

耐量子計算機暗号（PQC）リスト検討タスクフォース （第 2 回）

令和 8 年 8 月 31 日（月） 14:00～16:00
総務省 8 階 第 1 特別会議室
（ハイブリッド開催）

<議事次第>

1. 開会
2. 議事
 - (1) Security LevelとSecurity Categoryの使い分けについて
 - (2) 課題① Category 1・2の暗号等の取扱いについて
 - (3) 課題② 暗号利用モードや認証暗号等の取扱いについて
 - (4) 課題③ ハイブリッド構成の取扱いについて
 - (5) 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 | NISTから公表されているPQC関連資料内でのSecurity LevelとSecurity Categoryの使い分けについての報告 |
| 資料 3 | 課題① Category 1・2の暗号等の取扱い（第 1 回会合議論反映版） |
| 資料 4－1 | 課題② 暗号利用モードや認証暗号等の取扱い【前回会合と同様】 |
| 資料 4－2 | 課題② 諸外国動向調査 |
| 資料 5 | 課題③ ハイブリッド構成の取扱い【前回会合と同様】 |
| 資料 6 | その他検討すべき事項【前回会合と同様】 |
| 参考資料 1 | 「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 |
| 参考資料 2 | CRYPTREC暗号リストのPQC対応と検討課題 |
| 参考資料 3 | 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

NISTから公表されているPQC関連資料内での Security LevelとSecurity Categoryの使い分け についての報告

NICT

■背景：2026年度第1回PQC WGにおける相談事項

- PQCアルゴリズムの強度を表現するのにPQCガイドラインではレベル(Level)が用いられ、暗号リストではカテゴリ(Category)が用いられているため統一すべきか

■PQC WGでの議論の要旨

- Categoryという単語を使っているが、AESやSHAを入れることに違和感がある
- NISTのスタッフはLevelとCategoryを使い分けているらしい
- この場ではまとまらないため、事務局からNISTに問い合わせる

■事務局からNISTへの質問内容

- NISTのドキュメントではLevelとCategoryはどのように使い分けられているのか
- 使い分けや用語の定義に関して、参照先はどこをとれば良いのか

■NISTからの回答（抜粋）

- “security level” is an informal term
- The terms we try to use more regularly are "security strength" and "security category."
- If you need to refer to a document for these definitions, I think SP 800-57 part 1 revision 6 is a good one.

課題①

Category 1・2の暗号等の取扱い (第1回会合議論反映版)

検討ポイント① セキュリティカテゴリーの記載方法

- セキュリティカテゴリーは、暗号技術のセキュリティ水準を利用者が把握する上で参考となり、暗号技術を選択する上でも重要な要素であり、表 2 に記載することとしたが、その書き方や定義について修正すべき点はないか。

【考え方】

- ✓「パラメーターセット（セキュリティカテゴリー）」という書き方の場合、そもそも表示が見にくく、また、同一のパラメーターセットについて異なるセキュリティカテゴリーの設定が存在すると誤解を招く可能性があることから、**現行の書き方を改めて列を区切り**、「パラメーターセット」と「セキュリティカテゴリー」とで別の列とすることが適当。
 - ✓**カテゴリーの定義**については、米国NISTが2016年12月に公表したPQC標準化公募の際に示し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おり、**現行の記載内容は適当**。
- 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を、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を基準として定義されている。
 - また、例えばCategory 1では、128ビット鍵のブロック暗号に対する鍵探索に必要な計算資源を基準としており、当該ブロック暗号の例としてAES-128が明記されている。

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

変更

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

(注8) セキュリティのカテゴリーを合わせて記載する。各セキュリティカテゴリーはNISTの“Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”に従い、次のように、セキュリティカテゴリー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

(参考) セキュリティカテゴリーの定義 (米国NIST 2016年)

3

レイアウトのみ変更

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):

- 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)
- 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)
- 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)
- 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)
- 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)

【仮訳 (機械翻訳ベース)】

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ーを定義します。

- 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) 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) 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) 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) 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。

NIST SP 800-57 Rev. 6 (Initial Public Draft) (2025.12) "Recommendation for Key Management: Part 1 – General"

<https://csrc.nist.gov/pubs/sp/800/57/pt1/r6/ipd>

4.6.1. Cryptographic Algorithm Security Strengths (抜粋)

Cryptographic algorithms can provide different security strengths, depending on the algorithm and key size used (whenever keys are required by the algorithm). In previous versions of this document, the estimated (classical) **security strength** (s) that an algorithm or system could provide is defined in terms of the **amount of work** (i.e., the number of operations) that is required to break the algorithm or system (i.e., the amount of work to break the algorithm requires 2^s operations of some kind, where $s = 112, 128, 192$, or 256 bits). However, cryptanalytic advances (e.g., in factoring algorithms, general discrete-logarithm attacks, and elliptic-curve discrete-logarithm attacks) and the potential advent of quantum computing have brought into question the use of a single number to represent the security afforded by designating the same security strength for different algorithm types. In 2016, a NIST call for the submission of post-quantum algorithms categorized security strength in terms of the computational resources needed by an attacker to break a block cipher algorithm or hash function, essentially considering both classical and quantum computers. Listed in order of increasing strength, these **security categories** are:

1. Secure against an attacker that is presumed to lack the resources needed for a **key search of a block cipher algorithm with a 128-bit key** (e.g., AES-128).
2. Secure against an attacker that is presumed to lack the resources needed for a **collision search on a 256-bit hash function** (e.g., SHA-256, SHA3-256).
3. Secure against an attacker that is presumed to lack the resources needed for a **key search of a block cipher algorithm with a 192-bit key** (e.g., AES-192).
4. Secure against an attacker that is presumed to lack the resources needed for a **collision search on a 384-bit hash function** (e.g., SHA-384, SHA3-384).
5. Secure against an attacker that is presumed to lack the resources needed for a **key search of a block cipher algorithm with a 256-bit key** (e.g., AES-256).

