

# 耐量子計算機暗号（PQC）リスト検討タスクフォース （第 4 回）

令和 8 年 10 月 5 日（月） 16:00～18:00  
経済産業省本館17階 第 2 特別会議室  
（ ハイブリッド開催 ）

## <議事次第>

1. 開会
2. 議事
  - (1) 課題④ 公開鍵暗号方式のPQCの安全性評価等の進め方について
  - (2) 課題①・② Category 1・2及び暗号利用モード等の取扱いについて
  - (3) 課題③ ハイブリッド構成の取扱いについて
  - (4) 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   | 課題④ 公開鍵暗号方式のPQCの安全性評価等の進め方                                      |
| 資料 3   | 課題②に係る諸外国動向調査                                                   |
| 資料 4   | 課題①・② Category 1・2及び暗号利用モード等の取扱いについて                            |
| 資料 5   | 課題③ ハイブリッド構成の取扱い                                                |
| 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<br>（CRYPTREC暗号リスト）（令和 8 年 3 月 30 日更新） |

以上

# 課題④

## 公開鍵暗号方式のPQCの 安全性評価等の進め方

# 公開鍵暗号方式のPQCの安全性評価等の進め方

2

黄マーカ一部

- CRYPTREC暗号リストへの掲載に向けて安全性及び実装性能の評価を行うべき暗号として、現状、FIPS 203～205が予定されているが、**FIPS 203～205以外のPQCについてどのように取り扱うべきか。**

|                      |           |           |              |
|----------------------|-----------|-----------|--------------|
| ◆ FIPS 203 (ML-KEM)  | 格子暗号ベース   | 暗号化・鍵交換用途 | 2025年度末目途に評価 |
| ◆ FIPS 204 (ML-DSA)  | 格子暗号ベース   | 署名用途      | 2026年中頃目途に評価 |
| ◆ FIPS 205 (SLH-DSA) | ハッシュ関数ベース | 署名用途      | 2026年度末目途に評価 |

## 【考え方】

- ✓ **国内で利用が見込まれる暗号技術は、安全性評価等の対象となり得るが、PQCは多数存在するため、一定の基準を定めることが重要。**

(参考) CRYPTREC暗号リストの移行ルールとして、新たな暗号技術が、「標準化等により将来的な利用が見込まれ、安全性（CRQCへの耐性を見据えた評価を行う。）や実装性能が十分にあると暗号技術検討会が決定した場合」に表2へ追加することとしている。

- ✓ **安全性評価等の対象**の選定については次の観点を総合的に勘案する。

**(A)安全性の成熟度**：安全性について、複数国の専門家が参加する公開プロセス等において十分な評価実績があること

**(B)標準化の成熟度**：ISOその他複数の国際的な標準化機関・団体において標準化され、又は標準化が進められていること

**(C)実利用の具体性**：国内利用を想定した製品・サービスに使用され、又は具体的な使用の見込みがあること

- ✓ 上記観点到照して、次のように判断する。なお、評価スケジュールは暗号技術評価委員会において検討する。

- 今後策定予定の**FIPS標準**※について、世界的な利用が見込まれることから、**評価対象とする。**

※FN-DSA、HQC、NIST追加公募により今後選定される署名方式

- **LMS及びXMSS**について、標準化され、特定用途での利用が見込まれることから、**評価対象とする**※。

※ステートフル署名であり、署名回数や再利用防止等のステート管理に関する留意事項の整理が必要。HSS及びXMSS<sup>MT</sup>は評価対象にしない。  
また、米国CNSA2.0ではソフトウェア署名にML-DSAも認められていることから、LMS及びXMSSの今後の利用動向も踏まえつつ評価を行う。

- **NTRU**について、標準化の進展や国内利用が認められることから、**評価対象とする。**

# (参考) 各PQCにおける3つの観点の整理

➤ 前頁の3つの観点を踏まえ、各方式について安全性評価等の必要性を整理。

| 暗号技術                         | (A)安全性の成熟度               | (B)標準化の成熟度                   | (C)実利用の具体性                     | 取扱い案             |
|------------------------------|--------------------------|------------------------------|--------------------------------|------------------|
| <b>FN-DSA<br/>(FIPS 206)</b> | ◎ NIST標準化プロセスで十分な評価実績    | ◎ FIPSとして標準化予定               | ○ 今後広く利用されることが見込まれる            | 評価対象として検討        |
| <b>HQC</b>                   | ◎ NIST標準化プロセスで十分な評価実績    | ◎ FIPSとして標準化予定               | ○ 今後広く利用されることが見込まれる            | 評価対象として検討        |
| <b>NIST追加公募中の署名方式</b>        | ○ NIST標準化プロセスで評価が継続中     | ○ NIST標準候補として評価中             | ○ 標準化後は広く利用されることが見込まれる         | 標準化を踏まえ評価対象として検討 |
| <b>LMS / XMSS</b>            | ◎ 長期間の評価実績               | ◎ ISO/IECで標準化、RFC・NIST SPで規定 | ○ ファームウェア・コード署名等での利用が見込まれる     | 評価対象として検討        |
| <b>NTRU</b>                  | ◎ NIST Round 3まで長期間の評価実績 | ◎ ISO/IEC、IETF等で標準化が進展       | ◎ 国内事業者でVPN実装・商用展開の具体的計画あり     | 評価対象として検討        |
| <b>FrodoKEM</b>              | ◎ NIST Round 3まで長期間の評価実績 | ◎ ISO/IECで標準化、IETF等で標準化が進展   | △ 国内での具体的な製品・サービス利用は現時点では確認できず | 現時点では継続把握        |
| <b>Classic McEliece</b>      | ◎ NIST Round 4まで長期間の評価実績 | ○ ISO/IECで標準化                | △ 国内での具体的な製品・サービス利用は現時点では確認できず | 現時点では継続把握        |
| <b>NTRU+</b>                 | ○ 韓国KpqC公募で公開評価を経て最終選定   | ○ 韓国産業標準 (KS) 制定提案済          | △ 国内での具体的な製品・サービス利用は現時点では確認できず | 現時点では継続把握        |

米国 国立標準技術研究所 (NIST)

**NIST SP 800-208 "Recommendation for Stateful Hash-Based Signature Schemes"** (2020.10)

<https://csrc.nist.gov/pubs/sp/800/208/final>

## Abstract

This recommendation specifies two algorithms that can be used to generate a digital signature, both of which are stateful hash-based signature schemes: the Leighton-Micali Signature (**LMS**) system and the eXtended Merkle Signature Scheme (**XMSS**), along with their multi-tree variants, the Hierarchical Signature System (HSS) and multi-tree XMSS (XMSS<sup>MT</sup>).

米国 国立標準技術研究所 (NIST)

**NIST IR 8547 (Initial Public Draft)**

**"Transition to Post-Quantum Cryptography Standards"** (2024.11)

<https://csrc.nist.gov/pubs/ir/8547/ipd>

## 2.1.1. Digital Signature Algorithms

SP 800-208, *Recommendation for Stateful Hash-Based Signature Schemes*, specifies two stateful hash-based signature (HBS) schemes — the Leighton-Micali Signature (LMS) system and the eXtended Merkle Signature Scheme (XMSS) — along with their multi-tree variants, the Hierarchical Signature System (HSS) and multi-tree XMSS (XMSS<sup>MT</sup>). These schemes are also **resistant to attacks by quantum computers**. In stateful hash-based signature (HBS) schemes, the HBS private key consists of a large set of one-time signature (OTS) private keys. The security of these schemes relies on the signer to ensure that no individual OTS key is ever used to sign more than one message. Due to this need to maintain state, **HBS schemes are not intended for general use**.

## 【仮訳（機械翻訳ベース）】

### 概要

本勧告は、デジタル署名の生成に使用できる2つのアルゴリズム、すなわち Leighton-Micali Signature (**LMS**) システムとeXtended Merkle Signature Scheme (**XMSS**) を規定する。これらは共にステートフルなハッシュベース署名方式であり、それぞれのマルチツリー・バリエーションである Hierarchical Signature System (HSS) およびマルチツリーXMSS (XMSS<sup>MT</sup>) も対象に含まれる。

## 【仮訳（機械翻訳ベース）】

### 2.1.1. デジタル署名アルゴリズム

SP 800-208「ステートフル・ハッシュベース署名方式に関する推奨事項」では、2つのステートフル・ハッシュベース署名（HBS）方式、すなわち Leighton-Micali Signature (LMS) システムとeXtended Merkle Signature Scheme (XMSS) が、それらのマルチツリー版である Hierarchical Signature System (HSS) およびmulti-tree XMSS (XMSS<sup>MT</sup>) と共に規定されています。これらの方式は、**量子コンピュータによる攻撃に対しても耐性があります**。ステートフル・ハッシュベース署名（HBS）方式において、HBS秘密鍵は多数のワンタイム署名（OTS）秘密鍵の集合で構成されます。これらの方式の安全性は、署名者が個々のOTS鍵を複数のメッセージの署名に決して使用しないように管理することに依存しています。このように状態を維持する必要があるため、**HBS方式は一般的な用途には適していません**。

米国 国家安全保障局 (NSA)

“Announcing the Commercial National Security Algorithm Suite 2.0” (2022.9)

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

## Algorithms for software- and firmware-signing

The **reasons for choosing** separate algorithms for software- and firmware-signing are three-fold:

- NIST has standardized these algorithms already, while other post-quantum signatures are not yet standardized,
- This signature use-case is more urgent, and
- This selection places algorithms with the most substantial history of cryptanalysis in a use case where their potential performance issues have minimal impact. In particular, this usage coincides well with the requirement for keeping track of state—that is, how many times a given public key was used in signing software or firmware when deploying these signatures.

The algorithms chosen for software- and firmware-signing are those specified in NIST Special Publication 800-208. NSA recommends Leighton-Micali with SHA-256/192, but all NIST SP 800-208 algorithms are approved for this use case. Note that to avoid weakening the security of these signatures, you must meet all the requirements of SP 800-208, including the need to manage state and implement signing in hardware.

NSA encourages vendors to begin adopting NIST SP 800-208 signatures immediately. For more information on requirement timelines, see the Timing section. The following table lists CNSA 2.0 algorithms for software and firmware updates.

Table I: CNSA 2.0 algorithms for software and firmware updates

| Algorithm                              | Function                                                         | Specification   | Parameters                                                                      |
|----------------------------------------|------------------------------------------------------------------|-----------------|---------------------------------------------------------------------------------|
| Leighton-Micali Signature (LMS)        | Asymmetric algorithm for digitally signing firmware and software | NIST SP 800-208 | All parameters approved for all classification levels. SHA-256/192 recommended. |
| Xtended Merkle Signature Scheme (XMSS) | Asymmetric algorithm for digitally signing firmware and software | NIST SP 800-208 | All parameters approved for all classification levels.                          |

## 【仮訳（機械翻訳ベース）】

### ソフトウェアおよびファームウェアの署名用アルゴリズム

ソフトウェアおよびファームウェアの署名に個別のアルゴリズムが**選定された理由**は、以下の3点です。

- NISTがこれらのアルゴリズムをすでに標準化している一方で、他の耐量子署名はまだ標準化されていないこと、
- この署名のユースケースは緊急性が高いこと、そして
- 暗号解読の歴史が最も長いアルゴリズムを、潜在的な性能上の問題が及ぼす影響を最小限に抑えられるユースケースに適用できること。特に、この用途は「状態（ステート）」の追跡、すなわち署名展開時に特定の公開鍵がソフトウェアやファームウェアの署名に何回使用されたかを管理するという要件と、うまく整合しています。

ソフトウェアおよびファームウェアの署名用に選定されたアルゴリズムは、NIST Special Publication (SP) 800-208で規定されているものです。NSAはSHA-256/192を組み合わせたLeighton-Micali方式を推奨していますが、NIST SP 800-208に記載されているすべてのアルゴリズムが、このユースケースにおいて承認されています。なお、署名のセキュリティを低下させないためには、状態管理やハードウェアでの署名実装など、SP 800-208のすべての要件を満たす必要があることに留意してください。

NSAは、ベンダーに対し、NIST SP 800-208準拠の署名の採用を直ちに開始するよう推奨しています。要件のスケジュールに関する詳細については、「タイミング（Timing）」のセクションを参照してください。以下の表は、ソフトウェアおよびファームウェアの更新に使用されるCNSA 2.0アルゴリズムをまとめたものです。

表I：ソフトウェアおよびファームウェアの更新用CNSA 2.0アルゴリズム

| アルゴリズム                                 | 機能                                 | 仕様              | パラメータ                                        |
|----------------------------------------|------------------------------------|-----------------|----------------------------------------------|
| Leighton-Micali Signature (LMS)        | ファームウェア及びソフトウェアへのデジタル署名用非対称アルゴリズム  | NIST SP 800-208 | すべての分類レベルにおいて、すべてのパラメータが承認済み。SHA-256/192を推奨。 |
| Xtended Merkle Signature Scheme (XMSS) | ファームウェアおよびソフトウェアへのデジタル署名用非対称アルゴリズム | NIST SP 800-208 | すべての分類レベルにおいて、すべてのパラメータが承認済み。                |

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: Can I use HSS or XMSSMT from NIST SP 800-208?**

A: From NIST SP 800-208, NSA has only approved LMS and XMSS for use in NSS. The multi-tree algorithms **HSS and XMSSMT are not allowed**.

**Q: Can I use SLH-DSA (aka SPHINCS+) to sign software?**

A: While SLH-DSA is hash-based, it is not part of CNSA and is not approved for any use in NSS.

**Q: Can I use ML-DSA for firmware or software signing?**

A: **Yes**, however firmware roots of trust are a critical component to upgrade and NSA expects this to be implemented for some long-lived signatures in 2025, before validated ML-DSA is widely available. At this time, validated LMS and XMSS are commercially available. NSA **prefers to see this transition begin now (using LMS and XMSS) rather than wait for ML-DSA due to the long timeframes** involved in moving from small components and/or early designs to completed products.

**Validated ML-DSA is approved for all signing use cases and when it is available it may be the most appropriate choice for some software/firmware signing use cases.** For example, when a user's software signing strategy requires more signatures than can be reasonably used with a single LMS or XMSS key, or in software development environments with a distributed signing system, it would be reasonable to use ML-DSA.

