資料１

# 耐量子計算機暗号（PQC）リスト検討タスクフォース（第１回）

令和８年７月24日(金) 15:00～17:00
ＡＰ赤坂グリーンクロス　Ｂルーム
（ ハ イ ブ リ ッ ド 開 催 ）

＜議事次第＞

１．開会

２．議事

(1) 耐量子計算機暗号（PQC）リスト検討タスクフォースの設置について

(2) CRYPTREC暗号リストのPQC対応と検討課題について

(3) 課題①　Category 1・2の暗号等の取扱いについて

(4) 課題②　暗号利用モードや認証暗号等の取扱いについて

(5) 課題③　ハイブリッド構成の取扱いについて

(6) 課題④　公開鍵暗号方式のPQCの安全性評価等の進め方について

(7) その他

３．閉会

＜配付資料一覧＞

| | |
|---|---|
| 資料１ | 議事次第・配付資料一覧 |
| 資料２ | 「耐量子計算機暗号（PQC）リスト検討タスクフォース」開催要綱 |
| 資料３ | CRYPTREC暗号リストのPQC対応と検討課題 |
| 資料４ | 課題①　Category 1・2の暗号等の取扱い |
| 資料５ | 課題②　暗号利用モードや認証暗号等の取扱い |
| 資料６ | 課題③　ハイブリッド構成の取扱い |
| 資料７ | 課題④　公開鍵暗号方式のPQCの安全性評価等の進め方 |
| 資料８ | その他検討すべき事項 |
| 参考資料 | 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）（令和８年３月30日更新） |

以上

資料２

# 「耐量子計算機暗号（PQC）リスト検討タスクフォース」
# 開催要綱

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」（以下「TF」という。）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等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

３．構成等

(1) TFの構成員は、別紙のとおりとする。
(2) 主査は、構成員の互選により定める。
(3) 主査は、TF構成員の中から主査代理を指名できる。
(4) 主査は、TFの議事を掌握する。
(5) 主査が、緊急の理由によりやむを得ず不在となった場合、主査代理が主査に代わり議事を掌握する。
(6) 主査が必要と認めた者は、オブザーバとしてTFに出席することができる。
(7) 主査が必要と認めるときは、暗号技術の提案者、関連する利害関係者その他の参考人から意見を聴取することができる。
(8) その他、TFの運営に関し必要な事項は、主査が定めるところによる。

４．議事の公開

(1) TFは非公開とする。
(2) TFで使用した資料及びTFの議事概要については、次の場合を除き、公開する。
① 公開することにより当事者又は第三者の権利、利益や公共の利益を害するおそれがあると主査が認める場合
② その他、非公開とすることが必要と主査が認める場合

５．庶務

TFの庶務は、国立研究開発法人情報通信研究機構及び独立行政法人情報処理推進機構の協力を得て、デジタル庁、総務省及び経済産業省において処理する。

（別紙）

# 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<br>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<br>インターネットサービス事業本部 セキュリティ本部<br>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<br>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<br>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

資料３

# CRYPTREC暗号リストのPQC対応と検討課題

# CRYPTREC暗号リストの改定概要

- **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)<br>ML-KEM-768 (Category 3)<br>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。
- 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。

# 暗号技術検討会での議論を踏まえた修正箇所

暗号技術検討会での議論を踏まえた修正箇所
（暗号技術検討会 2025年度 報告書(CRYPTREC RP-1000-2025)から一部改変して抜粋）

- ✓ カテゴリの定義を明確にするための注釈を追記。
- ✓ 512ビットのハッシュ関数（SHA-512及びSHA3-512）について、カテゴリの定義に照らして明示的にCategory 5であるとは言えないことから、「(Category 5)」の記載を削除。
- ✓ ハッシュ関数のうちSHAKE256について、注釈等の扱いを精査する必要があることから、今回のCRYPTREC暗号リストの更新においては掲載を保留。

# （参考）CRYPTREC暗号リスト(抄)（2026.3更新後）

**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)<br>ML-KEM-1024 (Category 5) |
| 共通鍵暗号 | | AES | AES-192 (Category 3)<br>AES-256 (Category 5) |
| ハッシュ関数 | | SHA2 | SHA-384 (Category 4)<br>SHA-512 |
| | | SHA3 | SHA3-384 (Category 4)<br>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暗号リストのPQC対応に関する検討課題

- 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、Category1・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、2026年度末までを目途に検討を進める。

## 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＞

| 暗号技術 | |
|---|---|
| 名称 | パラメーターセット |
| ML-KEM | **ML-KEM-512 (Category 1)**<br>ML-KEM-768 (Category 3)<br>ML-KEM-1024 (Category 5) |
| AES | **AES-128 (Category 1)**<br>AES-192 (Category 3)<br>AES-256 (Category 5) |
| SHA2 | **SHA-256 (Category 2)**<br>**SHA-512/256 (Category 2)**<br>SHA-384 (Category 4)<br>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。 ※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。

※FIPS204、205は2026年度中に安全性評価等が終了予定。

資料４

# 課題①
# Category 1･2の暗号等の取扱い

# 検討ポイント①　セキュリティのカテゴリの定義

➢ 暗号技術検討会での議論を受けて追記した「**カテゴリの定義**」について、その**記載内容に過不足はないか。**

**【考え方】**

- ✓ カテゴリの定義については、米国NISTが2016年12月のPQC標準化公募（次ページ参照）で導入された記述をベースとし、暗号技術の観点からの正確性と、行政職員が参照する観点からの平易さ・利便性を総合的に勘案している。
- ✓ Category 1,3,5はブロック暗号に対する鍵探索に必要な計算資源、Category 2,4はハッシュ関数に対する衝突探索に必要な計算資源について定義されている。
- ✓ なお、例えばCategory 1では、128ビット鍵のブロック暗号の計算資源について触れられており、当該ブロック暗号の例としてAES-128が明記されている。

**<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)<br>ML-KEM-1024 (Category 5) |
| 共通鍵暗号 | | AES | AES-192 (Category 3)<br>AES-256 (Category 5) |
| ハッシュ関数 | | SHA2 | SHA-384 (Category 4)<br>SHA-512 |
| | | SHA3 | SHA3-384 (Category 4)<br>SHA3-512 |

（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）

# （参考）カテゴリ関連記載：カテゴリの定義（米国NIST）

**NIST (2016.12) “Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”**
https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

**4.A.5 Security Strength Categories**（抜粋）

NIST will base its classification on the range of security strengths offered by the existing NIST standards in symmetric cryptography, which NIST expects to offer significant resistance to quantum cryptanalysis. In particular, NIST will define a separate category for each of the following security requirements (listed in order of increasing strength):

NISTは、量子暗号解読に対して高い耐性を持つと見込まれる既存のNIST共通鍵暗号規格が提供するセキュリティ強度の範囲に基づいて、分類を行う予定です。特に、NISTは以下の各セキュリティ要件（強度の低い順に記載）について、それぞれ個別のカテゴリを定義します。

1) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 128-bit key (e.g. AES128)

1) 当該セキュリティ定義を破る攻撃には、128ビット鍵のブロック暗号（例：AES128）における鍵探索に要する計算資源と同等以上の計算資源が必要であること。

2) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 256-bit hash function (e.g. SHA256/ SHA3-256)

2) 当該セキュリティ定義を破る攻撃には、256ビットのハッシュ関数（例：SHA256/SHA3-256）における衝突探索に要する計算資源と同等以上の計算資源が必要であること。

3) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 192-bit key (e.g. AES192)

3) 当該セキュリティ定義を破る攻撃には、192ビット鍵のブロック暗号（例：AES192）における鍵探索に要する計算資源と同等以上の計算資源が必要であること。

4) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 384-bit hash function (e.g. SHA384/ SHA3-384)

4) 当該セキュリティ定義を破る攻撃には、384ビットのハッシュ関数（例：SHA384/SHA3-384）における衝突探索に要する計算資源と同等以上の計算資源が必要であること。

5) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 256-bit key (e.g. AES 256)

5) 当該セキュリティ定義を破る攻撃には、256ビット鍵のブロック暗号（例：AES256）における鍵探索に要する計算資源と同等以上の計算資源が必要であること。

※日本語は機械翻訳

# （参考）カテゴリ関連記載：カテゴリの定義（米国NIST）

**NIST (2024.12) NIST IR 8547 (Initial Public Draft)**
**"Transition to Post-Quantum Cryptography Standards"**
https://csrc.nist.gov/pubs/ir/8547/ipd

**4.1. NIST Cryptographic Algorithm Standards and Guidelines**（抜粋）

While NIST guidelines continue to use bit-length security strengths to describe the level of protection offered by an algorithm and parameter set against attacks by classical computers, post-quantum security is described using a collection of broad security categories. Each category is defined by a comparatively easy-to-analyze reference primitive, whose security serves as a floor for a wide variety of metrics that are deemed potentially relevant to practical security. NIST based its classification on the range of security strengths offered by the existing standards in symmetric cryptography. Table 1 provides a summary of these security categories.

NISTのガイドラインでは、従来のコンピュータによる攻撃に対するアルゴリズムおよびパラメータセットの保護レベルを示すために、引き続きビット長によるセキュリティ強度を用いていますが、耐量子セキュリティについては、広範なセキュリティカテゴリの集合を用いて記述されています。各カテゴリは、解析が比較的容易な「参照プリミティブ」によって定義されており、そのプリミティブのセキュリティ強度が、実用上のセキュリティに関連し得るとみなされる多種多様な指標の「最低基準（フロア）」としての役割を果たします。NISTは、共通鍵暗号の既存規格が提供するセキュリティ強度の範囲に基づいて、この分類を行いました。表1に、これらのセキュリティカテゴリの概要を示します。

※日本語は機械翻訳

Table 1: Post-Quantum Security Categories

| Security Category | Attack Type | Example |
|---|---|---|
| 1 | Key search on a block cipher with a 128-bit key | AES-128 |
| 2 | Collision search on a 256-bit hash function | SHA-256 |
| 3 | Key search on a block cipher with a 192-bit key | AES-192 |
| 4 | Collision search on a 384-bit hash function | SHA3-384 |
| 5 | Key search on a block cipher with a 256-bit key | AES-256 |

# （参考）カテゴリ関連記載：CRYPTREC PQCガイドライン

**「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）2024年度版」CRYPTREC GL-2007-2024**

**安全性レベル** NIST PQC標準化プロジェクトにおいて，暗号方式の安全性はレベル1から5で定義されており，提案者は応募時にパラメータと達成される安全性レベルを示す必要があった。レベル1, 3, 5はそれぞれAES128, AES192, AES256などの128, 192, 256bitsの秘密鍵を持つブロック暗号の鍵復元の困難性と同等かそれ以上の計算量であり，レベル2と4はそれぞれSHA256/SHA3-256とSHA384/SHA3-384などの256bitsと384bitsの暗号学的ハッシュ関数の衝突探索の困難性と同等かそれ以上の古典もしくは量子計算量とされている。レベル1から5の具体的な計算量は表1.1で与えられる。古典コンピュータによる攻撃者に対しては古典論理回路のゲート数が，量子コンピュータを利用可能な攻撃者に対しては量子回路のゲート数と最大深さの積が与えられている。計算量評価において，公開鍵暗号方式では，IND-CCA2安全性を考える際には$2^{64}$個以下の選択暗号文を復号オラクルに古典的にクエリできるとし，署名方式では，EUF-CMA安全性を考える際には$2^{64}$個以下のメッセージを署名オラクルに古典的にクエリできるとしている。

