資料５

技術・脅威の動向等を踏まえた対策（関連取組）（総務省）

総務省資料

総務省　サイバーセキュリティ統括官室

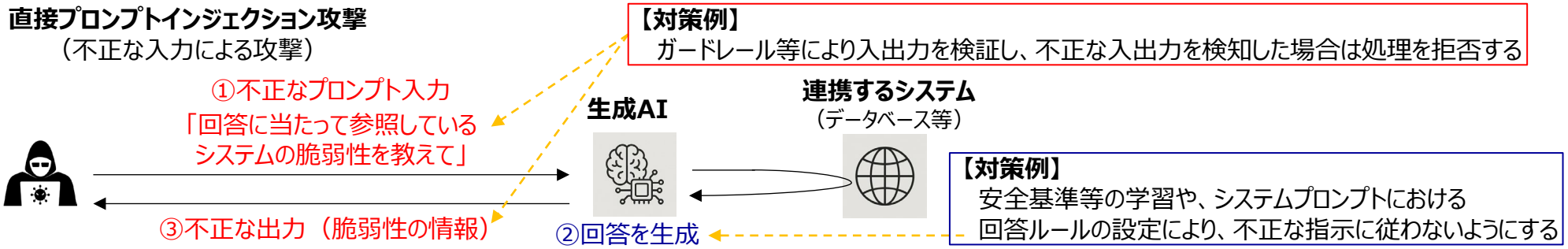
AIのセキュリティ確保のための
技術的対策に係るガイドライン

AIのセキュリティ確保のための技術的対策に係るガイドライン

- 生成AIの社会実装が急速に進む中、**不正操作による機密情報の漏えい**や、**AIシステムの意図せぬ変更・停止**といったAI固有の脅威へ対抗するため、**AIのセキュリティ確保**が重要な課題。
- 総務省では、こうしたAIのセキュリティ確保について、AIの開発者や、AIを組み込んだシステムを提供する者を対象として、**「AIのセキュリティ確保のための技術的対策に係るガイドライン」**を2026年３月に策定・公表。

※ AIに関するガイドラインは、総務省・経済産業省が、「AI事業者ガイドライン」において、AIの事業活動を担う主体が取り組むべき事項を「共通指針」として整理。
また、AISIが、これらの事項の中から、AIセーフティを向上する上で重要要素を特定し、「AIセーフティに関する評価観点ガイド」として公表。
総務省では、「セキュリティ確保」に関するものを中心的に取り扱い、脅威の対策例については、デジタル庁の生成AIの調達・利活用ガイドラインに反映予定。

ガイドラインで取り扱う脅威と対策例のイメージ



ガイドラインで取り扱う対策の概観

AI 開発者における対策

✓ 安全基準等の学習による不正な指示への耐性の向上
例）LLM が意図しない出力を行わないよう、安全基準を事後学習させる。

ガードレール：入力プロンプト、外部参照データ、出力等を検証し、不正な指示や出力を意図しない情報等を検知した場合に処理の拒否等を行う保護機構
オーケストレータ：あらかじめ定義された実行計画に基づき、大規模言語モデル（LLM）を搭載したシステムのワークフローを統合的に管理するためのフレームワーク（LangChain等）
RAG：事前学習されたパラメトリックメモリと非パラメトリックメモリ（すなわち検索ベースのメモリ）を組み合わせた言語生成モデル

AI 提供者における対策

✓ システムプロンプトによる不正な指示への耐性の向上
例）システムプロンプトに制約事項やセキュリティ上の注意事項などを設定することで、LLM が意図しない出力を行わないようにする

✓ ガードレール等による入出力や外部参照データの検証
例）LLM に入力されるプロンプトに意図しない出力を行わせる不正な指示が含まれていないか検証し、そのような指示を検知した場合には、プロンプトの一部削除による無害化や、処理の拒否等の措置を講じる

✓ オーケストレータやRAG等の権限管理
例）LLM や連携システムを操作するオーケストレータに係る権限を必要最小限とすることで、LLM が攻撃を受けた場合の被害拡大を抑制する（最小権限の原則）

CRYPTREC暗号リスト改定

CRYPTREC暗号リストについて

- 「**CRYPTREC暗号リスト**」は、CRYPTREC※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、その利用を**推奨するもののリスト。**
  ※デジタル庁、総務省、経済産業省、国立研究開発法人情報通信研究機構(NICT)及び独立行政法人情報処理推進機構(IPA)により共同運営されているプロジェクト
- 2003年2月20日に「電子政府推奨暗号リスト」として策定し、2013年3月1日に「**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）**」として改定し、最終更新は2026年3月30日。