Table 2. Security strength categories for post-quantum algorithms

Security Category	Minimum Attack Cost	Example
1	Same as key search on a block cipher with a 128-bit key	AES-128
2	Same as collision search on a 256-bit hash function	SHA-256
3	Same as key search on a block cipher with a 192-bit key	AES-192
4	Same as collision search on a 384-bit hash function	SHA3-384
5	Same as key search on a block cipher with a 256-bit key	AES-256

2025年の文書に差し替え

[仮訳 (機械翻訳ベース)]

4.6.1. 暗号アルゴリズムのセキュリティ強度 (抜粋)

暗号アルゴリズムは、使用するアルゴリズムや鍵のサイズ (アルゴリズムが鍵を必要とする場合) に応じて、異なるセキュリティ強度を提供し得ます。本文書の以前の版では、アルゴリズムやシステムが提供し得る推定 (古典的) **セキュリティ強度** (s) は、そのアルゴリズムやシステムを破るために**必要な作業量** (すなわち演算回数) に基づいて定義されていました (具体的には、アルゴリズムを破るための作業量が何らかの種類の演算で 2^s 回必要となる場合、 $s = 112, 128, 192$, または 256 ビットと定義)。しかし、暗号解読技術の進歩 (例: 素因数分解アルゴリズム、一般的な離散対数問題への攻撃、楕円曲線離散対数問題への攻撃) や量子コンピューティングの登場の可能性により、異なる種類のアルゴリズムに対して同一のセキュリティ強度を割り当て、単一の数値でそのセキュリティを表すことの妥当性が疑問視されるようになりました。2016年、NISTは耐量子計算機暗号 (PQC) アルゴリズムの公募において、ブロック暗号アルゴリズムやハッシュ関数を破るために攻撃者が必要とする計算リソースの観点からセキュリティ強度を分類しました。この分類では、古典的コンピュータと量子コンピュータの双方が考慮されています。強度の低い順に、これらの**セキュリティカテゴリー**を以下に示します。

1. **128ビット鍵のブロック暗号アルゴリズム** (例: AES-128) に対する**鍵探索**に必要なリソースを持たないと想定される攻撃者に対して安全である。
2. **256ビットのハッシュ関数** (例: SHA-256、SHA3-256) に対する**衝突探索**に必要なリソースを持たないと想定される攻撃者に対して安全である。
3. **192ビット鍵のブロック暗号アルゴリズム** (例: AES-192) に対する**鍵探索**に必要なリソースを持たないと想定される攻撃者に対して安全である。
4. **384ビットのハッシュ関数** (例: SHA-384、SHA3-384) に対する**衝突探索**に必要なリソースを持たないと想定される攻撃者に対して安全である。
5. **256ビット鍵のブロック暗号アルゴリズム** (例: AES-256) に対する**鍵探索**に必要なリソースを持たないと想定される攻撃者に対して安全である。

表2. 耐量子アルゴリズムのセキュリティ強度区分

セキュリティカテゴリー	最小攻撃コスト	例
1	128ビット鍵のブロック暗号における鍵探索と同じ	AES-128
2	256ビットハッシュ関数における衝突探索と同じ	SHA-256
3	192ビット鍵のブロック暗号における鍵探索と同じ	AES-192
4	384ビットハッシュ関数における衝突探索と同じ	SHA3-384
5	256ビット鍵のブロック暗号における鍵探索と同じ	AES-256

NIST SP 800-57 Rev. 6 (Initial Public Draft) (2025.12) "Recommendation for Key Management: Part 1 – General"

<https://csrc.nist.gov/pubs/sp/800/57/pt1/r6/ipd>

Appendix E. Glossary (抜粋)

security categories

The evaluation criteria for the security strength of an algorithm in terms of the computational resources needed to break block cipher algorithms or hash functions.

security strength

A number associated with the amount of work (i.e., the number of operations) that is required to break a cryptographic algorithm or system. In this recommendation, the security strength is specified in bits and is a specific value from the set {112, 128, 192, 256}. Also called "bits of security."

