JANOG57.5 Interim Meeting, Tokyo, Japan

CRYPTRECがPQCリストを追加してきた

IIJ
Internet Initiative Japan

須賀祐治

2026-06-19

Ongoing Innovation

Disclaimer

- **The views expressed in this talk are those of the author and do not necessarily reflect**

まずは参考情報

- 暗号技術検討会2025年度報告書
  CRYPTREC RP-1000-2025
  - https://www.cryptrec.go.jp/report/cryptrec-rp-1000-2025.pdf
- 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 LS-0001-2022R2
  - https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022r2.pdf
- CRYPTRECとは
  - https://www.cryptrec.go.jp/about.html
- CRYPTREC暗号リスト
  - https://www.cryptrec.go.jp/list.html
- 暗号技術ガイドライン一覧
  - https://www.cryptrec.go.jp/tech_guidelines.html

CRYPTRECとは何か

- 日本の暗号技術評価プロジェクト
  - Cryptography Research and Evaluation Committees
  - [暗号技術検討会報告書，2.2節，p.4]
- 電子政府推奨暗号等の安全性を評価・監視
- 暗号技術の普及促進も目的
- 2003年に電子政府推奨暗号リストを策定
  - [暗号技術検討会報告書，2.1節，p.4]

CRYPTRECとしてのPQCの解説

- PQC（Post-Quantum Cryptography）
  - 日本語では耐量子計算機暗号
  - ※「耐量子暗号」は誤用（委員長との対話において確認）
  - 量子計算機に耐性を持つ暗号技術
- PQCリスト：CRQCへの耐性を有することが確認された暗号技術のリスト
  - CRQC(Cryptographically Relevant Quantum Computer)
    ＝ 現行暗号を解読可能な水準の量子計算機のこと

CRYPTRECの体制

- 事務局はデジタル庁，総務省，経産省
  - 暗号技術検討会が全体を統括
  - 暗号技術評価委員会が安全性・実装性能を評価
  - 暗号技術活用委員会が利用・運用面を検討
- 2026年度はPQCリスト検討TFを設置予定

