

## 耐量子計算機暗号（PQC）リスト検討タスクフォース（第2回） 議事概要

### 1. 日時

令和8年8月31日（月） 14:00～16:20

### 2. 場所

総務省8階第1特別会議室

### 3. 出席者（敬称略）

#### <構成員>

岩田哲、漆畠賢二、垣内由梨香、國廣昇、須賀祐治、高木剛、細山田光倫、松本勉（主査）

#### <オブザーバ>

内閣官房国家サイバー統括室(NC0)（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（中川拓哉）

総務省サイバーセキュリティ統括官室（梅城崇師、遠藤琢、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、高和真、青野良範）

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) Security LevelとSecurity Categoryの使い分けについて

○事務局（NICT(青野)）から資料2に基づき説明。また、事務局（総務省(梅城)）から資料3に基づき5ページ目まで説明。その後の質疑応答は次のとおり。

##### <セキュリティカテゴリー部分の罫線の取扱い>

垣内構成員 資料3の2ページにおける「セキュリティカテゴリー」の記載について、現在の記載方法だと、例えば、ML-KEM-768にCategory 3とCategory 5があるような読み方もできてしまう。そのため、「パラメーターセット」と「セキュリティカテゴリー」との対応関係が明確となるよう、それぞれの行を区切って記載した方が分かりやすい。

松本主査 垣内構成員の指摘を踏まえ、パラメーターセットごとに対応するセキュリティカテゴリーが明確となるよう、表の記載を修正することとしたい。

##### <表の列名の取扱い>

松本主査 表の列名として「パラメーターセット」と記載しているが、ML-KEM-768等については適切である一方、AES-192やSHA-384等も含めて同一の名称を用いることが適切か確認が必要ではないか。

漆畠構成員 「パラメーターセット」ではなく、「アルゴリズム識別子」等とすることも考えられる。

松本主査 「名称」も一種の識別子であり、リスト全体としてどのように表現することが適切か考える必要がある。

総務省(梅城) 「パラメーターセット」について、PQCに関しては、NIST SP 800-57の4.6.1.3では「parameter sets」と呼んでおり違和感はない。一方でAES-192など現行暗号と重なる部分は検討が必要である。

松本主査 NIST SP 800-57の4.6.1.3において、「algorithms and parameter sets」と書いており、「parameter sets」に限らないのではないかと。

須賀構成員 FIPS 203においても冒頭のAbstractで「parameter sets」とされており、公文書で書かれていることから、間違いはないのではないかと。

松本主査 「three parameter sets」とあり、ML-KEM-512、ML-KEM-768、ML-KEM-1024の3つを

指していることから、一個一個は「parameter set」と理解。

國廣構成員 AESについては、「parameter」という表現はあるものの「parameter set」という表現は確認できず、ML-KEM、AES、SHA等について統一的に「パラメーターセット」と表現することは難しい可能性がある。

NC0(杉本) 利用者にも理解しやすい表現とすることが望ましい。当該欄はAES等では鍵長等のパラメーターを指すものと理解できる。一方、PQCでは、ML-KEM-768等の数字が何を意味するのかは必ずしも分かりやすすくない。

総務省(梅城) ML-KEMについては、FIPS 203上もML-KEM-512等がパラメーターセットとして扱われている。NIST SP 800-57では、従来のAES等では「security strength」をビット単位としていわゆるビットセキュリティで示していたが、PQCではビット数で表すことの妥当性が問題となり、「security categories」による整理が導入されている。このように、AES等とPQCとでは、用語の使われ方が異なるため、表2全体で統一的に表現することには難しさがある。

IPA(伊藤) FIPS 203において「three parameter sets」とある点について、例えばML-KEM-768というのはパラメーターセットの名称と理解できるのではないか。

松本主査 FIPS 203のTable 2にあるように、 $n$ 、 $q$ 、 $k$ 、 $\eta_1$ 、 $\eta_2$ 等のパラメーターの組合せのことをML-KEM-512等と称しているのではないかという趣旨と認識した。

岩田構成員 ML-KEM等について「パラメーターセット」と表現することには違和感はないが、AESやSHAについては鍵長や出力長等の単一のパラメーターであり、「パラメーターセット」と表現することには一定の違和感がある。

