CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会活動報告

2026年7月31日

暗号技術検討会 座長
産業技術総合研究所 フェロー
横浜国立大学 上席特別教授
松本 勉

目次

1. CRYPTRECの概要

CRYPTREC
Cryptography Research and Evaluation Committees

A) CRYPTRECとは

CRYPTography **R**esearch and **E**valuation **C**ommittees

CRYPTRECの概要

- デジタル庁・総務省・経済産業省・NICT・IPAが共同で開催する暗号技術評価プロジェクト
- 当プロジェクトは、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て、セキュアなIT社会の実現を目指すもの
- **暗号技術検討会**並びに暗号技術検討会の下に設置される**暗号技術評価委員会**及び**暗号技術活用委員会**により運営

CRYPTREC
Cryptography Research and Evaluation Committees

B) CRYPTREC活動体制(2026年度)

暗号技術検討会 (事務局:デジタル庁、総務省、経済産業省)

① CRYPTREC暗号のセキュリティ及び信頼性確保のための調査・検討
② CRYPTREC暗号リストの改定に関する調査・検討
③ 関係機関と連携した暗号技術の普及による情報セキュリティ対策の推進検討・提言

耐量子計算機暗号(PQC)リスト検討タスクフォース
(2026年7月～)

暗号技術評価委員会 (事務局:NICT、IPA)

① 暗号技術の安全性及び実装に係る監視及び評価
② 新世代暗号に係る調査
③ 暗号技術の安全な利用方法に関する調査

暗号技術調査WG(耐量子計算機暗号)
(2021年7月～)

暗号技術活用委員会 (事務局:IPA、NICT)

① 暗号の普及促進・セキュリティ産業の競争力強化に係る検討
② 暗号技術の利用状況に係る調査及び必要な対策の検討
③ 暗号政策の中長期的視点からの取組の検討

クラウド鍵管理ガイダンスWG
(2025年4月～)

CRYPTREC
Cryptography Research and Evaluation Committees

C）暗号技術検討会構成員（2026年度）

座長	松本 勉	国立研究開発法人産業技術総合研究所 フェロー　横浜国立大学 上席特別教授
構成員	阿部 正幸	日本電信電話株式会社 フェロー
	石井 義則	一般社団法人情報通信ネットワーク産業協会 常務理事
	上原 哲太郎	立命館大学 教授
	國廣 昇	筑波大学 教授
	黒田 真弓	一般社団法人テレコムサービス協会 技術・サービス委員会 副委員長
	島岡 政基	セコム株式会社 IS研究所 主幹研究員
	高木 剛	東京大学 教授
	田村 裕子	日本銀行 金融研究所 企画役
	本間 尚文	東北大学 教授
	松井 充	国立研究開発法人情報通信研究機構　主席研究員
	松浦 幹太	東京大学 教授
	松本 泰	特定非営利活動法人日本ネットワークセキュリティ協会 フェロー
	吉田 博隆	国立研究開発法人産業技術総合研究所 研究グループ長
	渡邊 創	国立研究開発法人産業技術総合研究所 研究部門長

