2025年度　第１回暗号技術検討会　議事概要

１．日時

令和８年３月25日（水）　9:00～11:00

２．場所

経済産業省本館17階第２特別会議室及びオンライン開催

３．出席者（敬称略）

構成員：松本勉（座長)、阿部正幸、石井義則、上原哲太郎、國廣昇、黒田真弓、島岡政基、
高木剛、田村裕子、本間尚文、松井充、松浦幹太、松本泰、吉田博隆、渡邊創

オブザーバー：

内閣官房 国家サイバー統括室 内閣参事官
個人情報保護委員会事務局 参事官
警察庁 長官官房 技術企画課 情報セキュリティ対策室長
総務省 自治行政局 住民制度課長（代理出席）
総務省 自治行政局 住民制度課 マイナンバー制度支援室長（代理出席）
法務省 民事局 商事課長（代理出席）
外務省 大臣官房 情報システム総括課長（代理出席）
財務省 大臣官房 文書課 業務企画室長
厚生労働省 大臣官房参事官（サイバーセキュリティ・情報システム管理担当）（代理出席）
経済産業省 イノベーション・環境局 国際電気標準課長（代理出席）
防衛省 整備計画局 サイバー整備課 AI・サイバーセキュリティ政策調整官
国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所長
国立研究開発法人産業技術総合研究所 サイバーフィジカルセキュリティ研究部門 首席研究員
独立行政法人情報処理推進機構 セキュリティセンター長（代理出席）
一般財団法人日本情報経済社会推進協会 デジタルトラスト評価センター 副センター長
公益財団法人金融情報システムセンター 監査安全部長

事務局：デジタル庁デジタル社会共通機能グループ

総務省サイバーセキュリティ統括官室
経済産業省商務情報政策局サイバーセキュリティ課
暗号技術評価委員会事務局
暗号技術活用委員会事務局

４．議事

(1)　2025年度暗号技術評価委員会 活動報告【報告】
(2)　CRYPTREC暗号リストにおける仕様書参照先の変更【承認】
(3)　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（案）【承認】
(4)　外部評価：耐量子計算機暗号への移行に関する技術動向調査（案）【承認】
(5)　2025年度暗号技術活用委員会 活動報告【報告】
(6)　政府機関等における耐量子計算機暗号（PQC）への移行【報告】
(7)　CRYPTREC暗号リストの改定 ～耐量子計算機暗号（PQC）対応～【審議】
(8)　「耐量子計算機暗号（PQC）タスクフォース」の設置【審議】
(9)　2026年度暗号技術評価委員会 活動計画(案)【承認】
(10) 2026年度暗号技術活用委員会 活動計画(案)【承認】
(11) 暗号技術検討会 2025年度 報告書（案）【承認】
(12) その他

５．配付資料

資料１　　議事次第・配付資料一覧
資料２　　暗号技術検討会 開催要綱（構成員・オブザーバ名簿）
資料３－１　2025年度 暗号技術評価委員会 活動報告
資料３－２　CRYPTREC暗号リストにおける仕様書参照先の変更（案）
資料３－３　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（案）
資料３－４　耐量子計算機暗号への移行に関する技術動向調査（案）
資料４　　2025年度 暗号技術活用委員会 活動報告
資料５　　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
資料６－１　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
資料６－２　CRYPTREC暗号リスト（案）
資料７　　「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（案）
資料８　　2026年度 暗号技術評価委員会 活動計画（案）
資料９　　2026年度 暗号技術活用委員会 活動計画（案）
資料10　　暗号技術検討会 2025年度 報告書（案）