【仮訳（機械翻訳ベース）】

**Q: NIST SP 800-208で規定されているHSSやXMSSMTを使用できますか？**

A: NIST SP 800-208に関して、NSAはNSS（国家安全保障システム）における使用についてLMSとXMSSのみを承認しています。マルチツリーアルゴリズムである**HSSやXMSSMTの使用は認められていません**。

**Q: ソフトウェアの署名にSLH-DSA（別名：SPHINCS+）を使用できますか？**

A: SLH-DSAはハッシュベースのアルゴリズムですが、CNSA（商用国家安全保障アルゴリズム）スイートには含まれておらず、NSSにおけるいかなる用途にも承認されていません。

**Q: ファームウェアやソフトウェアの署名にML-DSAを使用できますか？**

A: **はい、使用可能**です。ただし、ファームウェアの「信頼の起点（Root of Trust）」はアップグレードにおいて極めて重要な要素であり、NSAは、検証済みML-DSAが広く利用可能になる前の2025年時点で、長期にわたって有効性が求められる一部の署名に対して、この実装が行われることを想定しています。現時点では、検証済みのLMSおよびXMSSが商用利用可能です。小規模なコンポーネントや初期設計から完成品へと移行するには長い期間を要するため、NSAは**ML-DSAを待つのではなく、LMSやXMSSを用いて今すぐこの移行を開始すること**を推奨しています。

検証済みML-DSAはあらゆる署名用途で承認されており、利用可能になれば、特定のソフトウェアやファームウェアの署名用途において最適な選択肢となる**可能性があります**。例えば、ユーザーのソフトウェア署名戦略において、単一のLMSまたはXMSS鍵で現実的に扱える数を超える署名が必要な場合や、署名システムが分散化されたソフトウェア開発環境においては、ML-DSAを使用するのが合理的でしょう。

米国 国家安全保障局 (NSA)

“COMMERCIAL SOLUTIONS for CLASSIFIED (CSfC)

Mobile Access Capability Package 2.8.0”他 (2026.3)

<https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/capability-packages/>

## 5.10 SOFTWARE AND FIRMWARE SIGNINGS

There are **three acceptable algorithms** for software and firmware digital signatures, which are all included as part of the CNSA 2.0 cipher suites. These algorithms are enumerated within Table 3 and only one of the algorithms will be required to meet this requirement.

Table 3. CNSA 2.0 Algorithms for Software and Firmware Signing

| Algorithm                              | Function                                                         | Specification   | Parameters                                                                      |
|----------------------------------------|------------------------------------------------------------------|-----------------|---------------------------------------------------------------------------------|
| Leighton-Micali Signature (LMS)        | Asymmetric algorithm for digitally signing firmware and software | NIST SP 800-208 | All parameters approved for all classification levels. SHA-256/192 recommended. |
| Xtended Merkle Signature Scheme (XMSS) | Asymmetric algorithm for digitally signing firmware and software | NIST SP 800-208 | All parameters approved for all classification levels.                          |
| ML-DSA                                 | Asymmetric algorithm for digital signatures                      | FIPS 204        | Category 5 parameter, ML-DSA-87.                                                |

## 【仮訳（機械翻訳ベース）】

### 5.10 ソフトウェアおよびファームウェアの署名

ソフトウェアおよびファームウェアのデジタル署名には、CNSA 2.0暗号スイートの一部として含まれる**3種類のアルゴリズムが許容**されます。これらのアルゴリズムは表3に列挙されており、本要件を満たすために必要なアルゴリズムは、そのうちの1つのみです。

表3. ソフトウェアおよびファームウェア署名用CNSA 2.0アルゴリズム

| アルゴリズム                                 | 機能                                 | 仕様              | パラメータ                                        |
|----------------------------------------|------------------------------------|-----------------|----------------------------------------------|
| Leighton-Micali Signature (LMS)        | ファームウェア及びソフトウェアへのデジタル署名用非対称アルゴリズム  | NIST SP 800-208 | すべての分類レベルにおいて、すべてのパラメータが承認済み。SHA-256/192を推奨。 |
| Xtended Merkle Signature Scheme (XMSS) | ファームウェアおよびソフトウェアへのデジタル署名用非対称アルゴリズム | NIST SP 800-208 | すべての分類レベルにおいて、すべてのパラメータが承認済み。                |
| ML-DSA                                 | デジタル署名用非対称アルゴリズム                   | FIPS 204        | カテゴリ5のパラメータ、ML-DSA-87。                       |

# (参考) LMS/XMSSの利用状況

| 企業名等      | 製品名等                                 | LMS       | XMSS      | ML-DSA    | SLH-DSA   | 状況                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------|--------------------------------------|-----------|-----------|-----------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Thales    | Luna HSM<br>【HSM】                    | ◎<br>(*1) | ○<br>(*2) | ◎<br>(*1) | ○<br>(*2) | (*1) <a href="https://thalesdocs.com/gphsm/luna/7/docs/pci/Content/sdk/extension/s/pqc/post_quantum_algorithms.htm">https://thalesdocs.com/gphsm/luna/7/docs/pci/Content/sdk/extension/s/pqc/post_quantum_algorithms.htm</a><br>(*2) <a href="https://cpl.thalesgroup.com/sites/default/files/content/solution_briefs/field_document/2023-08/thales-luna-post-quantum-crypto-functionality-module-sb.pdf">https://cpl.thalesgroup.com/sites/default/files/content/solution_briefs/field_document/2023-08/thales-luna-post-quantum-crypto-functionality-module-sb.pdf</a><br>LMS/HSS及びML-DSAのファームウェアでの対応を確認。XMSS及びSPHINCS+は、追加機能（PQC Functionality Module）で対応を確認。 |
| Entrust   | nShield HSM<br>【HSM】                 | ○<br>(*4) | —         | ◎<br>(*3) | ◎<br>(*3) | (*3) <a href="https://nshielddocs.entrust.com/security-world-docs/v13.9.0/nshield-security-world-v13-9-0-release-notes.pdf">https://nshielddocs.entrust.com/security-world-docs/v13.9.0/nshield-security-world-v13-9-0-release-notes.pdf</a><br>(*4) <a href="https://nshielddocs.entrust.com/pqcop-docs/v1.1.3/nshield-pqc-option-pack-v1-1-3-release-notes.pdf">https://nshielddocs.entrust.com/pqcop-docs/v1.1.3/nshield-pqc-option-pack-v1-1-3-release-notes.pdf</a><br>ML-DSA及びSLH-DSAのファームウェアでの対応を確認。LMSは追加機能（PQC Option Pack）で対応を確認。XMSSについては確認できず。                                                                                                       |
| Utimaco   | u.trust General Purpose HSM<br>【HSM】 | ○<br>(*5) | ○<br>(*5) | ○<br>(*5) | △<br>(*5) | (*5) <a href="https://utimaco.com/data-protection/gp-hsm/application-package/quantum-protect">https://utimaco.com/data-protection/gp-hsm/application-package/quantum-protect</a><br>LMS/HSS及びXMSS/XMSS-MT、ML-DSAは、追加機能（Quantum Protect）で対応を確認。SLH-DSAは開発中。                                                                                                                                                                                                                                                                                                                                                                                                       |
| Cisco     | Catalyst / IOS XE<br>【ネットワーク機器】      | ◎<br>(*6) | —         | ◎<br>(*6) | —         | (*6) <a href="https://www.cisco.com/c/en/us/td/docs/switches/lan/c9000/sec-crypto/tws/trustworthy-systems-guide/post-quantum-cryptography.html">https://www.cisco.com/c/en/us/td/docs/switches/lan/c9000/sec-crypto/tws/trustworthy-systems-guide/post-quantum-cryptography.html</a><br>LMSによるブートローダー署名検証、ML-DSA-87による署名検証への対応を確認。XMSS及びSLH-DSAについては確認できず。                                                                                                                                                                                                                                                                                                       |
| Infineon  | OPTIGA TPM SLB 9672<br>【TPM】         | —         | ◎<br>(*7) | —         | —         | (*7) <a href="https://www.infineon.com/ja/part/OPTIGA-TPM-SLB-9672-FW15">https://www.infineon.com/ja/part/OPTIGA-TPM-SLB-9672-FW15</a><br>(*8) <a href="https://trustedcomputinggroup.org/new-computing-specification-impliments-pqc-measures-to-protect-users-from-quantum-attacks/">https://trustedcomputinggroup.org/new-computing-specification-impliments-pqc-measures-to-protect-users-from-quantum-attacks/</a><br>XMSSを用いたPQC保護付きファームウェア更新機構への対応を確認。LMS、ML-DSA及びSLH-DSAについては対応を確認できず。                                                                                                                                                                    |
| TCG       | <TPM 2.0>                            | —         | —         | ◎<br>(*8) | —         | TPM等の仕様を策定する業界団体であるTCG（Trusted Computing Group）の最新TPM 2.0仕様（v1.85）では、PQC署名方式としてML-DSAを規定。（SLB 9672のXMSSの対応はInfineon独自の製品機能。）                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Microsoft | Windows Server 2025<br>【OS・PKI基盤】    | —         | —         | ◎<br>(*9) | —         | (*9) <a href="https://learn.microsoft.com/ja-jp/windows-server/identity/ad-cs/post-quantum-cryptography-overview">https://learn.microsoft.com/ja-jp/windows-server/identity/ad-cs/post-quantum-cryptography-overview</a><br>Windows Server 2025の標準機能であるActive Directory Certificate Services（AD CS）でML-DSAへの対応を確認。ML-DSAを用いたCA署名やコード署名証明書等に対応。LMS、XMSS及びSLH-DSAについては対応を確認できず。                                                                                                                                                                                                                                                                                    |

（凡例）◎：製品機能・標準仕様で対応 ○：追加機能で対応 △：開発中 —：対応を確認できず

# 課題②

## 諸外国動向調査

# 今回の調査について

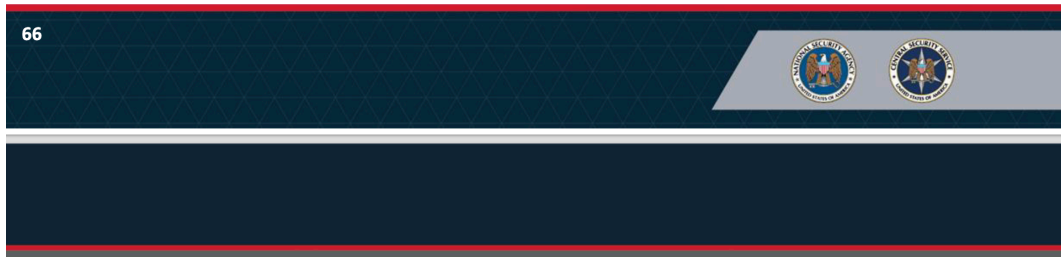
- 暗号利用モード、メッセージ認証コード、認証付き秘匿モード、認証暗号、Camellia、KCipher-2、SHAKE128、SHAKE256などに関する各国のCRQC対応について調査した。
- 調査方法
  - 諸外国で推奨されている暗号などが記載されている文献を調査対象とした。
  - 調査した文献の一覧をp.18-19に記載する。
- 諸外国の資料においてCRQC対応についての記載があった箇所を抜粋して掲載する。
- p.13以降に各用途別の調査結果を表にまとめる。記載例は以下とする。

|      | 記載基準                                                             |
|------|------------------------------------------------------------------|
| 推奨   | “耐量子計算機暗号として使用することを推奨”と記載が有る。<br>ただし、PQCコンペティションへの提出に関する推奨は除外する。 |
| 非推奨  | “耐量子計算機暗号として使用を推奨しない”と記載が有る。                                     |
| 記載なし | 参考とした文献には記載が無い                                                   |

# アメリカ

- NSA [US-1] 資料において、“公開鍵暗号では設計の根本的な変更が必要になる一方、共通鍵アルゴリズムは、鍵長が十分に大きければ安全であると考えられている。”（日本語訳）との記載があり、個別の暗号利用モードやハッシュ関数に関する記載はなかった。
- SHA-3、SHAKEにおいては、CNSA 2.0 における汎用ハッシュアルゴリズムとしての使用は推奨されておらず、その使用は限定されている。

Table 15. Approved CNSA 2.0 Algorithms for IPsec



| Security Service                   | Algorithm Suite     | Specifications                  |
|------------------------------------|---------------------|---------------------------------|
| Confidentiality (Encryption)       | AES-256- <b>GCM</b> | FIPS PUB 197                    |
| Authentication (Digital Signature) | ML-DSA-87           | FIPS 204                        |
| Key Establishment                  | ML-KEM-1024         | FIPS 203                        |
| Integrity (Hashing)                | SHA-384 or SHA-512  | FIPS PUB 180-4<br>IETF RFC 6234 |

[US-3] Mobile Access Capability Package Version 2.8.0, 27 March 2026より抜粋

## Q: Can I use SHA-3 as a hash?

A: No, neither SHA-3 nor **SHAKE** are approved for use in CNSA 2.0 as a general purpose hash algorithm. While NSA allows any parameter set of LMS, including some that call SHA-3 as a function, NSA has not approved SHA-3 as a general purpose hash algorithm. Its use is strictly limited to those cases where it is prescribed by the standard describing an NSA-approved algorithm, such as LMS within NIST SP 800-208, or for internal hardware system processes as described above.

The SHA-2 selections are sufficient for security, and their ubiquity in the commercial world ensures interoperability. Using SHA-3 or **SHAKE** outside those narrowly defined applications where it is completely self-contained, such as when called within an algorithm function, significantly increases the interoperability testing burden and breaks many use cases for CNSA 2.0.

## Q: Will quantum computers affect non-public-key (i.e., **symmetric**) algorithms?

A: Quantum computing techniques are generally considered much less effective against **symmetric** algorithms than against current widely used public-key algorithms. While public-key cryptography requires fundamental design changes, **symmetric** algorithms are considered secure, provided the key size is sufficiently large. CNSA 2.0 **symmetric** algorithms, which essentially are the same as their CNSA 1.0 counterparts, are quantum-resistant.

[US-1] The Commercial National Security Algorithm Suite2.0 and Quantum Computing FAQより抜粋

- 共通鍵暗号では、ブロックサイズが128ビット以上のブロック暗号のみを使用すべきで、ブロック暗号はAES-128、AES-192、AES-256を推奨する、との記載がある。
- 記述の抜粋と、推奨の一覧は以下のとおり。

### 3.1. Block Ciphers

**General Recommendations** A block cipher is an algorithm that encrypts a plaintext of fixed bit length (for example 128 bits) by means of a key to a ciphertext of the same bit length. This bit length is also called *block size* of the cipher. For the encryption of plaintexts of other lengths, block ciphers are applied in different modes, see [Section 3.1.1](#). For new cryptographic applications, only block ciphers whose block size is at least 128 bits should be used.

The following **block ciphers are recommended** for use in new cryptographic systems:

AES-128, AES-192, AES-256, see [\[93\]](#).

Table 3.1: Recommended block ciphers.

