暗号技術検討会
２０２５年度　報告書

２０２６年３月

目次

１．はじめに

情報通信技術の急速な発展により、自動車、家電、医療、農業、工場等の様々な分野で、あらゆるモノがネットワークにつながるIoT社会が到来し、サイバー空間と実空間の高度な融合により、多様なニーズにきめ細やかに対応したモノやサービスを提供できる社会への産業構造の変化が進みつつある。一方で、IoT機器の普及に伴うサイバー攻撃の起点の増加や、サイバー攻撃自体の巧妙化・複雑化が続く中で、その影響が実空間にまで到達するリスクも高まっている。このような産業構造、社会の変化に伴うサイバー攻撃の脅威の増大に対応したセキュリティ確保が求められる中、暗号技術は既に様々な製品やサービスに組み込まれ、セキュリティを支える基盤技術として欠かせないものであり、IoT機器から得られる大量のデータの流通・連携を支える観点からも、その重要性は一層高まっている。

さらに近年は、量子計算機技術の進展に伴い、現在広く利用されている公開鍵暗号の安全性が低下することが懸念され、量子計算機への耐性を有する「耐量子計算機暗号（PQC）」への移行も急を要する課題となっている。米国では2024年８月に３方式の耐量子計算機暗号（PQC）が標準化され、実際にベンダー等での対応も広がってきているほか、我が国政府においても、原則として、2035年を目途に耐量子計算機暗号（PQC）へ移行する方針を昨年11月に発表するなど、耐量子計算機暗号（PQC）への移行に向けた関心が高まっている。

こうした中で、電子政府推奨暗号等の安全性を評価・監視し、暗号技術の更なる普及促進を行うCRYPTRECにおいても、耐量子計算機暗号（PQC）への対応が喫緊の課題であると認識している。そのため今年度は、暗号技術評価委員会において耐量子計算機暗号（PQC）の安全性・実装性能評価を行うとともに、暗号技術活用委員会において耐量子計算機暗号（PQC）に対応したCRYPTREC暗号リストの在り方について検討を行い、これらの結果を踏まえて暗号技術検討会においてCRYPTREC暗号リストを耐量子計算機暗号（PQC）に対応するための審議を行うなど、CRYPTRECのプロジェクト全体として耐量子計算機暗号（PQC）への対応に向けて精力的に活動を行った。

このほか、各委員会においては、暗号技術評価委員会では耐量子計算機暗号（PQC）に関する調査報告書とガイドラインの2026年度の作成に向けて調査を実施するとともに、「素因数分解の困難性に関する計算量評価」及び「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図を更新した。暗号技術活用委員会では、クラウドにおける鍵管理ガイダンスの検討を行った。これらの2025年度の活動の詳細については、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が取りまとめる「CRYPTREC Report 2025」を参照いただきたい。

今後も暗号技術を用いた情報システム及び情報社会全体のセキュリティ確保のために、成果物の検討や情報発信等を行っていく所存である。

末筆ではあるが、暗号技術検討会及び関係委員会等に御協力いただいた構成員、オブザーバの方々をはじめ、関係者の皆様に心から謝意を表する次第である。

2026年３月

暗号技術検討会
座長　松本　勉

２．暗号技術検討会開催の背景及び開催状況

２．１．暗号技術検討会開催の背景

暗号技術は情報セキュリティの基盤技術であり、その安全性（セキュリティ）を暗号技術の専門家により技術的・専門的な見地から客観的に評価することが重要である。電子政府のセキュリティ確保のためには、安全性に優れた暗号技術を利用することが不可欠である。

このため、総務省及び経済産業省は、客観的な評価により安全性及び実装性に優れると判断される暗号技術をリスト化し、各府省に対してその利用を推奨することにより、高度な安全性と信頼性に支えられ、国民が安心して利用できる電子政府の構築に貢献することを目指し、2001年５月に最初の暗号技術検討会を開催した。

その後、2021年のデジタル庁発足に伴いデジタル庁が加わり、デジタル庁、総務省及び経済産業省は、電子政府推奨暗号等の安全性を評価・監視し、暗号技術の更なる普及促進を行うため、継続的に暗号技術検討会を開催している。

暗号技術検討会での検討を経て、2003年２月に策定された電子政府推奨暗号リストは、2013年３月にCRYPTREC暗号リストとして改定され、2023年３月に再改定（最終更新は2026年３月）された。

２．２．CRYPTRECの体制

CRYPTRECとは、Cryptography Research and Evaluation Committeesの略であり、デジタル庁、総務省及び経済産業省が共同で開催する暗号技術検討会（座長：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）と、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）が共同で開催する委員会から構成される暗号技術評価プロジェクトをいう。

委員会は、暗号技術評価委員会及び暗号技術活用委員会から構成され、それぞれ2025年度は「暗号技術調査WG（耐量子計算機暗号）」及び「クラウド鍵管理ガイダンスWG」を設置して検討を行った。

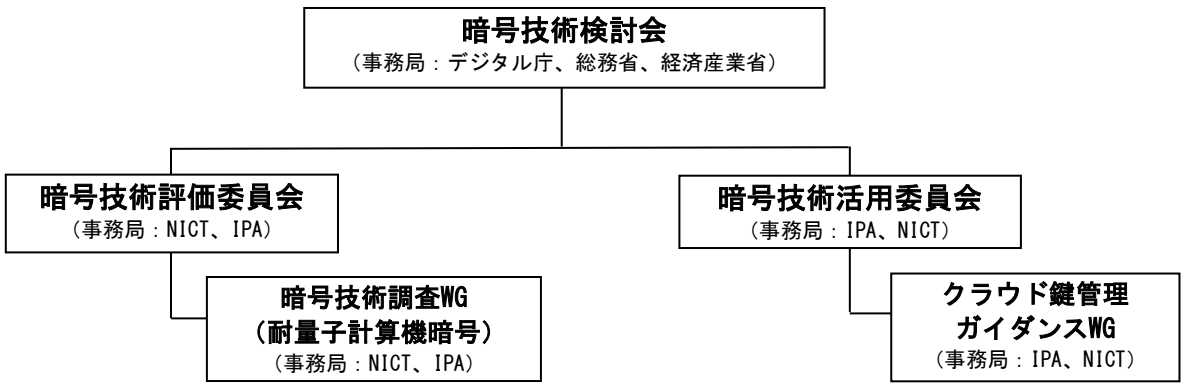

図2.2-1　CRYPTREC体制図（2025年度）

２．３．暗号技術検討会の開催実績

2025年度は、暗号技術検討会を１回開催し、各委員会の活動内容について報告・承認等を行うとともに、耐量子計算機暗号（PQC）に対応するためのCRYPTREC暗号リストの更新に関する審議等を行った。詳細は以下のとおり。

【第１回】2026年３月25日（水）9:00～11:00

○ 暗号技術評価委員会の2025年度の活動についてNICTから報告が行われた。
○ CRYPTREC暗号リスト仕様書の参照先変更、並びに「耐量子計算機暗号ML-KEMの安全性・実装性能に関する評価及び調査」及び「耐量子計算機暗号の移行に関する技術動向調査」に関する外部評価報告書について、特段の質疑はなく、原案のとおり承認された。
○ 暗号技術活用委員会の2025年度の活動についてIPAから報告が行われた。
○ 政府機関等における耐量子計算機暗号（PQC）への移行について、国家サイバー統括室（NCO）から報告が行われた。
○ 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審議が行われ、修正意見については座長一任とした上で、CRYPTREC暗号リストの改定について了承された。また、CRYPTREC暗号リストの耐量子計算機暗号（PQC）対応に関する課題等の整理を行うため、「耐量子計算機暗号（PQC）タスクフォース」を設置することについて審議が行われ、タスクフォースの詳細については座長に一任した上で、タスクフォースの設置について了承された。いずれも詳細は次節のとおり。
○ 暗号技術評価委員会における2026年度の活動計画案について、特段の質疑はなく、原案のとおり承認された。
○ 暗号技術活用委員会における2026年度の活動計画案について、質疑があり、意見の取扱いについては座長に一任とした上で、活動計画案が承認された。
○ 本報告書について、検討会における議論の反映等について座長に一任した上で承認された。

