資料１

耐量子計算機暗号（PQC）リスト検討タスクフォース（第５回）

令和８年10月23日(金) 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) CRYPTREC暗号リストの改定（PQC対応）に対する意見公募について

(4) 課題③　ハイブリッド構成の取扱いについて

(5) その他

３．閉会

＜配付資料一覧＞

資料１　議事次第・配付資料一覧

資料２　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３－１　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３－２　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)【改定イメージ】

資料４　CRYPTREC暗号リストの改定（PQC対応）に対する意見公募について

資料５　課題③　ハイブリッド構成の取扱い【前回会合と同様】

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

以上

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

前回会合からの主な修正点について

1．安全性評価等のスケジュールについて

→各暗号技術の標準化の進展状況等を踏まえ、暗号技術評価委員会において検討することを明記。（→p3）
また、表の記載順は評価の優先順位を示すものではない旨を注記。（→p4）

2．暗号技術（PQC）について

→暗号技術の概要を追記するとともに、Classic McElieceに関する最新状況を追記（→p4~5）

3．CNSA 2.0におけるソフトウェア・ファームウェア署名用のLMS及びXMSSの位置付けについて

→CNSA 2.0では、LMS及びXMSSによる早期移行を推奨する一方、ML-DSAの利用も認めている。（→p8）
2026年のNSAのCSfC※関連文書でも、３方式のいずれかを使用すれば要件を満たすことを確認。（→p9）
※Commercial Solutions for Classified。米国NSAが定める、民間のIT製品や暗号技術を組み合わせて機密情報を安全に保護するための枠組み。

4．LMS・XMSSの規定状況について

→米国以外の状況を追記（→p10,11）

5．MicrosoftのLMS・XMSS等への対応状況について

→暗号ライブラリ「SymCrypt」に関する記載を追記（→p12）

次ページ以降の黄マーカー部分が前回会合からの修正箇所

公開鍵暗号方式のPQCの安全性評価等の進め方

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

◆ FIPS 203 (ML-KEM)	格子暗号ベース	暗号化・鍵交換用途	CRYPTREC暗号リストに掲載済
◆ FIPS 204 (ML-DSA)	格子暗号ベース	署名用途	2026年度に評価
◆ FIPS 205 (SLH-DSA)	ハッシュ関数ベース	署名用途	2026年度に評価

【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

✓ 上記観点に照らして、次のように判断する。
なお、評価スケジュールは、各暗号技術の標準化動向等を踏まえ、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^{MT}は評価対象にしない。
  また、ソフトウェア署名等にはML-DSAも利用可能であることから、LMS、XMSS及びML-DSAの利活用状況等も踏まえつつ評価対象とする。
- **NTRU**について、標準化の進展や国内利用の計画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(A)～(C)の3つの観点を踏まえ、主要なPQC方式について整理。

暗号技術	暗号技術の概要	(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
FN-DSA (FIPS 206)	格子暗号ベース／署名用途。2022年7月にNISTの標準化方式に選定。署名サイズが小さいが、浮動小数点演算による実装上の難しさがある。	◎ 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※
HQC	符号ベース／暗号化・鍵交換用途。2025年3月にNISTの標準化方式に選定。ML-KEMとは異なる数学的問題に基づく代替方式として位置付けられる。	◎ 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※
NIST追加公募中の署名方式	署名用途。追加の標準化候補としてNISTが選定中。（2026年5月に追加方式の第３ラウンドの候補として９方式が公表）	○ 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※
LMS / XMSS	ハッシュベース／署名用途。署名できる回数に制限があり、署名鍵の使用状態を管理する必要があるため、ファームウェア署名等、署名処理を厳格に管理できる用途に適する。	◎ 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※
NTRU	格子暗号ベース／暗号化・鍵交換用途。NIST標準化プロセスの第３ラウンド候補。NTTの研究者が提案に参画している。	◎ 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※
FrodoKEM	格子暗号ベース／暗号化・鍵交換用途。NIST標準化プロセスの第３ラウンド候補。鍵サイズ等が大きい一方、ドイツBSI等の欧州のセキュリティ機関が推奨。	◎ 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確認できず	継続的に情報収集
Classic McEliece	符号ベース／暗号化・鍵交換用途。NIST標準化プロセスの第４ラウンド候補。公開鍵サイズが非常に大きい一方、暗号文サイズが小さいことが特徴。	△暗号解析の進展を受け、独BSIが2026年10月1日、新規採用を控えるよう勧告(参考)	○ ISO/IECで標準化(2026年6月)	△ 国内での具体的な製品・サービス利用は現時点で確認できず	継続的に情報収集
NTRU+	格子暗号ベース／暗号化・鍵交換用途。NTRU系の数学的構造を利用する韓国発の方式。NTRUとは異なる設計で、韓国のKpqC公募で最終選定された。	○ 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確認できず	継続的に情報収集

(参考) https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/2026/Classic-McEliece_261001.html

※本表の記載順は評価の優先順位を示すものではない。

（参考）Classic McElieceの安全性に関するBSIの見解

- **ドイツ**連邦情報セキュリティ庁(**BSI**)は、2026年9月29日付けの文書で、**Classic McElieceに対する暗号解析の進展**を踏まえ、安全性に関する暫定的な評価を公表。実用的な攻撃は確認されていないものの、**新規開発での利用を推奨しない方針**を示した。
  https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/2026/Classic-McEliece_261001.html

BSIによるClassic McElieceの取扱い

- Classic McElieceは、NISTのPQC標準化プロセスにおける第4ラウンド候補であり、**2026年6月にISO/IECにおいて標準化**。暗号文が特に小さい一方、公開鍵が非常に大きいという特徴を持つ。
- 新規開発や新たな暗号アプリケーションの計画において、**Classic McElieceの利用を避ける※ことを推奨**。
  ※代替としてFrodoKEM、ML-KEM又はHQC（対応する標準が公表され次第）の利用を推奨。
- 現行の技術指針※では、**Classic McElieceをハイブリッド構成に限定して推奨**しており、従来型暗号と同等の安全性は確保。
  ※TR-02102-1。2027年初頭に予定される次期改訂で推奨内容を見直す方針。
- 鍵共有について、遅くとも**2031年までにPQCへの移行を完了することを引き続き強く推奨**。
- 暗号解析の進展に備え、暗号アジリティの確保及びハイブリッド構成の採用の重要性を強調。

Classic McElieceの安全性に関する研究

- Classic McElieceに対しては、**従来**、公開鍵から秘密鍵を復元する構造的攻撃に**2^{3000}を超える計算量が必要と推定**。
- 近年、公開鍵に用いられる特殊な構造を識別する攻撃手法や、識別攻撃を応用した鍵復元攻撃が相次いで提案。
- **2026年9月の研究では計算量が2^{99}～2^{102}に低下**すると推定※。
  ※最新の研究成果は十分な検証を経ておらず、計算量推定や攻撃コストは精査が必要。
- Classic McElieceに対し、実用的な攻撃が可能になったわけではない。

BSI文書に記載された計算量の推移

研究（時期）	攻撃種類	推定計算量
従来	鍵復元	2^{3000} 超
Ran24 (2024.7)	識別	2^{683} 以上
HW26 (2025.9)	識別	2^{550} 以上
BLRT26 (2026.6)	鍵復元	2^{742} 以上
GIJS26 (2026.8)	識別	2^{120}～2^{124}
	鍵復元	2^{140}～2^{148}
Wei26 (2026.9)	鍵復元	2^{99}～2^{102}

※「識別攻撃」は、公開鍵に用いられる特殊な構造を識別する攻撃。
識別に成功しても、直ちに秘密鍵を復元できるわけではない。
「鍵復元攻撃」は、公開鍵から秘密鍵を復元し、暗号文の復号を可能にする攻撃。

（参考）LMS／XMSSの規定状況（米国①）

➢ 米国NISTでは、LMS及びXMSSを標準化するとともに、ステート管理の必要性から一般的な用途での利用は想定していない。

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^{MT}).

