総務省提出資料①

耐量子計算機暗号（PQC）に対応した CRYPTREC暗号リストの在り方について

2025年度 第１回 暗号技術検討会(R8.3.25) 資料より抜粋

検討ポイント①　文書として別にするか

➢ PQC対応のリストについて、**現行の文書（CRYPTREC暗号リスト）の中にリストを追加する方法【案１】**と、**新たに別の文書を作成する方法【案２】**とのどちらにすべきか。
※「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）」（CRYPTREC LS-0001-2022R1）

【案１】 現行の文書（CRYPTREC暗号リスト）の中にPQC対応のリストを追加する。

✓ （特に懸念点等はない。）

＜案１のイメージ＞

＜CRYPTREC暗号リスト＞
電子政府推奨暗号リスト
推奨候補暗号リスト
運用監視暗号リスト
＋
PQCリスト(仮)

【案２】 現行の文書（CRYPTREC暗号リスト）とは別に新たに別の文書を作成する。

✓ 参照すべき文書が２つになることは、現状の運用から大きく変わることになり、利用する政府機関側にとってわかりにくく混乱を招きかねない。

＜案２のイメージ＞

＜CRYPTREC暗号リスト＞
電子政府推奨暗号リスト
推奨候補暗号リスト
運用監視暗号リスト

＋

＜PQC対応新リスト＞
PQCリスト(仮)

→ **案１、現行の文書の中にPQC対応のリストを追加してはどうか。**
※政府統一基準を担当する国家サイバー統括室(NCO)においても案１とすることに特段の異論がないとの回答。

検討ポイント②　リストとして別にするか

➢ PQC対応のリストについて、**「電子政府推奨暗号リスト」の中にPQC対応の表を追加する方法【案１】**と、**既存の３リストとは別に、新たにリストを追加する方法【案２】**とのどちらにすべきか。

【案１】「電子政府推奨暗号リスト」の中にPQC対応の表を追加する。

- ✓「電子政府推奨暗号リスト」の名称は変わらず、政府統一基準群等の関連文書の変更が最低限となる。
- ✓ CRYPTREC暗号リスト内の「電子政府推奨暗号リスト」の定義文について変更検討が必要。
  ※「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」という部分のPQCへの適用について、PQCは今後の普及が見込まれると判断できるか検討し、合致しない場合は定義の文面の変更について検討が必要。
- ✓「電子政府推奨暗号リスト」に、表１・表２などの細区分が必要で、名称や説明文の有無の検討が必要。
- ✓ 長期的にPQC移行完了後も、３リスト構成自体は変更されないため長期的にわかりやすい。
  ※移行が進展した場合、PQC対応していない暗号技術は、電子政府推奨暗号リストから運用監視暗号リストに移行されると想定。

＜案１のイメージ＞

＜CRYPTREC暗号リスト＞
①電子政府推奨暗号リスト
　表１　現行暗号リスト(仮)
　表２　PQCリスト(仮)
②推奨候補暗号リスト
③運用監視暗号リスト

【案２】既存の３リストとは別に、新たにリストを追加する。

- ✓ リスト構成が変わるため、政府統一基準群等の各種文書で利用する用語の全面見直しが必要。
- ✓「電子政府推奨暗号リスト」の定義文について再検討する必要がない。
- ✓ １リストで１つの表となるため、文書構成はわかりやすいが、PQCのリストが「電子政府推奨暗号リスト」と同程度(以上)に推奨されることを明確化する必要。
- ✓ 長期的にPQC移行完了後も、改めて全面的なリスト構成の見直しが必要。

＜案２のイメージ＞

＜CRYPTREC暗号リスト＞
①電子政府推奨暗号リスト
②推奨候補暗号リスト
③運用監視暗号リスト
④PQCリスト(仮)

→ 政府関連文書への影響を鑑み**案１、「電子政府推奨暗号リスト」の中にPQC対応の表を追加してはどうか。**

※NCOにおいても次の理由で案１とすることに特段の異論がないとの回答。

○政府統一基準においては、「暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」に基づき」としており、利用実績や普及見込には直接言及していないため、案1のように「電子政府推奨暗号リスト」の中にPQC対応の表を追加する方向性であれば、政府統一基準の改定をすることなく対応することが可能と考えられる（ガイドラインの改定については、別途、検討が必要）。

