協-03

基礎研究 | 応用研究 | 技術実証 | 社会実装

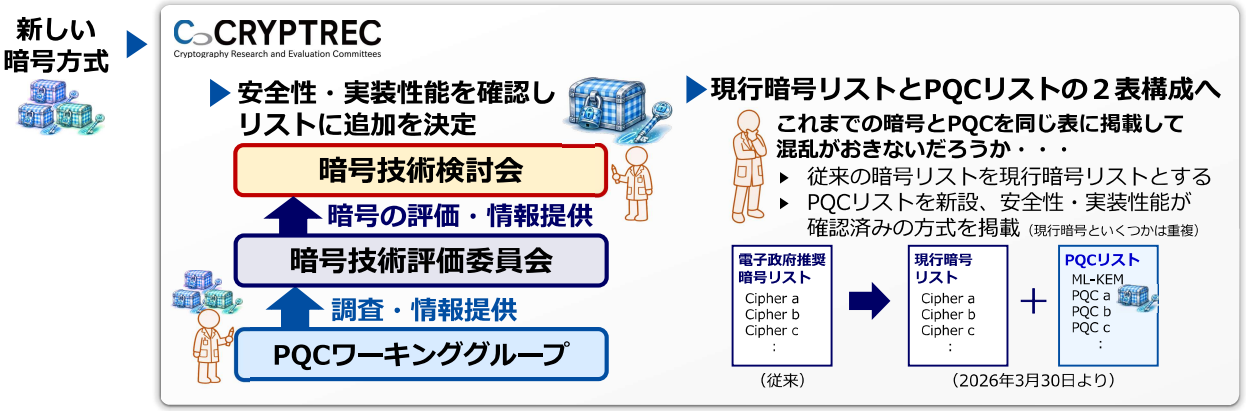
CRYPTREC（クリプトレック）電子政府推奨暗号リストの更新

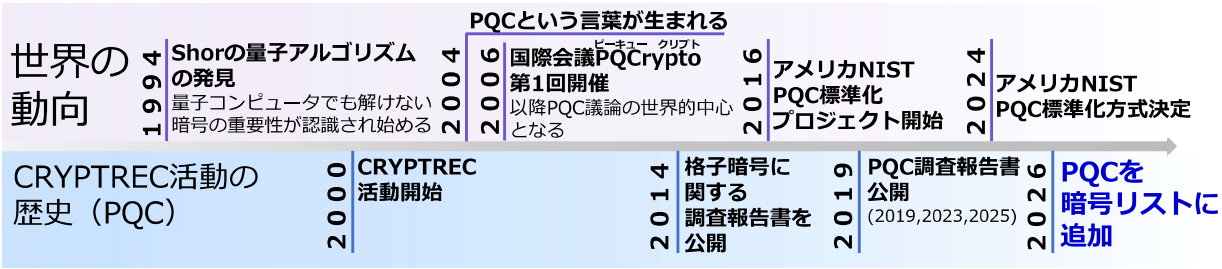
～量子コンピュータ時代に備えた耐量子計算機暗号（PQC）の追加～

概要

量子コンピュータの高性能化時代に備え、CRYPTREC電子政府推奨暗号リストに量子コンピュータでも解読が困難と期待される「耐量子計算機暗号（PQC）」が2026年追加されました。

CRYPTREC暗号リストに新たなPQCの暗号方式を追加





CRYPTRECの取り組み

- 電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）を管理
- 暗号をリストに追加するため安全性・実装性能を評価
- NICTは事務局として、暗号技術評価委員会やPQCワーキンググループを運営

量子コンピュータの高性能化

- RSA暗号方式など一部の暗号は量子コンピュータにより高速に解読される
- 安全な暗号方式への移行が必要

耐量子計算機暗号の追加

- 量子コンピュータでも解読が困難と期待される公開鍵暗号方式「ML-KEM（エムエルケム）」が2026年CRYPTREC暗号リストに追加された
- 他の方式も追加に向けて活動中

【お問合せ先】
サイバーセキュリティ研究所 セキュリティ基盤研究室
Mail：security@ml.nict.go.jp

NICTオープンハウス2026