【仮訳（機械翻訳ベース）】

付録E. 用語集（抜粋）

セキュリティカテゴリー (security categories)

ブロック暗号アルゴリズムやハッシュ関数を解読するために必要な計算資源の観点から、アルゴリズムのセキュリティ強度を評価するための基準。

セキュリティ強度 (security strength)

暗号アルゴリズムやシステムを解読するために必要な作業量（すなわち、演算回数）に関連付けられた数値。本勧告において、セキュリティ強度はビット単位で指定され、{112, 128, 192, 256} の集合から選ばれる特定の値である。「セキュリティビット数 (bits of security)」とも呼ばれる。

検討ポイント② 512ビットハッシュ関数の取扱い

- **512ビットのハッシュ関数**（SHA-512及びSHA3-512）のセキュリティカテゴリーの記載は保留（空欄）としていくところ、何を記載すべきか。

【考え方】

- ✓ セキュリティカテゴリーが空欄であると利用者の混乱を招くため、**何らかのカテゴリーを記載することが適当。**
- ✓ ハッシュ関数に対する衝突探索を基準とするカテゴリーのうち最も高い「**Category 4**」とすることが適当。
- ✓ 「Category 4」は384ビットハッシュ関数に対する衝突探索を基準としているため、512ビットハッシュ関数はこれを上回る計算資源が必要となること（よりセキュアであること）が伝わるようにすることが適当。
- ✓ 具体的には、「**Category 4**」に**注釈を付し**、512ビットハッシュ関数に対する衝突探索には、**384ビットハッシュ関数に対する衝突探索よりも大きな計算資源が必要となる旨**を明記することが適当。

※「Category 4以上」や「Category 4+」等の表記も考えられるが、NISTに定義のない新たな表記となり、Category 5との関係も不明確となることから、採用しないことが適当。

＜確認事項＞

注9の文言についてよりよい案はあるか。

例：（注9）512ビットのハッシュ関数に対する衝突探索には、384ビットのハッシュ関数に対する衝突探索よりも大きな計算資源が必要となるため、ハッシュ関数の衝突探索を基準とする最上位のCategory 4として記載する。

＜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	セキュリティカテゴリー(注8)
公開鍵暗号	署名	—	—	—
	鍵共有	ML-KEM	ML-KEM-768 ML-KEM-1024	Category 3 Category 5
共通鍵暗号		AES	AES-192 AES-256	Category 3 Category 5
ハッシュ関数		SHA2	SHA-384 SHA-512	Category 4 Category 4 (注9)
		SHA3	SHA3-384 SHA3-512	Category 4 Category 4 (注9)

（注8）セキュリティのカテゴリーを合わせて記載する。各セキュリティカテゴリーはNISTの“Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”に従い、次のように、セキュリティカテゴリー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）

（注9）512ビットのハッシュ関数に対する衝突探索の計算資源が攻撃に必要であり、Category 4に属する。

検討ポイント③ Category 1・2の取扱い

- **Category 1・2**（128ビットセキュリティ程度相当）の**暗号技術**（公開鍵暗号、ブロック暗号、ハッシュ関数）について、表2に掲載することが適当か。

【考え方】

- ✓ 表2は、PQC移行後も**長期的に利用していく暗号技術を示すリスト**としての性格を有することから、**Category 1・2の暗号技術を積極的に掲載することは適当でない**。

- 量子コンピュータ技術の進展状況等を踏まえ、表1については、暗号技術検討会が危殆化したと決定した場合は、電子政府推奨暗号から外れ、表2のみが電子政府推奨暗号として残ることが想定される。そのため、2035年以降も利用予定のシステムについては、表1ではなく表2を参照して整備することになると考えられる。
- 「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」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。

- ✓ **公開鍵暗号**のうち**ML-KEM**については、**Category 3・5の実装が広く見られ、Category 1でなければPQC移行できない具体的な支障も現時点では確認されていないことから、ML-KEM-512（Category 1）は表2に掲載しないことが適当**。

- ✓ **公開鍵暗号**のうち**署名方式**については、**ML-DISA-44（Category 2）が広く利用される可能性もあることから、ML-DISA・SLH-DISAのCategory 1・2については、実利用・標準化動向を確認した上で掲載要否を判断することが適当**。 **<今後議論>**

- ✓ **Category 1・2を掲載する場合**には、「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取り扱う用途ではこれを強く推奨する。」と**注釈を付すことが適当**。

- ✓ **ブロック暗号及びハッシュ関数**については、Category 1・2の暗号技術は、当面は**現行暗号リスト（表1）に基づき引き続き利用可能**であり、PQC移行後の利用を想定する表2に追加する必要性も乏しい※ことから、**表2に掲載しないことが適当**。

※表2はそもそも量子コンピュータ（CRQC）への耐性を有する暗号技術を掲載するものであるが、例えばAES-128は量子コンピュータの進展によりGroverのアルゴリズムを適用できれば64ビット全数探索で解読できてしまうことから、表2にブロック暗号及びハッシュ関数のCategory 1・2を掲載することは適当ではない。

- ✓ Category 1・2については、当面の間、調達や相互運用性の観点からフォローが必要。

<参考：関係する暗号技術の例>

技術分類	暗号技術		
	名称	パラメータセット	セキュリティ カテゴリー(注8)
公開鍵暗号	署名	ML-DISA	ML-DISA-44(注) ML-DISA-65 ML-DISA-87 Category 2 Category 3 Category 5
		SLH-DISA	SLH-DISA-SHA2-128[s/f] (注) SLH-DISA-SHAKE-128[s/f] (注) SLH-DISA-SHA2-192[s/f] SLH-DISA-SHAKE-192[s/f] SLH-DISA-SHA2-256[s/f] SLH-DISA-SHAKE-256[s/f] Category 1 Category 1 Category 3 Category 3 Category 5 Category 5
	鍵共有	ML-KEM	ML-KEM-512 ML-KEM-768 ML-KEM-1024 Category 1 Category 3 Category 5
	共通鍵暗号	AES	AES-128 AES-192 AES-256 Category 1 Category 3 Category 5
	ハッシュ関数	SHA2	SHA-256 SHA-512/256 SHA-384 SHA-512 Category 2 Category 2 Category 4 Category 4 (注9)
		SHA3	SHA3-256 SHA3-384 SHA3-512 Category 2 Category 4 Category 4 (注9)

