量子コンピュータ時代に向けた暗号の在り方検討タスクフォース（第３回）
議事概要

１．日時
令和元年12月24日（火）10:00～12:00

２．場所
総務省11階　1101会議室

３．出席者（敬称略）
構成員：松本勉、宇根正志、國廣昇、高木剛、松井充、松本泰、満塩尚史
オブザーバ：徳永竜一、山田晃潤、岡野孝子、上根雄大、内山諒子、荒木美敬、村上匠、
藤森英俊、椛木隆慎、衛門愛子、松田隆宏
事務局：（総務省）赤阪晋介、梅城崇師
（経済産業省）鴨田浩明、上田翔太
（国立研究開発法人情報通信研究機構（NICT））野島良
（独立行政法人情報処理推進機構（IPA））神田雅透

４．議事
（１）前回議事概要の確認について
（２）これまでの議論とCRYPTREC暗号リストに関する論点等について
（３）その他

５．配付資料
資料１　第２回会合議事概要（案）
資料２　最近の量子超越性実験による暗号の安全性に関する影響
資料３　これまでの議論とCRYPTREC暗号リストに関する論点等について
参考資料　電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）
参考資料　2011年度第１回暗号技術検討会資料３－２（抜粋）

６．議事概要
６．１．開会
松本勉座長から開会の宣言があった。

６．２．議事
（１）前回議事概要の確認について
資料１の第２回会合議事概要（案）について確認が行われ、原案のとおり承認された。

また、國廣構成員より、令和元年10月の発表を踏まえた量子超越性実験による暗号の安全性に関する影響について資料２に基づき説明が行われた。主な質疑は以下のとおり。

高木構成員：今回発表があった実験に関する量子コンピュータは、アニーリング方式では

なくゲート方式という理解でよいか。ゲート方式であった場合、量子のもつれ状態は数ミリ秒しか保てず、すぐにコヒーレンスが壊れるという理解をしているが、今回の実験時間が200秒というのは、コヒーレンスタイムとの関係はどうなっているのか。

國廣構成員：量子コンピュータはゲート方式である。今回の論文によればサンプル数は10^6とされており、これをサンプルするのに200秒とすると、計算１回当たりでは0.2ミリ秒となる。

宇根構成員：今回の実験ではサンプリングアルゴリズムを用いたということであるが、暗号の安全性に関する考察として、別のアルゴリズムを量子回路で実装したとするとどのような結果となるのか。

國廣構成員：量子コンピュータを何に使うかにもよるが、今回の実験で用いた53量子ビットで1,500程度の量子ゲートでは、乱数を出力する程度しかできない。また、今回の実験は1,500程度の量子ゲートであり、同時に多数の量子ゲートに演算をさせる並列計算をかなり使用しているが、回路の深さは40程度で少ない特殊な計算回路である。もう少し深さのある回路に対して適用できる量子コンピュータがないと、おそらく他のアルゴリズムは動かないかと思う。

松本勉座長：「深さ」というのは、普通の回路の深さと同様で、前の量子ゲートの出力を次の量子ゲートが使い、通常１段、２段と数えるもので40段という理解で良いか。

國廣構成員：ご理解のとおり。まず全ての量子ビットに対してオペレーションを同時に行い、この段階で深さは１である。次の段階で、選択的に２つの量子ビットを選び、片方をコントロールビット、もう片方をオペレーションされるビットにするといったことを10程度行い、そこも全て同時にオペレーションを行うため、深さは１で、それらを20回繰り返すことで、深さの合計が40になる。

松本泰構成員：誤り訂正が可能な4,098量子ビットの量子ゲート型の量子コンピュータを作ることができれば解読できるという理解で正しいか。

國廣構成員：誤り訂正付きとする場合は、その誤り訂正を行うにも量子ビットを多く使うため、10^6程度の量子ビットが必要。ただ、少なくとも4,098量子ビットと10^{12}量子ゲートを達成しないとどんなに頑張っても解読できない。