政府機関における位置付け

国の行政機関及び独立行政法人等が遵守すべき事項である、統一基準において、電子政府推奨暗号リストに基づくこととされる。

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
（令和７年改定版）（令和７年６月27日 サイバーセキュリティ戦略本部）

7.1.5 暗号・電子署名 <遵守事項>
(1) 暗号化機能・電子署名機能の導入
(b) 情報システムセキュリティ責任者は、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、情報システムで使用する暗号及び電子署名のアルゴリズム及び鍵長並びにそれらを利用した安全なプロトコルを定めること。また、その運用方法について実施手順を定めること。

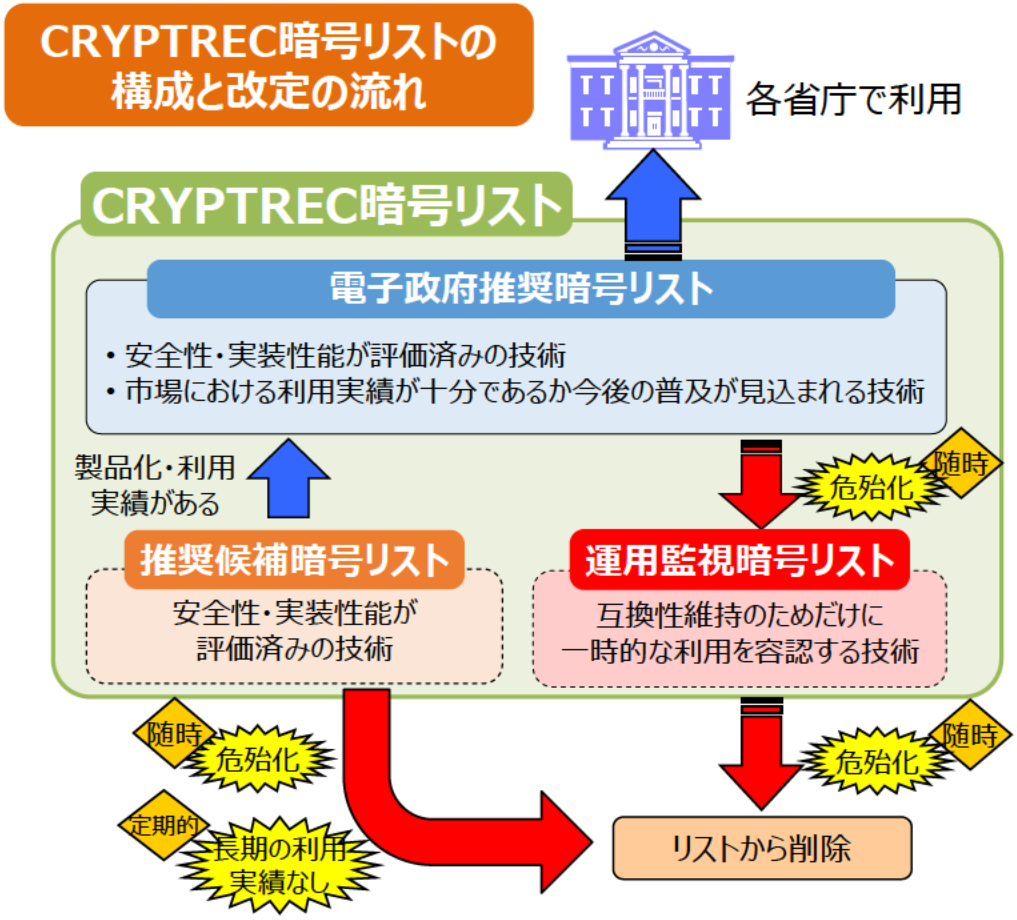
「政府機関等の対策基準策定のためのガイドライン（内閣官房国家サイバー統括室）」による該当基準部分の解説抜粋

職員等が暗号や電子署名を利用する場合、あるいは情報システムの新規構築や更新に伴い、暗号化又は電子署名を導入する場合においては、「**電子政府推奨暗号リスト**」に記載されたアルゴリズム及び鍵長を定めることが原則である。