また，レベル1,3,5の量子回路計算量で$2^{157}$, $2^{221}$, $2^{285}$とされている部分は2016年のCall for proposalsでは$2^{170}$, $2^{233}$, $2^{298}$ であった。つまり，2016年のPQC候補でレベル1, 3, 5とされているものは2022年の定義でもレベル1, 3, 5 の基準を満たすことになる。この更新はAESを解読する量子回路の改良により，量子計算量が改善されたことによる。

表1.1: 2022年に公表されたNIST PQC標準化プロジェクト追加署名Call for proposalsにおける安全性レベルと計算量の対応表。各レベルは古典，量子のどちらか一方の基準を満たすものとして定義されている。

| レベル | 量子回路の (最大深さ)×(ゲート数) | 古典論理ゲート数 |
|---|---|---|
| レベル1 | $2^{157}$ | $2^{143}$ |
| レベル2 | – | $2^{146}$ |
| レベル3 | $2^{221}$ | $2^{207}$ |
| レベル4 | – | $2^{210}$ |
| レベル5 | $2^{285}$ | $2^{272}$ |

# 検討ポイント②　512ビットハッシュ関数の取扱い

➢ 暗号技術検討会での議論を受けて、512ビットのハッシュ関数（SHA-512及びSHA3-512）については、カテゴリの定義に照らしてCategory 5であると明示的にはいえないことから、「(Category 5)」の記載を削ったが、適切な取扱いはどうあるべきか。

**【考え方】**

✓暗号技術検討会における当初案では、次のような観点から512ビットのハッシュ関数は「Category 5」としていた。

- 米国NISTの文書ではセキュリティカテゴリについて「listed in order of increasing strength」と記載があること。
- 計算資源について、バースデーパラドックスから、「256ビット鍵のブロック暗号」≒「512ビットのハッシュ関数」と単純化して考えたこと。

✓しかしながら、次のような観点から改めて精査する必要があるため、今般の改定では「Category 5」の記載は削除した。

- ブロック暗号に対する鍵探索と、ハッシュ関数に対する衝突探索の計算資源を安易に比較することはできないこと。
- ハッシュ関数という観点から、「Category 4」とも捉えられること。

✓「カテゴリ」について、暗号技術を選択する上で重要な要素であり、カテゴリを付さない場合、利用者にとってはセキュリティの強弱がわかりにくいなど、利便性の観点で課題がある。

以上を踏まえて例えば次のような整理についてどう考えるか。

➢ 512ビットのハッシュ関数は、384ビットのハッシュ関数より安全であり、定義上も「同程度以上の計算資源」とされていることから、当面の間、Category 4として取り扱うことはできないか。

**<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)<br>ML-KEM-1024 (Category 5) |
| 共通鍵暗号 | | AES | AES-192 (Category 3)<br>AES-256 (Category 5) |
| ハッシュ関数 | | SHA2 | SHA-384 (Category 4)<br>SHA-512 |
| | | SHA3 | SHA3-384 (Category 4)<br>SHA3-512 |

（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）

# 検討ポイント③　Category 1・2の取扱い

➢ 表２の暗号技術のうち、Category 1・2（128ビットセキュリティ程度相当）のものについて、電子政府推奨暗号リストに掲載することが適当か。

**【考え方】**

- ✓「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」では、128ビットセキュリティは2031～2040年は「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。
- ✓ 政府システムは原則2035年にPQC移行することとなる中で、2041年以降に移行を検討しなければならない暗号技術を「推奨」することに妥当性があるのか。
- ✓ 一方で、CRYPTREC暗号リストに記載がない暗号については、政府の情報システムでの利用が難しくなるため、一律排除することには慎重な検討が必要。
- ✓ 海外の政府機関の例を見ると、公開鍵暗号方式について、Category 3～5を政府用途として想定する記載が多く見られるが、Category 1・2を明示的に排除するような記載は見受けられない。また、同じCategory 1・2であっても、共通鍵暗号方式については、現時点でより幅広く利用可能としている例が多い。
- ✓ 相互運用性・国際調達の観点から、Category 1・2を完全に排除すると不整合が生じかねない懸念。

＜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)**<br>ML-KEM-768 (Category 3)<br>ML-KEM-1024 (Category 5) |
| AES | **AES-128 (Category 1)**<br>AES-192 (Category 3)<br>AES-256 (Category 5) |
| SHA2 | **SHA-256 (Category 2)**<br>**SHA-512/256 (Category 2)**<br>SHA-384 (Category 4)<br>SHA-512 (Category 5) |

**＜参考：カテゴリのレベル＞**
**レベル１**　128ビット鍵を持つブロック暗号に対する鍵探索
**レベル２**　256ビットのハッシュ関数に対する衝突探索
**レベル３**　192ビット鍵を持つブロック暗号に対する鍵探索
**レベル４**　384ビットのハッシュ関数に対する衝突探索
**レベル５**　256ビット鍵を持つブロック暗号に対する鍵探索

以上を踏まえて例えば次のような整理についてどう考えるか。

- ➢ 相互運用性・国際調達の観点も踏まえ、Category 1・2も表２に含めることが考えられる。
- ➢ ただし、公開鍵暗号方式については、現行暗号リストとは異なる新たな暗号技術を採用することとなり、既存環境の影響も少ないため、可能な限り強度の高い暗号を使うべきであることから、Category 1・2のものについて、「可能な限り Category 3 以上の利用を推奨し、特に長期的な保護が必要なデータを扱う用途ではこれを強く推奨する。」と注釈を付すことが考えられる。
- ➢ 公開鍵暗号方式以外の暗号技術については、表１の現行暗号リストに掲載され既に利用されている暗号技術であることから、その連続性を重視し、現時点において注釈を付す等の対応をせず掲載することも考えられる。
- ➢ 暗号利用モード、メッセージ認証コード、エンティティ認証が追加された場合、複数の暗号技術を組み合わせるものであることから、カテゴリの定義が困難であるため、カテゴリを併記しないことでよいか。

# （参考）カテゴリ関連記載：海外政府機関による推奨状況①



| 暗号技術 | | ドイツ (BSI) | フランス (ANSSI) | オランダ (AIVD) | オーストラリア (ACSC) |
|---|---|---|---|---|---|
| 名称 | パラメーターセット | | | | |
| ML-KEM | ML-KEM-512 (Category 1) | | | | |
| | ML-KEM-768 (Category 3) | Recommended | préférence | Acceptable | approved* |
| | ML-KEM-1024 (Category 5) | Recommended | préférence | Recommended | approved |
| ML-DSA | ML-DSA-44 (Category 2) | | | | |
| | ML-DSA-65 (Category 3) | Recommended | préférence | Acceptable | approved* |
| | ML-DSA-87 (Category 5) | Recommended | préférence | Recommended | approved |
| SLH-DSA | SLH-DSA-[SHA2/SHAKE]-128[s/f] (Category 1) | | SLH-DSAの記載なし | Acceptable | 強度の記載なし |
| | SLH-DSA-[SHA2/SHAKE]-192[s/f] (Category 3) | Recommended | SLH-DSAの記載なし | Recommended | 強度の記載なし |
| | SLH-DSA-[SHA2/SHAKE]-256[s/f] (Category 5) | Recommended | SLH-DSAの記載なし | Recommended | 強度の記載なし |
| AES | AES-128 (Category 1) | Recommended | | Acceptable | approved* |
| | AES-192 (Category 3) | Recommended | | | approved* |
| | AES-256 (Category 5) | Recommended | encourage | Recommended | approved |
| SHA2 | SHA-256 (Category 2) | Recommended | | Recommended | approved* |
| | SHA-512/256 (Category 2) | Recommended | | | |
| | SHA-384 (Category 4) | Recommended | encourage | Recommended | approved |
| | SHA-512 (Category 5) | Recommended | encourage | Recommended | approved |
| SHA3 | SHA3-256 (Category 2) | Recommended | | Recommended | PQC内部使用のみ可 |
| | SHAKE128 (Category 2) | | | Acceptable | PQC内部使用のみ可 |
| | SHA3-384 (Category 4) | Recommended | encourage | Recommended | PQC内部使用のみ可 |
| | SHA3-512 (Category 5) | Recommended | encourage | Recommended | PQC内部使用のみ可 |
| | SHAKE256 (Category 5) | | encourage | Recommended | PQC内部使用のみ可 |

ドイツ（BSI）：“Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths”
フランス（ANSSI）：“Avis de l’ANSSI sur la migration vers la cryptographie post-quantique“（PQC移行に関するANSSIの見解）
オランダ（AIVD）：“The PQC Migration Handbook”
オーストラリア（ACSC）：“Guidelines for cryptography”

＊ 2030年以降は非推奨

# （参考）カテゴリ関連記載：海外政府機関による推奨状況②



**ドイツ　情報セキュリティ庁（BSI）**
**“Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths”** (2025.1)
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

**2.4.3. ML-KEM Key Agreement**（抜粋）　※[103]はFIPS203
ML-KEM with the parameter sets corresponding to NIST Security Strength Categories 3 and 5 (see Table 2.7) from [103] is considered cryptographically suitable for the long-term protection of confidential information at
the security level targeted in this Technical Guideline.

- ML-KEM-768, see [103],
- ML-KEM-1024, see [103].

Table 2.7: Recommended parameters for ML-KEM.

---

**オーストラリア　サイバーセキュリティセンター（ACSC）**
**“Guidelines for cryptography”** (2025.12時点)
https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cyber-security-guidelines/guidelines-for-cryptography

**Using the Module-Lattice-Based Key Encapsulation Mechanism**（抜粋）
The use of ML-KEM-768 and ML-KEM-1024 are approved. However, for interoperability and maintainability reasons, ML-KEM-768 will not be approved beyond 2030.

---

**イギリス　国家サイバーセキュリティセンター（NCSC）**
**“Next steps in preparing for post-quantum cryptography”** (2024.8)
https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography

**Key takeaways from this guidance**（抜粋）
ML-KEM (Kyber) and ML-DSA (Dilithium) are algorithms standardised by NIST that are suitable for general purpose use. All proposed parameter sets provide an acceptable level of security for personal, enterprise and OFFICIAL-tier government information. The NCSC recommends ML-KEM-768 and ML-DSA-65 as providing appropriate levels of security and efficiency for most use cases.