６．議事概要

６．１．開会

経済産業省奥家大臣官房審議官（商務情報政策局担当）及びデジタル庁楠デジタル社会共通機能グループ長より開会の挨拶が行われた。

６．２．議事

(1) 2025年度暗号技術評価委員会 活動報告【報告】

資料３－１について暗号技術評価委員会事務局から説明が行われ、特段の質疑はなかった。

(2) CRYPTREC暗号リストにおける仕様書参照先の変更【承認】

(3) 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（案）【承認】

(4) 外部評価：耐量子計算機暗号への移行に関する技術動向調査（案）【承認】

資料３－２から資料３－４までについて暗号技術評価委員会事務局から説明が行われ、特段の質疑もなく、いずれも原案のとおり承認された。

(5) 2025年度暗号技術活用委員会 活動報告【報告】

資料４について暗号技術活用委員会事務局から説明が行われ、特段の質疑はなかった。

(6) 政府機関等における耐量子計算機暗号（PQC）への移行【報告】

資料５について内閣官房国家サイバー統括室から説明が行われた。主な質疑内容は以下のとおり。

（松本座長）「移行」という言葉は、耐量子計算機暗号を使い始めるという意味なのか、それとも耐量子計算機暗号に置き換わるという意味なのか。

（内閣官房）2035年の段階で、原則としてという言葉は付きつつも、PQCを使い始めていただくことは必要と考えている。一方、現行暗号の利用については、今後の技術進展を踏まえて決まっていくものと考えている。

（松浦構成員）最初のページで安全保障がエンファサイズされていたが、経済安全保障という言葉が入っていないのは何か意図があるか。

（内閣官房）「経済」を除くような特段の意図はなく、経済安全保障も含んでいる。

(7) CRYPTREC暗号リストの改定 ～耐量子計算機暗号（PQC）対応～【審議】

(8) 「耐量子計算機暗号（PQC）タスクフォース」の設置【審議】

資料６－１及び資料６－２並びに資料７について事務局から説明が行われた。主な質疑内容は以下のとおりであり、質疑において発生した修正意見の取扱い及びタスクフォースの詳細については座長に一任した上で、CRYPTREC暗号リストの改定及びタスクフォースの設置について了承された。（座長一任されたCRYPTREC暗号リストの改定に関する修

正内容は別紙のとおり。）

＜CRYPTREC暗号リストに関する質疑内容＞

（島岡構成員）資料６－１の検討ポイント⑤について、パラメーターセットにカテゴリを記載することは問題ないが、カテゴリのレベルの定義はどこかに記載されるのか。

（事務局）来年度に暗号強度要件の見直しを行うことになり、そちらと併せて整備していくことになると理解している。

（島岡構成員）来年度に整備されるまで少し混乱があるかと思い、手当いただきたい。

（事務局）政府関係機関には、CRYPTREC暗号リストの改定内容について説明する機会を設けたいと考えている。

（阿部構成員）カテゴリのレベルが同じであるパラメーターセットは、同じような暗号強度・安全性を提供すると理解している。複数の暗号技術を組み合わせる場合、例えばML-KEMとAESではCategory 3が双方のパラメーターセットに含まれるが、組合せが取れない場合もあるように思う。どう理解したらよいか。

（事務局）カテゴリのレベルはブロック暗号とハッシュ関数が混じっているため、一概に安全性順だと言いにくいが、いずれにせよCRYPTREC暗号リストは、使ってよい暗号技術のリストを示しているだけである。暗号強度要件の観点から補足があるか。

（IPA）検討をどう進めるかまでは決まっていないが、課題としては認識している。

（吉田構成員）ISO SC27 WG2で暗号の国際標準化について国際議長を務めている。国際標準化の議論でも、PQCのパラメーターセットやセキュリティカテゴリは非常に重要視されている。CRYPTREC暗号リストにおいても、こうした情報を扱うとともに、その際に十分な説明を行うことが適当と考えている。

（上原構成員）先ほども議論があったカテゴリの意味について、暗号強度要件で取り扱うとのことだが、CRYPTREC暗号リスト内のどこかに記載しないと、定義が宙に浮いた期間があると混乱するのではないか。

（事務局）資料６－１の６ページに、「カテゴリのレベル」について参考として示しているが、例えばこの定義をCRYPTREC暗号リストの注釈として記載することで、より分かりやすくなると考えるがどうか。

（松本座長）どこにも定義がないと分からないため、方針だけでも決めていきたい。

（内閣官房）政府統一基準の担当でもあり発言したい。各府省庁におけるシステム担当は必ずしもサイバーセキュリティの専門家ではない。定義についてこれから御議論いただく内容ではあるが、参照文書を見ないと分からないとなると担当の負担が大きくなるため、可能であれば、CRYPTREC暗号リストを見れば全てが分かると担当側としては助かるかと思う。

