

改定イメージの考え方

検討ポイント① セキュリティカテゴリの記載方法

- セキュリティカテゴリは、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、その記載方法や定義は利用者にわかりやすいか。

【考え方】

- ✓「セキュリティカテゴリ」の記載方法について、各暗号技術とセキュリティカテゴリとの対応関係が明確となるよう、セキュリティカテゴリを別の列とするとともに、暗号技術ごとに行を点線で区切って対応関係を明確に記載することが適当。

※通常は「ML-KEM-768」と表記されるが、一般の行政職員にとっては、これが「ML-KEM-768 (Category 3)」と同じものであるのか判断が容易ではないと考える。
 (「Category 3」以外のML-KEM-768が存在するように見えるため。)

- ✓列名については、ML-KEMでは「ML-KEM-768」等がパラメータセットの名称として用いられている一方、AESやSHAでは同様の用語が用いられておらず、暗号技術によって用語の使われ方が異なる。このため、「名称」と「パラメータセット」を分けず、両者をまとめて「暗号技術」として記載することが適当。

- ✓カテゴリの定義については、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、2026年3月改訂の記載内容は適当。
 なお、列名の変更に伴う修正を実施。

技術分類		暗号技術	
		名称	パラメータセット (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		セキュリティカテゴリ (注2-1)
		署名	鍵共有	
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 (後述)
	SHA3		SHA3-384 SHA3-512	Category 4 (後述)

(注2-1) セキュリティカテゴリを合わせて記載する。各セキュリティカテゴリはNISTの“Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”に従い、次のように、セキュリティ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

(参考) セキュリティカテゴリの定義 (米国NIST 2016年)

- 米国NISTは、2016年のPQC標準化公募において、ブロック暗号に対する鍵探索又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、5段階のセキュリティカテゴリを定義。

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。

➤ 米国NISTは、2025年のSP 800-57 Rev. 6（初期公開草案）においても、2016年と同様のセキュリティカテゴリを示している。

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

【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**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	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

- 米国NISTは、セキュリティカテゴリを暗号アルゴリズムの解読に必要な計算資源に基づく評価基準として定義し、ビット数で表されるセキュリティ強度とは区別している。

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 (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の記載は保留（空欄）としているところ、利用者にとってわかりやすい記載方法は何か。

【考え方】

- ✓ セキュリティカテゴリ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。

<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		セキュリティカテゴリ ^(注2-1)
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	Category 3
			AES-256	Category 5
ハッシュ関数		SHA2	SHA-384	Category 4
			SHA-512	Category 4 ^(注2-4)
		SHA3	SHA3-384	Category 4
			SHA3-512	Category 4 ^(注2-4)

(注2-1) 各セキュリティカテゴリはNISTの“Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”に従い、次のように、セキュリティ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2-4) 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。

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**としての性格を有し、掲載後の削除には政府調達や相互運用性への影響等を考慮する必要があることから、**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**。（署名方式については検討ポイント④を参照）
- ✓ **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によるGroverのアルゴリズムにより、AES-192/256と比べ安全余裕が小さくなることから、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の暗号技術について、現時点で表2に掲載しないことは、将来的な掲載を否定するものではなく、今後の利用動向等を注視することが適当。

＜参考：関係する暗号技術の例＞

技術分類		暗号技術		セキュリティ カテゴリ
公開鍵暗号	署名	ML-DSA	(略)	(略)
		SLH-DSA	(略)	(略)
	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		AES	AES-128	Category 1
			AES-192	Category 3
			AES-256	Category 5
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	

※Camellia、KCipher-2、SHAKEについては後述。

検討ポイント④ 署名方式のCategory 1・2の取扱い

- **公開鍵暗号のうち署名方式（ML-DSA及びSLH-DSA）について、Category 1・2（128ビットセキュリティ程度相当）を表2に掲載することが適当か。**

【考え方】

- ✓ **ML-DSA-44**については、**証明書やDNSSEC等で広く利用**される可能性が高く、**表2に掲載することが適当**。

※米国CNSA 2.0ではML-DSAの使用は、ML-DSA-87に限定し、事前ハッシュ（HashML-DSA）の利用も認めていないが、CRYPTREC暗号リストとは目的や対象が異なるため、これらの制限を設ける必要はない。

- ✓ **SLH-DSAのCategory 1**については、現時点ではML-DSAと比べて利用が限定的であり、Category 1まで掲載対象を広げる必要性は乏しいことから、**表2に掲載しないことが適当**。