※Camellia、KCipher-2、SHAKEは記載していない。

(参考) カテゴリー関連記載：海外政府機関による推奨状況① 8

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

参考 ドイツ (BSI) : “Technical Guideline TR-02102-1 Cryptographic Mechanisms: Recommendations and Key Lengths”

* 2030年以降は非推奨

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”

※英国 (NCSC) : “Next steps in preparing for post-quantum cryptography” では、ML-KEM及びML-DSAについて、全パラメータセットを一般用途等で許容可能としている一方、多くの用途ではML-KEM-768及びML-DSA-65を推奨。

※米国 (NSA) : “Commercial National Security Algorithm Suite 2.0”では、国家安全保障システム向けに、ML-KEM-1024及びML-DSA-87を採用している。

ドイツ 情報セキュリティ庁 (BSI)

“Technical Guideline TR-02102-1 Cryptographic Mechanisms: Recommendations and Key Lengths” (2026.1)

<https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.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 [110] 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/documents/2024/12/3/the-pqc-migration-handbook>

4.2) Recommended Cryptographic Primitives (抜粋)

Primitive	Recommended	Acceptable
ML-KEM ¹	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) SLH-DSA-(SHA2/SHAKE)-192(s/f)	SLH-DSA-(SHA2/SHAKE)-128(s/f)
AES	AES-256	AES-128
SHA-3	SHA-3-256 SHA-3-384 SHA-3-512 (c)SHAKE256	SHA-3-224 (c)SHAKE128
SHA-2	SHA-256 SHA-384 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.

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	η_1	η_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
ζ - a 512th root of unity in $\mathbb{Z}_q$ [see §7.5]	1753	1753	1753
d - # of dropped bits from t [see §6.1]	13	13	13
τ - # of ± 1 's in polynomial c [see §6.2]	39	49	60
λ - collision strength of $\tilde{c}$ [see §6.2]	128	192	256
γ_1 - coefficient range of y [see §6.2]	2^{17}	2^{19}	2^{19}
γ_2 - low-order rounding range [see §6.2]	$(q-1)/88$	$(q-1)/32$	$(q-1)/32$
(k, ℓ) - dimensions of $\mathbf{A}$ [see §6.1]	(4,4)	(6,5)	(8,7)
η - private key range [see §6.1]	2	4	2
$\beta = \tau \cdot \eta$ [see §6.2]	78	196	120
ω - max # of 1's in the hint 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	16	63	7	9	12	14	4	30	1	32	7 856
SLH-DSA-SHAKE-128s	16	66	22	3	6	33	4	34	1	32	17 088
SLH-DSA-SHA2-128f	16	66	22	3	6	33	4	34	1	32	17 088
SLH-DSA-SHAKE-128f	16	66	22	3	6	33	4	34	1	32	17 088
SLH-DSA-SHA2-192s	24	63	7	9	14	17	4	39	3	48	16 224
SLH-DSA-SHAKE-192s	24	66	22	3	8	33	4	42	3	48	35 664
SLH-DSA-SHA2-192f	24	66	22	3	8	33	4	42	3	48	35 664
SLH-DSA-SHAKE-192f	24	66	22	3	8	33	4	42	3	48	35 664
SLH-DSA-SHA2-256s	32	64	8	8	14	22	4	47	5	64	29 792
SLH-DSA-SHAKE-256s	32	64	8	8	14	22	4	47	5	64	29 792
SLH-DSA-SHA2-256f	32	68	17	4	9	35	4	49	5	64	49 856
SLH-DSA-SHAKE-256f	32	68	17	4	9	35	4	49	5	64	49 856

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 耐性があるとは言えず、「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	-			
SHA-512/256	-	256	$2^{85.3}$	$2^{85.3}$
SHA3-256	512			
SHA-384	-			
SHA3-384	768	384	2^{128}	2^{128}
SHA-512	-			
SHA3-512	1024	512	$2^{170.7}$	$2^{170.7}$
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) ML-KEM-768 (Category 3) ML-KEM-1024 (Category 5)
共通鍵暗号	ブロック暗号	AES	AES-128 (Category 1) AES-192 (Category 3) AES-256 (Category 5)
		Camellia	Camellia-128 (Category 1) Camellia-192 (Category 3) 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) SHA-512/256 (Category 2) SHA-384 (Category 4) SHA-512 (Category 4)
		SHA3	SHA3-256 (Category 2) SHA3-384 (Category 4) SHA3-512 (Category 4)
		SHAKE	SHAKE128 (Category 2) 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

