耐量子計算機暗号（PQC）リスト検討タスクフォース（第１回）　議事概要

１．日時

令和８年７月24日(金) 15:00～17:20

２．場所

ＡＰ赤坂グリーンクロス（東京都港区）及びオンライン開催

３．出席者（敬称略）

＜構成員＞
岩田哲、漆嶌賢二、垣内由梨香、國廣昇、須賀祐治、高木剛、細山田光倫、松本勉（座長）

＜オブザーバ＞
内閣官房国家サイバー統括室(NCO)（杉本貴之）

＜事務局＞
デジタル庁デジタル社会共通機能グループ（北井上礼樹）
総務省サイバーセキュリティ統括官室（梅城崇師、内藤めい）
経済産業省商務情報政策局サイバーセキュリティ課（石坂知樹、橋本勝国）
国立研究開発法人情報通信研究機構(NICT)（小川一人、髙和真）
独立行政法人情報処理推進機構(IPA)（神田雅透、伊藤忠彦）

４．議事概要

(1) 耐量子計算機暗号（PQC）リスト検討タスクフォースの設置について

〇事務局（総務省）から資料２に基づき開催要綱を説明。開催要綱の３（２）に基づき主査の互選を行い、松本構成員を主査に選任。

(2) CRYPTREC暗号リストのPQC対応と検討課題について

〇事務局（総務省）から資料３に基づき説明。
〇事務局（総務省）から今後の予定として、暗号技術評価委員会においてFIPS 204及びFIPS 205をそれぞれ2026年９月及び同年11月に審議すること、暗号技術検討会についても年度途中で開催することを想定していることから、少なくとも課題①と課題②に関しては、暗号技術評価委員会の審議時期を踏まえて、10月末を目途に方向性を示したい旨を説明。

(3) 課題①　Category 1・2の暗号等の取扱いについて

〇事務局（総務省(梅城)）から資料４に基づき説明。その後の質疑応答は次のとおり

＜検討ポイント①　セキュリティカテゴリの定義＞

漆嶌構成員　従来のCRYPTREC暗号リストは、基本的に暗号プリミティブを掲載し、暗号強度については別に定める暗号強度要件で示す考え方であったと認識している。このため、CRYPTREC暗号リストにセキュリティカテゴリのような暗号強度に関する記載をしない方がよいのではないか。また、利用者側からみると、現行暗号リスト（表１）と耐量子計算機暗号（PQC）リスト（表２）に分かれている根拠が分からず複雑に見えるため、セキュリティカテゴリを外して一本化した方が分かりやすいのではないか。

松本主査　表１と表２に分ける構成は、これまでのCRYPTRECにおける議論を踏まえて決定したものであり、表２は表１とは異なる方針で記載することとしている。本日はこの構成を前提として議論を進め、今後、重大な問題が生じた場合には改めて検討することとしたい。

漆嶌構成員　SLH-DSAには多数のパラメーターセットが存在するため、全てを列挙すると表が煩雑になるのではないか。

総務省（梅城）　SLH-DSAのパラメーターセットの記載方法として、一部をまとめて記載する方式もあるため、今後調整していきたい。

松本主査　検討ポイント①のセキュリティカテゴリの定義については、現時点では記載内容に特段の過不足はないものとして進めたい。

＜検討ポイント②　512ビットハッシュ関数の取扱い＞

岩田構成員　512ビットハッシュ関数についてカテゴリが空欄となっていると、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望ましい。記載するとすれば「Category 4」が自然である。一方、単に「Category 4」と記載すると、512ビットハッシュ関数が384ビットハッシュ関数より高い安全性を有することが伝わりにくいため、その点が分かる記載とすることが望ましい。

NISTがCategory 1～5を定義しているが、自然に考えると512ビットのハッシュ関数の衝突探索に対応するCategory 6があってもおかしくないが、NISTの定義がCategory 5までである以上、現状では「Category 4」とすることが自然である。

細山田構成員　岩田構成員と同じくカテゴリを空欄とすることは不自然であり、現行の定義に基づけば「Category 4」又は「Category 4以上」とすることが適当と考える。

國廣構成員　Category 5までしか定義されていないことを踏まえると、カテゴリ定義にある「鍵探索又は衝突探索と同程度以上の計算資源」の「以上」が利用者に十分伝わるよう、記載上工夫することが考えられる。