○一方で、案2のように別途リストを作成し、当該リストを「電子政府推奨暗号リスト」と同レベルの位置付けにしようとするのであれば、サイバーセキュリティ戦略本部決定を経た上で政府統一基準の改定が必要となる可能性がある。また、リスト構成の見直し等の都度、同様に政府統一基準の改定が必要となる可能性がある。

検討ポイント③　量子計算機耐性を持つ共通鍵暗号等の取扱い

➢ PQC対応のリストについて、**公開鍵暗号方式の狭義のPQCだけをリスト(表)とする方法【案１】**と、**量子計算機耐性を持つ共通鍵暗号等についてもリスト(表)に追加する方法【案２】**のどちらにすべきか。

【案１】 公開鍵暗号方式の狭義のPQCだけをリスト(表)とする。

✓ 共通鍵暗号等の量子計算機耐性については、
CRYPTREC暗号リストの脚注か暗号強度要件※に規定することで十分。
※「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）

＜案１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

【案２】 量子計算機耐性を持つ共通鍵暗号等についてもリスト(表)に追加する。

✓ リスト(表)を確認すれば量子計算機耐性を持つ暗号が確認でき、利用者の利便性が向上する。

✓ 従来は、一つの暗号技術について、３つリストに重複して掲載されることはなかったが、
AES等については、検討ポイント②で細分した表１（現行暗号の表）と、
表２（PQC対応の表）に重複して掲載することになるため、
これが利用者の混乱を招くおそれはないか。
→CRYPTREC暗号リストにおいて混乱を招かないように十分に配慮。

＜案２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）

→ PQC移行（＝量子計算機対応）は、これまでの移行に比べても、何が“耐量子”で何が“非耐量子”なのかが直感的に分かりにくいことに加え、既存システムの大規模な改修が必要となるなど、より多くの関係者に理解してもらう必要があることから、**案２、量子計算機耐性を持つ共通鍵暗号等についてもリスト(表)に追加してはどうか。**
※NCOにおいても案２とすることに特段の異論がないとの回答。

検討ポイント④　リストの名称

➢ 検討ポイント②・③で新リストの概要が定まったところ、「電子政府推奨暗号リスト」の中に新たに作成される**表１（現行暗号の表）と、表２（PQC対応の表）**についてどのような**名称**とすべきか。

【考え方】

✓ 表１については、移行に際して現在主に用いられている暗号である趣旨がわかりやすいよう「現行暗号リスト」としてはどうか。
ただし、今後、PQC移行の進展に伴い、必要に応じて名称を見直すことも視野にいれるべきではないか。

✓ 表２について、政府部内において「耐量子計算機暗号（PQC）」という用語が定着していることも踏まえ、「耐量子計算機暗号（PQC）リスト」としてはどうか。
※2025年６月から検討が開始された政府の会合も「政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議」であり、サイバーセキュリティ戦略（閣議決定文書）においても「耐量子計算機暗号（PQC）への移行」などとされている。

✓ 検討ポイント③を踏まえると、表２は量子計算機への耐性を有する共通鍵暗号等も含む。
このため、「耐量子計算機暗号（PQC）」という用語について、改めて検討すると次のとおりであり、今後、必要に応じてどちらの意味で用いているか誤解のないようにしていく必要がある。

- 狭義には、量子計算機でも解読困難な数学的課題に基づいた公開鍵暗号方式を指す。
- 広義には、量子計算機への耐性を有する暗号技術を指す。
例えば「PQC移行」という場合には共通鍵暗号の移行（例：AES-128→AES-256）も含んで議論されることが多い。

→ **表１**については、「**現行暗号リスト**」とし、今後、必要があれば名称を見直すこととしてはどうか。
表２については、「**耐量子計算機暗号（PQC）リスト**」としてはどうか。