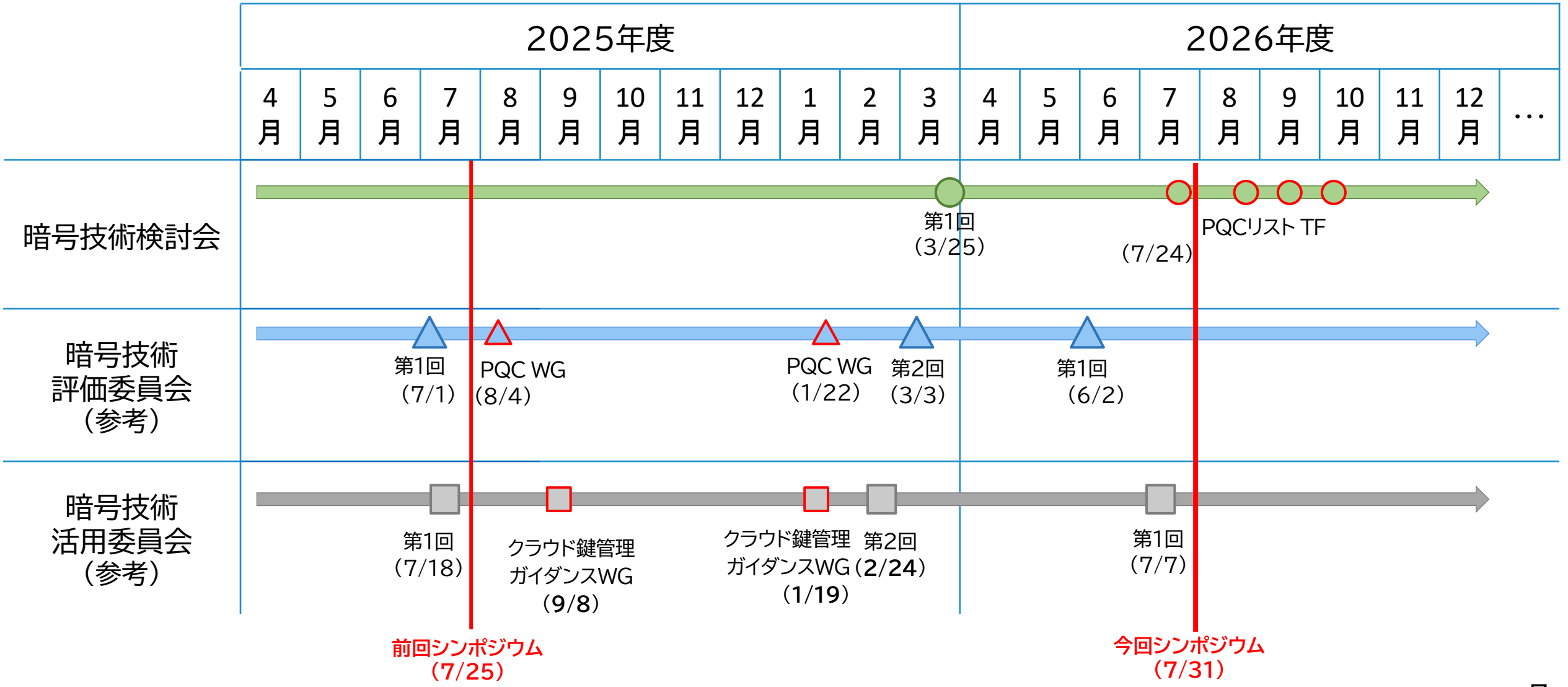
（五十音順、敬称略、所属は2026年6月時点のもの）

オブザーバ：国家サイバー統括室、警察庁、個人情報保護委員会、総務省、法務省、外務省、財務省、厚生労働省、経済産業省、防衛省、NICT、AIST、IPA、JIPDEC、FISC

事務局：デジタル庁、総務省、経済産業省

CRYPTREC
Cryptography Research and Evaluation Committees

D）暗号技術検討会等の開催の状況と予定



2. 暗号技術検討会の活動概要

CRYPTREC
Cryptography Research and Evaluation Committees

A）CRYPTREC暗号リストの概要

- CRYPTRECの活動を通して**安全性・実装性能等が確認された暗号技術**について、デジタル庁、総務省及び経済産業省において**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）**を策定。
- CRYPTREC暗号リストは以下の**3リスト**により構成される。（注：現在の3リスト構成は2013年より）

①電子政府推奨暗号リスト

安全性及び実装性能が確認された暗号技術で、市場における利用実績が十分であるか今後の普及が見込まれ、利用を推奨するもののリスト

②推奨候補暗号リスト

安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト

③運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったと確認されたが、互換性維持のために継続利用を容認する暗号技術のリスト

CRYPTREC Cryptography Research and Evaluation Committees

B）2025年度のCRYPTREC暗号リスト改訂の概要

- **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。

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、**従来から記載の表**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。

「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（Cryptographically Relevant Quantum Computer）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。

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）。

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。
- Category1・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。

<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

<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）

<パラメータセットの記載イメージ>

暗号技術	
名称	パラメーターセット
ML-KEM	ML-KEM-512 (Category 1) ML-KEM-768 (Category 3) ML-KEM-1024 (Category 5)

CRYPTREC Cryptography Research and Evaluation Committees

C) CRYPTREC暗号リスト(抄)(2026年3月改訂後)

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会(以下「CRYPTREC」という。)により安全性(セキュリティ)及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

なお、利用する鍵長について、「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」[3]の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。

<表１　現行暗号リスト>

技術分類		暗号技術
公開鍵暗号	署名	DSA（注１）
		ECDSA
		EdDSA
		RSA-PSS
		RSASSA-PKCS1-v1_5
	守秘	RSA-OAEP
	鍵共有	DH
		ECDH（注２）
共通鍵暗号	64ビットブロック暗号（注３）	該当なし
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128（注４）
		SHAKE256（注４）
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		XTS（注５）
	認証付き秘匿モード（注６）	CCM
		GCM（注７）
メッセージ認証コード		CMAC
		HMAC
認証暗号		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3
		ISO/IEC 9798-4