松本主査　512ビットハッシュ関数については「Category 4」を追記することとしつつ、384ビットハッシュ関数に比べてセキュアだということが利用者に伝わるように注釈等をつけていくことについてどうか。

（異議なし）

松本主査　それでは「Category 4」を追記することとし、注８の文言を検討することとしたい。事務局から何か案はあるか。

総務省(梅城)　注８の「同程度以上」の「以上」に下線を引いて目立たせることがある。また、先ほども意見が出た「Category 4以上」と記載する案も考えられるのではないか。

IPA(神田)　認証制度等では、基準を上回ることを「＋」を付して表記する例がある。

松本主査　「Category 4以上」や「Category 4+」といった表記を用いるとなると、新たに定義を置く必要があり容易ではない。また、「Category 4以上」というと、「Category 5」とどのような上下関係があるのかも説明が難しい。

総務省(梅城)　仮に「Category 4+」等の表記を採用するのであれば、注８において、384ビットを超えるハッシュ関数についてそのように表記する旨を定義する方法も考えられる。

松本主査　NISTにCategory 6が定義されていれば異なる整理も可能であるが、現時点ではNISTにそのような定義はないので「Category 4」のままとすることがよいと考える。その上で、「Category 4」に新たに「注９」を付し、セキュアになっている旨を触れることも考えられる。また、そこまで手当しなくても、利用者は認識できるという考えもあり得る。

垣内構成員　少々話が逸れるかもしれないが、利用者視点では、製品選定時に実際に選択するものはML-KEM-768等のパラメーターセットであり、Category 3等のセキュリティカテゴリはそもそも製品に記載されていない。パラメーターセットの後に括弧書きでカテゴリを併記すると、同一のパラメーターセットについて異なるセキュリティカテゴリの設定が存在するとの誤解を招く可能性がある。このため、「パラメーターセット」と「セキュリティカテゴリ」を別の列として記載し、カテゴリについては別途注記する方が分かりやすい。こうすることで、先ほど「注９」を入れる話も出ていたが、その場合でも何に対する注なのかが分かりやすくなる。

松本主査　パラメーターセットとセキュリティカテゴリを別の列として整理する方法は分かりやすく、先に指摘のあった表の煩雑さについても一定程度解消できると考える。冒頭の漆嶌構成員の指摘があった点も一定程度解消されるのではないか。

（賛同する意見）

須賀構成員　「セキュリティカテゴリ」という用語について、NIST文書においても用いられていることを確認したため、この表現で問題ないと考える。

総務省（梅城）　NISTの2024年の文書でも「Security Category」と記載されており、これをカタカナ表記したものである。

松本主査　残る論点は、512ビットハッシュ関数に「Category 4」と記載した上で、「注９」にどのような注釈を付けるかということである。
高木構成員　注釈には、「512ビットハッシュ関数に対する衝突探索」と記載し、384ビットハッシュ関数より大きいことが分かるようにした方がよい。Category 6に相当する説明である。
國廣構成員　512ビットハッシュ関数について、衝突探索に必要な計算資源を記載する形が最も簡潔で分かりやすいのではないか。「Category 4に属する」と記載してもよい。
松本主査　512ビットハッシュ関数については、「Category 4」に「（注９）512ビットのハッシュ関数に対する衝突探索の計算資源が攻撃に必要であり、Category 4に属する。」と注釈を付す方向で整理する。具体的な文言について、より適切な案があれば後ほど修正することとしたい。
漆嶌構成員　NISTの2016年の原文では「Security Strength Categories」との表現が用いられており、日本語でも「セキュリティ強度カテゴリ」などに変更する必要はないか。
総務省(梅城)　NISTの2024年の文書では「Security Category」と記載されており、現在の「セキュリティカテゴリ」という表現でも問題ないと考える。
松本主査　厳密に「強度」と表現すると大変なので「カテゴリ」という表現にしたと聞いており、現行の記載内容で問題ないと考える。