検討ポイント⑤　PQCのパラメータセットの取扱い

➢ PQCでは、通常、パラメーターセットが定義されており、**各パラメーターセットもリストに掲載すべきか否か。**

【背景】 PQCでは複数のパラメーターセットが定義。

✓ 演算内容や安全性証明の枠組みは共通しているが、格子の次元やノイズ分布などの安全性を調整するパラメータが異なる。

✓ 例えばML-KEMではFIPS 203で次の３種類が定義される。
（パラメータセットとともにセキュリティのカテゴリもFIPSに明記。）
- ML-KEM-512 (Category 1)
- ML-KEM-768 (Category 3)
- ML-KEM-1024 (Category 5)

<参考：カテゴリのレベル>

レベル１	128ビット鍵を持つブロック暗号に対する鍵探索（例: **AES-128**）
レベル２	256ビットのハッシュ関数に対する衝突探索（例: **SHA-256** / SHA3-256）
レベル３	192ビット鍵を持つブロック暗号に対する鍵探索（例: **AES-192**）
レベル４	384ビットのハッシュ関数に対する衝突探索（例: **SHA-384** / SHA3-384）
レベル５	256ビット鍵を持つブロック暗号に対する鍵探索（例: **AES-256**）

【考え方】

✓ システム調達時に<u>暗号技術を選択する上でパラメータセットは重要な選択肢</u>であり、CRYPTREC暗号リストで明示することが適当ではないか。
※現行のCRYPTREC暗号リストでも、例えばSHA-384とSHA-512では、
演算内容が同じで出力長だけが異なるが、別の暗号技術として掲載される例がある。

<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)

✓ <u>「カテゴリ」</u>についても、暗号技術を選択する上で重要な要素であり、カテゴリが定義されているものは<u>併記することが適当</u>ではないか。
また、表２における<u>AESやSHAについてもカテゴリを併記</u>する（表１については従来どおりの表記とする）ことが適当ではないか。
※現行暗号は「Xビットセキュリティ」で暗号強度要件の議論をしていたが、PQCでは、「カテゴリX」として暗号強度要件の議論を行うことが想定される。

✓ <u>ハッシュ関数について、SHA2とSHA3を名称としてグループ化</u>（各暗号技術はパラメーターセットの扱い）とすることでよいか。

✓ PQC対応としている製品においてもパラメーターセットまで明示しているものは少なく、明示について周知啓発も必要ではないか。

→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となることから、
各パラメーターセットについて、カテゴリとともにリストに掲載してはどうか。
※「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）」の2024年度版では「安全性レベル」と表記していたが、今後は「カテゴリ（Category）」とする。
これは、定義が置かれた米国NISTの文書では「Security Strength Categories」とされているものを指すことをわかりやすく（紛れがないように）するものである。

検討ポイント⑥　引き続き議論が必要な課題

- CRYPTREC暗号リストのPQC対応に当たり、次の課題が未整理であり引き続き検討する必要があるのではないか。
  - 課題① **Category 1･2**の暗号の取扱い
  - 課題② **暗号利用モードや認証暗号等**の取扱い
  - 課題③ **ハイブリッド構成**の取扱い
  - 課題④ **PQCの安全性評価等の進め方**

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

✓ 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。

＜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 (Category 5)

課題② 暗号利用モードや認証暗号等の取扱い

※CRQC: Cryptographically Relevant Quantum Computer

✓ 現行暗号のCRQCへの耐性について、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）

✓ 一方で、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Camellia、KCipher-2については検討が必要。

課題③ ハイブリッド構成の取扱い

※従来は「ハイブリッドモード」と称していたが暗号技術評価委員会での取扱いを踏まえ今後は「ハイブリッド構成」と称する。

✓ 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。

→ これら課題の取扱いについては安全性評価の観点や利活用・普及促進の観点から横断した検討が必要であり、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（仮称）」**を立ち上げ、検討を行ってはどうか。

検討ポイント⑦　リストの説明文等

➢ これまでの検討ポイントを踏まえ、「電子政府推奨暗号リスト」の説明文を修正する必要があるか。
また、表１と表２に説明文を追加する必要はあるか。

【考え方】

- ✓ 政府機関等において原則2035年までにPQC移行が行われることとなり、PQCの普及が見込まれることから、当面の間、PQCは「今後の普及が見込まれる」と判断することでよいか。
- ✓ 「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」は、現在はPQCに対する規定がなく、2026年度に見直し予定。このため、規定の適用関係が明確になるように脚注を追加してはどうか。
- ✓ 表１について、従来のリストと同じであり特段の補足説明事項は不要ではないか。
- ✓ 表２について、新たに作成したものであり、表１との違いを説明する必要があるのではないか。
（広義の意味でPQCを用いていることに留意。）
- ✓ 表２について、今後、FIPS標準の評価を順次実施するほか、暗号利用モードや認証暗号等の取扱いについても今後議論を行うなど、暗号技術を今後も追加する見込みであり、予見可能性を高めるためにその旨の説明を追記。

