

耐量子計算機暗号（PQC）リスト検討タスクフォース （第3回）

令和8年9月16日（水） 16:00～18:00
A P 赤坂グリーンクロス C ルーム
（ハイブリッド開催）

<議事次第>

1. 開会
2. 議事
 - (1) NTRUについて
 - (2) 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
 - (3) 課題② 暗号利用モードや認証暗号等の取扱いについて
 - (4) 課題① Category 1・2の暗号等の取扱いについて
 - (5) 課題③ ハイブリッド構成の取扱いについて
 - (6) 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 | NTRUの最新状況 |
| 資料 3 | 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 4 | 課題② 暗号利用モードや認証暗号等の取扱い：諸外国動向調査 |
| 資料 5 | 課題① Category 1・2の暗号等の取扱い 等 |
| 資料 6 | 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 |
| 参考資料 3 | 電子政府における調達のために参照すべき暗号のリスト
（CRYPTREC暗号リスト）（令和8年3月30日更新） |

以上

NTRUの最新状況

2026年 9月 16日
NTT社会情報研究所

- **NTRUは、約30年にわたる研究・解析実績を持つ、成熟した耐量子KEMです。** NTRU-DPKEとNTTのSXY変換を組み合わせ、選択暗号文攻撃に対する強い安全性（IND-CCA2）を実現します。
- **性能面では、ML-KEMと競争力があります。** 鍵生成はML-KEMより重い一方、暗号化処理は高速であり、公開鍵・暗号文サイズを含めた総合的なバランスに優れています。
- **特に、128ビット安全で十分な用途に適しています。** ICカードやIoT機器など、処理性能やメモリに制約がある環境に向け、128ビット安全の軽量パラメータをISO/IEC 29192-4で標準化中です。
- **研究成果だけでなく、実際に利用できるOSSと実装環境を整備しています。** liboqsやBouncy Castleで利用できるほか、参照実装、テストベクトルを公開し、TMVP等を用いた高速化も継続しています。
- **国際標準化と既存仕様への採用を、多方面から進めています。** ISO/IECでのNTRU自体の標準化に加え、CFRG・IPSECMEでの仕様化、GlobalPlatformのTEE仕様でサポートされています。
- **NTRUは、既に実システムへの適用段階に進んでいます。** Interop Tokyo 2026／ShowNetでは、NTRUを搭載した耐量子VPNを実ネットワーク上で動態展示し、通信と性能の検証を実施しました。2027年に商用利用開始予定です。

- NTRU公開鍵暗号と**SXY変換（NTT技術）**を組み合わせた耐量子鍵カプセル化技術（耐量子KEM）
- 量子攻撃を考慮したモデル（QROM）で強い安全性（IND-CCA2）を実現

耐量子KEM : NTRU



基礎公開鍵暗号部 NTRU-DPKE*

耐量子安全性

NTRU格子問題に基づく耐量子安全性ではあるが、弱い安全性（OW-CPA）



安全性強化部 **SXY変換****

CCA2安全性

量子計算機を持つ攻撃者にとって有利な条件（QROM）で選択暗号文攻撃に対する安全性(IND-CCA2安全性)を緊密に証明

* NTRU Algorithm Specifications and Supporting Documentation, NIST PQC submission

** T. Saito, K. Xagawa, T. Yamakawa, "Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model," EUROCRYPT 2018.

NTRUは1996年の提案以来、**約30年にわたる研究・解析実績の中で攻撃は見つかっておらず、特許も期限切れ**となっているため訴訟リスクも極めて低い。

カテゴリ	
安全性	IND-CCA2 (選択暗号文攻撃に対する強い安全性)
パラメタ	Category 1, 3, 5 (128, 192, 256ビットセキュリティ) ※これ以外にも柔軟に作成可能
成熟度	NTRUアルゴリズム: 2019 (初版は1996年) , SXY変換: 2018 (ML-KEMは2023年、FrodoKEMは2016年に初版公開)
処理速度	ML-KEMと比較して鍵生成は低速、暗号化は高速、復号は同程度
特許	パテントフリー (期限切れ)
論文	NTRU : ANTS 1998 / SXY変換 : EUROCRYPT 2018
仕様書	ISO/IEC 29192-4: 現在進行中 IETF: NTRU Key Encapsulation (ietf.org/archive/id/draft-fluhrer-cfrg-ntru-03.txt) NISTコンペ提出仕様: Algorithm Specifications And Supporting Documentation (ntru.pdf)

処理速度比較(192-bit, Category 3)

- NTRUはML-KEMと最も競争力のある方式。
- TLS/HTTPSサーバやVPNゲートウェイでは、クライアント側が鍵生成と復号を行う一方で、サーバ側が暗号化を多数行うため、暗号化の負荷が低いことが望ましい

SUPERCOP 2025-04-15 / Intel Core i3-1215U Golden Cove

KEMs	Parameter (192-bit)	Speed (CPU cycles)			Size (bytes)	
		鍵生成	暗号化	復号	公開鍵サイズ	暗号文サイズ
NTRU	hps4096821	275,518	26,304	52,831	1,230	1,230
ML-KEM	768	30,676	39,284	31,981	1,184	1,088
HQC	192 (Round 4)	164,738	399,923	650,421	4,522	9,042
Classic McEliece	460896f	77,375,495	60,233	247,309	524,160	156
FrodoKEM	976-AES	1,821,584	2,306,027	2,265,530	15,632	15,792

<https://bench.cr.yp.to/results-kem/amd64-alder2%2C1f626960%2C5600000.html>

本ページは構成員限り

処理速度比較(128-bit, Category 1)

- Category 1 (128-bit)においても、NTRUはKyber(ML-KEM)と最も競争力のある方式。

SUPERCOP 2025-04-15 / Intel Core i3-1215U Golden Cove

KEMs	Parameter (128-bit)	Speed (CPU cycles)			Size (bytes)	
		鍵生成	暗号化	復号	公開鍵サイズ	暗号文サイズ
NTRU	hps2048667	202,578	22,458	38,492	930	930
	hrss701	196,581	17,287	39,684	1,138	1,138
Kyber	512	17,916	25,962	20,972	800	768
HQC	128	69,460	175,773	308,836	2,249	4,497
Classic McEliece	348864	58,695,440	28,039	99,785	261,120	96
FrodoKEM	640AES	918,610	1,247,004	1,187,728	9,616	9,720

<https://bench.cr.yp.to/results-kem/amd64-alder2%2C1f626960%2C5600000.html>

NTRUの実装・OSS化状況

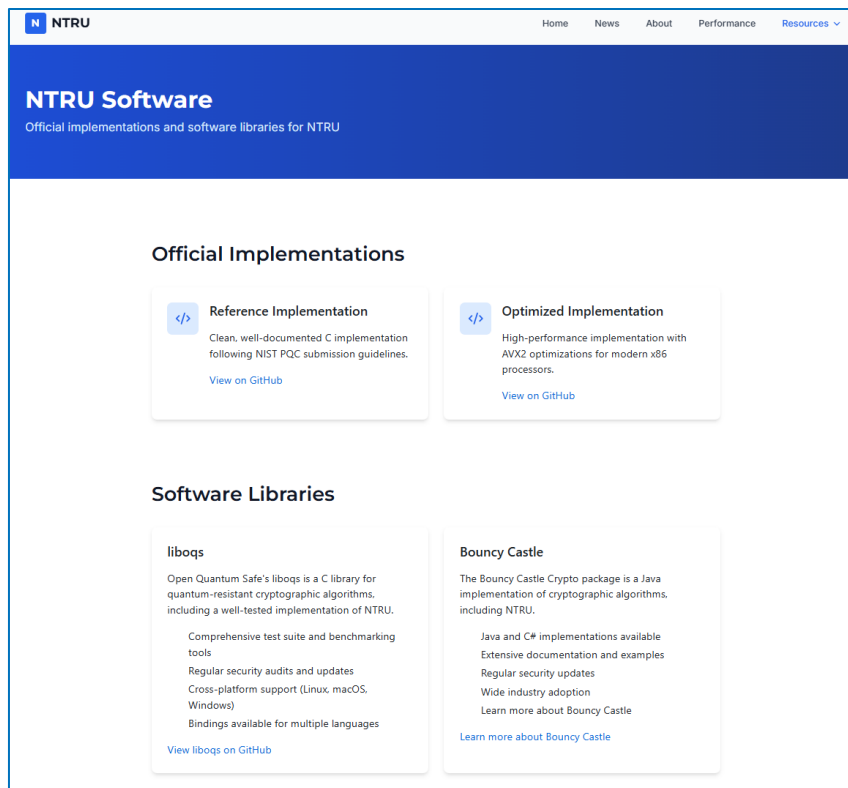
NTRUの利用促進に向け、OSSを提供。liboqsについてはNTTにて保守体制も構築済みのため、安心して利用可能。

また、複数の言語にも対応することで、様々なシステムやアプリに対応可能

項目	状況	内容	参照先
OSSライブラリ	OSS化済	Open Quantum SafeのPQCライブラリ liboqs 0.15.0にNTRUを再追加。	https://github.com/open-quantum-safe/liboqs/releases?utm_source=chatgpt.com
		Java暗号ライブラリBouncy CastleでもNTRUをサポート	https://downloads.bouncycastle.org/java/docs/bcprov-jdk18on-javadoc/org/bouncycastle/pqc/crypto/ntru/package-summary.html?utm_source=chatgpt.com
リファレンス実装	公開	NTRUの参照実装、実装ガイド、テストベクタをHPにて公開	https://info.isl.ntt.co.jp/crypt/ntru/?utm_source=chatgpt.com
組み込み向け実装	公開	ARM Cortex-M4を向けコードがPQM4から公開	https://github.com/mupq/pqm4/tree/Round3/crypto_kem?utm_source=chatgpt.com
高速実装	継続実施	TMVP等を用いたNTRUの高速実装を実施しており、liboqsに提供予定	https://info.isl.ntt.co.jp/crypt/ntru/?utm_source=chatgpt.com#/news

対応言語

C	Go	Java	Python	C++	Rust	C#	Swift	JavaScript
済 (liboqs)	済 (liboqsのラッパーを利用することで利用可)				未			



The screenshot shows the 'NTRU Software' homepage. It features a dark blue header with the NTRU logo and navigation links (Home, News, About, Performance, Resources). Below the header, the main content area is white. The first section is 'Official Implementations', which contains two cards: 'Reference Implementation' (Clean, well-documented C implementation following NIST PQC submission guidelines, with a 'View on GitHub' link) and 'Optimized Implementation' (High-performance implementation with AVX2 optimizations for modern x86 processors, with a 'View on GitHub' link). The second section is 'Software Libraries', which contains two cards: 'liboqs' (Open Quantum Safe's liboqs is a C library for quantum-resistant cryptographic algorithms, including a well-tested implementation of NTRU, with a 'View liboqs on GitHub' link) and 'Bouncy Castle' (The Bouncy Castle Crypto package is a Java implementation of cryptographic algorithms, including NTRU, with a 'Learn more about Bouncy Castle' link).