【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・バリアントであるHierarchical Signature System（HSS） およびマルチツリーXMSS（XMSS^{MT}）も対象に含まれる。

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^{MT}). 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）】

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^{MT}）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。

（参考）LMS／XMSSの規定状況（米国②）

➢ 米国CNSA 2.0（2022年）では、ML-DSAやSLH-DSAが標準化されていなかったことや、ソフトウェア・ファームウェア署名への対応の緊急性等を踏まえ、既に標準化されていたLMS及びXMSSを採用し、早期導入を推奨。

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）】

ソフトウェア及びファームウェアの署名用アルゴリズム

ソフトウェア及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既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。

ソフトウェア及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に記載されている全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の全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：ソフトウェア及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	全ての分類レベルにおいて、全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	全ての分類レベルにおいて、全てのパラメータが承認済み。

（参考）LMS／XMSSの規定状況（米国③）

- 米国CNSA 2.0のFAQ（2024年）では、ML-DSAの利用を認める一方、LMSやXMSSを用いた早期の移行を推奨。
- また、HSS、XMSSMT及びSLH-DSAの利用は認めていない。

米国　国家安全保障局（NSA）
“The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ” (2024.12)
https://www.nsa.gov/Press-Room/Digital-Media-Center/Document-Gallery/igtag/CNSA/

Q: 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。

（参考）LMS／XMSSの規定状況（米国④）

➢ 米国NSAのCSfC（Commercial Solutions for Classified：機密情報保護に民間製品を活用するためのプログラム）の技術要件文書（2026年）では、ソフトウェア・ファームウェア署名にLMS、XMSS及びML-DSAの３方式を認め、いずれか１方式の使用で要件を満たすことを明記。

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の規定状況（米国以外①）

➢ 各国の政府機関では、多くがLMS／XMSSを量子耐性を有する署名方式として位置付け、署名鍵の状態を適切に管理できる用途やソフトウェア更新等の特定用途での利用を推奨等している。

国名	LMS	XMSS	文書
カナダ	**推奨※** （署名を短時間に生成する必要がなく、秘密鍵の状態を適切に管理できる用途）	**推奨※** （署名を短時間に生成する必要がなく、秘密鍵の状態を適切に管理できる用途）	**カナダ サイバーセキュリティセンター** **"Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information – ITSP.40.111"**（2026.5） https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111
ドイツ	**推奨※** （ソフトウェア更新等の安全かつ確実な状態管理が保証できる用途）	**推奨※** （ソフトウェア更新等の安全かつ確実な状態管理が保証できる用途）	**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
フランス	**適切な選択肢※** （ソフトウェア更新等の署名回数が限定され状態を適切に管理できる用途）	**適切な選択肢※** （ソフトウェア更新等の署名回数が限定され状態を適切に管理できる用途）	**フランス 国家情報システムセキュリティ庁（ANSSI）** **“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
オランダ	**推奨** （署名回数に制限があり署名鍵の使用状態を厳格に管理できる用途）	**推奨※** （署名回数に制限があり署名鍵の使用状態を厳格に管理できる用途）	**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
イギリス	**推奨※** （ソフトウェア署名等、署名鍵の有効期間を通じて安全な状態管理ができる用途）	**推奨※** （ソフトウェア署名等、署名鍵の有効期間を通じて安全な状態管理ができる用途）	**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
スペイン	**記載なし** （以前からXMSSを推奨）	**推奨※** （ファームウェア・ソフトウェア更新の署名用途）	**スペイン 国家暗号センター（CCN）** **“CCN-TEC 009 BP/37: Recomendaciones para una transición postcuántica segura”**（2026.7） https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/boletines-pytec/495-ccn-tec-009-recomendaciones-transicion-postcuantica-segura/file

※量子耐性を有する暗号技術として明示的に位置付けているもの。

（参考）LMS／XMSSの規定状況（米国以外②）

国名	LMS	XMSS	文書
チェコ	推奨※ （ファームウェア・ソフトウェアの完全性保護用途に限定）	推奨※ （ファームウェア・ソフトウェアの完全性保護用途に限定）	チェコ NÚKIB **"Minimální požadavky na kryptografické algoritmy, v4.1"** (2026.3) https://portal.nukib.gov.cz/informacni-servis/podpurne-materialy/69a82264c32c1c948f0686a4
スロバキア	推奨※ （ファームウェア・ソフトウェアの完全性保護用途に限定）	推奨※ （ファームウェア・ソフトウェアの完全性保護用途に限定）	スロバキア NBÚ **"Odporúčania pre kryptografické algoritmy, v1.0"** (2025.10) https://www.nbu.gov.sk/data/att/3483.pdf
フィンランド	記載なし （承認暗号アルゴリズムの対象外）	記載なし （承認暗号アルゴリズムの対象外）	フィンランド Traficom **"Kryptografiset vahvuusvaatimukset – kansalliset turvallisuusluokat"** (2024.12) https://kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kryptografiset_vahvuusvaatimukset_-_kansalliset_turvallisuusluokat_1.pdf
ノルウェー	推奨※ （ソフトウェアの署名等の秘密鍵の状態を適切に管理できる用途）	推奨※ （ソフトウェアの署名等の秘密鍵の状態を適切に管理できる用途）	ノルウェー NSM **"NSM Cryptographic Recommendations"** (2025.3) https://nsm.no/advice-and-guidance/publications/cryptographic-recommendations
マレーシア	承認 （電子署名方式として承認）	承認 （電子署名方式として承認）	マレーシア CyberSecurity Malaysia **MySEAL 2.1 Approved Cryptographic Algorithms** https://mykripto.cybersecurity.my/index.php/services/myseal/myseal-category/aksa-myseal/aksa-myseal-approved
オーストラリア	記載なし （承認暗号アルゴリズムの対象外）	記載なし （承認暗号アルゴリズムの対象外）	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
ニュージーランド	記載なし （承認暗号アルゴリズムの対象外）	記載なし （承認暗号アルゴリズムの対象外）	ニュージーランド GCSB/NCSC **"New Zealand Information Security Manual, Version 3.9"** （2025.11） https://nzism.gcsb.govt.nz/

※量子耐性を有する暗号技術として明示的に位置付けているもの。

（参考）LMS／XMSSの利用状況

➢ LMS／XMSSについては、HSM等で対応が進んでおり、標準機能や追加機能での対応も確認されている。

企業名等	製品名等	LMS	XMSS	ML-DSA	SLH-DSA	状況
Thales	Luna HSM 【HSM】	◎ (*1)	○ (*2)	◎ (*1)	○ (*2)	(*1) https://thalesdocs.com/gphsm/luna/7/docs/pci/Content/sdk/extensions/pqc/post_quantum_algorithms.htm (*2) https://cpl.thalesgroup.com/sites/default/files/content/solution_briefs/field_document/2023-08/thales-luna-post-quantum-crypto-functionality-module-sb.pdf 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 【HSM】	○ (*4)	–	◎ (*3)	◎ (*3)	(*3) https://nshielddocs.entrust.com/security-world-docs/v13.9.0/nshield-security-world-v13-9-0-release-notes.pdf (*4) https://nshielddocs.entrust.com/pqcop-docs/v1.1.3/nshield-pqc-option-pack-v1-1-3-release-notes.pdf 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 【HSM】	○ (*5)	○ (*5)	○ (*5)	△ (*5)	(*5) https://utimaco.com/data-protection/gp-hsm/application-package/quantum-protect 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 【ネットワーク機器】	◎ (*6)	–	◎ (*6)	–	(*6) https://www.cisco.com/c/en/us/td/docs/switches/lan/c9000/sec-crypto/tws/trustworthy-systems-guide/post-quantum-cryptography.html 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 【TPM】	—	◎ (*7)	–	–	(*7) https://www.infineon.com/ja/part/OPTIGA-TPM-SLB-9672-FW15 (*8) https://trustedcomputinggroup.org/new-computing-specification-implements-pqc-measures-to-protect-users-from-quantum-attacks/ 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。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。）
TCG	＜TPM 2.0＞	—	—	◎ (*8)	–	
Microsoft	Windows Server 2025 (AD CS) 【OS･PKI基盤】	—	—	◎ (*9)	–	(*9) https://learn.microsoft.com/ja-jp/windows-server/identity/ad-cs/post-quantum-cryptography-overview 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。
Microsoft	SymCrypt 【暗号ライブラリ】	◎ (*10)	◎ (*10)	◎ (*10)	△ (*10)	(*10) https://techcommunity.microsoft.com/blog/microsoft-security-blog/microsofts-quantum-resistant-cryptography-is-here/4238780 及び https://learn.microsoft.com/en-us/windows/win32/seccng/cng-algorithm-identifiers Microsoftの暗号ライブラリSymCrypt（Windowsにも搭載）では、LMS、XMSS及びML-DSAの実装、及びSLH-DSAの開発を確認。Windowsの標準暗号API（CNG）では、ML-DSAに対応している一方、LMS、XMSS及びSLH-DSAについては、Windows標準の暗号プロバイダーでは未実装。なお、SLH-DSAについては、CNGのアルゴリズム識別子及び.NET 10のAPI（試験的機能）として定義済み。

（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

資料３－１

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

前回会合からの主な修正点について

1．ML-DSA-44の取扱いについて

→ML-DSA-44を表２に掲載する方針を整理するとともに、
乱数生成器のセキュリティ強度に応じてCategory 1又はCategory 2となることを明記。（→p10）
また、Category 3以上の利用を推奨する注釈を付す案を整理。（→p10）

2．SLH-DSAのCategory 1の取扱いについて

→現時点での利用状況等を踏まえ、表２には掲載しない方針を整理。（→P10）

3．CNSA 2.0におけるML-DSA-87への限定について

→CNSA 2.0では、ML-DSA-87が指定されていることを確認。（→p13）
ただし、CNSA 2.0は米国の国家安全保障システム向けの暗号要件で、使用される暗号技術を限定しており、
目的や対象が異なるCRYPTREC暗号リストでは、ML-DSA-87に限定する必要はないと整理。（→p10）

4．CNSA 2.0におけるML-DSAの事前ハッシュの禁止について

→CNSA 2.0では、ML-DSAの事前ハッシュ（HashML-DSA）の利用は認められていないことを確認。（→p13）
HashML-DSAは、大容量のデータに署名する場合や、署名装置にデータ全体を渡せない場合に有用であり、
CNSA 2.0との目的や対象の違いを踏まえれば、CRYPTREC暗号リストで除外する必要はない。(→p10)