＜ML-DSA-44の掲載について＞

- ✓ Category 1・2の暗号技術の利用は最低限に留めるため、
- ・表2の説明文に「Category 3以上の利用を推奨する。」と追記することが適当
 - ・また、「**ML-DSA-44**」に対して**次の注釈を付すことが適当**。

（注2-2）可能な限りML-DSA-65又はML-DSA-87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。

- ✓ ML-DSA-44は、鍵生成に用いる**乱数生成器のセキュリティ強度によりセキュリティカテゴリが異なることから注釈を付し、その条件を明確化することが適当**。

※乱数生成器のセキュリティ強度に応じてCategory 1又はCategory 2となるが、①両カテゴリの実質的な安全性の差を単純に評価することは難しいこと、②可能な限りCategory 3以上の利用を推奨する方針であること、③政府情報システムの調達時に乱数生成器のセキュリティ強度まで把握することは困難であること等を踏まえ、192ビット以上のセキュリティ強度を必須とはせず、カテゴリが異なる条件を明確化することとした。

（注2-3）ML-DSA-44について、鍵生成に用いる乱数生成器のセキュリティ強度が192ビット以上の場合はCategory 2、128ビット以上192ビット未満の場合はCategory 1となる。

＜参考：関係する暗号技術の例＞

技術分類	暗号技術	セキュリティカテゴリ
公開鍵暗号	署名 ML-DSA	ML-DSA-44 (注2-2) Category 1 (注2-3) Category 2 (注2-3)
		ML-DSA-65 Category 3
		ML-DSA-87 Category 5
	署名 SLH-DSA	SLH-DSA-SHA2-128[s/f] Category 1
		SLH-DSA-SHAKE-128[s/f] Category 1
		SLH-DSA-SHA2-192[s/f] Category 3
		SLH-DSA-SHAKE-192[s/f] Category 3
		SLH-DSA-SHA2-256[s/f] Category 5
		SLH-DSA-SHAKE-256[s/f] Category 5
	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	AES	AES-128 Category 1
		AES-192 Category 3
		AES-256 Category 5
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

※Camellia、KCipher-2、SHAKEについては後述。

(参考) 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)
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)			Acceptable (注)	SLH-DSAの記載なし
	SLH-DSA-[SHA2/SHAKE]-192[s/f] (Category 3)	Recommended		Recommended	SLH-DSAの記載なし
	SLH-DSA-[SHA2/SHAKE]-256[s/f] (Category 5)	Recommended		Recommended	SLH-DSA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 4)	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	
	SHA3-512 (Category 4)	Recommended	encourage	Recommended	PQC内部使用のみ可
	SHAKE256 (Category 4)		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”

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

(注) SLH-DSAについて、ハッシュ関数の安全性のみに依拠する保守的な方式であることを理由に、セキュリティレベル1のパラメータセットもAcceptableとしている (Section 4.2.1、Table 4.2)。

※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。

(参考) 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-02102-1 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” (2026.9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**. 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.

Table 4.2 | Recommended parameter instantiations of the cryptographic primitives.

(参考) 米国CNSA2.0におけるML-DSAの規定状況

- 米国CNSA 2.0のFAQ（2024年）では、ML-DSAのパラメータはML-DSA-87に限定。
- また、ML-DSAの事前ハッシュ方式（HashML-DSA）は、通常のML-DSA-87等で代替可能であり、現時点で認めていない。

米国 国家安全保障局（NSA）

“The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ”（2024.12）

<https://www.nsa.gov/Press-Room/Digital-Media-Center/Document-Gallery/igtag/CNSA/>

Q: What is the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)?

A: CNSA 2.0 is the suite of QR algorithms approved for NSS use. The following table lists the algorithms and their functions, specifications, and parameters.

Table: Commercial National Security Algorithm Suite 2.0

Algorithm	(略)	Specification	Parameters
General Purpose Algorithms			
(略)	(略)	(略)	(略)
ML-DSA (previously CRYSTALS-Dilithium)	(略)	FIPS PUB 204	ML-DSA-87 for all classification levels.
(略)	(略)	(略)	(略)

Q: Is HashML-DSA, aka the pre-hash mode of ML-DSA, allowed in CNSA 2.0?