This is the case for the following **recommended modes of operation**, which are adequate for the block ciphers listed in [Table 3.1](#):

Federal Office for Information Security (BSI) 41

Technical Guideline – Cryptographic Algorithms and Key Lengths

- Modes of operation without data authentication:
  - Cipher Block Chaining (CBC), see [\[92\]](#), and
  - Counter Mode (CTR), see [\[92\]](#).
- Modes of operation with data authentication:
  - Counter with Cipher Block Chaining Message Authentication (CCM), see [\[94\]](#),
  - Galois/Counter Mode (GCM), see [\[95\]](#),
  - Galois/Counter Mode with Synthetic Initialization Vector for AES (AES-GCM-SIV), see [\[62\]](#).

Table 3.2: Recommended modes of operation for block ciphers.

- SHA-256, SHA-512/256, SHA-384 and SHA-512, see [\[99\]](#).
- SHA3-256, SHA3-384, SHA3-512, see [\[100\]](#).

Table 4.1: Recommended hash functions.

- CMAC, see [\[102\]](#),
- HMAC, see [\[11\]](#),
- KMAC128, KMAC256, see [\[101\]](#),
- GMAC, see [\[95\]](#).

Table 5.1: Recommended MAC schemes.

| Scheme                 | CMAC  | HMAC  | KMAC128 | KMAC256 | GMAC  |
|------------------------|-------|-------|---------|---------|-------|
| Key length             | ≥ 128 | ≥ 128 | ≥ 128   | ≥ 256   | ≥ 128 |
| Recommended tag length | ≥ 96  | ≥ 128 | ≥ 96    | ≥ 96    | ≥ 96  |

Table 5.2: Parameters for recommended MAC schemes.

# オランダ

- 共通鍵暗号では、256ビット鍵の使用を推奨し、128ビット鍵も許容可能な代替、としている。
- 記述の抜粋と、推奨の一覧は以下のとおり。

## 4.2.3 Symmetric-Key Cryptography

Theoretically, symmetric-key primitives can be attacked by Grover’s quantum algorithm in quadratically fewer steps than a classical brute-force attack. This suggests a halving of the security level, which can be counteracted by doubling the key length. More concretely, this implies that a key length of 128 bits should be avoided, and 256 bit keys are advisable. However, a more detailed analysis of the Grover quantum attack shows that its costs are at least comparable to the costs of a classical attack [JNRV20]. The main reason is that, unlike the quantum attack, the classical attack can be parallelised. Therefore, it is likely that 128 bit symmetric-key primitives will remain secure far beyond the realisation of quantum computers capable of breaking asymmetric-key primitives.

In general, we recommend the use of 256 bit keys when possible and consider 128-bit keys an acceptable alternative. The key takeaway is that organisations should prioritise the migration of asymmetric-key primitives. In fact, we recommend that organisations only allocate resources to increasing symmetric key lengths if they have migrated all of their asymmetric primitives to post-quantum alternatives.

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

<sup>1</sup> Recommended to be deployed in a hybrid combination with ECDH. <sup>2</sup> Recommended to be deployed in a hybrid combination with either ECDSA or EdDSA. <sup>3</sup> 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.

| Functionality                                         | Type       | Recommended                                   | Acceptable                                             | Deprecated                                                   |
|-------------------------------------------------------|------------|-----------------------------------------------|--------------------------------------------------------|--------------------------------------------------------------|
| Key Exchange/<br>Key Encapsulation                    | Asymmetric | ML-KEM <sup>1</sup>                           | FrodoKEM <sup>1</sup><br>Classic McEliece <sup>1</sup> | ECDH <sup>3</sup> RSA <sup>3</sup>                           |
| Digital Signature<br>– Stateless                      | Asymmetric | ML-DSA <sup>2</sup><br>SLH-DSA                | FN-DSA <sup>2</sup>                                    | ECDSA <sup>3</sup><br>EdDSA <sup>3</sup><br>RSA <sup>3</sup> |
| Digital Signature<br>– Stateful                       | Asymmetric | XMSS<br>LMS<br>HSS                            |                                                        |                                                              |
| Hash Function                                         | Hash       | SHA-2<br>SHA-3                                | BLAKE2                                                 | MD5<br>SHA-1                                                 |
| Block Cipher                                          | Symmetric  | AES                                           | Camellia                                               | (T)DES<br>IDEA<br>Blowfish                                   |
| Stream Cipher                                         | Symmetric  | AES-CTR<br>ChaCha20                           |                                                        | RC4                                                          |
| Encryption                                            | Symmetric  | AES-CTR<br>ChaCha20                           |                                                        |                                                              |
| Authenticated<br>Encryption (with<br>Associated Data) | Symmetric  | AES-GCM(-SIV)<br>AES-OCB<br>ChaCha20-Poly1305 |                                                        |                                                              |
| Message<br>Authentication Code                        | Symmetric  | CMAC-AES<br>HMAC-SHA-2<br>KMAC                | CMAC-Camellia<br>BLAKE2-MAC                            | CBC-MAC                                                      |

<sup>1</sup> Recommended to be deployed in a hybrid combination with ECDH. <sup>2</sup> Recommended to be deployed in a hybrid combination with either ECDSA or EdDSA. <sup>3</sup> Secure against classical attacks and can be part of a hybrid scheme.

Table 4.1 | Cryptographic primitive recommendations.

# チェコ (1/4)

- 共通鍵暗号アルゴリズムについては、以下を推奨している。
  - ストリーム暗号よりもブロック暗号を使用すること。
  - ブロック暗号については、AES、Camellia、Serpent の順に優先すること。
  - 256ビットの鍵長を使用すること。

## Doporučujeme preferovat:

- Použití blokových šifer před proudovými.
- V případě blokových šifer: AES, Camellia a Serpent (v uvedeném pořadí).
- Délku klíče 256 bitů.

## Kvantová zranitelnost a kvantová odolnost:

- Všechny šifry s délkami klíčů 128 bitů a 192 bitů jsou kvantově zranitelné.
- Všechny šifry s délkou klíče 256 bitů jsou kvantově odolné.

**Kvantová odolnost:** Všechny schválené módy symetrické kryptografie jsou kvantově odolné, pokud jsou kvantově odolné symetrické šifry a hašovací funkce, které jsou v nich použity.

[CZ] Minimální požadavky na kryptografické algoritmyより抜粋

## (日本語訳)

### 量子脆弱性および量子耐性

- 鍵長が 128ビットまたは192ビットのすべての暗号は、量子計算機に対して脆弱である。
- 鍵長が 256ビットのすべての暗号は、量子計算機耐性を有する。

---

### 量子耐性

承認されたすべての共通鍵暗号モードは、そのモードで使用される共通鍵暗号およびハッシュ関数が量子計算機耐性を有する場合、量子計算機耐性を有する。

# チェコ (2/4)

## ●暗号利用モードなどの推奨は以下のとおり。

### d) Módy šifrování pro složená schémata typu „Encrypt-then-MAC“

1. CTR
2. OFB
3. CBC (rovněž CBC-CS)
4. CFB

#### Upozornění:

- Módy CBC a CFB musí být použity s náhodným, pro útočníka nepředpověditelným, inicializačním vektorem.
- Při použití módu OFB se pro daný klíč nesmí opakovat hodnota inicializačního vektoru.
- Při použití módu CTR se pro daný klíč nesmí opakovat hodnota čítače.
- Samostatné použití módů šifrování mimo schémata typu „Encrypt-then-MAC“ není schváleno.

### d) 「Encrypt-then-MAC」型合成方式で使用する暗号化モード

1. CTR
2. OFB
3. CBC (CBC-CSを含む)
4. CFB

#### 注意事項

- CBCおよびCFBは、ランダムであり、かつ攻撃者にとって予測不可能な初期化ベクトルとともに使用しなければならない。
- OFBを使用する場合、同一鍵について初期化ベクトルの値を再使用してはならない。
- CTRを使用する場合、同一鍵についてカウンタ値を再使用してはならない。
- 「Encrypt-then-MAC」型方式の外で、これらの暗号化モードを単独で使用することは承認されない。

[CZ] Minimální požadavky na kryptografické algoritmyより抜粋

日本語訳

# チェコ (3/4)

## ●MACなどの推奨は以下のとおり。

### e) Módy pro ochranu integrity (Message Authentication Code – MAC)

1. HMAC pouze s hašovací funkcí z kapitoly 5
2. CMAC
3. KMAC
4. GMAC s inicializačním vektorem dlouhým 96 bitů a s tagem dlouhým 128 bitů
5. EMAC<sup>2</sup>
6. UMAC<sup>2</sup>

### Upozornění:

- Při použití módu GMAC se pro daný klíč nesmí opakovat hodnota inicializačního vektoru. Nejpozději po  $2^{32}$  hodnotách inicializačního vektoru musí dojít k výměně klíče.
- Při použití módu UMAC se pro daný klíč nesmí opakovat hodnota inicializačního vektoru.
- U všech výše uvedených algoritmů musí být délka tagu alespoň 96 bitů, pokud není uvedeno jinak.

### 5 Algoritmy hašovacích funkcí

#### a) Hašovací funkce SHA-2

1. SHA-256
2. SHA-384
3. SHA-512
4. SHA-512/256

#### b) Hašovací funkce SHA-3

1. SHA3-256
2. SHA3-384
3. SHA3-512
4. SHAKE128
5. SHAKE256

#### c) Ostatní hašovací funkce

1. Whirlpool
2. BLAKE2

**Upozornění:** Všechny schválené hašovací funkce musí mít délku výstupu alespoň 256 bitů. Doporučujeme však preferovat délku výstupu alespoň 384 bitů.

#### Kvantová zranitelnost a kvantová odolnost:

- Všechny schválené hašovací funkce s délkou výstupu 384 bitů nebo větší jsou kvantově odolné.
- Všechny schválené hašovací funkce s délkou výstupu 256 bitů nebo menší jsou kvantově zranitelné.

### e) 完全性保護用モード (Message Authentication Code : MAC)

1. HMAC  
第5章に記載されたハッシュ関数との組合せに限る。
2. CMAC
3. KMAC
4. GMAC  
初期化ベクトルを96ビット、タグを128ビットとする。
5. EMAC<sup>2</sup>
6. UMAC<sup>2</sup>

### 注意事項

- GMACを使用する場合、同一鍵について初期化ベクトルの値を再使用してはならない。  
遅くとも  $2^{32}$  個の初期化ベクトルを使用した時点で、鍵を交換しなければならない。
- UMACを使用する場合、同一鍵について初期化ベクトルの値を再使用してはならない。
- 別途規定されていない限り、上記すべてのアルゴリズムについてタグ長を少なくとも96ビットとしなければならない。

### 5 ハッシュ関数アルゴリズム

#### a) SHA-2 ハッシュ関数

1. SHA-256
2. SHA-384
3. SHA-512
4. SHA-512/256

#### b) SHA-3 ハッシュ関数

1. SHA3-256
2. SHA3-384
3. SHA3-512
4. SHAKE128
5. SHAKE256

#### c) その他のハッシュ関数

1. Whirlpool
2. BLAKE2

### 注意事項

承認されたすべてのハッシュ関数は、出力長を少なくとも256ビットとしなければならない。ただし、出力長は少なくとも384ビットとすることを推奨する。

### 量子脆弱性および量子耐性

出力長が384ビット以上の承認されたすべてのハッシュ関数は、量子計算機耐性を有する。出力長が256ビット以下の承認されたすべてのハッシュ関数は、量子計算機に対して脆弱である。

# チェコ (4/4)

## ● 認証付き秘匿モード、認証暗号などでの推奨は以下のとおり。

### c) Módy autentizovaného šifrování

1. CCM
2. EAX
3. OCB1 a OCB3, doporučujeme preferovat OCB3 před OCB1
4. GCM s inicializačním vektorem dlouhým 96 bitů a s tagem dlouhým 128 bitů
5. ChaCha20 + Poly1305 se zatížením klíče menším než 256 GB
6. Složená schémata typu „Encrypt-then-MAC“

### Upozornění

- Schválené módy šifrování musí používat blokové šifry uvedené v kapitole 2 písm. a).
- Složená schémata typu „Encrypt-then-MAC“ musí k výpočtu MAC používat pouze módy pro ochranu integrity uvedené v kap. 2 písm. e) a k šifrování pouze módy šifrování uvedené v kap. 2 písm. d), nebo v případě šifrování disků i módy uvedené v kap. 2 písm. f). Zároveň tato schémata nesmí pro šifrování a pro výpočet MAC používat stejný klíč.
- Inicializační vektor musí být součástí vstupu pro výpočet MAC.
- Při použití módu GCM se pro daný klíč nesmí opakovat hodnota inicializačního vektoru. Nejpozději po  $2^{32}$  hodnotách inicializačního vektoru musí dojít k výměně klíče.

[CZ] Minimální požadavky na kryptografické algoritmyより抜粋

### c) 認証暗号モード

1. CCM
2. EAX
3. OCB1 および OCB3  
OCB1 より OCB3 を優先して使用することを推奨する。
4. GCM  
初期化ベクトルを96ビット、タグを128ビットとする。
5. ChaCha20 + Poly1305  
同一鍵で処理するデータ量を 256 GB 未満とする。
6. 「Encrypt-then-MAC」型の合成方式

### 注意事項

- 承認された暗号モードでは、本章 a) に記載されたブロック暗号を使用しなければならない。
- 「Encrypt-then-MAC」型の合成方式では、MACの計算には本章 e) に記載された完全性保護用モードのみを使用し、暗号化には本章 d) に記載された暗号化モードのみを使用しなければならない。  
ディスク暗号化の場合は、本章 f) に記載されたモードを使用することもできる。  
また、暗号化とMAC計算に同一の鍵を使用してはならない。
- 初期化ベクトルをMAC計算の入力に含めなければならない。
- GCMを使用する場合、同一鍵について初期化ベクトルの値を再使用してはならない。  
遅くとも  $2^{32}$  個の初期化ベクトルを使用した時点で、鍵を交換しなければならない。

<sup>1</sup> ここでいう「同一鍵で処理するデータ量 (key load)」とは、同一の鍵で暗号化してよいデータの最大量を意味する。

# スロバキア（1/2）

## ●共通鍵暗号では、少なくとも256ビット長の鍵の使用を推奨する、と記載がある。

### Symetrické algoritmy

#### Odporúčanie pre symetrické algoritmy:

Pri používaní symetrických algoritmov, či už blokových alebo prúdových, odporúčame používať kľúče s dĺžkou minimálne 256 bitov, aby bola zabezpečená vysoká odolnosť aj v budúcnosti voči kvantovým útokom.

Použitie 192 alebo 128 bitových kľúčov je možné, avšak efektívna bezpečnosť v takom prípade klesá, najmä pri potenciálnych kvantových hrozbách.

Preferujeme blokové šifry pred prúdovými, pretože poskytujú vyššiu odolnosť proti rôznym typom útokov a umožňujú flexibilnejšie využitie v rôznych bezpečnostných režimoch.

#### Blokové šifry

Odporúčané dĺžky kľúčov sú aktuálne najväčšie podporované dĺžky pre dané algoritmy.