課題②

諸外国動向調査

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及びエンティティ認証について、岩田委員への回答

NICT

暗号利用モード

国・機関	CBC	CFB	OFB	CTR	XTS	引用箇所
米国 NSA	—	—	—	—	—	[US] p.15
英国 NCSC	—	—	—	—	—	[UK] p.2
カナダ Cyber Centre	Recommended	Recommended	Recommended	Recommended	Recommended	[CA] p.11-12
オーストラリア ASD	AES-CBC (IPsec/IKEv2)	—	—	AES-CTR (IPsec/IKEv2)	—	[AU] Web
ニュージーランド NCSC/GCSB	CBC、CFB、OFB、CTRを「other modes」として記載				—	[NZ] §17.2.28, p.309
フランス ANSSI	—	—	—	—	—	[FR] p.2
ドイツ BSI	Recommended	—	—	Recommended	—	[DE] p.42
オランダ AIVD/NCSC/TNO	—	—	—	Recommended (AES-CTR)	—	[NL] p.57
スペイン CCN	—	—	—	—	—	[ES] p.20
チェコ NÚKIB	Approved※	Approved※	Approved※	Approved※	Approved (disk encryption)	[CZ] p.5
スロバキア NBÚ	—	—	—	—	—	[SK] p.4
フィンランド Traficom	—	—	—	—	—	[FI] p.3
ノルウェー NSM	—	—	—	—	Default: 256 bit / Alternate: 128 bit	[NO] p.15
サウジアラビア NCA	Accepted	Accepted	Accepted	Accepted	Accepted (data at rest only)	[SA] p.16
マレーシア CyberSecurity Malaysia	—	—	—	—	Approved (XTS-AES 128/256)	[MY] Web

※チェコのCBC、CFB、OFB、CTRはEncrypt-then-MAC構成で使用されます。また、承認された共通鍵暗号モードについて、使用する共通鍵暗号及びハッシュ関数がquantum-resistantである場合に当該モードもquantum-resistantとしている。[CZ] p.5

メッセージ認証コード (MAC) など

国・機関	HMAC	CMAC	GMAC	KMAC	Poly1305	引用箇所
米国 NSA	—	—	—	—	—	[US] p.15
英国 NCSC	—	—	—	—	—	[UK] p.2
カナダ Cyber Centre	Recommended	Recommended (AES)	Recommended (AES)	Recommended (KMAC128/256)	—	[CA] p.21
オーストラリア ASD	HMAC-SHA256/384/512 (IPsec)	—	—	—	—	[AU] Web
ニュージーランド NCSC/GCSB	SHOULD use HMAC-SHA256 / HMAC-SHA384 / HMAC-SHA512	—	—	—	—	[NZ] §17.8.14, p.318
フランス ANSSI	—	—	—	—	—	[FR] p.2
ドイツ BSI	Recommended	Recommended	Recommended	Recommended (KMAC128/256)	—	[DE] p.49-50
オランダ AIVD/NCSC/TNO	Recommended (HMAC-SHA-2)	Recommended (CMAC-AES)	—	Recommended	—	[NL] pp.57, 94-95
スペイン CCN	—	—	—	—	—	[ES] p.20
チェコ NÚKIB	Approved	Approved	Approved	Approved	—	[CZ] p.5
スロバキア NBÚ	—	—	—	—	—	[SK] p.4
フィンランド Traficom	SHA-256 / SHA-384 / SHA-512	—	—	KMAC-128/128、KMAC-256/192、KMAC-256/256	—	[FI] p.3
ノルウェー NSM	Default	—	—	Alternate	—	[NO] p.16
サウジアラビア NCA	Accepted	Accepted	Accepted	Accepted	—	[SA] p.17
マレーシア CyberSecurity Malaysia	Approved	Approved	Approved	Approved	Approved	[MY] Web

認証付き秘匿モード、認証暗号など

国・機関	CCM	EAX	OCB1 / OCB3	GCM	GCM-SIV	ChaCha20-Poly1305	Encrypt-then-MAC	引用箇所
米国 NSA	—	—	—	—	—	—	—	[US] p.15
英国 NCSC	—	—	—	—	—	—	—	[UK] p.2
カナダ Cyber Centre	Recommended	—	—	Recommended	—	—	—	[CA] p.13
オーストラリア ASD	AES-CCM (IKEv2)	—	—	AES-GCM (IPsec/IKEv2)	—	—	—	[AU] Web
ニュージーランド NCSC/GCSB	—	—	—	—※	—	—	—	[NZ] §17.2, pp.3-4
フランス ANSSI	—	—	—	—	—	—	—	[FR] p.2
ドイツ BSI	Recommended	—	—	Recommended	Recommended (AES-GCM-SIV)	—	—	[DE] p.41
オランダ AIVD/NCSC/TNO	—	—	Recommended (AES-OCB)	Recommended	Recommended	Recommended	—	[NL] p.57
スペイン CCN	—	—	—	—	—	—	—	[ES] p.20
チェコ NÚKIB	Approved※	Approved※	Approved※	Approved※※	—	Approved※	Approved※	[CZ] p.4
スロバキア NBÚ	—	—	—	—	—	—	—	[SK] p.4
フィンランド Traficom	—	—	—	—	—	—	—	[FI] p.3
ノルウェー NSM	—	—	—	Default: AES-GCM-256 Alternate: AES-GCM-128	Alternate	Alternate	—	[NO] p.13
サウジアラビア NCA	Accepted	—	—	Accepted	—	—	—	[SA] p.16
マレーシア CyberSecurity Malaysia	Approved (AES-CCM 128/192/256)	—	—	Approved (AES-GCM 128/192/256)	Approved (AES-GCM-SIV 128/256)	Approved	—	[MY] Web