２．４．CRYPTREC暗号リストの改定

２．４．１．CRYPTREC暗号リストの改定経緯

量子計算機技術の進展に伴い、現在広く利用されている公開鍵暗号の安全性低下（危殆化）や、解読可能となることを見越してデータを保存する攻撃（Harvest Now, Decrypt Later攻撃）が懸念されており、政府機関等における耐量子計算機暗号（PQC）への移行は急を要する課題である。

このため、内閣官房及びCRYPTREC事務局であるデジタル庁、総務省、経済産業省等の関係府省庁により、2025年６月に「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」が設置された。同年11月に中間取りまとめが行われ、政府機関等の情報システムについては、原則として、2035年を目途に耐量子計算機暗号（PQC）へ移行することとされた。

政府で利用可能な暗号は、CRYPTREC暗号リストに定められており[1]、CRYPTRECにおいても耐量子計算機暗号（PQC）への対応を速やかに進める必要があることから、暗号技術評価委員会では耐量子計算機暗号（PQC）の安全性・実装性能に関する評価を実施するとともに、暗号技術活用委員会では耐量子計算機暗号（PQC）に対応したCRYPTREC暗号リストの在り方について検討を行った。

CRYPTREC暗号リストの在り方については、論点が多岐にわたったことから、暗号技術活用委員会での検討を踏まえ、事務局、NICT、IPA等が連携して、論点やその考え方について整理した。当該整理については、暗号技術活用委員会及び暗号技術評価委員会での議論を経て、暗号技術検討会において審議された。審議結果を踏まえた修正を行った上で、2026年３月30日にCRYPTREC暗号リストの更新が行われ、CRYPTREC暗号リストの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」が新たに追加された（２．４．２参照）。

なお、CRYPTREC暗号リストにおける耐量子計算機暗号（PQC）への対応に当たっては、引き続き検討すべき課題（２．４．３参照）もあり、当該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るため、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」を立ち上げ、検討を行うこととした。

なお、「耐量子計算機暗号（PQC）」という用語には、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技術（例えばFIPS 203（ML-KEM）等）を指す場合と、量子計算機への耐性を有する暗号技術を指す場合の双方の意味で用いられるため留意を要する。例えば、「耐量子計算機暗号（PQC）への移行」という文脈においては、主に後者の意味として、共通鍵暗号の強度向上（例：AES-128→AES-256）も含むものとして用いられる。

[1] 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群において規定。

２．４．２．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）への対応に関する改定概要は次のとおり。

まず、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」とした上で、新たに「表２　耐量子計算機暗号（PQC）リスト」を作成した。これは、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おり、位置付けを同じとすることで関連文書への影響も少なく理解もしやすくなると考えられるためである。また、耐量子計算機暗号（PQC）への移行完了後においても、３リスト[2]構成自体は変更する必要がなく、長期的な観点からも理解しやすいためである。

この新しい「表２　耐量子計算機暗号（PQC）リスト」について、標準化等が行われている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を持つものはリストに掲載することとした。これは、耐量子計算機暗号（PQC）への移行にあたっては、暗号技術がCRQC[3]への耐性を有するか否かの判別が一般にわかりにくいため、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ためである。

耐量子計算機暗号（PQC）については、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[4]についてもリストに掲載することとし、合わせて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掲載することとした。これは、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であるためである。

こうしたCRYPTREC暗号リストの改定に際しての考え方については、暗号技術検討会資料（CRYPTREC MT-1011-2025）の資料６－１及び資料６－２を参照されたい。

なお、暗号技術検討会での議論を踏まえて修正が行われている。まず、カテゴリの定義を明確にするための注釈を追記した。また、512ビットのハッシュ関数（SHA-512及びSHA3-512）について、カテゴリの定義に照らして明示的にCategory 5であるとは言えないことから、「(Category 5)」の記載を削った。さらに、SHAKE256について、注釈等の扱いを精査する必要があることから、今回のCRYPTREC暗号リストの更新においては掲載を保留した。

[2] 「電子政府推奨暗号リスト」、「推奨候補暗号リスト」及び「運用監視暗号リスト」

[3] 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。

[4] 例えばFIPS 203であるML-KEMにおいては、ML-KEM-512 (Category 1)／ML-KEM-768 (Category 3)／ML-KEM-1024 (Category 5)の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）。

２．４．３．更なる検討が必要な課題

CRYPTREC暗号リストの耐量子計算機暗号（PQC）対応に関して、更なる検討が必要な課題は次のとおりである。

１つめの課題は、Category 1・2である128ビットセキュリティ程度相当の暗号の取扱いである。暗号強度要件では、128ビットセキュリティは2040年までの利用とされており、一方で政府システムの耐量子計算機暗号（PQC）への移行は原則2035年とされていることから、「電子政府推奨暗号」にこれらの暗号技術を掲載することについて検討が必要である。今回の改定でも、Category 1・2の掲載は保留している。また、カテゴリの定義に関連し、512ビットのハッシュ関数の取扱いについても検討を行う。

２つめの課題は、掲載暗号利用モード、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（Camellia、KCipher-2）とハッシュ関数（SHAKE-256）の取扱いである。今回の改定では、CRQCへの耐性がCRYPTRECの外部評価報告書等から明らかなAES、SHA2、SHA3についてのみ掲載しており、これら以外の暗号技術の取扱いについて検討が必要である。

３つめの課題は、現行暗号とPQCを組み合わせたハイブリッド構成の取扱いである。

４つめの課題は、今後策定予定のFIPS標準や、FIPS標準以外の量子計算機暗号（PQC）の安全性評価等の進め方である。安全性評価等について、FIPS 204及びFIPS 205の終了後における実施順序について検討が必要である。

これらの課題については、「耐量子計算機暗号（PQC）リスト検討タスクフォース」において検討を進めることとしている。

３．各委員会の活動報告

３．１．暗号技術評価委員会

３．１．１．活動の概要

暗号技術評価委員会は、CRYPTREC暗号リストに掲載されている暗号技術や電子政府システム等で利用される暗号技術の安全性維持及び信頼性確保のために安全性及び実装に係る監視及び評価を行う。主要な検討課題は以下のとおりである。

- ○ 暗号技術の安全性及び実装に係る監視及び評価
- ○ 暗号技術の電子政府推奨暗号リストからの降格
- ○ 暗号技術に関する注意喚起レポートのCRYPTRECホームページでの公表
- ○ 推奨候補暗号リストへの新規暗号（事務局選出）の追加
- ○ 新技術暗号等に係る調査

また、CRYPTREC暗号リストとは別の文書として、「暗号技術ガイドライン（耐量子計算機暗号）2026年度版」及び「耐量子計算機暗号の研究動向調査報告書2026年度版」の作成を目指し、調査を実施した。基本方針は以下のとおりである。

- ○ 耐量子計算機暗号（PQC）に関するガイドライン（2026年度版）及び研究動向調査報告書（2026年度版）を作成するため、耐量子計算機暗号（PQC）に関するワーキンググループを2025年度も引き続き設置した。
- ○ 2025年度はガイドライン（2026年度版）及び研究動向調査報告書（2026年度版）を作成するための調査を実施した。

さらに、CRYPTREC暗号リストへの掲載に向けた耐量子計算機暗号（PQC）の技術的検討、及び耐量子計算機暗号（PQC）への移行に向けた技術的検討を実施した。基本方針は以下のとおりである。

- ○ 耐量子計算機暗号（PQC）であるML-KEMの安全性・実装性能に関する評価を外部評価により実施し、評価結果に基づき、外部評価報告書「耐量子計算機暗号ML-KEMの安全性に関する調査及び評価」及び「CRYPTREC: ML-KEM Evaluation Report」を作成した。
- ○ 耐量子計算機暗号（PQC）への移行に関する技術動向調査を外部評価により実施し、調査結果に基づき、外部評価報告書「耐量子計算機暗号への移行に関する技術動向調査」を作成した。