NTRU Software

Official implementations and software libraries for NTRU

Official Implementations

Reference Implementation

Clean, well-documented C implementation following NIST PQC submission guidelines.

[View on GitHub](#)

Optimized Implementation

High-performance implementation with AVX2 optimizations for modern x86 processors.

[View on GitHub](#)

Software Libraries

liboqs

Open Quantum Safe's liboqs is a C library for quantum-resistant cryptographic algorithms, including a well-tested implementation of NTRU.

- Comprehensive test suite and benchmarking tools
- Regular security audits and updates
- Cross-platform support (Linux, macOS, Windows)
- Bindings available for multiple languages

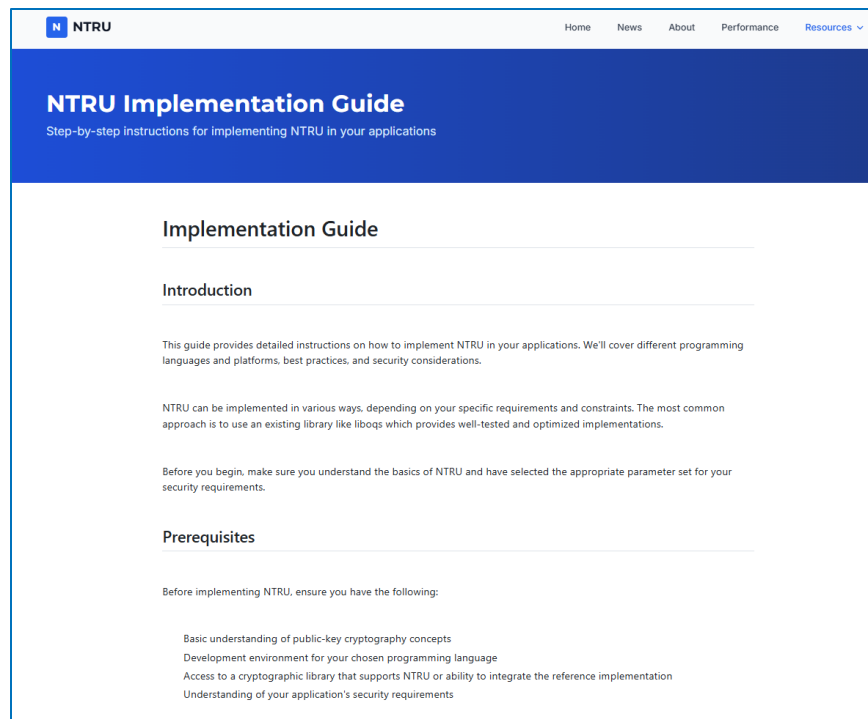
[View liboqs on GitHub](#)

Bouncy Castle

The Bouncy Castle Crypto package is a Java implementation of cryptographic algorithms, including NTRU.

- Java and C# implementations available
- Extensive documentation and examples
- Regular security updates
- Wide industry adoption
- Learn more about Bouncy Castle

[Learn more about Bouncy Castle](#)



The screenshot shows the 'NTRU Implementation Guide' page. It features a dark blue header with the NTRU logo and navigation links (Home, News, About, Performance, Resources). Below the header, the main content area is white. The first section is 'Implementation Guide', which contains an 'Introduction' section. The 'Introduction' section states that the guide provides detailed instructions on how to implement NTRU in your applications, covering different programming languages and platforms, best practices, and security considerations. It also mentions that NTRU can be implemented in various ways, depending on your specific requirements and constraints, and that the most common approach is to use an existing library like liboqs which provides well-tested and optimized implementations. Before you begin, it advises understanding the basics of NTRU and having selected the appropriate parameter set for your security requirements. The second section is 'Prerequisites', which lists the following: Basic understanding of public-key cryptography concepts, Development environment for your chosen programming language, Access to a cryptographic library that supports NTRU or ability to integrate the reference implementation, and Understanding of your application's security requirements.

NTRU Implementation Guide

Step-by-step instructions for implementing NTRU in your applications

Implementation Guide

Introduction

This guide provides detailed instructions on how to implement NTRU in your applications. We'll cover different programming languages and platforms, best practices, and security considerations.

NTRU can be implemented in various ways, depending on your specific requirements and constraints. The most common approach is to use an existing library like liboqs which provides well-tested and optimized implementations.

Before you begin, make sure you understand the basics of NTRU and have selected the appropriate parameter set for your security requirements.

Prerequisites

Before implementing NTRU, ensure you have the following:

- Basic understanding of public-key cryptography concepts
- Development environment for your chosen programming language
- Access to a cryptographic library that supports NTRU or ability to integrate the reference implementation
- Understanding of your application's security requirements

<https://info.isl.ntt.co.jp/crypt/ntru/#/>

NTRUの標準化状況（2026/09/03時点）

利用促進に向けデ・ジュール（ISO/IEC, ITU-T）とデファクト（IETF, GlobalPlatform）の両面から標準化を実施中

団体			状況
ISO/IEC	29192-4	情報技術分野（29192は軽量暗号）の国際標準を策定	現在、DAmd(Draft of Amendment)ステージ。1年以内に出版の見込み。
IETF	CFRG	インターネットで利用する暗号技術を研究・仕様化	NTRU KEMの仕様書および安全性に関する文書の2件のInternet-Draftが進行中
	IPSECME	IPsec・IKEプロトコルを標準化	NTRUをIKEv2の鍵交換に利用する方式を定義するInternet-Draftが進行中
GlobalPlatform	TEE Committee	TEEやSecure Element等のセキュアデバイス技術の業界仕様を策定	TEE Internal Core API Specification v1.4において、TEE内のTrusted Applicationが利用可能な暗号アルゴリズムとしてNTRUをサポート
	STF	GlobalPlatform仕様のセキュリティ要件・暗号技術を検討	セキュリティタスクフォースにて、128ビットパラメータを含めて提案中
ITU-T	X.1197	通信ネットワーク・サービスに関する国際標準を策定	IPTVの暗号化・鍵交換用途の推奨アルゴリズムとしてNTRUを掲載

ISO/IECでの標準化パラメータについて

- NTRUのみ128-bitの軽量なパラメータが国際標準として規格化予定
- ICカードやIoT機器などでは128-bit軽量暗号のニーズがあるため提案

規格		アルゴリズム	セキュリティレベル		
			128	192	256
ISO/IEC	29192-4 (軽量暗号)	NTRU	✓	✓	✓
	18033-2 (公開鍵暗号)	ML-KEM		✓	✓
		FrodoKEM		✓	✓
		Classic McEliece		✓	✓

本ページは構成員限り

(Category 1 (128-bit) NTRU VS Category 3 (192-bit) ML-KEM)

Category 1 (128ビット安全)で十分な用途では、NTRUは処理性能と鍵・暗号文サイズのバランスに優れ、ユースケースによっては有力な選択肢となり得る。

SUPERCOP 2025-04-15 / Intel Core i3-1215U Golden Cove

KEMs	Parameter (128-bit)	Speed (CPU cycles)		Size (bytes)	
		暗号化	復号	公開鍵サイズ	暗号文サイズ
NTRU	hps2048667	22,458	38,492	930	930
	hrss701	17,287	39,684	1,138	1,138
ML-KEM	768	39,284	31,981	1,184	1,088

1. NTRU Key Encapsulation (ietf.org/archive/id/draft-fluhrer-cfrg-ntru-03.txt)
 - CFRG Internet-Draft
 - Cisco Systems, mesur.io, Brave, Entrust, TII, and NTT
 - アルゴリズムそのものの技術仕様
2. NTRU KEM Security Considerations (ietf.org/archive/id/draft-kosuge-cfrg-ntru-kem-security-considerations-00.txt)
 - CFRG Internet-Draft
 - TII, and NTT
 - NTRUのアルゴリズム仕様そのものではなく、**NTRUをIETFプロトコルで安全に使用するためのセキュリティ指針**
3. Post-quantum Hybrid Key Exchange with NTRU in the Internet Key Exchange Protocol Version 2 (IKEv2) (ietf.org/archive/id/draft-skyline-ipsecme-ntru-ikev2-00.txt)
 - IPSECME Internet-Draft
 - NTT docomo Business, NTT Data Intellilink, NTT, and Cisco Systems
 - **NTRUをIpssec-VPNの鍵交換アルゴリズムとして利用するための技術仕様**

GrobalPlatform と ITU-T X.1197

GlobalPlatform・ITU-Tでは、既存仕様へのNTRU採用実績あり
(NTRU自体の規格化ではなく、既存仕様・勧告の中でNTRUを採用)



TEE Internal Core API Specification v1.4 | GPD_SPE_010
Published Nov 2025



A minor version release with the following additions and bug fixes applied.

- Added calling client (CA or TA) path identity chain, enabling a TEE to describe all entities in the calling path to a TA.
- Added calling TEE path identity chain, enabling a TEE to describe all entities below the TA.
- Added ability to open TA-TA session in remote EE.
- To increase the readability of the code, moved the annotations from the function definitions to the textual description of the parameters.
- Added TEE_MAX_RETAINED_DATE, defining the maximum amount of data that a cipher operation retains in bytes.
- Deprecated the use of Operation State; the state of the operation is now defined using the TEE_HANDLE flags.
- Added PQC optional algorithm support.
 - TEE_TYPE_MLKEM
 - TEE_TYPE_MLDSA
 - TEE_TYPE_FALCON
 - TEE_TYPE_SLHDSA
 - TEE_TYPE_LMOTS
 - TEE_TYPE_LMS
 - TEE_TYPE_XMSS
 - TEE_TYPE_WOTS
 - TEE_TYPE_FRODOKEM
 - TEE_TYPE_NTRU
- Added optional CHACHA and POLY1305 algorithm support (partly added to better enable TLS 1.3).
- Expanded RSA asymmetric key sizes up to 8192.
- Added new section 4.7.0, Implementation Stack Properties.
- Added Panic masking mode for certain hard to programmatically avoid panic types.
- Added _PS functions to enable return of error code instead of Panic (generally for previous void return functions).
- Added functions TEE_EncapsulateKey and TEE_DecapsulateKey.
- Divided Table 6-4 into one table for algorithms that SHALL be supported and one table for those that are optional.
- Deprecated the TEE Arithmetical API described in section 8.