A: Not at the present time. HashML-DSA is a variant on ML-DSA in FIPS 204, which describes a method of compressing a message before signing while intentionally breaking interoperability with ML-DSA to prevent a vulnerability in the case of key reuse. Because HashML-DSA does not offer any functionality not already offered by the CNSA hash functions combined in a standard way with ML-DSA-87, and because standard ML-DSA-87 is expected to be widely supported, NSA anticipates there will be no need for HashML-DSA in NSS. Hence, at this time, HashML-DSA is not allowed. If at a later date protocol usage demands it, NSA will provide specific guidance on its limited usage at that time.

【仮訳（機械翻訳ベース）】

Q: CNSA 2.0とは何ですか？

A: CNSA 2.0は、NSSでの使用が承認された暗号アルゴリズムのセットです。以下の表に、各アルゴリズムとその機能、仕様、およびパラメータを記載します。

表：Commercial National Security Algorithm Suite 2.0

アルゴリズム	(略)	仕様	パラメータ
汎用アルゴリズム			
(略)	(略)	(略)	(略)
ML-DSA (旧 CRYSTALS-Dilithium)	(略)	FIPS PUB 204	全ての機密区分レベルに対し ML-DSA-87 を使用。
(略)	(略)	(略)	(略)

Q: CNSA 2.0において、HashML-DSA（ML-DSAのプレハッシュモード）は認められていますか？

A: 現時点では認められていません。HashML-DSAはFIPS 204で規定されるML-DSAのバリエーションの一つであり、鍵の再利用時に生じうる脆弱性を防ぐために、あえて標準のML-DSAとの相互運用性を断ち切った上で、署名前にメッセージを圧縮する手法を採用しています。HashML-DSAは、ML-DSA-87とCNSAハッシュ関数を標準的な方法で組み合わせた場合に実現できる機能以上のものを提供しないこと、また標準的なML-DSA-87が広くサポートされると見込まれることから、NSAはNSS（国家安全保障システム）においてHashML-DSAは不要であると判断しています。そのため、現時点ではHashML-DSAは認められていません。将来的にプロトコル上の必要性が生じた場合には、その時点で限定的な使用に関する具体的な指針がNSAから示される予定です。

- 米国NISTのFIPS 204では、ML-DSAのセキュリティカテゴリについて、鍵生成に用いる乱数生成器のセキュリティ強度に関する条件を規定しており、ML-DSA-44では、乱数生成器の強度によってCategory 2からCategory 1に低下する場合がある。

米国 国立標準技術研究所 (NIST)

FIPS204 "Module-Lattice-Based Digital Signature Standard" (2024.8)

<https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.204.pdf>

3.6.1 Randomness Generation

Algorithm 1, implementing key generation for ML-DSA, uses an RBG to generate the 256-bit random seed ξ . The seed ξ shall be a fresh (i.e., not previously used) random value generated using an approved RBG, as prescribed in SP 800-90A, SP 800-90B, and SP 800-90C. Moreover, the RBG used shall have a security strength of at least 192 bits for ML-DSA-65 and 256 bits for ML-DSA-87. For ML-DSA-44, the RBG should have a security strength of at least 192 bits and shall have a security strength of at least 128 bits. **If an approved RBG with at least 128 bits of security but less than 192 bits of security is used, then the claimed security strength of ML-DSA-44 is reduced from category 2 to category 1.**

【仮訳（機械翻訳ベース）】

3.6.1 乱数生成

ML-DSAの鍵生成を実装するアルゴリズム1では、RBG（乱数生成器）を用いて256ビットの乱数シード ξ を生成する。シード ξ は、SP 800-90A、SP 800-90B、およびSP 800-90Cに規定される承認済みのRBGを使用して生成された、新規の（すなわち、以前に使用されたことのない）乱数値でなければならない。さらに、使用するRBGは、ML-DSA-65に対しては少なくとも192ビット、ML-DSA-87に対しては少なくとも256ビットのセキュリティ強度を備えている必要がある。ML-DSA-44の場合、RBGは少なくとも192ビットのセキュリティ強度を備えることが推奨され、かつ少なくとも128ビットのセキュリティ強度を備えていなければならない。**128ビット以上192ビット未満のセキュリティ強度を持つ承認済みRBGを使用する場合、ML-DSA-44の公称セキュリティ強度は、カテゴリ2からカテゴリ1へと引き下げられる。**