これらの課題について2025年度に行った具体的な検討内容を、以下のとおり報告する。

３．１．２．暗号技術の安全性及び実装に係る監視及び評価

学会等での情報収集に基づくCRYPTREC暗号等の監視活動を行った。監視報告の詳細については、CRYPTREC Report 2025（暗号技術評価委員会報告）に掲載する。

３．１．３．CRYPTREC暗号リストにおける仕様書参照先の変更

公開鍵暗号（鍵共有）であるECDHに関し、CRYPTREC暗号の仕様書一覧に掲載されている仕様書参照先を更新した。さらに、CRYPTREC暗号リストにおける注釈として「（注２）使用するMACはHMAC又はCMACに限る。」を追加した。

３．１．４．外部評価：耐量子計算機暗号ML-KEMの安全性・実装性能に関する評価及び調査

３．１．４．１．背景

2022年７月５日にNISTから耐量子計算機暗号（PQC）の標準化方式として、公開鍵暗号１方式と電子署名３方式が発表された。これら４方式のうち、格子に基づく公開鍵暗号方式であるML-KEMはFIPS 203として、格子に基づく署名方式であるML-DSAはFIPS 204として、ハッシュ関数に基づく署名方式であるSLH-DSAはFIPS 205として、それぞれ2024年８月13日に標準化された。

2024年度暗号技術検討会において、耐量子計算機暗号（PQC）への対応について議論が行われ、CRYPTREC暗号リストへの掲載に向けた耐量子計算機暗号（PQC）の技術的検討と、耐量子計算機暗号（PQC）への移行方針の検討を両輪として並行に進めていくべきであるとの合意が得られた。これに伴い、ML-KEM、ML-DSA及びSLH-DSAの安全性・実装性能の評価を先行して実施することで合意された。

2025年度第１回暗号技術評価委員会において、ML-KEMの安全性・実装性能に関する評価及び調査を実施することが承認された。

３．１．４．２．評価・実施概要

ML-KEMの安全性評価に関する１件目の外部評価を安田雅哉様（立教大学）に依頼した。選出理由と依頼内容は次のとおり。

(1) 選出理由

ML-KEMの安全性を支える数学問題とその数学問題の求解アルゴリズムにおける計算量見積に関して広い知見をお持ちである。当該分野に関する数多くの実績があるとともに、「CRYPTREC暗号技術ガイドライン（耐量子計算機暗号）」の第３章「格子に基づく暗号技術」の執筆における主担当者としての実績がある。

(2)依頼内容

耐量子計算機暗号ML-KEMの安全性について、公開されている解析手法や評価結果の有無を調査し、存在する場合はその影響範囲等についてまとめるなど、安全性評価を実施した上で報告書を作成する。

ML-KEMの安全性評価に関する２件目の外部評価に加え、実装性能評価に関する外部評価を勝又秀一様（PQShield）に依頼した。選出理由と依頼内容は次のとおり。

(1) 選出理由

勝又様は格子暗号の安全性評価やその応用先である暗号プロトコルの安全性評価に関する

広い知見をお持ちであり、当該分野に関する数多くの実績がある。また、共同執筆者に関しては、実装性能評価に関する広い知見をお持ちであり、当該分野に関する数多くの実績がある。

(2) 依頼内容

耐量子計算機暗号ML-KEMの安全性・実装性能について、公開されている解析手法や評価結果の有無を調査し、存在する場合はその影響範囲等についてまとめるなど、安全性と実装性能を評価した上で報告書を作成する。

３．１．４．３．外部評価報告書の概要：ML-KEMの安全性に関する評価及び調査

ML-KEMの安全性に関する評価結果は、以下のとおり。

(1) 安全性証明

○ 古典ランダムオラクルモデルにおいて、使用される２つのハッシュ関数がランダムオラクルと仮定した場合、タイトなIND-CCA2安全性を持つことが確認された。

○ 量子ランダムオラクルモデルにおいて、IND-CCA2安全性はノンタイトであり漸近的な保証を与えるにとどまることが確認された。しかし、耐量子性の観点で十分に高い信頼性を有する結果とみなされている。

(2) Module-LWE問題に対する計算量見積

① BKZシミュレーション[5]とdimension-for-free技術に基づく計算量見積

primal攻撃の計算量（攻撃に必要なゲートコストとメモリ量）を見積もった結果[6]、攻撃に必要なゲートコストは、ML-KEMの全てのパラメーターセットにおいてNIST安全性水準を上回っており、十分な安全性を有することが確認された（表3.1-1）。

表3.1-1. BKZシミュレーションとdimension-for-free技術に基づくprimal攻撃の計算量見積

	ML-KEM-512	ML-KEM-768	ML-KEM-1024
NIST安全性レベル	レベル1 (AES-128相当)	レベル3 (AES-192相当)	レベル5 (AES-256相当)
要求されるゲートコスト（ビット）	**143**	**207**	**272**
攻撃に必要なゲートコスト（ビット）	**151.5**	**215.1**	**287.3**
攻撃に必要なメモリ量（ビット）	93.8	138.5	189.7

② 幾何級数仮定（GSA）とMATZOV計算量モデルに基づく計算量見積

primal攻撃、dual攻撃及びhybrid攻撃の計算量を見積った結果、攻撃に必要なゲートコストは、ML-KEMの全てのパラメーターセットにおいてNIST安全性レベルの水準を下回っていることが確認された（表3.1-2）。しかし、これらの見積では計算量に影響しうる重要な性質[7]が考慮されておらず、計算量見積が過小評価されている可能性がある。これらの性質を考慮し

[5] BKZはBlock-Korkine-Zolotarevの略であり、格子基底簡約を行うBKZアルゴリズムのシミュレーターを指す。

[6] 既存研究において、dual攻撃がprimal攻撃と比較して計算コストがかかると予想されているため、ここではprimal攻撃の計算量見積のみ提供されている。

[7] 例えば、篩処理のprogressive化による格子基底の理想的な挙動からのずれ、BDGL型篩処理で発生するオーバーヘッド等がある。

た場合には、攻撃者に最も有利な状況を仮定しても、NIST安全性水準を上回ることが議論されている。

表3.1-2. 幾何級数仮定（GSA）とMATZOV計算量モデルに基づく計算量見積

	ML-KEM-512	ML-KEM-768	ML-KEM-1024
NIST安全性レベル	レベル1 (AES-128相当)	レベル3 (AES-192相当)	レベル5 (AES-256相当)
要求されるゲートコスト（ビット）	**143**	**207**	**272**
primal攻撃のゲートコスト（ビット）	**140.2**	**201.0**	**270.7**
dual攻撃のゲートコスト（ビット）	149.9	214.3	288.5
hybrid攻撃のゲートコスト（ビット）	**139.7**	**196.4**	**262.3**

(3) Module構造を考慮した攻撃

Module構造を考慮した攻撃は、現時点において、Module構造を考慮しない攻撃を上回るものではないということが確認された。

(4) 暗号強度に関する考察

① 安田様の見解

表3.1-1に示すとおり、攻撃に必要とされるゲートコストは、ML-KEMの全てのパラメーターセットにおいてNIST安全性水準を上回っており、十分な安全性を有する。さらに、最新の技術動向を踏まえても、現時点では表3.1-1の評価結果が覆る可能性は低い。

② 勝又様の見解

調査対象とした全ての攻撃クラスにおいて、ML-KEM のいずれのパラメーターセットに対しても、現実的な脅威とみなせる脆弱性は現在のところ発見されていない。さらに、具体的な計算量見積に基づく評価の結果、古典計算及び量子計算の双方について攻撃者側に極めて有利な仮定を置いた場合であっても、NIST 安全性レベルに対して十分な安全性マージンを有していると考えられる。