**Advanced Encryption Standard (AES)** [\[1\]](#) s dĺžkou kľúča 256 bitov

**Camellia** s dĺžkou kľúča 256 bitov [\[2\]](#)

**Twofish** s dĺžkou kľúča 256 bitov

**Serpent** s dĺžkou kľúča 256 bitov

#### Prúdové šifry

Odporúčané dĺžky kľúčov sú aktuálne najväčšie podporované dĺžky pre dané algoritmy.

**ChaCha20** [\[3\]](#) s dĺžkou kľúča 256 bitov a obmedzením využitia kľúča na menej než 256 GB dát  
**SNOW 3G** [\[4\]](#) s dĺžkou kľúča 256 bitov

Dôvod výberu:

Groverov kvantový algoritmus (Lov Grover -1996 ) umožňuje hľadanie kľúčov ľubovoľného kryptografického systému hrubou silou, ktorý je však tiež podstatne menej efektívny než Shorov algoritmus. Dôsledkom je, že za bezpečné voči Groverovmu algoritmu považujeme iba tie blokové a prúdové šifry, ktoré majú kľúče dlhé 256 bitov alebo viac.

[SK] Odporúčania pre kryptografické algoritmyより抜粋

### 共通鍵アルゴリズム

#### 共通鍵アルゴリズムに関する推奨

ブロック暗号またはストリーム暗号のいずれであるかを問わず、共通鍵アルゴリズムを使用する場合には、将来の量子攻撃に対しても高い耐性を確保するため、**少なくとも256ビット長の鍵を使用することを推奨する。**

192ビットまたは128ビットの鍵を使用することも可能であるが、その場合、特に将来的な量子脅威を考慮すると、実効的な安全性は低下する。

ブロック暗号は、さまざまな種類の攻撃に対してより高い耐性を有し、またさまざまなセキュリティモードにおいてより柔軟に利用できることから、**ストリーム暗号よりもブロック暗号を優先する。**

#### ブロック暗号

推奨する鍵長は、現時点で各アルゴリズムがサポートする最大の鍵長である。

- Advanced Encryption Standard (AES) [\[1\]](#): **256ビット鍵**
- Camellia [\[2\]](#): **256ビット鍵**
- Twofish: **256ビット鍵**
- Serpent: **256ビット鍵**

#### ストリーム暗号

推奨する鍵長は、現時点で各アルゴリズムがサポートする最大の鍵長である。

- ChaCha20 [\[3\]](#): **256ビット鍵**、かつ1つの鍵で使用するデータ量を256 GB未満に制限
- SNOW 3G [\[4\]](#): **256ビット鍵**

#### 選定理由

Groverの量子アルゴリズム（原文表記：“Lov Grover -1996”）を用いると、任意の暗号システムに対する総当たりによる鍵探索が可能になるが、これはShorのアルゴリズムと比べると大幅に効率が低い。

その結果、本書では、**鍵長が256ビット以上であるブロック暗号およびストリーム暗号のみを、Groverのアルゴリズムに対して安全であるとみなす。**

日本語訳

# スロバキア（2/2）

## ●SHAKEに関しては、SHAKE256のみを推奨し、256 bit以上の出力長としている。

### Algoritmy digitálneho odtlačku (hash funkcie)

#### SHA-2

SHA-384 [\[12\]](#)  
SHA-512 [\[12\]](#)

#### SHA-3

SHA3-384 [\[13\]](#)  
SHA3-512 [\[13\]](#)  
SHAKE256 [\[13\]](#)

#### Ostatné

BLAKE2 [\[14\]](#) (s výstupom  $\geq 384$  bitov)

#### Odporúčanie:

Všetky schválené algoritmy digitálneho odtlačku funkcie by mali mať výstup aspoň 256 bitov, ale pre kvantovú odolnosť odporúčame dĺžku minimálne 384 bitov.

Funkcie s výstupom 384 bitov a viac sú považované za kvantovo odolné, zatiaľ čo tie s 256 bitmi alebo menej sú kvantovo zraniteľné.

#### Dôvod výberu:

BHT-algoritmus (Brassard, Høyer a Tapp - 1997) vychádzajúci z Groverovho algoritmu znižuje náročnosť hľadania kolízií hašovacích funkcií v porovnaní s klasickými algoritmami hľadajúcimi kolízie na báze narodeninového paradoxu. Za bezpečné voči útoku zmieneným kvantovým algoritmom dnes považujeme iba tie hašovacie funkcie, ktorých výstupy sú dlhé aspoň 384 bitov.

Ostatné algoritmy digitálneho odtlačku, napríklad SHA-256 alebo SHA3-256, sú pri kvantových útokoch menej bezpečné a preto sa neodporúčajú pre kritické aplikácie. Stačí nahradiť hašovacie funkcie s dĺžkou výstupu 256 bitov hašovacími funkciami s dĺžkou výstupu 384 bitov.

### ハッシュ関数

#### SHA-2

SHA-384 [\[12\]](#)  
SHA-512 [\[12\]](#)

#### SHA-3

SHA3-384 [\[13\]](#)  
SHA3-512 [\[13\]](#)  
SHAKE256 [\[13\]](#)

#### その他

BLAKE2 [\[14\]](#) (出力長 384ビット以上)

#### 推奨

承認されたすべてのハッシュ関数は、少なくとも256ビットの出力長を持つべきである。

ただし、量子計算機に対する耐性を考慮する場合には、**少なくとも384ビットの出力長を推奨する**。

出力長が384ビット以上の関数は量子計算機耐性を有するとみなす一方、出力長が256ビット以下のものは量子攻撃に対して脆弱であるとみなす。

#### 選定理由

Groverのアルゴリズムを基礎とするBHTアルゴリズム (Brassard, Høyer and Tapp, 1997) は、誕生日パラドックスに基づく古典的な衝突探索アルゴリズムと比較して、ハッシュ関数の衝突探索の計算量を削減する。

この量子アルゴリズムによる攻撃に対して安全であると現在みなしているのは、**出力長が少なくとも384ビットであるハッシュ関数のみ**である。

SHA-256やSHA3-256など、その他のハッシュ関数は量子攻撃に対する安全性がより低いため、**重要な用途には推奨しない**。

出力長256ビットのハッシュ関数を、出力長384ビットのハッシュ関数に置き換えればよい。

## 日本語訳

- SHAKEは、ML-KEM、一部のデジタル署名方式、KMAC等との組合せに限って推奨しているが、SHAKE自体を耐量子計算機暗号として推奨しているとの明示的な記載はない。

## 8.1 SHAKE

We recommend SHAKE128, as specified in [NIST FIPS 202: SHA-3 Standard: Permutation Based Hash and Extendable-Output Functions](#), for use in the following:

- ML-KEM ([section 5.4 Module-Lattice-Based Key-Encapsulation Mechanism](#))
- The digital signature schemes
  - RSA ([section 6.1 Rivest-Shamir-Adelman](#))
  - ECDSA ([section 6.3 Elliptic Curve Digital Signature Algorithm](#))
  - ML-DSA ([section 6.5 Module-Lattice-Based Digital Signature Algorithm](#))
- KECCAK Message Authentication Code (KMAC) ([section 9.4 KECCAK Message Authentication Code](#))

We recommend SHAKE256, as specified in [NIST FIPS 202: SHA-3 Standard: Permutation Based Hash and Extendable-Output Functions](#), for use in the following:

- ML-KEM ([section 5.4 Module-Lattice-Based Key-Encapsulation Mechanism](#))
- The digital signature schemes
  - RSA ([section 6.1 Rivest-Shamir-Adelman](#))
  - ECDSA ([section 6.3 Elliptic Curve Digital Signature Algorithm](#))
  - EdDSA ([section 6.4 Edwards Curve Digital Signature Algorithm](#)) with curve Edwards448
  - ML-DSA ([section 6.5 Module-Lattice-Based Digital Signature Algorithm](#))
  - SLH-DSA ([section 6.6 Stateless Hash-Based Digital Signature Algorithm](#))
  - Stateful hash-based digital signature schemes ([section 6.7 Stateful hash-based signature schemes](#))
- KMAC ([section 9.4 KECCAK Message Authentication Code](#))

# 暗号利用モード

| 国・機関     | CBC  | CFB  | OFB  | CTR  | XTS  | 参考文献・引用ページ            |
|----------|------|------|------|------|------|-----------------------|
| 米国       | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし |                       |
| 英国       | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし |                       |
| カナダ      | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし |                       |
| オーストラリア  | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし |                       |
| ニュージーランド | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし |                       |
| フランス     | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし |                       |
| ドイツ      | 推奨   | 記載なし | 記載なし | 推奨   | 記載なし | [DE] pp.40, 42        |
| オランダ     | 記載なし | 記載なし | 記載なし | 推奨   | 記載なし | [NL] pp.57, 59, 92-93 |
| スペイン     | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし |                       |
| チェコ      | 推奨   | 推奨   | 推奨   | 推奨   | 推奨   | [CZ] p.5              |
| スロバキア    | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし |                       |
| フィンランド   | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし |                       |
| ノルウェー    | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし |                       |
| マレーシア    | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし |                       |

# メッセージ認証コード(MAC)など

| 国・機関     | HMAC | CMAC | GMAC | KMAC | Poly1305 | 参考文献・引用ページ            |
|----------|------|------|------|------|----------|-----------------------|
| 米国       | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし     |                       |
| 英国       | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし     |                       |
| カナダ      | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし     |                       |
| オーストラリア  | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし     |                       |
| ニュージーランド | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし     |                       |
| フランス     | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし     |                       |
| ドイツ      | 推奨   | 推奨   | 推奨   | 推奨   | 記載なし     | [DE] pp.49–50         |
| オランダ     | 推奨   | 推奨   | 記載なし | 推奨   | 記載なし     | [NL] pp.57, 59, 94–95 |
| スペイン     | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし     |                       |
| チェコ      | 推奨   | 推奨   | 推奨   | 推奨   | 記載なし     | [CZ] p.5              |
| スロバキア    | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし     |                       |
| フィンランド   | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし     |                       |
| ノルウェー    | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし     |                       |
| マレーシア    | 記載なし | 記載なし | 記載なし | 記載なし | 記載なし     |                       |

# 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 | 参考文献<br>引用ページ         |
|----------|------|------|-------------|--------|---------|-------------------|------------------|-----------------------|
| 米国       | 記載なし | 記載なし | 記載なし        | 推奨(※1) | 記載なし    | 記載なし              | 記載なし             | [US-3]                |
| 英国       | 記載なし | 記載なし | 記載なし        | 記載なし   | 記載なし    | 記載なし              | 記載なし             |                       |
| カナダ      | 記載なし | 記載なし | 記載なし        | 記載なし   | 記載なし    | 記載なし              | 記載なし             |                       |
| オーストラリア  | 記載なし | 記載なし | 記載なし        | 記載なし   | 記載なし    | 記載なし              | 記載なし             |                       |
| ニュージーランド | 記載なし | 記載なし | 記載なし        | 記載なし   | 記載なし    | 記載なし              | 記載なし             |                       |
| フランス     | 記載なし | 記載なし | 記載なし        | 記載なし   | 記載なし    | 記載なし              | 記載なし             |                       |
| ドイツ      | 推奨   | 記載なし | 記載なし        | 推奨     | 推奨      | 記載なし              | 記載なし             | [DE] pp.40, 42        |
| オランダ     | 記載なし | 記載なし | 推奨          | 推奨     | 推奨      | 推奨                | 記載なし             | [NL] pp.57, 59, 92-95 |
| スペイン     | 記載なし | 記載なし | 記載なし        | 記載なし   | 記載なし    | 記載なし              | 記載なし             |                       |
| チェコ      | 推奨   | 推奨   | 推奨          | 推奨     | 記載なし    | 推奨                | 推奨               | [CZ] pp.4-5           |
| スロバキア    | 記載なし | 記載なし | 記載なし        | 記載なし   | 記載なし    | 記載なし              | 記載なし             |                       |
| フィンランド   | 記載なし | 記載なし | 記載なし        | 記載なし   | 記載なし    | 記載なし              | 記載なし             |                       |
| ノルウェー    | 記載なし | 記載なし | 記載なし        | 記載なし   | 記載なし    | 記載なし              | 記載なし             |                       |
| マレーシア    | 記載なし | 記載なし | 記載なし        | 記載なし   | 記載なし    | 記載なし              | 記載なし             |                       |

※1 CNSA 2.0のAES-256-GCMのみで推奨

# Camellia、KCipher-2、SHAKE128、SHAKE256

| 国・機関     | Camellia | KCipher-2 | SHAKE128 | SHAKE256 | 参考文献・引用ページ      |
|----------|----------|-----------|----------|----------|-----------------|
| 米国       | 記載なし     | 記載なし      | 記載なし(※2) | 記載なし(※2) | [US-1] PDF p.8  |
| 英国       | 記載なし     | 記載なし      | 記載なし     | 記載なし     |                 |
| カナダ      | 記載なし     | 記載なし      | 記載なし(※3) | 記載なし(※3) | [CA] §8.1, p.19 |
| オーストラリア  | 記載なし     | 記載なし      | 記載なし     | 記載なし     |                 |
| ニュージーランド | 記載なし     | 記載なし      | 記載なし     | 記載なし     |                 |
| フランス     | 記載なし     | 記載なし      | 記載なし     | 記載なし     |                 |
| ドイツ      | 記載なし     | 記載なし      | 記載なし     | 記載なし     |                 |
| オランダ     | 推奨       | 記載なし      | 推奨       | 推奨       | [NL] pp.57-58   |
| スペイン     | 記載なし     | 記載なし      | 記載なし     | 記載なし     |                 |
| チェコ      | 非推奨(※4)  | 記載なし      | 非推奨(※6)  | 非推奨(※6)  | [CZ] pp.4, 9    |
|          | 推奨(※5)   |           | 推奨(※7)   | 推奨(※7)   |                 |
| スロバキア    | 推奨       | 記載なし      | 記載なし     | 非推奨(※6)  | [SK] pp.4, 7    |
|          |          |           |          | 推奨(※7)   |                 |
| フィンランド   | 記載なし     | 記載なし      | 記載なし     | 記載なし     |                 |
| ノルウェー    | 記載なし     | 記載なし      | 記載なし     | 記載なし     |                 |
| マレーシア    | 記載なし     | 記載なし      | 記載なし     | 記載なし     |                 |