※ニュージーランドは参考文献としてRFC 5288およびNIST SP 800-38Dを掲載しているが、§17.2ではGCMそのものを Approved、Recommended、quantum-resistant とする記述はない。

※※ チェコはCCM、EAX、OCB1 / OCB3、GCM、ChaCha20+Poly1305、Encrypt-then-MACを記載しており、GCMについてはIV 96 bit、tag 128 bitを指定している。[CZ] p.4

Camellia、KCipher-2、SHAKE128、SHAKE256

国・機関	Camellia	KCipher-2	SHAKE128	SHAKE256	引用箇所
米国 NSA	—	—	General-purposeでは Approvedでない	General-purposeでは Approvedでない	[US] p.8
英国 NCSC	—	—	—	—	[UK] p.2
カナダ Cyber Centre	—	—	指定用途で利用	指定用途で利用	[CA] p.20
オーストラリア ASD	—	—	—	—	[AU] Web
ニュージーランド NCSC/GCSB	—	—	—	—	[NZ] §17.2.10– 11, pp.1–2
フランス ANSSI	—	—	—	—	[FR] p.2
ドイツ BSI	—	—	—	—	[DE] p.37
オランダ AIVD/NCSC/TNO	Acceptable	—	Acceptable	Recommended	[NL] pp.57–58
スペイン CCN	—	—	—	—	[ES] p.20
チェコ NÚKIB	128/192 bit: quantum- vulnerable / 256 bit: quantum-resistant	—	Approved※	Approved※	[CZ] pp.4, 9
スロバキア NBÚ	Camellia-256	—	—	SHAKE256※※	[SK] pp.4, 7
フィンランド Traficom	—	—	SHAKE-128/128、 SHAKE-128/256	SHAKE-256/192、/256、/384、 /512	[FI] p.3
ノルウェー NSM	—	—	—	—	[NO] —
サウジアラビア NCA	128/192 bit: MODERATE / 256 bit: ADVANCED	—	MODERATE、 output ≥256 bit	ADVANCED、 output ≥512 bit	[SA] pp.12–13
マレーシア CyberSecurity Malaysia	Approved (128/192/256 bit)	Approved (128 bit)	—	—	[MY] Web

※ チェコではSHAKE128及びSHAKE256を承認ハッシュ関数として記載し、承認ハッシュ関数一般について、出力長384 bit以上をquantum-resistant、256 bit以下をquantum-vulnerableとしている。[CZ] p.9

※※ スロバキアではSHAKE256を記載し、出力長384 bit以上のハッシュ関数をquantum-resistantとしている。[SK] p.7

エンティティ認証

- ISO/IEC 9798-2/-3/-4のようなエンティティ認証プロトコルそのものを「CRQC-resistant」「quantum-resistant」「quantum-safe」と判定した、ないしは記述した諸外国の資料は確認できなかった。

参考文献

- [US] 米国 NSA, Commercial National Security Algorithm Suite 2.0 FAQ, Version 2.1 https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF
- [CA] カナダ Cyber Centre, Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information (ITSP.40.111) <https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111>
- [FR] フランス ANSSI, Follow-up position paper on post-quantum cryptography <https://messervices.cyber.gouv.fr/guides/en-follow-position-paper-post-quantum-cryptography>
- [DE] ドイツ BSI, BSI TR-02102-1, Cryptographic Mechanisms: Recommendations and Key Lengths <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.htm>
- [NL] オランダ AIVD/NCSC, The PQC Migration Handbook <https://english.aivd.nl/documents/2024/12/3/the-pqc-migration-handbook>
- [ES] スペイン CCN, CCN-TEC 009, Recomendaciones de transición postcuántica Segura <https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/boletines-pytec/495-ccn-tec-009-recomendaciones-transicion-postcuantica-segura/file>
- [CZ] チェコ NÚKIB, Doporučení v oblasti kryptografických prostředků, v4.1, 2026-03-04 https://portal.nukib.gov.cz/storage/uploads/2026/03/04/doporuceni-kryptograficka-bezpecnost-v4-1_uid_69a8216e3deb1.pdf
- [SK] スロバキア NBÚ, Cryptographic recommendations / national guidance, v1.0 <https://www.nbu.gov.sk/data/att/3483.pdf>
- [FI] フィンランド Traficom, Kryptografiset vahvuusvaatimukset – kansalliset turvallisuuksluokat, 2024-12-09 https://www.kyberturvallisuuskeskus.fi/files/media/file/Kryptografiset_vahvuusvaatimukset_-_kansalliset_turvallisuuksluokat_1.pdf
- [NO] ノルウェー NSM, NSM Cryptographic Recommendations 2025 <https://nsm.no/getfile.php/1314334-1742808614/NSM/Filer/Dokumenter/Veiledere/NSM%20Cryptographic%20Recommendations%202025.pdf>
- [UK] 英国 NCSC, Next steps in preparing for post-quantum cryptography <https://www.ncsc.gov.uk/paper/next-steps-in-preparing-for-post-quantum-cryptography>
- [SA] サウジアラビア NCA, National Cryptographic Standards, NCS-2:2025 <https://istitlaa.ncc.gov.sa/en/security/nca/ncs/Documents/NCS-2-en.pdf>
- [MY] マレーシア CyberSecurity Malaysia, MySEAL 2.1 Approved Cryptographic Algorithms <https://mykripto.cybersecurity.my/index.php/services/myseal/myseal-category/aksa-myseal/aksa-myseal-approved>
- [AU] オーストラリア ASD, Information Security Manual, Guidelines for cryptography <https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cyber-security-guidelines/guidelines-for-cryptography>
- [NZ] ニュージーランド GCSB/NCSC, New Zealand Information Security Manual <https://nzism.gcsb.govt.nz/ism-document/pdf>