(参考) ML-DSA・SLH-DSAのIETFでの標準化状況

➤ ML-DSA及びSLH-DSAについては、X.509やCMSで標準化が完了しており、その他の用途でも標準化が進められている。

暗号技術		X.509	CMS 暗号メッセージ構文	TLS	SSH	DNSSEC
ML-DSA	ML-DSA-44 (Category 2)	RFC 9881 ^(*1)	RFC 9882 ^(*3)	WGドラフト ^(*5)	WGドラフト ^(*6)	個人ドラフト ^(*8)
	ML-DSA-65 (Category 3)	RFC 9881 ^(*1)	RFC 9882 ^(*3)	WGドラフト ^(*5)	—	—
	ML-DSA-87 (Category 5)	RFC 9881 ^(*1)	RFC 9882 ^(*3)	WGドラフト ^(*5)	WGドラフト ^(*6)	—
SLH-DSA	SLH-DSA-[SHA2/SHAKE]-128[s/f] (Category 1)	RFC 9909 ^(*2)	RFC 9814 ^(*4)	—	個人ドラフト ^(*7)	個人ドラフト ^(*9) 128sのみ
	SLH-DSA-[SHA2/SHAKE]-192[s/f] (Category 3)	RFC 9909 ^(*2)	RFC 9814 ^(*4)	—	(NIST SP 800-230 案の追加パラメータセット が提案)	—
	SLH-DSA-[SHA2/SHAKE]-256[s/f] (Category 5)	RFC 9909 ^(*2)	RFC 9814 ^(*4)	—	個人ドラフト ^(*7)	—

✓ **X.509**及び**CMS**では、**ML-DSA**及び**SLH-DSA**の各パラメータセットを利用するための**仕様がRFC化**されている。

✓ **TLS**では、**ML-DSA**の各パラメータセットをハンドシェイク署名等に利用するための**仕様が検討中**（Internet-Draft）で、**IETFのTLS WG文書**となっている。**SLH-DSA**についても、同様の仕様が個人提出のInternet-Draftとして提案されたが、**現在は失効**しており、WGドラフトにはなっていない。

※署名サイズがML-DSAでは2.4~4.6KBなのに対し、SLH-DSAでは7.9~50KB程度と大きいので、エンドエンティティのハンドシェイク署名として適していない。

✓ **SSH**では、**ML-DSA**の各パラメータセットを利用するための**仕様が検討中**（Internet-Draft）で、**IETFのSSH WG文書**※となっている。**SLH-DSA**についても、単独又は従来署名と組み合わせて利用するための仕様が**個人提出のInternet-Draftとして提案**されているが、WG文書にはなっていない。
※WG文書は、ML-DSAと従来署名を組み合わせた合成署名の仕様。
ML-DSA単独で利用する仕様は個人提出のInternet-Draftとして別途提案。

✓ **DNSSEC**では、**ML-DSA-44**を利用するための**仕様が検討中**（Internet-Draft）であるが、WG文書にはなっていない。**SLH-DSA**についても、SLH-DSA-[SHA2/SHAKE]-128sを利用する仕様が**個人提出のInternet-Draftとして提案**されているが、WG文書にはなっていない。

(*1) RFC 9881 Internet X.509 Public Key Infrastructure -- Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA)
<https://www.rfc-editor.org/rfc/rfc9881.html>

(*2) RFC 9909 Internet X.509 Public Key Infrastructure -- Algorithm Identifiers for the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)
<https://www.rfc-editor.org/rfc/rfc9909.html>

(*3) RFC 9882 Use of the ML-DSA Signature Algorithm in the Cryptographic Message Syntax (CMS)
<https://www.rfc-editor.org/rfc/rfc9882.html>

(*4) RFC 9814 Use of the SLH-DSA Signature Algorithm in the Cryptographic Message Syntax (CMS)
<https://www.rfc-editor.org/rfc/rfc9814.html>

(*5) Use of ML-DSA in TLS 1.3
draft-ietf-tls-mldsa-06
<https://datatracker.ietf.org/doc/draft-ietf-tls-mldsa-06/>

(*6) Post-Quantum Composite Signatures in SSH
draft-ietf-sshm-composite-sigs-00
<https://datatracker.ietf.org/doc/draft-ietf-sshm-composite-sigs-00/>

(*7) Stateless Hash-Based Signatures for Secure Shell (SSH)
draft-josefsson-ssh-sphincs-02
<https://datatracker.ietf.org/doc/draft-josefsson-ssh-sphincs/>

(*8) Module-Lattice Digital Signature Algorithm for DNSSEC
draft-westerbaan-dnssec-mldsa-04
<https://datatracker.ietf.org/doc/draft-westerbaan-dnssec-mldsa/>