＜検討ポイント③　Category 1・2の取扱い（公開鍵暗号の扱い）＞

総務省(梅城)　ネットワーク機器ベンダー等からPQC対応状況を聞いていると、ML-KEMはCategory 3又はCategory 5を実装している例は多く、Category 1のみしか実装していない例は認識していない。
松本主査　ML-KEMのCategory 1の取扱いは、表１の現行暗号にも掲載されているAES等とは分けて考える必要がある。その上で、耐量子計算機暗号（PQC）として、Category 1・2を掲載しない場合にどのような問題が生じるか確認する必要がある。また、掲載する場合には、可能な限りCategory 3以上の利用を強く推奨する旨の注釈を付すことも考えられる。過去にそのような注釈を付したことはあるか。
IPA(神田)　RC4や64ビット暗号等について利用を避けるようにした例がある。
松本主査　過去の例は廃止される方向の暗号技術に対するものと理解した。Category 1・2を掲載する場合には、2035年を目途にPQC移行を行う際、その後はCategory 1・2をどうするのか、互換性維持リストに移すのか等も含めて検討していきたい。
須賀構成員　Category 1・2の取扱いは、暗号技術活用委員会での議論や、現在の実装状況等を踏まえて判断すべきであり、Internet-DraftやRFC等における利用状況についても調査が必要である。特に、Category 3以上を利用したくても、ネットワークアプライアンス等の制約によりCategory 1に下げざるを得ないケースが存在する可能性もあるため、実装状況を十分確認せずにCategory 1・2を除外すると、利用者に支障が生じるおそれがある。このため、現時点で結論を出すことは難しいと考える。
松本主査　暗号技術活用委員会においてTLS暗号設定ガイドラインの改定を行おうとしているが、須賀構成員からの指摘についてどうか。
IPA(神田)　TLS暗号設定ガイドラインは、CRYPTREC暗号リストの整理を踏まえて改定される。つまり、CRYPTREC暗号リストにCategory 1・2を入れることになれば、TLS暗号設定ガイドラインでもCategory 1・2を入れることになる。
須賀構成員　関係性について理解した。
松本主査　８ページ目の諸外国に関する資料では、Category 1・2に相当する方式がブランクなものがある。オランダではSLH-DSAのCategory 1がAcceptable。アメリカはどういう状況なのか。
國廣構成員　Category 1・2に相当する方式がブランクなものは、利用不可としているという意味か。
総務省(梅城)　海外のガイドラインは推奨する暗号技術のみを記載している場合が多く、記載がないことが直ちに利用不可を意味するものではない。一方、日本のCRYPTREC暗号リストは政府統一基準との関係で、リストに掲載されていない暗号技術は政府情報システムで通常利用できないこととなるため、海外のガイドラインとは性格が異なる。米国を含む海外

の最新状況については、改めて確認したい。

＜検討ポイント③　Category 1・2の取扱い（公開鍵暗号の扱い）＞

漆嶌構成員　ML-DSA-44はCategory 2に相当するが、PKI分野ではエンドエンティティ向けの証明書等で利用される可能性が高いと考えている。このため、今後ML-DSAがCRYPTREC暗号リストに掲載される際にCategory 1・2を一律に除外すると、ML-DSA-44が利用できなくなることを懸念している。

総務省(梅城)　実際にML-DSAがデファクトベースで使われ始めており、その中でML-DSA-44が主に使われているということか。

漆嶌構成員　エンドエンティティ向けではML-DSA-44が多く使われている。

松本主査　エンドエンティティ向けの実装については、ML-DSAであってもサイドチャネル攻撃耐性を確保することが容易ではなく、何が正しいのかは悩ましい。一方で、ML-KEM-512についても、実装攻撃への対策として冗長化やマスキング等を行うと計算資源を多く必要とするため、特に低リソース機器でどこまで対応できるかという問題がある。IoT機器等の低リソース環境のものの実情について、垣内構成員で情報を持っていないか。

垣内構成員　現時点ではどの程度まで対応可能か十分な知見が蓄積されておらず、情報収集中である。参考までに、Windows及びMicrosoft製品で利用される暗号ライブラリであるSymCryptでは、ML-KEMについてCategory 1・3・5の実装が存在しているが、Microsoftとしては、利用者に対してCategory 3以上を利用するよう推奨している。

岩田構成員　Category 1・2を完全に排除することは大きな判断である。仮にCategory 1・2を表２に含めるのであれば、Category 3以上の利用を強く推奨する旨を明記することが自然である。また、その際には、将来的にはCategory 1・2が利用できなくなる可能性があることも利用者に伝えるべきであり、過去にRC4等を段階的に廃止していった場合と同様の考え方が必要になると考える。

IPA(伊藤)　NISTの関係者と先日話すことができた。セキュリティカテゴリを最初に作ったのは約10年前であり、現時点でCategory 1・2を積極的に進めていくかというとよく分からないということ。また、IoT等の低リソースのものでCategory 1・2が必要になってくる可能性はあるということであった。

