

耐量子計算機暗号（PQC）リスト検討タスクフォース

- **CRYPTREC暗号リストの耐量子計算機暗号(PQC)対応**については、詳細検討が必要な課題を保留した上で、**2026年3月にリスト改定の第一弾を実施**。（改定概要：p2参照／検討が必要な課題：p3参照）
- 残された課題の検討のため、CRYPTRECに「**耐量子計算機暗号（PQC）リスト検討タスクフォース**」を設置し、2026年7月から検討を開始し、5回の会合を開催し、CRYPTREC暗号リストのPQC対応について議論※。
- 同タスクフォースの議論を踏まえた**CRYPTREC暗号リストの改定イメージ**に関して、今般、**意見募集**を実施。
意見募集は、①**ML-DSA・SLH-DSAに関する意見**※、②**その他の意見**に分けて求めている。

※会議資料等は https://www.cryptrec.go.jp/board_wg_materials.html に掲載

※ML-DSA及びSLH-DSAのCategory 1・2について、利用状況や将来的な利用見込み等も踏まえたCRYPTREC暗号リストにおける取扱い（掲載に関する考え方及びその理由）

検討課題

課題① Category 1・2の暗号等の取扱い

課題② 暗号利用モードや認証暗号等の取扱い

課題③ ハイブリッド構成の取扱い

課題④ PQCの安全性評価等の進め方

議論を踏まえ
別添2を作成し
意見募集対象
(別添3は参考資料)

意見募集の対象外

構成員

岩田 哲

名古屋大学 未来材料・システム研究所 教授

漆畠 賢二

GMOグローバルサイン株式会社 CTO室 フェロー

垣内 由梨香

日本マイクロソフト株式会社 カスタマープロテクション リスクマネージャー

國廣 昇

筑波大学 システム情報系 教授

須賀 祐治

株式会社インターネットイニシアティブ ネットワークサービス事業本部
セキュリティ本部 セキュリティ情報統括室 シニアエンジニア

高木 剛

東京大学 大学院情報理工学系研究科 数理情報学専攻 教授

細山田 光倫

NTT社会情報研究所 情報保護技術研究プロジェクト 暗号基礎グループ

松本 勉

国立研究開発法人産業技術総合研究所 フェロー

(主査)

横浜国立大学 上席特別教授

※事務局は、デジタル庁、総務省及び経済産業省がNICT及びIPAの協力を得て実施。

タスクフォースの開催履歴

第1回（2026年7月24日）

- ✓ タスクフォースの設置について
- ✓ CRYPTREC暗号リストのPQC対応と検討課題について
- ✓ 課題①・②・④について

第2回（2026年8月31日）

- ✓ Security LevelとSecurity Categoryの使い分けについて
- ✓ 課題①～③について

第3回（2026年9月16日）

- ✓ NTRUについて
- ✓ 課題①～④について

第4回（2026年10月5日）

- ✓ 課題①～④について

第5回（2026年10月23日）

- ✓ 課題①～④について
- ✓ CRYPTREC暗号リストの意見公募について

(参考) CRYPTREC暗号リストの2026年3月改定の概要

2

- CRYPTREC暗号リストの耐量子計算機暗号(PQC)対応のため、「電子政府推奨暗号リスト」に「表2 耐量子計算機暗号(PQC)リスト」を新たに追加する改定を2026年3月に実施。
- CRYPTRECにおいて更なる検討が必要な課題については保留した上で継続検討。

最新のCRYPTREC暗号リストは
<https://www.cryptrec.go.jp/list.html>

CRYPTREC暗号リストのリスト構成

- CRYPTREC暗号リストの「電子政府推奨暗号リスト」において、**従来記載されている表**を「表1 現行暗号リスト」とし、**新たに「表2 耐量子計算機暗号(PQC)リスト」**を作成。
 - ✓ 政府関連文書では「電子政府推奨暗号リスト」という文言が既に浸透していることから、3リスト構成は維持。
 - ✓ PQCへの移行完了後も、3リスト構成自体は変更の必要がなく、長期的な観点からも理解しやすい。

<リスト構成のイメージ>

- ① 電子政府推奨暗号リスト
 - 表1 現行暗号リスト
 - 表2 耐量子計算機暗号(PQC)リスト
- ② 推奨候補暗号リスト
- ③ 運用監視暗号リスト

「耐量子計算機暗号(PQC)リスト」の対象範囲

- 公開鍵暗号技術だけでなく、従来の**共通鍵暗号技術等についても量子計算機耐性が確認されたものは「表2 耐量子計算機暗号(PQC)リスト」に掲載**。
 - ✓ PQCへの移行に際して、暗号技術がCRQC※への**耐性**を有するか否かの判別が一般にわかりにくく、CRYPTREC暗号リストの利用者に対して選択可能な暗号リストを明確に示す必要がある。