5．暗号利用モード等に関する注釈の整理について

→表１及び表２の暗号利用モード等に関する注釈を整理。（→p20・21）

次ページ以降の黄マーカー部分が前回会合からの修正箇所

検討ポイント①　セキュリティカテゴリの記載方法

➢ **セキュリティカテゴリ**は、暗号技術の**セキュリティ水準を利用者が把握する上で参考**となり、暗号技術を**選択する上でも重要な要素**であり、表２に記載することとしたが、その**記載方法や定義は利用者にわかりやすいか。**

【考え方】

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

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

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

✓**カテゴリの定義**については、米国NISTが2016年12月に公表したPQC標準化公募の際に示した記述をベースとし、暗号技術の観点からの正確性と、行政職員が参照する観点からの平易さ・利便性を総合的に勘案しており、**2026年3月改訂の記載内容は適当**。なお、列名の変更に伴う修正を実施。

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

変更

技術分類		暗号技術		セキュリティカテゴリ(注B1)
公開鍵暗号	署名	－	－	－
	鍵共有	ML-KEM	ML-KEM-768	Category 3
			ML-KEM-1024	Category 5
共通鍵暗号		AES	AES-192	Category 3
			AES-256	Category 5
ハッシュ関数		SHA2	SHA-384	Category 4
			SHA-512	（後述）
		SHA3	SHA3-384	Category 4
			SHA3-512	（後述）

（注B1）~~セキュリティのカテゴリを合わせて記載する。~~各セキュリティカテゴリはNISTの“Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”に従い、次のように、セキュリティカテゴリ名の右に記載の鍵探索又は衝突探索と同程度以上の計算資源が攻撃に必要であることを意味する。

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

（参考）セキュリティカテゴリの定義（米国NIST 2016年）

➢ 米国NISTは、2016年のPQC標準化公募において、ブロック暗号に対する鍵探索又はハッシュ関数に対する衝突探索に必要な計算資源を基準として、５段階のセキュリティカテゴリを定義。

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

4.A.5 Security Strength Categories（抜粋）

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

1) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 128-bit key (e.g. AES128)
2) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 256-bit hash function (e.g. SHA256/ SHA3-256)
3) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 192-bit key (e.g. AES192)
4) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 384-bit hash function (e.g. SHA384/ SHA3-384)
5) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 256-bit key (e.g. AES 256)

【仮訳（機械翻訳ベース）】

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

1) 当該セキュリティ定義を破る攻撃には、128ビット鍵のブロック暗号（例：AES128）における鍵探索に要する計算資源と同等以上の計算資源が必要であること。
2) 当該セキュリティ定義を破る攻撃には、256ビットのハッシュ関数（例：SHA256/SHA3-256）における衝突探索に要する計算資源と同等以上の計算資源が必要であること。
3) 当該セキュリティ定義を破る攻撃には、192ビット鍵のブロック暗号（例：AES192）における鍵探索に要する計算資源と同等以上の計算資源が必要であること。
4) 当該セキュリティ定義を破る攻撃には、384ビットのハッシュ関数（例：SHA384/SHA3-384）における衝突探索に要する計算資源と同等以上の計算資源が必要であること。
5) 当該セキュリティ定義を破る攻撃には、256ビット鍵のブロック暗号（例：AES256）における鍵探索に要する計算資源と同等以上の計算資源が必要であること。

（参考）NIST SP 800-57 Rev. 6 (Initial Public Draft) ①

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

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

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

4.6.1. Cryptographic Algorithm Security Strengths（抜粋）

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

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

Table 2. Security strength categories for post-quantum algorithms

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

【仮訳（機械翻訳ベース）】

4.6.1. 暗号アルゴリズムのセキュリティ強度（抜粋）

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

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

表2. 耐量子アルゴリズムのセキュリティ強度区分

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

（参考）NIST SP 800-57 Rev. 6 (Initial Public Draft) ②

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

NIST SP 800-57 Rev. 6 (Initial Public Draft)　(2025.12)
"Recommendation for Key Management: Part 1 – General”
https://csrc.nist.gov/pubs/sp/800/57/pt1/r6/ipd

Appendix E. Glossary（抜粋）

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

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

【仮訳（機械翻訳ベース）】

付録E. 用語集（抜粋）

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

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

（参考）カテゴリ関連記載：FIPS 203･204･205

➢ 米国NISTが標準化したFIPS203～205については、各パラメータセットに対応するセキュリティカテゴリが明記されている。

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

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

8. Parameter Sets（抜粋）

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

Table 2. Approved parameter sets for ML-KEM

	n	q	k	η_1	η_2	d_u	d_v	required RBG strength (bits)
ML-KEM-512	256	3329	2	3	2	10	4	128
ML-KEM-768	256	3329	3	2	2	10	4	192
ML-KEM-1024	256	3329	4	2	2	11	5	256

FIPS204 “Module-Lattice-Based Digital Signature Standard”

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

4. Parameter Sets（抜粋）

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

Table 1. ML-DSA parameter sets

Parameters (see Sections 6.1 and 6.2 of this document)	Values assigned by each parameter set ML-DSA-44	ML-DSA-65	ML-DSA-87
q - modulus [see §6.1]	8380417	8380417	8380417
ζ - a 512th root of unity in $\mathbb{Z}_q$ [see §7.5]	1753	1753	1753
d - # of dropped bits from $\mathbf{t}$ [see §6.1]	13	13	13
τ - # of ± 1's in polynomial c [see §6.2]	39	49	60
λ - collision strength of $\tilde{c}$ [see §6.2]	128	192	256
γ_1 - coefficient range of $\mathbf{y}$ [see §6.2]	2^{17}	2^{19}	2^{19}
γ_2 - low-order rounding range [see §6.2]	$(q-1)/88$	$(q-1)/32$	$(q-1)/32$
(k, ℓ) - dimensions of $\mathbf{A}$ [see §6.1]	(4,4)	(6,5)	(8,7)
η - private key range [see §6.1]	2	4	2
$\beta = \tau \cdot \eta$ [see §6.2]	78	196	120
ω - max # of 1's in the hint $\mathbf{h}$ [see §6.2]	80	55	75
Challenge entropy $\log_2 \binom{256}{\tau} + \tau$ [see §6.2]	192	225	257
Repetitions (see explanation below)	4.25	5.1	3.85
Claimed security strength	Category 2	Category 3	Category 5

FIPS205 “Stateless Hash-Based Digital Signature Standard”

https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.205.pdf

11. Parameter Sets（抜粋）

Concretely, the parameter sets with $n = 16$ are
claimed to be in security category 1,
the parameter sets with $n = 24$ are
claimed to be in security category 3,
and the parameter sets with $n = 32$ are
claimed to be in security category 5.

Table 2. SLH-DSA parameter sets

	n	h	d	h'	a	k	lg_w	m	security category	pk bytes	sig bytes
SLH-DSA-SHA2-128s SLH-DSA-SHAKE-128s	16	63	7	9	12	14	4	30	1	32	7 856
SLH-DSA-SHA2-128f SLH-DSA-SHAKE-128f	16	66	22	3	6	33	4	34	1	32	17 088
SLH-DSA-SHA2-192s SLH-DSA-SHAKE-192s	24	63	7	9	14	17	4	39	3	48	16 224
SLH-DSA-SHA2-192f SLH-DSA-SHAKE-192f	24	66	22	3	8	33	4	42	3	48	35 664
SLH-DSA-SHA2-256s SLH-DSA-SHAKE-256s	32	64	8	8	14	22	4	47	5	64	29 792
SLH-DSA-SHA2-256f 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、利用者にとってわかりやすい記載方法は何か。

【考え方】

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

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

<表２　耐量子計算機暗号（PQC）リスト>

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

技術分類		暗号技術		セキュリティカテゴリ(注B1)
公開鍵暗号	署名	－	－	－
	鍵共有	ML-KEM	ML-KEM-768	Category 3
			ML-KEM-1024	Category 5
共通鍵暗号		AES	AES-192	Category 3
			AES-256	Category 5
ハッシュ関数		SHA2	SHA-384	Category 4
			SHA-512	Category 4 (注B4)
		SHA3	SHA3-384	Category 4
			SHA3-512	Category 4 (注B4)

（注B1）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B4）512ビットのハッシュ関数に対する衝突探索には、384ビットのハッシュ関数に対する衝突探索よりも大きな計算資源が必要となるため、ハッシュ関数の衝突探索を基準とする最上位のCategory 4として記載する。

検討ポイント③　Category 1・2の取扱い

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

【考え方】

✓ **表2**は、PQC移行後も**長期的に利用していく暗号技術を示すリスト**としての性格を有し、掲載後の削除には政府調達や相互運用性への影響等を考慮する必要があることから、**Category 1・2の暗号技術を積極的に掲載することは適当でない。**

- 量子コンピュータ技術の進展状況等を踏まえ、表１については、暗号技術検討会が危殆化したと決定した場合は、電子政府推奨暗号から外れ、表２のみが電子政府推奨暗号として残ることが想定される。そのため、2035年以降も利用予定のシステムについては、表１ではなく表２を参照して整備することになると考えられる。
- 「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」では、128ビットセキュリティは2031～2040年は「利用可」だが、2041年以降は「移行完遂期間」とされ、2051年以降は順次「利用不可」となる。