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」[5]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。

凡例
赤下線：現行からの改正部分
赤文字：本頁における検討部分

<表１　現行暗号リスト>
【表略】

<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]。
【表略】

1･2　（略）
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
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/[前ページの資料を整形して掲載]

→上に示すように、「電子政府推奨暗号リスト」の**説明文や注釈について、必要な修正**を行うこととしてはどうか。

検討ポイント⑦’ リストの説明文等

➢ 今回の更新と合わせ、CRYPTREC暗号リストの記載を適正化するため、次の修正を合せて行うこととする。

- ✓「安全性」について「safety」と「security」のどちらであるか明確とするため、追記を行うこととする。
- ✓ RSA暗号の強度について、注１として「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RSA 1024に係る移行指針」の記載があるが、現在は強度について「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」に規定されており、当該注釈は冗長であるため削る。
  ※運用監視暗号リストの注８も同様に削る。
- ✓ 注番号及び脚注番号について、番号がこれまで追記してきた順となっており複雑化していたことから、文書冒頭からの出現順となるよう番号を振替え。
- ✓ このほか、暗号技術評価委員会において提案のあった注釈を追加。
  ※ECDHに「使用するMACはHMAC又はCMACに限る。」との注を付すもの。

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<u>（セキュリティ）</u>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」[~~5~~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18）
		ECDSA
		EdDSA
		RSA-PSS~~（注１）~~
		RSASSA-PKCS1-v1_5~~（注１）~~
	守秘	RSA-OAEP~~（注１）~~
	鍵共有	（略）
（略）	（略）	（略）

＜表２ 耐量子計算機暗号（PQC）リスト＞

【略】

（略）

~~（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）~~

（略）

検討ポイント⑧　CRYPTREC暗号リスト・移行ルール

- 「電子政府推奨暗号リスト」を表１・表２としたこと、及びPQC（ML-KEM等）については、移行のためその普及を積極的に図っていく必要があること等から、**移行ルールについて次のように赤字部分を追加してはどうか。**
- 今後、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、移行ルールは適宜見直しを行う。

＜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る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
表１　現行暗号リスト
表２　耐量子計算機暗号(PQC)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必要があるため、いきなりリストから削除することはしない。

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る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」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。

（参考）カテゴリ関連記載：カテゴリの定義（米国NIST）

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)

（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	Values assigned by each parameter set		
(see Sections 6.1 and 6.2 of this document)	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

（参考）カテゴリ関連記載：CRYPTREC PQCガイドライン

「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）2024年度版」CRYPTREC GL-2007-2024

安全性レベル NIST PQC標準化プロジェクトにおいて，暗号方式の安全性はレベル1から5で定義されており，提案者は応募時にパラメータと達成される安全性レベルを示す必要があった。レベル1, 3, 5はそれぞれAES128, AES192, AES256などの128, 192, 256bitsの秘密鍵を持つブロック暗号の鍵復元の困難性と同等かそれ以上の計算量であり，レベル2と4はそれぞれSHA256/SHA3-256とSHA384/SHA3-384などの256bitsと384bitsの暗号学的ハッシュ関数の衝突探索の困難性と同等かそれ以上の古典もしくは量子計算量とされている。レベル1から5の具体的な計算量は表1.1で与えられる。古典コンピュータによる攻撃者に対しては古典論理回路のゲート数が，量子コンピュータを利用可能な攻撃者に対しては量子回路のゲート数と最大深さの積が与えられている。計算量評価において，公開鍵暗号方式では，IND-CCA2安全性を考える際には2^{64}個以下の選択暗号文を復号オラクルに古典的にクエリできるとし，署名方式では，EUF-CMA安全性を考える際には2^{64}個以下のメッセージを署名オラクルに古典的にクエリできるとしている。
　また，レベル1,3,5の量子回路計算量で2^{157}, 2^{221}, 2^{285}とされている部分は2016年のCall for proposalsでは2^{170}, 2^{233}, 2^{298} であった。つまり，2016年のPQC候補でレベル1, 3, 5とされているものは2022年の定義でもレベル1, 3, 5 の基準を満たすことになる。この更新はAESを解読する量子回路の改良により，量子計算量が改善されたことによる。