(*9) Stateless Hash-Based Digital Signatures with Merkle Tree Ladder Mode for DNSSEC
draft-fregly-dnsop-slh-dsa-mtl-dnssec
<https://datatracker.ietf.org/doc/draft-fregly-dnsop-slh-dsa-mtl-dnssec/>

(参考) ML-DSA・SLH-DSAの実装・利用状況

- ML-DSAは、主要なクラウドサービスや暗号ライブラリで各パラメータセットへの対応が進んでおり、特にML-DSA-44は実際のサービスでの利用や推奨が確認されている。一方、SLH-DSAについては、実装が進みつつあるものの、実際のサービスでの利用は限定的。

暗号技術		Cloudflare 1.1.1.1 ^(*1) 【DNSSEC】	Cloudflare ^(*2) 【オリジン認証】	GoogleCloud KMS ^(*3) 【電子署名】	AWS KMS ^(*4) 【電子署名】	OpenSSL 3.5 ^(*5) 【暗号ライブラリ】
ML-DSA	ML-DSA-44 (Category 2)	対応	対応 (推奨)	対応	対応	対応
	ML-DSA-65 (Category 3)	—	対応	対応	対応	対応
	ML-DSA-87 (Category 5)	—	対応	対応	対応	対応
SLH-DSA	SLH-DSA-[SHA2/SHAKE]-128[s/f] (Category 1)	—	—	対応 (SHA2-128sのみ)	—	対応
	SLH-DSA-[SHA2/SHAKE]-192[s/f] (Category 3)	—	—	—	—	対応
	SLH-DSA-[SHA2/SHAKE]-256[s/f] (Category 5)	—	—	—	—	対応

- ✓ CloudflareのパブリックDNSサービス (1.1.1.1) では、**ML-DSA-44で署名されたDNSSECレコードをデフォルトで検証可能。**
- ✓ **ML-DSA**は、GoogleCloudやAWSは**44/65/87を全て提供**する一方、**Cloudflareは全てに対応した上で、通常用途にはML-DSA-44を推奨。**
※ML-DSA-44が最もパフォーマンスが高いため。
- ✓ **SLH-DSA**は、**OpenSSLは全てのパラメータセットを実装。**
Google CloudではSLH-DSA-SHA2-128sを商用提供。

(*1) Cloudflare, "1.1.1.1 now supports post-quantum DNSSEC"

<https://blog.cloudflare.com/post-quantum-dnssec-1111/>

(*2) Cloudflare, "Post-quantum authentication to origins is now supported"

<https://blog.cloudflare.com/post-quantum-authentication-to-origins/>

(*3) Google Cloud KMS, "Digital signatures"

<https://docs.cloud.google.com/kms/docs/digital-signatures?hl=ja>

(*4) AWS KMS, "ML-DSA keys in AWS KMS"

<https://docs.aws.amazon.com/kms/latest/developerguide/mldsa.html>

(*5) OpenSSL, "OpenSSL 3.5 Final Release"

<https://openssl-library.org/post/2025-04-08-openssl-35-final-release/>

検討ポイント⑤ Camellia・KCipher-2・SHAKEの取扱い

- 表1にある暗号技術のうち、CRQCへの耐性について引き続き検討が必要とされた、共通鍵暗号（Camellia及びKCipher-2）並びにハッシュ関数（SHAKE128及びSHAKE256）について、表2に追加すべきか。

【考え方】

<Camellia>

- ✓ 鍵長は128, 192, 256ビットがあり、2024年度外部評価報告書※において、同じ鍵長のAESと同等の安全性とされる。
- ✓ このため、**128ビット鍵長**は、**Category 1相当**であり、検討ポイント③の整理を踏まえ、**表2に掲載しないことが適当**。
- また、**192ビット及び256ビット鍵長**は、それぞれ「Category 3」、「Category 5」として表2に掲載することが適当。

<KCipher-2>

- ✓ 鍵長は128ビットがあり、2024年度外部評価報告書※において、AES-128と同等の安全性とされる。
- ✓ このため、**Category 1相当**であり、検討ポイント③の整理を踏まえ、**表2に掲載しないことが適当**。

<SHAKE128>

- ✓ 2024年度外部評価報告書※において、出力長が $n(\geq 256)$ 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 $\min(2^{256/3}, 2^{n/3}) = 2^{256/3}$ である。これはSHA-256の概算値 ($2^{256/3}$) と同じ。
- ✓ このため、**Category 2相当**であり、検討ポイント③の整理を踏まえ、**表2に掲載しないことが適当**。