✓ **公開鍵暗号**のうち**ML-KEM**については、**Category 3・5の実装が広く見られ**、Category 1でなければPQC移行できない具体的な支障も現時点では確認されていないことから、**ML-KEM-512（Category 1）は表2に掲載しないことが適当。**（署名方式については検討ポイント④を参照）

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

※表２はそもそも量子コンピュータ（CRQC）への耐性を有する暗号技術を掲載するものであるが、例えばAES-128は量子コンピュータによるGroverのアルゴリズムにより、AES-192/256と比べ安全余裕が小さくなることから、表２にブロック暗号及びハッシュ関数のCategory 1・2を掲載することは適当ではない。

✓ Category 1・2の暗号技術について、現時点で表２に掲載しないことは、将来的な掲載を否定するものではなく、今後の利用動向等を注視することが適当。

＜参考：関係する暗号技術の例＞

技術分類		暗号技術		セキュリティカテゴリ
公開鍵暗号	署名	ML-DSA	（略）	（略）
		SLH-DSA	（略）	（略）
	鍵共有	ML-KEM	~~ML-KEM-512~~	~~Category 1~~
			ML-KEM-768	Category 3
			ML-KEM-1024	Category 5
共通鍵暗号		AES	~~AES-128~~	~~Category 1~~
			AES-192	Category 3
			AES-256	Category 5
ハッシュ関数		SHA2	~~SHA-256~~	~~Category 2~~
			~~SHA-512/256~~	~~Category 2~~
			SHA-384	Category 4
			SHA-512	Category 4
		SHA3	~~SHA3-256~~	~~Category 2~~
			SHA3-384	Category 4
			SHA3-512	Category 4

※Camellia、KCipher-2、SHAKEについては後述。

検討ポイント④　署名方式のCategory 1・2の取扱い

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

【考え方】

✓ **ML-DSA-44**については、**証明書やDNSSEC等で広く利用**される可能性が高く、**表２に掲載することが適当。【要精査】**
※米国CNSA 2.0ではML-DSAの使用は、ML-DSA-87に限定し、事前ハッシュ（HashML-DSA）の利用も認めていないが、CRYPTREC暗号リストとは目的や対象が異なるため、これらの制限を設ける必要はない。

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

＜ML-DSA-44の掲載について＞

✓ Category1・2の暗号技術の利用は最低限としてもらいたいことから、**「ML-DSA-44」に対して次の注釈を付す**ことが適当

（注B2）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。【要精査；「ML-DSA-65又はML-DSA-87」と明記すべきか】

✓ ML-DSA-44は、鍵生成に用いる**乱数生成器のセキュリティ強度によりセキュリティカテゴリが異なる**ことから**注釈を付し、その条件を明確化することが適当。**
※乱数生成器のセキュリティ強度に応じてCategory 1又はCategory 2となるが、①両カテゴリの実質的な安全性の差を単純に評価することは難しいこと、②可能な限りCategory 3以上の利用を推奨する方針であること、③政府情報システムの調達時に乱数生成器のセキュリティ強度まで把握することは困難であること等を踏まえ、192ビット以上のセキュリティ強度を必須とはせず、カテゴリが異なる条件を明確化することとした。

（注B3）ML-DSA-44について、鍵生成に用いる乱数生成器のセキュリティ強度が192ビット以上の場合はCategory 2、128ビット以上192ビット未満の場合はCategory 1となる。【要精査；192ビット以上の利用に限るべきか】

＜参考：関係する暗号技術の例＞

技術分類		暗号技術		セキュリティカテゴリ(注８)
公開鍵暗号	署名	ML-DSA	ML-DSA-44(注B2)	Category 1(注B3) Category 2(注B3)
			ML-DSA-65	Category 3
			ML-DSA-87	Category 5
		SLH-DSA	~~SLH-DSA-SHA2-128[s/f]~~	~~Category 1~~
			~~SLH-DSA-SHAKE-128[s/f]~~	~~Category 1~~
			SLH-DSA-SHA2-192[s/f]	Category 3
			SLH-DSA-SHAKE-192[s/f]	Category 3
			SLH-DSA-SHA2-256[s/f]	Category 5
			SLH-DSA-SHAKE-256[s/f]	Category 5
	鍵共有	ML-KEM	~~ML-KEM-512~~	~~Category 1~~
			ML-KEM-768	Category 3
			ML-KEM-1024	Category 5
共通鍵暗号		AES	~~AES-128~~	~~Category 1~~
			AES-192	Category 3
			AES-256	Category 5
ハッシュ関数		SHA2	~~SHA-256~~	~~Category 2~~
			~~SHA-512/256~~	~~Category 2~~
			SHA-384	Category 4
			SHA-512	Category 4
		SHA3	~~SHA3-256~~	~~Category 2~~
			SHA3-384	Category 4
			SHA3-512	Category 4

※Camellia、KCipher-2、SHAKEについては後述。

（参考）海外政府機関による推奨状況①

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

* 2030年以降は非推奨

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”

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

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

Table 4.2 | Recommended parameter instantiations of the cryptographic primitives.

（参考）米国CNSA2.0におけるML-DSAの規定状況

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

米国　国家安全保障局（NSA）
“The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ” (2024.12)
https://www.nsa.gov/Press-Room/Digital-Media-Center/Document-Gallery/igtag/CNSA/

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

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

Table: Commercial National Security Algorithm Suite 2.0

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

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

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

【仮訳（機械翻訳ベース）】

Q: CNSA 2.0とは何ですか？

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

表：Commercial National Security Algorithm Suite 2.0

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

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

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

（参考）ML-DSAのセキュリティカテゴリについて

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

米国　国立標準技術研究所（NIST）
FIPS204 “Module-Lattice-Based Digital Signature Standard" (2024.8)
https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.204.pdf

3.6.1 Randomness Generation

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

【仮訳（機械翻訳ベース）】

3.6.1 乱数生成

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

（参考）ML-DSA･SLH-DSAのIETFでの標準化状況

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

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

- ✓ **X.509**及び**CMS**では、**ML-DSA**及び**SLH-DSA**の各パラメータセットを利用するための**仕様がRFC化**されている。
- ✓ **TLS**では、**ML-DSA**の各パラメータセットをハンドシェイク署名等に利用するための**仕様が検討中**（Internet-Draft）で、**IETFのTLS WG文書となっている。**
  SLH-DSAについても、同様の仕様が個人提出のInternet-Draftとして提案されたが、**現在は失効**しており、WGドラフトにはなっていない。
  ※署名サイズがML-DSAでは2.4~4.6KBなのに対し、SLH-DSAでは7.9～50KB程度と大きいため、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

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

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

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

(*1) Cloudflare, “1.1.1.1 now supports post-quantum DNSSEC” https://blog.cloudflare.com/post-quantum-dnssec-1111/

(*2) Cloudflare, “Post-quantum authentication to origins is now supported” https://blog.cloudflare.com/post-quantum-authentication-to-origins/

(*3) Google Cloud KMS, “Digital signatures” https://docs.cloud.google.com/kms/docs/digital-signatures?hl=ja

(*4) AWS KMS, “ML-DSA keys in AWS KMS” https://docs.aws.amazon.com/kms/latest/developerguide/mldsa.html

(*5) OpenSSL, “OpenSSL 3.5 Final Release” https://openssl-library.org/post/2025-04-08-openssl-35-final-release/

検討ポイント⑤ Camellia・KCipher-2・SHAKEの取扱い

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

【考え方】

<Camellia>

✓鍵長は128, 192, 256ビットがあり、2024年度外部評価報告書※において、同じ鍵長のAESと同等の安全性とされる。

✓このため、**128ビット鍵長**は、**Category 1相当**であり、検討ポイント③の整理を踏まえ、**表２に掲載しない**ことが適当。
また、**192ビット及び256ビット鍵長**は、それぞれ**「Category 3」、「Category 5」として表２に掲載する**ことが適当。

<KCipher-2>

✓鍵長は128ビットがあり、2024年度外部評価報告書※において、AES-128と同等の安全性とされる。

✓このため、**Category 1相当**であり、検討ポイント③の整理を踏まえ、**表２に掲載しない**ことが適当。

<SHAKE128>

✓2024年度外部評価報告書※において、出力長がn(≧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(≧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。

※量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価 2024年度版（CRYPTREC-EX-3401-2024）

検討ポイント⑥　暗号利用モード等の取扱い

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

【考え方】

＜暗号利用モード及びメッセージ認証コード＞

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

＜認証暗号（ChaCha20-Poly1305）＞

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

＜エンティティ認証＞

- ✓エンティティ認証は、暗号プリミティブそのものではなく、それらを組み合わせて構成されるプロトコルレイヤの技術。**ISO/IEC 9798**で認証メカニズムが規定されるが、具体的な**暗号プリミティブやパラメータ等は一意に定まらない**※2。
- ✓エンティティ認証の安全性は、使用する暗号プリミティブの安全性だけでなく、プロトコル全体の設計・実装に依存。
- ✓そのため、具体的にどのような構成が耐量子性を有すると判断されたのかが不明確になるおそれがあり、単一の暗号技術と同じ粒度で**CRQCへの耐性を有すると判断することは難しく、表２の掲載を保留**する。

※１　2024年度外部評価報告書：量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価 2024年度版（CRYPTREC-EX-3401-2024）
※２　ISO/IEC 9798 プロトコルの安全性評価（CRYPTREC-EX-2013-2010）