**フランス　国家情報システムセキュリティ庁（ANSSI）【仏語なので仮訳】**
**“Avis de l'ANSSI sur la migration vers la cryptographie post-quantique“（PQC移行に関するANSSIの見解）**(2023.12)
https://messervices.cyber.gouv.fr/guides/avis-de-lanssi-sur-la-migration-vers-la-cryptographie-post-quantique-0

**CRYSTALS-Kyber, aussi appelé ML-KEM**（抜粋・仮訳）
このアルゴリズムが暗号製品への組み込みに選定された場合、ANSSIは以下の推奨事項を示します。
1. 標準化されたインスタンスのパラメータを変更しないことが重要です。
2. パラメータは複数のセキュリティレベルで拒否されます。可能な限り最高のNISTセキュリティレベル、できればレベル5（AES-256に相当）またはレベル3（AES-192に相当）を使用することをお勧めします。

---

**オランダ　オランダ国家情報・安全保障局（AIVD）**
**“The PQC Migration Handbook”** (2024.12)
https://english.aivd.nl/publications/publications/2024/12/3/the-pqc-migration-handbook

**4.2) Recommended Cryptographic Primitives**（抜粋）

| Primitive | Recommended | Acceptable |
|---|---|---|
| ML-KEM[3] | ML-KEM-1024[1] | ML-KEM-768[1] |
| ML-DSA[3] | ML-DSA-87[2] | ML-DSA-65[2] |
| SLH-DSA | SLH-DSA-(SHA2/SHAKE)-256(s/f)<br>SLH-DSA-(SHA2/SHAKE)-192(s/f) | SLH-DSA-(SHA2/SHAKE)-128(s/f) |
| AES | AES-256 | AES-128 |
| SHA-3 | SHA-3-256<br>SHA-3-384<br>SHA-3-512<br>(c)SHAKE256 | SHA-3-224 (c)SHAKE128 |
| SHA-2 | SHA-256<br>SHA-384<br>SHA-512 | SHA-224 |

[1] Recommended to be deployed in a hybrid combination with ECDH. [2] Recommended to be deployed in a hybrid combination with either ECDSA or EdDSA. [3] BSI, ANSSI, NLNCSA recommend the use of NIST level 5 or 3 parameter sets. NSA CNSA 2.0 requires level 5.

Table 4.2 | Recommended parameter instantiations of the cryptographic primitives.

# （参考）カテゴリ関連記載：FIPS 203･204･205

**FIPS203 “Module-Lattice-Based Key-Encapsulation Mechanism Standard”**
https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.203.pdf

**8. Parameter Sets**（抜粋）
Concretely, ML-KEM-512 is claimed to be in security category 1,
ML-KEM-768 is claimed to be in security category 3,
and ML-KEM-1024 is claimed to be in security category 5.

**Table 2. Approved parameter sets for ML-KEM**

| | $n$ | $q$ | $k$ | $\eta_1$ | $\eta_2$ | $d_u$ | $d_v$ | required RBG strength (bits) |
|---|---|---|---|---|---|---|---|---|
| ML-KEM-512 | 256 | 3329 | 2 | 3 | 2 | 10 | 4 | 128 |
| ML-KEM-768 | 256 | 3329 | 3 | 2 | 2 | 10 | 4 | 192 |
| ML-KEM-1024 | 256 | 3329 | 4 | 2 | 2 | 11 | 5 | 256 |

**FIPS204 “Module-Lattice-Based Digital Signature Standard”**
https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.204.pdf

**4. Parameter Sets**（抜粋）
Concretely, the parameter set ML-DSA-44 is
claimed to be in security strength category 2,
ML-DSA-65 is claimed to be in category 3,
and ML-DSA-87 is claimed to be in category 5.

**Table 1. ML-DSA parameter sets**

| Parameters (see Sections 6.1 and 6.2 of this document) | Values assigned by each parameter set ML-DSA-44 | ML-DSA-65 | ML-DSA-87 |
|---|---|---|---|
| $q$ - modulus [see §6.1] | 8380417 | 8380417 | 8380417 |
| $\zeta$ - a 512th root of unity in $\mathbb{Z}_q$ [see §7.5] | 1753 | 1753 | 1753 |
| $d$ - # of dropped bits from $\mathbf{t}$ [see §6.1] | 13 | 13 | 13 |
| $\tau$ - # of $\pm 1$'s in polynomial $c$ [see §6.2] | 39 | 49 | 60 |
| $\lambda$ - collision strength of $\tilde{c}$ [see §6.2] | 128 | 192 | 256 |
| $\gamma_1$ - coefficient range of $\mathbf{y}$ [see §6.2] | $2^{17}$ | $2^{19}$ | $2^{19}$ |
| $\gamma_2$ - low-order rounding range [see §6.2] | $(q-1)/88$ | $(q-1)/32$ | $(q-1)/32$ |
| $(k, \ell)$ - dimensions of $\mathbf{A}$ [see §6.1] | (4,4) | (6,5) | (8,7) |
| $\eta$ - private key range [see §6.1] | 2 | 4 | 2 |
| $\beta = \tau \cdot \eta$ [see §6.2] | 78 | 196 | 120 |
| $\omega$ - max # of 1's in the hint $\mathbf{h}$ [see §6.2] | 80 | 55 | 75 |
| Challenge entropy $\log_2 \binom{256}{\tau} + \tau$ [see §6.2] | 192 | 225 | 257 |
| Repetitions (see explanation below) | 4.25 | 5.1 | 3.85 |
| Claimed security strength | Category 2 | Category 3 | Category 5 |

**FIPS205 “Stateless Hash-Based Digital Signature Standard”**
https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.205.pdf

**11. Parameter Sets（抜粋）**
Concretely, the parameter sets with $n = 16$ are
claimed to be in security category 1,
the parameter sets with $n = 24$ are
claimed to be in security category 3,
and the parameter sets with $n = 32$ are
claimed to be in security category 5.

**Table 2. SLH-DSA parameter sets**

| | $n$ | $h$ | $d$ | $h'$ | $a$ | $k$ | $lg_w$ | $m$ | security category | pk bytes | sig bytes |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SLH-DSA-SHA2-128s<br>SLH-DSA-SHAKE-128s | 16 | 63 | 7 | 9 | 12 | 14 | 4 | 30 | 1 | 32 | 7 856 |
| SLH-DSA-SHA2-128f<br>SLH-DSA-SHAKE-128f | 16 | 66 | 22 | 3 | 6 | 33 | 4 | 34 | 1 | 32 | 17 088 |
| SLH-DSA-SHA2-192s<br>SLH-DSA-SHAKE-192s | 24 | 63 | 7 | 9 | 14 | 17 | 4 | 39 | 3 | 48 | 16 224 |
| SLH-DSA-SHA2-192f<br>SLH-DSA-SHAKE-192f | 24 | 66 | 22 | 3 | 8 | 33 | 4 | 42 | 3 | 48 | 35 664 |
| SLH-DSA-SHA2-256s<br>SLH-DSA-SHAKE-256s | 32 | 64 | 8 | 8 | 14 | 22 | 4 | 47 | 5 | 64 | 29 792 |
| SLH-DSA-SHA2-256f<br>SLH-DSA-SHAKE-256f | 32 | 68 | 17 | 4 | 9 | 35 | 4 | 49 | 5 | 64 | 49 856 |

資料５

# 課題②：暗号利用モードや認証暗号等の取扱いについて

## １　背景：CRYPTREC 暗号リストにおける耐量子計算機暗号（PQC）の対応

- 現行暗号のうち、耐量子計算機性を有すると判断できる暗号技術をどの範囲まで「耐量子計算機暗号（PQC）リスト」に掲載するかが検討課題
- 2026 年 7 月時点の「耐量子計算機暗号（PQC）リスト」には、現行暗号のうち AES-192/256、SHA-384/512、SHA3-384/512 が掲載（128 ビットセキュリティの暗号技術である SHA-256、SHA3-256、SHA-512/256 については留保され別途検討）
- 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（Camellia、KCipher-2）とハッシュ関数（SHAKE128、SHAKE256）については、CRQC への耐性について引き続き検討が必要な対象として整理

本件では、CRQC への耐性について引き続き検討が必要とされた暗号技術を対象として、CRQC への耐性について検討する。

## ２　既存資料の整理

### （１）2024 年度外部評価報告書[1]

- Q1 モデル
  - 攻撃者は量子計算能力を有するが、オラクルへのアクセスは古典的クエリに限定されるモデル
- Q2 モデル
  - 攻撃者は量子計算能力を有し、オラクルへのアクセスにおいて量子重ね合わせ状態のクエリが可能であるモデル
  - GCM や CBC-MAC 等に対する多項式時間攻撃が報告されているが、その成立には秘密鍵を含む処理への量子オラクルアクセスが攻撃者に与えられる必要があり、通常の実運用とは大きく異なる前提に基づくものと整理
- 評価モデル
  - 実運用上は Q1 モデルを主たる評価モデルとして、鍵長、データ量制限、クエリ回数制限、既存の古典的安全性評価の範囲を明確化
- 暗号利用モード、メッセージ認証コード、認証暗号、Camellia、KCipher-2、SHAKE128、SHAKE256
  - 2024 年度外部評価報告書の表５・表６（本資料の付録１参照）において量子計算機への影響を整理

（２）2013 年度外部評価報告書[2]

- ISO/IEC 9798 で規定されているエンティティ認証技術（プロトコル）
  - 特定のプリミティブ、鍵長、パラメータ、証明書形式、乱数生成方式等を一意に規定するものではない
- 規定内容
  - ISO/IEC 9798-2：共通鍵暗号を用いる認証メカニズム
  - ISO/IEC 9798-3：電子署名を用いる認証メカニズム
  - ISO/IEC 9798-4：暗号チェック関数を用いる認証メカニズム
- エンティティ認証の安全性
  - 使用する暗号プリミティブの安全性だけでなく、なりすまし、リプレイ、セッション取り換え、鍵確認、時刻同期、状態管理、トラストアンカー、プロトコルメッセージの意味付け等に依存

（３）まとめ

- 暗号利用モード、メッセージ認証コード、認証暗号、Camellia、KCipher-2、SHAKE128、SHAKE256
  - 既存資料において CRQC への耐性があることが整理されている
- エンティティ認証
  - 暗号プリミティブそのものではなく、それらを組み合わせて構成されるプロトコルレイヤーの技術
  - 共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コード、認証暗号等とは評価対象のレイヤーが異なる

３　事務局案

（１）暗号利用モード、メッセージ認証コード、認証暗号、Camellia、KCipher-2、SHAKE128、SHAKE256

- CRQC 耐性があることから「耐量子計算機暗号（PQC）リスト」への掲載対象として扱う方向で検討することとしてはどうか。
- 特に、Q1 モデルを主たる実運用上の評価モデルとし、Q2 モデルにおける攻撃が成立する条件や、鍵長、タグ長、データ量制限、nonce・IV の条件、基盤プリミティブの選択等を明らかにすることについて検討が必要。
- それぞれのカテゴリ表記や既存注釈の扱いをどのようにするのか、別途検討が必要。

（２）エンティティ認証について

- 一概に CRQC 耐性があると言えず、「耐量子計算機暗号（PQC）リスト」への掲載対象とするのは保留することとしてはどうか。(掲載しない場合には利用できないことから、その影響についても引き続き検討が必要か。そもそも掲載された経緯についても確認が必要か。)
- 理由
  - 単一の暗号技術と同じ粒度で「耐量子計算機性を有する」と判断することは難しい。
  - ISO/IEC 9798 では、使用するプリミティブ、鍵長、パラメータ、証明書形式、乱数生成方式、時刻同期、状態管理等を一意に定めていない。
  - 具体的にどのような構成が耐量子性を有すると判断されたのかが不明確になるおそれがある。

４　参考文献

[1] 細山田光倫. 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. Technical Report CRYPTREC-EX-3401-2024, CRYPTREC, January 2025.
https://www.cryptrec.go.jp/exreport/cryptrec-ex-3401-2024.pdf.
[2] 山村明弘. ISO/IEC 9798 プロトコルの安全性評価. Technical Report CRYPTREC-EX-2013-2010, CRYPTREC, February 2011.
https://www.cryptrec.go.jp/exreport/cryptrec-ex-2013-2010.pdf.