※ML-DSAでは、内部処理にSHAKE128及びSHAKE256を使用するが、ML-DSA内部の構成要素としての利用であるため、個別の掲載対象とはしない。

※「SLH-DSA-SHAKE-128[s/f]」について、「128」はセキュリティパラメータ(n)を表し、内部処理にSHAKE256を使用（プレハッシュではSHAKE128も使用可能）。

<SHAKE256>

- ✓ 2024年度外部評価報告書※において、出力長が $n(\geq 256)$ 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。出力長（ハッシュ長）により強度が変わる。
- ✓ このため、検討ポイント③の整理を踏まえ、SHA-384の概算値 ($2^{384/3}$) 以上の安全性を確保するため、**「ハッシュ長は384ビット以上とする。」との注釈を付した上で、「Category 4」として表2に掲載することが適当**。

※表1のSHAKE128及びSHAKE256には「ハッシュ長は256ビット以上とすること。」の注釈が付されている。

検討ポイント⑥ 暗号利用モード等の取扱い

- 表 1 にある暗号技術のうち、CRQCへの耐性について引き続き検討が必要とされた、**暗号利用モード、メッセージ認証コード、認証暗号及びエンティティ認証**について、**表 2 に追加すべきか。**

【考え方】

＜暗号利用モード及びメッセージ認証コード＞

- ✓ 鍵長がkビットのとき、2024年度外部評価報告書※¹において、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。（参考：AES-256の安全性が期待できる範囲は「時間 $\leq 2^{128}$ 」）
- ✓ 暗号利用モード及びメッセージ認証コードは、組み合わせて利用する暗号技術（ブロック暗号又はハッシュ関数）の安全性に依存することから、セキュリティカテゴリを単独で付すのではなく、次のように表記した上で、**表 2 に掲載することが適当。**
セキュリティカテゴリ：「組み合わせて利用する暗号技術のセキュリティカテゴリに準ずる。」
- ✓ また、**組み合わせる暗号技術は表 2 のものに限る旨の注釈を付すことが適当。**（→検討ポイント⑦）

＜認証暗号（ChaCha20-Poly1305）＞

- ✓ 鍵長は256ビットがあり、2024年度外部評価報告書※¹において、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。（参考：AES-256の安全性が期待できる範囲は「時間 $\leq 2^{128}$ 」）
- ✓ AES-256と同等と整理できることから、「**Category 5**」として**表 2 に掲載することが適当。**

＜エンティティ認証＞

- ✓ エンティティ認証は、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の技術。
ISO/IEC 9798で認証メカニズムが規定されるが、具体的な**暗号プリミティブやパラメータ等は一意に定まらない**※²。
- ✓ エンティティ認証の安全性は、使用する暗号プリミティブの安全性だけでなく、プロトコル全体の設計・実装に依存。
- ✓ そのため、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り、
 単一の暗号技術と同じ粒度で**CRQCへの耐性を有すると判断することは難しく、表 2 の掲載を保留**する。

※ 1 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）

※ 2 ISO/IEC 9798 プロトコルの安全性評価（CRYPTREC-EX-2013-2010）

(参考) 2024年度外部評価報告書について

- 2024年度外部評価報告書※では、Q1モデルを主たる評価の前提とし、鍵長等に応じた安全性の目安を整理。
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)
- ハッシュ関数については、BHTアルゴリズムによる量子衝突探索を踏まえ、出力長・キャパシティ等に応じた安全性の目安を整理。
- また、既存の古典的安全性評価に基づくデータ量・クエリ回数等の制約がQ1モデルでも基本的に維持されることを確認。

<参考：Q1モデルとQ2モデル>
【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

量子コンピュータが暗号技術の安全性に及ぼす影響 Groverアルゴリズムに必要な計算時間の概算値

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 $\leq 2^k$ 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 $\leq 2^k$ 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 $\leq 2^k$ 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

(2024年度外部評価報告書の表 5 を一部表記を変更・簡略化)
※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としては、小さい多項式サイズの量子計算機が 1 つ使い、QRAMは必要な分だけ大きなものを使う状態。
※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。

量子コンピュータがハッシュ関数の安全性に及ぼす影響 BHTアルゴリズムに必要な計算時間および量子メモリの概算値

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	$\ell (\geq 256)$	$\min(2^{170.7}, 2^{\ell/3})$	$\min(2^{170.7}, 2^{\ell/3})$

(2024年度外部評価報告書の表 6 を一部表記を変更・簡略化)
※BHTの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。
※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) 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。