FREE MEMBER DOWNLOAD

FREE NON-MEMBER DOWNLOAD

Table I.1 – Examples of possible cryptographic algorithms for IPTV SCP

Classification		Status	Algorithms
	Encryption and key exchange	RECOMMENDED (Note 1)	<u>NTRU [b-IEEE 1363.1-2008]</u>
	Key exchange	DEPRECATED (Note 2) [b-NIST IR 8105] Note to implementers: Check valid DH-Groups in [b-IETF RFC 8247] 2.4. Type 4 – IKEv2 Diffie-Hellman Group Transforms!	DH [b-IETF RFC 2136] ECDH [b-IETF RFC 6090]
NOTE 1 – With the caveat that currently only pre-shared keys can prevent Man-in-the-Middle attacks [b-MitM-NTRU-KE]. NOTE 2 – [b-ACM] and [b-NIST IR 8105] - use physical key distribution when possible. NOTE 3 – See clause 5 for the conventions used in the status column.			

Table I.2 describes safety of the key and its lengths supported in IPTV SCP.

https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1197-201909-!!Amd1!PDF-E&type=items

各団体における規格提案状況

NTRUは複数の規格団体にて、一定の評価を得られており、今後規格化やサポートされる可能性が高く、利用が見込まれると考える。

Algorithm	CRYPT REC	ISO/IEC	IETF	GlobalPlatform	ITU-T	NIST (FIPS)
NTRU		✓	✓	✓ (一部)	✓	
ML-KEM	✓	✓	✓	✓	✓	✓
HQC					✓	✓
Classic McEliece		✓	✓		✓	
FrodoKEM		✓	✓	✓ (一部)		

- 既に商用利用されているソフトウェアルータ KamueeにNTRUを実装し、Interop Tokyo / ShowNet 2026にて耐量子VPNの動態展示を実施（世界初のNTRUの動態展示+性能試験デモ）
 - Interop Tokyoは、ネットワーク機器と技術の展示会で毎年6月に幕張メッセで開催。来場者は12万人と世界最大規模。
 - ShowNetは、Interop Tokyoの中の動態展示ネットワークで、数年後に業界に浸透する技術を先駆けて実践する場。
- Kamuee (PQC-VPN)の商用利用開始は2027年を計画。



PQC-VPN: 耐量子暗号VPN

高性能な量子コンピュータの登場で、従来の暗号が突破されるリスクが現実。安全な通信を維持するには量子コンピュータでも破ることのできない暗号への早急な移行が不可欠です。

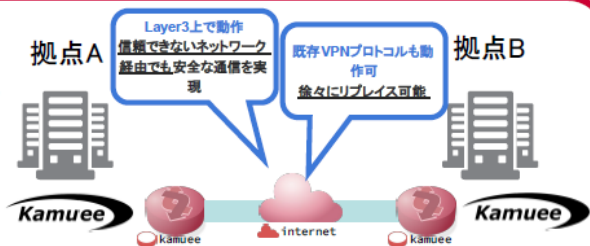
Kamueeは次世代のITインフラを支える量子コンピュータでも破ることのできない暗号通信技術“PQC-VPN”を実現しました。

既存の暗号技術は危険化
量子コンピュータで効率的に既存暗号を
突破可能なアルゴリズムがある



ユースケース例: 拠点間VPN

PQC-VPNは、金融機関・医療機関、個人情報を扱うデータセンターなどの高いセキュリティが求められる拠点間での安全な通信を実現し、次世代のサイバー攻撃から企業や政府の安全を強力に支えます。



Innovating a Sustainable Future for People and Planet



課題④

公開鍵暗号方式のPQCの 安全性評価等の進め方

公開鍵暗号方式のPQCの安全性評価等の進め方

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

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

【考え方（第1回会合までの議論）】

- ✓ 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※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へ追加することとなる。

※CRQCへの耐性を見据えた評価を行う。

- ✓ FIPS 203～205以外の暗号技術についても、**国内で利用が見込まれる暗号技術についても、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**。

【考え方】

- ✓ 安全性評価等の対象については次の観点を総合的に勘案することとしてはどうか。

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

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

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

- ✓ 上記観点到照させば、今後策定予定の**FIPS標準**（FN-DSA、HQC、追加公募中の署名方式等）についても、世界的な利用が見込まれることから、原則として**安全性評価等の対象とすることが考えられる**のではないかと。

- ✓ また、**NTRU**のように、FIPS標準ではないが、国内利用や標準化の進展が認められる方式についても、同様の観点から**評価対象とし得る**のではないかと。

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

(参考) 各PQCにおける3つの観点の整理

➤ 前頁の3つの観点を踏まえ、各方式について安全性評価等の必要性を整理。

暗号技術	(A)安全性の成熟度	(B)標準化の成熟度	(C)実利用の具体性	取扱い案
FN-DSA (FIPS 206)	◎ 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	◎ 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	○ 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
NTRU	◎ 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	◎ NIST Round 3まで長期間の評価実績	○ ISO/IECで標準化	△ 国内での具体的な製品・サービス利用は現時点では確認できず	現時点では継続把握
Classic McEliece	◎ NIST Round 4まで長期間の評価実績	○ ISO/IECで標準化	△ 国内での具体的な製品・サービス利用は現時点では確認できず	現時点では継続把握
NTRU+	○ 韓国KpqC公募で公開評価を経て最終選定	○ 韓国産業標準 (KS) 制定提案済	△ 国内での具体的な製品・サービス利用は現時点では確認できず	現時点では継続把握

(参考) CRYPTREC暗号リスト・移行ルール

- CRYPTREC暗号リストにおける**移行ルール**は次のとおり。(赤字がPQCで追加した部分)
 なお、PQC移行の進捗状況やPQC対応製品の普及状況を踏まえ必要に応じ、適宜見直しを行うこととなっている。

＜表2への追加に関するルール＞

標準化等により将来的な利用が見込まれ、
安全性や実装性能が十分にありと
 暗号技術検討会が決定した場合
 (公募や事務局提案等)



① 電子政府推奨暗号リスト

安全性及び実装性能が確認された暗号技術で、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、利用を推奨するもののリスト

＜表2新設に関する臨時ルール＞

表1の暗号技術のうち、CRQCへの
 耐性があると暗号技術検討会が決定したものを表2に追加する

次の条件のいずれかを満たすと暗号技術検討会が決定した場合

- ✓ 5年ごとの**利用実績調査**により、複数の利用実績を確認した場合
- ✓ その他、普及していることが明らか又は急速な普及が大いに見込まれる場合



安全性維持が困難(危殆化した)と
 暗号技術検討会が決定した場合

※ 電子政府推奨暗号リストに掲載された暗号技術は、利用者がいる前提であり、原則として、危殆化以外の理由では遷移させず、また、移行のための時間を確保するため、いきなりリストから削除することはない。



標準化等により将来的な利用が見込まれ、
安全性や実装性能が十分にありと
 暗号技術検討会が決定した場合
 (公募や事務局提案等)



② 推奨候補暗号リスト

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のリスト

③ 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確認されたが、互換性維持
 のために継続利用を容認する暗号技術のリスト

- CRYPTREC暗号リストへの掲載から20年を超えた後に実施する最初の**利用実績調査**までに、十分な利用実績を確認できなかったもの
- 公募提案暗号について、提案会社より自主取下げ要望があり、暗号技術検討会における審議の結果「今後の普及が見込まれない公募提案暗号」とであると判断されたもの



安全性維持が
 困難(危殆化した)
 と判断した場合

次の条件のいずれかを満たすと暗号技術検討会が決定した場合、削除猶予期間を定めて周知を行った上で、その期間の満了後に自動的に削除する。

- ✓ 運用監視暗号リストに掲載している注釈で示した互換性維持のための利用形態が必要なくなり、削除が妥当と判断した場合
- ✓ 互換性維持の継続利用として使うにしても安全性維持が極めて困難で、互換性維持の継続利用が容認できないと判断した場合
- ✓ その他、運用監視暗号リストに掲載している必要性の根拠を満たさなくなったと判断した場合



リストから削除

※ **利用実績調査**の具体的な実施内容・評価基準は、暗号技術活用委員会において検討し、暗号技術検討会の承認を経た上で実施する。

※ ①・②への追加・遷移における**安全性**については、CRQCへの耐性を見据えて評価を行う。

課題② 諸外国動向調査

記載例

記号	記載基準
量子	“耐量子計算機暗号として使用することを推奨”と記載有
非推奨	“耐量子計算機暗号として使用を推奨しない”と記載有
古典	“現行暗号としての使用可能”の記載有 耐量子計算機暗号としての使用については記載なし
記載無し	一切の記載なし

暗号利用モード

国・機関	CBC	CFB	OFB	CTR	XTS	参考文献・引用ページ
米国(※1)	古典	古典	古典	古典	記載なし	
英国	古典(推奨はしない)	古典(保管等のみ)	古典(保管等のみ)	古典	古典(推奨)	[UK] p.2
カナダ	古典(推奨)	古典(推奨)	古典(推奨)	古典(推奨)	古典(推奨)	[CA] pp.11-12
オーストラリア	古典(AES-CBC、IPsec/IKEv2)	記載なし	記載なし	古典(AES-CTR、IPsec/IKEv2)	記載なし	[AU] Web
ニュージーランド	古典(“other modes”として例示)	古典(同左)	古典(同左)	古典(同左)	記載なし	[NZ] §17.2.28, p.309
フランス	記載なし	記載なし	記載なし	記載なし	記載なし	[FR] §1.3, p.2
ドイツ	古典(推奨)	記載なし	記載なし	古典(推奨)	記載なし	[DE] p.42
オランダ	記載なし	記載なし	記載なし	量子(推奨:AES-CTR)	記載なし	[NL] pp.57, 92-93
スペイン	記載なし	記載なし	記載なし	記載なし	記載なし	[ES] §4.5, p.20
チェコ(※2)	量子(Approved)	量子(Approved)	量子(Approved)	量子(Approved)	量子(disk encryption)	[CZ] pp.5-6
スロバキア	記載なし	記載なし	記載なし	記載なし	記載なし	[SK] p.4
フィンランド	記載なし	記載なし	記載なし	記載なし	記載なし	[FI] p.3
ノルウェー	記載なし	記載なし	記載なし	記載なし	古典(Default: 256 bit/Alternate: 128 bit)	[NO] p.15
サウジアラビア	古典(Basicのみ)	古典(NCS-2掲載)	古典(NCS-2掲載)	古典(NCS-2掲載)	古典(NCS-2掲載)	[SA] NCS-2:2025, p.15
マレーシア	記載なし	記載なし	記載なし	記載なし	古典(Approved: XTS-AES 128/256)	[MY] Web