３．１．４．４．外部評価報告書の概要：ML-KEMの実装性能に関する評価及び調査

ML-KEMの実装性能に関する評価結果は、以下のとおり。

(1) サイドチャネル攻撃耐性

秘密鍵の復元につながるサイドチャネル攻撃の可能性が確認された。これに対する対策として、マスキング及びハイディングの適用が推奨される。

(2) ハードウェア実装性能

回路面積の最適化実装[XL21]、計算時間の最適化実装[DMG23]及びサイドチャネル攻撃対策が施された実装[Kam+22]について紹介された（表3.1-3）。

表3.1-3. ML-KEM（Kyber）のFPGA実装比較

参考文献	パラメータ	計算時間（μs）			回路面積		FPGA
		KeyGen	Encap	Decap	LUT(x1000)	FF(x1000)	
[XL21]	512	23.4	31.5	41.4	**7.4**	**4.6**	Artix-7
	768	39.2	49.2	62.4	**7.4**	**4.6**	
	1024	58.3	70.3	86.4	**7.4**	**4.6**	
[DMG23]	512	**10.0**	**14.7**	**20.5**	9.5	8.5	Artix-7
	768	**12.0**	**17.0**	**22.2**	10.5	9.8	
	1024	**16.2**	**21.7**	**26.4**	11.6	11.1	
[Kam+22] (M+H)	512	-	**88.1**	**137.7**	**163.6**	-	Virtex-7

※ M+Hはマスキング対策とハイディング対策の両方を施した実装を表す。

(3) ソフトウェア実装性能

① 計算時間

OpenSSL 3.6.0を使用して測定した結果、ML-KEMはECDHと同等以上の性能を発揮することが確認された（表3.1-4）。

表3.1-4. ECDHとML-KEMにおける計算時間の比較（ミリ秒）

鍵交換アルゴリズム		安全性レベル	KeyGen	Encap	Decap
古典	EC X25519	1†	0.027	0.058	0.029
	EC P-256	1†	0.008	0.058	0.047
	EC P-384	3†	0.088	0.327	0.229
	EC P-521	5†	0.098	0.341	0.226
量子	ML-KEM-512	1	**0.020**	**0.014**	**0.023**
	ML-KEM-768	3	**0.031**	**0.020**	**0.032**
	ML-KEM-1024	5	**0.047**	**0.028**	**0.043**
ハイブリッド	X25519 + ML-KEM-768	1† + 3	0.061	0.076	0.060
	P-256 + ML-KEM-768	1† + 3	0.044	0.076	0.076
	P-384 + ML-KEM-1024	3† + 5	0.143	0.344	0.256

※ †はECの古典安全性レベルを表しており、耐量子安全性は考慮していない。

② 帯域幅

ML-KEMとECDHの帯域幅（具体的には、鍵長と暗号文長）を比較した結果、最大で25倍の差が生じていることが確認された（表3.1-5）。なお、帯域幅の増加は対処可能であり、インターネット上でのML-KEMの使用を妨げるものではないことが実証された。

(4) 実装性能に関する考察

ML-KEMの計算時間は従来方式と比べて高速である一方、鍵長や暗号文長が増加するため、メモリ制約があるデバイス等においては実装上の課題が生じる可能性があるが、それ以外の用途においては問題なく利用できる。

サイドチャネル攻撃に対して厳密に保護されていることを前提として、政府及び重要インフラシステムへの広範な展開にも適していると考えられる。

表3.1-5. ECDHとML-KEMにおける帯域幅（鍵長と暗号文長）の比較（バイト）

鍵交換アルゴリズム		安全性レベル	カプセル化鍵	暗号文
古典	EC X25519	1†	32	32
	EC P-256	1†	65	65
	EC P-384	3†	97	97
	EC P-521	5†	123	123
量子	ML-KEM-512	1	800	768
	ML-KEM-768	3	1184	1088
	ML-KEM-1024	5	1568	1568
ハイブリッド	X25519 + ML-KEM-768	1† + 3	1216	1120
	P-256 + ML-KEM-768	1† + 3	1249	1153
	P-384 + ML-KEM-1024	3† + 5	1665	1617

※ †は古典的な安全性レベルを表しており、耐量子安全性は考慮していない。

３．１．４．５．外部評価報告書に対する暗号技術評価委員会の見解

2025年度外部評価報告書に基づき、以下の結論を得た。

- ○ ML-KEMは、全てのパラメーターセット（ML-KEM-512/768/1024）において、米国NISTが規定する安全性レベル1/3/5を満たしている。
- ○ ML-KEMは、従来方式と比較して高速である一方、鍵長及び暗号文長が増加するが、メモリ制約が厳しいデバイスを除き、実用上問題なく利用できる。
- ○ ML-KEMは、サイドチャネル攻撃対策が不十分な場合に脆弱性が生じる可能性があるものの、適切な対策の実装を前提とすれば、電子政府システムを含む多様なシステムへの広範な展開が可能である。

また、2025年度外部評価報告書は、ML-KEMの安全性・実装性能に関する技術動向調査として十分な内容を含んでいると考えられる。このため、本報告書をCRYPTRECの技術調査報告書とすることが承認された。

３．１．５．外部評価：耐量子計算機暗号の移行に関する技術動向調査

３．１．５．１．背景

2022年７月５日にNISTから耐量子計算機暗号（PQC）の標準化方式として、公開鍵暗号１方式と電子署名３方式が発表された。これら４方式のうち、格子に基づく公開鍵暗号方式ML-KEMはFIPS 203として、格子に基づく署名方式ML-DSAはFIPS 204として、ハッシュ関数に基づく署名方式SLH-DSAはFIPS 205として、それぞれ2024年８月13日に標準化された。

2024年度暗号技術検討会において、耐量子計算機暗号（PQC）への対応について議論が行われ、CRYPTREC暗号リストへの掲載に向けた耐量子計算機暗号（PQC）の技術的検討と、耐量子計算機暗号（PQC）への移行方針の検討を両輪として並行に進めていくべきであるとの合意が得られた。

2025年度第１回暗号技術評価委員会において、耐量子計算機暗号（PQC）への移行に関する技術動向調査を外部評価により実施することが承認された。

３．１．５．２．評価・調査実施概要

鈴木茜様（日立製作所）に外部評価を依頼した。選出理由と依頼内容は次のとおりである。

(1) 選出理由

暗号の2010年問題における政府認証基盤の暗号移行に関する事業に携わるほか、近年は耐量子計算機暗号（PQC）の導入に向けた政府動向や標準技術仕様の調査を実施するとともに、今後の耐量子計算機暗号（PQC）への移行に向けて認証基盤システムへの影響を検討するなど、当該分野における知識・経験が豊富である。

(2) 依頼内容

耐量子計算機暗号（PQC）への移行に関する技術動向を調査し、公開情報を基にまとめ、考察等を行い、報告書を作成する。

３．１．５．３．外部評価報告書の概要

(1) 耐量子計算機暗号（PQC）への移行時・導入時における課題

耐量子計算機暗号（PQC）への移行時及び導入時に直面する技術的課題について、用途別（署名用途／守秘用途／鍵共有用途）に整理された。

(2) 耐量子計算機暗号（PQC）導入へのアプローチ

耐量子計算機暗号（PQC）の導入に伴う全体プロセス、移行計画策定の検討事項、用途別の導入アプローチ、及び段階的な移行モデルであるハイブリッド構成の位置付けについて整理された。特に、ハイブリッド構成は、既存システムとの連続性を確保しつつ、新たな暗号方式を段階的に導入するための現実的な構成例として位置付けられていると整理された。

(3) ハイブリッド構成に関する解説

ハイブリッド構成は単一の技術要素ではなく、複数のレイヤーにまたがる設計課題を内包していることが確認された。この認識に基づき、ハイブリッド構成を目的（後方互換性の確保及び安全性の維持）と運用主体（アルゴリズム／プロトコル／システム）の各レイヤーから体系的に整理された。

(4) ハイブリッド構成の安全性に関する解説

標準化文書に記載された内容を基に、ハイブリッド構成における安全性について整理された。特に、安全性が成立するための条件と、それらの条件が実際の運用においてどのような構成要素に依存して具体化されるのかという点に着目された。

(5) ハイブリッド構成の実装・運用に関する解説

耐量子計算機暗号（PQC）及びハイブリッド構成の実装に関する主要なOSSの整備状況と、実運用環境における実装・移行事例が整理された。特に、国際会議PQC Conferenceで報告された以下の事例について紹介された。