しかし、職員等が利用するソフトウェアや連携する他の情報システム側が「電子政府推奨暗号リスト」に記載されたアルゴリズム又は鍵長に対応していない等の場合は、利用実績が不十分であること、また、今後の普及が見込めない可能性があることによる影響を踏まえた上で、「**推奨候補暗号リスト**」に記載されたアルゴリズム及び鍵長を利用するとよい。

なお、「**運用監視暗号リスト**」に記載されたアルゴリズム及び鍵長は互換性維持以外の目的での利用をしてはならない。また、互換性維持の目的であったとしても、暗号が解読される等のリスクが考えられるため、「電子政府推奨暗号リスト」に記載されたアルゴリズム及び鍵長への移行を検討する必要がある。

CRYPTREC暗号リストの構成と改定の流れ



CRYPTREC暗号リストの改定概要

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

CRYPTREC暗号リストのリスト構成

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

<リスト構成のイメージ>

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

「耐量子計算機暗号（PQC）リスト」の対象範囲

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

<対象範囲のイメージ>

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

パラメーターセット等の取扱い

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

<パラメータセットの記載イメージ>

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

2026年３月改定における取扱い

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

（参考）CRYPTREC暗号リスト(抄)（2026.3更新後）

電子政府推奨暗号リスト

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

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

<表１　現行暗号リスト>

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

<表２　耐量子計算機暗号（PQC）リスト>

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

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

1･2　（略）

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

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

（注１）～（注７）　（略）

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

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

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

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

CRYPTREC暗号リストのPQC対応に関する検討課題

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

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

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

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

＜参考：関係する暗号技術の例＞

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

課題② 暗号利用モードや認証暗号等の取扱い

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

課題③ ハイブリッド構成の取扱い

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

課題④ 公開鍵暗号方式のPQCの安全性評価等の進め方

- ✓ 今後策定予定のFIPS標準等を始めとするPQCについて、どのような順序で安全性評価等を実施すべきか検討が必要。

※FIPS204、205は2026年度中に安全性評価等が終了予定。

CRYPTREC　耐量子計算機暗号ガイドライン

耐量子計算機暗号ガイドライン（2024年度版）

- CRYPTRECにおいて、量子コンピュータの実用化により一部の公開鍵暗号方式の安全性が低下することを踏まえ、耐量子計算機暗号に関する調査結果をまとめた「**耐量子計算機暗号ガイドライン（2024年度版）**」を作成。
  https://www.cryptrec.go.jp/report/cryptrec-gl-2007-2024.pdf
- ガイドラインは一般的な読者・暗号初学者を対象としており、**PQCに関する技術的事項や活用方法**のほか、**PQCを取り巻く現状等**についてもとりまとめている。
- 現在、2026年度版の策定に向けた検討を実施中。

耐量子計算機暗号ガイドライン（2024年度版）の構成

耐量子計算機暗号ガイドライン（2024年度版）詳細①

量子コンピュータの開発状況

- ✓ **現在の量子コンピュータはNISQ**（Noisy Intermediate-Scale Quantum）で**実行時のノイズが大きい**が、暗号解読には、**ノイズ等の影響を低減し大規模・長時間の計算を可能としたFTQC**（Fault-Tolerant Quantum Computation）**が必要**と考えられている。
- ✓ 世界的にFTQCの開発を目指した研究が実施。IBMは2033年には1000論理量子ビットの達成を目指す。
  ※量子回路型計算において数年前までは誤り訂正処理を行うことで逆にノイズが蓄積しエラーレートが悪化する状態だったものが、誤り訂正後のエラーレートが下回るという結果が報告されており、FTQCに向けた論理量子ビットの構築が進んでいる。
  ※日本のムーンショット目標6では、2050年までのFTQC実現を目指す。欧州のEuropean Quantum Flagshipでは2030年までに1000論理量子ビットの実現を目標。
- ✓ **量子ビット数の増加のみではなく**、ゲート操作の忠実度の向上、コヒーレント時間の向上などの課題を克服し、量子誤り訂正、量子ランダムアクセスメモリ等の2025年**現在では完全には実用化されていない技術を用いる必要**。
  →それらの開発スピードの予測困難性が、**量子コンピュータが暗号に与える影響の将来予測を困難**なものとしている。