検討ポイント⑦ 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**を追加することに当たり、組み合わせて利用する暗号技術に関する注釈をどのように記載すべきか。

【考え方】

- ✓ 表 2 に追加する暗号利用モード及びメッセージ認証コードについては、**組み合わせる暗号技術を表 2 に掲載されたものに限定する旨の注釈を付すことが適当。**
- ✓ 一方、**表 1**に掲載する暗号利用モード、メッセージ認証コード及びエンティティ認証については、**従来どおり**、推奨候補暗号リスト等も含めた**CRYPTREC暗号リストに掲載される暗号技術との組合せを認めることが適当。**
- ✓ このため、**表 1 と表 2 で注釈を分けて記載**するとともに、従来の注釈の趣旨を維持しつつ、**記載の明確化**を図ることが適当。

（参考：組み合わせる暗号技術）

暗号利用モード＝共通鍵暗号のうちブロック暗号

CMAC＝共通鍵暗号のうちブロック暗号

HMAC＝ハッシュ関数

ISO/IEC 9798-2＝共通鍵暗号

ISO/IEC 9798-3＝公開鍵暗号のうち署名

ISO/IEC 9798-4＝メッセージ認証コード

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（略）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。（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。

＜表 1 現行暗号リスト＞

技術分類	(略)
(略)	(略)
暗号利用モード(注1-4)	(略)
メッセージ認証コード(注1-4)	(略)
認証暗号	(略)
エンティティ認証(注1-4)	(略)

＜表 2 耐量子計算機暗号（PQC）リスト＞

技術分類	(略)
(略)	(略)
暗号利用モード(注2-6)	(略)
メッセージ認証コード(注2-6)	(略)
認証暗号	(略)

(注1-4) CRYPTREC暗号リストに掲載する他の技術分類の暗号技術と組み合わせて利用すること。

(注2-6) 表 2 に掲載する他の技術分類の暗号技術と組み合わせて利用すること。

検討ポイント⑧ 暗号利用モードに係る注釈の取扱い

- 表1（現行暗号リスト）に掲載されている暗号利用モードを表2（耐量子計算機暗号（PQC）リスト）に追加するに当たり、既存の注釈をどのように取り扱うべきか。

【考え方】

✓「XTS」に係る注釈

→表1の「XTS」に付される注釈について、前段（ブロック暗号に関する規定）は、64ビットブロック暗号が表2に存在せず、追加予定もないことから、当該注釈を不要とすることが適当。

→一方、後段（利用用途及び実装方法に関する規定）は、XTS自体の制限事項であるため同様の注釈を表2の「XTS」にも付すことが適当。

✓「認証付き秘匿モード」に係る注釈

→表1の「認証付き秘匿モード」に付される注釈について、ブロック暗号と組み合わせることで認証暗号として利用できることを示すものであり、同様の注釈を表2の「認証付き秘匿モード」にも付すことが適当。

なお、「暗号利用モード」の注釈（検討ポイント⑦）により、組み合わせる暗号技術が表2のものに限定される。このため、「認証付き秘匿モード」に付される注釈は「CRYPTREC暗号リスト掲載のブロック暗号」ではなく、「表2のブロック暗号」とすることが適当。

✓「GCM」に係る注釈

→表1の「GCM」に付される注釈について、初期化ベクトル(IV)長に関する推奨事項は、処理効率等の観点から定められたものであり※、表2においても同様の注釈を付すことが適当。

※NIST SP 800-38Dでは、相互運用性、効率性及び設計の単純性の観点から、IV長96ビットを推奨。96ビットの場合は固定値を連結し、それ以外の場合はハッシュ関数（GHASH）で処理して、いずれも128ビットの初期値を生成する。IV長を96ビットより長くしても、安全性は向上しない。

＜表1 現行暗号リスト＞

技術分類		暗号技術
(略)		(略)
暗号利用モード	秘匿モード	(略)
		XTS(注1-5)
	認証付き秘匿モード(注1-6)	CCM GCM(注1-7)
(略)		(略)

(注1-5) 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 SP 800-38Eに従うこと。

(注1-6) 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1-7) 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＞

技術分類		暗号技術	(略)
(略)		(略)	(略)
暗号利用モード	秘匿モード	(略)	(略)
		XTS(注2-7)	
	認証付き秘匿モード(注2-8)	CCM	
		GCM(注2-9)	

(注2-7) 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 SP 800-38Eに従うこと。

(注2-8) CRYPTREC暗号リスト掲載表2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2-9) 初期化ベクトル長は96ビットを推奨する。