① 実運用を想定した耐量子計算機暗号（PQC）への移行及び性能評価の事例
② Web PKIにおける段階的な耐量子計算機暗号（PQC）導入の事例
③ PKI階層設計におけるハイブリッド構成の活用事例
④ S/MIME電子メールにおけるハイブリッド構成の実装事例

(6) 耐量子計算機暗号（PQC）への移行に関わる標準化動向の調査

耐量子計算機暗号（PQC）への移行期におけるハイブリッド方式の取扱いに着目し、国際的な標準化団体及び関連組織における検討状況が整理された。

表3.1-6. 調査対象組織の一覧

No.	組織名	URL
1	NIST	https://www.nist.gov/
2	IETF	https://www.ietf.org/
3	ITU	https://www.itu.int/
4	ETSI	https://www.etsi.org/
5	IEEE	https://www.ieee.org/
6	ISO	https://www.iso.org/
7	ASC X9	https://x9.org/
8	NSA	https://www.nsa.gov/
9	CSA	https://cloudsecurityalliance.org/
10	PQCRYPTO	https://pqcrypto.eu.org/
11	PQCC	https://pqcc.org/

(7) 調査結果に関する考察

2020年度外部評価報告書「ハイブリッドモードの技術動向調査」の公開時点[8]では、ハイブリッドモードは概念レベルにとどまり、標準化活動も議論が始まったばかりの段階であった。一方、2025年以降は主要な標準化機関において本格的な標準化活動が進展しており、その動きが活発化していることが確認された。

特に、2026年１月時点では、ハイブリッド構成は主要な標準化機関において技術仕様として確立されており、TLS、X.509、VPN等の各種プロトコルやPKIに関しても、具体的な実装指針が整備されていることが確認された。

これらの具体的な整備により、ハイブリッド構成は単なる概念段階を超えて、既存プロトコル・証明書・運用基盤の中で「移行期に採用可能な実装構成」として体系的に確立されたと評価できる。

３．１．５．４．外部評価報告書に対する暗号技術評価委員会の見解

2025年度外部評価報告書は、耐量子計算機暗号（PQC）への移行に関する技術動向調査として十分な内容を含んでいると考えられる。このため、本報告書をCRYPTRECの技術調査報告書とすることが承認された。

[8] 2020年度の報告書では、ハイブリッド構成のことをハイブリッドモードと称していた。

３．１．６．暗号技術調査WG（耐量子計算機暗号）

2021年度から活動を継続している暗号技術調査WG（耐量子計算機暗号）（以下「PQC WG」という。）の活動背景と2025年度の活動報告を記述する。

３．１．６．１．活動の背景

2020年度第２回暗号技術検討会において、大規模な量子コンピューターが実用化された後でも量子攻撃に対して安全性を確保できると期待される暗号（耐量子計算機暗号（PQC））の研究開発及び標準化活動が各国で進められていることから、PQC WGを設置することが承認された。活動内容として、２年間かけて調査活動を行い、耐量子計算機暗号（PQC）に関するガイドライン・調査報告書を作成することが承認された。また、「素因数分解の困難性に関する計算量評価」及び「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の更新をWGで実施することが承認された。2023年３月に2022年度版のガイドライン及び調査報告書を公開した。

2023年度第１回暗号技術評価委員会において、耐量子計算機暗号（PQC）関連の技術開発、標準化活動が世界的に活発であることから、引き続き、PQC WGを設置することが承認された。２年間かけて耐量子計算機暗号（PQC）に関する技術動向調査を行い、耐量子計算機暗号（PQC）に関するガイドライン・調査報告書（2024年度版）を作成することが承認された。また、「素因数分解の困難性に関する計算量評価」及び「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の更新をWGで実施することが承認された。2025年３月に2024年度版のガイドライン及び調査報告書を公開した。

2025年度暗号技術評価委員会において、引き続き、PQC WGの設置及び以下の活動を行うことが承認された。

- ○ NISTにおける耐量子計算機暗号（PQC）の標準化において３件の標準化文書（FIPS 203から205まで）が公開され、今後も２件の標準化（FALCON及びHQC）、並びに追加署名の選定プロジェクトが進行中であることをはじめ、世界各国の機関において技術開発、標準化活動が引き続き活発であり、情勢が流動的であることから、2024年度版の調査報告書・ガイドラインが出版された以降の研究技術動向を2026年度末までに調査・把握し、調査報告書・ガイドラインを作成する。
- ○ 「素因数分解の困難性に関する計算量評価」及び「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の更新についても検討し、更新する。

上記活動の成果は以下のとおりであり、2025年度第２回暗号技術評価委員会にて報告され、了承された。

３．１．６．２．耐量子計算機暗号（PQC）に関する調査報告書・ガイドライン

調査報告書・ガイドライン執筆の基本的な方針は2024年度版調査報告書・ガイドラインを踏襲し、以下のとおりである。

- ○ 取り扱う耐量子計算機暗号（PQC）は2024年度版調査報告書にあるとおり「古典アルゴリズムの組み合わせにより定式化され，かつ耐量子計算機性を持つことを技術的に判断できる暗号方式」とし、特に公開鍵暗号である公開鍵暗号方式（Public-key encryption）、署名方式

（Digital signature）及び鍵共有（Key exchange）に関して調査を行う。

○ 調査対象を安全性の根拠となる計算問題に応じて分類し、格子に基づく暗号、符号に基づく暗号、多変数多項式に基づく暗号、同種写像に基づく暗号及びハッシュ関数に基づく署名に分けて調査・執筆を行う。

○ 耐量子計算機暗号（PQC）の研究成果が発表される主要な国際会議Crypto、Eurocrypt、Asiacrypt及びPQCryptoを中心に、開発・標準化（ISO, IETF, NIST, ETSI等）の動向に関しても2026年９月30日までの情報を可能な限り調査する。その他主要な動向があれば可能な限り取り上げる。

○ 調査報告書には可能な限り詳細な情報を記載し、ガイドラインでは暗号初学者を対象とし技術的な詳細を省き簡略化する。

○ 調査報告書・ガイドラインの章立ては以下を予定する。第８章が追加されるかどうかは来年度の議論とする。また、A.2、A.3の節タイトルに関しては計算問題の名称との組み合わせにより読みやすい形に各章担当者が調整することで合意された。

表3.1-7　ガイドラインの章立て

章	タイトル
１	はじめに
２	耐量子計算機暗号（PQC）の活用方法
３	格子に基づく暗号技術
４	符号に基づく暗号技術
５	多変数多項式に基づく暗号技術
６	同種写像に基づく暗号技術
７	ハッシュ関数に基づく署名技術
８	総括（追加される場合）
３章以降の構成（Ａ章の場合：Ａは３～７を表す）	
Ａ．１．	安全性の根拠となる問題（例：LWE問題、シンドローム復号問題）
Ａ．２．	暗号方式の基本設計
Ａ．３． Ａ．３．１． Ａ．３．２． Ａ．３．３． ・・・	実用的な暗号方式 暗号方式１（例：CRYSTALS-KYBER, Classic McEliece） 暗号方式２ 暗号方式３ ・・・
Ａ．４．	まとめ

３．１．６．３．「素因数分解の困難性に関する計算量評価」及び「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の更新

「素因数分解の困難性に関する計算量評価」及び「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図（以下単に「予測図」という。）は公開鍵暗号方式のセキュリティパラメータの選択について検討を行うため、2006年度に設置された暗号技術調査WG（公開鍵暗号）において作

成された。2019年度暗号技術評価委員会において、今後の予測図の取扱いについて審議し対応方針（「今後の予測図の取扱い」及び「今後の公開鍵暗号のパラメータ選択」）を決定した。2025年度において、対応方針は以下のとおりとなっている。

予測図の取扱い対応方針

＜今後の予測図の取扱い＞

(1) いわゆるムーアの法則を仮定して外挿線を年度末からプラス20年後まで従来どおり直線で引き、評価に大きな変動がないと考えられる限りにおいては、安全サイドに倒した評価として予測図を当面の間更新していく。