松本泰構成員：まだ最終確定していないが、量子技術イノベーション戦略の検討において、量子誤り訂正された論理量子ビットとして、50量子ビット程度の量子コンピュータの出現が20年後ぐらいの目標といった記載がある。この50が4,098になったらということか。

國廣構成員：誤り訂正を行う部分が入っているかどうかで数え方が違う。例えば、古典コンピュータの場合でも、３ビットの情報を伝える際に、誤り訂正を加えて７ビットとなったりするのと同じようなイメージ。20年後を考えると、おそらく50量子ビットについて誤り訂正を経てフルに使いたいという状況かと思われる。その誤り訂正を経たものが4,098量子ビットあれば解読できるという理解。

松本勉座長：4,098量子ビットで量子ゲート数が10^{13}程度という記述と、6,146量子ビットで量子ゲート数が10^{12}程度という記述とがあるが、何が異なるのか。

國廣構成員：アルゴリズムが異なり、回路構成に違いが生じる。4,098量子ビットのアルゴリズムについては、少量の量子ビットで計算可能だが量子ゲートを多く必

要とする。6,146量子ビットのアルゴリズムはその逆である。トレードオフの関係であり、どちらかが達成できれば十分である。

松本勉座長：4,098量子ビットが同時にコヒーレントになっている必要はあるのか。

國廣構成員：同時にコヒーレントになっている必要があり、コヒーレントなまま10^{13}個の量子ゲートでの演算を行う必要がある。

松本勉座長：4,098量子ビットよりも量子ビットを減らし、代わりに量子ゲートを増やすことで素因数分解は可能となるのか。

國廣構成員：情報を蓄えるためには4,098量子ビットが必要であり、これを減らすことはできない。しかし、特殊な構成をした数の素因数分解であれば減らすことができ、これまで素因数分解したという成果があるものはそうした数である。

高木構成員：量子ゲート数が10^{13}ということだが、深さはどれくらいか。

國廣構成員：深さもほぼ同じで、10^{13}である。

高木構成員：深さが計算時間につながると思うが、どの程度の時間となるのか。

國廣構成員：今回の発表であれば、200マイクロ秒で深さ40のところ、10^{13}必要となるため、5×10^{13}マイクロ秒である。

事務局（総務省）：計算すると約1.5年。

高木構成員：1.5年、量子状態を保つ必要があるということと理解した。

（２）これまでの議論とCRYPTREC暗号リストに関する論点等について

資料３に沿って、事務局より説明が行われた。主な意見等は次のとおり。

＜論点１－１　リスト構成について＞

松井構成員：「引き続き検討が必要」とあるが、検討を2023年まで続けるという意味か。

松本勉座長：本日の会合で具体的な決定をしないという趣旨であり、意見をお願いしたい。

「推奨候補暗号リスト」も含めて、安全性に関わる動向をフォローし続ける必要があるため、メンテナンスの観点からは少ない方がありがたい。

また、「候補」としているため、将来使用される可能性があるものに絞る考え方もあるが、「推奨候補暗号リスト」に掲載されていることを提案者等が宣伝に使っている場合には影響も考えられ、単純な話ではないのではないか。

満塩構成員：利用者側としては、p.7の３ポツ目、今後の可能性があるものと、掲載から期間が経ち普及していないものが混在すると分かりにくくなる。

高木構成員：「運用監視暗号リスト」は安全性に問題が生じ、使って欲しくないことをアピールするリストである。そのため、利用実績がないものを「運用監視暗号リスト」に入れることは適当ではなく、どのように取り扱うかが問題である。また、「推奨候補暗号リスト」から外すことをどう判断するのかも重要である。

松本勉座長：御指摘のような取扱いを決め、一貫した形とすることが重要。また、「推奨候補暗号リスト」から外すことは影響も大きく、ロジックをしっかりと組み立てておく必要がある。