松本主査 全体の対称性で言えば、ML-KEMやAESでは、名称に数字がついたものがパラメーターセットになっているが、SHA2の場合はそのようになっていないという点も気になる。

細山田構成員 SHA2については、名称が紛らわしいのはそのとおりだが、公式の名称がこのような関係となっており、変更することは難しいと考える。

松本主査 そうすると、SHA2のパラメーターがSHA-384ということではなく、SHA-384等を含む集合をSHA2と称しているということではないか。SHA-384をパラメーターやパラメーターセットとは称していないのではないか。

総務省(梅城) パラメーターセットをリストに入れるということは、昨年度末の暗号技術検討会において議論しましたが、列名部分については十分に議論ができていなかったと思う。これまでの議論を踏まえれば、例えば、「名称」と「パラメーターセット」の2列を合わせて「名称」と書いてしまうのも一案ではないか。

細山田構成員 2列を統合した上で、「名称・パラメーターセット」という列名とすることも考えられる。

松本主査 「名称・パラメーターセット」とする場合、AES等の「パラメーター」は「パラメーターセット」に含まれているという理解になるのか。

総務省(梅城) 先ほどの議論を踏まえればSHA2は「名称」に含まれているとも考えられる。

松本主査 列名を「名称」として、「パラメーターセット」という言葉をリスト内のどこかでリファースすることも考えられる。

NC0(杉本) 暗号技術ごとに具体的な表現方法は異なるものの、利用可能な方式をより細かく指定するために何らかのパラメーター等を指して規定しているという考え方に違和感はない。

高木構成員 現行暗号リスト(表1)を見ると、「暗号技術」としか書いていない。今回は暗号技術の中でどのようなパラメーターがどのようなセキュリティカテゴリーかということに記載しているため、「名称」と「パラメーターセット」を分けずに「暗号技術」としてまとめ、「セキュリティカテゴリー」は括弧や縦線で区切る形としてはどうか。

松本主査 「名称」と「パラメーターセット」をまとめて「暗号技術」とし、その右側に「セキュリティカテゴリー」の列を設ける形であれば、表として分かりやすいと考える。結合した部分の右側は何と呼ぶのかと言われたときに、「パラメーターセット」と言うという情報は落ちてしまいましたが、それでも機能はすると思うがどうか。

(異論なし)

松本主査 それではこの案で進めることとしたい。

## (2) 課題① Category 1・2の暗号等の取扱いについて

○事務局（総務省（梅城））から資料3に基づき6ページ目から説明。その後の質疑応答は次のとおり。

### <検討ポイント② 512ビットハッシュ関数の取扱い>

國廣構成員 提示された注釈案は、512ビットハッシュ関数と384ビットハッシュ関数との関係が分かりやすく、適当と考える。

岩田構成員 提示された注釈案は十分に丁寧であり、誤解を与えることはないと思う。

松本主査 注釈については提示された案で進めることとしたい。

（異論なし）

### <検討ポイント③ Category 1・2の取扱い>

松本主査 前回議論したようにML-KEM、AES、SHA2及びSHA3について、Category 1・2に該当する方式は表2に掲載しない方向で整理したい。

（異論なし）

松本主査 署名方式については、ML-DSA-44やSLH-DSAのCategory 1に該当するパラメータセットを掲載する可能性を残し、掲載する場合には「可能な限りCategory 3以上の利用を推奨し、特に長期的な保護が必要なデータを取り扱う用途ではこれを強く推奨する」との注釈を付す案となっていることについて意見はあるか。

國廣構成員 ML-DSA-44を掲載するか否かについては、本日の会合ではなく、今後改めて議論するとの理解でよい。また、SLH-DSAのCategory 1についても、ML-DSA-44と同様の考え方で掲載を検討するのか。

総務省（梅城） ML-DSA及びSLH-DSAについては、標準化動向や実利用状況を十分に調査できていないため、資料を整理し改めて掲載範囲を議論したい。現時点では、表に記載している方式について掲載する可能性があるという位置付けである。ML-DSA-44については、エンドエンティティ証明書やウェブ証明書等での利用があると考えているが、SLH-DSAについては具体的な利用実績を現時点では十分確認できていない。