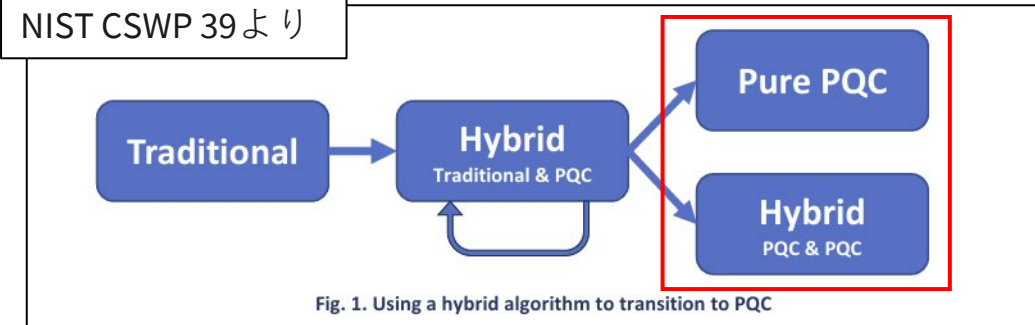
課題③

ハイブリッド構成の取扱い

「ハイブリッド」の位置付け

• NIST 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。



• 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。

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

$$\text{KeyCombine}(K_1, K_2, c_1, c_2, ek_1, ek_2, p) := H(K_1, K_2, c_1, c_2, ek_1, ek_2, \text{domain_sep}). \quad (15)$$

※ 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

目的 主体	後方互換性確保	安全性維持
アルゴリズム	なし	<u>鍵共有アルゴリズム</u> • NIST SP 800-227(4.6. Multi-Algorithm KEMs and PQ/T Hybrids) [4] • NIST SP 800-56C Rev. 2³ [9] • draft-irtf-cfrg-hybrid-kems-07 [10] • draft-ietf-lamps-pq-composite-kem-12 [11]⁴ <u>署名アルゴリズム</u> • draft-ietf-lamps-pq-composite-sigs-14 [12]⁴
	<u>通信プロトコル</u> • RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3 [13] ※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 <u>証明書構造</u> • draft-ietf-lamps-certdiscovery-02 [18] • ITU-T X.509(9.8 Alternative cryptographic algorithms and digital signature extensions) [19]	<u>通信プロトコル</u> • draft-ietf-tls-hybrid-design-16 [14] • draft-ietf-mls-combiner-02 [15] • ETSI TS 103 744 [16] • IEEE 802.11 Hybrid PQC Proposal [17] • draft-ietf-lamps-pq-composite-kem-12 [11]⁴ <u>証明書構造</u> • draft-ietf-lamps-pq-composite-sigs-14 [12]⁴
	(後方互換性確保/安全性維持 共通) • 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 Architecting PKI Hierarchies for Graceful PQ Migration(PQC Conference) [20] - 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

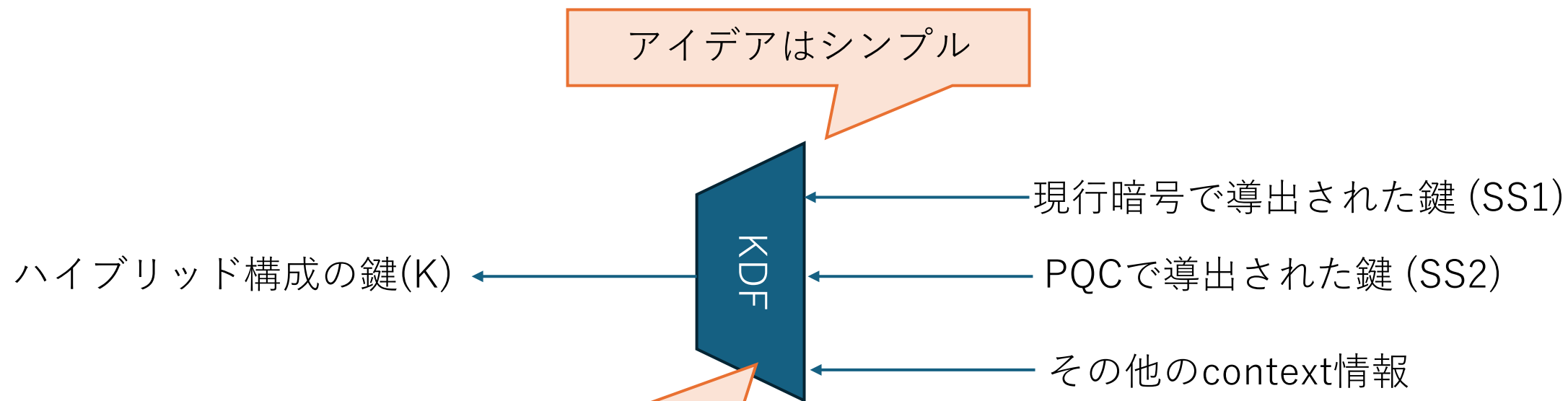
• 秘匿（KEM）用途

- 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みを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. $K = \text{KDF}(\text{SS1} || \text{SS2} || \text{context})$)