※2 : NSA CNSA 2.0の汎用用途は非推奨

※3 §8.1の指定用途 (ML-KEM、RSA・ECDSA・KMAC等) では推奨しているが、耐量子計算機暗号として推奨するとの記載はない

※4 鍵長 128, 192 bit

※5 鍵長 256 bit

※6 出力長 ≤ 256 bit において

※7 出力長 ≥ 384 bit において

# 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(米国)

| 番号    | 公式資料                                                                                                                         |
|-------|------------------------------------------------------------------------------------------------------------------------------|
| US-1  | <a href="#">NSA, The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ, Ver. 2.1, December 2024</a> |
| US-2  | <a href="#">NSA, CSfC Capability Packages</a>                                                                                |
| US-3  | <a href="#">NSA, Mobile Access Capability Package Version 2.8.0, 27 March 2026</a>                                           |
| US-4  | <a href="#">NSA, Multi-Site Connectivity Capability Package Version 1.3.0, 27 March 2026</a>                                 |
| US-5  | <a href="#">NSA, Data-at-Rest Capability Package Version 5.1.0, March 2026</a>                                               |
| US-6  | <a href="#">NSA, Symmetric Key Management Requirements Annex Version 3.0.0, 27 March 2026</a>                                |
| US-7  | <a href="#">NIST IR 8547 Initial Public Draft, Transition to Post-Quantum Cryptography Standards Nov 2024</a>                |
| US-8  | <a href="#">NIST Post-Quantum Cryptography FAQ Aug 2026</a>                                                                  |
| US-9  | <a href="#">NIST SP 800-38A, CBC・CFB・OFB・CTR Dec 2001</a>                                                                    |
| US-10 | <a href="#">NIST Message Authentication Codes Jun 2025 / SP 800-185 (KMAC, Dec 2016)</a>                                     |
| US-11 | <a href="#">NIST SP 800-38B, CMAC May 2005 (Updated Oct 2016)</a>                                                            |
| US-12 | <a href="#">NIST SP 800-38C, CCM May 2004 (Errata Jul 2007)</a>                                                              |
| US-13 | <a href="#">NIST SP 800-38D, GCM・GMAC Nov 2007</a>                                                                           |
| US-14 | <a href="#">NIST SP 800-38E, XTS-AES Jan 2010 / Rev.1 IPD Sep 2026</a>                                                       |

# 参考文献(米国以外)

---

- [CA] カナダ Cyber Centre, ITSP.40.111, Version 5 May 2026 [www.cyber.gc.ca](http://www.cyber.gc.ca) (資料)
- [FR] フランス ANSSI, Follow-up position paper on post-quantum cryptography Dec 2023 [messervices.cyber.gouv.fr](http://messervices.cyber.gouv.fr) (資料) + プロトコル別移行資料 Feb 2026
- [DE] ドイツ BSI, BSI TR-02102-1, Cryptographic Mechanisms: Recommendations and Key Lengths Jan 2026 [www.bsi.bund.de](http://www.bsi.bund.de) (資料)
- [NL] オランダ AIVD/CWI/TNO, The PQC Migration Handbook Dec 2024 [english.aivd.nl](http://english.aivd.nl) (資料)
- [ES] スペイン CCN, CCN-TEC 009, Recomendaciones para una transición postcuántica segura July 2026 [www.ccn.cni.es](http://www.ccn.cni.es) (資料)
- [CZ] チェコ NÚKIB, Minimální požadavky na kryptografické algoritmy, v4.1, 2026-03-04 [portal.nukib.gov.cz](http://portal.nukib.gov.cz) (資料)
- [SK] スロバキア NBÚ, Odporúčania pre kryptografické algoritmy, v1.0 2025-10-08 [www.nbu.gov.sk](http://www.nbu.gov.sk) (資料)
- [FI] フィンランド Traficom, Kryptografiset vahvuusvaatimukset – kansalliset turvallisuusluokat, 2024-12-09 [kyberturvallisuuskeskus.fi](http://kyberturvallisuuskeskus.fi) (資料)
- [NO] ノルウェー NSM, NSM Cryptographic Recommendations Mar 2025 [nsm.no](http://nsm.no) (資料)
- [UK] 英国 NCSC, Next steps (PQC) Aug 2024 [www.ncsc.gov.uk](http://www.ncsc.gov.uk) (資料) + 移行日程 Mar 2025
- [MY] マレーシア CyberSecurity Malaysia, MySEAL 2.1 Approved Cryptographic Algorithms [mykripto.cybersecurity.my](http://mykripto.cybersecurity.my) (資料) + 2026-2030計画
- [AU] オーストラリア ASD, Information Security Manual, Guidelines for cryptography Sep 2026 [www.cyber.gov.au](http://www.cyber.gov.au) (資料)
- [NZ] ニュージーランド GCSB/NCSC, New Zealand Information Security Manual Nov 2025 [nzism.gcsb.govt.nz](http://nzism.gcsb.govt.nz) (資料)

**課題①**

**Category 1・2の暗号等の取扱い 等**  
**(第1・2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、その書き方や定義について修正すべき点はないか。

## 【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、**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     | パラメータセット (注8)                                       |
| 公開鍵暗号  | 署名  | —      | —                                                   |
|        | 鍵共有 | ML-KEM | ML-KEM-768 (Category 3)<br>ML-KEM-1024 (Category 5) |
| 共通鍵暗号  |     | AES    | AES-192 (Category 3)<br>AES-256 (Category 5)        |
| ハッシュ関数 |     | SHA2   | SHA-384 (Category 4)<br>SHA-512                     |
|        |     | SHA3   | SHA3-384 (Category 4)<br>SHA3-512                   |

変更

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

(注8) 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)

## 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。

## 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  |

## 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。

# (参考) カテゴリ関連記載 : FIPS 203・204・205

## FIPS203 “Module-Lattice-Based Key-Encapsulation Mechanism Standard”

<https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.203.pdf>

### 8. Parameter Sets (抜粋)

Concretely, **ML-KEM-512** is claimed to be in security **category 1**, **ML-KEM-768** is claimed to be in security **category 3**, and **ML-KEM-1024** is claimed to be in security **category 5**.

Table 2. Approved parameter sets for ML-KEM

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

## FIPS204 “Module-Lattice-Based Digital Signature Standard”

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

### 4. Parameter Sets (抜粋)

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

Table 1. ML-DSA parameter sets

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

# 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、何を記載すべきか。

## 【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<sup>4</sup>。

| 技術分類   |     | 暗号技術   |                           | セキュリティカテゴリ <sup>(注8)</sup> |
|--------|-----|--------|---------------------------|----------------------------|
| 公開鍵暗号  | 署名  | —      | —                         | —                          |
|        | 鍵共有 | ML-KEM | ML-KEM-768<br>ML-KEM-1024 | Category 3<br>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 <sup>(注9)</sup> |
|        |     | SHA3   | SHA3-384                  | Category 4                 |
|        |     |        | SHA3-512                  | Category 4 <sup>(注9)</sup> |

（注8）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。

# 検討ポイント③ Category 1・2の取扱い

**確認中**(ML-DSA/SLH-DSA部分)

- **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-DSA-44（Category 2）が広く利用される可能性もあることから、ML-DSA・SLH-DSA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**。
- ✓ **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    | セキュリティ<br>カテゴリ(注8)                   |
|--------|------|---------|--------------------------------------|
| 公開鍵暗号  | 署名   | ML-DSA  | ML-DSA-44(注) Category 2              |
|        |      |         | ML-DSA-65 Category 3                 |
|        |      |         | ML-DSA-87 Category 5                 |
|        |      | SLH-DSA | SLH-DSA-SHA2-128[s/f](注) Category 1  |
|        |      |         | SLH-DSA-SHAKE-128[s/f](注) Category 1 |
|        |      |         | SLH-DSA-SHA2-192[s/f] Category 3     |
|        | 鍵共有  |         | SLH-DSA-SHAKE-192[s/f] Category 3    |
|        |      |         | SLH-DSA-SHA2-256[s/f] Category 5     |
|        |      |         | SLH-DSA-SHAKE-256[s/f] Category 5    |
|        |      | ML-KEM  | ML-KEM-512 Category 1                |
| 共通鍵暗号  | AES  |         | ML-KEM-768 Category 3                |
|        |      |         | ML-KEM-1024 Category 5               |
|        |      |         |                                      |
| ハッシュ関数 | SHA2 |         | AES-128 Category 1                   |
|        |      |         | AES-192 Category 3                   |
|        |      |         | AES-256 Category 5                   |
|        |      |         |                                      |
|        | SHA3 |         | SHA-256 Category 2                   |
|        |      |         | SHA-512/256 Category 2               |
|        |      |         | SHA-384 Category 4                   |
|        |      |         | SHA-512 Category 4(注9)               |
|        |      |         | SHA3-256 Category 2                  |
|        |      |         | SHA3-384 Category 4                  |
|        |      |         | SHA3-512 Category 4(注9)              |

※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<br>(BSI) | フランス<br>(ANSSI) | オランダ<br>(AIVD) | オーストラリア<br>(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 <sup>1</sup> | ML-KEM-1024 <sup>1</sup>                                       | ML-KEM-768 <sup>1</sup>       |
| ML-DSA <sup>3</sup> | ML-DSA-87 <sup>2</sup>                                         | ML-DSA-65 <sup>2</sup>        |
| SLH-DSA             | SLH-DSA-(SHA2/SHAKE)-256(s/f)<br>SLH-DSA-(SHA2/SHAKE)-192(s/f) | SLH-DSA-(SHA2/SHAKE)-128(s/f) |
| AES                 | AES-256                                                        | AES-128                       |
| SHA-3               | SHA-3-256<br>SHA-3-384<br>SHA-3-512<br>(c)SHAKE256             | SHA-3-224 (c)SHAKE128         |
| SHA-2               | SHA-256<br>SHA-384<br>SHA-512                                  | SHA-224                       |

<sup>1</sup> Recommended to be deployed in a hybrid combination with ECDH. <sup>2</sup> Recommended to be deployed in a hybrid combination with either ECDSA or EdDSA. <sup>3</sup> 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) ML-DSA・SLH-DSAのIETFでの標準化状況

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

- ✓ **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SSHM 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

12

確認中

| 暗号技術    |                                                | Cloudflare<br>1.1.1.1 <sup>(*1)</sup><br>【DNSSEC】 | Cloudflare <sup>(*2)</sup><br>【オリジン認証】 | GoogleCloud<br>KMS <sup>(*3)</sup><br>【電子署名】 | AWS KMS <sup>(*4)</sup><br>【電子署名】 | OpenSSL 3.5 <sup>(*5)</sup><br>【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]-<br>128[s/f] (Category 1) | —                                                 | —                                      | 対応<br>(SHA2-128sのみ)                          | —                                 | 対応                                       |
|         | SLH-DSA-[SHA2/SHAKE]-<br>192[s/f] (Category 3) | —                                                 | —                                      | —                                            | —                                 | 対応                                       |
|         | SLH-DSA-[SHA2/SHAKE]-<br>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/>

- ✓ ML-DSA-44／ML-DSA-65／ML-DSA-87のセキュリティカテゴリは、Category 2／Category 3／Category 5に分類される。
- ✓ これらのセキュリティカテゴリを確保するためには、鍵生成に用いる乱数生成器の安全性強度にも留意する必要がある。
  - ✓ ML-DSA-44：192ビット以上の安全性強度が推奨
  - ✓ ML-DSA-65：192ビット以上の安全性強度が要求
  - ✓ ML-DSA-87：256ビット以上の安全性強度が要求
- ✓ ML-DSA-44については、128ビット以上192 ビット未満の乱数生成器の使用も許容されているが、その場合、セキュリティカテゴリはCategory 2からCategory 1に低下する。

→ML-DSA-44を掲載する場合、「Category 2」と現状記載しているが注記が必要ではないか。

例) 鍵生成に用いる乱数生成器のセキュリティ強度が128ビット以上192ビット未満の場合、セキュリティカテゴリはCategory 1に低下する。

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  $\xi$ . The seed  $\xi$  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.

# 検討ポイント④ Camellia・KCipher-2・SHAKEの取扱い

**確認中**

- 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⑤ 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※<sup>1</sup>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⑥）

### ＜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※<sup>1</sup>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**※<sup>2</sup>。
- ✓ 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

16

## 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)

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。

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<br>(ビット) | Q1モデルで安全性が<br>期待できる範囲                    |
|----------------|-------------------------------|-------------|------------------------------------------|
| ブロック暗号         | AES,<br>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,<br>CTR,<br>OFB, XTS | k           | 時間 $\leq 2^k$ かつ 古典的に<br>安全性が保障される範囲     |
| 認証付き<br>秘匿モード  | CCM, GCM                      | k           | 時間 $\leq 2^k$ かつ 古典的に<br>安全性が保障される範囲     |
| メッセージ<br>認証コード | CMAC,<br>HMAC                 | k           | 時間 $\leq 2^k$ かつ 古典的に<br>安全性が保障される範囲     |
| 認証暗号           | ChaCha20-<br>Poly1305         | 256         | 時間 $\leq 2^{128}$ かつ 古典的に<br>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     | —      |                   |                               |                               |
| SHA-512/256 | —      | 256               | $2^{85.3}$                    | $2^{85.3}$                    |
| 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⑥ 暗号利用モード等に関する注釈

**全面修正**  
前回と同じ

- 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伴い、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】

- ✓ 表2に暗号利用モード及びメッセージ認証コードを掲載することに伴い、**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。
- ✓ 従来から、「電子政府推奨暗号リスト」の本文において、「暗号技術」に注釈が付され、**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の利用時に組み合わせる暗号技術**についてCRYPTREC暗号リストに掲載されたものとするよう**限定**されており、この既存注釈と合わせて注釈を整理。

## 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<sup>1</sup>（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<sup>2</sup>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A)    | (略) |
| メッセージ認証コード (注A) | (略) |
| 認証暗号            | (略) |
| エンティティ認証 (注A)   | (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B)    | (略) |
| メッセージ認証コード (注B) | (略) |
| 認証暗号            | (略) |

（注A）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B）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。

## ＜前回の議論の反映＞

- ✓ **組み合わせる暗号技術を明確にすべき。**

→組み合わせることができる暗号技術は注釈に付さなくても仕様上明らかであること、及びエンティティ認証（ISO/IEC 9798-4）はメッセージ認証コードを用いるため、羅列すると逆にわかりにくくなる可能性があると考え、個別列挙をしないこととした。

例）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

- ✓ **従来の文言も必要に応じて見直しを行うべき。**

→冗長な表現を排除するとともに、「掲載された」という過去形の表現を修正。

# 検討ポイント⑦ 暗号利用モードに係る注釈の取扱い

**全面修正**  
前回と同じ

- 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】

### ✓「XTS」に係る注釈

→表 1 の「XTS」に付される注 5 について、  
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。）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。

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。）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 6 について、  
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。

### ✓「GCM」に係る注釈

→表 1 の「GCM」に付される注 7 について、  
同様の注釈を表 2 の「GCM」にも付すことが適当。

＜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5)             |
|         | 認証付き秘匿モード (注6) | CCM (注7)<br>GCM (注7) |
| (略)     |                | (略)                  |