※1 米国:暗号利用モード、MAC、認証暗号はHMACのみFIPSで規格、他はSPでRecommendationとして規定されているが、いずれも耐量子計算機暗号としての記載なし。

※2 チェコ:量子耐性を持つブロック暗号またはハッシュ関数と組み合わせることが条件。またCBC・CFB・OFB・CTRの単独使用はApprovedではなく、Encrypt-then-MAC内での使用に限定。

メッセージ認証コード(MAC)など

国・機関	HMAC	CMAC	GMAC	KMAC	Poly1305	参考文献・引用ページ
米国(※1)	古典	古典(推奨)	古典(推奨)	古典(推奨)	記載なし	
英国	古典	古典	古典	古典	記載なし	[UK] p.2
カナダ	古典(推奨)	古典(推奨:AES)	古典(推奨:AES)	古典(推奨: KMAC128/256)	記載なし	[CA] p.20
オーストラリア	古典(HMAC- SHA256/384/512、 IPsec)	記載なし	記載なし	記載なし	記載なし	[AU] Web
ニュージーランド	古典(SHOULD use HMAC- SHA256/384/512)	記載なし	記載なし	記載なし	記載なし	[NZ] §17.8.14, p.318
フランス	記載なし	記載なし	記載なし	記載なし	記載なし	[FR] §1.3, p.2
ドイツ(※3)	量子(256-bit鍵)	量子(256-bit鍵)	量子(256-bit鍵)	量子(256-bit鍵)	記載なし	[DE] pp.49-50
オランダ	量子(量子安全なハッ シュが条件)	量子(量子安全な下位 方式が条件)	記載なし	量子(Quantum-safe: Yes)	記載なし	[NL] pp.57, 94-95
スペイン	記載なし	記載なし	記載なし	記載なし	記載なし	[ES] §4.5, p.20
チェコ(※4)	量子	量子	量子	量子	記載なし	[CZ] p.6
スロバキア	記載なし	記載なし	記載なし	記載なし	記載なし	[SK] p.4
フィンランド	古典(SHA- 256/384/512)	記載なし	記載なし	古典(KMAC各パラメー タ)	記載なし	[FI] p.3
ノルウェー	古典(Default)	記載なし	記載なし	古典(Alternate)	記載なし	[NO] p.16
サウジアラビア	古典(NCS-2掲載)	古典(NCS-2掲載)	古典(NCS-2掲載)	古典(NCS-2掲載)	記載なし	[SA] NCS-2:2025, p.16
マレーシア	古典(Approved)	古典(Approved)	古典(Approved)	古典(Approved)	古典(Approved)	[MY] Web

※3 ドイツ:MACは、将来の量子計算機を考慮し、高保護・長期保護用途では推奨MACに256-bit鍵を用いるよう明記。

※4 チェコ:量子耐性を持つブロック暗号またはハッシュ関数との組合せが条件。

認証付き秘匿モード、認証暗号など

国・機関	CCM	EAX	OCB1 / OCB3	GCM	GCM-SIV	ChaCha20-Poly1305	Encrypt-then-MAC	参考文献 引用ページ
米国(※5)	古典	記載なし	記載なし	古典	記載なし	記載なし	記載なし	
英国	古典(推奨)	記載なし	記載なし	古典(推奨)	記載なし	記載なし	記載なし	[UK] p.2
カナダ	古典(推奨)	記載なし	記載なし	古典(推奨)	記載なし	記載なし	記載なし	[CA] p.12
オーストラリア	古典(AES-CCM、 IKEv2)	記載なし	記載なし	古典(AES-GCM、 IPsec/IKEv2)	記載なし	記載なし	記載なし	[AU] Web
ニュージーランド	記載なし	記載なし	記載なし	記載なし	記載なし	記載なし	記載なし	[NZ] §17.2, pp.3–4
フランス	記載なし	記載なし	記載なし	記載なし	記載なし	記載なし	記載なし	[FR] §1.3, p.2
ドイツ	古典(推奨)	記載なし	記載なし	古典(推奨)	古典(推奨:AES- GCM-SIV)	記載なし	記載なし	[DE] p.42
オランダ	記載なし	記載なし	量子(推奨:AES- OCB)	量子(推奨:AES- GCM)	量子(推奨:AES- GCM-SIV)	量子(推奨)	記載なし	[NL] pp.57, 92–95
スペイン	記載なし	記載なし	記載なし	記載なし	記載なし	記載なし	記載なし	[ES] §4.5, p.20
チェコ	量子(※6)	量子(※6)	量子(※6)	量子(※6)	記載なし	量子(※6)	量子(※6)	[CZ] pp.5–6
スロバキア	記載なし	記載なし	記載なし	記載なし	記載なし	記載なし	記載なし	[SK] p.4
フィンランド	記載なし	記載なし	記載なし	記載なし	記載なし	記載なし	記載なし	[FI] p.3
ノルウェー	記載なし	記載なし	記載なし	古典(Default: AES-GCM-256/ Alternate: AES- GCM-128)	古典(Alternate)	古典(Alternate)	記載なし	[NO] p.13
サウジアラビア	古典(NCS-2掲載)	記載なし	記載なし	古典(NCS-2掲載)	記載なし	記載なし	記載なし	[SA] NCS-2:2025, pp.15–16
マレーシア	古典(Approved: AES-CCM 128/192/256)	記載なし	記載なし	古典(Approved: AES-GCM 128/192/256)	古典(Approved: AES-GCM-SIV 128/256)	古典(Approved)	記載なし	[MY] Web

※5 米国:GCMは、2026年3月版NSA Capability PackageのCNSA 2.0構成で指定されたAES-256-GCMに限定。

※6 チェコ:量子耐性ブロック暗号・ハッシュ関数の使用、IV、タグ長、鍵使用量等の条件を満たす場合のみ。

Camellia、KCipher-2、SHAKE128、SHAKE256

国・機関	Camellia	KCipher-2	SHAKE128	SHAKE256	参考文献・引用ページ
米国	記載なし	記載なし	非推奨(※7)	非推奨(※7)	[US-1] PDF p.8, 「Can I use SHA-3 as a hash?」
英国	記載なし	記載なし	記載なし	記載なし	[UK] p.2
カナダ(※8)	記載なし	記載なし	量子※(ML-KEM・ML-DSA等の内部で指定)	量子※(ML-KEM・ML-DSA・SLH-DSA等の内部で指定)	[CA] pp.16, 19
オーストラリア	記載なし	記載なし	記載なし	記載なし	[AU] Web
ニュージーランド	記載なし	記載なし	記載なし	記載なし	[NZ] §17.2.10-11
フランス	記載なし	記載なし	記載なし	記載なし	[FR] §1.3, p.2
ドイツ	記載なし	記載なし	記載なし	記載なし	[DE] §§3-4, pp.40-48
オランダ	量子※(PQC移行表でAcceptable)	記載なし	量子(Acceptable)	量子(推奨)	[NL] pp.57-58, 92-95
スペイン	記載なし	記載なし	記載なし	記載なし	[ES] §4.5, p.20
チェコ(※9)	非推奨(128/192 bit)	記載なし	非推奨(出力≤256 bit)	非推奨(出力≤256 bit)	[CZ] pp.5, 10
	量子(256 bit)		量子(出力≥384 bit)	量子(出力≥384 bit)	
スロバキア	量子(Camellia-256)	記載なし	記載なし	非推奨(出力≤256 bit)	[SK] pp.4, 7
				量子(出力≥384 bit)	
フィンランド	記載なし	記載なし	古典(指定出力長)	古典(指定出力長)	[FI] p.3
ノルウェー	記載なし	記載なし	記載なし	記載なし	[NO] —
サウジアラビア	古典(128/192: Basic, 256: Advanced)	記載なし	古典(出力≥256 bit: Basic)	古典(出力≥512 bit: Advanced)	[SA] NCS-2:2025, pp.11-12
マレーシア	古典(Approved: 128/192/256 bit)	古典(Approved: 128 bit)	記載なし	記載なし	[MY] Web

※7 米国: SHAKE128, 256は、CNSA 2.0の汎用ハッシュ用途において非承認。

※8 カナダ: SHAKE単独の耐量子性判定ではなく、標準化PQC方式の内部構成要素としてのPQC対応。

※9 チェコ: 出力257~383 bitの耐性判定が明示されていない。

エンティティ認証

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

米国政府資料・参考文献

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

参考文献

- [CA] カナダ **Cyber Centre**, Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information (ITSP.40.111) May 2026 <https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111>
- [FR] フランス **ANSSI**, Follow-up position paper on post-quantum cryptography Nov 2023 <https://messervices.cyber.gouv.fr/guides/en-follow-position-paper-post-quantum-cryptography>
- [DE] ドイツ **BSI**, BSI TR-02102-1, Cryptographic Mechanisms: Recommendations and Key Lengths Jan 2026 <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.htm>
- [NL] オランダ **AIVD/NCSC**, The PQC Migration Handbook Nov 2024 <https://english.aivd.nl/documents/2024/12/3/the-pqc-migration-handbook>
- [ES] スペイン **CCN**, CCN-TEC 009, Recomendaciones de transición postcuántica Segura July 2026 <https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/boletines-pytec/495-ccn-tec-009-recomendaciones-transicion-postcuantica-segura/file>
- [CZ] チェコ **NÚKIB**, Doporučení v oblasti kryptografických prostředků, v4.1, 2026-03-04 https://portal.nukib.gov.cz/storage/uploads/2026/03/04/doporuceni-kryptograficka-bezpecnost-v4-1_uid_69a8216e3deb1.pdf
- [SK] スロバキア **NBÚ**, Cryptographic recommendations / national guidance, v1.0 Aug 2025 <https://www.nbu.gov.sk/data/att/3483.pdf>
- [FI] フィンランド **Traficom**, Kryptografiset vahvuusvaatimukset – kansalliset turvallisuuksuokat, 2024-12-09 https://www.kyberturvallisuuskeskus.fi/files/media/file/Kryptografiset_vahvuusvaatimukset_-_kansalliset_turvallisuuksuokat_1.pdf
- [NO] ノルウェー **NSM**, NSM Cryptographic Recommendations Mar 2025 <https://nsm.no/getfile.php/1314334-1742808614/NSM/Filer/Dokumenter/Veiledere/NSM%20Cryptographic%20Recommendations%202025.pdf>
- [UK] 英国 **NCSC**, Next steps in preparing for post-quantum cryptography Aug 2024 <https://www.ncsc.gov.uk/paper/next-steps-in-preparing-for-post-quantum-cryptography>
- [SA] サウジアラビア **NCA**, National Cryptographic Standards, NCS-2:2025 <https://istitlaa.ncc.gov.sa/en/security/nca/ncs/Documents/NCS-2-en.pdf>
- [MY] マレーシア **CyberSecurity Malaysia**, MySEAL 2.1 Approved Cryptographic Algorithms <https://mykripto.cybersecurity.my/index.php/services/myseal/myseal-category/aksa-myseal/aksa-myseal-approved>
- [AU] オーストラリア **ASD**, Information Security Manual, Guidelines for cryptography Sep 2026 <https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cyber-security-guidelines/guidelines-for-cryptography>
- [NZ] ニュージーランド **GCSB/NCSC**, New Zealand Information Security Manual Nov 2025 <https://nzism.gcsb.govt.nz/ism-document/pdf>