（参考）2024年度外部評価報告書について

- 2024年度外部評価報告書※では、Q1モデルを主たる評価の前提とし、鍵長等に応じた安全性の目安を整理。
  量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価 2024年度版（CRYPTREC-EX-3401-2024）
- ハッシュ関数については、BHTアルゴリズムによる量子衝突探索を踏まえ、出力長・キャパシティ等に応じた安全性の目安を整理。
- また、既存の古典的安全性評価に基づくデータ量・クエリ回数等の制約がQ1モデルでも基本的に維持されることを確認。

＜参考：Q1モデルとQ2モデル＞
【Q1モデル】攻撃者は量子計算能力を有するが、オラクルへのアクセスは古典的クエリに限定されるモデル。
【Q2モデル】攻撃者は量子計算能力を有し、オラクルへのアクセスにおいて量子重ね合わせ状態のクエリが可能であるモデル。GCMやCBC-MAC等に対する多項式時間攻撃が報告されているが、その成立には秘密鍵を含む処理への量子オラクルアクセスが攻撃者に与えられる必要があり、通常の実運用とは大きく異なる前提に基づくものと整理

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

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

（2024年度外部評価報告書の表５を一部表記を変更・簡略化）
※Q1モデルで安全性が期待できる範囲。古典計算機のみが使える典型的な安全性評価と整合性を取るため、単一鍵の安全性に焦点を当て、量子計算機のリソースとしては、小さい多項式サイズの量子計算機が１つ使え、QRAMは必要な分だけ大きなものを使える状態。
※この表にある暗号技術については、Q1モデルにおいて（古典的に考慮すべき事項から追加して）現状考慮すべきと思われる事柄はGrover のアルゴリズムによる鍵回復のみである。

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

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

（2024年度外部評価報告書の表６を一部表記を変更・簡略化）
※BHTのアルゴリズムを適用する際に必要な計算時間と量子メモリの概算値。
※計算時間の値はそのまま、安全性が期待できる時間の範囲の上限に対応する。
※なお出力長とキャパシティの単位はいずれもビットである。
※スポンジ構造のハッシュ関数、特にXOF（SHAKE128，SHAKE256）については、内部状態のキャパシティ部分で衝突を見つける攻撃も考慮に入っていることに注意。

検討ポイント⑦　暗号利用モード等に関する注釈

➢ **表２**（耐量子計算機暗号（PQC）リスト）に**暗号利用モード等を追加**することに当たり、組み合わせて利用する暗号技術に関する注釈をどのように記載すべきか。

【考え方】

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

（参考：組み合わせる暗号技術）
暗号利用モード＝共通鍵暗号のうちブロック暗号
CMAC＝共通鍵暗号のうちブロック暗号
HMAC＝ハッシュ関数
ISO/IEC 9798-2＝共通鍵暗号
ISO/IEC 9798-3＝公開鍵暗号のうち署名
ISO/IEC 9798-4＝メッセージ認証コード

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

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

<表１ 現行暗号リスト>

技術分類	（略）
（略）	（略）
暗号利用モード（注A4） | （略）	（略）
メッセージ認証コード（注A4）	（略）
認証暗号	（略）
エンティティ認証（注A4）	（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B6） | （略）	（略）
メッセージ認証コード（注B6）	（略）
認証暗号	（略）

（注A4）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B6）表２に掲載する他の技術分類の暗号技術と組み合わせて利用すること。

検討ポイント⑧　暗号利用モードに係る注釈の取扱い

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

【考え方】

✓**「XTS」に係る注釈**
→表１の「XTS」に付される注５について、前段（ブロック暗号に関する規定）は、64ビットブロック暗号が表２に存在しないことから（追加予定もないことから）、同様の注釈は不要。
→一方、後段（利用用途及び実装方法に関する規定）は、XTS自体の制限事項であるため同様の注釈を表２の「XTS」にも付すことが適当。

✓**「認証付き秘匿モード」に係る注釈**
→表１の「認証付き秘匿モード」に付される注６について、ブロック暗号と組み合わせることで認証暗号として利用できることを示すものであり、同様の注釈を表２の「認証付き秘匿モード」にも付すことが適当。
　なお、「暗号利用モード」に付される注釈により、組み合わせる暗号技術が表２に掲載されたものに限定されることとなる。

✓**「GCM」に係る注釈**
→表１の「GCM」に付される注７について、初期化ベクトル長に関する推奨事項であり、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A5）
	認証付き秘匿モード（注A6）	CCM
		GCM（注A7）
（略）		（略）

（注A5）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A6）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A7）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B7）	
	認証付き秘匿モード（注B8）	CCM	
		GCM（注B9）	

（注B7）~~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B8）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B9）初期化ベクトル長は96ビットを推奨する。

検討ポイント⑨　用語・表記の統一

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

【考え方】

✓ 同一概念を異なる用語で表記している場合、原則として**用語を統一**し、使い分けを明確化することが適当。

✓「量子コンピュータ」と「量子計算機」について、原則として「**量子コンピュータ**」**に統一**し、**初出時には「量子コンピュータ（量子計算機）」と併記**することが適当。ただし、「**耐量子計算機暗号（PQC）**」等の**既に定着している名称**は変更しないことが適当。

＜長音表記について＞

✓ **外来語の長音表記**（英語の語末の「-er」「-or」「-ar」等）については、公用文では**原則として長音符号「ー」を用いることとされているが、慣用に応じて「ー」を省略する**ことも認められている。

✓ このため、慣用や専門用語としての定着状況、政府関係文書における使用実態等を踏まえ、**語ごとに表記を統一**することが適当。具体的には、「コンピュータ」「パラメータ」「カテゴリ」については、長音符号を付さない表記とすることが適当。

（参考）外来語の表記に関する文書

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

文化庁　外来語の表記（平成３年内閣告示第２号）

https://www.bunka.go.jp/kokugo_nihongo/sisaku/joho/joho/kijun/naikaku/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

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
エ　長音は、原則として長音符号を使って書く
長音は、長音符号を使って書く。
例）エネルギー　オーバーコート　グループ　ゲーム　ショー　メール
ただし、次のようなものは慣用に従い、長音符号を用いずに書く。
例）バレエ（舞踊）　ミイラ　エイト　ペイント　レイアウト　サラダボウル
英語の語末の-er、-or、-arなどに当たるものは、ア列の長音とし、長音符号を用いて書くのが原則である。そのほか、-ty、-ryなど、yで終わる語も長音符号を用いて書く。
例）コンピューター（computer）　エレベーター（elevator）
カレンダー（calendar）　コミュニティー（community）
カテゴリー（category）
（略）

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

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

1.2　現行の規定（抜粋）
英語などの語末の-er，-or，-ar，-yは原則として長音符号をつけて表記し，のばして発音する。
〈例〉 オーソリティー　コンピューター　エレベーター　パーティー

（参考）電子政府推奨暗号リスト～再改定後のイメージ

暗号技術検討会及び関連委員会（以下「CRYPTREC」という。）により安全性（セキュリティ）及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。なお、利用する鍵長について、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。

＜表１　現行暗号リスト＞

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

＜表２　耐量子計算機暗号（PQC）リスト＞

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

技術分類		暗号技術		セキュリティカテゴリ
公開鍵暗号	署名	ML-DSA	ML-DSA-44	Category 2
			ML-DSA-65	Category 3
			ML-DSA-87	Category 5
		SLH-DSA	SLH-DSA-SHA2-192[s/f]	Category 3
			SLH-DSA-SHAKE-192[s/f]	Category 3
			SLH-DSA-SHA2-256[s/f]	Category 5
			SLH-DSA-SHAKE-256[s/f]	Category 5
	鍵共有	ML-KEM	ML-KEM-768	Category 3
			ML-KEM-1024	Category 5
共通鍵暗号	ブロック暗号	AES	AES-192	Category 3
			AES-256	Category 5
		Camellia	Camellia-192	Category 3
			Camellia-256	Category 5
	ストリーム暗号	–	–	–
ハッシュ関数		SHA2	SHA-384	Category 4
			SHA-512	Category 4
		SHA3	SHA3-384	Category 4
			SHA3-512	Category 4
		SHAKE	SHAKE256	Category 4
暗号利用モード	秘匿モード		CBC	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。
			CFB	
			CTR	
			OFB	
			XTS	
	認証付き秘匿モード		CCM	
			GCM	
メッセージ認証コード			CMAC	
			HMAC	
認証暗号			ChaCha20-Poly1305	Category 5

＜表２に掲載されない暗号技術＞
SLH-DSA-SHA2-128[s/f]（Category 1）
SLH-DSA-SHAKE-128[s/f]（Category 1）
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

資料３－２

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）【改定イメージ】

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

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下「CRYPTREC」という。）により安全性（セキュリティ）及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。なお、利用する鍵長について、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[3]の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。