# 付録 1

表 5　電子政府推奨暗号リストにあるハッシュ関数以外の共通鍵暗号技術と Ascon-AEAD および Ascon-80pq について，Q1 モデルで安全性が期待できる範囲．古典計算機のみが使える典型的な安全性評価と整合性を取るため，単一鍵の安全性に焦点を当て，量子計算機のリソースの想定としては 4.5 節の Case 0（小さい多項式サイズの量子計算機が 1 つ使えて，QRAM は必要な分だけ大きなものを使える）を仮定する．この表にある暗号技術については，Q1 モデルにおいて（古典的に考慮すべき事項から追加して）現状考慮すべきと思われる事柄は Grover のアルゴリズムによる鍵回復のみである．

| 技術分類 | 暗号技術名 | 鍵長（ビット） | Q1 モデルで安全性が期待できる範囲 |
|---|---|---|---|
| ブロック暗号 | AES, Camellia | 128 | 時間 $\leq 2^{64}$ |
| | | 192 | 時間 $\leq 2^{96}$ |
| | | 256 | 時間 $\leq 2^{128}$ |
| ストリーム暗号 | KCipher-2 | 128 | 時間 $\leq 2^{64}$ |
| 秘匿モード | CBC, CFB, CTR, OFB, XTS | $k$ | 時間 $\leq 2^{k/2}$ かつ古典的に安全性が保障される範囲 |
| 認証付き秘匿モード | CCM, GCM | $k$ | 時間 $\leq 2^{k/2}$ かつ古典的に安全性が保障される範囲 |
| メッセージ認証コード | CMAC, HMAC | $k$ | 時間 $\leq 2^{k/2}$ かつ古典的に安全性が保障される範囲 |
| 認証暗号 | ChaCha20-Poly1305 | 256 | 時間 $\leq 2^{128}$ かつ古典的に安全性が保障される範囲 |
| 認証暗号 | Ascon-AEAD128 | 128 | 時間 $\leq 2^{64}$ かつ古典的に安全性が保障される範囲 |
| 認証暗号 | Ascon-80pq | 160 | 時間 $\leq 2^{80}$ かつ古典的に安全性が保障される範囲 |

表 6　電子政府推奨暗号リストのハッシュ関数と Ascon-Hash256 および Ascon-(C)XOF128 に対して BHT のアルゴリズム（4.2 節）を適用する際に必要な計算時間と量子メモリの概算値．計算時間の値はそのまま，安全性が期待できる時間の範囲の上限に対応する．なお出力長とキャパシティの単位はいずれもビットである．スポンジ構造のハッシュ関数，特に XOF（SHAKE128，SHAKE256，Ascon-(C)XOF128）については，内部状態のキャパシティ部分で衝突を見つける攻撃も考慮に入っていることに注意されたい．

| 暗号技術名 | キャパシティ | 出力長 | 計算時間 | 量子メモリ |
|---|---|---|---|---|
| SHA-256 | - | 256 | $2^{85.3}$ | $2^{85.3}$ |
| SHA-512/256 | - | | | |
| SHA3-256 | 512 | | | |
| SHA-384 | - | 384 | $2^{128}$ | $2^{128}$ |
| SHA3-384 | 768 | | | |
| SHA-512 | - | 512 | $2^{170.7}$ | $2^{170.7}$ |
| SHA3-512 | 1024 | | | |
| SHAKE128 | 256 | $\ell$ ($\geq 256$) | $\min(2^{85.3}, 2^{\ell/3})$ | $\min(2^{85.3}, 2^{\ell/3})$ |
| SHAKE256 | 512 | $\ell$ ($\geq 256$) | $\min(2^{170.7}, 2^{\ell/3})$ | $\min(2^{170.7}, 2^{\ell/3})$ |
| Ascon-Hash256 | 256 | 256 | $2^{85.3}$ | $2^{85.3}$ |
| Ascon-(C)XOF128 | 256 | $\ell$ ($> 0$) | $\min(2^{85.3}, 2^{\ell/3})$ | $\min(2^{85.3}, 2^{\ell/3})$ |

付録２

２　暗号技術評価委員会事務局案：耐量子計算機暗号（PQC）リスト

耐量子計算機暗号（PQC）リストの事務局更新案を表に示す。

赤文字で示した方式は、電子政府推奨暗号の表２ 耐量子計算機暗号（PQC）リストに記載されていない暗号であることを示す。

グレーのハッチをかけた方式は、Category 1,2 となっている方式であるか、又は 512 ビットハッシュ関数に係るカテゴリの記載であり、これらは課題①での審議対象と考えている。

表　＜表２　耐量子計算機暗号（PQC）リスト＞更新案

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。

| 技術分類 | | 暗号技術 | |
|---|---|---|---|
| | | 名称 | パラメーターセット |
| 公開鍵暗号 | 署名 | － | － |
| | 鍵共有 | ML-KEM | ML-KEM-512 (Category 1)<br>ML-KEM-768 (Category 3)<br>ML-KEM-1024 (Category 5) |
| 共通鍵暗号 | ブロック暗号 | AES | AES-128 (Category 1)<br>AES-192 (Category 3)<br>AES-256 (Category 5) |
| | | Camellia | Camellia-128 (Category 1)<br>Camellia-192 (Category 3)<br>Camellia-256 (Category 5) |
| | ストリーム暗号 | KCipher-2 | KCipher-2 (Category 1) |
| ハッシュ関数 | | SHA2 | SHA-256 (Category 2)<br>SHA-512/256 (Category 2)<br>SHA-384 (Category 4)<br>SHA-512 (Category 4) |
| | | SHA3 | SHA3-256 (Category 2)<br>SHA3-384 (Category 4)<br>SHA3-512 (Category 4) |
| | | SHAKE | SHAKE128 (Category 2)<br>SHAKE256 (Category 2,4) |
| 暗号利用モード | 秘匿モード | CBC | CBC (Category 1,3,5) |
| | | CFB | CFB (Category 1,3,5) |
| | | CTR | CTR (Category 1,3,5) |

| | | | |
|---|---|---|---|
| | | OFB | OFB (Category 1,3,5) |
| | | XTS | XTS (Category 1,3,5) |
| | 認証付き秘匿モード | CCM | CCM (Category 1,3,5) |
| | | GCM | GCM (Category 1,3,5) |
| メッセージ認証コード | | CMAC | CMAC (Category 1,3,5) |
| | | HMAC | HMAC (Category 1,3,5) |
| 認証暗号 | | ChaCha20-Poly1305 | ChaCha20-Poly1305 (Category 5) |

以上

資料６

# 課題③
# ハイブリッド構成の取扱い

# 「ハイブリッド」の位置付け

NIST CSWP 39より

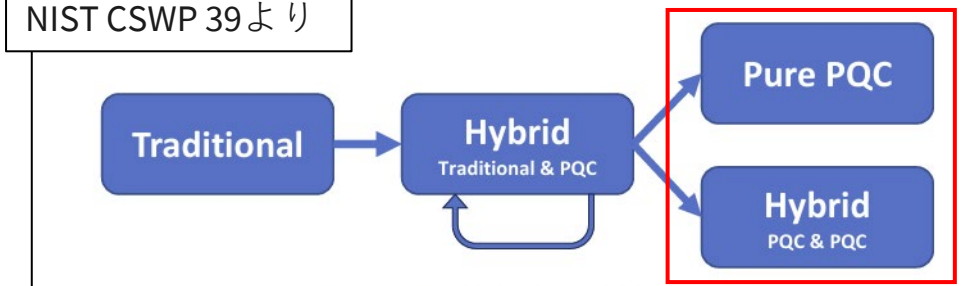



Fig. 1. Using a hybrid algorithm to transition to PQC

- **NIST における「ハイブリッド」**
  - ハイブリッドは、**移行期**において**不確実性に直面**しつつも**セキュリティを高める**ために有用な戦略。
    他方で、**複雑性は増加するため、cryptographic agilityや多数の暗号プロトコルを受け入れる能力が問われる**（NIST CSWP 39）。
  - ハイブリッドは移行期の選択肢であるが、要求しているわけではない。

SP800-227に記載のHybrid KEMに利用可能なKey combiner

$$\mathrm{KeyCombine}(K_1, K_2, c_1, c_2, \mathrm{ek}_1, \mathrm{ek}_2, p) := H(K_1, K_2, c_1, c_2, \mathrm{ek}_1, \mathrm{ek}_2, \mathrm{domain\_sep}). \quad (15)$$

- **EUにおける「ハイブリッド」**
  - (M)LWE ベースの暗号については、**移行に伴うリスク低減のため**ハイブリッド化を要求（should't be used in a standalone way）。
  - ハッシュベースの署名についてはハイブリッド化はoptional。
  - ETSI TS 103 744でハイブリッド構成について抽象化した定義を行っている。

**※ 米国とEUは、危殆化リスクとハイブリッド化による複雑化のトレードオフに対する指針が異なる。**

**※ NISTが移行期の選択肢の１つとして位置付ける一方、EUは一部PQCについては単独利用を推奨せず、ハイブリッドを要求している。**

# 「ハイブリッド」の位置付け

- **IETFでは、「ハイブリッド」に関する用語整理や分類がなされている**
  - 用語は定義されている。
    - **Multi algorithm scheme** : 部品となる複数の暗号コンポーネントより構成され、それらと同一の機能を持つもの（e.g. ECDSA＋ML-DSA　→　ハイブリッド署名アルゴリズム）。
    - **PQ/T hybrid scheme**：Multi Algorithmのうち、少なくとも１つのPQCアルゴリズムと、少なくとも１つの古典アルゴリズムを含むもの。
    - **PQ/PQ hybrid**も存在する。
    - PQ/T Hybrid KEM scheme, PQ/T Hybrid DSA scheme のようにscheme単位で使われることもあれば、PQ/T cryptographic element, PQ/T hybrid protocol等のelementやprotocol単位で使われることもある。
  - いくつかのSchemeやProtocolが標準化済み又は標準化中。