課題①

Category 1・2の暗号等の取扱い 等
(第1・2回会合議論反映版)

検討ポイント① セキュリティカテゴリの記載方法

黄マーカ一部

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

【考え方】

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

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

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

- ✓ カテゴリの定義については、米国NISTが2016年12月に公表したPQC標準化公募の際に示した記述をベースとし、暗号技術の観点からの正確性と、行政職員が参照する観点からの平易さ・利便性を総合的に勘案しており、現行の記載内容は適当。

- Category 1,3,5はブロック暗号に対する鍵探索に必要な計算資源を、Category 2,4はハッシュ関数に対する衝突探索に必要な計算資源を基準として定義されている。
- また、例えばCategory 1では、128ビット鍵のブロック暗号に対する鍵探索に必要な計算資源を基準としており、当該ブロック暗号の例としてAES-128が明記されている。

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

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

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

(参考) セキュリティカテゴリの定義 (米国NIST 2016年)

NIST (2016.12) "Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process"

<https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf>

4.A.5 Security Strength Categories (抜粋)

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

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

【仮訳 (機械翻訳ベース)】

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

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

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

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

4.6.1. Cryptographic Algorithm Security Strengths (抜粋)

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

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

Table 2. Security strength categories for post-quantum algorithms

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

【仮訳（機械翻訳ベース）】

4.6.1. 暗号アルゴリズムのセキュリティ強度（抜粋）

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

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

表2. 耐量子アルゴリズムのセキュリティ強度区分

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

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

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

Appendix E. Glossary (抜粋)

security categories

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

security strength

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

【仮訳（機械翻訳ベース）】

付録E. 用語集（抜粋）

セキュリティカテゴリ (security categories)

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

セキュリティ強度 (security strength)

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

(参考) カテゴリ関連記載 : FIPS 203・204・205

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

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

8. Parameter Sets (抜粋)

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

Table 2. Approved parameter sets for ML-KEM

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

FIPS204 “Module-Lattice-Based Digital Signature Standard”

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

4. Parameter Sets (抜粋)

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

Table 1. ML-DSA parameter sets

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

FIPS205 “Stateless Hash-Based Digital Signature Standard”

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

11. Parameter Sets (抜粋)

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

Table 2. SLH-DSA parameter sets

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

検討ポイント② 512ビットハッシュ関数の取扱い

7

黄マーカ部

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

【考え方】

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

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

＜表2 耐量子計算機暗号（PQC）リスト＞

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

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	—	—	—
	鍵共有	ML-KEM	ML-KEM-768 ML-KEM-1024	Category 3 Category 5
共通鍵暗号		AES	AES-192	Category 3
			AES-256	Category 5
ハッシュ関数		SHA2	SHA-384	Category 4
			SHA-512	Category 4 ^(注9)
		SHA3	SHA3-384	Category 4
			SHA3-512	Category 4 ^(注9)

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

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

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

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

検討ポイント③ Category 1・2の取扱い

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

【考え方】

- ✓ 表2は、PQC移行後も**長期的に利用していく暗号技術を示すリスト**としての性格を有することから、**Category 1・2の暗号技術を積極的に掲載することは適当でない**。
 - 量子コンピュータ技術の進展状況等を踏まえ、表1については、暗号技術検討会が危殆化したと決定した場合は、電子政府推奨暗号から外れ、表2のみが電子政府推奨暗号として残ることが想定される。そのため、2035年以降も利用予定のシステムについては、表1ではなく表2を参照して整備することになると考えられる。
 - 「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」では、128ビットセキュリティは2031～2040年は「利用可」だが、2041年以降は「移行完遂期間」とされ、2051年以降は順次「利用不可」となる。
- ✓ 公開鍵暗号のうち**ML-KEM**については、**Category 3・5の実装が広く見られ、Category 1でなければPQC移行できない具体的な支障も現時点では確認されていないことから、ML-KEM-512（Category 1）は表2に掲載しないことが適当**。
- ✓ 公開鍵暗号のうち**署名方式**については、**ML-DSA-44（Category 2）が広く利用される可能性もあることから、ML-DSA・SLH-DSAのCategory 1・2については、実利用・標準化動向を確認した上で掲載要否を判断することが適当。** **<議論>**
- ✓ **Category 1・2を掲載する場合**には、「可能な限りCategory 3以上の利用を推奨し、特に長期的な保護が必要なデータを取り扱う用途ではこれを強く推奨する。」と**注釈を付すことが適当**。
- ✓ **ブロック暗号及びハッシュ関数**については、Category 1・2の暗号技術は、当面は**現行暗号リスト（表1）に基づき引き続き利用可能**であり、PQC移行後の利用を想定する表2に追加する必要性も乏しい※ことから、**表2に掲載しないことが適当**。

※表2はそもそも量子コンピュータ（CRQC）への耐性を有する暗号技術を掲載するものであるが、例えばAES-128は量子コンピュータによるGroverのアルゴリズムにより、AES-192/256と比べ安全余裕が小さくなることから、表2にブロック暗号及びハッシュ関数のCategory 1・2を掲載することは適当ではない。
- ✓ Category 1・2については、当面の間、調達や相互運用性の観点からフォローが必要。

<参考：関係する暗号技術の例>

技術分類		暗号技術	セキュリティ カテゴリ(注8)
公開鍵暗号	署名	ML-D ML-D ML-D	Category 2 Category 3 Category 5
		SLH-D SLH-D SLH-D	Category 1 Category 1 Category 3
		SLH-D SLH-D SLH-D	Category 3 Category 3 Category 5
	鍵共有	ML-K ML-K ML-K	Category 1 Category 3 Category 5
		ML-K ML-K ML-K	Category 3 Category 3 Category 5
		ML-K ML-K ML-K	Category 3 Category 3 Category 5
	共通鍵暗号	AES AES AES	Category 1 Category 3 Category 5
		AES AES AES	Category 3 Category 3 Category 5
		AES AES AES	Category 3 Category 3 Category 5
	ハッシュ関数	SHA2 SHA2 SHA2	Category 2 Category 2 Category 4
		SHA2 SHA2 SHA2	Category 4 Category 4 Category 4
		SHA3 SHA3 SHA3	Category 2 Category 4 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

黄マーカー部

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

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

* 2030年以降は非推奨

フランス (ANSSI) : “Avis de l’ANSSI sur la migration vers la cryptographie post-quantique” (PQC移行に関するANSSIの見解)

オランダ (AIVD) : “The PQC Migration Handbook”

オーストラリア (ACSC) : “Guidelines for cryptography”

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

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

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

(参考) 海外政府機関による推奨状況②

ドイツ 情報セキュリティ庁 (BSI)
“Technical Guideline TR-02102-1 Cryptographic Mechanisms: Recommendations and Key Lengths” (2026.1)
<https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html>

2.4.3. ML-KEM Key Agreement (抜粋) ※[103]はFIPS203 ML-KEM with the parameter sets corresponding to NIST Security Strength **Categories 3 and 5** (see Table 2.7) from [110] is considered cryptographically suitable for **the long-term protection of confidential information** at the security level targeted in this Technical Guideline.

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

Table 2.7: Recommended parameters for ML-KEM.

オーストラリア サイバーセキュリティセンター (ACSC)
“Guidelines for cryptography” (2026.9時点)
<https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cyber-security-guidelines/guidelines-for-cryptography>

Using the Module-Lattice-Based Key Encapsulation Mechanism (抜粋)

The use of **ML-KEM-768 and ML-KEM-1024 are approved**. For interoperability and maintainability reasons, ML-KEM-768 will not be approved beyond 2030.

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

Key takeaways from this guidance (抜粋)

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

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

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

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

4.2) Recommended Cryptographic Primitives (抜粋)

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

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

Table 4.2 | Recommended parameter instantiations of the cryptographic primitives.