＜表１　現行暗号リスト＞

技術分類		暗号技術
公開鍵暗号	署名	DSA（注~~１~~Ａ１）
		ECDSA
		EdDSA
		RSA-PSS
		RSASSA-PKCS1-v1_5
	守秘	RSA-OAEP
	鍵共有	DH
		ECDH（注~~２~~Ａ２）
共通鍵暗号	~~64ビットブロック暗号（注3）~~	~~該当なし~~
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128（注~~４~~Ａ３）
		SHAKE256（注~~４~~Ａ３）
（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（注Ａ４）	秘匿モード	CBC
		CFB
		CTR
		OFB
		XTS（注~~５~~Ａ５）
	認証付き秘匿モード（注~~６~~Ａ６）	CCM
		GCM（注~~７~~Ａ７）
メッセージ認証コード（注Ａ４）		CMAC
		HMAC
認証暗号		ChaCha20-Poly1305
エンティティ認証（注Ａ４）		ISO/IEC 9798-2
		ISO/IEC 9798-3
		ISO/IEC 9798-4

（注~~１~~Ａ１）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~~Ａ２）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~~Ａ３）ハッシュ長は256ビット以上とすること。

（注Ａ４）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~~５~~Ａ５）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~~Ａ６）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~~Ａ７）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コンピュータ（量子計算機（；CRQC：Cryptographically Relevant Quantum Computer）への耐性を有することが確認された暗号技術のリスト[4]。

技術分類		暗号技術		セキュリティカテゴリ（注Ｂ１）
公開鍵暗号	署名	ML-DSA	ML-DSA-44（注Ｂ２）	Category 1（注Ｂ３） Category 2（注Ｂ３）
			ML-DSA-65	Category 3
			ML-DSA-87	Category 5
		SLH-DSA	SLH-DSA-SHA2-192[s/f]	Category 3
			SLH-DSA-SHAKE-192[s/f]	Category 3
			SLH-DSA-SHA2-256[s/f]	Category 5
			SLH-DSA-SHAKE-256[s/f]	Category 5
	鍵共有	ML-KEM	ML-KEM-768	Category 3
			ML-KEM-1024	Category 5
共通鍵暗号	ブロック暗号	AES	AES-192	Category 3
			AES-256	Category 5
		Camellia	Camellia-192	Category 3
			Camellia-256	Category 5
	ストリーム暗号	ー	ー	ー
ハッシュ関数		SHA2	SHA-384	Category 4
			SHA-512	Category 4（注Ｂ４）
		SHA3	SHA3-384	Category 4
			SHA3-512	Category 4（注Ｂ４）
		SHAKE	SHAKE256（注Ｂ５）	Category 4
暗号利用モード（注Ｂ６）	秘匿モード		CBC	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。
			CFB	
			CTR	
			OFB	
			XTS（注Ｂ７）	
	認証付き秘匿モード（注Ｂ８）		CCM	
			GCM（注Ｂ９）	
メッセージ認証コード（注Ｂ６）			CMAC	
			HMAC	
認証暗号			ChaCha20-Poly1305	Category 5

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~~８~~Ｂ１）~~セキュリティの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

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Ｂ２）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。

（注Ｂ３）ML-DSA-44について、鍵生成に用いる乱数生成器のセキュリティ強度が192ビット以上の場合はCategory 2、128ビット以上192ビット未満の場合はCategory 1となる。

（注Ｂ４）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。

（注Ｂ５）ハッシュ長は384ビット以上とする。

（注Ｂ６）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。

（注Ｂ７）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Ｂ８）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Ｂ９）初期化ベクトル長は96ビットを推奨する。

推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術[5]のリスト。なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[6]の規定に合致する鍵長を用いることが求められることに留意すること。

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM(注~~9~~ C１)
共通鍵暗号	64ビットブロック暗号(注~~10~~C２)	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~~Ｃ３)
ハッシュ関数		該当なし
暗号利用モード(注Ｃ４)	秘匿モード	該当なし
	認証付き秘匿モード(注~~12~~Ｃ５)	該当なし
メッセージ認証コード(注Ｃ４)		PC-MAC-AES
認証暗号		該当なし
エンティティ認証(注Ｃ４)		該当なし

(注~~9~~ Ｃ１)KEM (Key Encapsulating Mechanism) - DEM (Data Encapsulating Mechanism) 構成における利用を前提とする。

(注~~10~~Ｃ２)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~~Ｃ３)平文サイズは64ビットの倍数に限る。

(注Ｃ４)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~~12~~Ｃ５)CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

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

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

運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったとCRYPTRECにより確認された暗号技術[7]のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持[8]以外の目的での利用は推奨しない。なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[9]の規定に合致する鍵長を用いることが求められることに留意すること。

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5（注~~13~~Ｄ１）
	鍵共有	該当なし
共通鍵暗号	64ビットブロック暗号（注~~14~~Ｄ２）	3-key Triple DES（注~~15~~Ｄ３）
	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（注Ｄ４）	秘匿モード	該当なし
	認証付き秘匿モード（注~~16~~Ｄ５）	該当なし
メッセージ認証コード（注Ｄ４）		CBC-MAC（注~~17~~Ｄ６）
認証暗号		該当なし
エンティティ認証（注Ｄ４）		該当なし

（注~~13~~Ｄ１）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~~Ｄ２）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~~Ｄ３）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Ｄ４）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~~16~~Ｄ５）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~~Ｄ６）安全性の観点から、メッセージ長を固定して利用すべきである。

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

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

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

資料４

CRYPTREC暗号リストの改定（PQC対応）に対する意見公募について

意見公募の実施について

➢ **CRYPTREC暗号リストの改定（PQC対応）**について、暗号技術の利用状況等も考慮しつつ、幅広い観点から検討を行うため、**資料３－１及び資料３－２**を提示して、**意見を募集することとしてはどうか**。

意見募集の対象

CRYPTREC暗号リストの改定イメージ（資料３－２）を対象に意見募集。

※資料３－１は、改定イメージの考え方を説明する資料として併せて公表する。

※安全性評価等が完了していない段階で作成したものであり、確定したものではないことに留意。

ML-DSA及びSLH-DSAのCategory 1・2（ML-DSA-44及びSLH-DSA-[SHA2/SHAKE]-128[s/f]）について、利用状況や将来的な利用見込み等も踏まえたCRYPTREC暗号リストにおける取扱い（掲載に関する考え方及びその理由）について、特に意見を求めることとする。

意見募集の実施方法

募集主体：デジタル庁・総務省・経済産業省（CRYPTREC暗号リスト策定主体）

募集期間：２週間程度

募集方法：e-Gov、ウェブサイト等を通じて実施

意見募集の結果

事務局において整理し、タスクフォースに報告。

提出意見を踏まえ、タスクフォースで検討を行い、検討結果は暗号技術検討会に報告。

（今般のCRYPTREC暗号リスト改定を全面改定と扱うこととしてはどうか）

（参考）CRYPTREC暗号リストに係る意見募集の実施状況

- CRYPTREC暗号リストについては、2013年の策定時及び2023年の改定時に、リスト案に対する意見募集を実施している。（CRYPTREC暗号リストは、小改定等を除き10年程度の運用を想定して策定。）

意見募集	2003年策定時	2008年改訂骨子案	2013年改定時	2023年改定時
募集対象	電子政府推奨暗号リスト（案）	電子政府推奨暗号リストの改訂に関する骨子(案)	CRYPTREC暗号リスト（案）	CRYPTREC暗号リスト（案）
募集主体	総務省・経済産業省	総務省・経済産業省	総務省・経済産業省	デジタル庁・総務省・経済産業省
募集期間	2002年11月28日～同年12月25日（28日間）	2008年8月6日～同年9月5日（31日間）	2012年12月12日～2013年1月10日（30日間）	2023年3月9日～同年3月23日（15日間）
募集方法	確認できず	確認できず	e-Gov、電子メール等	e-Gov、電子メール、郵送
募集結果	２件の意見提出	７件の意見提出	６件の意見提出	４件の意見提出
案の決定日	2003年2月20日	2008年12月1日（意見募集結果の公表日）	2013年3月1日	2023年3月30日
参考URL	https://www.cryptrec.go.jp/report/cryptrec-rp-1000-2002-jp.pdf https://www.cryptrec.go.jp/events/2002/slides/2_fujimoto.pdf	https://www.cryptrec.go.jp/report/cryptrec-rp-1000-2008.pdf	https://public-comment.e-gov.go.jp/pcm/1040?CLASSNAME=PCM1040&id=595212035&Mode=2	https://public-comment.e-gov.go.jp/pcm/1040?CLASSNAME=PCM1040&id=290303011&Mode=2