➤ CRYPTRECにおける**用語・表記**について、どのような方針で統一することが適当か。

【考え方】

- ✓ 同一概念を異なる用語で表記している場合、原則として**用語を統一**し、使い分けを明確化することが適当。
- ✓ 「量子コンピュータ」と「量子計算機」について、原則として「**量子コンピュータ**」に統一し、初出時には「量子コンピュータ（量子計算機）」と併記することが適当。ただし、「耐量子計算機暗号（PQC）」等の既に定着している名称は変更しないことが適当。

＜長音表記について＞

- ✓ **外来語の長音表記**（英語の語末の「-er」「-or」「-ar」等）については、公用文では原則として長音符号「ー」を用いることとされているが、慣用に応じて「ー」を省略することも認められている。
- ✓ このため、慣用や専門用語としての定着状況、政府関係文書における使用実態等を踏まえ、**語ごとに表記を統一**することが適当。具体的には、「コンピュータ」「パラメータ」「カテゴリ」については、長音符号を付さない表記とすることが適当。

(参考) 外来語の表記に関する文書

➤ 外来語の長音表記について、国の表記基準では原則として長音符号「ー」を用いることとされ、慣用に応じた省略も認められている。

文化庁 外来語の表記（平成3年内閣告示第2号）

https://www.bunka.go.jp/kokugo_nihongo/sisaku/joho/joho/kijun/naika/ku/gairai/honbun06.html

留意事項その2(細則的な事項) (抜粋)

Ⅲ 撥（はつ）音、促音、長音その他に関するもの

3 長音は、原則として長音符号「ー」を用いて書く。

〔例〕 エネルギー オーバーコート グループ ゲーム ショー
テーブル パーティー
ウェールズ（地） ポーランド（地） ローマ（地）
ゲーテ（人） ニュートン（人）

注1・2 （略）

注3 英語の語末の-er、-or、-arなどに当たるものは、原則としてア列の長音とし長音符号「ー」を用いて書き表す。ただし、慣用に応じて「ー」を省くことができる。

〔例〕 エレベーター ギター コンピューター マフラー
エレベータ コンピュータ スリッパ

JIS Z 8301:2019（規格票の様式及び作成方法）

附属書H(規定) 文章の書き方並びに用字、用語、記述符号及び数字

H.6 外来語の表記
3.6.28 外来語の表記は、主として“外来語の表記（平成3.6.28 内閣告示第2号）”による。

情報処理学会 カタカナ語末尾の長音符号に対する情報処理学会の対応について（2009年1月23日）

<https://www.ipsj.or.jp/magazine/topics/katakana.html>

標記について情報処理学会として対応を検討してきましたが、その結果、

- (1)当面は現行通りの対応（3音節以上はのばさない）とする
- (2)世の中の推移を注意深く見守り、今後必要に応じて再検討することに決まりましたのでお知らせいたします。

使用例：コンピュータ、プリンタ

公用文作成の考え方（建議）

（令和4年1月7日 文化審議会）

https://www.bunka.go.jp/seisaku/bunkashingikai/kokugo/hokoku/93650/001_01.html

I 表記の原則

3 外来語の表記

外来語の表記は、「外来語の表記」（平成3年内閣告示第2号）に基づくものとする。（略）

公用文作成の考え方（文化審議会建議）解説

I－3 外来語の表記

Ⅰ 長音は、原則として長音符号を使って書く

長音は、長音符号を使って書く。

例）エネルギー オーバーコート グループ ゲーム ショー メール
ただし、次のようなものは慣用に従い、長音符号を用いずに書く。

例）バレエ（舞踊） ミイラ エイト ペイント レイアウト サラダボウル
英語の語末の-er、-or、-arなどに当たるものは、ア列の長音とし、長音符号を用いて書くのが原則である。そのほか、-ty、-ryなど、yで終わる語も長音符号を用いて書く。

例）コンピューター（computer） エレベーター（elevator）
カレンダー（calendar） コミュニティー（community）
カテゴリー（category）

（略）

NHK放送文化研究所 第1472回放送用語委員会（東京） 外来語における語末の長音の発音について（2024年6月14日）

https://www.nhk.or.jp/bunken/research/kotoba/20240901_1.html

1.2 現行の規定（抜粋）

英語などの語末の-er、-or、-ar、-yは原則として長音符号をつけて表記し、のばして発音する。

〈例〉 オーソリティー コンピューター エレベーター パーティー