(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＞

| 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C) |     |
|         | 認証付き秘匿モード (注D) | CCM      |     |
|         |                | GCM (注E) |     |

(注 C) 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 D) 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 E) 初期化ベクトル長は96ビットを推奨する。

## ＜前回の議論の反映＞

- ✓ 認証付き秘匿モードで用いるブロック暗号を表 2 に掲載されたものに制限すべきではないかとの意見があったが、検討ポイント⑥で、暗号利用モード全体にその旨の制限が係っており、重複しての規定は不要と整理。

- **用語・表記の統一方針**を整理する必要があるか。

## 【考え方】

- ✓ 同一概念を異なる用語で表記している場合、**用語の統一又は使い分けの明確化**が必要ではないか。
- ✓ 「**量子コンピュータ**」と「**量子計算機**」について、一般的な記述では**いずれかに統一**する一方、  
「**耐量子計算機暗号（PQC）**」のように**既に定着している専門用語・固有の名称は変更しない**こととしてはどうか。

### ＜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、公用文としては、  
**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」を省くことができる**とされている。
- ✓ 実際に政府関係文書においても長音符号の有無が語によって異なることから、**慣用や専門用語としての定着状況、関連文書における使用実態を踏まえ、語ごとに表記を統一**することとしてはどうか。  
→**具体例：コンピュータ パラメータ カテゴリ**

# (参考) 外来語の表記に関する文書

20

新規  
前回と同じ

## 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/naiku/gairai/honbun06.html](https://www.bunka.go.jp/kokugo_nihongo/sisaku/joho/joho/kijun/naiku/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  
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/93650001\\_01.html](https://www.bunka.go.jp/seisaku/bunkashingikai/kokugo/hokoku/93650001_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

#### Ⅱ 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](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

# (参考) 関連文書における外来語の長音表記の使用状況

**新規**  
前回と同じ

✓ 次の5種類の文書を対象に、外来語の長音表記の状況を整理。

- 政府機関等のサイバーセキュリティ対策のための統一基準
- 政府機関等の対策基準策定のためのガイドライン
- サイバーセキュリティ戦略
- サイバーセキュリティ2026（2025年度年次報告・2026年度年次計画）
- 暗号技術検討会 報告書 2021～2025年度

✓ 対象語は、英語語末の-er、-or、-ar 等に対応する外来語のうち、長音表記の有無が論点となるもの。（ただし、5種類の文書で合計登場回数が5回以上の外来語に限る。）

✓ 各文書について、長音なし・長音ありの出現回数を集計。表中の [n]/[m] は、[長音なしの件数]/[長音ありの件数] を表す。

✓ 表の中で、長音なしが多いものは濃い紫色に、長音ありが多いものは濃い緑色に塗りつぶし。

| 長音なし    | 長音あり     | 政府統一基準 | 政府統一基準<br>ガイドライン | サイバーセキュ<br>リティ戦略 | CS2026 | 暗号技<br>検討会報 |
|---------|----------|--------|------------------|------------------|--------|-------------|
| アーキテクチャ | アーキテクチャー | 6/0    | 8/0              | 1/0              | 8/1    | 0/0         |
| アクタ     | アクター     | 0/0    | 0/1              | 0/7              | 0/0    | 0/0         |
| アドバイザ   | アドバイザー   | 0/4    | 0/17             | 0/0              | 0/6    | 0/0         |
| アンカ     | アンカー     | 0/0    | 0/2              | 0/0              | 0/3    | 0/0         |
| イノベータ   | イノベーター   | 0/0    | 0/0              | 0/0              | 0/7    | 0/0         |
| エラ      | エラー      | 0/0    | 0/9              | 0/0              | 0/1    | 0/3         |
| オーバ     | オーバー     | 0/0    | 0/21             | 0/0              | 0/0    | 0/1         |
| オブザーバ   | オブザーバー   | 0/0    | 0/0              | 0/0              | 0/5    | 5/0         |
| カウンタ    | カウンター    | 0/0    | 0/0              | 0/1              | 0/8    | 0/0         |
| クローラ    | クローラー    | 0/0    | 6/0              | 0/0              | 0/0    | 0/0         |
| コンピュータ  | コンピューター  | 0/0    | 1/0              | 2/0              | 21/0   | 31/12       |
| サーバ     | サーバー     | 98/0   | 536/0            | 6/0              | 26/0   | 6/0         |
| サイバ     | サイバー     | 0/19   | 0/155            | 0/554            | 0/2532 | 0/29        |
| シグネチャ   | シグネチャー   | 0/0    | 8/0              | 0/0              | 0/0    | 0/0         |
| ステーキホルダ | ステーキホルダー | 0/0    | 0/0              | 0/1              | 0/5    | 0/0         |
| セミナ     | セミナー     | 0/0    | 0/1              | 0/0              | 0/88   | 0/0         |
| センサ     | センサー     | 0/1    | 0/1              | 0/5              | 4/22   | 0/0         |
| センタ     | センター     | 0/0    | 0/7              | 0/5              | 0/52   | 0/0         |
| タンパ     | タンパー     | 0/0    | 19/0             | 0/0              | 0/0    | 0/0         |
| トナ      | トナー      | 0/0    | 0/6              | 0/1              | 1/19   | 0/0         |
| ナンバ     | ナンバー     | 0/0    | 0/1              | 0/1              | 0/8    | 0/0         |
| ニュースレタ  | ニュースレター  | 0/0    | 0/0              | 0/0              | 0/6    | 0/0         |
| バッファ    | バッファー    | 0/0    | 9/0              | 0/0              | 0/0    | 0/0         |
| パートナ    | パートナー    | 0/0    | 0/5              | 0/1              | 0/19   | 0/0         |
| パラメータ   | パラメーター   | 1/0    | 12/0             | 0/0              | 0/0    | 24/8        |
| フィルタ    | フィルター    | 0/0    | 21/0             | 0/0              | 0/2    | 0/0         |
| フォルダ    | フォルダー    | 0/0    | 10/0             | 0/0              | 0/0    | 0/0         |
| ブラウザ    | ブラウザー    | 0/0    | 58/0             | 0/0              | 1/0    | 3/0         |
| プロバイダ   | プロバイダー   | 1/0    | 2/0              | 0/0              | 0/0    | 2/0         |
| ヘッダ     | ヘッダー     | 0/0    | 21/0             | 0/0              | 0/0    | 0/0         |
| ベンダ     | ベンダー     | 1/0    | 26/0             | 0/10             | 6/23   | 6/1         |
| ベンチャ    | ベンチャー    | 0/0    | 0/0              | 0/0              | 0/5    | 0/0         |
| メーカ     | メーカー     | 0/0    | 0/0              | 0/2              | 0/7    | 0/0         |
| モニタ     | モニター     | 3/0    | 4/0              | 0/0              | 3/0    | 0/0         |
| ユーザ     | ユーザー     | 0/0    | 38/0             | 0/2              | 2/13   | 4/0         |
| リーダ     | リーダー     | 0/0    | 0/2              | 0/2              | 0/9    | 0/0         |
| ルータ     | ルーター     | 1/0    | 6/0              | 0/0              | 0/0    | 0/0         |
| レイヤ     | レイヤー     | 0/0    | 0/0              | 0/0              | 1/2    | 0/2         |

# (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             |
|            | 守秘           | RSA-PSS           |
|            |              | RSASSA-PKCS1-v1_5 |
| 共通鍵暗号      | 鍵共有          | RSA-OAEP          |
|            |              | DH                |
|            | 64ビットブロック暗号  | ECDH              |
|            |              | 該当なし              |
|            |              | AES               |
| ハッシュ関数     | 128ビットブロック暗号 | Camellia          |
|            |              | KCipher-2         |
|            | ストリーム暗号      | SHA-256           |
|            |              | SHA-384           |
|            |              | SHA-512           |
| 暗号利用モード    | 秘匿モード        | SHA-512/256       |
|            |              | SHA3-256          |
|            |              | SHA3-384          |
|            | 認証付き秘匿モード    | SHA3-512          |
|            |              | SHAKE128          |
| メッセージ認証コード | 秘匿モード        | SHAKE256          |
|            |              | CBC               |
|            |              | CFB               |
|            | 認証付き秘匿モード    | CTR               |
|            |              | OFB               |
| 認証暗号       | 秘匿モード        | XTS               |
|            |              | CCM               |
|            |              | GCM               |
|            | 認証付き秘匿モード    | CMAC              |
|            |              | HMAC              |
| エンティティ認証   | 秘匿モード        | ChaCha20-Poly1305 |
|            |              | ISO/IEC 9798-2    |
|            |              | ISO/IEC 9798-3    |
|            | 認証付き秘匿モード    | 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              | セキュリティ<br>カテゴリ(注8)        |
|------------|-----------|-------------------|---------------------------|
| 公開鍵暗号      | 署名        | ML-DSA            | ML-DSA-44(注)              |
|            |           |                   | ML-DSA-65                 |
|            |           |                   | ML-DSA-87                 |
|            |           |                   | SLH-DSA-SHA2-128[s/f](注)  |
|            |           |                   | SLH-DSA-SHAKE-128[s/f](注) |
|            | 鍵共有       | SLH-DSA           | SLH-DSA-SHA2-192[s/f]     |
|            |           |                   | SLH-DSA-SHA2-192[s/f]     |
|            |           |                   | SLH-DSA-SHAKE-192[s/f]    |
|            |           |                   | SLH-DSA-SHA2-256[s/f]     |
|            |           |                   | SLH-DSA-SHAKE-256[s/f]    |
| 共通鍵暗号      | ブロック暗号    | ML-KEM            | ML-KEM-768                |
|            |           |                   | ML-KEM-1024               |
|            | ストリーム暗号   | AES               | AES-192                   |
|            |           |                   | AES-256                   |
| ハッシュ関数     | ブロック暗号    | Camellia          | Camellia-192              |
|            |           |                   | Camellia-256              |
|            | ストリーム暗号   | —                 | —                         |
|            |           |                   | —                         |
|            |           |                   | —                         |
| 暗号利用モード    | 秘匿モード     | SHA2              | SHA-384                   |
|            |           |                   | SHA-512                   |
|            | 認証付き秘匿モード | SHA3              | SHA3-384                  |
|            |           |                   | SHA3-512                  |
|            |           | SHAKE             | SHAKE256                  |
| メッセージ認証コード | 秘匿モード     | CBC               |                           |
|            |           | CFB               |                           |
|            | 認証付き秘匿モード | CTR               |                           |
|            |           | OFB               |                           |
|            |           | XTS               |                           |
| 認証暗号       | 秘匿モード     | CCM               |                           |
|            |           | GCM               |                           |
|            | 認証付き秘匿モード | CMAC              |                           |
|            |           | HMAC              |                           |
|            |           | ChaCha20-Poly1305 |                           |

＜表 2 に掲載されない暗号技術＞  
ML-KEM-512 (Category 1)  
AES-128 (Category 1)  
Camellia-128 (Category 1)  
KCipher-2 (Category 1)  
SHA-256 (Category 2)  
SHA-512/256 (Category 2)  
SHA3-256 (Category 2)  
SHAKE128 (Category 2)  
ISO/IEC 9798-2  
ISO/IEC 9798-3  
ISO/IEC 9798-4

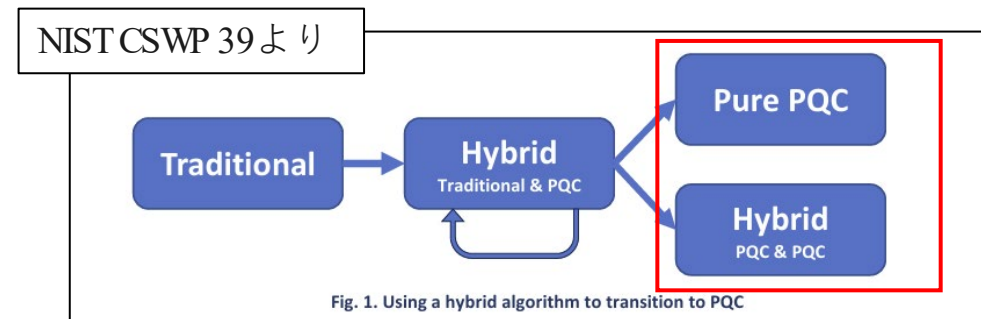
## 課題③

ハイブリッド構成の取扱い

# ハイブリッドの位置づけ

## • NIST

- ハイブリッドは移行期の選択肢であるが、**要求や推奨**をしているわけではない。
- 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）。



## • EU関連

- **ECCG**（EUの暗号エキスパートチーム）：
  - Agreed Cryptographic Mechanisms Version 3 (Public Review)では、
    - (M)LWEベースの暗号については、**単独利用を推奨していない**（shouldn'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。
- **BSI**（ドイツ）
  - "Post-quantum schemes **should only be used in combination with classical schemes ("hybrid") if possible.**"  
[BSI - Quantum Technologies and Quantum-Safe Cryptography](#)
  - BSI-TR-02102-1（2026年）では、ETSI TS 103 744 のCatKDFを引用（※引用先は744 v1.2.2でなく744）。
- **ANSSI**（フランス）
  - 移行ロードマップにおけるPhase 1及びPhase 2でハイブリッドを推奨。
  - 具体的な構成方法についての記載は見当たらなかった。  
[ANSSI views on the Post-Quantum Cryptography transition \(EN\) | MesServicesCyber](#)
- **ENISA**（EUのサイバーセキュリティ機関、ECCGより政策寄り）：
  - ハイブリッドについては整理しているが、推奨する文章は確認できなかった。

欧州においても立場は一樣ではない。

ECCG、BSI、ANSSIはハイブリッド利用に比較的積極的である一方、ENISAはハイブリッドを重要な移行技術として整理・分析しているものの、確認した文書の範囲では利用推奨を確認できなかった。

幾つかの国・地域においてハイブリッド利用を支持する傾向にある一方、具体的なハイブリッド構成方法については各国ガイドラインではなく、標準化団体（ETSI、IETF、ANSI X9等）で検討・標準化が進められている。

# ハイブリッドの仕組みについての検討状況

- **ETSI**
  - TS 103 744 v1.2.2でハイブリッド鍵共有を構成する暗号プリミティブ及びパラメータセットについて定義。
    - IETFで標準化される方式を参照している模様。
  - TR 103 966 v1.1.1でハイブリッド構成を行う上での考え方や考慮点を示す。
- **IETF**
  - 用語定義や分類。
    - **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が標準化中又は標準化済み。
- **ANSI X9 (米国・金融)**
  - Hybridの実装方式を標準化している模様。検討範囲にはChimera, Composite, Chameleonの証明書形式やDual Signature方式が含まれる模様。
  - ETSIやIETFで標準化が進む方式との相互運用性についての検討状況は不明。
- **Chrome (ブラウザ)**
  - TLS (暗号化) : ハイブリッド鍵共有をサービス提供済み。
  - TLS (認証) : MTCを推奨 (未標準化、ML-DSA44 を想定)。
- **Apple (ブラウザ)**
  - TLS (認証) : MTCを採用予定。co-signerにML-DSA44 × 2 とECDSA256 × 1 を要求予定 (アプリケーションレベルでのハイブリッド化)。
    - **アプリケーションレベルのハイブリッド**。合成か混成かは明示されていない。
  - S/MIME (認証) : Composite証明書を採用予定 (**証明書レベルのハイブリッド**)。
- **Microsoft (ブラウザ)**
  - X.509 Pure証明書の実証パイロットプロジェクトを実施中。TLS向けのMTCも検討中。