※Cryptographically Relevant Quantum Computer。現行暗号の解読に利用可能な水準の量子計算機。

<対象範囲のイメージ>

技術分類		暗号技術
公開鍵暗号	署名	ML-DSA
		SLH-DSA
	鍵共有	ML-KEM
共通鍵暗号		AES
ハッシュ関数		SHA-2
		SHA-3
(略)		(略)

パラメーターセット等の取扱い

- 暗号強度等を変えるために複数用意されている**パラメーターセット**についてもリストに**掲載**。
- 各パラメーターセットに対応する**セキュリティのカテゴリ**もリストに**掲載**。
 - ✓ パラメーターセット及びカテゴリともに、システム調達時に暗号技術を選択する上で**重要な選択肢**。

※例えばML-KEMでは、右記の記載イメージのように3種が定義（括弧内はそれぞれに対応するセキュリティのカテゴリ）。

<パラメーターセットのイメージ>

名称	パラメーターセット (セキュリティカテゴリ)
ML-KEM	ML-KEM-512 (Category 1)
	ML-KEM-768 (Category 3)
	ML-KEM-1024 (Category 5)

2026年3月改定における取扱い

- 公開鍵暗号技術はML-KEMのみ掲載。※ML-DSA及びSLH-DSAは安全性・実装性能評価が終了次第掲載予定（2026年度想定）
- 暗号利用モード等や一部の共通鍵暗号とハッシュ関数についても継続検討中であり掲載していない。
- Category 1・2の暗号技術については継続検討中であり掲載していない。

(参考) CRYPTREC暗号リストのPQC対応に関する検討課題

3

- 2025年度の暗号技術検討会において、CRYPTREC暗号リストの耐量子計算機暗号（PQC）対応に関する検討を行い、更なる検討が必要な課題について保留※した上でCRYPTREC暗号リストの改定を実施。
※現時点で、表2（耐量子計算機暗号（PQC）リスト）には、Category 1・2の暗号技術や、暗号利用モードや認証暗号等の暗号技術は掲載していない。
- これらの課題については、安全性評価の観点のほか、利活用・普及促進の観点も含めた横断的な検討が必要。
- 暗号技術評価委員会及び暗号技術活用委員会の協力も得ながら、暗号技術検討会の直下に、新たに「耐量子計算機暗号（PQC）リスト検討タスクフォース」を設け、検討を進めている。

課題① Category 1・2（128ビットセキュリティ程度相当）の暗号等の取扱い

- ✓ 暗号強度要件※では、128ビットセキュリティは2040年までは「利用可」だが、2041年以降は「移行完遂期間」とされ、2051年以降は順次「利用不可」となる。
※暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準（CRYPTREC LS-0003-2022R1）
- ✓ 政府システムのPQC移行は原則2035年が期限とされており、この時期を念頭においた際、128ビットセキュリティの暗号技術を「推奨」することとしてよいか検討が必要。
- ✓ 海外機関では、Category 3以上を想定する記載が多く見られるが、Category 1・2を排除するような記載はなく、相互運用性・国際調達の観点からも検討が必要。
- ✓ このほか、カテゴリに関する記載等について改めて精査を行う。

＜参考：関係する暗号技術の例＞

名称	パラメーターセット (セキュリティカテゴリ)
ML-KEM	ML-KEM-512 (Category 1) ML-KEM-768 (Category 3) ML-KEM-1024 (Category 5)
AES	AES-128 (Category 1) AES-192 (Category 3) AES-256 (Category 5)
SHA2	SHA-256 (Category 2) SHA-512/256 (Category 2) SHA-384 (Category 4) SHA-512

課題② 暗号利用モードや認証暗号等の取扱い

- ✓ 現行暗号のCRQC（Cryptographically Relevant Quantum Computer）への耐性に関して、AES、SHA2、SHA3については、CRYPTRECの外部評価報告書※等から明らかな。 ※量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価 2024年度版（CRYPTREC-EX-3401-2024）
- ✓ 暗号利用モード、メッセージ認証コード、認証暗号、エンティティ認証や一部の共通鍵暗号とハッシュ関数※については検討が必要。
※Camellia、KCipher-2、SHAKE-256等

課題③ ハイブリッド構成の取扱い

- ✓ 現行暗号とPQCを組み合わせたハイブリッド構成について、CRYPTRECとしてどのように取り扱うか検討が必要。

課題④ 公開鍵暗号方式のPQCの安全性評価等の進め方

- ✓ 今後策定予定のFIPS標準等を始めとするPQCについて、どのような順序で安全性評価等を実施すべきか検討が必要。
※FIPS 204、205は2026年度中に安全性評価等が終了予定。