NGO（杉本） 政府調達の観点からは、表2に掲載される暗号技術の基準が明確だとありがたい。政府システムは概ね5年程度で更改される例が多く、2035年に導入したシステムを2040年前後まで利用するとした場合、2035年時点で何年程度利用可能な暗号技術を表2に掲載するのかという考え方が明確であると、調達側としても参照しやすい。

松本主査 議論を踏まえ、タスクフォースとしての報告を取りまとめていくこととしたい。

## (3) 課題② 暗号利用モードや認証暗号等の取扱いについて

○事務局（NICT（高））から資料4-2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 Q1モデルを主たる安全性評価モデルとする方針は合理的と考える。一方、マレーシアで128ビット鍵のKCipher-2がApprovedとされていることなどを踏まえると、今回参照した資料の中には、PQCや耐量子性を前提とした資料と、必ずしもそうではない資料が混在しているのではないかと。特に128ビット鍵長やSHAKE128等の取扱いについては、PQCを考慮した資料か否かを区別して議論する必要がある。

NICT（青野） マレーシアの資料では、KCipher-2はストリーム暗号として分類されており、耐量子性を有するとは明示されていない。同じ資料内にはPost-Quantum KEMという別分類も存在するが、そちらには含まれていないため、KCipher-2が耐量子方式として掲載されているとは考えにくい、明確な断定はできない。

松本主査 諸外国資料については、基本的にはPQC対応している文献を参照すべきで、ほかは参考情報かと考えており、PQCや量子計算機を考慮した文書であるかを改めて確認してほしい。

NICT（高） Camellia-256等について各資料に記載はあるものの、耐量子性を有する方式として明示されているとは限らないため、各資料の位置付けを再確認したい。

岩田構成員 前回事務局から示された、暗号利用モード等を表2への掲載対象として扱う方向性自体は合理的と考える。ただし、128ビット鍵長の方式等が混在しているため、Category 1・2の取扱いとの整合を取りつつ整理する必要がある。

細山田構成員 今回の諸外国調査は参考資料として一定の不明点があるものの、前回事務局か

ら示された方向性自体には問題ないと思う。また、先ほど岩田構成員が提示した論点については、Category 1・2に該当する方式を表2に掲載しない前提であれば、現時点で大きな問題はないと思う。

松本主査 米国について、共通鍵暗号は対象となっている一方で、暗号利用モード等の記載がほとんどないように見えるため、そもそも当該資料の対象外なのか、別資料に規定があるのかを確認する必要がある。

NICT(小川) 米国資料等の解釈については、持ち帰って整理の上、改めて報告したい。

松本主査 KCipher-2や暗号利用モード、メッセージ認証コード等については、諸外国資料の位置付けや記載内容を再確認した上で最終判断することが適当と考える。特に、FIPSとの関係を含め、米国の状況はきちんと把握しておいた方がよい。ChaCha20-Poly1305については、CRYPTREC暗号リストに最初から入っていたわけではなくて、使用が多くなってきたので、それを評価して入れたという経緯があるが、何か意見はあるか。

細山田構成員 ChaCha20-Poly1305は256ビット鍵を用いる方式であり、セキュリティカテゴリー的にも問題はなく、特段の脆弱性が確認されているものでもないことから、表2に掲載しない理由は特になくはないと考える。

岩田構成員 細山田構成員と同意見であり、ChaCha20-Poly1305はQ1モデルにおける数学的な安全性証明があり、鍵長にも問題がないため、掲載しない理由はないと考える。

資料4-1の付録2において、SHA-512、SHA3-512及びSHAKE256の一部が灰色表示されている理由は何か。

総務省(梅城) 資料4-1は前回資料をそのまま掲載しており、その時点では512ビットハッシュ関数のCategoryやCategory 1・2の取扱いが未確定であったため灰色表示としている。これらは別途の議論結果を踏まえて更新することとなる。