<表２　耐量子計算機暗号（PQC）リスト>

現行暗号の解読に利用可能な水準の量子計算機（CRQC: Cryptographically Relevant Quantum Computer）への耐性を有することが確認された暗号技術のリスト[4]。

技術分類		暗号技術	
		名称	パラメーターセット（注８）
公開鍵暗号	署名	－	－
	鍵共有	ML-KEM	ML-KEM-768 (Category 3) ML-KEM-1024 (Category 5)
共通鍵暗号		AES	AES-192 (Category 3) AES-256 (Category 5)
ハッシュ関数		SHA2	SHA-384 (Category 4) SHA-512
		SHA3	SHA3-384 (Category 4) SHA3-512

1･2　（略）

3 CRYPTREC, 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, https://www.cryptrec.go.jp/list.html
なお、当該設定基準の見直しの検討を行う予定であり、当面の間、表２（耐量子計算機暗号（PQC）リスト）の公開鍵暗号は、当該設定基準を適用しない。

4 暗号技術の耐量子計算機暗号（PQC）リストへの追加について検討中である。
https://www.cryptrec.go.jp/report/cryptrec-mt-1501-2026.pdf

（注１）～（注７）　（略）

（注８）　セキュリティのカテゴリを合わせて記載する。各カテゴリはNISTの“Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”に従い、次のように、カテゴリ名の右に記載の鍵探索又は衝突探索と同程度以上の計算資源が攻撃に必要であることを意味する。

- ･Category 1 128ビット鍵を持つブロック暗号に対する鍵探索
- ･Category 2 256ビットのハッシュ関数に対する衝突探索
- ･Category 3 192ビット鍵を持つブロック暗号に対する鍵探索
- ･Category 4 384ビットのハッシュ関数に対する衝突探索
- ･Category 5 256ビット鍵を持つブロック暗号に対する鍵探索

https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf （令和８年３月25日現在）

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

CRYPTREC Cryptography Research and Evaluation Committees

D）CRYPTREC暗号リスト移行ルール

<表２への追加に関するルール>
標準化等により将来的な利用が見込まれ、安全性や実装性能が十分にあると暗号技術検討会が決定した場合
（公募や事務局提案等）

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

<表２新設に関する臨時ルール>
表１の暗号技術のうち、CRQCへの耐性があると暗号技術検討会が決定したものを表２に追加する

次の条件のいずれかを満たすと暗号技術検討会が決定した場合

1. ５年ごとの利用実績調査により、複数の利用実績を確認した場合
2. その他、普及していることが明らか又は急速な普及が大いに見込まれる場合

標準化等により将来的な利用が見込まれ、安全性や実装性能が十分にあると暗号技術検討会が決定した場合
（公募や事務局提案等）
→ **②推奨候補暗号リスト**

- CRYPTREC暗号リストへの掲載から20年を超えた後に実施する最初の利用実績調査までに、十分な利用実績を確認できなかったもの
- 公募提案暗号について、提案会社より自主取下げ要望があり、暗号技術検討会における審議の結果「今後の普及が見込まれない公募提案暗号」であると判断されたもの

安全性維持が困難（危殆化した）と
暗号技術検討会が決定した場合

※電子政府推奨暗号リストに掲載された暗号技術は、利用者がいる前提であり、原則として、危殆化以外の理由では遷移させず、また、移行のための時間を確保する必要があるため、いきなりリストから削除することはしない。

③運用監視暗号リスト

（2019年度暗号技術検討会　決定事項）
次の条件のいずれかを満たすと暗号技術検討会が決定した場合、削除猶予期間を定めて周知を行った上で、その期間の満了後に自動的に削除する。

1. 運用監視暗号リストに掲載している注釈で示した互換性維持のための利用形態が必要なくなり、削除が妥当と判断した場合
2. 互換性維持の継続利用として使うにしても安全性維持が極めて困難で、互換性維持の継続利用が容認できないと判断した場合
3. その他、運用監視暗号リストに掲載している必要性の根拠を満たさなくなったと判断した場合

安全性維持が困難(危殆化した)と判断した場合

リストから削除

※利用実績調査の具体的な実施内容・評価基準は、暗号技術活用委員会において検討し、暗号技術検討会の承認を経た上で実施する。

※ ①・②への追加・遷移における安全性については、 CRQCへの耐性を見据えて評価を行う。

CRYPTREC Cryptography Research and Evaluation Committees

E) CRYPTREC暗号リストの耐量子計算機(PQC)対応に関する検討課題

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※1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。

※1: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>

暗号技術	
名称	パラメーターセット
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※2等から明らか。

