

耐量子計算機暗号（PQC）リスト検討タスクフォース（第3回） 議事概要

1. 日時

令和8年9月16日（水） 16:00～18:00

2. 場所

A P 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(NCO)（杉本貴之）

<ヒアリング対象>

NTT社会情報研究所（永井彰、高屋和幸）

<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）

国立研究開発法人情報通信研究機構(NICT)（小川一人）

独立行政法人情報処理推進機構(IPA)（神田雅透）

4. 議事概要

(1) NTRUについて

○設置要綱の3(7)の規定に基づき、NTT社会情報研究所の永井氏、高屋氏を説明者として、NTRUについて資料2に基づき説明。その後の質疑応答は次のとおり。

<標準化・展開について>

漆畠構成員 NTRUのOSS実装について、Open Quantum Safeには対応しているとの説明があったが、OpenSSLへの対応についてはどのような状況か。

NTT社会情報研究所(永井) ソフトウェアVPNでの利用を念頭に、まずOpen Quantum Safeのliboqsへの対応を優先した。liboqsに対応することで、IPsecで利用されているstrongSwanでも利用可能となる。OpenSSLへの対応も目標としており、今後、OpenSSLで採用されるよう活動していく予定である。

須賀構成員 NTRUに関するIETFのInternet-Draftについて、現時点では期限切れとなっているように見えるが、今後も継続して更新していくとの理解でよいのか。

NTT社会情報研究所(永井) 御理解のとおり。現時点で期限切れとなっているInternet-Draftはあるが、仕様の更新活動自体を停止しているわけではなく、Git上で仕様の更新を進めている。特に「NTRU Key Encapsulation」については、Cisco及びカナダでPKI事業を行うEntrustと連携して作業を進めており、現在、更新内容についてプルリクエストを提出している。これが確認・反映されればInternet-Draftも更新され、期限切れの状態は解消される見込みである。

須賀構成員 Internet-Draftはindividual draftとの理解でよいのか。また、今後どのグループで議論していく予定か。加えて、複数の事業者が共同で仕様を作成するのであれば、相互接続性の確保も必要になると考えるが、どのように進める予定か。

NTT社会情報研究所(永井) individual draftである。議論のグループは資料13ページのそれぞれ1ポツ目に記載のとおり、1番と2番はCFRG、3番はIPSECMEである。また、RFC化に向けては相互接続性を示すことが必要であるため、特にNTRUのKEM仕様についてはCisco及び

Entrustと連携して進めている。今後、NTTで実装したものをCiscoにも実装してもらい、VPNの接続試験を行うことを考えている。

須賀構成員 現時点ではdraftも初期段階であり、様々な関係者を巻き込み、NTRUが実際に普及するところまで進めていただきたい。

NTT社会情報研究所(永井) NTTだけで進めることは難しいため、Cisco等と連携して進めることを基本的な戦略としている。それによってIETFにおいても認められるようにしていきたい。

NC0(杉本) NTRUを今後普及させていくに当たり、国内企業とはどのような協業を行っているのか。また、将来的にターゲットとしている国や地域があれば伺いたい。

NTT社会情報研究所(永井) 国内については、資料9ページに記載のGlobalPlatformを通じて、NTTグループ以外の事業者とも連携しながら、ICカードへのNTRUの実装や性能検証を進めている。国外については、特定の国・地域をターゲットとしているわけではないが、Ciscoはグローバルに事業を展開しており、また、NTTグループも海外で事業を展開しているため、これらを通じてNTRUを利用したPQC対応製品を展開していきたいと考えている。

<Category 1について>

高木構成員 NTRUについてはCategory 1が特徴として挙げられているが、Category 3以上を利用することとなった場合に何か問題はあるか。

NTT社会情報研究所(永井) 欧州全体として192ビット以上とするコンセンサスが得られている状況ではないと認識している。特にICカード等では、128ビットから192ビットとすることによる産業上の影響が大きいと、128ビットという選択肢は現時点では残されていると認識している。

高木構成員 本年3月にCRYPTRECで公表したリストではCategory 1を掲載していないが、その点についてどのように考えているか。また、Category 3以上のみとなった場合、NTTとして社会実装上の問題はあるか。

NTT社会情報研究所(永井) 128ビットについては期限にもよるが、現時点から選択肢をなくすのではなく、もう少し後でもよいと考えている。一方、Category 3以上のみとなった場合でも、社会実装上は問題ない。Category 1も使えるとよいが、日本では2040年以降は192ビットとすると認識しており、それと整合していれば問題はないと考えている。