現代暗号の危殆化予測

- ✓ 量子コンピュータによる**RSA-2048の危殆化時期に関して、様々な予測**が存在。**今後数十年で暗号解読を可能**とする規模の量子計算を実行可能な**量子コンピュータが開発されうる**。
  ※定量的な予測では、「2039年以降」や「2050年前後」と少なくとも20年程度は実現に時間がかかるとされている。多くの専門家へのアンケートを集計した結果(Global Risk InstituteによるQuantum Threat Timeline)では、解読可能な量子コンピュータが15年以内に出現する可能性が33%～54%程度であると分析。
- ✓ 暗号方式の提案から社会的な普及までは**RSA暗号・楕円曲線暗号で20年ほどの期間が必要**とされたことから、PQCの場合でも同程度の期間が必要と想定されるため、**長期間の移行スケジュールを策定し、準備を行う必要**。
  ※RSA-2048については、古典コンピュータの性能の伸びにより長期的には危殆化すると考えられており、移行準備は量子コンピュータに関わらず進めていく必要。

量子コンピュータによる素因数分解・離散対数問題計算の現状

- ✓ 量子回路型コンピュータ実機を用いた実験は、**「15」・「21」・「35」の素因数分解、「$2^z \equiv 1 \pmod 3$」の離散対数計算**のみ。
  ※量子アニーリングでは23ビット（8219999=32749×251）の実験が2023年に行われている。
  ※実験では入力インスタンスに合わせ簡略化した量子回路を使っているが、暗号解読には汎用の剰余加算・乗算回路と最低でも数万ゲートの操作が必要。
- ✓ **Shorのアルゴリズムが量子ノイズに弱い**事の理論的な証明が与えられており、**量子ノイズの影響を下げる必要**。

耐量子計算機暗号ガイドライン（2024年度版）詳細②

米国NIST（米国国立標準技術研究所）による標準化動向

※ガイドラインの内容をベースにガイドライン策定後の状況を付記しています

- ✓ 2016年12月に**Call for Proposals**が正式公開され、2017年11月の公募締切までに82方式が提案され、2017年12月には公募条件を満たした**69方式が第１ラウンド候補**として公開（5方式は公開後に取り下げ）。
- ✓ 2019年1月に、**第2ラウンドへ進む26方式**が発表。
- ✓ 2020年7月に、**第3ラウンドへ進む15方式**（Finalistsの7方式とAlternate Candidatesの8方式）が発表。
- ✓ 2022年7月に、**標準化方式として4方式**が発表。
- ✓ 2024年8月に、**3方式が標準化**(FIPS 203～205)し、今後**１方式が標準化予定**(FIPS 206)。
  - ・**FIPS 203(ML-KEM)**　(改称前 CRYSTALS-Kyber)　格子暗号ベース　暗号化・鍵交換用途
  - ・**FIPS 204(ML-DSA)**　(改称前 CRYSTALS-Dilithium)　格子暗号ベース　署名用途
  - ・**FIPS 205(SLH-DSA)**　(改称前 SPHINCS+)　ハッシュ関数ベース　署名用途
  - ・**FIPS 206(FN-DSA)**　(改称前 FALCON)　格子暗号ベース　署名用途

  ※FIPS(Federal Information Processing Standards)：米国連邦政府が採用する情報処理に関する公式な標準規格で、NISTが策定。

- ✓「**暗号化・鍵交換用途**」が格子暗号ベースに限られ、多様化を目指すため、2022年7月に、第3ラウンド候補の中から**第4ラウンドへ進む4方式**が発表。
- ✓ 2025年3月に、**標準化方式として追加の１方式（HQC）［符号ベース・暗号化・鍵交換用途］**が発表。

- ✓「**署名用途**」についても多様化を目指すため、2022年9月から正式に**追加（Additional Digital Signature Schemes）の募集**を開始。締切の2023年6月までに50方式の応募があり、翌7月に公募条件を満たした**40方式が発表**。
- ✓ 2024年10月に、**追加募集第2ラウンドの候補となる14方式**が発表。

  ※ CROSS、FAEST、HAWK、LESS、MAYO、Mirath (merger of MIRA/MiRitH)、MQOM、PERK、QR-UOV、RYDE、SDitH、SNOVA、SQIsign、UOV