※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※3については検討が必要。

※3 :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。(FIPS204、205は2026年度中に安全性評価等が終了予定。)

CRYPTREC Cryptography Research and Evaluation Committees

F) 2026年度　耐量子計算機暗号(PQC)リスト検討タスクフォース設置

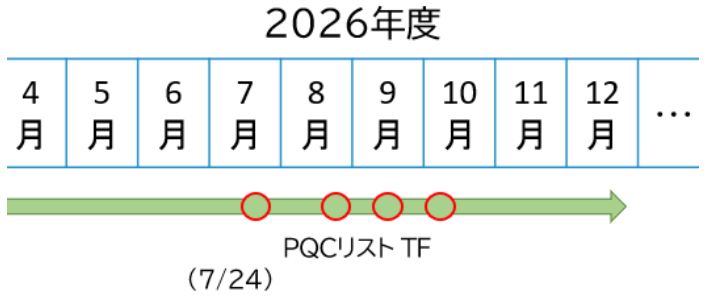
構成員・オブザーバ名簿（五十音順、敬称略）

■ 構成員

岩田 哲	名古屋大学　未来材料・システム研究所　教授
漆嶌 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 インターネットサービス事業本部 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
主査	
松本 勉	国立研究開発法人産業技術総合研究所　フェロー 横浜国立大学　先端科学高等研究院　上席特別教授

■ オブザーバ

内閣官房国家サイバー統括室



開催要綱から抜粋

1. 開催の趣旨・目的

量子計算機技術の進展に伴い、現在広く利用される公開鍵暗号の安全性が著しく低下すると想定され、耐量子計算機暗号(PQC)への移行は急を要する課題である。

CRYPTRECでは、CRYPTREC暗号リストのPQC対応を図るため、2025年度の暗号技術検討会において、電子政府推奨暗号リストに「耐量子計算機暗号(PQC)リスト」を加える改定を実施したところであるが、当該改定に関連して、**更なる検討を要する課題**が残されており、**安全性評価の観点に加え、利活用及び普及促進の観点も踏まえた専門的かつ横断的な整理**が必要となっている。

このため、CRYPTREC暗号リストのPQC対応に関する課題等の整理を行うことを目的として、**暗号技術検討会の下に「耐量子計算機暗号(PQC)リスト検討タスクフォース」**を開催する。

2. 検討事項

(1) 128ビットセキュリティ相当の暗号技術の取扱いに関する検討
(2) 暗号利用モード、メッセージ認証コード、認証暗号、エンティティ認証等の取扱いに関する検討
(3) 現行暗号とPQCを組み合わせたハイブリッドモードの取扱いに関する検討
(4) 公開鍵暗号方式のPQCの安全性評価等の進め方に関する検討
(5) その他、耐量子計算機暗号(PQC)リストの運用に関し必要な事項

CRYPTREC
Cryptography Research and Evaluation Committees

G) 2025年度の技術調査報告書等作成(暗号技術評価委員会)

■ 外部評価「耐量子計算機暗号ML-KEMの安全性・実装性能に関する評価及び調査」

- 耐量子計算機暗号ML-KEMの安全性・実装性能について、公開されている解析手法や評価結果の有無を調査し、存在する場合はその影響範囲等についてまとめるなど、安全性と実装性能を評価した上で報告書を作成した。
- 2025年度外部評価報告書に基づき、以下の結論を得た。
  - ML-KEMは、全てのパラメーターセット(ML-KEM-512/768/1024)において、米国NISTが規定するCategory1/3/5を満たしている。
  - ML-KEMは、従来方式と比較して高速である一方、鍵長及び暗号文長が増加するが、メモリ制約が厳しいデバイスを除き、実用上問題なく利用できる。
  - ML-KEMは、サイドチャネル攻撃対策が不十分な場合に脆弱性が生じる可能性があるものの、適切な対策の実装を前提とすれば、電子政府システムを含む多様なシステムへの広範な展開が可能である。

■ 外部評価「耐量子計算機暗号の移行に関する技術動向調査 」

- 耐量子計算機暗号(PQC)への移行に関する技術動向を調査し、公開情報を基にまとめ、考察等を行い、報告書を作成した。

CRYPTREC Cryptography Research and Evaluation Committees

H) 2025年度のガイドライン類等作成(暗号技術活用委員会)

■ 耐量子計算機暗号(PQC)の取扱いに係る検討

- PQCの取扱基準や位置付け・記載内容等についての検討を行った。具体的には、日本における「耐量子計算機暗号(PQC)への移行(方針)」を検討する際の素材としてもらうため、「耐量子計算機暗号(PQC)への移行(方針)」の政策的側面からの整理、及び「CRYPTREC暗号リスト」におけるPQCの位置付けや移行ルールを変更すべきかどうかを検討し、暗号技術活用委員会としての見解を取りまとめた。