※ SP800-227, draft-ietf-lamps-pq-composite-kem, draft-ietf-tls-ecdhe-mlkem

なお、**Cascade方式も存在** (e.g. $K = \text{KDF2}(\text{KDF1}(\text{SS1}) || \text{SS2})$) ※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、**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	[RFC8892]
31	id-RSASSA-PSS-SHAKE256	[RFC8892]
32	id-ecdsa-with-shake128	[RFC8892]
33	id-ecdsa-with-shake256	[RFC8892]
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-MLDSA85-RSA3072-PSS-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
42	id-MLDSA85-RSA3072-PKCS15-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
43	id-MLDSA85-RSA4096-PSS-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
44	id-MLDSA85-RSA4096-PKCS15-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
45	id-MLDSA85-ECDSA-P256-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
46	id-MLDSA85-ECDSA-P384-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
47	id-MLDSA85-ECDSA-brainpoolP256r1-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
48	id-MLDSA85-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]

8

- **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)

- **实施例：**

- X25519MLKEM768 (右表内の4588)

$$\text{Derive-Secret}(\text{Secret}, \text{Label}, \text{Messages}) = \text{HKDF-Expand-Label}(\underline{\text{Secret}}, \text{Label}, \text{Transcript-Hash}(\text{Messages}), \text{Hash.length})$$

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

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]
30	x448	Y	Y	[RFC-ietf-tls-rfc8446bis-13]
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-conolly-tls-mkem-key]
513	MLKEM768	Y	N	[draft-conolly-tls-mkem-key]
514	MLKEM1024	Y	N	[draft-conolly-tls-mkem-key]
515-2569	Unassigned			
2570	Reserved	Y	N	[RFC8701]
2571-4586	Unassigned			
4587	SecP256r1MLKEM768	Y	N	[draft-ietf-tls-ecdhe-mkem-0]
4588	X25519MLKEM768	Y	N	[draft-ietf-tls-ecdhe-mkem-0]
4589	SecP384r1MLKEM1024	Y	N	[draft-ietf-tls-ecdhe-mkem-0]
4590	curveSM2MLKEM768	N	N	[draft-yang-tls-hybrid-sm2-m]
4591-0001	Unassigned			

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, $\emptyset$.

(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.

署名に関する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するが、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する議論は未成熟

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の問題ないか。
- 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

その他検討すべき事項

- 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】

- ✓「電子政府推奨暗号リスト」は本文において、「暗号技術」には次の注釈が記載されている。

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。

- ✓暗号利用モード、メッセージ認証コード、エンティティ認証を表 2 に掲載する場合、量子コンピュータへの耐性について、この注釈に明記（追記）する必要があるのではないか。

例 1：なお、表 2（耐量子計算機暗号（PQC）リスト）に掲載する場合には、表 2 に掲載された暗号技術と組み合わせて利用することを前提とする。

例 2：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。

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（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。）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（追加予定もないことから）、同様の注釈は不要か。

後段（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。）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のではないか。

✓ 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

4

- 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】

紫字部分についてはCategory 1・2の取扱いを踏まえた前回資料からの修正

✓ 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 $\leq 2^{k/2}$ 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128192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 $\leq 2^{128}$ 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。表2に掲載しないこととしてよいか。

✓ 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。
ハッシュ長は384ビット以上とする。

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) 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

(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		
暗号利用モード	秘匿モード	SHAKE256
		CBC
		CFB
		CTR
	認証付き秘匿モード	XTS
CCM		
メッセージ認証コード	GCM	
	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) ML-KEM-768 (Category 3) ML-KEM-1024 (Category 5)
共通鍵暗号	ブロック暗号	AES	AES-128 (Category 1) AES-192 (Category 3) AES-256 (Category 5)
		Camellia	Camellia-128 (Category 1) Camellia-192 (Category 3) 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) SHA-512/256 (Category 2) SHA-384 (Category 4) SHA-512 (Category 4 ?)
	SHA3	SHA3と SHAKEの 分離・統合【P】	SHA3-256 (Category 2) SHA3-384 (Category 4) SHA3-512 (Category 4 ?)
	SHAKE		SHAKE128 (Category 2) SHAKE256 (Category 2, 4 ?)
暗号利用モード	秘匿モード	CBC (Category 1, 3, 5)	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】
		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	

「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
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

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

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）。

<パラメーター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)

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。

(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	KCiper-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
			SHA3-384 (Category 4) SHA3-512
	SHA3		

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）

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

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	—	—
	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

（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 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 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> 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 名称／パラメーターセット：－ 技術分類：公開鍵暗号－鍵共有 名称：ML-KEM パラメーターセット： ML-KEM-768 (Category 3) 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 名称：AES パラメーターセット： AES-192 (Category 3) 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 名称：SHA2 パラメーターセット： SHA-384 (Category 4) SHA-512 名称：SHA3 パラメーターセット： SHA3-384 (Category 4) 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 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。 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。 https://www.nisc.go.jp/pdf/policy/general/angou_ikoushishin.pdf （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。 https://www.nisc.go.jp/pdf/policy/general/angou_ikoushishin.pdf (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。 ・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)
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