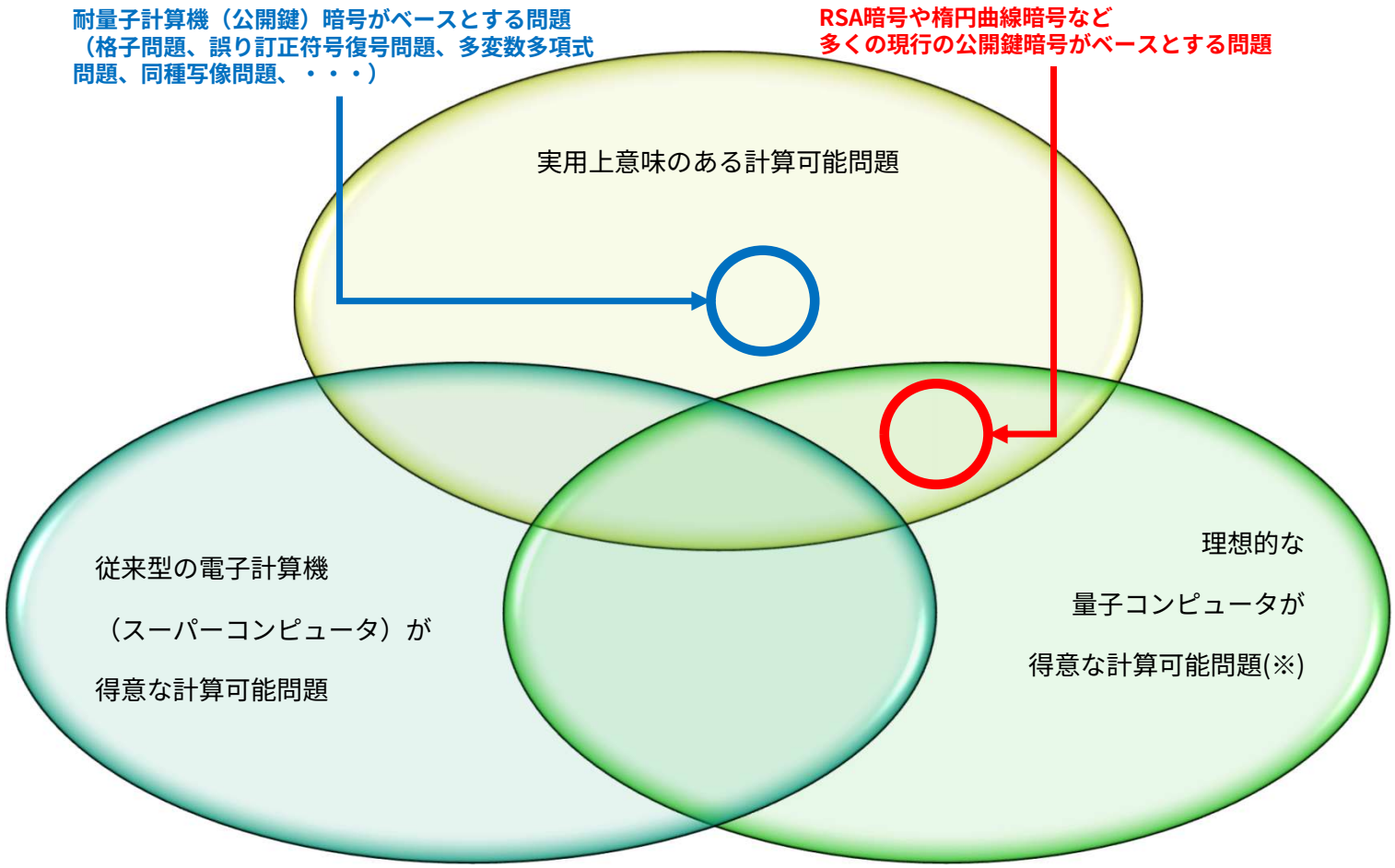
資料３

耐量子計算機暗号（PQC）について

松本　勉
国立研究開発法人産業技術総合研究所／横浜国立大学

2025年7月23日
第33回保険医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議

耐量子計算機暗号（PQC）の直感的説明（©2025 松本 勉）



※ 指数関数的に巨大なユニタリ行列（ベクトルの長さを不変に保つ行列）の乗算として表せる問題

量子計算機（量子コンピュータ）

- 量子力学の現象を利用して並列計算を実現し従来型の電子計算機（スーパーコンピュータ）では効率的に解けなかった問題の一部を効率よく解けると期待される次世代の計算機。
- まだ理想的な量子計算機は開発されていない。
- 量子計算機技術の進展に伴い、従来型の計算機に対してセキュリティを有している一部の暗号技術について、将来、そのセキュリティの低下（危殆化）が懸念されている。
- 量子計算機に耐性を持つ耐量子計算機暗号（PQC）への移行に向けて検討が進められているところ。

耐量子計算機暗号（PQC）

- 量子計算機および従来型の電子計算機の双方に対してセキュリティが確保される暗号技術。
- 量子計算機であっても計算を効率よく行うことが困難な数学的問題を利用することで、量子計算機による攻撃に耐性を持たせることを狙って開発・実装が進められている。