「推奨候補暗号リスト」に掲載されているものは、セキュリティ面でしっかりと評価をされ、その後も問題がないとされている。使用実績等がなく、「電子政府推奨暗号リスト」には入っていないが、そのような状態が20年近く続いている。そろそろ棚卸しをしてもよい。

松井構成員：「推奨候補暗号リスト」の取扱いは、長年の課題である。最初のCRYPTRECで

は、あまり絞り込むのではなく、ダメなものはきちんとダメとした上で、使えるものは将来のこともあり残していくという緩やかな方針であった。それから随分時間が経ち、使用実績等が見えてきた段階の取扱いは議論すべき。大変な課題とは思うが、問題意識は皆さんあると思う。

國廣構成員：たしかに「推奨候補暗号リスト」が混在している状況は非常にわかりにくい。「電子政府推奨暗号リスト」に載る可能性がほぼないものまで掲載されると、それはそれで間違ったメッセージを与えることになるため対応が必要である。一方で、どのようにリストから外していくのかということは難しい課題であり、引き続き検討は必要。

松本勉座長：勝手に心配しているだけで、全く問題がない可能性もある。

宇根構成員：「推奨候補暗号リスト」に掲載されていれば、安全性の監視等が必要になるため、リソースが必要となる。スクラップ＆ビルドしていくということは、耐量子計算機暗号や様々な課題が出てきている中で、リソース配分の最適化にもつながる。

金融分野では古い暗号を使用しているケースもあるが、その場合でも、「推奨候補暗号リスト」から外れた際に、多額の費用をかけて現在動いているシステムを入れ替えるということは考えにくく、システム更改等のタイミングで、最新の「電子政府推奨暗号リスト」に掲載された暗号をベースに調達をかけるということになるのではないか。

エンドユーザとしても、外れたからといってベンダにどうなっているかという問合せを行うこともイメージしにくい。

松井構成員：問題があるからリストから外れたと解釈される可能性も十分ある。CRYPTRECのリストは見ている人は見ているため、混乱を招かないよう、CRYPTRECとしての方針を決め、説明をしっかり行っていく必要がある。

松本勉座長：CRYPTRECのリストを参照していると、「推奨候補暗号リスト」に載っていることに意味があり、それを意図しているケースでは、影響が出る可能性がある。

高木構成員：例えば10年以上使われていないものが将来急に使われ始めることは、よっぽどの理由がない限りはないかと思う。そのため、リストに載った年を追記するなどして、最近加えたものと昔からあるものとの区別がつくようにする。その上で時間をかけて改めて検討していく方法はどうか。

松本勉座長：掲載された年についてはすぐわかる。一方で、使われているどうかの調査は本当に難しい。使用していることを積極的に開示していないケースもある。その当たりをどのように考えていくかである。

満塩構成員：何年後に見直すということにして方針を調整することもあり得る。その場合は、別の論点である改定タイミングとの議論とも絡んでくる。

＜論点１－２　技術分類について＞

松本泰構成員：次の論点のパラメータとの関係で、「共通鍵暗号」で「128ビットブロック暗号」として「AES」があるが、フルディスクエンクリプションのようなものでは256ビットが使われているが表現できているのか。

松本勉座長：ここではブロック長であり、それは鍵長ではないか。

松本泰構成員：失礼しました。パラメータの話ですね。

松本勉座長:「電子政府推奨暗号リスト」では、「共通鍵暗号」の「64ビットブロック暗号」は「該当なし」となっているが、「推奨候補暗号リスト」と「運用監視暗号リスト」には「64ビットブロック暗号」に属する暗号技術があるため、現在の分類のままとなっている。

＜論点１－３　暗号技術の公募について＞

高木構成員：これは現在の技術分類の話か。例えば耐量子計算機暗号、軽量暗号、高機能暗号という話ではないという理解でよいか。

松本勉座長：論点１は、現行リストの在り方であり、論点１－３に関しては、現行リストにある技術分類について公募するかどうかというである。新しい種類の暗号の取扱いについては別立てで議論したい。