■ クラウドにおける鍵管理ガイダンスの作成

- クラウド鍵管理ガイダンスWGを設置し、クラウドサービスを利用した情報システムにおける暗号鍵管理のガイダンス作成を開始した。2026年度末での完成に向けて、2025年度はガイダンスの骨子を整理した。

■ 「暗号鍵管理システム設計指針(基本編)」の改訂

- 暗号鍵管理システムの設計に関わる中心となる解説書である「暗号鍵管理システム設計指針(基本編)」の作成から約5年が経過し、記載に古い箇所がある、誤記がある等の問題が見つかった。修正の必要な箇所を洗い出し、改訂方針を議論した。

CRYPTREC Cryptography Research and Evaluation Committees

I) 2026年度における耐量子計算機暗号に関連する活動の全体像

■ **暗号技術検討会**においては、「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、CRYPTREC暗号リストにおける耐量子計算機暗号(PQC)への対応に関する課題等の整理を行う。

- 例年、暗号技術検討会は年度末に開催していたが、同タスクフォースにおける検討状況や暗号技術評価委員会におけるFIPS 204(ML-DSA)及びFIPS 205(SLH-DSA)に係る安全性・実装性能に関する調査及び評価の状況を踏まえながら、CRYPTREC暗号リストの速やかな改定に必要があれば、年度途中の開催も含めて開催することとする。

■ **暗号技術評価委員会**においては、

- 「暗号技術調査WG(耐量子計算機暗号)」において、耐量子計算機暗号(PQC)に関する技術動向を継続して調査・把握するとともに、ガイドライン及び調査報告書を作成する。また、「素因数分解の困難性に関する計算量評価」「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の更新についても同WGで検討し、更新を行う。
- CRYPTREC暗号リスト掲載に向けた耐量子計算機暗号(PQC)の技術的検討に資するための外部評価を実施する。具体的には、FIPS 204(ML-DSA)及びFIPS 205(SLH-DSA)の暗号技術について、安全性・実装性能に関する調査及び評価を行う。

■ **暗号技術活用委員会**においては、

- 「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」について、耐量子計算機暗号(PQC)の取扱いを含めた形での見直しを実施する。
- 「TLS暗号設定ガイドライン」について耐量子計算機暗号(PQC)のサポートに向けたTLS1.3への移行や電子証明書の有効期限の短縮化等に対応するため、2027年度の見直しに向けた検討を実施する。
- 「クラウド鍵管理ガイダンスWG」において、クラウドサービスを利用したシステムにおける暗号鍵管理の適切な設計・構築・運用のために、クラウド鍵管理ガイダンスを作成する。

CRYPTREC
Cryptography Research and Evaluation Committees

（参考）耐量子計算機暗号移行に関する最近の政府の動向

- **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」を2025年6月30日に設置。**
- 2025年11月に第2回 関係府省庁連絡会議を開催し、中間とりまとめにおいて、政府機関等の耐量子計算機暗号（PQC）への移行に向けた**工程表（ロードマップ）の骨子を策定。**

→サイバーセキュリティ戦略（閣議決定）：原則として、2035年までの移行を目指し、2026年度に工程表（ロードマップ）を策定

耐量子計算機暗号(PQC)利用に関する関係府省庁連絡会議

＜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）

工程表(ロードマップ)の骨子（概要）

移行対象	・**「政府機関等のサイバーセキュリティ対策のための統一基準」(※)の適用対象**となる情報システム ※サイバーセキュリティ基本法に基づく、**政府機関等（政府機関及び独立行政法人等）**の情報セキュリティ水準を維持・向上させるための統一的な枠組み
移行期限	・原則として、**2035年を目処**に移行。ただし、**情報の重要性や暗号技術の利用状況等を把握**した上で、どのように移行を進めるかを検討し、適切に判断 ・**例えば、特に機微な情報や保護期間が非常に長期となることが想定される情報等を扱う場合等**においては、**より早期に移行**を行うことも含め、情報システムごとに適切に検討を行う
移行に向けた取組	・今後策定する工程表（ロードマップ）において、政府機関等が移行に向けた計画を策定できるよう、**移行に向けた計画に盛り込むべき基本的事項や留意すべき事項**を示す ・**政府機関等は、今後策定する工程表（ロードマップ）を踏まえ、移行に向けた計画を策定し、移行期限までにPQCへ移行**を行う

関係府省庁の連携の下、**2026年度中に、工程表（ロードマップ）を策定する予定**

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