(2) 予測図における500位のプロットに係る削除について検討した、TOP500.Orgにおける500位のプロットは2024年度までとし、以降の外挿線を削除する。

(3) 暗号強度要件（アルゴリズム及び鍵長）に関する設定基準[9]における基本設定方針に沿ったパラメータ（利用可・移行完遂期間、2022年３月策定以降）を黄色部分で示した。

(4) セキュリティ強度が112ビットセキュリティ相当のBinary Fields及びKoblitz Curves （群位数233ビット）を追記した（図3.1-2）。

＜今後の公開鍵暗号のパラメータ選択＞

(5) 公開鍵暗号のパラメータ選択に関する対応方針については、安全性以外にも相互接続性等、運用上の観点もあるため、暗号技術評価委員会だけではなく、暗号技術検討会及び暗号技術活用委員会や関係各所等を含めて検討する。

なお、予測図は各国・国際標準化機関等により示されている主要な暗号技術の安全性基準と比較すると、より現状に則した評価であり、危殆化時期がそれらよりも先に延びるものとなっている。

予測図の更新について

素因数分解問題の困難性及び楕円曲線上の離散対数問題の困難性に関する計算量評価に大幅な進展はなかったため、TOP500.orgにおける2025年６月と11月のベンチマーク結果を追加して予測図の更新を行った（図3.1-1及び図3.1-2）。

[9] https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022r1.pdf

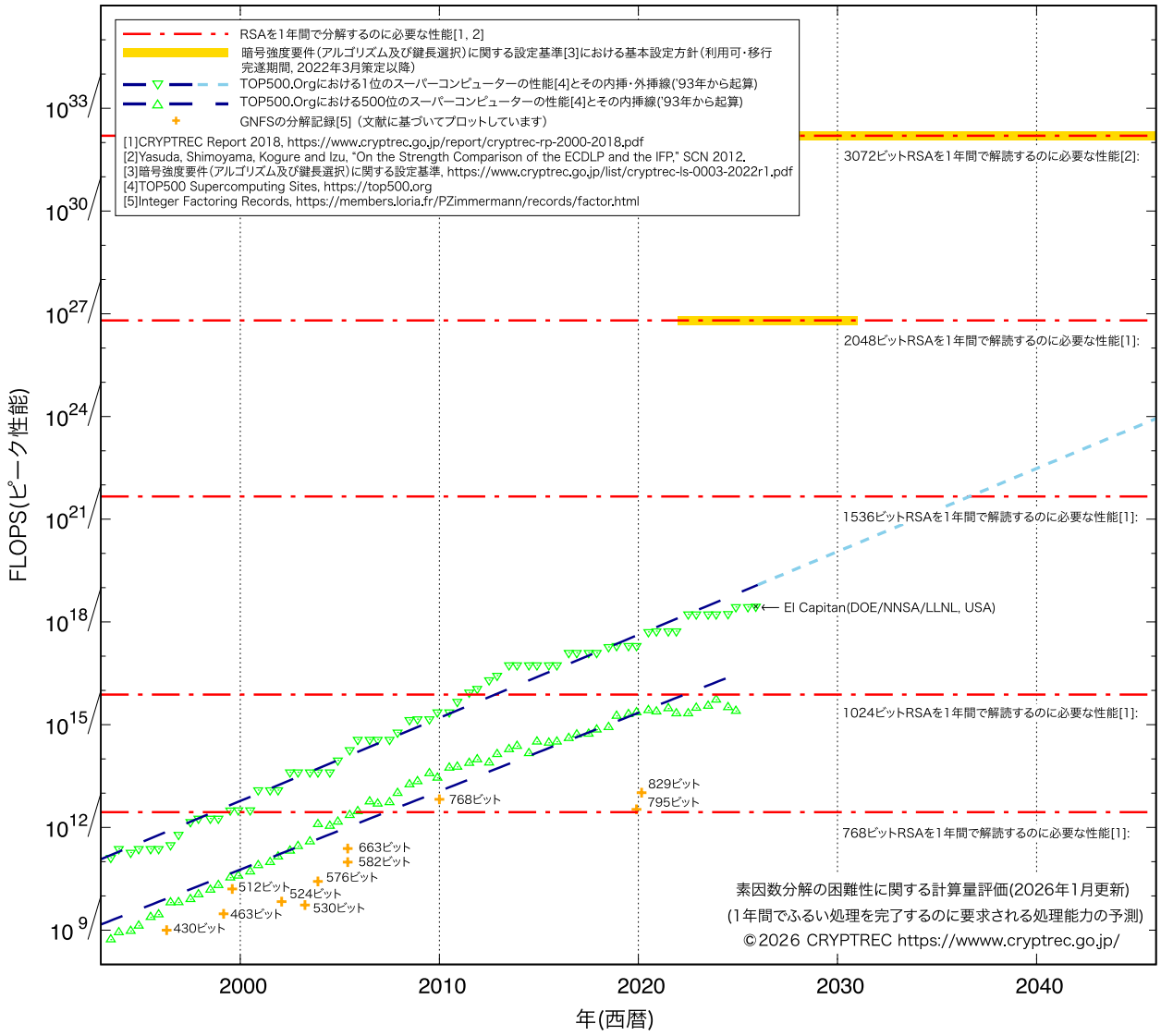

図3. 1-1：素因数分解の困難性に関する計算量評価（2026年１月更新）[10]