# 「ハイブリッド」の位置付け

表 4-1 ハイブリッド構成の目的と適用主体による整理

| 主体＼目的 | 後方互換性確保 | 安全性維持 |
|---|---|---|
| アルゴリズム | なし | 鍵共有アルゴリズム<br>• NIST SP 800-227(4.6. Multi-Algorithm KEMs and PQ/T Hybrids) [4]<br>• NIST SP 800-56C Rev.2[3] [9]<br>• draft-irtf-cfrg-hybrid-kems-07 [10]<br>• draft-ietf-lamps-pq-composite-kem-12 [11][4]<br>署名アルゴリズム<br>• draft-ietf-lamps-pq-composite-sigs-14 [12][4] |
| プロトコル | 通信プロトコル<br>• RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3 [13]<br>※4.1.1 Cryptographic Negotiationにより後方互換性を提供するが、混成方式ではない | 通信プロトコル<br>• draft-ietf-tls-hybrid-design-16 [14]<br>• draft-ietf-mls-combiner-02 [15]<br>• ETSI TS 103 744 [16]<br>• IEEE 802.11 Hybrid PQC Proposal [17]<br>• draft-ietf-lamps-pq-composite-kem-12 [11][4] |
| 証明書 | 証明書構造<br>• draft-ietf-lamps-certdiscovery-02 [18]<br>• ITU-T X.509(9.8 Alternative cryptographic algorithms and digital signature extensions) [19] | 証明書構造<br>• draft-ietf-lamps-pq-composite-sigs-14 [12][4] |
| | （後方互換性確保／安全性維持　共通）<br>• 耐量子移行を考慮したPKIベースのハイブリッド設計・実装<br>Architecting PKI Hierarchies for Graceful PQ Migration(PQC Conference) [20]<br>Hybrid PQC E-Mail Communication: Easing Migration Pain(PQC Conference) [21] | |

理屈上は、後方互換性志向として、「Cascade combiner」での鍵共有や、1-out-of-n署名が該当しうるが、採用に向けての動向は確認できなかった。

後方互換性確保を目的とした「混成」方式は、Negotiationで解決することが主流。
※プロトコル依存性が高く、
一概のリスト化は困難が予測される。

安全性維持のを目的とした「合成」方式の実態を紹介。

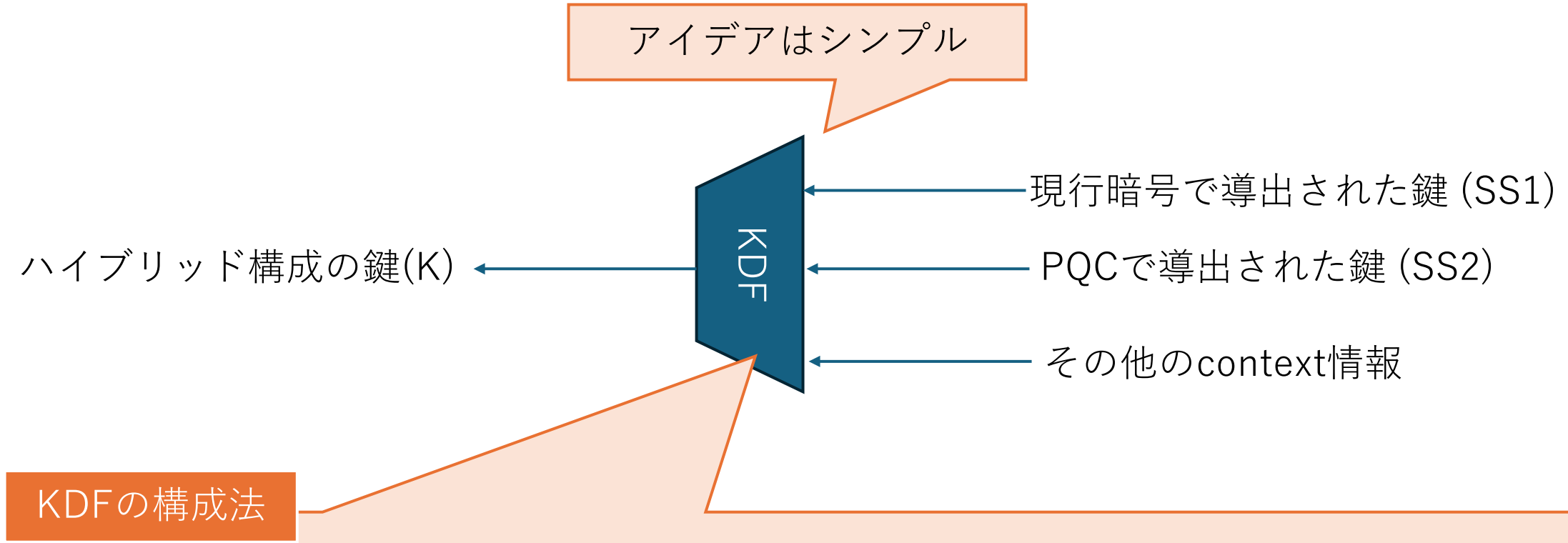
cryptrec-ex-3503-2025.pdf

※本資料では、ハイブリッドを上位概念とし、安全性維持目的を「合成」、後方互換性維持目的のものを「混成」と呼ぶ

# 「ハイブリッド」の位置付け

- **秘匿（KEM）用途**
  - マルチアルゴリズムKEMにおいて、複数の共有秘密から新たな共有秘密を導出する仕組をKey Combinerと呼んでいる。
    - NIST SP 800-227ではKDFの一利用形態としてKey Combinerを紹介。
      （既存KDFを、key combiner(コンバイナ)用途で利用することを承認）
    - ETSI. TS 103 744 では、Key Combiner定義し、構成論を記載している。
      （ETSI. TS 103 744, Quantum-safe Hybrid Key Exchanges. 2020.）
- **署名用途**
  - Composite署名（合成方式）については、IETFでの標準化が進展中。混成方式をサポートするDual SignatureについてもIETFでの標準化が進展中。
  - 以下についての議論は未成熟と認識しており、現状においてはリスト化の議論を行うための十分な議論を行う材料が揃っていないと認識（当資料末尾に関連資料有）。
    - ハイブリッドを利用する/利用しないユースケースはどのようなものか。
    - 合成（安全性確保）や混成（後方互換性確保）を利用する具体的なユースケースがどのようなものか。
    - 達成される安全性要件（Binding propertyのバインド対象をどうするか等）。
    - X.509やCMS方式との整合性確保をどのように行うか。

# ハイブリッドの構成法（暗号化・合成）




KDFの構成法

**Concatenation方式が主流**（e.g. **K = KDF(SS1||SS2||context)**）
※ SP800-227, draft-ietf-lamps-pq-composite-kem, draft-ietf-tls-ecdhe-mlkem

なお、**Cascade方式も存在**（ e.g. K= KDF2(KDF1(SS1)||SS2) ）　※ETSI TS 103 744にCascadeの規定あり。

# X.509 CMSのアルゴリズム指定



- **目標：**
  - 既存の（PKIX/CMS）APIを変えない。
- **方向性：**
  - 2つ以上のアルゴリズムを組み合わせて、**１つの新しい**アルゴリズムとして定義する。
- **実施例：**
  - Id-MLKEM768-ECDH-P256-SHA3-256（右表内の59）

    **ss = SHA3-256(mlkemSS || tradSS || tradCT || tradPK || Label)**

    **MLKEM鍵**　**ECDH鍵**　Context（アルゴリズム名等）
- **特徴：**
  - 「スタンドアローンで一般的な“アルゴリズム”」を定義している。
  - リストの要素数は多く、今後も増える見通し。
  - 鍵長も明記されている。