MTC : Merkle Tree Certificate

**KEMについては、ハイブリッド方式が主流であり、標準化・サービス化が進展中。**

**デジタル署名については、様々なアプローチが存在する (同一組織でも用途によってアプローチが異なる場合がある)。**

# 「ハイブリッド」の分類 (アルゴリズム・プロトコル・アプリケーションレベル及び、混成と合成)

表 4-1 ハイブリッド構成の目的と適用主体による整理

| 主体 \ 目的           | 後方互換性確保                                                                                                                                                                                                                                                                                                                                                                                                                          | 安全性維持                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アルゴリズム            | なし                                                                                                                                                                                                                                                                                                                                                                                                                               | <p><u>鍵共有アルゴリズム</u></p> <ul style="list-style-type: none"> <li>NIST SP 800-227(4.6. Multi-Algorithm KEMs and PQ/T Hybrids) [4]</li> <li>NIST SP 800-56C Rev. 2<sup>3</sup> [9]</li> <li>draft-irtf-cfrg-hybrid-kems-07 [10]</li> <li>draft-ietf-lamps-pq-composite-kem-12 [11]<sup>4</sup></li> </ul> <p><u>署名アルゴリズム</u></p> <ul style="list-style-type: none"> <li>draft-ietf-lamps-pq-composite-sigs-14 [12]<sup>4</sup></li> </ul> |
| プロトコル             | <p><u>通信プロトコル</u></p> <ul style="list-style-type: none"> <li>RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3 [13]</li> <li>※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</li> </ul> <p><u>証明書構造</u></p> <ul style="list-style-type: none"> <li>draft-ietf-lamps-certdiscovery-02 [18]</li> <li>ITU-T X.509(9.8 Alternative cryptographic algorithms and digital signature extensions) [19]</li> </ul> | <p><u>通信プロトコル</u></p> <ul style="list-style-type: none"> <li>draft-ietf-tls-hybrid-design-16 [14]</li> <li>draft-ietf-mls-combiner-02 [15]</li> <li>ETSI TS 103 744 [16]</li> <li>IEEE 802.11 Hybrid PQC Proposal [17]</li> <li>draft-ietf-lamps-pq-composite-kem-12 [11]<sup>4</sup></li> </ul> <p><u>証明書構造</u></p> <ul style="list-style-type: none"> <li>draft-ietf-lamps-pq-composite-sigs-14 [12]<sup>4</sup></li> </ul>         |
| システム <sup>5</sup> | <p>(後方互換性確保/安全性維持 共通)</p> <ul style="list-style-type: none"> <li>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]</li> <li>Hybrid PQC E-Mail Communication: Easing Migration Pain(PQC Conference) [21]</li> </ul>                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                       |

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。

安全性維持を目的とした「合成」方式の実態を紹介。

合成：例えばECDHとML-KEMを両方実行し、両方の共有秘密を組み合わせて鍵を作る（片方が解読できても安全性が担保）

混成：例えば相手がPQC対応ならPQC方式を使い、未対応なら従来方式を使えるように切り替える

※「合成」と「混成」はcryptrec-ex-3503-2025における用語

[cryptrec-ex-3503-2025.pdf](https://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

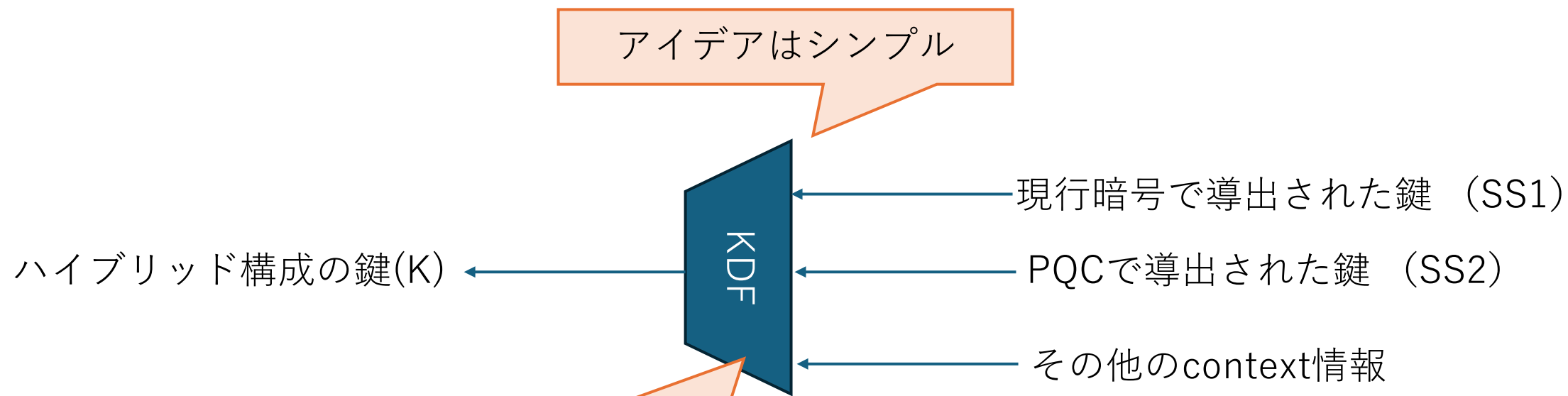
## • 秘匿（KEM）用途

- 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 v1.2.2ではハイブリッド鍵共有のパラメータセットを定義している。

## • 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 (CatKDF) 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。

| 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-ecdsa-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]      |

# TLS 1.3 の方向性 (RFC 9846, 2026年 7 月)

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

- 実施例：
  - X25519MLKEM768（右表内の4588, RFC 10024で標準化済）

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

ECDHE鍵 || MLKEMの鍵

- 特徴：
  - TLS1.2ではPQC対応を行わない（RFC 9851, 2026年7月）。
  - 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<br>(コードポイント) |                          |   |   |  | Transport Layer Security (TLS) Parameters |  |  |  |  |
|-------------------------------|--------------------------|---|---|--|-------------------------------------------|--|--|--|--|
| 13                            | secl571k1                | Y | N |  |                                           |  |  |  |  |
| 14                            | secl571r1                | Y | N |  |                                           |  |  |  |  |
| 15                            | secp160k1                | Y | D |  |                                           |  |  |  |  |
| 16                            | secp160r1                | Y | D |  |                                           |  |  |  |  |
| 17                            | secp160r2                | Y | D |  |                                           |  |  |  |  |
| 18                            | secp192k1                | Y | D |  |                                           |  |  |  |  |
| 19                            | secp192r1                | Y | D |  |                                           |  |  |  |  |
| 20                            | secp224k1                | Y | D |  |                                           |  |  |  |  |
| 21                            | secp224r1                | Y | D |  |                                           |  |  |  |  |
| 22                            | secp256k1                | Y | N |  |                                           |  |  |  |  |
| 23                            | secp256r1                | Y | Y |  |                                           |  |  |  |  |
| 24                            | secp384r1                | Y | Y |  |                                           |  |  |  |  |
| 25                            | secp521r1                | Y | N |  |                                           |  |  |  |  |
| 26                            | brainpoolP256r1          | Y | N |  |                                           |  |  |  |  |
| 27                            | brainpoolP384r1          | Y | N |  |                                           |  |  |  |  |
| 28                            | brainpoolP512r1          | Y | N |  |                                           |  |  |  |  |
| 29                            | x25519                   | Y | Y |  |                                           |  |  |  |  |
| 30                            | x448                     | Y | Y |  |                                           |  |  |  |  |
| 31                            | brainpoolP256r1tls13     | Y | N |  |                                           |  |  |  |  |
| 32                            | brainpoolP384r1tls13     | Y | N |  |                                           |  |  |  |  |
| 33                            | brainpoolP512r1tls13     | Y | N |  |                                           |  |  |  |  |
| 34                            | GC256A                   | Y | N |  |                                           |  |  |  |  |
| 35                            | GC256B                   | Y | N |  |                                           |  |  |  |  |
| 36                            | GC256C                   | Y | N |  |                                           |  |  |  |  |
| 37                            | GC256D                   | Y | N |  |                                           |  |  |  |  |
| 38                            | GC512A                   | Y | N |  |                                           |  |  |  |  |
| 39                            | GC512B                   | Y | N |  |                                           |  |  |  |  |
| 40                            | GC512C                   | Y | N |  |                                           |  |  |  |  |
| 41                            | curveSM2                 | N | N |  |                                           |  |  |  |  |
| 42-255                        | Unassigned               |   |   |  |                                           |  |  |  |  |
| 256                           | ffdhe2048                | Y | N |  |                                           |  |  |  |  |
| 257                           | ffdhe3072                | Y | N |  |                                           |  |  |  |  |
| 258                           | ffdhe4096                | Y | N |  |                                           |  |  |  |  |
| 259                           | ffdhe6144                | Y | N |  |                                           |  |  |  |  |
| 260                           | ffdhe8192                | Y | N |  |                                           |  |  |  |  |
| 261-507                       | Unassigned               |   |   |  |                                           |  |  |  |  |
| 508-511                       | Reserved for Private Use |   |   |  |                                           |  |  |  |  |
| 512                           | MLKEM512                 | Y | N |  |                                           |  |  |  |  |
| 513                           | MLKEM768                 | Y | N |  |                                           |  |  |  |  |
| 514                           | MLKEM1024                | Y | N |  |                                           |  |  |  |  |
| 515-2569                      | Unassigned               |   |   |  |                                           |  |  |  |  |
| 2570                          | Reserved                 | Y | N |  |                                           |  |  |  |  |
| 2571-4586                     | Unassigned               |   |   |  |                                           |  |  |  |  |
| 4587                          | SecP256r1MLKEM768        | Y | N |  |                                           |  |  |  |  |
| 4588                          | X25519MLKEM768           | Y | N |  |                                           |  |  |  |  |
| 4589                          | SecP384r1MLKEM1024       | Y | N |  |                                           |  |  |  |  |
| 4590                          | curveSM2MLKEM768         | N | N |  |                                           |  |  |  |  |
| 4591-0001                     | Unassigned               |   |   |  |                                           |  |  |  |  |

# ETSI TS 103 744 v1.2.2

## TS 103 744 - V1.2.2 - CYBER; Quantum-Safe Cryptography (QSC); Quantum-safe Hybrid Key Establishment

- ハイブリッドKEMを構成するための  
暗号プリミティブを**定義**している。
  - Hash
  - Context Formatting
  - PRF
  - KDF
  - ECDH
  - KEM
  - ハイブリッドKEMのプリミティブパラメータセット（右に一覧）

### 7.7.2 Parameter sets

HKDFwSHA256\_P256\_ML-KEM-512,  
 HKDFwSHA256\_X25519\_ML-KEM-512,  
 HKDFwSHA256\_BP-P256\_ML-KEM-512,  
 HMACwSHA256\_P256\_ML-KEM-512,  
 HMACwSHA256\_X25519\_ML-KEM-512,  
 HMACwSHA256\_BP-P256\_ML-KEM-512,  
 KMAC128\_P256\_ML-KEM-512,  
 KMAC128\_X25519\_ML-KEM-512,  
 KMAC128\_BP-P256\_ML-KEM-512,  
 HKDFwSHA256\_P256\_ML-KEM-768,  
 HKDFwSHA256\_X25519\_ML-KEM-768,  
 HKDFwSHA256\_BP-P256\_ML-KEM-768,  
 HMACwSHA256\_P256\_ML-KEM-768,  
 HMACwSHA256\_X25519\_ML-KEM-768,  
 HMACwSHA256\_BP-P256\_ML-KEM-768,  
 KMAC128\_P256\_ML-KEM-768,  
 KMAC128\_X25519\_ML-KEM-768,  
 KMAC128\_BP-P256\_ML-KEM-768,  
 HKDFwSHA384\_P384\_ML-KEM-768,  
 HKDFwSHA384\_X448\_ML-KEM-768,  
 HKDFwSHA384\_BP-P384\_ML-KEM-768,  
 HMACwSHA384\_P384\_ML-KEM-768,  
 HMACwSHA384\_X448\_ML-KEM-768,  
 HMACwSHA384\_BP-P384\_ML-KEM-768,  
 KMAC256\_P384\_ML-KEM-768,  
 KMAC256\_X448\_ML-KEM-768,  
 KMAC256\_BP-P384\_ML-KEM-768,  
 HKDFwSHA384\_P384\_ML-KEM-1024,  
 HKDFwSHA384\_X448\_ML-KEM-1024,  
 HKDFwSHA384\_BP-P384\_ML-KEM-1024,  
 HMACwSHA384\_P384\_ML-KEM-1024,  
 HMACwSHA384\_X448\_ML-KEM-1024,  
 HMACwSHA384\_BP-P384\_ML-KEM-1024,  
 KMAC256\_P384\_ML-KEM-1024,  
 KMAC256\_X448\_ML-KEM-1024,  
 KMAC256\_BP-P384\_ML-KEM-1024.