　一方、TLS等の通信プロトコルでは、Category 3程度の方式を選択している例が多いと認識している。

須賀構成員　セキュリティプロトコルにおいてCategory 1・2はあまり推奨されていないという認識でよいか。

IPA(伊藤)　IETFではCategory 1・2を明示的に非推奨とするのではなく、コードポイントやOID等を用意した上で、利用するか否かは利用者側の判断に委ねる整理が一般的である。

須賀構成員　公開鍵暗号系と共通鍵暗号系で少しずれているか。

IPA(伊藤)　公開鍵暗号と共通鍵暗号で求める強度をそろえるか、PQCの成熟度を考慮してより高い強度を求めるかについては、設計者の考え方による。

松本主査　Category 1・2であればPQC移行が可能だが、Category 1・2が認められなければPQC移行ができないというケースが実際に存在するのか。また、低リソース機器ではPQC移行ができないことが認められるならば、この場で低リソース機器を取り扱う必要がなくなる。PQC移行を進める側として、NCOからコメントいただきたい。

NCO(杉本)　政府統一基準の観点からは、将来的にはPQCである表２が残り、現行暗号リストである表１は順次縮小していくものと認識している。利用者から見れば、表２に掲載されている暗号技術を採用すれば2035年以降もシステムを継続して利用できると理解することが想定される。このため、表２については、2035年直前に大きく内容を変更するよりも、当初から一定程度厳格な基準とし、「これを選んでおけば将来も安心である」という基準として示すことが望ましい。これは、政府の調達側だけでなく、国内の製造・提供側に対するメッセージにもなる。

松本主査　これまでの議論を踏まえると、Category 1・2を含めない案と、含めた上でCategory 3以上の利用を強く推奨する注釈を付す案が考えられる。後者の場合、将来Category 1・2をリストから外す際の対応が必要となるため、強い不都合がなければ当初から掲載しない

方が整理しやすいと考える。一方、実利用上の支障が生じる可能性については確認が必要である。

漆嶌構成員　ウェブ系の証明書では、Merkle Tree証明書という新しい証明書が使われようとしており、その中で、サーバー証明書にML-DSA-44を利用する案がある。また、認証局業界として、タイムスタンプや利用者・サーバー向けのPQCの証明書について、ML-DSA-44を利用する方向になる可能性がある。このため、ML-DSA-44をリストから除外すると、政府が調達できる製品が存在しない状況になることを懸念している。Category 3以上の利用を強く推奨しつつ、ML-DSA-44についてはリストに掲載しておくことも検討すべきである。

須賀構成員　オランダの「The PQC Migration Handbook」が参考になる。発行が2024年で時間が経過しており少し古い情報になりつつあるが、失敗事例など赤裸々な話も書いている。

IPA(伊藤)　IETFでは現在、セキュリティカテゴリ自体が大きな論点となっているわけではない。暗号化方式については議論が比較的収束しつつある一方、署名方式については引き続き議論の余地があり、まだ方向性が固まっていないと認識している。

松本主査　以上を踏まえ、ML-KEM-512（Category 1）については、現時点では表２に掲載しないこととしたい。一方、ML-DSA-44（Category 2）については、本日は結論を出さず、掲載する可能性があるということで、現状や今後の動向を調査した上で判断することとしたい。（首肯する構成員あり）

＜検討ポイント③　Category 1・2の取扱い（共通鍵等の扱い）＞

総務省(梅城)　これまでの議論では、ML-KEMのCategory 1は表２に掲載せず、ML-DSA及びSLH-DSAのCategory 1・2については継続検討となったと理解している。次にAES、SHA2、SHA3等のCategory 1・2についても検討いただきたい。

松本主査　AES、SHA2、SHA3については、表１の現行暗号リストに掲載されており、表１がいつ無くなるのか無くならないのかも決まっていない。表１と表２が併存している現状で、同じ暗号技術が異なる取扱いとなり得る状況をどのように考えるべきか。

NCO(杉本)　表２をどのような性格のリストとして位置付けるかを明確にすることが重要である。例えば、2035年の時点で利用可能期間が５年を切っているものは掲載しないとするなど、そのような定義が明確になれば、何を表２に掲載し、何を掲載しないかも整理しやすい。制度所管省庁としても、どのような基準で暗号技術が選定されているかが明確であれば、調達者に対して表２の位置付けや利用上の留意点を説明しやすい。