(このほか、サイドチャネル攻撃耐性と実装性能について議論があった。)

(2) 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

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

<安全性評価等の対象選定について>

漆畠構成員 安全性評価の対象として、LMS・XMSSといったステートフルなハッシュベース署名も検討する必要があるのではないか。米国ではCNSA 2.0においてコード署名にLMS・XMSSを利用することとされており、米国の製品やOS等で利用されるようになった場合、日本でもそれらを利用する可能性がある。CRYPTREC暗号リストに掲載されていないことで利用上の問題が生じないよう、評価を進める必要があると考える。

松本主査 まず、検討すべき暗号技術としてはLMS・XMSSも含めるべきと考える。その上で、CRYPTREC暗号リストがどこまでを対象とするのか、例えば組込み機器のファームウェアまで対象に含めるのかについても整理する必要がある。また、安全性評価にはリソース上の制約もあるため、評価対象の選定と評価スケジュールの双方を考える必要がある。

漆畠構成員 CRYPTREC暗号リストは政府調達のみならず、民間の制度等でも参照されている。例えば、総務大臣認定のタイムスタンプにおいてもCRYPTREC暗号リストに掲載された暗号技術を利用することが要件となっている。CRYPTREC暗号リストで認められていない暗号技術を使う場合には追加説明が必要になるため、今後広く利用されそうな暗号技術については、可能な限りCRYPTREC暗号リストでカバーされていることが望ましい。

NC0(杉本) 政府統一基準では、原則として電子政府推奨暗号を利用することとしており、推奨候補暗号リスト等についても一定の場合に利用できる旨を規定している。現状では、例えばML-KEM以外のPQCを利用すると統一基準に適合しないこととなる。利用者としては、安全性について個別に判断するのではなく、CRYPTREC暗号リストに掲載された暗号を利用でき

ることが望ましい。

須賀構成員 民間の立場から、暗号技術が利用されるのであれば、それがCRYPTREC暗号リストに掲載されていないことは望ましくない。一方、安全性評価等には時間やリソースを要するため、今後評価する予定の暗号技術を「評価対象リスト」のような形であらかじめ示すことも考えられるのではないか。

松本主査 評価対象として示した後に、安全性評価の結果として採用できないこととなる可能性には留意が必要である。

須賀構成員 評価の結果として採用できないのであれば、それはやむを得ないと考える。

<評価対象を選定する観点について>

須賀構成員 暗号アジリティの観点から候補となる暗号技術の幅を広く持つべきと考える。また、評価対象の選定として(A)・(B)・(C)の観点が示されているが、中立的に評価していくことが重要で、理由を説明できるようにしておく必要がある。

総務省(梅城) 御指摘の点に対応できるよう、(A)・(B)・(C)の観点を総合的に勘案することとして資料を作成している。

高木構成員 (A)・(B)・(C)の基準は妥当と考える。LMS・XMSSについても、安全性について十分な実績があり、標準化され、実際に利用する者もいるのであれば、用途はファームウェア署名等に限定されるかもしれないが、評価対象に含めることが適当と考える。また、LMS・XMSS以外にも評価すべき暗号技術が今後次々に出てくると、評価リソースの観点から対応が難しくなるため、ほかに対象となり得る暗号技術がないか確認する必要がある。

NCQ(杉本) 政府機関が調達する際、CRYPTRECに掲載されていない暗号技術について各省庁が個別に安全性を確認することは困難である。このため、政府機関が利用する可能性が高い暗号技術については、CRYPTRECで安全性を評価することが望ましい。また、一度に全てを評価することが難しいのであれば、今後どの暗号技術をどのような順序で評価する予定かを示すことで、利用者側の予見可能性を確保することも有用である。

松本主査 (A)安全性の成熟度、(B)標準化の成熟度、(C)実利用の具体性、の3点を総合的に勘案して安全性評価等の対象を定めることとし、資料に示されたFN-DSA、HQC、NISTで追加公募中の署名方式及びNTRUIに加え、LMS・XMSSについても安全性評価等の対象とすることとしてよい。

(異論なし)

総務省(梅城) 次回の資料にLMS及びXMSSを追加するとともに、利用状況等についても確認して資料に加えたい。また、LMS及びXMSSについては、ステートフルな署名方式であり、これまでCRYPTREC暗号リストで取り扱っていないため、ステートの管理方法を含め別途検討が必要になると考える。

松本主査 利用方法に関する注意事項も必要になると考える。

(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(小川))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。

岩田構成員 資料5ページで、オランダやチェコにおいて量子耐性があるとされている認証暗号について、組み合わせるブロック暗号の鍵長等について条件は付されているのか。また、資料3ページの暗号利用モードについても、組み合わせるブロック暗号等による条件があるのか。

NICT(小川) チェコについては、量子耐性を有するブロック暗号やハッシュ関数を組み合わせることが条件とされている。一方、どのブロック暗号やハッシュ関数が量子耐性を有するとされているかまでは今回確認していないため、改めて確認する。

岩田構成員 英国では、暗号利用モード等について資料全体で「記載なし」とされているように見えるが、実際にはどのような暗号利用モードを利用しているのか。また、フランスについても同様に、何も利用できないようにも見えるため確認が必要ではないか。

NICT(小川) 英国については米国に準じた利用をしていると認識しているが、根拠となる記載を含め、改めて確認する。フランスについても併せて確認する。

須賀構成員 岩田構成員の先ほどの質問について、オランダについては、例えばGCM自体は推奨されるアルゴリズムとして記載されている一方、実際にTLS等で利用する場合には128ビット

ト又は256ビットの鍵長とするなど、利用場面ごとに別途条件が付されている。
松本主査 今回の調査結果については参考情報として指摘の点を修正・精査した上で、今後の議論に活用することとしたい。

(4) 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5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・②について＞

松本主査 資料2ページの検討ポイント①及び資料7ページの検討ポイント②については認識に相違がないか。

（異論なし）

＜検討ポイント③（Category 1・2の取扱い）について＞

松本主査 ML-DSA-44やSLH-DSAのCategory 1のパラメータセットについて、諸外国の推奨状況、標準化状況、実装状況等を踏まえ、CRYPTREC暗号リストに掲載するか改めて意見を伺いたい。

総務省(梅城) 調査をした結果として、ML-DSA-44については、Cloudflare等で利用されている例はあるものの、現時点で広く利用されている状況ではなく、今後デファクトとして普及していくかも明確ではない。一度リストに掲載すると、実際のシステムで利用されるため後から外すことが難しくなることも踏まえると、現時点で掲載するか否かを判断できる状況にあるか悩ましい。

漆畠構成員 署名のPQC移行はまだ十分に進んでおらず、現時点で利用例が少ないことのみを理由にML-DSA-44を除外することは適当ではないと考える。次世代のTLS証明書であるMerkle Tree Certificate等でもML-DSA-44が利用されており、今後、エンドエンティティの署名や、性能が求められるTLS等においてML-DSA-44が利用される可能性は高いと考える。

松本主査 SLH-DSAのCategory 1についてはどうか。

漆畠構成員 SLH-DSAは署名サイズが非常に大きいため、現時点ではCategory 1のパラメータセットを利用しなければならない具体的なユースケースはそれほど多くないと考える。

須賀構成員 ML-DSAについて、推奨状況だけでなく実装状況も含めて確認しているが、現時点では判断できる状況にないため保留としたい。

松本主査 ML-DSA-44及びSLH-DSAのCategory 1の取扱いについては、引き続き検討することとしたい。

（異論なし）

＜検討ポイント④（Camellia・KCipher-2・SHAKEの取扱い）について＞

松本主査 Camellia、KCipher-2、SHAKE128及びSHAKE256について、前回までの議論を踏まえて事務局から示された案について意見を伺いたい。

岩田構成員 合理的な方針であると考ええる。

細山田構成員 合理的な方針であると考ええる。

漆畠構成員 SLH-DSAのパラメータセットに「SHAKE-128」という記載があったが、SHAKE128をリストに掲載しない場合との関係を確認する必要があるのではないか。

松本主査 その点については確認することとし、SHAKE128の取扱いについては保留としたい。

（異論なし）

＜検討ポイント⑤（暗号利用モード等の取扱い）について＞

松本主査 暗号利用モード及びメッセージ認証コードについては表2に掲載し、認証暗号についても表2に掲載する一方、エンティティ認証については引き続き掲載を保留するとの整理でよいか。また、暗号利用モード等に付す注釈についても、事務局案を基本として進めることとしてよいか。

（異論なし）

(5) 課題③ ハイブリッド構成の取扱いについて

○事務局（IPA(神田)）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。

漆畠構成員 ハイブリッド構成については、まず用語の定義を整理する必要がある。また、方針についてコンセンサスを得た上で、個別の議論に入ることが望ましい。

松本主査 本件については、次回以降、引き続き議論することとしたい。

(6) その他

○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