満塩構成員：公募をしない場合、新しいものについて応募することはできなくなるのか。

松本勉座長：国際的にデファクトであったり影響力のある団体が使っていたりすることにより、CRYPTRECでも追加した方がよいのではとする事務局提案という形はこれまでもある。

＜論点２　暗号技術のパラメータについて＞

松本勉座長：現在のCRYPTRECの暗号リストでは、暗号の仕様については（Webサイト上で）参照先を明記しているが、パラメータとして、例えば、何年までだったら何ビットでよいであるとか、そうしたものについては決めていない。これについて議論したい。

高木構成員：共通鍵暗号とハッシュ関数はビット長が固定されているため、公開鍵暗号が対象になるという理解でよいか。

松本勉座長：そうとも限らない。例えばSHA-1はこうであるだとか、ブロック暗号のブロックサイズは規格で決まっており鍵長も選択肢はあるがその中でもこれは除外されるであるだとか、そのような規定もありえる。

高木構成員：例えばRSA暗号ではビット長が明示されていないのでこれを明示するのか。それともハッシュ関数も含めて何ビットセキュリティが何年まで使えるというNISTのSP800のようなものを作成し、その上でRSAの何ビットは何年までと規定をするのか。

松本勉座長：まだ事務局として具体案にまで至っていない。パラメータが規定されていないことが、利用者側にとって別途判断が必要な項目になっているため、CRYPTRECの暗号リストを見たときにどう使えば良いかも分かる形にした方が望ましいのではないかということ。

　規定の方法も、高木構成員の御指摘のように様々あるが、その方法についても今後議論をして決めていく必要がある。

高木構成員：NISTのST800-57では、2030年に向けてRSAの2048ビットを伸ばしていかない状況があり、その移行にも非常に時間がかかる。CRYPTRECで明示的に記載することによって、鍵長がどういったものが推奨されているかということをアピールすることは是非進めていくべき。

松本泰構成員：鍵長は非常に重要。暗号アルゴリズムの2010年問題があり、RSA1024からRSA2048として鍵長を変えるだけでも相当苦労した。実際に移行に10年程度を

要したと理解している。そのため、何らかの形で鍵長も含めて移行しなければならないことを示すことは非常に重要である。

満塩構成員：松本座長が御指摘されたように、利用者側として、実装の際にはパラメータが必要であり、その意味では是非お願いしたい。また、パラメータの移行のタイミングを考えていく上でも、パラメータが別文書で必要と認識している。

松井構成員：資料にも記載がある「相互接続性」はメーカーとしては重要。そこまで踏み込むかは別として、例えば楕円曲線暗号等の曲線になるとか様々なパラメータがあるし、これからの新しい暗号ではより多様なパラメータがでてきて、相互に接続できないといったことも考えられる。そのため、産業振興という意味でも、相互接続性を担保するためにCRYPTRECが何かできるとしたら、非常に興味がある。「どこまで決めるか」等の多くの課題があるかもしれないが、相互接続性は非常に大きなキーワード。

松本泰構成員：RSA1024の移行の際には、相互接続性とのトレードオフが一番難しかった。Webサーバの証明書に関して移行が困難だった理由の一つは、携帯電話で実装できなかったことがある。こうした相互接続性を理解した上で移行を示す必要があり、早期から鍵長の問題や、RSAからECDSAへの移行を促すなどしていかないと、実質的には移行できない。困難な問題だが、産業界にとっては重要である。

松本勉座長：産業界にとどまらず、全ての方にとって重要な問題となる。

＜論点３　暗号リストの今後の改定について＞

國廣構成員：資料中「改定後５年以内を目途に」のあとに「(以後５年以内ごとに)」とある部分は、５年以内にまず検討し、不要であれば更にその５年以内に改めてということか。