耐量子計算機暗号（PQC）に関するCRYPTRECの最近の活動

1. **耐量子計算機暗号ガイドライン（2024年度版）** https://www.cryptrec.go.jp/report/cryptrec-gl-2007-2024.pdf
   - 量子コンピュータの実用化により一部の公開鍵暗号方式の安全性が低下することを踏まえ、耐量子計算機暗号に関する調査結果をまとめた文書。
2. **量子コンピュータが共通鍵暗号の安全性に及ぼす影響（2024年度版）** https://www.cryptrec.go.jp/exreport/cryptrec-ex-3401-2024.pdf
   - CRYPTREC電子政府推奨暗号リスト掲載の共通鍵暗号技術とNIST標準軽量暗号Asconの安全性に量子計算機が及ぼす影響は、汎用量子アルゴリズム（特に、Groverのアルゴリズムと BHTのアルゴリズム※）のみを考慮すれば十分であるという結論を得た。※ Groverのアルゴリズムを応用し n ビットハッシュ関数の衝突探索を時間 $O(2^{n/3})$ で探索するアルゴリズム。
3. **暗号技術検討会（2025年3月25日）** https://www.cryptrec.go.jp/report/cryptrec-rp-1000-2024.pdf
   - 耐量子計算機暗号（PQC）への対応について議論し、CRYPTREC暗号リストへの掲載に向けたPQCの技術的検討と、PQCへの移行方針の検討を両輪として並行に進めていくことを合意した。また、FIPS-203 (ML-KEM)、FIPS-204 (ML-DSA)、FIPS-205 (SLH-DSA) の安全性・実装性能の評価を先行して実施することを合意した。
4. **暗号技術評価委員会のPQCに関する活動（2025年度）**
   - 米国NIST（国立標準技術研究所）をはじめとする世界各国の機関において耐量子計算機暗号の選定・標準化活動が継続されており、情勢が流動的であることを踏まえ2024年度までの暗号技術調査ワーキンググループ（耐量子計算機暗号）を継続して設置して、耐量子計算機暗号に関する最新動向を把握するとともに、社会的動向を踏まえ、NIST標準として公開されたFIPS-203, 204, 205について安全性評価・実装性能評価関連の活動を開始している。
5. **暗号技術活用委員会のPQCに関する活動（2025年度）**
   - 耐量子計算機暗号をめぐる社会的動向を踏まえ、耐量子計算機暗号の取扱い基準や位置づけ・記載内容等についての検討を開始した。具体的には各国政府・公的機関等が公表している「PQCへの移行（方針）」の政策やガイドラインについて政策的側面からの整理、及び「CRYPTREC暗号リスト」上のPQCの位置づけやリスト間での移行ルールの検討を行い、委員会としての見解を取りまとめる活動を開始している。
6. **CRYPTRECシンポジウム2025（2025年7月25日 (金) 13:00～16:40）** https://conferenceservice.jp/registration/cryptrec2025/
   - KABUTO ONE 4F ホール＆カンファレンス（東京都中央区日本橋兜町）およびオンラインのハイブリッド開催

https://www.cryptrec.go.jp/index.html

- **CRYPTREC**とは Cryptography Research and Evaluation Committees の略であり、電子政府推奨暗号等の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討すること等を通じ、セキュアなIT社会の実現を目指すプロジェクトを指す。
- デジタル庁、総務省及び経済産業省が共同で運営する**暗号技術検討会**と、その下で国立研究開発法人情報通信研究機構(NICT)及び独立行政法人情報処理推進機構(IPA)が共同で運営する**暗号技術評価委員会**及び、**暗号技術活用委員会**とから構成される。

耐量子計算機暗号（PQC）への移行に関する最近の政府の動向

- サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項
  2025年 (令和７年) ５月29日 サイバーセキュリティ戦略本部
  - 量子技術については、その進展に伴い、現在広く使われている公開鍵暗号の危殆化が懸念されているところ。そのため、諸外国や暗号技術検討会（CRYPTREC）における検討状況を踏まえ、多岐にわたる課題に対応するための関係省庁による検討体制を立ち上げ、政府機関等における耐量子計算機暗号（PQC）への移行の方向性について、次期サイバーセキュリティ戦略に盛り込む。
- 政府機関等におけるPQC利用に関し、関係府省庁の緊密な連携のもと必要な施策を検討・推進するため、内閣官房とりまとめのもと「耐量子計算機暗号(PQC)利用に関する関係府省庁連絡会議」が、2025年(令和7年)６月30日に設置された。（⇒　参考資料１参照）
  - 年内に工程表（ロードマップ）の骨子（移行の方向性）をとりまとめ、 サイバーセキュリティ戦略の改定に反映される予定。

＜参加者＞

議長	内閣官房副長官補（内政担当）
副議長	内閣官房内閣審議官（国家安全保障局） 内閣官房内閣審議官（国家サイバー統括室）
主査	デジタル庁統括官（デジタル社会共通機能担当） 総務省サイバーセキュリティ統括官 経済産業省商務情報政策局長
構成員	内閣官房内閣審議官（内閣官房副長官補付） 内閣府科学技術・イノベーション推進事務局統括官 警察庁長官官房技術総括審議官 デジタル庁統括官（戦略・組織担当） 外務省大臣官房サイバーセキュリティ・情報化参事官 文部科学省研究振興局長 経済産業省イノベーション・環境局長 防衛省大臣安房サイバーセキュリティ・情報化審議官

※会議は非公開（議事要旨及び配付資料は原則公開）

＜スケジュール＞

令和７年６月30日	令和７年７～11月	令和７年11月頃	令和８年度中
第１回関係府省庁連絡会議 〇検討開始	○課長級会合による検討	第２回関係府省庁連絡会議 ○工程表(ロードマップ)の骨子	第３回関係府省庁連絡会議 ○工程表(ロードマップ)の策定

＜検討すべき論点＞

1. 量子計算機の開発・普及状況、危殆化する公開鍵暗号等の特定とその時期
2. 諸外国の動向の把握
3. PQCの安全性等の評価・確認とその時期
4. PQCへの移行期限及び危殆化した公開鍵暗号等の利用に係る停止の時期
5. 政府機関等の移行への対応に必要な支援策等
6. 政府機関等の移行に向けた工程表（ロードマップ）の策定
7. その他