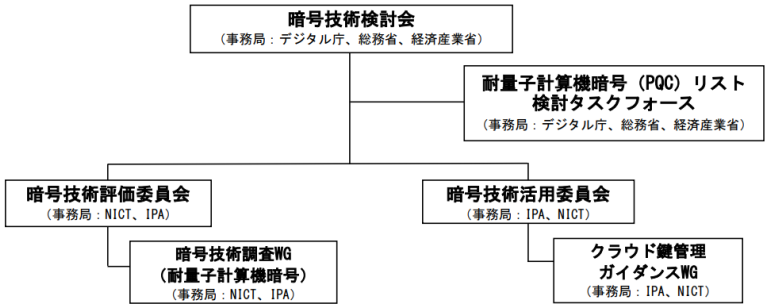

図4-1 CRYPTREC体制図（2026年度）（予定）

個人的に熱いと思っている組織変更

- 2026年度はPQCリスト検討TFを設置予定

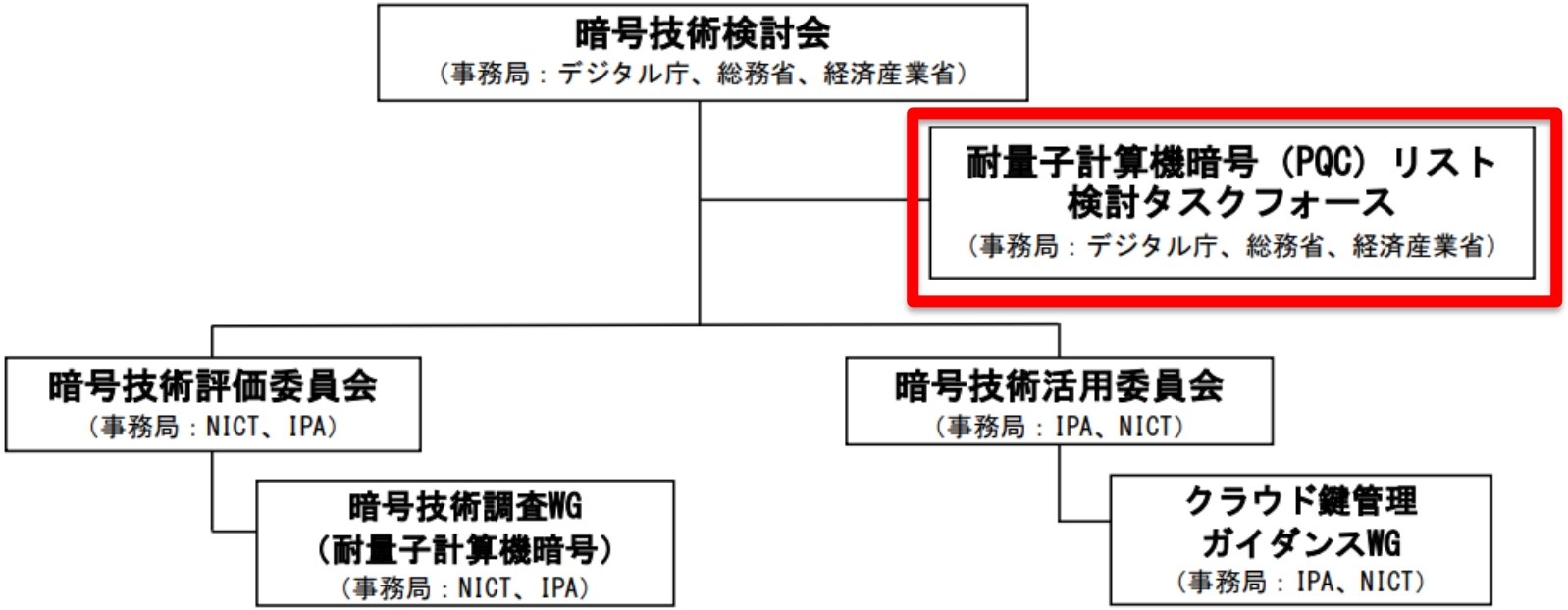

図4-1 CRYPTREC体制図（2026年度）（予定）

CRYPTREC暗号リストの更新

- CRYPTREC暗号リストを2026年3月30日に更新
  - 文書番号はCRYPTREC LS-0001-2022R2
- 表2「耐量子計算機暗号（PQC）リスト」を新設
  - 従来の表を表1「現行暗号リスト」と整理

PQCリスト新設の意図

- 「電子政府推奨暗号リスト」という文言の定着
- 既存関連文書への影響の抑制
- 従来の3リスト構成を長期的に維持しやすい整理
- CRQC耐性を持つ暗号技術の明示
- 利用者が選択可能な暗号を判断しやすくする意図
  - [暗号技術検討会報告書，2.4.2節，p.7]

PQCリスト

- 鍵共有：ML-KEM（ML-KEM-768, -1024）
- 署名は現時点では掲載なし
- 共通鍵暗号・ハッシュ関数も記載
  - AES-192，AES-256
  - SHA-384，SHA-512，SHA3-384，SHA3-512
- 192ビットセキュリティ以上のものだけをチョイス(NIST Categoryも見て欲しい)

2026年度の評価対象

- PQCリスト検討TFを設置予定
  - CRYPTREC暗号リストのPQC対応課題を整理
  - [暗号技術検討会報告書，4章，p.27]
- ML-DSA（FIPS204）
  SLH-DSA（FIPS205）
  　の安全性・実装性能を今後評価予定
  - FIPS203だけ前倒しで評価しただけなのでご安心を
  - 必要に応じ年度途中のリスト改定も検討

TLS暗号設定ガイドラインの今後

- スケジュール感：2027年度見直し
  - 2026年度に見直し検討を実施予定
  - [暗号技術検討会報告書，4章，p.27]
- PQCサポートに向けたTLS 1.3への移行が論点
  - これもやらなあかんこと：
    電子証明書の有効期限短縮化等への対応
    暗号強度要件設定基準も見直し予定

Key Takeaways

- CRYPTRECは暗号アルゴリズム選定の公的参照点
- 2026年3月改定でPQCリストを新設
  - ML-KEMが鍵共有として掲載
  - 署名方式は現時点では未掲載だけど評価対象になってる
- TLS暗号設定ガイドラインも見直し検討へ

Appendix：今後の検討課題となりうるもの

- Category 1・2相当暗号の扱い
- Camellia，KCipher-2, SHAKE-256は現在掲載保留
- 現行暗号とPQCを組み合わせたハイブリッド構成の扱い
- FIPS 204／FIPS 205後の評価順序
  - [暗号技術検討会報告書，2.4.3節，p.8]

Appendix：ハイブリッド構成の扱いをどうするか

- ハイブリッド構成をPQCリストに含めると複雑化
  - TLS暗号設定ガイドライン等で扱う案
- 上記は報告書中の意見であり決定事項ではない
  - [暗号技術検討会報告書，3.2.2節，p.24]
- 一方，TLSガイドライン見直し検討は予定として明記してて，私もちゃんとやります
  - [暗号技術検討会報告書，4章，p.27]

Ongoing Innovation

IIJ Internet Initiative Japan

Stay safe and healthy