松本勉座長：その趣旨である。

國廣構成員：例えば10年後ではなく、13年後に改定されることもあり得るのか。

松本勉座長：その理解でよいが、いずれにしても５年以内には何か考える必要があるということが趣旨である。

國廣構成員：その際に改定の必要がないとしても、更に５年以内に考えるということか。了解した。

松本勉座長：「必要に応じて」判断するとした場合には、結局何もしないこともありえるため、判断については５年以内に行う旨の縛りをつけるという案である。

宇根構成員：改定してから５年以内に今後どうするかを検討して判断し、改定する場合は実質５年程度かかるため、直近の改定から10年以内に改定を行うイメージか。

松本勉座長：最長で10年である。例えば、2023年に改定をして、翌年に再改定についての判断が行われる場合もあり、その場合はそこから５年程度かけて検討が始まるイメージである。実質的な作業があるので、判断して１年で改定ができるかはわからないが、最短１年での改定ということもあり得る。

宇根構成員：改定を行って５年以内を目途に判断する。その判断として、改定しなくてもこのままで大丈夫ということになれば、そのままということか。

松本勉座長：書きたかったこととしては、改定後５年以内に次の改定の必要性を判断する。その次は、その「改定の必要性の判断」をした後の５年以内にまた判断すると

いうことである。

宇根構成員：つまり、少なくとも５年ごとにはチェックのタイミングが入るということか。理解できた。

満塩構成員：実質やろうとしていることは変わらないかもしれないが、例えば制定文書に有効期限を書くということも一つの方法である。その場合、検討して改定の必要がなければ有効期限だけを延すという判断を行うこととなる。

松本勉座長：10年ごとの改定というものは、もともとアーキテクチャも変わりうるといった考えがあり、前回の2013年の改定時にはかなり変わった。今回の改定は、新たな文書を追加するといったものはあるが、一見して大幅に変わった印象は出てこないかもしれない。その次の改定では、耐量子計算機暗号等をCRYPTREC暗号リストに位置付けるということになるかもしれないし、そうした際には構造から大きく変わる可能性がある。そうした改定の必要性については、判断を必ずせよということにしていきたい。

高木構成員：小規模な変更は、現在のリストの形を保ったまま、既に行われている。この５年に１回というものは、松本座長からあったように、何か非常に新しい技術が急速に普及したことに対して、リストの形も変えるようなことも含めて、それを５年に１回考えようという理解でよいか。

松本勉座長：その理解でよい。少なくとも５年に１回は考えるということ。

高木構成員：その場合、先ほど公募について議論があったが、新しい技術については公募をしてリストに入れるかどうか検討するということもあるのか。

松本勉座長：それはあり得る。例えば、耐量子計算機暗号について、現在NISTが検討している暗号以外にも良い暗号が登場するかもしれない。そうした場合に公募するかどうかも含めて議論を行い、改定の必要性を判断していけばよい。

公募で提案された暗号の評価は非常に大変である。予算の確保も含めて何年も前から検討をしないといけない。

＜論点４　CRYPTRECの文書体系について＞

國廣構成員：耐量子計算機暗号等に係る文書は、「GL」として暗号技術ガイドラインと同じ位置づけになるのか。あるいは、その下に位置づけるのか。

松本勉座長：「GL」には、暗号技術ガイドラインと暗号運用ガイドラインがある。このうち暗号技術ガイドラインとして、実際には数多くの文書が既にあるが、その一つに位置付けるもの。

高木構成員：耐量子計算機暗号に関して新しいガイドラインを作成するのか。既に研究動向調査報告書があり、ある程度安全性や使用されるパラメータ等は議論されている。暗号技術ガイドラインは利用を目的として書かれている印象があるが、既存の研究動向調査報告書は、かなりテクニカルなことが記載されている。これについて、もっと利用を前提とした書き方が求められていることから、暗号技術ガイドラインに入れるという理解でよいか。