[10] スーパーコンピューターの性能の伸びに関する外挿線は僅かであるが鈍化してきている。

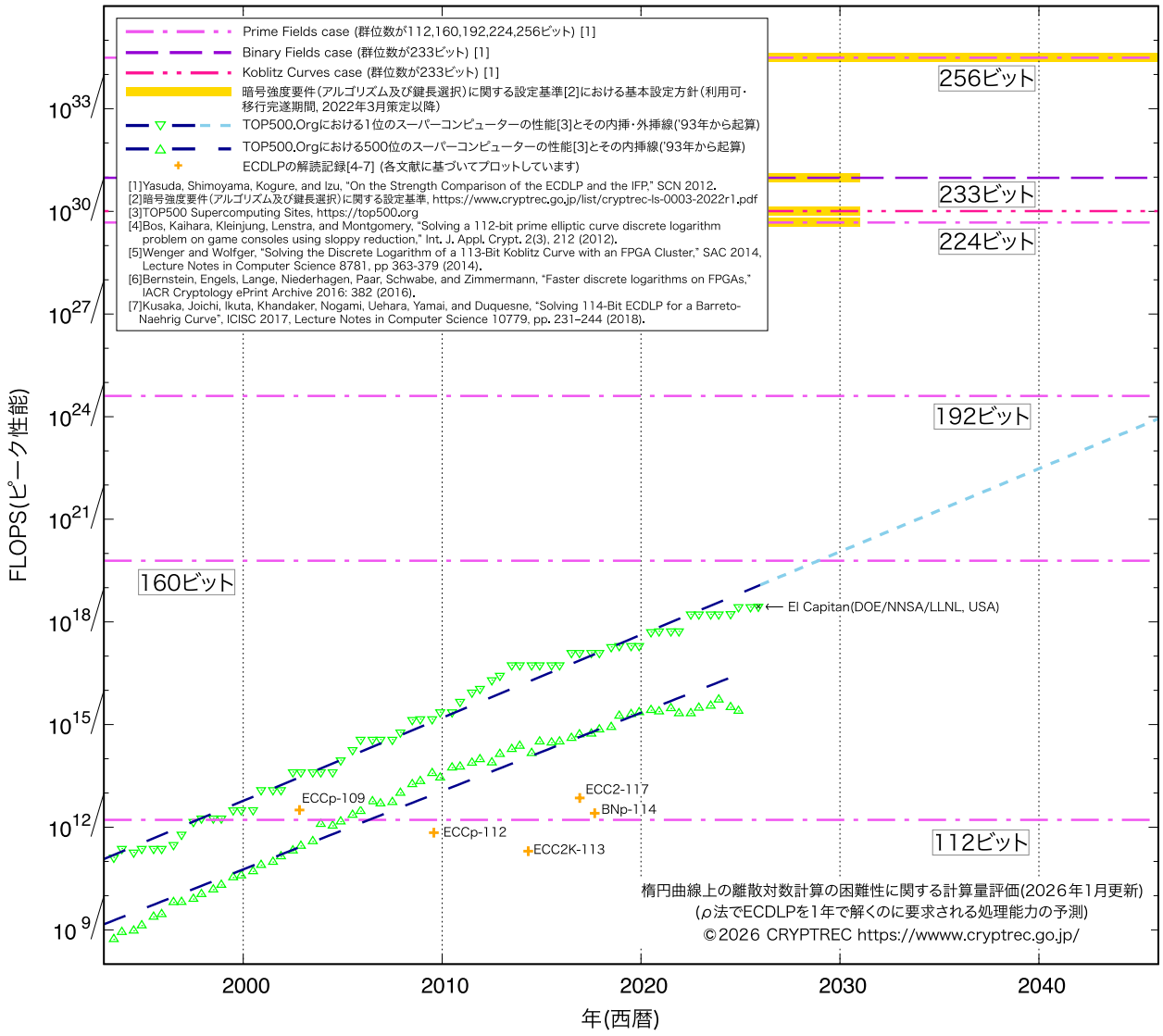

図3.1-2：楕円曲線上の離散対数計算の困難性に関する計算量評価（2026年１月更新）[11]

[11] スーパーコンピューターの性能の伸びに関する外挿線は僅かであるが鈍化してきている。

３．１．７．暗号技術評価委員会の開催実績

暗号技術評価委員会は計２回開催された。各回会合の概要は表3.1-8のとおりである。

表3.1-8　暗号技術評価委員会の開催状況

回	開催日	議案
第１回	2025年７月１日	○ 暗号技術調査 WG（耐量子計算機暗号）の活動計画案に関する審議 ○ 耐量子計算機暗号（PQC）への対応方針と 2025 年度外部評価「ML-KEM の安全性・実装性能に関する評価及び調査」及び「耐量子計算機暗号への移行に関する技術動向調査」の実施に関する審議 ○ CRYPTREC 暗号リストにおける仕様書参照先の変更に関する審議 ○ 監視状況報告
第２回	2026年３月３日	○ 暗号技術調査 WG（耐量子計算機暗号）の活動内容に関する報告 ○ メール審議「ECDH における仕様書参照先の変更」及び「外部評価スケジュールの変更と ML-DSA 外部評価の実施」に関する報告 ○ 外部評価スケジュールの再変更と SLH-DSA 外部評価の実施に関する審議 ○ 外部評価報告書「ML-KEM の安全性・実装性能に関する評価及び調査」及び「耐量子計算機暗号への移行に関する技術動向調査」に関する概要報告、並びに本外部評価に関する審議 ○ 監視状況報告 ○ 2025 年度暗号技術評価委員会活動報告案の確認 ○ 2026 年度暗号技術評価委員会活動計画案の確認 ○ CRYPTREC Report 2025 の目次案の確認

また、PQC WGは計２回開催した。2025年度のPQC WG各回の概要は表3.1-9のとおりである。

表3.1-9　PQC WGの開催状況

回	開催日	ガイドラインの議論・決定・報告
第１回	2025年８月４日	○ 追記・改定の方針について議論 ○ 執筆担当者を議論・決定
第２回	2026年１月22日	○ 追記・改定すべき項目及びその章立ての決定 ○ 調査の中間報告

３．２．暗号技術活用委員会

３．２．１．活動の概要

2025年度の活動概要は以下のとおりである。詳細については、CRYPTREC Report 2025（暗号技術活用委員会報告）を参照されたい。

(1) 耐量子計算機暗号（PQC）の取扱いに係る検討

耐量子計算機暗号（PQC）をめぐる社会的動向を踏まえ、耐量子計算機暗号（PQC）の取扱基準や位置付け・記載内容等についての検討を行った。具体的には、日本における「耐量子計算機暗号（PQC）への移行（方針）」を検討する際の素材としてもらうため、「耐量子計算機暗号（PQC）への移行（方針）」の政策的側面からの整理、及び「CRYPTREC暗号リスト」における耐量子計算機暗号（PQC）の位置付けや移行ルールを変更すべきかどうかを検討し、暗号技術活用委員会としての見解を取りまとめた。

(2) クラウドにおける鍵管理ガイダンスの作成

クラウド鍵管理ガイダンスWGを設置し、クラウドサービスを利用した情報システムにおける暗号鍵管理のガイダンス作成を開始した。2026年度末での完成に向けて、今年度はガイダンスの骨子を整理した。

(3) 「暗号鍵管理システム設計指針（基本編）」の改訂

暗号鍵管理システムの設計に関わる中心となる解説書である「暗号鍵管理システム設計指針（基本編）（以下「設計指針」という。）」の作成から約５年が経過し、記載に古い箇所がある、誤記がある等の問題が見つかったため、改訂方針を議論した。

３．２．２．耐量子計算機暗号（PQC）の取扱いに係る検討

(1) 「耐量子計算機暗号（PQC）への移行（方針）」の政策的側面からの取りまとめ

各国政府・公的機関等が発行している耐量子計算機暗号（PQC）への移行に関する政策やガイドラインの情報について時系列的観点での整理を行った。

G7での国際協調方針が打ち出されたこともあり、欧米各国とも国家安全保障システムや高セキュリティシステム等は2030年頃を、その他のシステムは2035年を耐量子計算機暗号（PQC）への移行完了時期に設定した移行方針が打ち出されている。併せて、耐量子計算機暗号（PQC）ではない従来の暗号技術、特に公開鍵暗号についての取扱いについても言及されつつあることが分かった。

これらの結果を踏まえて、2026年度は「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」の改定を進めることとする。

(2) 「CRYPTREC暗号リストでの取扱いルール」を変更すべきかどうかの検討

以下の観点を中心に耐量子計算機暗号（PQC）に対応したCRYPTREC暗号リストの在り方について議論し、暗号技術活用委員会としての見解をまとめた。また、これらの見解を踏まえつつ作成

された「耐量子計算機暗号（PQC）に対応したCRYPTREC暗号リストの在り方（案）」に対してその内容を確認し、暗号技術活用委員会としても同意した。

① 耐量子計算機暗号（PQC）リストの形式

現行の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」及び「運用監視暗号リスト」）の技術分類をそのまま使うか、「耐量子計算機暗号（PQC）」のカテゴリを追加するか、あるいは、それらのリストとは別の「量子計算機耐性を備えた暗号方式に関わる独立したリスト（耐量子計算機暗号（PQC）リスト）」を作るべきかを議論した。

その結果、現時点においては既存のCRYPTREC暗号リストに耐量子計算機暗号（PQC）を加えるのではなく、新たに量子コンピューターに耐性のある暗号のみを記載したリストを作成したほうがよいとの見解で一致した。また、新たなリストに掲載するアルゴリズムについて、量子計算機耐性を備えた公開鍵暗号だけではなく、共通鍵暗号やハッシュ関数等も含めて、量子計算機耐性を備えた暗号方式全般を含むリストとするのがよいとの見解で一致した。さらに、アルゴリズムの強度を規定するパラメータもリスト中に記載するのがよいとの意見もあった。

これは、耐量子計算機暗号（PQC）リストを参照することで量子計算機耐性を備えた一通りの暗号方式を選択可能であり、利用者にとって利便性が高いと考えられるためである。

② 移行ルール・選定ルールについての検討

「耐量子計算機暗号（PQC）リストを新たに作成すること自体はよく、そのためのルールが設けられることも理解できる。ただし、電子政府推奨暗号リストとの関係は整理すべき」との指摘があった。例えば、両リストの使い分けをどうするのか、両リストは将来的に一本化されていくのか、耐量子計算機暗号（PQC）リストと推奨暗号リストの両方に記載されるアルゴリズムはあるのか、耐量子計算機暗号（PQC）リストでも将来は監視暗号リストが必要である、などである。

