PQCの安全性等の評価について

総務省
サイバーセキュリティ統括官室

CRYPTRECにおけるPQC安全性評価への対応

➢ CRYPTRECの暗号技術検討会（2025年3月）において、**CRYPTREC暗号リストの更新**が可能となるよう、NIST標準として公開された**FIPS 203** (ML-KEM)、**FIPS 204**(ML-DSA)、**FIPS 205**(SLH-DSA)などについて、**安全性評価・実装性能評価に関する活動を開始**することとした。

暗号技術検討会（2025年3月）資料 **<原案のとおり承認>**

✓ 2020年度に「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」でCRYPTREC暗号リストへのPQC掲載を見据えて検討したが、「PQCは、多数の方式が提案され安全性を検討している段階で、利用実績等に言及できる段階ではない」ことから、CRYPTREC暗号リストに組み込まず、別途ガイドラインを作成することとした。

✓ 上記の検討から約４年が経過。**政策的な観点（各国取組との調和性、国内における議論の高まりなど）を踏まえ**れば、上記の方針を見直すべき時期にあるのではないか。

✓ 今後、**安全性等が確認されたPQCを推奨候補リストに順次掲載できるよう準備**を始めてはどうか。

➢ 米欧をはじめ、複数の国においてPQCへの移行に関する方針や推奨アルゴリズムに関する情報が発出されている。我が国政府におけるPQC移行の旗振り・総合調整役は定まっておらず、移行方針もないが、CRYPTRECリスト掲載に向けたPQCの技術的検討は、移行方針の検討と両輪で進めるべきもの。サイバー空間における経済安全保障の観点からも、PQCのリスト掲載を遅滞なく行うことがCRYPTRECに求められている。

➢ 機動的なスケジュールを前提とすれば、まずは諸外国において**多くの専門家による検証を経て決定された方式（例えばFIPS 203(ML-KEM)、FIPS 204(ML-DSA)、FIPS 205(SLH-DSA)など）の安全性評価・実装性能評価を先行**し、その後、国産PQCを含めた他のアルゴリズムの取扱を順次検討し、追加の評価を実施してはどうか。なお、CRYPTRECとしてPQCの公募を行うことも考えられるが、人的・予算的リソースを勘案すると直ちに実施することは困難であるため、今後、公募のメリット・デメリットを精査しつつ引き続き検討する。

・FIPS 203(ML-KEM)	(改称前 CRYSTALS-Kyber)	格子暗号ベース	暗号化・鍵交換用途
・FIPS 204(ML-DSA)	(改称前 CRYSTALS-Dilithium)	署名格子暗号ベース	署名用途
・FIPS 205(SLH-DSA)	(改称前 SPHINCS+)	ハッシュ関数ベース	署名用途
・FIPS 206(FN-DSA)[ドラフト]	(改称前 FALCON)	格子暗号ベース	署名用途

※FIPS(Federal Information Processing Standards)：米国連邦政府が採用する情報処理に関する公式な標準規格で、NISTが策定。