(参考) ML-DSA・SLH-DSAのIETFでの標準化状況

11

新規

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

- ✓ **X.509**及び**CMS**では、**ML-DSA**及び**SLH-DSA**の各パラメータセットを利用するための**仕様がRFC化**されている。
- ✓ **TLS**では、**ML-DSA**の各パラメータセットをハンドシェイク署名等に利用するための**仕様が検討中**（Internet-Draft）で、**IETFのTLS WG文書**となっている。**SLH-DSA**についても、同様の仕様が個人提出のInternet-Draftとして提案されたが、**現在は失効**しており、WGドラフトにはなっていない。
※署名サイズがML-DSAでは2.4~4.6KBなのに対し、SLH-DSAでは7.9~50KB程度と大きいので、エンドエンティティのハンドシェイク署名として適していない。
- ✓ **SSH**では、**ML-DSA**の各パラメータセットを利用するための**仕様が検討中**（Internet-Draft）で、**IETFのSSHM WG文書**※となっている。**SLH-DSA**についても、単独又は従来署名と組み合わせて利用するための仕様が**個人提出のInternet-Draftとして提案**されているが、WG文書にはなっていない。
※WG文書は、ML-DSAと従来署名を組み合わせた合成署名の仕様。
ML-DSA単独で利用する仕様は個人提出のInternet-Draftとして別途提案。
- ✓ **DNSSEC**では、**ML-DSA-44**を利用するための**仕様が検討中**（Internet-Draft）であるが、WG文書にはなっていない。**SLH-DSA**についても、SLH-DSA-[SHA2/SHAKE]-128sを利用する仕様が**個人提出のInternet-Draftとして提案**されているが、WG文書にはなっていない。

- (*1) RFC 9881 Internet X.509 Public Key Infrastructure -- Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA)
<https://www.rfc-editor.org/rfc/rfc9881.html>
- (*2) RFC 9909 Internet X.509 Public Key Infrastructure -- Algorithm Identifiers for the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)
<https://www.rfc-editor.org/rfc/rfc9909.html>
- (*3) RFC 9882 Use of the ML-DSA Signature Algorithm in the Cryptographic Message Syntax (CMS)
<https://www.rfc-editor.org/rfc/rfc9882.html>
- (*4) RFC 9814 Use of the SLH-DSA Signature Algorithm in the Cryptographic Message Syntax (CMS)
<https://www.rfc-editor.org/rfc/rfc9814.html>
- (*5) Use of ML-DSA in TLS 1.3
draft-ietf-tls-mldsa-06
<https://datatracker.ietf.org/doc/draft-ietf-tls-mldsa/06/>
- (*6) Post-Quantum Composite Signatures in SSH
draft-ietf-sshm-composite-sigs-00
<https://datatracker.ietf.org/doc/draft-ietf-sshm-composite-sigs/00/>
- (*7) Stateless Hash-Based Signatures for Secure Shell (SSH)
draft-josefsson-ssh-sphincs-02
<https://datatracker.ietf.org/doc/draft-josefsson-ssh-sphincs/>
- (*8) Module-Lattice Digital Signature Algorithm for DNSSEC
draft-westerbaan-dnssec-mldsa-04
<https://datatracker.ietf.org/doc/draft-westerbaan-dnssec-mldsa/>
- (*9) Stateless Hash-Based Digital Signatures with Merkle Tree Ladder Mode for DNSSEC
draft-fregly-dnsop-slh-dsa-mtl-dnssec
<https://datatracker.ietf.org/doc/draft-fregly-dnsop-slh-dsa-mtl-dnssec/>

(参考) ML-DSA・SLH-DSAの実装・利用状況

12

新規

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/>

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

【考え方】

<Camellia>

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

<KCipher-2>

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

<SHAKE128>

- ✓ 2024年度外部評価報告書※において、出力長が $n(\geq 256)$ ビットに対して、BHTアルゴリズムを適用する際に必要な計算時間と量子メモリの概算値は $\min(2^{256/3}, 2^{n/3}) = 2^{256/3}$ である。これはSHA-256の概算値 ($2^{256/3}$) と同じ。
- ✓ このため、**Category 2相当**であり、検討ポイント③の整理を踏まえ、**表2に掲載しないことが適当**。

<SHAKE256>

- ✓ 2024年度外部評価報告書※において、出力長が $n(\geq 256)$ ビットに対して、BHTアルゴリズムを適用する際に必要な計算時間と量子メモリの概算値は $\min(2^{512/3}, 2^{n/3})$ である。出力長（ハッシュ長）により強度が変わる。
 - ✓ このため、検討ポイント③の整理を踏まえ、SHA-384の概算値 ($2^{384/3}$) 以上の安全性を確保するため、**「ハッシュ長は384ビット以上とする。」との注釈を付した上で、「Category 4」として表2に掲載することが適当**。
- ※表1のSHAKE128及びSHAKE256には「ハッシュ長は256ビット以上とすること。」の注釈が付されている。

検討ポイント⑤ 暗号利用モード等の取扱い

新規＋課題②

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

【考え方】

<暗号利用モード及びメッセージ認証コード>

- ✓ 鍵長がkビットのとき、2024年度外部評価報告書※¹において、安全性が期待できる範囲は、「時間 $\leq 2^{k/2}$ かつ古典的に安全性が保障される範囲」とされる。（参考：AES-256の安全性が期待できる範囲は「時間 $\leq 2^{128}$ 」）
- ✓ 暗号利用モード及びメッセージ認証コードは、組み合わせて利用する暗号技術（ブロック暗号又はハッシュ関数）の安全性に依存することから、セキュリティカテゴリを単独で付すのではなく、次のように表記した上で、**表 2 に掲載することが適当。**
セキュリティカテゴリ：「組み合わせて利用する暗号技術のセキュリティカテゴリに準ずる。」
- ✓ また、**組み合わせる暗号技術は表 2 のものに限る旨の注釈を付すことが適当。**（→検討ポイント⑥）

<認証暗号（ChaCha20-Poly1305）>

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

<エンティティ認証>

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

※ 1 2024年度外部評価報告書：量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価 2024年度版（CRYPTREC-EX-3401-2024）

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

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

Q1モデルを主たる評価の前提とし、鍵長等に応じた安全性の目安を整理。

ハッシュ関数については、BHTアルゴリズムによる量子衝突探索を踏まえ、出力長・キャパシティ等に応じた安全性の目安を整理。

また、既存の古典的安全性評価に基づくデータ量・クエリ回数等の制約がQ1モデルでも基本的に維持されることを確認。

<参考：Q1モデルとQ2モデル>

【Q1モデル】攻撃者は量子計算能力を有するが、オラクルへのアクセスは古典的クエリに限定されるモデル

【Q2モデル】攻撃者は量子計算能力を有し、オラクルへのアクセスにおいて量子重ね合わせ状態のクエリが可能であるモデル

GCMやCBC-MAC等に対する多項式時間攻撃が報告されているが、その成立には秘密鍵を含む処理への量子オラクルアクセスが攻撃者に与えられる必要があり、通常の実運用とは大きく異なる前提に基づくものと整理

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

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

(2024年度外部評価報告書の表 5 を一部表記を変更・簡略化)

※Q1モデルで安全性が期待できる範囲。古典計算機のみが使える典型的な安全性評価と

整合性を取るため、単一鍵の安全性に焦点を当て、量子計算機のリソースとしては、

小さい多項式サイズの量子計算機が1つ使い、QRAMは必要な分だけ大きなものを使う状態。

※この表にある暗号技術については、Q1モデルにおいて（古典的に考慮すべき事項から追加して）

現状考慮すべきと思われる事柄はGrover のアルゴリズムによる鍵回復のみである。

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

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

(2024年度外部評価報告書の表 6 を一部表記を変更・簡略化)

※BHTのアルゴリズムを適用する際に必要な計算時間と量子メモリの概算値。

※計算時間の値はそのまま、安全性が期待できる時間の範囲の上限に対応する。

※なお出力長とキャパシティの単位はいずれもビットである。

※スポンジ構造のハッシュ関数、特にXOF (SHAKE128, SHAKE256) については、内部状態のキャパシティ部分で衝突を見つける攻撃も考慮に入っていることに注意。

検討ポイント⑥ 暗号利用モード等に関する注釈

全面修正

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

【考え方】

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

電子政府推奨暗号リスト

暗号技術検討会及び関連委員会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A)	(略)
メッセージ認証コード (注A)	(略)
認証暗号	(略)
エンティティ認証 (注A)	(略)

＜表2 耐量子計算機暗号（PQC）リスト＞

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

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

（注B）表2に掲載する他の技術分類の暗号技術と組み合わせて利用すること。

＜前回の議論の反映＞

✓ 組み合わせる暗号技術を明確にすべき。

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

例）暗号利用モード＝共通鍵暗号のうちブロック暗号
CMAC＝共通鍵暗号のうちブロック暗号
HMAC＝ハッシュ関数
ISO/IEC 9798-2＝共通鍵暗号
ISO/IEC 9798-3＝公開鍵暗号のうち署名
ISO/IEC 9798-4＝メッセージ認証コード

✓ 従来の文言も必要に応じて見直しを行うべき。

→冗長な表現を排除するとともに、「掲載された」という過去形の表現を修正。

検討ポイント⑦ 暗号利用モードに係る注釈の取扱い

全面修正

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

【考え方】

✓「XTS」に係る注釈

→表 1 の「XTS」に付される注 5 について、
前段（ブロック暗号には、CRYPTREC暗号リスト掲載128ビットブロック暗号を使う。）は、64ビットブロック暗号が表 2 に存在しないことから（追加予定もないことから）、同様の注釈は不要。

後段（利用用途はストレージデバイスの暗号化に限り、実装方法はNIST SP800-38Eに従うこと。）はXTS自体の制限事項であるため同様の注釈を表 2 の「XTS」にも付すことが適当。

✓「認証付き秘匿モード」に係る注釈

→表 1 の「認証付き秘匿モード」に付される注 6 について、
同様の注釈を表 2 の「認証付き秘匿モード」にも付すことが適当。

✓「GCM」に係る注釈

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

＜表 1 現行暗号リスト＞

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

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

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

(注 7) 初期化ベクトル長は96ビットを推奨する。

＜表 2 耐量子計算機暗号（PQC）リスト＞

技術分類		暗号技術	(略)
(略)		(略)	(略)
暗号利用モード	秘匿モード	(略)	(略)
		XTS (注C)	
	認証付き秘匿モード (注D)	CCM	
		GCM (注E)	

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

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

(注 E) 初期化ベクトル長は96ビットを推奨する。

＜前回の議論の反映＞

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

- **用語・表記の統一方針**を整理する必要があるか。

【考え方】

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

＜長音表記について＞

- ✓ **外来語の長音表記**（英語の語末の「-er」「-or」「-ar」等）については、公用文としては、
原則として長音符号「ー」を用いることとされているが、慣用に応じて「ー」を省くことができるとされている。
- ✓ 実際に政府関係文書においても長音符号の有無が語によって異なることから、**慣用や専門用語としての定着状況、関連文書における使用実態を踏まえ、語ごとに表記を統一**することとしてはどうか。
→**具体例：コンピュータ パラメータ カテゴリ**