表1.1: 2022年に公表されたNIST PQC標準化プロジェクト追加署名Call for proposalsにおける安全性レベルと計算量の対応表。各レベルは古典，量子のどちらか一方の基準を満たすものとして定義されている。

レベル	量子回路の (最大深さ)×(ゲート数)	古典論理ゲート数
レベル1	2^{157}	2^{143}
レベル2	–	2^{146}
レベル3	2^{221}	2^{207}
レベル4	–	2^{210}
レベル5	2^{285}	2^{272}

（参考）カテゴリ関連記載：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)
名称	パラメーターセット				
ML-KEM	ML-KEM-512 (Category 1)				
	ML-KEM-768 (Category 3)	Recommended	préférence	Acceptable	approved*
	ML-KEM-1024 (Category 5)	Recommended	préférence	Recommended	approved
ML-DSA	ML-DSA-44 (Category 2)				
	ML-DSA-65 (Category 3)	Recommended	préférence	Acceptable	approved*
	ML-DSA-87 (Category 5)	Recommended	préférence	Recommended	approved
SLH-DSA	SLH-DSA-[SHA2/SHAKE]-128[s/f] (Category 1)		SLH-DSAの記載なし	Acceptable	強度の記載なし
	SLH-DSA-[SHA2/SHAKE]-192[s/f] (Category 3)	Recommended	SLH-DSAの記載なし	Recommended	強度の記載なし
	SLH-DSA-[SHA2/SHAKE]-256[s/f] (Category 5)	Recommended	SLH-DSAの記載なし	Recommended	強度の記載なし
AES	AES-128 (Category 1)	Recommended		Acceptable	approved*
	AES-192 (Category 3)	Recommended			approved*
	AES-256 (Category 5)	Recommended	encourage	Recommended	approved
SHA2	SHA-256 (Category 2)	Recommended		Recommended	approved*
	SHA-512/256 (Category 2)	Recommended			
	SHA-384 (Category 4)	Recommended	encourage	Recommended	approved
	SHA-512 (Category 5)	Recommended	encourage	Recommended	approved
SHA3	SHA3-256 (Category 2)	Recommended		Recommended	PQC内部使用のみ可
	SHAKE128 (Category 2)			Acceptable	PQC内部使用のみ可
	SHA3-384 (Category 4)	Recommended	encourage	Recommended	PQC内部使用のみ可
	SHA3-512 (Category 5)	Recommended	encourage	Recommended	PQC内部使用のみ可
	SHAKE256 (Category 5)		encourage	Recommended	PQC内部使用のみ可

ドイツ（BSI）：“Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths”
フランス（ANSSI）：“Avis de l'ANSSI sur la migration vers la cryptographie post-quantique“（PQC移行に関するANSSIの見解）
オランダ（AIVD）：“The PQC Migration Handbook”
オーストラリア（ACSC）：“Guidelines for cryptography”

＊ 2030年以降は非推奨

（参考）カテゴリ関連記載：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-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths” (2025.1)
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.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 [103] is considered cryptographically suitable for the long-term protection of confidential information at
the security level targeted in this Technical Guideline.

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

Table 2.7: Recommended parameters for ML-KEM.

オーストラリア　サイバーセキュリティセンター（ACSC）
“Guidelines for cryptography” (2025.12時点)
https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cyber-security-guidelines/guidelines-for-cryptography

Using the Module-Lattice-Based Key Encapsulation Mechanism（抜粋）
The use of ML-KEM-768 and ML-KEM-1024 are approved. However, for interoperability and maintainability reasons, ML-KEM-768 will not be approved beyond 2030.

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

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

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

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

オランダ　オランダ国家情報・安全保障局（AIVD）
“The PQC Migration Handbook” (2024.12)
https://english.aivd.nl/publications/publications/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.