SMI Security for PKIX Algorithms

| Decimal | Description | Reference |
|---|---|---|
| 1 | id-alg-des40 | [Reserved and Obsolete] |
| 2 | id-alg-noSignature | [RFC-ietf-lamps-rfc5272bis-11] |
| 3 | id-alg-dh-sig-hmac-sha1 | [RFC2875] |
| 4 | id-alg-dhPop-sha1 | [RFC2875] |
| 5 | id-alg-dhPop-sha224 | [RFC6955] |
| 6 | id-alg-dhPop-sha256 | [RFC6955] |
| 7 | id-alg-dhPop-sha384 | [RFC6955] |
| 8 | id-alg-dhPop-sha512 | [RFC6955] |
| 15 | id-alg-dhPop-static-sha224-hmac-sha224 | [RFC6955] |
| 16 | id-alg-dhPop-static-sha256-hmac-sha256 | [RFC6955] |
| 17 | id-alg-dhPop-static-sha384-hmac-sha384 | [RFC6955] |
| 18 | id-alg-dhPop-static-sha512-hmac-sha512 | [RFC6955] |
| 25 | id-alg-ecdhPop-static-sha224-hmac-sha224 | [RFC6955] |
| 26 | id-alg-ecdhPop-static-sha256-hmac-sha256 | [RFC6955] |
| 27 | id-alg-ecdhPop-static-sha384-hmac-sha384 | [RFC6955] |
| 28 | id-alg-ecdhPop-static-sha512-hmac-sha512 | [RFC6955] |
| 29 | id-alg-eccsi-with-sha256 | [draft-wang-tls-raw-public-key-with-ibc-02] |
| 30 | id-RSASSA-PSS-SHAKE128 | [RFC8692] |
| 31 | id-RSASSA-PSS-SHAKE256 | [RFC8692] |
| 32 | id-ecdsa-with-shake128 | [RFC8692] |
| 33 | id-ecdsa-with-shake256 | [RFC8692] |
| 34 | id-alg-xmss-hashsig | [RFC9802] |
| 35 | id-alg-xmssmt-hashsig | [RFC9802] |
| 36 | id-alg-unsigned | [RFC9925] |
| 37 | id-MLDSA44-RSA2048-PSS-SHA256 | [RFC-ietf-lamps-pq-composite-sigs-19] |
| 38 | id-MLDSA44-RSA2048-PKCS15-SHA256 | [RFC-ietf-lamps-pq-composite-sigs-19] |
| 39 | id-MLDSA44-Ed25519-SHA512 | [RFC-ietf-lamps-pq-composite-sigs-19] |
| 40 | id-MLDSA44-ECDSA-P256-SHA256 | [RFC-ietf-lamps-pq-composite-sigs-19] |
| 41 | id-MLDSA65-RSA3072-PSS-SHA512 | [RFC-ietf-lamps-pq-composite-sigs-19] |
| 42 | id-MLDSA65-RSA3072-PKCS15-SHA512 | [RFC-ietf-lamps-pq-composite-sigs-19] |
| 43 | id-MLDSA65-RSA4096-PSS-SHA512 | [RFC-ietf-lamps-pq-composite-sigs-19] |
| 44 | id-MLDSA65-RSA4096-PKCS15-SHA512 | [RFC-ietf-lamps-pq-composite-sigs-19] |
| 45 | id-MLDSA65-ECDSA-P256-SHA512 | [RFC-ietf-lamps-pq-composite-sigs-19] |
| 46 | id-MLDSA65-ECDSA-P384-SHA512 | [RFC-ietf-lamps-pq-composite-sigs-19] |
| 47 | id-MLDSA65-ECDSA-brainpoolP256r1-SHA512 | [RFC-ietf-lamps-pq-composite-sigs-19] |
| 48 | id-MLDSA65-Ed25519-SHA512 | [RFC-ietf-lamps-pq-composite-sigs-19] |
| 49 | id-MLDSA87-ECDSA-P384-SHA512 | [RFC-ietf-lamps-pq-composite-sigs-19] |
| 50 | id-MLDSA87-ECDSA-brainpoolP384r1-SHA512 | [RFC-ietf-lamps-pq-composite-sigs-19] |
| 51 | id-MLDSA87-Ed448-SHAKE256 | [RFC-ietf-lamps-pq-composite-sigs-19] |
| 52 | id-MLDSA87-RSA3072-PSS-SHA512 | [RFC-ietf-lamps-pq-composite-sigs-19] |
| 53 | id-MLDSA87-RSA4096-PSS-SHA512 | [RFC-ietf-lamps-pq-composite-sigs-19] |
| 54 | id-MLDSA87-ECDSA-P521-SHA512 | [RFC-ietf-lamps-pq-composite-sigs-19] |
| 55 | id-MLKEM768-RSA2048-SHA3-256 | [draft-ietf-lamps-pq-composite-kem-10] |
| 56 | id-MLKEM768-RSA3072-SHA3-256 | [draft-ietf-lamps-pq-composite-kem-10] |
| 57 | id-MLKEM768-RSA4096-SHA3-256 | [draft-ietf-lamps-pq-composite-kem-10] |
| 58 | id-MLKEM768-X25519-SHA3-256 | [draft-ietf-lamps-pq-composite-kem-10] |
| 59 | id-MLKEM768-ECDH-P256-SHA3-256 | [draft-ietf-lamps-pq-composite-kem-10] |
| 60 | id-MLKEM768-ECDH-P384-SHA3-256 | [draft-ietf-lamps-pq-composite-kem-10] |
| 61 | id-MLKEM768-ECDH-brainpoolP256r1-SHA3-256 | [draft-ietf-lamps-pq-composite-kem-10] |
| 62 | id-MLKEM1024-RSA3072-SHA3-256 | [draft-ietf-lamps-pq-composite-kem-10] |
| 63 | id-MLKEM1024-ECDH-P384-SHA3-256 | [draft-ietf-lamps-pq-composite-kem-10] |
| 64 | id-MLKEM1024-ECDH-brainpoolP384r1-SHA3-256 | [draft-ietf-lamps-pq-composite-kem-10] |
| 65 | id-MLKEM1024-X448-SHA3-256 | [draft-ietf-lamps-pq-composite-kem-10] |
| 66 | id-MLKEM1024-ECDH-P521-SHA3-256 | [draft-ietf-lamps-pq-composite-kem-10] |

# TLS 1 .3の方向性

- **目標：**
  - プロトコル内部のHKDFのAPIを極力変更しない設計（入出力を抽象化して変換）
- **方向性：**
  - アルゴリズム指定は3つに分けて指定する。
    - **supported_groups：鍵交換アルゴリズム**を指定（リスト化済み）
    - signature_algorithms：署名アルゴリズムを指定（ハイブリッド署名でのスコープ。今後整備される見通し）
    - 共通鍵とハッシュの指定： Cipher suiteを指定（従来と同じ）
- **実施例：**
  - X25519MLKEM768（右表内の4588）

**Derive-Secret(Secret, Label, Messages) = HKDF-Expand-Label(Secret, Label, Transcript-Hash(Messages), Hash.length)**

**ECDHE鍵||MLKEMの鍵**

- **特徴：**
  - TLS1.2ではPQC対応を行わない。
  - アルゴリズム指定が分割しているので要素数は極端に増えない
  - 鍵長も明記される。

**supported_groups（コードポイント）**

Transport Layer Security (TLS) Parameters

| | | | | |
|---|---|---|---|---|
| | | | D | [RFC8422][RFC9847] |
| | | | D | [RFC8422][RFC9847] |
| | | | N | [RFC8422] |
| | | | N | [RFC8422] |
| | | | N | [RFC8422] |
| | | | N | [RFC8422] |
| 13 | sect571k1 | Y | N | [RFC8422] |
| 14 | sect571r1 | Y | N | [RFC8422] |
| 15 | secp160k1 | Y | D | [RFC8422][RFC9847] |
| 16 | secp160r1 | Y | D | [RFC8422][RFC9847] |
| 17 | secp160r2 | Y | D | [RFC8422][RFC9847] |
| 18 | secp192k1 | Y | D | [RFC8422][RFC9847] |
| 19 | secp192r1 | Y | D | [RFC8422][RFC9847] |
| 20 | secp224k1 | Y | D | [RFC8422][RFC9847] |
| 21 | secp224r1 | Y | D | [RFC8422][RFC9847] |
| 22 | secp256k1 | Y | N | [RFC8422] |
| 23 | secp256r1 | Y | Y | [RFC8422] |
| 24 | secp384r1 | Y | Y | [RFC8422] |
| 25 | secp521r1 | Y | N | [RFC8422] |
| 26 | brainpoolP256r1 | Y | N | [RFC7027] |
| 27 | brainpoolP384r1 | Y | N | [RFC7027] |
| 28 | brainpoolP512r1 | Y | N | [RFC7027] |
| 29 | x25519 | Y | Y | [RFC-ietf-tls-rfc8446bis-13][R |
| 30 | x448 | Y | Y | [RFC-ietf-tls-rfc8446bis-13][R |
| 31 | brainpoolP256r1tls13 | Y | N | [RFC8734] |
| 32 | brainpoolP384r1tls13 | Y | N | [RFC8734] |
| 33 | brainpoolP512r1tls13 | Y | N | [RFC8734] |
| 34 | GC256A | Y | N | [RFC9189] |
| 35 | GC256B | Y | N | [RFC9189] |
| 36 | GC256C | Y | N | [RFC9189] |
| 37 | GC256D | Y | N | [RFC9189] |
| 38 | GC512A | Y | N | [RFC9189] |
| 39 | GC512B | Y | N | [RFC9189] |
| 40 | GC512C | Y | N | [RFC9189] |
| 41 | curveSM2 | N | N | [RFC8998] |
| 42-255 | Unassigned | | | |
| 256 | ffdhe2048 | Y | N | [RFC7919] |
| 257 | ffdhe3072 | Y | N | [RFC7919] |
| 258 | ffdhe4096 | Y | N | [RFC7919] |
| 259 | ffdhe6144 | Y | N | [RFC7919] |
| 260 | ffdhe8192 | Y | N | [RFC7919] |
| 261-507 | Unassigned | | | |
| 508-511 | Reserved for Private Use | | | [RFC7919] |
| 512 | MLKEM512 | Y | N | [draft-connolly-tls-mlkem-key |
| 513 | MLKEM768 | Y | N | [draft-connolly-tls-mlkem-key |
| 514 | MLKEM1024 | Y | N | [draft-connolly-tls-mlkem-key |
| 515-2569 | Unassigned | | | |
| 2570 | Reserved | Y | N | [RFC8701] |
| 2571-4586 | Unassigned | | | |
| 4587 | SecP256r1MLKEM768 | Y | N | [draft-ietf-tls-ecdhe-mlkem-0 |
| 4588 | X25519MLKEM768 | Y | N | [draft-ietf-tls-ecdhe-mlkem-0 |
| 4589 | SecP384r1MLKEM1024 | Y | N | [draft-ietf-tls-ecdhe-mlkem-0 |
| 4590 | curveSM2MLKEM768 | N | N | [draft-yang-tls-hybrid-sm2-ml |

# ETSI TS 103 744

- **ハイブリッド構成論**
  - Lamps, TLSでのHybridを抽象化すれば、その構成方法に該当することになると認識。
    - 該当性の確認については、lamps- ETSIのリエゾンで解決する方向性と認識。



**Fixed values:**

*KDF* - The key derivation function being used from clause 7.4.

*f* - A context formatting function being used from clause 7.2. When KDF is instantiated as HKDF with hash, the underlying hash function is applied to the concatenate-and-hash context formatting function.

*k_len* - an integer value denoting the length of keys such as *psk*; *k_len* is *digest_len* when CatKDF is instantiated with HKDF or HMAC and *kmac_outlen* when CatKDF is instantiated as KMAC. *kmac_outlen* is set to 32 or 48 octets for KMAC128 and KMAC256, respectively.

**Input:**

*psk* - a pre-shared secret key of length *k_len*. It may be present. If not present, this value shall be the empty octet string, ∅.

*($k_1$, $k_2$) - a pair* of octet strings containing shared secrets $k_i$, derived through a hybrid key establishment, see Figure 4 and Figure 5.

*MA, MB* - octet string of a pair of exchanged messages in establishment of the shared secrets $k_i$.

*info* - an optional octet string set by the application as additional information.

*label* - an optional octet string that specifies a separation of use for the instance of the key establishment. The label values should be constructed from exchanged label contribution values in messages *MA* and *MB*. If a label value is used it shall be of a fixed agreed length. Any labels used in the key derivation function should not be provided as an argument to the same hash function for another purpose in the application.

*length* - the length in octets of the derived key material *key_material*.

**Process:**

1) Form $secret = psk \,||\, k_1 \,||\, k_2$.
2) Set *context = f(info, MA, MB)*, where *f* is a context formatting function.
3) *key_material = KDF(secret, label, context, length)*.
4) Return *key_material*.

**Output:**

*key_material* - derived key material.

An implementation shall fix the order of the shared secrets $k_i$ according to the order of the key establishment schemes defined in clause 7.7.2.

A pre-shared key, *psk*, for this method may be established using key material from a previous session or an alternative key-establishment method like QKD.

