該当時期以降、量子脆弱性をもつ公開鍵暗号を単独で使用してはならない旨が記載されている。

諸外国における耐量子計算機暗号（PQC）移行の状況

＜英国＞

耐量子計算機暗号(PQC)への移行のタイムライン(2025年3月20日)

Timelines for migration to post-quantum cryptography

○ 2028年まで
- 移行のゴールを定義。
- 調査の実施（資産を評価し、どのサービスとインフラをPQCにアップグレードする必要があるかの把握）。
- 移行に関する初期計画を策定。

○ 2031年まで
- 最重要の資産を保護するために、最優先の移行活動を完了。
- 2035年までの移行完了に向けた移行計画の見直し。

○ 2035年まで
- すべてのシステム、サービス、製品について、PQCへの移行を完了。

＜カナダ＞

耐量子計算機暗号(PQC)移行に向けたロードマップ（2025年6月23日）

Roadmap for the migration to post-quantum cryptography for the Government of Canada (ITSM.40.001)

○ 2026年4月まで
- (非機密情報を取り扱うITシステムについて)PQCへの移行計画の策定。

○ 2026年4月から
- PQC移行の進捗状況を毎年報告。

○ 2031年まで
- 優先度の高いシステムについて、PQCへの移行を完了。

○ 2035年まで
- 残りのシステムについて、PQCへの移行を完了。

＜韓国＞

耐量子計算機暗号(PQC)移行マスタープラン(2023年7月12日)

汎국가 양자내성암호 전환 마스터플랜

○ PQC移行に向けた目標及び2035年までのロードマップ提示。

＜豪州＞

情報セキュリティマニュアル(2025年7月現在(随時更新))

Information Security Manual

○ 2030年以降、SHA-256、RSA、ECDSA、ECDH等の使用を許容しない方針。

（参考）諸外国における耐量子計算機暗号（PQC）移行の状況（出典）

＜米国＞

米ホワイトハウスウェブサイト

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2022/05/04/executive-order-on-enhancing-the-national-quantum-initiative-advisory-committee/

Sustaining Select Efforts To Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144

https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/

NISTウェブサイト

Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography

https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved

DODウェブサイト

Announcing the Commercial National Security Algorithm Suite 2.0

https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

＜欧州（EU）＞

欧州委員会ウェブサイト

COMMISSION RECOMMENDATION of 11.4.2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

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

A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography Part 1, Version: 1.1

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

＜英国＞

NCSCウェブサイト

Timelines for migration to post-quantum cryptography

https://www.ncsc.gov.uk/guidance/pqc-migration-timelines#section_3

＜カナダ＞

カナダ政府ウェブサイト

Roadmap for the migration to post-quantum cryptography for the Government of Canada (ITSM.40.001)

https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001

＜韓国＞

NCSCウェブサイト

양자 大전환 시대 대비, 관계부처 합동 마스터플랜 발표

https://www.ncsc.go.kr/cop/bbs/selectBoardArticle.do?bbsId=Notification_main&nttId=59449

＜豪州＞

ASDウェブサイト

Information Security Manual

https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism

※URLは令和７年７月31日現在のもの