（松本座長）現行のCRYPTREC暗号リストにおいても、個別の暗号技術の参照先が仕様書として紐付いており、その参照先で記載されていれば問題ないのだがどうか。

（事務局）資料６－１の12ページ目にFIPS 203の参照先となる米国NISTの文書を引用しているが、ML-KEM-512がCategory 1という記載はあるが、カテゴリの定義について

記載はない。カテゴリの定義については、前ページにある2016年のリクワイアメント文書まで遡る必要がある認識。先ほど内閣官房からあったように、現状、関係文書をたどらないと定義にたどりつけない状況。例えば、表２の「パラメーターセット」という文言に注釈を振り、資料６ページ目にあるカテゴリの定義をその注釈に記載することが考えられるがどうか。

（高木構成員）文書をたどっていくのは大変であり、６ページの定義の記載は分かりやすく、注釈として入れてもそれほど多い分量でもないのではないか。また、必要であれば、定義となる文書へのリンクを記載することも検討してよいかと思う。

（田村構成員）現行暗号リストでは暗号技術のアルゴリズム名のみ記載してあり、安全性についてはリストとは別に暗号強度要件に鍵長などを記載している。PQCリストではパラメーターに加えて安全性に関するカテゴリを併記している。パラメーターとカテゴリの両方を書かないと誤解してしまうことがあるのか。また、カテゴリの記述は暗号強度要件における今後の検討として、ここではパラメーターだけに記述を絞る選択肢がありえるのか。

（総務省）暗号強度要件は来年度検討であり現状は固まっていない。その上で、カテゴリは非常に重要な概念であり、リスト内に記載したほうが分かりやすいだろうということで記載している。また、例えばML-KEM-768と書けば暗号技術は一意に特定できるため、特定の観点からカテゴリが必要ということではない。カテゴリと合わせたほうがわかりやすいかどうかという観点だけである。

（國廣構成員）注釈に追加する場合、表２の下に追加される形になるのか。

（事務局）御認識のとおり、表２の「パラメーターセット」に注釈を振って、「注８」のように注を一つ追加する形を想定している。

（國廣構成員）カテゴリは１より５のほうが、安全性が強いと我々は無意識に動いているが、５のほうが強いということを注釈で示せたほうがよいのではないか。

（事務局）資料６－１の６ページの記載であれば、５のほうが強いというのは分かるのではないか。

（松本座長）先ほど御提案があった形をベースとして、注を入れるという結論としたいが、よろしいか。他に意見はないか。

（高木構成員）表２に現在記載されている注８について、ハッシュ長が256ビットとある。これは現行暗号リストの注釈をそのまま持ってきているかと思うが、バースデーパラドックスで128ビットセキュリティにしかならないため、Category 5の256ビットセキュリティとするには、ハッシュ長を512ビットにする必要があるのではないか。

（事務局）御意見を踏まえて修正したい。

＜タスクフォースに関する質疑内容＞

（松本構成員）ハイブリッド構成の議論は非常に複雑であり、PQCの危殆化を懸念する観点からはハイブリッドを推す向きもあれば、実装に詳しい人からはハイブリッドが本当に良いのか懸念する向きもある。タスクフォースで検討を進めること自体は問題な

いが、ハイブリッド構成等に関して知見のある方、実装について知見のある方を構成員として検討を進めるべき。

(9)　2026年度暗号技術評価委員会 活動計画(案)【承認】

資料８について暗号技術評価委員会事務局から説明が行われ、特段の質疑もなく、原案のとおり承認された。

(10) 2026年度暗号技術活用委員会 活動計画(案)【承認】

資料９について暗号技術活用委員会事務局から説明が行われた。主な質疑内容は以下のとおりであり、質疑において発生した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)は承認された。

（松本構成員）鍵長ガイドラインやTLS暗号設定ガイドラインの改定について、ハイブリッド構成の取扱いなどの整理もあり、またPQCの標準化も途上であるため、短期的に再改定することも考慮が必要ではないか。