文化庁 外来語の表記（平成3年内閣告示第2号）

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

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

Ⅱ 長音は、原則として長音符号を使って書く

長音は、長音符号を使って書く。

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

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

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

（略）

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

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

1.2 現行の規定（抜粋）

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

〈例〉 オーソリティー コンピューター エレベーター パーティー

(参考) 関連文書における外来語の長音表記の使用状況

新規

✓ 次の5種類の文書を対象に、外来語の長音表記の状況を整理。

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

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

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

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

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

(参考) 電子政府推奨暗号リスト～再改定後のイメージ

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

＜表 1 現行暗号リスト＞

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

＜表 2 耐量子計算機暗号（PQC）リスト＞

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

技術分類		暗号技術	セキュリティ カテゴリ(注8)
公開鍵暗号	署名	ML-DSA	ML-DSA-44(注)
		[P]	ML-DSA-65
			ML-DSA-87
			SLH-DSA-SHA2-128[s/f](注)
			SLH-DSA-SHAKE-128[s/f](注)
	鍵共有	SLH-DSA	SLH-DSA-SHA2-192[s/f]
		[P]	SLH-DSA-SHA2-192[s/f]
			SLH-DSA-SHAKE-192[s/f]
			SLH-DSA-SHA2-256[s/f]
			SLH-DSA-SHAKE-256[s/f]
共通鍵暗号	ブロック暗号	ML-KEM	ML-KEM-768
			ML-KEM-1024
	ストリーム暗号	AES	AES-192
		Camellia	Camellia-192
ハッシュ関数	ブロック暗号	AES	AES-256
		Camellia	Camellia-256
	ストリーム暗号	—	—
			SHA2
			SHA3
暗号利用モード	秘匿モード	SHA2	SHA-384
			SHA-512
			SHA3-384
	認証付き秘匿モード	SHA3	SHA3-512
		SHAKE	SHAKE256
メッセージ認証コード	秘匿モード	SHA2	SHAKE
			SHAKE
			SHAKE
	認証付き秘匿モード	SHA3	SHAKE
		SHAKE	SHAKE
認証暗号	秘匿モード	SHA2	SHAKE
			SHAKE
			SHAKE
	認証付き秘匿モード	SHA3	SHAKE
		SHAKE	SHAKE
エンティティ認証	秘匿モード	SHA2	SHAKE
			SHAKE
			SHAKE
	認証付き秘匿モード	SHA3	SHAKE
		SHAKE	SHAKE

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

課題③

ハイブリッド構成の取扱い

「ハイブリッド」の位置付け

• NIST における「ハイブリッド」

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

NIST CSWP 39より



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

• EUにおける「ハイブリッド」

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

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

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

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

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

「ハイブリッド」の位置付け

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

「ハイブリッド」の位置付け

表 4-1 ハイブリッド構成の目的と適用主体による整理

目的 主体	後方互換性確保	安全性維持
アルゴリズム	なし	<u>鍵共有アルゴリズム</u> • NIST SP 800-227(4.6. Multi-Algorithm KEMs and PQ/T Hybrids) [4] • NIST SP 800-56C Rev. 2³ [9] • draft-irtf-cfrg-hybrid-kems-07 [10] • draft-ietf-lamps-pq-composite-kem-12 [11]⁴ <u>署名アルゴリズム</u> • draft-ietf-lamps-pq-composite-sigs-14 [12]⁴
	<u>通信プロトコル</u> • RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3 [13] ※4.1.1 Cryptographic Negotiationにより後方互換性を提供するが、混成方式ではない <u>証明書構造</u> • draft-ietf-lamps-certdiscovery-02 [18] • ITU-T X.509(9.8 Alternative cryptographic algorithms and digital signature extensions) [19]	<u>通信プロトコル</u> • draft-ietf-tls-hybrid-design-16 [14] • draft-ietf-mls-combiner-02 [15] • ETSI TS 103 744 [16] • IEEE 802.11 Hybrid PQC Proposal [17] • draft-ietf-lamps-pq-composite-kem-12 [11]⁴ <u>証明書構造</u> • draft-ietf-lamps-pq-composite-sigs-14 [12]⁴
	(後方互換性確保/安全性維持 共通) • 耐量子移行を考慮したPKIベースのハイブリッド設計・実装 Architecting PKI Hierarchies for Graceful PQ Migration(PQC Conference) [20] - Hybrid PQC E-Mail Communication: Easing Migration Pain(PQC Conference) [21]	

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

後方互換性確保を目的とした「混成」方式は、Negotiationで解決することが主流。

※プロトコル依存性が高く、一概のリスト化は困難が予測される。

安全性維持のを目的とした「合成」方式の実態を紹介。

cryptrec-ex-3503-2025.pdf

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

「ハイブリッド」の位置付け

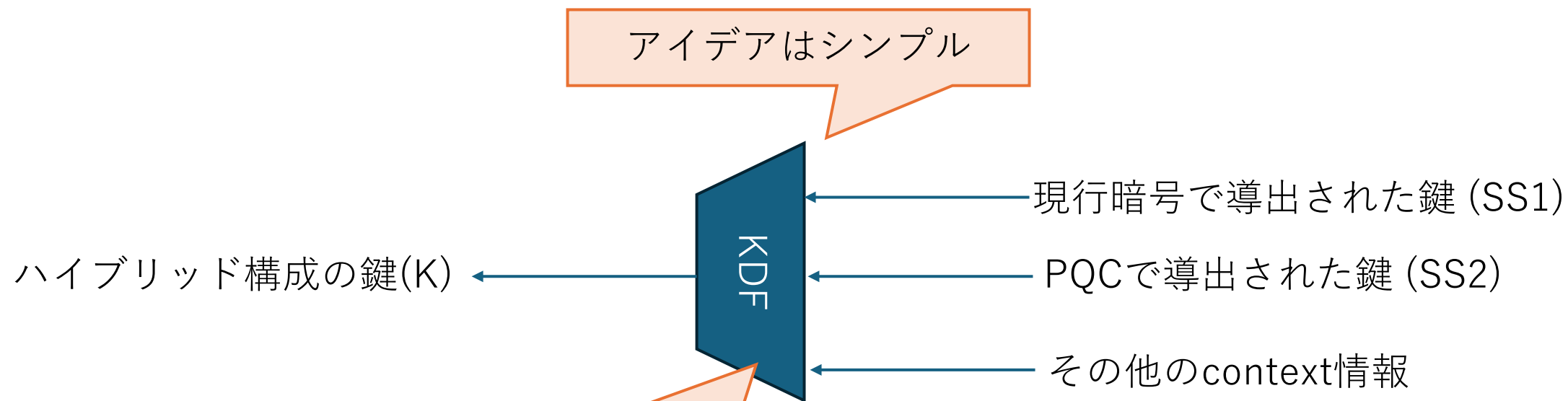
• 秘匿（KEM）用途

- マルチアルゴリズムKEMにおいて、複数の共有秘密から新たな共有秘密を導出する仕組みをKey Combinerと呼んでいる。
 - NIST SP 800-227ではKDFの一利用形態としてKey Combinerを紹介。
（既存KDFを、key combiner(コンバイナ)用途で利用することを承認）
 - ETSI TS 103 744 では、Key Combiner定義し、構成論を記載している。
（ETSI TS 103 744, Quantum-safe Hybrid Key Exchanges. 2020.）

• 署名用途

- Composite署名（合成方式）については、IETFでの標準化が進展中。混成方式をサポートするDual SignatureについてもIETFでの標準化が進展中。
- 以下についての議論は未成熟と認識しており、現状においてはリスト化の議論を行うための十分な議論を行う材料が揃っていないと認識（当資料末尾に関連資料有）。
 - ハイブリッドを利用する/利用しないユースケースはどのようなものか。
 - 合成（安全性確保）や混成（後方互換性確保）を利用する具体的なユースケースがどのようなものか。
 - 達成される安全性要件（Binding propertyのバインド対象をどうするか等）。
 - X.509やCMS方式との整合性確保をどのように行うか。

ハイブリッドの構成法（暗号化・合成）



KDFの構成法

Concatenation方式が主流 (e.g. $K = \text{KDF}(\text{SS1} || \text{SS2} || \text{context})$)

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

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

X.509 CMSのアルゴリズム指定

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

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

MLKEM鍵

ECDH鍵

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

SMI Security for PKIX Algorithms

Decimal	Description	Reference
1	id-alg-des40	[Reserved and Obsolete]
2	id-alg-noSignature	[RFC-ietf-lamps-rfc5272bis-11]
3	id-alg-dh-sig-hmac-sha1	[RFC2875]
4	id-alg-dhPop-sha1	[RFC2875]
5	id-alg-dhPop-sha224	[RFC6955]
6	id-alg-dhPop-sha256	[RFC6955]
7	id-alg-dhPop-sha384	[RFC6955]
8	id-alg-dhPop-sha512	[RFC6955]
15	id-alg-dhPop-static-sha224-hmac-sha224	[RFC6955]
16	id-alg-dhPop-static-sha256-hmac-sha256	[RFC6955]
17	id-alg-dhPop-static-sha384-hmac-sha384	[RFC6955]
18	id-alg-dhPop-static-sha512-hmac-sha512	[RFC6955]
25	id-alg-ecdhPop-static-sha224-hmac-sha224	[RFC6955]
26	id-alg-ecdhPop-static-sha256-hmac-sha256	[RFC6955]
27	id-alg-ecdhPop-static-sha384-hmac-sha384	[RFC6955]
28	id-alg-ecdhPop-static-sha512-hmac-sha512	[RFC6955]
29	id-alg-ecdsa-with-sha256	[draft-wang-tls-raw-public-key-with-ibc-02]
30	id-RSASSA-PSS-SHAKE128	[RFC8892]
31	id-RSASSA-PSS-SHAKE256	[RFC8892]
32	id-ecdsa-with-shake128	[RFC8892]
33	id-ecdsa-with-shake256	[RFC8892]
34	id-alg-xmss-hashsig	[RFC9802]
35	id-alg-xmssmt-hashsig	[RFC9802]
36	id-alg-unsigned	[RFC9925]
37	id-MLDSA44-RSA2048-PSS-SHA256	[RFC-ietf-lamps-pq-composite-sigs-19]
38	id-MLDSA44-RSA2048-PKCS15-SHA256	[RFC-ietf-lamps-pq-composite-sigs-19]
39	id-MLDSA44-Ed25519-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
40	id-MLDSA44-ECDSA-P256-SHA256	[RFC-ietf-lamps-pq-composite-sigs-19]
41	id-MLDSA85-RSA3072-PSS-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
42	id-MLDSA85-RSA3072-PKCS15-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
43	id-MLDSA85-RSA4096-PSS-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
44	id-MLDSA85-RSA4096-PKCS15-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
45	id-MLDSA85-ECDSA-P256-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
46	id-MLDSA85-ECDSA-P384-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
47	id-MLDSA85-ECDSA-brainpoolP256r1-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
48	id-MLDSA85-Ed25519-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
49	id-MLDSA87-ECDSA-P384-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
50	id-MLDSA87-ECDSA-brainpoolP384r1-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
51	id-MLDSA87-Ed448-SHAKE256	[RFC-ietf-lamps-pq-composite-sigs-19]
52	id-MLDSA87-RSA3072-PSS-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
53	id-MLDSA87-RSA4096-PSS-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
54	id-MLDSA87-ECDSA-P521-SHA512	[RFC-ietf-lamps-pq-composite-sigs-19]
55	id-MLKEM768-RSA2048-SHA3-256	[draft-ietf-lamps-pq-composite-kem-10]
56	id-MLKEM768-RSA3072-SHA3-256	[draft-ietf-lamps-pq-composite-kem-10]
57	id-MLKEM768-RSA4096-SHA3-256	[draft-ietf-lamps-pq-composite-kem-10]
58	id-MLKEM768-X25519-SHA3-256	[draft-ietf-lamps-pq-composite-kem-10]
59	id-MLKEM768-ECDH-P256-SHA3-256	[draft-ietf-lamps-pq-composite-kem-10]
60	id-MLKEM768-ECDH-P384-SHA3-256	[draft-ietf-lamps-pq-composite-kem-10]
61	id-MLKEM768-ECDH-brainpoolP256r1-SHA3-256	[draft-ietf-lamps-pq-composite-kem-10]
62	id-MLKEM1024-RSA3072-SHA3-256	[draft-ietf-lamps-pq-composite-kem-10]
63	id-MLKEM1024-ECDH-P384-SHA3-256	[draft-ietf-lamps-pq-composite-kem-10]
64	id-MLKEM1024-ECDH-brainpoolP384r1-SHA3-256	[draft-ietf-lamps-pq-composite-kem-10]
65	id-MLKEM1024-X448-SHA3-256	[draft-ietf-lamps-pq-composite-kem-10]
66	id-MLKEM1024-ECDH-P521-SHA3-256	[draft-ietf-lamps-pq-composite-kem-10]