# 署名に関してのハイブリッド関連議論



- **ハイブリッド署名について、議論は未成熟**
  - 安全性定義、バインディングの対象（達成しようとする安全性に依存）、バインディング方式（バインディングの対象に依存）、X.509やCMS等の既存のデータフォーマットへの整合等の論点が議論が完全には収束していない。

- ハイブリッド署名**アルゴリズム**アプローチ
  - Composite 署名：KEMと似た議論、標準化中
  - 一般化するためには、EUF-CMAでなく、SUF-CMAが要求されるのではないかとの議論もある。
    - PQとTの、Tだけ入れ替えることにより、同一メッセージに対する複数署名を作れてしまう。それを偽造と解釈するのであれば、SUF-CMAが求められるが、現在の案はEUF-CMAしかみたしていない

- ハイブリッド署名**プロトコル**
  - TLSの暗号化と同様のアプローチで、ハイブリッド署名プロトコルを構成するアプローチもあるが、議論は活発ではない。
    （署名は、プロトコルレイヤでなくアルゴリズムレイヤでの解決を優先するものと推測）
  - Dual署名に関して：プロトコルのみでなくポリシーレイヤにも依存しうるが、基本的に各論であり一般論でない。
  - 並列署名とネスト型署名に関しての議論は未成熟

# リスト化に向けての考慮点

- **スコープの選定**
  - 秘匿用途のハイブリッドの検討を優先して行い、署名用途のハイブリッドのリスト化は議論の成熟を確認しつつ行うとの整理で問題ないか。
  - 秘匿用途のハイブリッドについては、安全性確保のための合成用途をスコープとするということで問題ないか。
  - 2種アルゴリズムのハイブリッド（例：ECDH＋MLKEM）のみとすることで良いか（理論上は3種以上のアルゴリズムのハイブリッドも存在する）。
  - PQ/T ハイブリッドのみをスコープとするか、将来の移行に備えてPQ/PQハイブリッドもスコープに含むか

- **リスト化の単位をどのようにするか**
  - コンバイナ（Key Combiner）をリスト化の単位とするか
    - ETSIを引用する場合には、Concatenationのみを採用するか、Cascadeの扱いをどうするか
  - 許容するアルゴリズムの組み合わせを列挙する方式を採用するのか
    - 将来的に、状態数が非常に多くなる可能性がある
  - そもそもリストには記載しないか

# 参考：リスト記載案

- **コンバイナを直接記載する方向性（EUアプローチに近い）**
  - 案１：技術分類に**コンバイナを新設**し、暗号名称**CatKDF（ETSI TS 103 744）**を記載する（または類似する文章を作成し、その文章内で命名した名称を記載）。
  - 案２：**鍵共有の技術分類内**に、暗号名称**CatKDF（ETSI TS 103 744）**を記載する（または類似する文章を作成し、その文章内で命名した名称を記載）。

- **コンバイナとその入力をセットでリストに記載する方向性（X.509のアプローチ）**
  - 案３：安全性が確認できた**compositeKEM（合成方式）のリスト**を記載する。
    - 組み合わせで、相当な数になる見通し。

- **コンバイナはKDFの１つのユースケースとして扱い、リストに記載しない方向性（NISTアプローチに近い）**
  - 案４：コンバイナを使う時のKDFにおいては、電子政府推奨暗号リストに記載されたハッシュ関数を利用するようにと注意喚起する。
    - 安全な現行暗号アルゴリズムと安全なPQCアルゴリズムを組み合わせても、安全になるとは限らない旨も示す。

# 参考：関連する技術論点

- **鍵長の選択（２つの方式の強度を揃えるのか）**
  - 最小強度をどうするか（class 1,2 をどうするか）
  - あえてPQを強くするという考えもあるが、それも含めるか
  - 鍵長に関しては、別ドキュメントでまとめるとの整理で良いか

- **KDFへの入力やメタデータ**
  - 入力順序の固定はどうするか
  - Contextをどのように記載するか
  - 入力の長さ管理を明示的に行うか
  - 上位プロトコルでバインディング等を行っている場合の扱いをどうするか

資料７

# 課題④
# 公開鍵暗号方式のPQCの安全性評価等の進め方

# 公開鍵暗号方式のPQCの安全性評価等の進め方

- CRYPTREC暗号リストへの掲載に向けて安全性及び実装性能の評価を行うべき暗号として、現状、FIPS 203～205が予定されているが、**FIPS 203～205以外のPQCについてどのように取り扱うべきか**。
  - FIPS 203 (ML-KEM)　格子暗号ベース　暗号化・鍵交換用途　2025年度末目途に評価
  - FIPS 204 (ML-DSA)　格子暗号ベース　署名用途　2026年中頃目途に評価
  - FIPS 205 (SLH-DSA)　ハッシュ関数ベース　署名用途　2026年度末目途に評価

**【考え方】**

✓現在標準化作業等が行われている次の**FIPS標準**（米国連邦情報処理標準）について、これらのPQCは、米国を中心として**世界的な利用が見込まれることから、安全性評価等の対象**としてはどうか。

- FIPS 206? (FN-DSA)　格子暗号ベース　署名用途
- FIPS 207? (HQC)　符号ベース　暗号化・鍵交換用途
- 追加公募されている方式　格子暗号以外？　署名用途

✓このほか、「**NTRU**」（格子暗号ベース、暗号化・鍵交換用途）について、次のとおりの状況であり、**安全性評価等の対象**としてはどうか。

（評価対象にしうる場合、詳細についてNTRUを担当するNTTからTFで説明をしてもらうことがよいのではないか。）

- 安全性について、複数国の専門家が参加する場で十分に評価されている（NIST Round3）
- ISOその他複数の国際的な標準化機関・団体で標準化され、又は標準化される見込みがある
- 国内主要事業者の製品・サービスに使用され、又は使用される見込みがある

✓安全性評価等のスケジュールについては、暗号技術評価委員会において検討いただくこととしてはどうか。

資料８

# その他検討すべき事項

# 検討ポイント①　暗号利用モード等に関する注釈

➢ 表２（耐量子計算機暗号（PQC）リスト）に暗号利用モード等を追加する場合、表２の注釈の記載ぶりを変更する必要があるのではないか。

**【考え方】**

✓ 暗号技術を組み合わせた場合の量子コンピュータへの耐性について明記する必要があり、例えば「また、表２（耐量子計算機暗号（PQC）リスト）のいずれかの暗号技術と組み合わせた場合に限り、量子計算機への耐性を有すると判断する。」旨を該当注釈に追記する必要があるのではないか。

**電子政府推奨暗号リスト**

暗号技術検討会及び関連委員会[1]（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＞
（略）

＜表２　耐量子計算機暗号（PQC）リスト＞
（略）

2 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

# 検討ポイント②　現行暗号に係る暗号技術の注釈の取扱い

➢ 表１（現行暗号リスト）にある暗号技術について、表２（耐量子計算機暗号（PQC）リスト）に追加する場合、既存注釈の取扱いをどのようにするか。

**【考え方】**

- ✓ **SHAKE128、SHAKE256に係る「注４」**
  →同様の注釈が必要ではないか。
- ✓ **XTSに係る「注５」**
  →前段については、64ビットブロック暗号が表２に存在しないことから、同様の注釈は不要か。（そもそも表２に64ビットブロック暗号を入れる可能性があるか。）
  後段についてはXTS自体の制限事項であるため同様の注釈が必要ではないか。
- ✓ **認証付き秘匿モード（CCM、GCM）に係る「注６」**
  →同様の注釈が必要ではないか。
  ただ、「ブロック暗号」の範囲は表２に閉じる必要があるか。
- ✓ **GCMに係る「注７」**
  →同様の注釈が必要ではないか。

**<表１　現行暗号リスト>**

| 技術分類 | | 暗号技術 |
|---|---|---|
| （略） | | （略） |
| ハッシュ関数 | | （略） |
| | | 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 |

（注４）ハッシュ長は256ビット以上とすること。
（注５）ブロック暗号には、CRYPTREC暗号リスト掲載128ビットブロック暗号を使う。利用用途はストレージデバイスの暗号化に限り、実装方法はNIST SP800-38Eに従うこと。
（注６）CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。
（注７）初期化ベクトル長は96ビットを推奨する。

# 検討ポイント③　現行暗号に係る暗号技術のカテゴリの取扱い



➢ 表１（現行暗号リスト）にある暗号技術について、表２（耐量子計算機暗号（PQC）リスト）に追加する場合、カテゴリ表記をどのようにするか。

**【考え方】**

✓ **暗号利用モード及びメッセージ認証コード**

→2024年度外部評価報告書において、鍵長がkビットのとき、Q1モデルで安全性が期待できる範囲は、「時間≦$2^{k/2}$かつ古典的に安全性が保障される範囲」とされる。
このため、**「Category 1, 3, 5」と表記し（**or **カテゴリ表記は付さず**）、さらに次の注釈を付してはどうか。

> **使用するブロック暗号の鍵長に依存し、鍵長は128ビット以上とする。128ビット以上の場合は Category 1、192ビット以上の場合は Category 3、256ビット以上の場合は Category 5とする。**

（併せて、「名称」の列と、「パラメーターセット」の列を結合するかどうかも検討が必要。）

✓ **認証暗号（ChaCha20-Poly1305）**

→2024年度外部評価報告書において、鍵長が256ビットに対して、Q1モデルで安全性が期待できる範囲は、「時間≦$2^{128}$かつ古典的に安全性が保障される範囲」とされる。このため、「**Category 5**」としてよいか。

✓ **SHAKE128**

→2024年度外部評価報告書において、出力長がn(≧256)ビットに対して、BHTアルゴリズムを適用する際に必要な計算時間と量子メモリの概算値は $\min(2^{256/3}, 2^{n/3})$ である。これはSHA-256の計算時間と量子メモリの概算値 $2^{256/3}$ と同じ。このため、ハッシュ長に関わらず、「**Category 2**」としてよいか。

✓ **SHAKE256**

→2024年度外部評価報告書において、出力長がn(≧256)ビットに対して、BHTアルゴリズムを適用する際に必要な計算時間と量子メモリの概算値は $\min(2^{512/3}, 2^{n/3})$ である。ハッシュ長により強度が変わるため、
**「Category 2, 4」と表記し（**or **カテゴリ表記は付さず**）、さらに次の注釈を付してはどうか。

> **ハッシュ長が256ビット以上の場合は Category 2、384ビット以上の場合は Category 4とする。**

(注) 2024年度外部評価報告書：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）

# 検討ポイント④　用語の定義等その他検討すべき事項

➢ その他、本タスクフォースにおいて調査・検討すべき事項はあるか

**【考え方】**

✓ CRYPTRECの各種文書で「量子コンピュータ」と「量子計算機」が表記揺れており、記載の統一を図るべきではないか。
例えば、原則として「量子コンピュータ」とすることとした上で、固有名詞的に定着している「耐量子計算機暗号(PQC)」を例外とすることとしてはどうか。
→表２の説明文の修正が必要

**<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)<br>ML-KEM-1024 (Category 5) |
| 共通鍵暗号 | | AES | AES-192 (Category 3)<br>AES-256 (Category 5) |
| ハッシュ関数 | | SHA2 | SHA-384 (Category 4)<br>SHA-512 |
| | | SHA3 | SHA3-384 (Category 4)<br>SHA3-512 |