高木構成員 AES、SHA2、SHA3はカテゴリ一定義の基準となる方式であるため、本年3月の暗号技術検討会において、追加の安全性評価を経ず表2に掲載している。一方で、CamelliaやSHAKE256等を新たに掲載する場合、外部評価を実施する必要があるのか。また、CBC等の暗号利用モードについては、プードルアタックやオラクルパディングアタックといった既知の攻撃や利用上の注意事項があり、耐量子性だけを理由に表2へ掲載することには慎重な検討が必要ではないか。

総務省(梅城) Camelliaや暗号利用モード等のCRQC耐性については、2024年度に実施した共通鍵暗号の安全性評価結果を踏まえ、量子計算機が存在する場合でも一定の安全性が確保できるとの整理を行っている。この評価で十分と判断するかどうかということか。

高木構成員 まさにその点について、専門家もいるこのタスクフォースで議論したい。

細山田構成員 既存評価では、古典計算機に対して安全である範囲であれば、Q1モデルでは量子計算機によって新たな問題が生じるわけではないとの整理をしている。鍵長等の条件は必要であるが、量子的に新しい議論が必要ではないとの認識である。一方、古典的な安全性そのものを改めて評価することは当該評価の対象外である。繰り返しになるが、古典的に大丈夫だという前提の下において、量子に何か新しい脅威が発生するかということと特に発生しないということである。

高木構成員 その整理であれば、Camellia等については追加の外部評価を行わず、CRQC耐性があるものとして表2に掲載することも可能と考える。一方、暗号利用モードについては、古典的な安全性も含めて引き続き確認したい。

岩田構成員 暗号利用モードについても、既存評価は、古典的な安全性が確保されている範囲であればQ1モデルで新たな問題が生じるわけではないとの整理である。CBCの初期値やGCMのnonce再利用禁止等、モードごとに古典的な利用上の条件は存在するため、必要に応じて注釈等で対応することが考えられる。Q2モデルでは安全性上の問題が生じる方式も存在するが、Q1モデルでは既存評価のとおりと考える。

松本主査 Q1モデルを前提とすれば、古典的な安全性が確保されている方式について量子計算機特有の新たな問題はないとの既存評価を踏まえ、CRQC耐性があると整理することは妥当と考える。CBCやGCM等の具体的な利用条件については、現行CRYPTREC暗号リストにも注釈が設けられており、耐量子性とは別の論点として必要に応じて対応することが適当。

岩田構成員 利用条件等については今後詳細を詰める必要があるが、大きな方向性としては事

務局案のとおり進めてよいと考える。

須賀構成員 暗号利用モードについて、組み合わせて利用するブロック暗号のカテゴリーに準ずる旨の記載とする方が適切ではないか。そもそも暗号利用モード自体にカテゴリーを記載することには違和感がある。

#### **(4) 課題③ ハイブリッド構成の取扱いについて**

○時間の都合上、次回以降に改めて議論することとなった。

#### **(5) その他**

○事務局（総務省(梅城)）から資料6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 暗号利用モード等に関する注釈>**

松本主査 暗号利用モード等を表2に掲載する場合の注釈について、例2では、「量子計算機への耐性を有すると判断する」と記載されているが、使って良いかどうか明確に記載されていないため、例1のように直接記載することが分かりやすいのではないか。

岩田構成員 例1の「表2に掲載する場合には、表2に掲載された暗号技術と組み合わせて利用することを前提とする」という表現は、注釈としてやや違和感がある。「表2に掲載された暗号技術を利用する場合には、」等の表現の方が自然ではないか。

松本主査 「暗号技術」という表現だけでは、暗号利用モード同士を組み合わせる場合も入ると読む人がいないとも限らないため、ブロック暗号や共通鍵暗号等、組み合わせる対象となる暗号技術をより具体的に記載した方がよいのではないか。

総務省(梅城) 現行リストの注釈では「いずれかの暗号技術」と記載しているため、それに合わせた案としている。

松本主査 今回注釈を見直すのであれば、現行の表現に必ずしも合わせる必要はなく、解釈が一意となるよう、より明確な表現に修正することが適当と考える。

國廣構成員 「表2に掲載された」という過去形の表現にも違和感がある。

総務省(梅城) 現行の書きぶりを踏まえた表現としていたが、文言を検討したい。

##### **<検討ポイント② 現行暗号に係る暗号技術の注釈の取扱い>**

総務省(梅城) XTSを表2に掲載する場合、組み合わせるブロック暗号についても表2の暗号技術から選択する必要がある旨を明記した方がよいと考える。次回、修正版を提示したい。