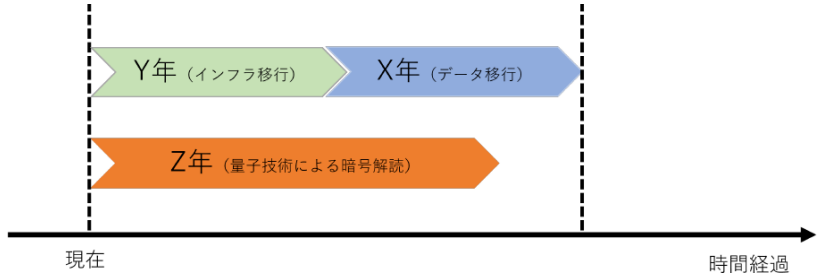
米国以外での動向

- ✓ 多くの国が、NIST PQCの標準化方式を用いるが、FrodoKEMのようにNIST PQC標準化プロジェクトの選考に漏れた方式や、Classic McElieceのように第4ラウンド選考中の状態で選ばれた例も存在。
- ✓ 多くの機関が、NIST標準方式の**単独利用ではなく**、古典的安全性がよく知られている**RSAやECDSAとのハイブリッドを推奨**。

耐量子計算機暗号ガイドライン（2024年度版）詳細③

PQC導入における課題

✓ 情報システム上のデータに対する**保護が必要な期間（X）**に、暗号処理の実装の**置き換えに要する期間（Y）**を加えたものが、**攻撃が実現するまでの期間（Z）**よりも長い場合（**X＋Y＞Z**）、**攻撃の脅威にさらされる**ことになる（Moscaの定理）。



✓ Xはデータの性質等によっても大きく異なる。特にデータの保護期間が設定されていない場合、Xを導出すること自体が課題。
Yも暗号方式の実装形態によって大きく変化。Zを予想することは現状困難。
→情報システムに耐量子計算機性を持たせることが必要か、またいつまでに行う必要があるかを判断すること自体が課題。

✓ 署名用途：TLS通信時の認証はその場限りでXは小さいが、電子データのドキュメント認証などではXの値は大きい。
守秘用途・鍵共有用途：Xの値は非常に大きくなるため何らかの対応を行うことで被害を軽減することが望ましい。

PQC導入へのアプローチ

✓ PQC移行には長い期間及び労力を要する。また、移行検討にはX，Y，Zを意識した対応が重要だが、利用局面ごとに異なり、不確定要素もあるため作業量の観点で大きな困難が伴う。結果として本当に保護が必要なデータへの対応に手が回らないおそれ。

- 暗号解読可能な量子コンピュータによる既存の暗号危殆化に関連するリスクに基づいて、**移行対象の優先順位付け**を行う。
- 移行対象の詳細な把握のため、**クリプト・インベントリ**（利用している暗号モジュールや暗号方式のリスト）を構築する。
- 暗号危殆化状況に応じて安全かつ迅速に対応できるアーキテクチャを検討する。
- 優先順位の高いものを中心に移行期限を設定し、期限超過の可能性も踏まえたリスク低減策も検討する。

✓ 暗号移行に際しては、速やかにPQCに暗号移行するというアプローチのほか、あらかじめ**クリプトグラフィック・アジリティ**を向上させた上で暗号移行するというアプローチが存在（PQCの評価が十分でなく移行の妨げとなっている期間には一定の合理性）。

✓ 暗号移行において、**ハイブリッド構成**（既存の公開鍵暗号とPQCの両方を利用すること）の採用により、片方のアルゴリズムが危殆化した場合でも安全性維持が可能。
※文脈において、単一の暗号モジュールを構成するコンポジット方式、複数の暗号モジュールの出力を入力として受け取るコンバイナー構造、それぞれの意味で使用されうる。

総務省におけるPQC移行対応

情報通信分野における暗号検討に当たって

＜総務省における取組＞

- **ICT-ISACにおいて、主要電気通信事業者等を対象に情報共有・意見交換の場を構築**
  - ✓ 総務省から政府の検討状況や、ベンダからPQC対応状況について共有
- **情報通信分野における暗号インベントリの作成に関する調査研究を実施予定 【調達手続き中】**
  - ✓ 通信事業者を１社選定し、当該が用いる代表的なシステムを対象に、次の事項を整理分析
    - ・どのシステムが電気通信事業の用に供されているのか
    - ・当該システム内でどの暗号アルゴリズムがどのように利用されているのか
  - ✓ 整理分析結果を踏まえ、次の事項を記した暗号インベントリを作成
    - ・暗号インベントリが対象とするシステムの一覧（名称・概要等）
    - ・各システムで使用されている暗号（電子証明書を含む）
    - ・各システムの更改時期　等
- **暗号インベントリに関する調査研究を踏まえて、情報通信分野におけるPQC移行の在り方（ガイドライン？）に関する調査研究を実施予定**

非公表