松本主査　今議論している点を改めて明確にしたい。

総務省(梅城)　公開鍵暗号以外についても、Category 1・2に該当するAES-128やSHA-256等を表２に掲載するかどうかがまず論点となる。そして掲載する場合には、より高いCategoryの利用を推奨する注釈を付すかどうかについても検討が必要である。例えばAES-128を掲載する場合、可能な限りAES-192又はAES-256を利用するよう注釈を付すことが考えられるが、その場合、表１のAES-128には注釈がついていないため、整合性も確認する必要がある。

松本主査　現行の表２には、Category 1・2に相当するAES-128や一部のハッシュ関数が掲載されていない。今後、表１が無くなり表２のみとなる場合を見据えると、まずはこれらを表２に掲載するかどうかを検討する必要があると理解した。

総務省(梅城)　政府におけるPQC移行を進める際には、いわゆるPQC対応システムは、表２の中から暗号技術を選択することが求められると考えている。その場合、表２に掲載されていないAES-128は、PQC対応システムでは利用できないことになる。

松本主査　現状は、PQCへ移行できるようにしていく必要があるという状況で、移行していないシステムがどうなるのか明確には決まっていないのではないか。NCOの認識を伺いたい。

NCO(杉本)　現時点で確定しているものではなく、NCO側のあくまで想定ではあるが、2035年以降、量子コンピュータの発展状況等を踏まえ、CRYPTRECで危殆化の状況を判断いただいた上で、表１は、電子政府推奨暗号から運用監視暗号リストへ移り、その後、運用監視暗号リストからも削除されるという段階的な対応を想定している。最終的には表２のみが電子政府推奨暗号として残ることを想定している。移行に長期間を要するシステムもあることから、2035年以降も利用する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ている。

松本主査　表２を耐量子計算機暗号(PQC)リストとしている以上は、AES-128を掲載することは適切ではないと考える。一方、PQC移行の対象とはしないものの、AES-128を継続利用する必要がある場合の取扱いは整理する必要がある。

NCO(杉本)　現時点では表１及び表２のいずれも電子政府推奨暗号であるため、表１に掲載されているAESを利用する限り、AES-128の利用も認められる。一方、2035年以降、量子コンピュータの発展等を踏まえて表１が順次格下げされれば、いずれAES-128は利用できなくなると考えられる。このため、2035年までに利用を終了するシステムであればAES-128で問題はないが、2035年以降も継続利用するシステムでは、表１が格下げされるリスクが始まり、システムをどれだけ長く使うかによると考える。

細山田構成員　松本主査の考えに基本的に賛同する。研究者によっては量子コンピュータが進展してもAES-128は破れないと考えている人もいるが、量子コンピュータが今後どのように発展するかは不確実であり、AES-128は長期的な保護が必要なデータを扱う用途では利用しない方がよいと考える。これはAES-128に限らず、Category 1・2に相当するハッシュ関数等についても同様である。

岩田構成員　松本主査及び細山田構成員の意見に同意する。表２の位置付けを踏まえると、AES-128を掲載することは適切ではない。

松本主査　これまでの議論を踏まえ、表１・表２の構成を踏まえれば、表２にCategory 1・2のAESやハッシュ関数を追加しないこととしたい。電子政府推奨暗号リスト全体を見直す際には、改めて取扱いを検討することとしたい。

総務省（梅城）　AES-128を表２に掲載しない場合、PQC移行に際して現在AES-128を利用しているシステムについては、AES-192又はAES-256への移行を併せて求めることとなるがその理解でよいか。また、Category 1・2を表２に掲載しない理由として、暗号強度要件における将来的な利用期限だけでなく、Groverのアルゴリズム等を用いた量子計算機による攻撃の影響も考慮するとの理解でよいか。

松本主査　Groverのアルゴリズムが完全に動けばAES-128は64ビット全数探索で終わってしまう。PQC移行を前提とするのであれば、AES-128を許容することは適切ではなく、量子計算機による攻撃の影響も考慮すべきである。

（首肯する構成員あり）

松本主査　細山田構成員から意見があるか。

細山田構成員　過ぎた話になってしまったが、仮にCategory 1・2を表２に追加する場合には、長期的な保護が必要なデータを扱う用途ではCategory 3以上を推奨する旨の注釈を付すことが望ましいと考えていたが、現時点では表２に追加しない方向で整理されたと理解している。

