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幹事会（第５回）議事要旨

１　日時

令和８年３月 30 日(月)10:30～11:30

２　場所

中央合同庁舎第８号館共用Ｃ会議室

３　出席者

○議　長

西山　英将　　内閣官房内閣審議官（内閣官房副長官補付）

○副議長

髙橋　文武　　内閣官房内閣参事官（国家安全保障局）

杉本　貴之　　内閣官房内閣参事官（国家サイバー統括室）

○主　査

北井上　礼樹　デジタル庁統括官（デジタル社会共通機能担当）付参事官補佐（代理出席）

梅城　崇師　　総務省サイバーセキュリティ統括官付企画官

武尾　伸隆　　経済産業省商務情報政策局サイバーセキュリティ課長

○構成員

石谷　寧希　　内閣官房内閣参事官（内閣官房副長官補付）

佐藤　彰洋　　内閣府科学技術・イノベーション推進事務局政策企画調査官

森田　正敏　　警察庁長官官房技術企画課長

増原　剛輝　　デジタル庁統括官（戦略・組織担当）付参事官

森田　光枝　　外務省大臣官房情報システム総括課長

田渕　敬一　　文部科学省研究振興局基礎・基盤研究課量子研究推進室長

黒田　隆之助　経済産業省イノベーション・環境局イノベーション政策課調整官（代理出席）

石丸　光宏　　防衛省整備計画局サイバー整備課 AI・サイバーセキュリティ政策調整官（代理出席）

○説明者

小川　一人　　国立研究開発法人情報通信研究機構サイバーセキュリティ研究所セキュリティ基盤研究室室長

青野　良範　　国立研究開発法人情報通信研究機構サイバーセキュリティ研究所セキュリティ基盤研究室主任研究員

４　議事要旨

○冒頭挨拶

西山議長から、連絡会議における中間とりまとめ等を踏まえ、2026 年度中の工程表（ロードマップ）の策定に向け、議論を行う旨挨拶がなされた。

○議事

（１）今後のスケジュールについて

杉本内閣官房内閣参事官から、資料１について、今後のスケジュールの説明があった。

（２）CRYPTREC 暗号リストの改定について

梅城総務省サイバーセキュリティ統括官付企画官から、資料２及び３に基づき、PQC に対応した CRYPTREC 暗号リストの改定内容について説明があった。

次に、意見交換が行われ、以下のような発言があった。

○高橋内閣官房内閣参事官

・今回の改定により、PQC を政府機関等のシステムに導入する際の制度上の支障が解消された理解で良いか。また、改定後の CRYPTREC 暗号リストの「耐量子計算機暗号（PQC）リスト」に掲載された ML-KEM については、安全性や実装性能が一定程度確認できたものになるのか。

○梅城総務省サイバーセキュリティ統括官付企画官

・「耐量子計算機暗号（PQC）リスト」を含めた CRYPTREC 暗号リストは、「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」から参照されているため、当該リストに掲載されている PQC を採用できる状況になっていると理解している。

・ML-KEM の安全性・実装性能については、外部評価により実施しており、その評価結果を CRYPTREC においても承認している。

○杉本内閣官房内閣参事官

・ML-KEM のほか、ML-DSA や SLH-DSA の安全性・実装性能の評価も進められているものと認識している。PQC に対応した製品等の開発が進められる状況になってきていると理解している。

（３）PQC の実装・活用状況調査について

国立研究開発法人情報通信研究機構から、資料４に基づき、PQC の実装・活用状況調査について説明があった。

次に、意見交換が行われ、以下のような発言があった。

○高橋内閣官房内閣参事官

・説明のあったブラウザや OS 等が実装している PQC は米国 NIST 標準に準拠しているのか。

○国立研究開発法人情報通信研究機構
・具体的な実装方法が公表されていないものも多いが、米国 NIST の標準化に関わっていた事業者もおり、米国 NIST 標準に準拠しているのではないか。
○武尾経済産業省商務情報政策局サイバーセキュリティ課長
・クライアントサイドに比べてサーバサイドの PQC 対応が進んでいない状況とのことであるが、その理由は分かるのか。
○国立研究開発法人情報通信研究機構
・企業によるところではあるが、サーバ側で必要なアップデートがなされていない可能性が考えられる。また、企業や組織のネットワークにおいて、規格化されていない等の理由で、アルゴリズムを遮断している場合も考えられる。
○杉本内閣官房内閣参事官
・説明のあったハイブリッド構成はどのように実装されているものか。
○国立研究開発法人情報通信研究機構
・TLS1.3 では、現行暗号と PQC のハイブリッド構成で暗号化が可能であり、具体的な暗号化の方法として、それぞれごとに鍵(の元となる値)の共有を行う。その後、現行暗号から得た情報と、PQC から得た情報の両者を用いて、特殊な関数によって最終的な共通鍵を生成している。
・したがって、最終的な鍵に現行暗号と PQC の両方式の情報が反映される設計となっており、仮に将来、現行暗号が量子計算機で解読可能となった場合でも、PQC 側が安全であれば、HNDL 攻撃への耐性は確保される。

（4）工程表（ロードマップ）に盛り込むべき事項について
工程表（ロードマップ）に盛り込むべき事項について意見交換が行われた。

（5）その他
杉本内閣官房内閣参事官から、デジタル庁と協力し、政府機関等に対して実施した暗号移行に係る調査内容について報告された。

○今後の予定
・今後は、必要に応じて幹事会を複数回開催し、工程表（ロードマップ）の具体的な検討を進めていくこととされた。