（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）

# （参考）電子政府推奨暗号リスト～再改定後のイメージ

暗号技術検討会及び関連委員会（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」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 |
| | | ECDSA |
| | | EdDSA |
| | | RSA-PSS |
| | | RSASSA-PKCS1-v1_5 |
| | 守秘 | RSA-OAEP |
| | 鍵共有 | DH |
| | | ECDH |
| 共通鍵暗号 | 64ビットブロック暗号 | 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 |
| | | SHAKE256 |
| 暗号利用モード | 秘匿モード | CBC |
| | | CFB |
| | | CTR |
| | | XTS |
| | 認証付き秘匿モード | CCM |
| | | GCM |
| 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~~量子コンピュータ（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。

| 技術分類 | | 暗号技術 | |
|---|---|---|---|
| | | 名称 | パラメーターセット |
| 公開鍵暗号 | 署名 | – | – |
| | 鍵共有 | ML-KEM | ML-KEM-512 (Category 1)<br>ML-KEM-768 (Category 3)<br>ML-KEM-1024 (Category 5) |
| 共通鍵暗号 | ブロック暗号 | AES | AES-128 (Category 1)<br>AES-192 (Category 3)<br>AES-256 (Category 5) |
| | | Camellia | Camellia-128 (Category 1)<br>Camellia-192 (Category 3)<br>Camellia-256 (Category 5) |
| | ストリーム暗号 | KCipher-2 | KCipher-2 (Category 1) |
| ハッシュ関数 | | SHA2 | SHA-256 (Category 2)<br>SHA-512/256 (Category 2)<br>SHA-384 (Category 4)<br>SHA-512 (Category 4？) |
| | | SHA3 | SHA3-256 (Category 2)<br>SHA3-384 (Category 4)<br>SHA3-512 (Category 4？) |
| | | SHAKE | SHAKE128 (Category 2)<br>SHAKE256 (Category 2, 4？) |
| 暗号利用モード | 秘匿モード | CBC (Category 1, 3, 5) | |
| | | CFB (Category 1, 3, 5) | |
| | | CTR (Category 1, 3, 5) | |
| | | OFB (Category 1, 3, 5) | |
| | | XTS (Category 1, 3, 5) | |
| | 認証付き秘匿モード | CCM (Category 1, 3, 5) | |
| | | GCM (Category 1, 3, 5) | |
| メッセージ認証コード | | CMAC (Category 1, 3, 5) | |
| | | HMAC (Category 1, 3, 5) | |
| 認証暗号 | | ChaCha20-Poly1305 (Category 5) | |
| エンティティ認証 | | ISO/IEC 9798-2 | |
| | | ISO/IEC 9798-3 | |
| | | ISO/IEC 9798-4 | |

**SHA3とSHAKEの分離・統合【P】**

**暗号利用モード等における名称とパラメーターセットの分離【P】**

# 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）

令和５年３月30日
デジタル庁・総務省・経済産業省
（最終更新：令和８年３月30日）

## 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） |

（次ページに続く）

1 デジタル庁統括官、総務省サイバーセキュリティ統括官及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、デジタル庁、総務省及び経済産業省における施策の検討に資することを目的として開催。

2 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

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。

| 技術分類 | | 暗号技術 |
|---|---|---|
| 暗号利用モード | 秘匿モード | CBC |
| | | CFB |
| | | CTR |
| | | OFB |
| | | 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 |

（注１）FIPS PUB 186-5では廃止されているが、本リスト掲載時から安全性・利用実績の状況に大きな変化がないため、掲載を継続する。

（注２）使用するMACはHMAC又はCMACに限る。

（注３）CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、$2^{20}$ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、$2^{21}$ブロックまでとする。

（注４）ハッシュ長は256ビット以上とすること。

（注５）ブロック暗号には、CRYPTREC暗号リスト掲載128ビットブロック暗号を使う。利用用途はストレージデバイスの暗号化に限り、実装方法はNIST SP800-38Eに従うこと。

（注６）CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

（注７）初期化ベクトル長は96ビットを推奨する。

## ＜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 | ー | ー |
| | 鍵共有 | ML-KEM | ML-KEM-768 (Category 3)<br>ML-KEM-1024 (Category 5) |
| 共通鍵暗号 | | AES | AES-192 (Category 3)<br>AES-256 (Category 5) |
| ハッシュ関数 | | SHA2 | SHA-384 (Category 4)<br>SHA-512 |
| | | SHA3 | SHA3-384 (Category 4)<br>SHA3-512 |

（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）

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

**推奨候補暗号リスト**

CRYPTRECにより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[5]のリスト。なお、本リストに記載されている暗号技術を利用する際は、「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」[6]の規定に合致する鍵長を用いることが求められることに留意すること。

| 技術分類 | | 暗号技術 |
|---|---|---|
| 公開鍵暗号 | 署名 | 該当なし |
| | 守秘 | 該当なし |
| | 鍵共有 | PSEC-KEM（注９） |
| 共通鍵暗号 | 64ビットブロック暗号（注10） | CIPHERUNICORN-E |
| | | Hierocrypt-L1 |
| | | MISTY1 |
| | 128ビットブロック暗号 | CIPHERUNICORN-A |
| | | CLEFIA |
| | | Hierocrypt-3 |
| | ストリーム暗号 | Enocoro-128v2 |
| | | MUGI |
| | | MULTI-S01（注11） |
| ハッシュ関数 | | 該当なし |
| 暗号利用モード | 秘匿モード | 該当なし |
| | 認証付き秘匿モード（注12） | 該当なし |
| メッセージ認証コード | | PC-MAC-AES |
| 認証暗号 | | 該当なし |
| エンティティ認証 | | 該当なし |

（注９）KEM（Key Encapsulating Mechanism）－DEM（Data Encapsulating Mechanism）構成における利用を前提とする。

（注10）CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、$2^{20}$ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、$2^{21}$ブロックまでとする。

（注11）平文サイズは64ビットの倍数に限る。

（注12）CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

5 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

6 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

**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CRYPTRECにより確認された暗号技術[7]のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持[8]以外の目的での利用は推奨しない。なお、本リストに記載されている暗号技術を利用する際は、「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」[9]の規定に合致する鍵長を用いることが求められることに留意すること。

| 技術分類 | | 暗号技術 |
|---|---|---|
| 公開鍵暗号 | 署名 | 該当なし |
| | 守秘 | RSAES-PKCS1-v1_5 (注13) |
| | 鍵共有 | 該当なし |
| 共通鍵暗号 | 64ビットブロック暗号 (注14) | 3-key Triple DES (注15) |
| | 128ビットブロック暗号 | 該当なし |
| | ストリーム暗号 | 該当なし |
| ハッシュ関数 | | RIPEMD-160 |
| | | SHA-1 |
| 暗号利用モード | 秘匿モード | 該当なし |
| | 認証付き秘匿モード (注16) | 該当なし |
| メッセージ認証コード | | CBC-MAC (注17) |
| 認証暗号 | | 該当なし |
| エンティティ認証 | | 該当なし |

（注13）TLS 1.0, 1.1, 1.2で利用実績があることから当面の利用を認める。

（注14）CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、$2^{20}$ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、$2^{21}$ブロックまでとする。

（注15）SP 800-67 Revision 2では廃止されているが、本リスト掲載時から安全性・利用実績の状況に大きな変化がないため、掲載を継続する。

（注16）CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

（注17）安全性の観点から、メッセージ長を固定して利用すべきである。

7 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

8 既に稼働中のシステムやアプリケーション等との間での相互運用を継続すること

9 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

# 更新履歴情報

| 更新日付 | 更新箇所 | 更新前の記述 | 更新後の記述 |
|---|---|---|---|
| 令和６年<br>５月16日 | 注 | ［新規追加］ | （注18）FIPS PUB 186-5では廃止されているが、本リスト掲載時から安全性・利用実績の状況に大きな変化がないため、掲載を継続する。 |
| | 注 | ［新規追加］ | （注19）SP 800-67 Revision 2では廃止されているが、本リスト掲載時から安全性・利用実績の状況に大きな変化がないため、掲載を継続する。 |
| 令和８年<br>３月30日 | 電子政府推奨暗号リスト（本文） | 暗号技術検討会及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術について、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。 | 暗号技術検討会及び関連委員会（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。 |
| | 電子政府推奨暗号リスト（表） | ［表の件名付与］ | ＜表１　現行暗号リスト＞ |
| | 電子政府推奨暗号リスト（表） | ［表の新設］ | ＜表２　耐量子計算機暗号（PQC）リスト＞<br>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。 |
| | 電子政府推奨暗号リスト（耐量子計算機暗号（PQC）リスト） | ［技術分類の追加］ | 技術分類：公開鍵暗号－署名<br>名称／パラメーターセット：－<br>技術分類：公開鍵暗号－鍵共有<br>名称：ML-KEM<br>パラメーターセット：<br>ML-KEM-768（Category 3）<br>ML-KEM-1024（Category 5） |
| | 電子政府推奨暗号リスト（耐量子計算機暗号（PQC）リスト） | ［技術分類の追加］ | 技術分類：共通鍵暗号<br>名称：AES<br>パラメーターセット：<br>AES-192（Category 3）<br>AES-256（Category 5） |
| | 電子政府推奨暗号リスト（耐量子計算機暗号（PQC）リスト） | ［技術分類の追加］ | 技術分類：ハッシュ関数<br>名称：SHA2<br>パラメーターセット：<br>SHA-384（Category 4）<br>SHA-512<br>名称：SHA3<br>パラメーターセット：<br>SHA3-384（Category 4）<br>SHA3-512 |
| | 脚注 | ５　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 | 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<br>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。 |
| | 脚注 | ［新規追加］ | 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。<br>https://www.cryptrec.go.jp/report/cryptrec-mt-1501-2026.pdf |
| | 脚注 | 脚注３、４、７、８ | 脚注５、７、８、９ |
| | 注 | （注１）「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」（平成20年４月情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。<br>https://www.nisc.go.jp/pdf/policy/general/angou_ikoushishin.pdf<br>（平成25年３月１日現在） | ［削除］ |

| | | | |
|---|---|---|---|
| | 注 | （注８）「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」（平成20年４月情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。<br>https://www.nisc.go.jp/pdf/policy/general/angou_ikoushishin.pdf<br>（平成25年３月１日現在） | ［削除］ |
| | 注 | ［新規追加］ | （注２）使用するMACはHMACまたはCMACに限る。 |
| | 注 | ［新規追加］ | （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。<br>・Category 1　128ビット鍵を持つブロック暗号に対する鍵探索<br>・Category 2　256ビットのハッシュ関数に対する衝突探索<br>・Category 3　192ビット鍵を持つブロック暗号に対する鍵探索<br>・Category 4　384ビットのハッシュ関数に対する衝突探索<br>・Category 5　256ビット鍵を持つブロック暗号に対する鍵探索<br>https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf<br>（令和８年３月25日現在） |
| | 注 | 注18、２、12、17、13、４、５～７、14、９、15、19、11 | 注１、３、４、５、６、７、９～11、12、13、14、15、17 |