これらの意見は、「耐量子計算機暗号（PQC）に対応した CRYPTREC 暗号リストの在り方（案）」を作成する際の参考としてもらうこととした。

③「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（案）」に対する意見

「耐量子計算機暗号（PQC）に対応した CRYPTREC 暗号リストの在り方（案）」に対して次のような意見があった。

- ○ 「耐量子計算機暗号（PQC）リスト」の説明文に関連して、例えば、現行の電子政府推奨暗号リストにのみ掲載されている方式について、いずれ耐量子計算機暗号（PQC）リストにも掲載される可能性があるのか、あるいは耐量子計算機暗号（PQC）リストには掲載されない方式であるのかが明確でない等の課題があるため、誤解が生じないような工夫がいる。
- ○ 耐量子計算機暗号（PQC）リストは、プリミティブとなるアルゴリズムだけの記載とするのがよい。ハイブリッド構成を含めると暗号リストとして複雑になることが予想され、ハイブリッド構成に関しては、例えばTLS暗号設定ガイドラインのようなプロトコルやアプリケーションを対象に作成するガイドラインの中で対応するのがよいのではないか。

３．２．３．クラウドにおける鍵管理ガイダンス

今年度はクラウド鍵管理ガイダンスの骨子となる資料を作成した。ここでは、ガイダンスの骨格となる目次構成を中心にまとめる。

クラウド鍵管理ガイダンスの目次案は以下のとおりである。

１．はじめに
２．基礎知識
３．クラウド鍵管理サービスについて
４．クラウド鍵管理サービスに関わる責任分界
５．暗号鍵管理システムのフレームワーク要求からの整理
６．その他
Appendix. 参考資料

１章ではイントロダクションとして、本ガイダンスの位置付けや想定読者、スコープをまとめる。２章では、クラウド鍵管理に関わる基礎技術や政府システムにおけるクラウドサービス利用時の要件等の基礎知識をまとめる。３章では、クラウドサービスプロバイダ（CSP）が提供するクラウド鍵管理サービスを体系化し、比較する。４章では、クラウド鍵管理サービスにおけるCSPと利用者の責任分界の原則を説明する。５章では、NIST SP 800-130を基に鍵管理における管理策を抽出した管理策一覧表を示し、この管理策一覧表を利用してクラウド鍵管理サービス利用時の責任分界を整理した例を説明する。さらに、利用者側に実施責任がある事項における注意点について、より詳細に説明する。６章では、本ガイダンスで取り上げていない周辺事項に触れる。

３．２．４．「暗号鍵管理システム設計指針（基本編）」の改訂

2020年に発行した「暗号鍵管理システム設計指針（基本編）」の修正について検討した。検討の背景は、2023年度から2024年度までに実施した「暗号鍵管理ガイダンスPart 2」の作成過程で、同ガイダンスの親文書に相当する「設計指針」に対する修正の意見があったことである。「設計指針」の執筆から約５年が経過し、記載内容の最新化や明確化を行うのが適当な箇所や誤記も多数見つかったため、修正すべき箇所と修正方針、修正案を議論した。結果として、「設計指針v1.1」として改訂を行う方針とした。

３．２．５．暗号技術活用委員会の開催状況

2025年度の暗号技術活用委員会での審議概要は表3.2-1のとおりである。

表3.2-1　暗号技術活用委員会の開催状況

回	開催日	議案
第１回	2025年７月18日	○ 2025 年度暗号技術活用委員会活動計画の確認 ○ 2025 年度クラウド鍵管理ガイダンス WG 活動計画の審議 ○ 耐量子計算機暗号（PQC）の取扱いに関する検討 ○「暗号鍵管理システム設計指針（基本編）」の修正について
第２回	2026年２月24日	○ 耐量子計算機暗号（PQC）の取扱いに関する検討 ○ 2025 年度クラウド鍵管理ガイダンス WG 活動状況及び WG 活動報告の審議 ○ 「暗号鍵管理システム設計指針（基本編）」の修正案の審議 ○ 2025 年度暗号技術活用委員会活動報告案について

４．2026年度のCRYPTRECの活動について

CRYPTRECでは、2026年度も、電子政府推奨暗号等の安全性を評価・監視するとともに、暗号技術の更なる普及促進を行うべく検討を進める。

暗号技術検討会においては、「耐量子計算機暗号（PQC）リスト検討タスクフォース」を設置し、CRYPTREC暗号リストにおける耐量子計算機暗号（PQC）への対応に関する課題等の整理を行う。

例年、暗号技術検討会は年度末に開催していたが、同タスクフォースにおける検討状況や暗号技術評価委員会におけるFIPS 204（ML-DSA）及びFIPS 205（SLH-DSA）に係る安全性・実装性能に関する調査及び評価の状況を踏まえながら、CRYPTREC暗号リストの速やかな改定に必要があれば、年度途中の開催も含めて開催することとする。

暗号技術評価委員会においては、「暗号技術調査WG（耐量子計算機暗号）」において、耐量子計算機暗号（PQC）に関する技術動向を継続して調査・把握するとともに、ガイドライン及び調査報告書を作成する。また、「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の更新についても同WGで検討し、更新を行う。また、CRYPTREC暗号リスト掲載に向けた耐量子計算機暗号（PQC）の技術的検討に資するための外部評価を実施する。具体的には、FIPS 204（ML-DSA）及びFIPS 205（SLH-DSA）の暗号技術について、安全性・実装性能に関する調査及び評価を行う。

暗号技術活用委員会においては、「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」について、耐量子計算機暗号（PQC）の取扱いを含めた形での見直しを実施するとともに、「TLS暗号設定ガイドライン」について耐量子計算機暗号（PQC）のサポートに向けたTLS1.3への移行や電子証明書の有効期限の短縮化等に対応するため、2027年度の見直しに向けた検討を実施する。また、「クラウド鍵管理ガイダンスWG」において、クラウドサービスを利用したシステムにおける暗号鍵管理の適切な設計・構築・運用のために、クラウド鍵管理ガイダンスを作成する。

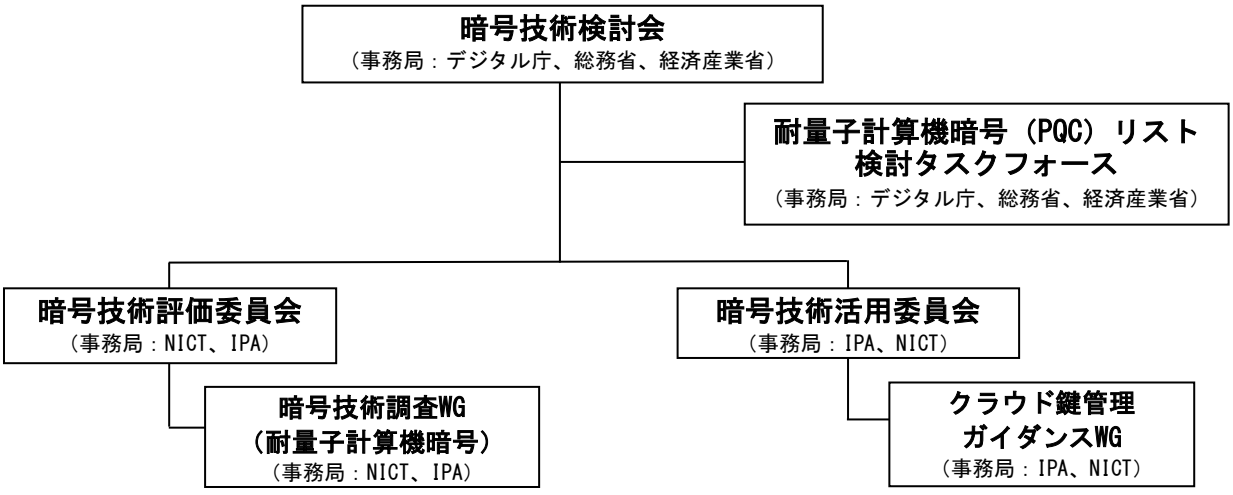

図4-1 CRYPTREC体制図（2026年度）（予定）