また、CRYPTRECの範疇かわからないが、暗号アジリティに関する文書も必要になるのではないか。システムの中には10年以上のライフサイクルを持つものも多く、これから調達するものは、暗号アジリティの考慮が必要となる。そのために、PQCに移行可能なシステムを調達するためのガイドラインのようなものが必要になると思う。海外では、PQC製品が調達できない現状で、暗号アジリティを調達要件に加えているところもある。

(IPA) ハイブリッド構成については、鍵長ガイドラインに入れられるか分からないが、できるだけ早くガイドラインを更新したほうが良いため、2026年度末には一旦更新を行い、必要に応じて短期でも更新していくスケジュールで進めていきたい。暗号アジリティの取扱いに関しては持ち帰り、どこがつくるかを含めて検討させてほしい。

（事務局）暗号アジリティについては、暗号技術活用委員会以外にも、政府全体の取組としてのロードマップの策定や、暗号技術評価委員会におけるPQCガイドラインにも関係しうるため、全体を見ながら必要に応じた検討を行うことになると考える。

（内閣官房）ハイブリッド構成・暗号アジリティのいずれも、世界的に見ても関心の高い話題である。暗号アジリティについてはPQC移行の文脈だけでなく、PQCの危殆化やその先の暗号移行を見据えても検討しておく必要があり、今後ロードマップを作成する中でキーワードとして出てくるであろうという認識である。

(11) 暗号技術検討会 2025年度 報告書（案）【承認】

資料10について事務局から説明が行われ、特段の質疑もなく、検討会議論の反映等について座長に一任した上で承認された。

(12) その他

議事全体を通じた意見交換があり、主な質疑内容は以下のとおり。また、事務局よりCRYPTRECシンポジウム2026についてアナウンスが行われた。

（松本座長）先ほどの審議内容を踏まえて修正を行うことになるが、新しいCRYPTREC暗号リストの公表時期の想定はどのようになるか。

（事務局）速やかに公表したいと考えており、３月30日(月)を目途に公表できるよう関係省庁で調整をしたい。

（田村構成員）来年度のCRYPTREC暗号リストの改定について、評価委員会での検討がうまく進めば９月頃にFIPS 204の評価が終わるため、その後、秋頃に検討会を開いてリストを改定するイメージで合っているか。

（事務局）カテゴリCategory１・2等の議論もあるため、その状況も見ながら必要に応じて開催することを考えている。

６．３．閉会

総務省三田サイバーセキュリティ統括官から閉会の挨拶が行われた。

以上

（別紙）

CRYPTREC暗号リストの改定に関する意見を踏まえた資料修正内容

暗号技術検討会における議事「CRYPTREC暗号リストの改定 ～耐量子計算機暗号（PQC）対応～」において、CRYPTREC暗号リストに新たに追加予定の＜表２　耐量子計算機暗号（PQC）リスト＞に関して、次の２点の意見があった。

①カテゴリの定義について文書内に記載する必要があるのではないか。

②「SHAKE256 (Category 5)」に係る注釈について、「ハッシュ長は256ビット以上」とあるが、512ビット以上とする必要があるのではないか。

この対応については座長一任となり、それぞれ次のように対応を行うこととした。

１　CRYPTREC暗号リストの＜表２　耐量子計算機暗号（PQC）リスト＞について

上記①に関して、カテゴリの定義を明確にするため、次の注釈を追記する。

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）

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)」の記載を削る。

上記②に関して、「SHAKE256」の取扱いについては、来年度に新たに設置予定の「耐量子計算機暗号（PQC）リスト検討タスクフォース」において暗号利用モードや認証暗号等の取扱いと合わせて議論を行うこととし、今回のCRYPTREC暗号リストの改定においては掲載を保留する。

２　注釈４に紐付く検討課題資料（資料６－１の最終ページ）について

カテゴリの定義や512ビットのハッシュ関数の取扱いについてもタスクフォースにおいて改めて精査することを想定し、課題①の記載を修正する。

暗号利用モードや認証暗号等の取扱いと合わせて「SHAKE256」の取扱いも課題に含まれることが明確となるように、課題②の記載を修正する。また、わかりやすさの観点から「CRQC」の用語解説のため正式名称を追記する。

以上