松本主査 認証付き秘匿モードに係る注6についても、基本的には現行注釈を維持しつつ、組み合わせるブロック暗号の範囲を表2に限る必要があると考える。

岩田構成員 注6の「CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせ、『認証暗号』として使うことができる」との記載の趣旨を確認したい。

松本主査 認証暗号の欄にはChaCha20-Poly1305しか記載されていないが、ブロック暗号とCCMやGCM等の認証付き秘匿モードを組み合わせることで認証暗号として利用できるため、その旨を示すための注釈と理解している。

細山田構成員 SHAKEに係る「注4」について、SHAKE128はそもそも対象外と理解している。SHAKE256は、「ハッシュ長は256ビット以上」との条件をそのまま用いるとCategory 2相当となるため、表2では、例えば384ビット以上とするなど、Category 1・2を掲載しない方針との整合を取る必要がある。

松本主査 SHAKEについては次の検討ポイントとも重なるので、次の検討ポイントに議論を移したい。

##### **<検討ポイント③ 現行暗号に係る暗号技術のカテゴリの取扱い>**

細山田構成員 SHAKE128はcapacityが256ビットであり、SHA-256と同様の水準となるため、Category 1・2を表2に掲載しない整理を踏まえれば、掲載しないことが適当と考える。

一方、SHAKE256はcapacityが512ビットあり、出力長を十分長く設定すれば既知の衝突攻撃に必要なコストも十分に大きくなるため、出力長を384ビット以上とするなどの条件を付した上でCategory 4と整理してよいと考える。

岩田構成員 SHAKE256の整理について理解した。暗号利用モード及びメッセージ認証コード並びにChaCha20-Poly1305を掲載し、SHAKE128を掲載しないという方向性についても問題ない

と考える。

総務省(梅城) 暗号利用モードやメッセージ認証コードについて、資料では「Category 1, 3, 5」と記載する案と、セキュリティカテゴリー自体を付さない案の双方を示しており、検討いただきたい。

高木構成員 先ほど須賀構成員からも意見があったように、暗号利用モード自体に「Category 1, 3, 5」等を付すのではなく、「利用する共通鍵暗号のセキュリティカテゴリーに準ずる」といった記載が適切ではないか。

松本主査 暗号利用モード自体に独立したセキュリティカテゴリーを付すよりも、組み合わせて利用する暗号技術のセキュリティカテゴリーに準ずる旨を記載する方が妥当であり、その方向で整理することとしたい。

#### ＜検討ポイント④ 用語の定義等その他検討すべき事項＞

松本主査 CRYPTRECの文書中で「量子コンピュータ」と「量子計算機」が混在しているため、表記は統一した方がよい。「耐量子計算機暗号」という名称との整合を考えれば、「量子計算機」に統一することも考えられる。資料6では、原則として「量子コンピュータ」とし、「耐量子計算機暗号(PQC)」を例外とする案が示されている。

高木構成員 「耐量子計算機暗号」という用語が既に用いられていることから、「量子計算機」とする考え方もある。また、「カテゴリー／カテゴリ」等、外来語の長音表記についてもCRYPTREC文書内で統一した方がよい。

総務省(梅城) 昨年度の暗号技術検討会報告書では「量子コンピュータ」に統一し、「耐量子計算機暗号」のみ例外として用いた。一方、「パラメーター」等も含め、外来語の長音表記について統一する必要がある。文化庁の外来語表記のルールやJISの改定もあった認識。

垣内構成員 外来語表記については、JISや文化庁の表記に合わせる方向で見直された経緯がある。

松本主査 用語についてはCRYPTREC文書内で表記が混在しないよう、事務局で整理した上で次回確認することとしたい。

○事務局(総務省(遠藤))から、次回会合日程等について連絡。

以上