## ETSI TS 103 744 v1.2.2の定義対象

## NIST SP 800シリーズでの定義対象

現状の  
CRYPTREC暗号リスト

KEM

ECDH

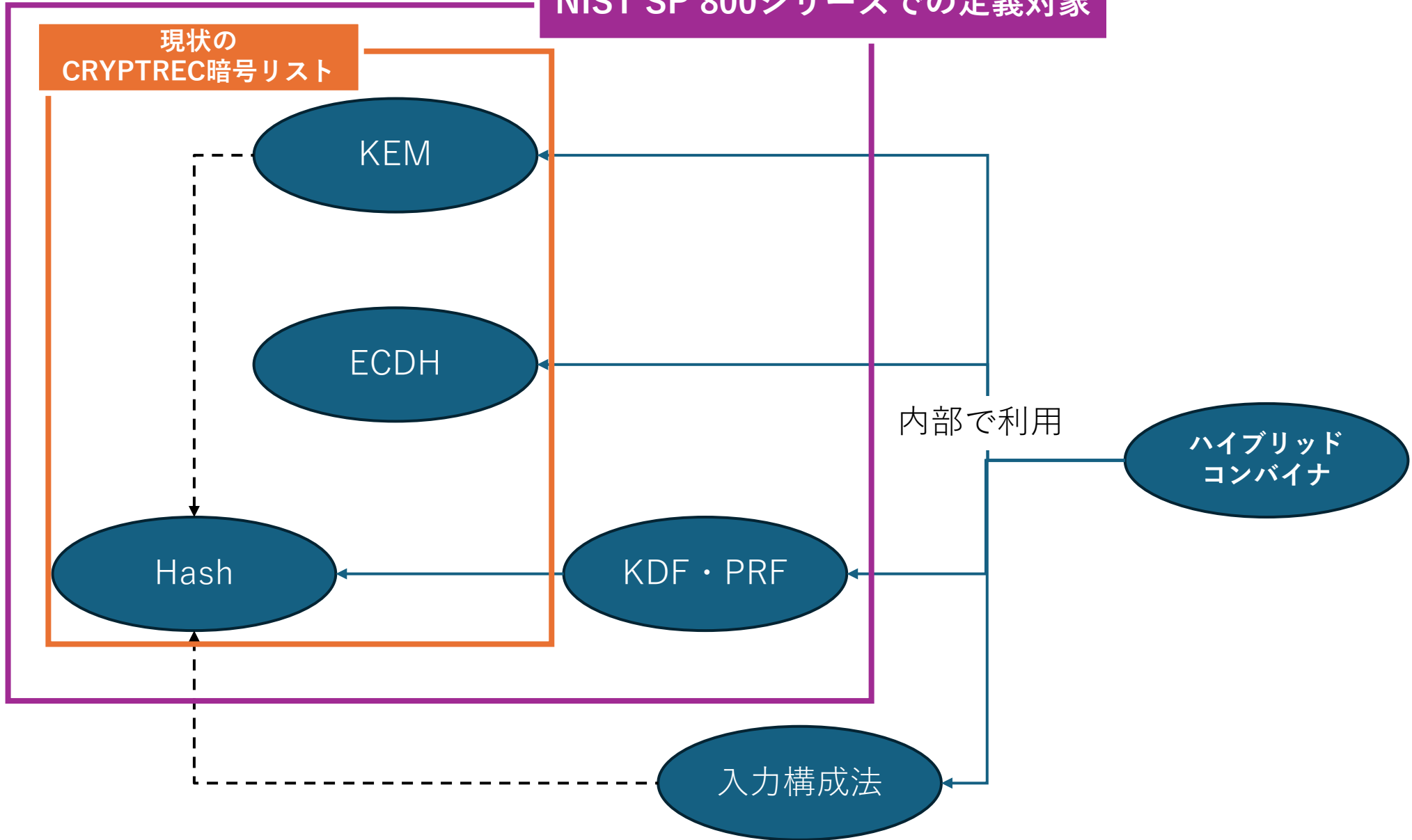
Hash

KDF・PRF

内部で利用

ハイブリッド  
コンバイナ

入力構成法



# ハイブリッドKEM関連の動向

- ハイブリッドKEM（合成）は、既に広く利用されている。
- パラメータセットは多数存在。
- パラメータセットの記載方法も複数存在。

# 「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 v1.2.2ではハイブリッド鍵共有のパラメータセットを定義している。

## • 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。

# 署名に関してのハイブリッド関連議論の動向

- **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。

- **デジタル署名（X.509証明書）は、比較的議論が進んでいるものの、収束まで時間を要する見通し**

- ユースケースに合わせて構成法が異なる傾向がある。

# 署名に関するハイブリッド関連議論の動向

- 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。
  - EUF-CMAしかみたしていない場合、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。どちらの安全性を目指すべきかについては、議論が継続している。

- ハイブリッド署名プロトコル/アプリケーション

- プロトコルレベルのハイブリッド化の実施形態は、既存プロトコルの設計に大きく依存する。
  - 一般的・具体的な構成法は議論しにくい。
- Dual署名に関して：プロトコルのみでなくポリシーレイヤにも依存しうるが、基本的に各論であり一般論でない。
- 並列署名とネスト型署名に関する議論は未成熟。
- 少数ながらアプリケーションレベルの提案も存在（MTCプロトコルに対するAppleの提案）。

# リスト化に向けての論点

## • 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。
  - 組み合わせは、現行暗号（公開鍵）、PQC（公開鍵）、ハッシュ関数（KDF内）、鍵長等を含みうる。
  - 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：関連する考慮点

## • SHA-256の扱い

- **コンバイナ（やKDF）内部でのSHA-256の利用**をどのように整理するか。

※なお、ハッシュベース署名内部でもSHA-256を利用している。

- 内部利用のみSHA-256を許容する場合の整理の方向性（例）

- 例1：単純な衝突耐性が要求される用途との違いを記載する。
- 例2：リストにKDFを定義し、その内部利用でのみ許容するとの記載にする。

## • 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（入力構成法に関して）

- 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。

# 参考：リスト記載案（暗号化）

- **KDF又はコンバイナをリストへの記載範囲とする。**  
**（ETSI TS 103 744 v1.2.2における7.4及び8節に対応）**
  - 案1：技術分類に**KDF 又はコンバイナを新設**し、暗号名称**CatKDF**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、暗号名称内で**CatKDF**を記載する。（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しても良い）。
- **上記に加え、コンバイナが利用する暗号アルゴリズム や 入力もセットでリストに記載する。**  
**（X.509やETSI TS 103 744 v1.2.2 7 節～8節に対応）**
  - 案3：安全性が確認できた**ハイブリッドKEMのアルゴリズムの組み合わせリスト**を記載する。
    - 既存アルゴリズム + PQCアルゴリズム + ハッシュ関数の組み合わせなので数は多い。
- **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。
    - コンバイナ内部でSHA-256を呼び出す場合等、暗号リスト未記載のハッシュ関数利用するケースを、どのように扱うかの整理をどのようにするかは要検討。

## 「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  
ネットワークサービス事業本部  
セキュリティ本部 セキュリティ情報統括室 シニアエンジニア

高木 剛      東京大学 大学院情報理工学系研究科 数理情報学専攻 教授

細山田 光倫 NTT社会情報研究所  
情報保護技術研究プロジェクト 暗号基礎グループ

松本 勉      国立研究開発法人産業技術総合研究所 フェロー  
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<sup>1</sup>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<sup>2</sup>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」<sup>3</sup>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<br>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<br>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<br>GCM（注7）    |
| メッセージ認証コード |                 | CMAC<br>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<sup>4</sup>。

| 技術分類   |      | 暗号技術   |                                                     |
|--------|------|--------|-----------------------------------------------------|
|        |      | 名称     | パラメーターセット（注8）                                       |
| 公開鍵暗号  | 署名   | —      | —                                                   |
|        | 鍵共有  | ML-KEM | ML-KEM-768 (Category 3)<br>ML-KEM-1024 (Category 5) |
| 共通鍵暗号  |      | AES    | AES-192 (Category 3)<br>AES-256 (Category 5)        |
| ハッシュ関数 | SHA2 |        | SHA-384 (Category 4)<br>SHA-512                     |
|        |      |        | SHA3-384 (Category 4)<br>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 | <b>ML-KEM-512 (Category 1)</b>  |
|        | ML-KEM-768 (Category 3)         |
|        | ML-KEM-1024 (Category 5)        |
| AES    | <b>AES-128 (Category 1)</b>     |
|        | AES-192 (Category 3)            |
|        | AES-256 (Category 5)            |
| SHA2   | <b>SHA-256 (Category 2)</b>     |
|        | <b>SHA-512/256 (Category 2)</b> |
|        | 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<sup>1</sup>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<sup>2</sup>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」<sup>3</sup>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 <sup>(注 1)</sup>      |
|           |                              | ECDSA                     |
|           |                              | EdDSA                     |
|           |                              | RSA-PSS                   |
|           |                              | RSASSA-PKCS1-v1_5         |
|           | 守秘                           | RSA-OAEP                  |
|           | 鍵共有                          | DH                        |
|           |                              | ECDH <sup>(注 2)</sup>     |
| 共通鍵暗号     | 64ビットブロック暗号 <sup>(注 3)</sup> | 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 <sup>(注 4)</sup> |
|           |                              | SHAKE256 <sup>(注 4)</sup> |
| (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<sup>4</sup>。

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

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

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

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

<sup>4</sup> 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<sup>5</sup>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」<sup>6</sup>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。

<sup>5</sup> 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。

<sup>6</sup> 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<sup>7</sup>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<sup>8</sup>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」<sup>9</sup>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 <sup>(注13)</sup> |
|            | 鍵共有                          | 該当なし                              |
| 共通鍵暗号      | 64ビットブロック暗号 <sup>(注14)</sup> | 3-key Triple DES <sup>(注15)</sup> |
|            | 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 <sup>(注16)</sup>   | 該当なし                              |
| メッセージ認証コード |                              | CBC-MAC <sup>(注17)</sup>          |
| 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。

<sup>7</sup> 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。

<sup>8</sup> 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

<sup>9</sup> CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, <https://www.cryptrec.go.jp/list.html>

## 更新履歴情報

| 更新日付            | 更新箇所                          | 更新前の記述                                                                                                                                                                                                                                                                                                      | 更新後の記述                                                                                                                                                                                                        |
|-----------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 令和 6 年<br>5月16日 | 注                             | [新規追加]                                                                                                                                                                                                                                                                                                      | (注18) FIPS PUB 186-5では廃止されているが、本リスト掲載時から安全性・利用実績の状況に大きな変化がないため、掲載を継続する。                                                                                                                                       |
|                 | 注                             | [新規追加]                                                                                                                                                                                                                                                                                                      | (注19) SP 800-67 Revision 2では廃止されているが、本リスト掲載時から安全性・利用実績の状況に大きな変化がないため、掲載を継続する。                                                                                                                                 |
| 令和 8 年<br>3月30日 | 電子政府推奨暗号リスト（本文）               | 暗号技術検討会及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。                                                                                                                                                                                           | 暗号技術検討会及び関連委員会（以下「CRYPTREC」という。）により安全性（セキュリティ）及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。                                                                                      |
|                 | 電子政府推奨暗号リスト（表）                | [表の件名付与]                                                                                                                                                                                                                                                                                                    | <表 1 現行暗号リスト>                                                                                                                                                                                                 |
|                 | 電子政府推奨暗号リスト（表）                | [表の新設]                                                                                                                                                                                                                                                                                                      | <表 2 耐量子計算機暗号（PQC）リスト><br>現行暗号の解読に利用可能な水準の量子計算機（CRQC: Cryptographically Relevant Quantum Computer）への耐性を有することが確認された暗号技術のリスト。                                                                                   |
|                 | 電子政府推奨暗号リスト（耐量子計算機暗号（PQC）リスト） | [技術分類の追加]                                                                                                                                                                                                                                                                                                   | 技術分類：公開鍵暗号－署名<br>名称／パラメーターセット：－<br>技術分類：公開鍵暗号－鍵共有<br>名称：ML-KEM<br>パラメーターセット：<br>ML-KEM-768 (Category 3)<br>ML-KEM-1024 (Category 5)                                                                           |
|                 | 電子政府推奨暗号リスト（耐量子計算機暗号（PQC）リスト） | [技術分類の追加]                                                                                                                                                                                                                                                                                                   | 技術分類：共通鍵暗号<br>名称：AES<br>パラメーターセット：<br>AES-192 (Category 3)<br>AES-256 (Category 5)                                                                                                                            |
|                 | 電子政府推奨暗号リスト（耐量子計算機暗号（PQC）リスト） | [技術分類の追加]                                                                                                                                                                                                                                                                                                   | 技術分類：ハッシュ関数<br>名称：SHA2<br>パラメーターセット：<br>SHA-384 (Category 4)<br>SHA-512<br>名称：SHA3<br>パラメーターセット：<br>SHA3-384 (Category 4)<br>SHA3-512                                                                         |
|                 | 脚注                            | 5 CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, <a href="https://www.cryptrec.go.jp/list.html">https://www.cryptrec.go.jp/list.html</a>                                                                                                                                                                           | 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, <a href="https://www.cryptrec.go.jp/list.html">https://www.cryptrec.go.jp/list.html</a><br>なお、当該設定基準の見直しの検討を行う予定であり、当面の間、表 2（耐量子計算機暗号（PQC）リスト）の公開鍵暗号は、当該設定基準を適用しない。 |
|                 | 脚注                            | [新規追加]                                                                                                                                                                                                                                                                                                      | 4 暗号技術の耐量子計算機暗号（PQC）リストへの追加について検討中である。<br><a href="https://www.cryptrec.go.jp/report/cryptrec-mt-1501-2026.pdf">https://www.cryptrec.go.jp/report/cryptrec-mt-1501-2026.pdf</a>                               |
|                 | 脚注                            | 脚注 3、4、7、8                                                                                                                                                                                                                                                                                                  | 脚注 5、7、8、9                                                                                                                                                                                                    |
|                 | 注                             | (注 1) 「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」（平成 20 年 4 月情報セキュリティ政策会議決定、平成 24 年 10 月情報セキュリティ対策推進会議改定）を踏まえて利用すること。<br><a href="https://www.nisc.go.jp/pdf/policy/general/angou_ikoushishin.pdf">https://www.nisc.go.jp/pdf/policy/general/angou_ikoushishin.pdf</a><br>（平成 25 年 3 月 1 日現在） | [削除]                                                                                                                                                                                                          |

|   |                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 注 | (注8)「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」(平成20年4月情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定)を踏まえて利用すること。<br><a href="https://www.nisc.go.jp/pdf/policy/general/angou_ikoushishin.pdf">https://www.nisc.go.jp/pdf/policy/general/angou_ikoushishin.pdf</a><br>(平成25年3月1日現在) | [削除]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 注 | [新規追加]                                                                                                                                                                                                                                                                                  | (注2)使用するMACはHMACまたはCMACに限る。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 注 | [新規追加]                                                                                                                                                                                                                                                                                  | (注8)セキュリティのカテゴリを合わせて記載する。各カテゴリはNISTの“Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”に従い、次のように、カテゴリ名の右に記載の鍵探索又は衝突探索と同程度以上の計算資源が攻撃に必要であることを意味する。<br>・Category 1 128ビット鍵を持つブロック暗号に対する鍵探索<br>・Category 2 256ビットのハッシュ関数に対する衝突探索<br>・Category 3 192ビット鍵を持つブロック暗号に対する鍵探索<br>・Category 4 384ビットのハッシュ関数に対する衝突探索<br>・Category 5 256ビット鍵を持つブロック暗号に対する鍵探索<br><a href="https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf">https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf</a><br>(令和8年3月25日現在) |
| 注 | 注18、2、12、17、13、4、5～7、14、9、15、19、11                                                                                                                                                                                                                                                      | 注1、3、4、5、6、7、9～11、12、13、14、15、17                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |