耐量子計算機暗号（PQC）リスト検討タスクフォース（第４回）　議事概要

１．日時

令和８年10月５日(月) 16:00～18:40

２．場所

経済産業省本館17階　第２特別会議室

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（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）

＜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、高和馬）
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) 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２に基づき説明。その後の質疑応答は次のとおり。

漆嶌構成員　資料２の２ページにおいて、「米国CNSA 2.0ではソフトウェア署名にML-DSAも認められている」と記載されているが、コード署名についてはLMS及びXMSSがプライマリーとされていたと記憶しており、ML-DSAも同様に扱ってよいのか懸念がある。また、CNSA 2.0におけるML-DSAの利用については、ML-DSA-87に限定されていることや、事前ハッシュが禁止されていることなどの条件があったと認識している。こうした条件をCRYPTREC暗号リストにおいてどのように反映するのかについても確認が必要ではないか。

総務省(梅城)　調査した範囲では、LMS及びXMSSがプライマリーであるとの明確な記載は確認できていない。CNSA 2.0本体ではML-DSAが記載されておらず、その後のFAQにおいて利用が認められていることが、そのような認識につながっている可能性はある。ML-DSAの利用に係る条件と合わせて改めて確認したい。

松本主査　これらの点については、事務局において引き続き確認することとしたい。

垣内構成員　資料２の８ページに記載されたMicrosoftの対応状況について、Windows Server 2025のActive Directory Certificate Servicesにおける証明書発行機能への対応と、OS自体における暗号アルゴリズムへの対応は区別する必要がある。OSとしての対応状況については、LMS及びXMSSは既に内部ライブラリに実装されているほか、SLH-DSAについても対応がロードマップに含まれている。

松本主査　８ページは参考扱いであり確認できた範囲でアップデートすることが望ましい。

須賀構成員　安全性評価等を進める際の優先順位は、本タスクフォースで議論するのか。また、資料２の３ページにある表に記載された順番で評価を進めることを想定しているのか。

松本主査　評価の優先順位やスケジュールについては、基本的に暗号技術評価委員会において検討することを想定している。ただし、本タスクフォースとして留意すべき事項があれば、意見を示すことは可能と考える。また、資料２の３ページに記載された順番で評価を進めることを想定しているわけではない。

総務省(梅城)　各暗号技術の標準化の進展状況等も踏まえながら、評価スケジュールを検討する必要があると認識している。

(2) 課題①・② Category 1・2及び暗号利用モード等の取扱いについて

〇事務局（NICT(高)）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。

細山田構成員　今回の諸外国動向調査について、フランスにおける暗号利用モード等に関する記載は確認されなかったのか。

NICT(高)　フランスについても調査を行ったが、CRQC対応に関する記載は確認できなかった。従来の暗号技術に関する記載は存在する可能性があるが、今回の調査結果には含めていない。

松本主査　フランスについても調査したものの、CRQC対応に関する記載が確認できなかったという理解でよいか。

NICT(高)　御理解のとおり。

岩田構成員　資料３の６ページにおいて、チェコでは128ビット又は192ビットの鍵長の暗号は量子計算機に対して脆弱であるとされているが、これはAES-192等も含め、CRYPTREC暗号リストにおけるCategory 3に相当する暗号技術についても推奨しないという理解でよいか。

NICT(高)　チェコでは、AES等についても256ビットの鍵長を使用することが推奨されている。

岩田構成員　チェコでは、CRYPTREC暗号リストにおけるCategory 3に相当する暗号技術についても推奨していないということと理解した。各国の暗号政策は必ずしも一致する必要はなく、それぞれの方針に基づいて定められるものであるが、CRYPTRECの方針と諸外国の方針に相違があることは認識した上で、今後の検討を進めることが望ましい。

松本主査　今回の調査結果については、今後の議論の参考とすることとし、追加情報があれば適宜更新することとしたい。

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③：ML-DSA・SLH-DSAの実装・利用状況について＞

松本主査　資料４の12ページに記載された利用・実装状況について、資料２の８ページに記載された調査結果との整合性は確認されているか。

総務省(梅城)　資料２はLMS及びXMSSを中心に調査しており、その用途はどうしても限られてしまう。一方、資料４の12ページでは署名方式が利用される幅広い用途を対象としている。このように、調査対象の観点が異なるため別々に整理している。

＜検討ポイント③：ML-DSA-44のセキュリティカテゴリについて＞

高木構成員　ML-DSA-44を掲載するか否かの議論の前に、資料４の13ページに、暗号技術評価委員会で話題になった件が記載されている。ML-DSA-44について、鍵生成に用いる乱数生成器のセキュリティ強度が192ビット未満の場合、セキュリティカテゴリがCategory 1となる。また、ML-DSA-44をCategory 2として掲載するのであれば、その条件として乱数生成器のセキュリティ強度に関する条件をML-DSA-44の条件として注記する必要がある。

漆嶌構成員　ML-DSA-44は、エンドエンティティ証明書やMerkle Treeを利用した仕組み等、様々な用途で利用が見込まれている。このため、ML-DSA-44を掲載対象から除外した場合、海外等で利用されている技術がCRYPTREC暗号リストでは利用できなくなる可能性があり、懸念がある。例えば、TLSで利用するエンドエンティティ証明書にML-DSA-44が使用されることが考えられるが、その際の乱数生成器のセキュリティ強度については、特段の制限がないと認識している。

松本主査　Category 1となるML-DSA-44についても利用できるようにする必要性がどの程度あるかが重要であり、Category 2となるものに限定できるのであれば、そのように整理すればよい。

須賀構成員　ML-DSA-44については、Category 1・2の利用に関する一般的な注釈と、乱数生成器のセキュリティ強度に関する注釈の両方が必要になると理解したが、利用者にとって分かりやすい記載とする必要がある。

総務省(梅城)　192ビット以上のセキュリティ強度を持つ乱数生成器に限定する場合には、「ML-DSA-44」に注釈を付すことになると考える。一方、128ビット以上192ビット未満の乱数生成器の利用も許容するのであれば、「Category 2」に注釈を付し、特定の場合にはCategory 1となる旨を記載することになると考える。

松本主査　ML-DSA-44について、乱数生成器の条件に応じて２行に分け、Category 1とCategory

2をそれぞれ記載する方法も考えられるのではないか。

総務省(梅城)　一般の行政職員にとっては、同一の暗号技術が２行に分かれている場合に、その意味が理解できないと考えられ、１行で記載する方が分かりやすいと考える。

國廣構成員　Category 2を掲載する理由は広く利用される可能性があるためと理解しており、Category 1となるML-DSA-44が実際にどの程度利用されるかを踏まえて判断する必要がある。Category 1の利用実態がないのであれば、Category 1については掲載しない方が、今後の方向性とも整合的ではないか。

高木構成員　Category 2を掲載する場合、それはいつまで使えるのか。2035年以降、５年間は使うが10年後には使わなくなるといった予見があれば、一定期間後に見直すことや、利用期限を注記することも考えられる。

松本主査　これまでのCRYPTREC暗号リストでは、将来の利用期限をあらかじめ示すのではなく、改定時点で利用可能な暗号技術を示してきたため、利用期限を設ける場合には、その実現可能性や政府調達への影響を検討する必要がある。

総務省(梅城)　製品等の内部で利用される乱数生成器のセキュリティ強度を外部から把握することは難しく、利用実態を調査するには個々の事業者への確認が必要になると考えられる。
　また、Category 1とCategory 2については、現時点ではいずれも原則として掲載しない方向で一緒に検討している。そのため、ML-DSA-44を掲載する場合、Category 1よりCategory 2が望ましいといった区別をそもそもする必要があるのかという点も議論が必要である。

國廣構成員　Category 1・2の取扱いについては、現行暗号リスト（表１）の今後の取扱いを決めるタイミングと合わせて検討することも考えられる。

総務省(梅城)　その場合、PQCへの移行が進む2035年以降の時期という程度しかわからない。

須賀構成員　可能性論として、CRYPTREC暗号リストには過去に擬似乱数生成器が掲載されていたことも踏まえ、乱数生成器に関する規定を改めて設けることも考えられるのではないか。具体的なアルゴリズムを指定するのではなく、192ビット以上のセキュリティ強度を持つ乱数生成器の利用を推奨する旨を記載すれば、個別の実装状況を調査することなく、必要なメッセージを示せることとなる。

IPA(神田)　過去のCRYPTREC暗号リストでは、擬似乱数生成器は「例示」として掲載されていたと記憶している。

松本主査　乱数生成器に192ビット以上のセキュリティ強度を求める方法も考えられるが、既に広く利用されている暗号技術がCategory 1に分類される場合、実務上の問題が生じる可能性がある。このため、実際の利用状況を把握することが望ましいが、調査は可能か。

須賀構成員　乱数生成器の仕様は製品等の内部情報に当たるため、アンケートや事業者へのヒアリングによっても実態を把握することは難しいと考える。

総務省(梅城)　政府調達では、システムインテグレータ等がCRYPTREC暗号リストを参照して製品や部品を調達するため、CRYPTREC暗号リストで内部の乱数生成器に192ビット以上のセキュリティ強度を求めたとしても、実際にその条件を確認して調達することは難しいのではないか。そうであれば、理念はともかく実務が回らない。また、Category 1・2は同列に取扱いを検討しており、Category 1を必ずしも排除する必要はないのではないか。このため、仕様上認められている128ビット以上の乱数生成器の利用を許容しつつ、Category 1となる場合があることを注記する方法も考えられるのではないか。

松本主査　乱数生成器のセキュリティ強度が確認できず、Category 1とCategory 2のいずれに該当するか判断できない場合には、Category 1として扱わざるを得ないのではないか。

細山田構成員　Category 1・3・5はブロック暗号の鍵探索、Category 2・4はハッシュ関数の衝突探索を基準としているため、異なる尺度に基づくカテゴリをCategory 1から5まで一律に強度の順序として扱えるのか確認したい。特に、ML-DSA-44について「Category 2からCategory 1に低下する」と表現することが適切なのか疑問がある。

総務省(梅城)　NISTの2016年の文書に定義があり、Category 1から5までが「強度の低い順に記載」と表記されている。一方、CRYPTRECにおけるこれまでの議論では、異なる尺度で定義されたカテゴリは、厳密には比較できないのではないかという指摘もあった。なお、「低下する」という表現はFIPS 204における記載を訳したものであり、日本語としての表現については精査が必要である。

IPA(伊藤)　NISTのセキュリティカテゴリは、PQC標準化公募の際に設定されたもので、概ね数字の順番どおりの強さに見えてはいるが、厳密な強度の順序が証明されているわけではないと認識している。一方、量子回路による攻撃等を考慮すると、Category 1から5までの順に必要な計算資源が大きくなるという認識があると理解している。こうした定義の性質を踏まえて整理する必要がある。

＜検討ポイント③：ML-DSA-44の掲載について＞

松本主査　ML-DSA-44の表２への掲載自体についてはどう考えるか。特に、PKI等の証明書において、ML-DSA-44が長期的に利用される可能性はあるか。

漆嶌構成員　ML-DSAを証明書に利用する場合、データ通信量の増加が課題となるため、ML-DSA-44よりも署名長等が大きい方式を利用することは難しい面があると考える。

國廣構成員　128ビットの安全性を持つ暗号技術については、2040年が一つの目安になると考えられるが、利用期限を2040年と明記すると、それまでは利用してよいというメッセージになりかねない。このため、具体的な利用期限をどのように設定するかについては慎重な検討が必要と考える。

松本主査　政府機関等には長寿命のシステムも多く、導入後に暗号技術を変更することは容易ではないため、現在の調達可能性と将来的な移行の必要性の両方を考慮する必要がある。

IPA(伊藤)　ML-DSA-44を採用しようとしている事業者の中には、ソフトウェアによる実装で暗号技術の入替えが比較的容易であることから、当面の間、軽量な方式としてML-DSA-44を選択している例があると認識している。このような用途であれば、Category 1・2について定期的に見直す旨を注釈に記載し、必要に応じて暗号技術を変更できる場合に利用を認めることも考えられる。一方、長寿命のシステムへの採用については慎重になるような記載が望ましいと考える。

NCO(杉本)　政府調達では、例えば、2035年に調達したシステムを５年間利用すると2040年に達することも想定されるため、Category 1・2の取扱いについては、このような場合と2035年という移行期限との整合性を考慮する必要がある。

　また、諸外国ではML-DSA-44を推奨する例があまり確認できず、国際的な通信の相手方が当該方式を受け入れない可能性も考慮する必要がある。技術的な観点だけでなく、政府調達や国際的な相互運用性の観点からも、一貫性のある方針が望ましい。

松本主査　ML-DSA-44の利用を認めると、利用が増え、将来的な変更が難しくなる。先ほどIPAの意見でもあったように、現在の実装を変更できるなら、ML-DSA-44を入れなくても良いという考えもあるがどうか。

漆嶌構成員　ML-DSA-44については、DNSSECや証明書等の様々な用途で当面利用されることが見込まれ、民間では５年から10年程度利用される可能性もあると考える。また、仕様策定やスマートカード等の製品開発が進んだ場合、一度採用した暗号技術を短期間で変更することは容易ではない。このため、政府調達においてML-DSA-44の利用を制限した場合の影響についても検討する必要がある。

松本主査　ML-DSA-44については、今回改定するCRYPTREC暗号リストに掲載する方向で概ね合意が得られたものと考えてよろしいか。一方、Category 1となる場合の取扱いや、掲載に当たっての具体的な条件及び注釈の記載方法については、引き続き検討する必要がある。

須賀構成員　ML-DSA-44を表２ではなく表１に掲載する方法も考えられるのではないか。表１に掲載されていれば、政府調達上の問題を回避できる可能性がある。

松本主査　PQCへの移行を進める観点からは、表２に掲載されている暗号技術を利用する必要があるため、表１への掲載は適当ではないと考える。

NCO(杉本)　現行の政府統一基準からすると、原則として、電子政府推奨暗号リストに掲載された暗号技術を利用することとなると考えられるため、現時点では表１に掲載されていれば調達上の問題はない。一方、今後、表１の取扱いが変更された場合には、新規調達が認められなくなる可能性がある。また、表２に掲載された暗号技術が短期間で利用できなくなることも、調達側の予見可能性の観点から問題となるため、将来の取扱いを考慮する必要がある。

松本主査　ML-DSA-44を表１に掲載することは適当ではないと考えるため、表２に掲載する方向

とし、具体的な掲載条件や注釈の記載方法については、次回会合で引き続き検討することとしたい。

IPA(神田)　過去のCRYPTREC暗号リストでは、トリプルDES等について、代替となる暗号技術が利用可能な場合にはそちらを使用する旨の注釈を付した例があったと記憶している。ML-DSA-44についても、こうした注釈の記載方法が参考になるのではないか。

＜検討ポイント③：SLH-DSAの取扱いについて＞

松本主査　SLH-DSAのCategory1の部分は掲載しないことでよいか。

総務省(梅城)　SLH-DSAについては、署名長等が大きいこともあり、現時点ではML-DSAと比較して利用が限定的であると認識している。このため、Category 1まで掲載対象を広げる必要性は高くないと考える。

松本主査　SLH-DSAの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。

（異議なし）

総務省(梅城)　今後、SLH-DSAのCategory 1の利用状況が変化した場合には、改めて暗号技術検討会等で掲載の必要性を検討することもあり得るという理解でよいか。

松本主査　その理解でよい。現時点では掲載しないこととし、今後の利用状況等に応じて改めて検討することとしたい。

＜検討ポイント④　SHAKE128の取扱い＞

松本主査　SHAKE128については、単独では表２に掲載しないこととしてよいか。

（異議なし）

松本主査　SHAKE128については、単独では表２に掲載しないこととしたい。

＜検討ポイント⑥　暗号利用モード等に関する注釈＞

松本主査　資料４の17ページにおける注Ａについて、注Ｂでは表２に掲載された暗号技術との組合せを規定している一方、注ＡではCRYPTREC暗号リストに掲載された暗号技術との組合せとしており、表２の暗号技術も含まれるように読める。注Ａについても表１に限定した方がよいのではないか。

総務省(梅城)　注Ａは現行の暗号リストの記載を踏襲したものである。推奨候補暗号リストに掲載された暗号技術等との組合せも認める趣旨で、対象を限定しない記載としていたと認識している。この考え方については、資料に補足説明を追加したい。

松本主査　注Ａ及び注Ｂについては、事務局案の記載を維持しつつ、注Ａで対象を表１に限定していない理由を資料に補足することとしてよいか。

（異議なし）

＜検討ポイント⑦　暗号利用モードに係る注釈の取扱い＞

松本主査　資料４の18ページにおける注Ｄについても、注Ａと同様に、組み合わせる暗号技術を表１に限定する記載とすることが考えられるが、推奨候補暗号リストに掲載された暗号技術との組合せも認めるという従来の考え方を踏まえ、事務局案の記載を維持することとしてよいか。また、表１に限定しない理由については、資料への追記が望ましい。

（異議なし）

松本主査　それでは、注Ｄについては事務局案の記載を維持し、その理由を資料に補足することとしたい。

＜検討ポイント⑧　用語・表記の統一＞

総務省(梅城)　長音表記については、原則として長音を付すことが適当と考える一方、「コンピュータ」「パラメータ」「カテゴリ」等については、CRYPTRECや政府の文書でも長音を付さない表記が多く使用されているため、一定のルールを設けて統一したい。

松本主査　長音表記については、資料４の19ページに示された具体例に従って統一することとしてよいか。

（異議なし）

松本主査　また、「量子コンピュータ」と「量子計算機」については、既に定着している「耐量子計算機暗号（PQC)」という名称は維持しつつ、政府の文書等で用いられている「量子コンピュータ」を基本とすることが適当と考える。その上で、両者が同義であることが分か

るよう、初出時に「量子コンピュータ（量子計算機）」と記載してはどうか。

総務省(梅城)　政府のサイバーセキュリティ戦略では「量子コンピュータ」を使用しており、「耐量子計算機暗号（PQC）」については固有の名称として扱っている。CRYPTRECにおいては松本主査の提案の表記方法で問題ないと考える。

松本主査　「耐量子計算機暗号（PQC）」という名称との関係を明確にするため、「量子コンピュータ」と「量子計算機」が同義であることを示す必要がある。このため、「量子コンピュータ」を基本とし、初出時には「量子計算機」を括弧書きで併記することとしたい。

（異議なし）

＜改定イメージ　SHA-3及びSHAKEの分類について＞

総務省(梅城)　SHAKEはSHA-3の系列として扱われる場合もあるため、暗号リストにおいてSHA-3とSHAKEを統合して記載することも考えられるが、いかがか。

岩田構成員　SHAKEがFIPS 202においてSHA-3とともに規定されているのであれば、まとめて記載することも合理的と考える。

細山田構成員　SHA-3とSHAKEでは、ハッシュ値を計算する際のパディング処理等の内部処理が異なると認識しており、同一の関数として扱うことには違和感がある。

総務省(梅城)　FIPS 202の表題は「SHA-3 Standard」となっており、概要においても、SHA-3ファミリーには４種類のハッシュ関数（SHA3-224、SHA3-256、SHA3-384及びSHA3-512）と、２種類の可変長出力関数（SHAKE128及びSHAKE256）が含まれると記載されている。このため、SHAKEをSHA-3の系列として整理することも考えられる。

岩田構成員　FIPS 202の記載を踏まえると、SHAKEをSHA-3ファミリーの一つとしてまとめて記載することも合理的と考える。一方、SHA-3とSHAKEは機能が異なり、同一の分類として扱うことには違和感もあるため、現行の分類を維持することでもよいと考える。

松本主査　SHA-3とSHAKEは同じファミリーに属するものの、異なる名称及び機能を持つことから、原案のように分けて記載することでよいのではないか。

岩田構成員　SHAKEはハッシュ関数として利用できるものの、可変長出力関数としての特徴もあるため、SHA-3と分けて記載する現行の分類に賛成する。

細山田構成員　FIPS 202においてSHAKEがSHA-3ファミリーに含まれることは理解したが、現行のように分けて記載する方が望ましいと考える。

＜改定イメージ　表内の区切り線について＞

松本主査　暗号リストの表において、一部のセルが結合されており、縦の区切り線がない箇所については、区切り線を追加するのではなく、暗号技術の名称等を適切に字下げすることで、上段の項目との位置関係が分かりやすくなるようにしてはどうか。

（異議なし）

松本主査　それでは、表内の区切り線は原案のままとし、字下げで配置調整することとしたい。

(3) 課題③　ハイブリッド構成の取扱いについて

○事務局（IPA(伊藤)）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。

細山田構成員　ハイブリッド構成に用いるKDF（鍵導出関数）について、現在のCRYPTREC暗号リストにSHA-2やSHA-3等が掲載されているのと同様に、使用すべきKDFを暗号リストに追加することを想定しているのか。

IPA(伊藤)　KDFを暗号リストに追加する方法と、別の文書で整理する方法のいずれも考えられる。資料５の11ページは、あくまで現状についての整理である。

漆嶌構成員　ハイブリッド構成の取扱いを検討するに当たっては、実際に市場でどの程度利用されるかという見通しを踏まえて対象範囲を定めることが重要と考える。例えば、PQ/PQハイブリッドや、IETFがメインストリームになるのであればETSIの定義等については詳細に検討する必要性は低いのではないか。

　また、資料５の最終ページに示された案１～４について、タスクフォースとしてまずどの方針とするかを決めた方が、議論の方向性を決めやすいのではないか。個人的には案４が適当と考える。CRYPTREC暗号リストは従来から暗号プリミティブを掲載するものであり、例えばメッセージ認証コードについて、組み合わせるハッシュ関数等を個別に指定してき

たわけではない。このため、ハイブリッド構成についてもML-KEMやML-DSA等の暗号プリミティブを掲載するにとどめ、具体的な組合せについては原則として規定しないことが適当と考える。組合せに関する仕様の多くはいまだドラフト段階にあり、実装も十分に進んでいないため、現時点で個別の方式を規定することには慎重であるべきと考える。

細山田構成員　具体的な問題を想定しているわけではないが、安全性上の問題が生じる可能性もあるので、KDFの定義や安全性について慎重に検討する必要があるのではないか。

松本主査　ハイブリッド構成についてはTLSで最も実装が進んでおり、TLSでは「TLS暗号設定ガイドライン」を作成して重宝されている。暗号リストに掲載するには技術や標準化の成熟度が十分ではない面があり、現時点で具体的な構成を細かく規定すると、今後の技術の発展を阻害する可能性もある。一方、KDF等については安全性を確保するための適切な選択が重要であり、暗号リストに掲載するか、別の文書とするかが論点となる。

岩田構成員　案１にあるKDFやコンバイナの新設について、KDFやPRF（擬似乱数関数）はハイブリッド構成以外にも様々な用途で利用されるものである。このため、新たに暗号リストに掲載するのであれば、他の用途も考慮した上で検討する必要がある。

松本主査　KDF等を暗号リストに掲載する場合には、対象とする用途や適用範囲を明確にし、それに応じた要件を整理する必要がある。

高木構成員　ハイブリッド構成について、利用者の観点から、どのような構成や使用方法に危険性があり、何を守る必要があるのかをガイドライン等で示すことが重要と考える。また、KDFやPRF等に関して、部品として安全なものをホワイトリストとして整理し、長期的にはCRYPTREC暗号リストへの掲載について議論することが考えられる。

國廣構成員　現時点では案４として、ハイブリッド構成をCRYPTREC暗号リストに直接掲載するのではなく、ガイドライン等の別の文書で整理する方向が適当と考える。

須賀構成員　ハイブリッド構成を現時点で暗号リストに掲載することは時期尚早と考える。一方、将来的にKDFという技術分類を新設し、安全性評価を経たKDFを掲載することは、安全でない使用方法を防ぐという観点から賛成である。その際、例えばETSI TS 103 744には安全性証明が付されていることを踏まえ、掲載に当たっては暗号技術評価委員会において適切な評価を行う必要がある。

松本主査　KDFはハイブリッド構成以外でも広く利用されているため、CRYPTREC暗号リストに特定のKDFを掲載することで、他の用途における利用まで制約することにならないよう注意が必要である。今回の議論では、KDF一般というよりも、ハイブリッド構成におけるコンバイナの構成方法や、その構成要素としてのKDFの取扱いを検討することが適当ではないか。

IPA(伊藤)　KDFには既存のシステム等に組み込まれているものもあるため、いきなり特定のKDF以外はだめだと言われても対応が難しい場合がある。また、別の文書で整理する場合も、コンバイナに用いるKDFを対象として検討することが考えられる。

須賀構成員　ハイブリッド構成については現在も標準化等の議論が進んでいるため、今後も調査を継続し、数年以内を目途にハイブリッド構成に関するガイドライン等を策定することが望ましい。

NCO(杉本)　CRYPTREC暗号リストの利用者の観点からは、システムに利用されている暗号技術が幅広く示されていることが望ましい。また、掲載されていない技術は利用できないと解釈される可能性もあり、整理していく必要がある。技術の変化が激しいのであれば基本的な考え方を示し、技術が固まってくれば具体的な方式を示すということではないか。

高木構成員　ハイブリッド構成は複雑であり、今後、暗号技術の構成や利用方法に起因する深刻な脆弱性が発見される可能性もある。このため、暗号リストやガイドラインの整備に加え、問題が生じた場合に利用者に対して注意喚起を行うことができる体制についても検討しておく必要がある。

松本主査　ハイブリッド構成の取扱いについては、今回の議論で様々な論点が示されたが、現時点で結論を出すことは難しいため、次回会合において引き続き検討することとしたい。

(4) 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