資料５

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）。

NIST CSWP 39より

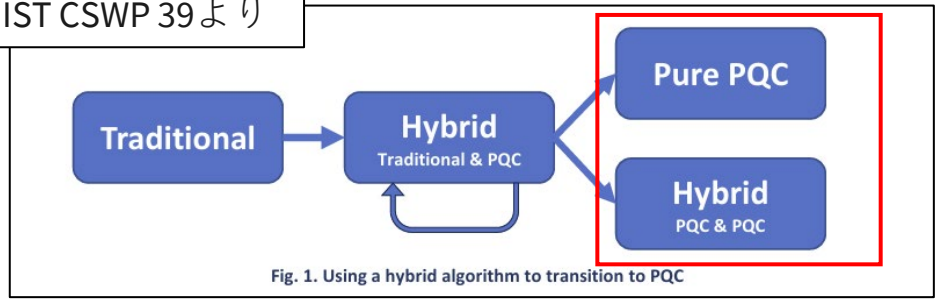


Fig. 1. Using a hybrid algorithm to transition to PQC

- **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様ではない。
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	鍵共有アルゴリズム • NIST SP 800-227(4.6. Multi-Algorithm KEMs and PQ/T Hybrids) [4] • NIST SP 800-56C Rev.2[3] [9] • draft-irtf-cfrg-hybrid-kems-07 [10] • draft-ietf-lamps-pq-composite-kem-12 [11][4] 署名アルゴリズム • draft-ietf-lamps-pq-composite-sigs-14 [12][4]
プロトコル	通信プロトコル • RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3 [13] ※4.1.1 Cryptographic Negotiationにより後方互換性を提供するが、混成方式ではない 証明書構造 • draft-ietf-lamps-certdiscovery-02 [18] • ITU-T X.509(9.8 Alternative cryptographic algorithms and digital signature extensions) [19]	通信プロトコル • draft-ietf-tls-hybrid-design-16 [14] • draft-ietf-mls-combiner-02 [15] • ETSI TS 103 744 [16] • IEEE 802.11 Hybrid PQC Proposal [17] • draft-ietf-lamps-pq-composite-kem-12 [11][4] 証明書構造 • draft-ietf-lamps-pq-composite-sigs-14 [12][4]
システム[5]	（後方互換性確保／安全性維持　共通） • 耐量子移行を考慮したPKIベースのハイブリッド設計・実装 Architecting PKI Hierarchies for Graceful PQ Migration(PQC Conference) [20] Hybrid PQC E-Mail Communication: Easing Migration Pain(PQC Conference) [21]	

cryptrec-ex-3503-2025.pdf

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

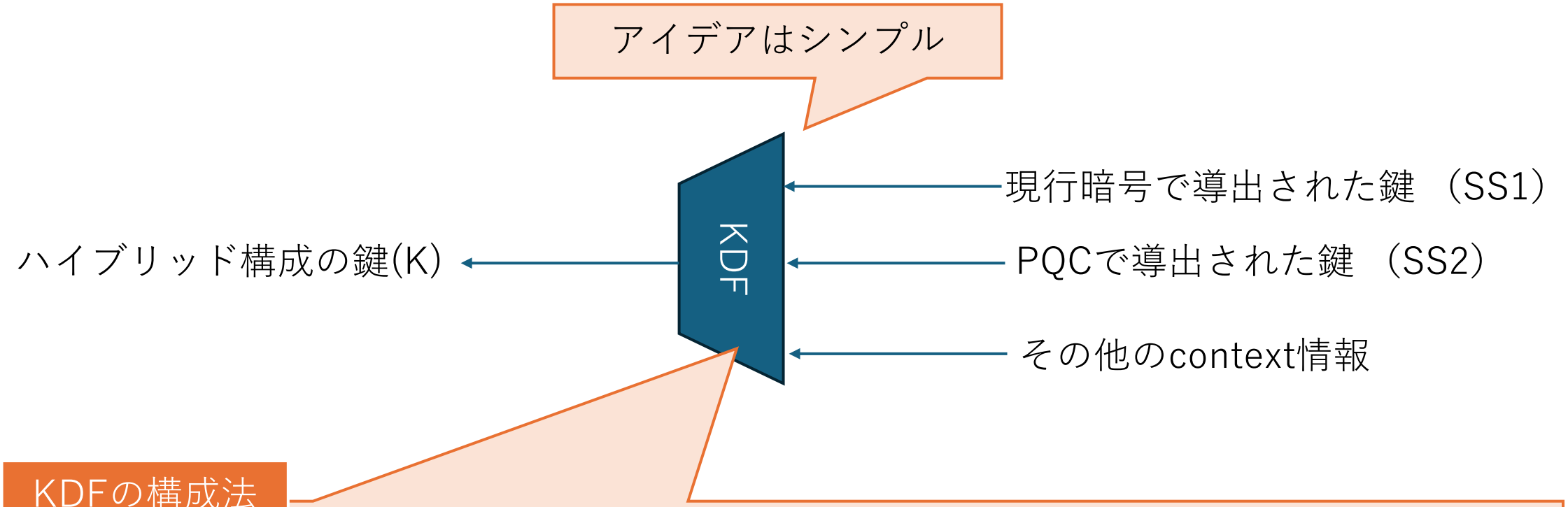
※「合成」と「混成」はcryptrec-ex-3503-2025における用語

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

「ハイブリッド」の位置付け

- **秘匿（KEM）用途**
  - マルチアルゴリズムKEMにおいて、複数の共有秘密から新たな共有秘密を導出する仕組をKey Combinerと呼んでいる。
    - NIST SP 800-227ではKDFの一利用形態としてKey Combinerを紹介。
      （既存KDFを、key combiner（コンバイナ）用途で利用することを承認）
    - ETSI TS 103 744 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 = KDF(SS1||SS2||context)**）
※ SP800-227, draft-ietf-lamps-pq-composite-kem, draft-ietf-tls-ecdhe-mlkem

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

X.509 CMSのアルゴリズム指定

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

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

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

SMI Security for PKIX Algorithms

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

TLS 1.3の方向性 (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（コードポイント）
Transport Layer Security (TLS) Parameters

			D	[RFC8422][RFC9847]
			D	[RFC8422][RFC9847]
			N	[RFC8422]
			N	[RFC8422]
			N	[RFC8422]
			N	[RFC8422]
13	sect571k1	Y	N	[RFC8422]
14	sect571r1	Y	N	[RFC8422]
15	secp160k1	Y	D	[RFC8422][RFC9847]
16	secp160r1	Y	D	[RFC8422][RFC9847]
17	secp160r2	Y	D	[RFC8422][RFC9847]
18	secp192k1	Y	D	[RFC8422][RFC9847]
19	secp192r1	Y	D	[RFC8422][RFC9847]
20	secp224k1	Y	D	[RFC8422][RFC9847]
21	secp224r1	Y	D	[RFC8422][RFC9847]
22	secp256k1	Y	N	[RFC8422]
23	secp256r1	Y	Y	[RFC8422]
24	secp384r1	Y	Y	[RFC8422]
25	secp521r1	Y	N	[RFC8422]
26	brainpoolP256r1	Y	N	[RFC7027]
27	brainpoolP384r1	Y	N	[RFC7027]
28	brainpoolP512r1	Y	N	[RFC7027]
29	x25519	Y	Y	[RFC-ietf-tls-rfc8446bis-13][R
30	x448	Y	Y	[RFC-ietf-tls-rfc8446bis-13][R
31	brainpoolP256r1tls13	Y	N	[RFC8734]
32	brainpoolP384r1tls13	Y	N	[RFC8734]
33	brainpoolP512r1tls13	Y	N	[RFC8734]
34	GC256A	Y	N	[RFC9189]
35	GC256B	Y	N	[RFC9189]
36	GC256C	Y	N	[RFC9189]
37	GC256D	Y	N	[RFC9189]
38	GC512A	Y	N	[RFC9189]
39	GC512B	Y	N	[RFC9189]
40	GC512C	Y	N	[RFC9189]
41	curveSM2	N	N	[RFC8998]
42-255	Unassigned			
256	ffdhe2048	Y	N	[RFC7919]
257	ffdhe3072	Y	N	[RFC7919]
258	ffdhe4096	Y	N	[RFC7919]
259	ffdhe6144	Y	N	[RFC7919]
260	ffdhe8192	Y	N	[RFC7919]
261-507	Unassigned			
508-511	Reserved for Private Use			[RFC7919]
512	MLKEM512	Y	N	[draft-connolly-tls-mlkem-key
513	MLKEM768	Y	N	[draft-connolly-tls-mlkem-key
514	MLKEM1024	Y	N	[draft-connolly-tls-mlkem-key
515-2569	Unassigned			
2570	Reserved	Y	N	[RFC8701]
2571-4586	Unassigned			
4587	SecP256r1MLKEM768	Y	N	[draft-ietf-tls-ecdhe-mlkem-0
4588	X25519MLKEM768	Y	N	[draft-ietf-tls-ecdhe-mlkem-0
4589	SecP384r1MLKEM1024	Y	N	[draft-ietf-tls-ecdhe-mlkem-0
4590	curveSM2MLKEM768	N	N	[draft-yang-tls-hybrid-sm2-ml
4591-0001	Unassigned			