(4) 課題②　暗号利用モードや認証暗号等の取扱いについて

〇事務局（NICT(髙)）から資料５に基づき説明。その後の質疑応答は次のとおり

岩田構成員　AESやハッシュ関数が表２に掲載される一方で、暗号利用モードやメッセージ認証コード等が掲載されない場合には、リストとして片手落ちとなり、使い勝手が悪くなる。表２に掲載可能なものは掲載していくことが必要である。また、Q1モデルを主たる評価モデルとする方針も合理的である。

一方、128ビット暗号については、AES-128等の議論だけでなく、Category 2に相当するハッシュ関数を用いるMAC等についても検討が必要である。

また、暗号利用モード、メッセージ認証コード、認証暗号の掲載とエンティティ認証の保留に関する事務局案はいずれも合理的と考えるが、諸外国における取扱いについても確認した上で議論したい。

松本主査　諸外国の状況については、この場で回答することが困難であるため、次回以降、調査結果を反映した上で議論することとしたい。

須賀構成員　諸外国の事例として、オランダの「The PQC Migration Handbook」の4.2が参考になると考える。

細山田構成員　基本的には岩田構成員と同様の考えである。特に重要なのはCategory 1・2の取扱いであり、エンティティ認証以外の暗号技術については、Category 1・2に該当するもの

を除外するのであれば、現時点の案のとおり表２に掲載しても問題ないと考える。

高木構成員　資料５付録２の「暗号利用モード」について、「Category 1, 3, 5」と記載されているが、どのような考え方でセキュリティカテゴリを付しているのか。

総務省(梅城)　暗号利用モードのセキュリティカテゴリについては、資料８の４ページ目に論点として整理しており、別途議論したい。

松本主査　議論は概ね方向性が固まったのではないか。Category 1・2の取扱いについては継続検討とし、それを除いた形で表２に掲載する。また、暗号利用モードやメッセージ認証コードに関するセキュリティカテゴリについては別途検討することとしたい。

(5) 課題③　ハイブリッド構成の取扱いについて

〇時間の都合上、次回以降に改めて議論することとなった。

(6) 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

〇事務局（総務省(梅城)）から資料７に基づき説明。その後の質疑応答は次のとおり

NCO（杉本）　世界的に利用が見込まれる暗号技術だけでなく、国内で利用が見込まれる暗号技術についても検討していくということであれば、安全性評価もしっかり実施してほしい。一方、欧州等では独自のPQCの標準化・採用に向けた動きもあることから、通信相手がそのような方式を利用する場合に、我が国政府としてその利用を認めるか否かという観点にも留意する必要がある。

松本主査　各国・地域において独自のPQCの標準化等を進めている例があるが、国際的に利用できなくてもよいという考えの下で進めていると認識している。

NTRUについて、国内事業者において具体的な利用意向があり、CRYPTREC暗号リストへの掲載意向があるのであれば、安全性評価の対象とし得るということに違和感はないと考えるがどうか。

（特に発言なし）

松本主査　それではそのように進めていきたい。また、各国・地域における独自のPQCに関しても、どのように判断していくかを今後整理していく必要がある。

須賀構成員　安全性評価の対象とする暗号技術を選定するための基準は定められているのか。

松本主査　現時点では定められていない。

須賀構成員　欧州等で採用が検討されている方式を含め、評価対象となり得るPQCは多数存在するため、まず評価対象を選定するための基準を定めることも重要である。

松本主査　評価対象を無制限に拡大することは適切ではないため、評価対象の選定基準について検討が必要である。一方で、NTRUが安全性評価の対象とし得るというコンセンサスが得られるのであれば、その検討は早く進めた方がよい。NTRU以外を評価しないというわけではなく、国際的な情勢も踏まえて、必要なものを評価できるよう今後検討したい。

須賀構成員　評価対象については一定程度広く検討することが望ましいが、安全性評価のコストとのバランスが大変重要である。

松本主査　PQCの安全性評価については、NTRUが対象になり得ることとし、その検討を早めに進めていただきたい。

(7) その他

〇時間の都合上、資料８については次回以降に改めて議論することとなった。

〇事務局（総務省(梅城)）から、次回については、８月開催を含めて日程調整をしたい旨を連絡。

以上