8

- **目標：**

- プロトコル内部のHKDFのAPIを極力変更しない設計（入出力を抽象化して変換）

- **方向性：**

- アルゴリズム指定は3つに分けて指定する。
 - **supported_groups** : 鍵交換アルゴリズムを指定 (リスト化済み)
 - signature_algorithms : 署名アルゴリズムを指定 (ハイブリッド署名でのスコープ。今後整備される見通し)
 - 共通鍵とハッシュの指定 : Cipher suiteを指定 (従来と同じ)

- **实施例：**

- X25519MLKEM768 (右表内の4588)

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

ECDHE鍵 || MLKEMの鍵

- 特徴：

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

supported_groups
(コードポイント)

Transport Layer Security (TLS) Parameters

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

ETSI TS 103 744

• ハイブリッド構成論

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

Fixed values:

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

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

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

Input:

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

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

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

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

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

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

Process:

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

Output:

key_material - derived key material.

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

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

署名に関するハイブリッド関連議論

- ハイブリッド署名について、議論は未成熟

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

- ハイブリッド署名 アルゴリズム アプローチ

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

- ハイブリッド署名 プロトコル

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

リスト化に向けての考慮点

• スコープの選定

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

• リスト化の単位をどのようにするか

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

参考：リスト記載案

- **コンバイナを直接記載する方向性（EUアプローチに近い）**
 - 案1：技術分類に**コンバイナを新設**し、暗号名称**CatKDF（ETSI TS 103 744）**を記載する（または類似する文章を作成し、その文章内で命名した名称を記載）。
 - 案2：**鍵共有の技術分類内**に、暗号名称**CatKDF（ETSI TS 103 744）**を記載する（または類似する文章を作成し、その文章内で命名した名称を記載）。
- **コンバイナとその入力をセットでリストに記載する方向性（X.509のアプローチ）**
 - 案3：安全性が確認できた**compositeKEM（合成方式）**のリストを記載する。
 - 組み合わせで、相当な数になる見通し。
- **コンバイナはKDFの1つのユースケースとして扱い、リストに記載しない方向性（NISTアプローチに近い）**
 - 案4：コンバイナを使う時のKDFにおいては、電子政府推奨暗号リストに記載されたハッシュ関数を利用するようにと注意喚起する。
 - 安全な現行暗号アルゴリズムと安全なPQCアルゴリズムを組み合わせても、安全になるとは限らない旨も示す。

参考：関連する技術論点

- **鍵長の選択（2つの方式の強度を揃えるのか）**
 - 最小強度をどうするか（class 1,2 をどうするか）
 - あえてPQを強くするという考えもあるが、それも含めるか
 - 鍵長に関しては、別ドキュメントでまとめるとの整理で良いか
- **KDFへの入力やメタデータ**
 - 入力順序の固定はどうか
 - Contextをどのように記載するか
 - 入力の長さ管理を明示的に行うか
 - 上位プロトコルでバインディング等を行っている場合の扱いをどうするか

「耐量子計算機暗号（PQC）リスト検討タスクフォース」 開催要綱

1. 開催の趣旨・目的

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

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

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

2. 検討事項

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

3. 構成等

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

4. 議事の公開

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

5. 庶務

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

(別紙)

構成員・オブザーバ名簿
(五十音順、敬称略)

(構成員)

岩田 哲 名古屋大学 未来材料・システム研究所 教授

漆畠 賢二 GMOグローバルサイン株式会社 CTO室 フェロー

垣内 由梨香 日本マイクロソフト株式会社
カスタマープロテクション リスクマネージャー

國廣 昇 筑波大学 システム情報系 教授

須賀 祐治 株式会社インターネットイニシアティブ
ネットワークサービス事業本部
セキュリティ本部 セキュリティ情報統括室 シニアエンジニア

高木 剛 東京大学 大学院情報理工学系研究科 数理情報学専攻 教授

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

松本 勉 国立研究開発法人産業技術総合研究所 フェロー
横浜国立大学 先端科学高等研究院 上席特別教授

(オブザーバ)

内閣官房国家サイバー統括室

CRYPTREC暗号リストのPQC対応と 検討課題

CRYPTREC暗号リストの改定概要

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

CRYPTREC暗号リストのリスト構成

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

<リスト構成のイメージ>

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

「耐量子計算機暗号(PQC)リスト」の対象範囲

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

※Cryptographically Relevant Quantum Computer。現行暗号の解読に利用可能な水準の量子計算機。

<対象範囲のイメージ>

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

パラメーターセット等の取扱い

- 暗号強度等を変えるために複数用意されている**パラメーターセット**についてもリストに**掲載**。
- 各パラメーターセットに対応する**セキュリティのカテゴリ**もリストに**掲載**。
 - ✓ パラメーターセット及びカテゴリともに、システム調達時に暗号技術を選択する上で**重要な選択肢**。

※例えばML-KEMでは、右記の記載イメージのように3種が定義（括弧内はそれぞれに対応するセキュリティのカテゴリ）。

<パラメーターセットの記載イメージ>

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

2026年3月改定における取扱い

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

(参考) CRYPTREC暗号リスト(抄) (2026.3更新後)

電子政府推奨暗号リスト

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

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

<表 1 現行暗号リスト>

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

<表 2 耐量子計算機暗号（PQC）リスト>

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

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

CRYPTREC暗号リストのPQC対応に関する検討課題

- 2025年度の暗号技術検討会において、CRYPTREC暗号リストの耐量子計算機暗号（PQC）対応に関する検討を行い、更なる検討が必要な課題について保留※した上でCRYPTREC暗号リストの改定を実施。
※現時点で、表2（耐量子計算機暗号（PQC）リスト）には、Category1・2の暗号技術や、暗号利用モードや認証暗号等の暗号技術は掲載していない。
 - これらの課題については、安全性評価の観点のほか、利活用・普及促進の観点も含めた横断的な検討が必要。
- 暗号技術評価委員会及び暗号技術活用委員会の協力も得ながら、暗号技術検討会の直下に、新たに「耐量子計算機暗号（PQC）リスト検討タスクフォース」を設け、2026年度末までを目途に検討を進める。

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

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

＜参考：関係する暗号技術の例＞

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

課題② 暗号利用モードや認証暗号等の取扱い

- ✓ 現行暗号のCRQC（Cryptographically Relevant Quantum Computer）への耐性に関して、AES、SHA2、SHA3については、CRYPTRECの外部評価報告書※等から明らかな。 ※量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価 2024年度版（CRYPTREC-EX-3401-2024）
- ✓ 暗号利用モード、メッセージ認証コード、認証暗号、エンティティ認証や一部の共通鍵暗号とハッシュ関数※については検討が必要。
※Camellia、KCipher-2、SHAKE-256等

課題③ ハイブリッド構成の取扱い

- ✓ 現行暗号とPQCを組み合わせたハイブリッド構成について、CRYPTRECとしてどのように取り扱うか検討が必要。

課題④ 公開鍵暗号方式のPQCの安全性評価等の進め方

- ✓ 今後策定予定のFIPS標準等を始めとするPQCについて、どのような順序で安全性評価等を実施すべきか検討が必要。
- ※FIPS204、205は2026年度中に安全性評価等が終了予定。

電子政府における調達のために参照すべき暗号のリスト (CRYPTREC暗号リスト)

令和 5 年 3 月 30 日

デジタル庁・総務省・経済産業省

(最終更新：令和 8 年 3 月 30 日)

電子政府推奨暗号リスト

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

<表 1 現行暗号リスト>

技術分類		暗号技術
公開鍵暗号	署名	DSA ^(注 1)
		ECDSA
		EdDSA
		RSA-PSS
		RSASSA-PKCS1-v1_5
	守秘	RSA-OAEP
	鍵共有	DH
		ECDH ^(注 2)
共通鍵暗号	64ビットブロック暗号 ^(注 3)	該当なし
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128 ^(注 4)
		SHAKE256 ^(注 4)
(次ページに続く)		

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

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

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

技術分類		暗号技術
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
		XTS（注５）
	認証付き秘匿モード（注６）	CCM
		GCM（注７）
メッセージ認証コード		CMAC
		HMAC
認証暗号		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3
		ISO/IEC 9798-4

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

(注2) 使用するMACはHMAC又はCMACに限る。

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

(注4) ハッシュ長は256ビット以上とすること。

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

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

(注7) 初期化ベクトル長は96ビットを推奨する。

＜表 2 耐量子計算機暗号（PQC）リスト＞

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

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

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

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

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

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

推奨候補暗号リスト

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

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

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

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

(注11) 平文サイズは64ビットの倍数に限る。

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

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

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

運用監視暗号リスト

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

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

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

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

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

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

(注17) 安全性の観点から、メッセージ長を固定して利用すべきである。

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

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

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

更新履歴情報

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

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