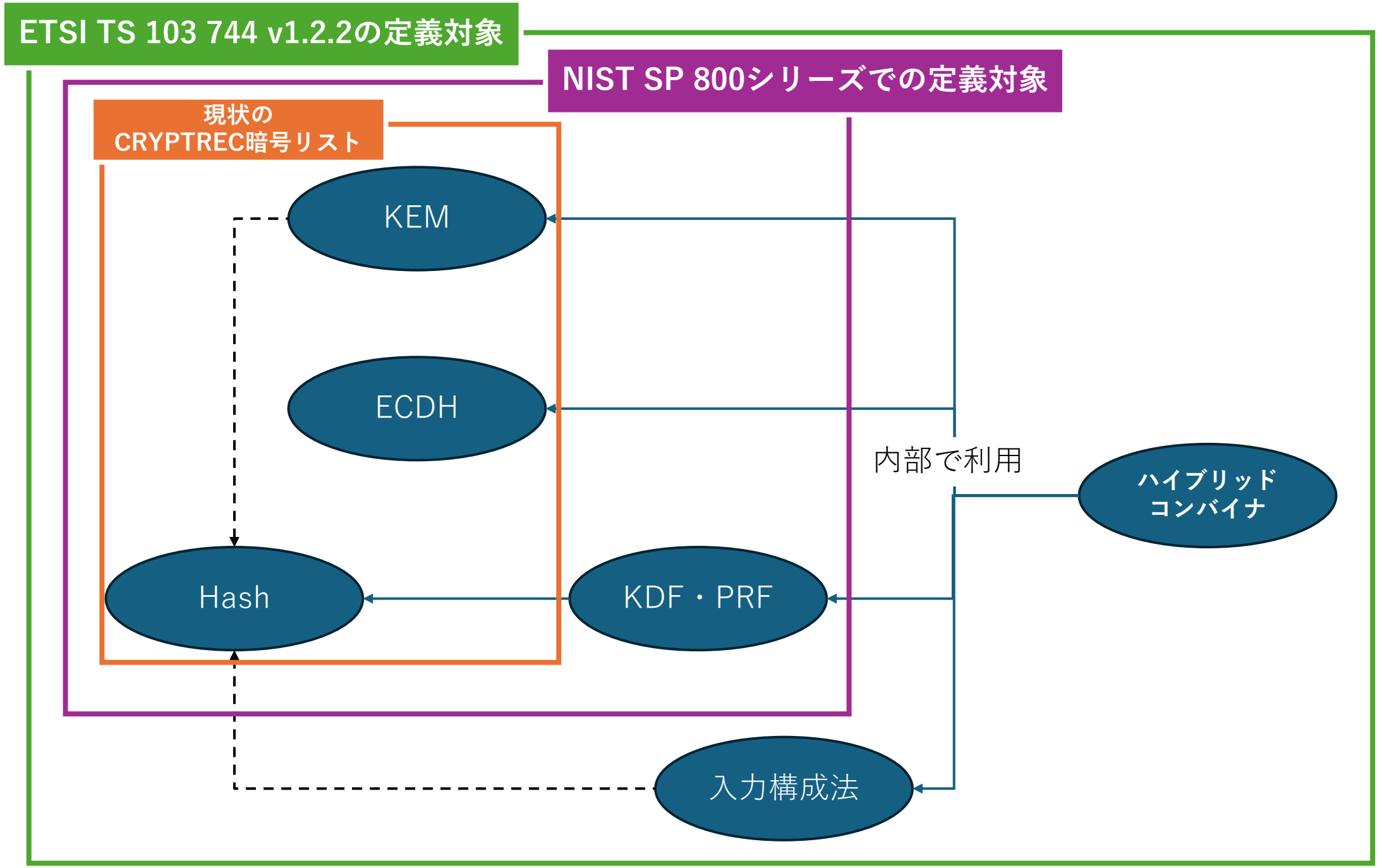
ETSI TS 103 744 v1.2.2

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。
- 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しての議論は未成熟。
  - 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で問題ないか。
  - 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するか。
  - Contextをどのように記載するか。
  - 入力の長さ管理を明示的に行うか。
  - 上位プロトコルでバインディング等を行っている場合の扱いをどうするか。

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。

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

１．開催の趣旨・目的

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

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

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

２．検討事項

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

３．構成等

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

４．議事の公開

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

５．庶務

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

（別紙）

構成員・オブザーバ名簿
（五十音順、敬称略）

（構成員）

岩田 哲	名古屋大学　未来材料・システム研究所　教授
漆嶌 賢二	ＧＭＯグローバルサイン株式会社　ＣＴＯ室　フェロー
垣内 由梨香	日本マイクロソフト株式会社 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　上席特別教授

（オブザーバ）

内閣官房国家サイバー統括室

参考資料２

CRYPTREC暗号リストのPQC対応と検討課題

CRYPTREC暗号リストの改定概要

- **CRYPTREC暗号リスト**の耐量子計算機暗号(**PQC**)**対応**のため、「電子政府推奨暗号リスト」に「**表２ 耐量子計算機暗号（PQC）リスト**」を新たに**追加**する改定を**2026年３月**に実施。
- CRYPTRECにおいて更なる検討が必要な課題については保留した上で継続検討。

CRYPTREC暗号リストのリスト構成

- CRYPTREC暗号リストの「電子政府推奨暗号リスト」において、**従来記載されている表**を「表１ **現行暗号リスト**」とし、**新たに**「表２ **耐量子計算機暗号（PQC）リスト**」を作成。
  - ✓ 政府関連文書では「電子政府推奨暗号リスト」という文言が既に浸透していることから、３リスト構成は維持。
  - ✓ PQCへの移行完了後も、３リスト構成自体は変更の必要がなく、長期的な観点からも理解しやすい。

<リスト構成のイメージ>

① 電子政府推奨暗号リスト
　表１ 現行暗号リスト
　表２ 耐量子計算機暗号(PQC)リスト
② 推奨候補暗号リスト
③ 運用監視暗号リスト

「耐量子計算機暗号（PQC）リスト」の対象範囲

- 公開鍵暗号技術だけでなく、従来の**共通鍵暗号技術等についても量子計算機耐性が確認されたもの**は「表２ 耐量子計算機暗号（PQC）リスト」に**掲載**。
  - ✓ PQCへの移行に際して、暗号技術がCRQC※への**耐性**を有するか否かの判別が一般にわかりにくく、CRYPTREC暗号リストの利用者に対して選択可能な暗号リストを明確に示す必要がある。
    ※Cryptographically Relevant Quantum Computer。現行暗号の解読に利用可能な水準の量子計算機。

<対象範囲のイメージ>

技術分類		暗号技術
公開鍵暗号	署名	ML-DSA
		SLH-DSA
	鍵共有	ML-KEM
共通鍵暗号		AES
ハッシュ関数		SHA-2
		SHA-3
（略）		（略）

パラメーターセット等の取扱い

- 暗号強度等を変えるために複数用意されている**パラメーターセット**についてもリストに**掲載**。
- 各パラメーターセットに対応する**セキュリティのカテゴリ**もリストに**掲載**。
  - ✓ パラメーターセット及びカテゴリともに、システム調達時に暗号技術を選択する上で**重要な選択肢**。
    ※例えばML-KEMでは、右記の記載イメージのように３種が定義（括弧内はそれぞれに対応するセキュリティのカテゴリ）。

<パラメータセットの記載イメージ>

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

2026年３月改定における取扱い

- 公開鍵暗号技術はML-KEMのみ掲載。※ML-DSA及びSLH-DSAは安全性・実装性能評価が終了次第掲載予定（2026年度想定）
- 暗号利用モード等や一部の共通鍵暗号とハッシュ関数についても継続検討中であり掲載していない。
- Category1・2の暗号技術については継続検討中であり掲載していない。

（参考）CRYPTREC暗号リスト(抄)（2026.3更新後）

電子政府推奨暗号リスト

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

なお、利用する鍵長について、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[3]の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。

<表１　現行暗号リスト>

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

<表２　耐量子計算機暗号（PQC）リスト>

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

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

1･2　（略）

3 CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準,
https://www.cryptrec.go.jp/list.html
なお、当該設定基準の見直しの検討を行う予定であり、当面の間、表２（耐量子計算機暗号（PQC）リスト）の公開鍵暗号は、当該設定基準を適用しない。

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

（注１）～（注７）　（略）

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

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

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

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

CRYPTREC暗号リストのPQC対応に関する検討課題

- 2025年度の暗号技術検討会において、CRYPTREC暗号リストの耐量子計算機暗号（PQC）対応に関する検討を行い、更なる検討が必要な課題について保留※した上でCRYPTREC暗号リストの改定を実施。
  ※現時点で、表２（耐量子計算機暗号（PQC）リスト）には、Category1・2の暗号技術や、暗号利用モードや認証暗号等の暗号技術は掲載していない。
- これらの課題については、安全性評価の観点のほか、利活用・普及促進の観点も含めた横断的な検討が必要。

→ 暗号技術評価委員会及び暗号技術活用委員会の協力も得ながら、暗号技術検討会の直下に、新たに**「耐量子計算機暗号（PQC）リスト検討タスクフォース」**を設け、2026年度末までを目途に検討を進める。

課題① Category 1・2（128ビットセキュリティ程度相当）の暗号等の取扱い

- ✓ 暗号強度要件※では、128ビットセキュリティは2040年までは「利用可」だが、2041年以降は「移行完遂期間」とされ、2051年以降は順次「利用不可」となる。
  ※暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準（CRYPTREC LS-0003-2022R1）
- ✓ 政府システムのPQC移行は原則2035年が期限とされており、この時期を念頭においた際、128ビットセキュリティの暗号技術を「推奨」することとしてよいか検討が必要。
- ✓ 海外機関では、Category 3以上を想定する記載が多く見られるが、Category 1・2を排除するような記載はなく、相互運用性・国際調達の観点からも検討が必要。
- ✓ このほか、カテゴリに関する記載等について改めて精査を行う。

＜参考：関係する暗号技術の例＞

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

課題② 暗号利用モードや認証暗号等の取扱い

- ✓ 現行暗号のCRQC（Cryptographically Relevant Quantum Computer）への耐性に関して、AES、SHA2、SHA3については、CRYPTRECの外部評価報告書※等から明らか。 ※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。