松本勉座長：軽量暗号と全く同じトーンにする必要はない。現在の耐量子計算機暗号の研究動向調査報告書は、研究動向であるため理解することが難しいため、より端的に暗号の種類や現状が整理されていると良い。どのように具体化するかについては今後の議論で、少なくとも現在のまま、場所だけの移動にならないよ

うにしてはどうか。

高木構成員：執筆については、新しくワーキンググループ等を立ち上げて１～２年程度かけて作成するのか。

事務局（NICT）：新しく立ち上げることもあり得るが、既存のWGに人を追加して検討することも考えられる。なるべく使いやすい状態にしたい。

高木構成員：確かに今の研究動向調査報告書は、かなり論文に近く、解説記事といった印象がある。今後、普及を目指す場合は、使い方を含めて記載したガイドラインはいずれ必要。どの程度までプラクティカルなことを記載するかは今決めることはできないが、作成することは賛成である。

宇根構成員：重要なので、文書については是非作成すべきである。従来の暗号から耐量子計算機暗号に新しく乗りかえる際にはどういうことを考える必要があるとか、留意点なども盛り込んでいただけると使いやすくなると思う。

満塩構成員：耐量子計算機暗号等の文書については特段の異論はないが、一般の方に量子コンピュータに根拠のない不安というものがある気がする。まさに我々が理解したところを、ガイドラインなのか読み物なのかわからないが、何かにまとめてほしい。専門家ではなく、一般の方にもわかるようなものがCRYPTRECとしてできないか検討をお願いしたい。

松本泰構成員：量子コンピュータの実用化によって既存の公開鍵暗号がすぐに破られると思われている節もたくさんあり、そうではないということを何らかの形で示す文書が欲しい。暗号の移行は非常に時間がかかるため、移行の準備をしないといけないことは間違いなく、考えなければいけない時期にきている。

また、量子コンピュータのロードマップの中で、公開鍵暗号がいつ危殆化するかということを示していく必要がある。従来暗号にはスーパーコンピュータの計算能力をベースにした図があり説明しやすかった。そうした図に代わる、説得力があるものを作っていく必要がある。

資料のp.1で「ゲート型量子コンピュータの量子ビット数が数千程度以上ないと（ノイズ等に関わらず）暗号解読はできない」とある表現がそもそも一般にわかりにくく、ここでいう量子ビットは、論理量子ビットである。ノイズがあると全然桁が違う量子ビット数となるわけで、誤解されかねない。誤り訂正の有無で量子ビット数の意味が全然異なり、時間軸でも20年以上は違うのではないか。ただ、移行自身も20年程度はかかると思っており、そうした時間軸を含めて示してく必要があるのではないか。

事務局（総務省）：本タスクフォースで量子コンピュータに関する多数の知見を頂戴しており、今後、機会を捉えて発信していきたい。

高木構成員：昨年度の「耐量子計算機暗号の研究動向調査報告書」でも序文には記述したが、まだ技術者に対するアピールにとどまり、一般の人に対しては記載していない。ガイドラインを作成されるのであれば、技術的内容に入る前に、長期的にはどのようなことが起こっていくのか、といった部分も記載できるとよい。

松本勉座長：本タスクフォースで議論してきたことを分かりやすく解説できないか。

CRYPTRECの活動でこのような新しい技術についてはどこで検討すべきか。既存の体制のほか別の体系も考えられるが、テクニカルな部分は暗号技術評価委員会か。非常に高度な技術でなかなか理解することが難しいとされてい

るものを、また、社会的な影響力も強まってきている中で、少ないリソースで今まで頑張ってきているわけだが、更に重要性が高まっているという認識。

＜暗号技術検討会への報告について＞

松本勉座長：耐量子計算機暗号等の文書と、パラメータに関する文書について、それぞれ「CRYPTREC暗号リストから参照する」とある。パラメータに関する文書は、リストから直に指し示すという形かと思うが、耐量子計算機暗号等の文書はガイドラインと位置づけて、積極的に活用してもらうための広報活動は別途実施するとして、CRYPTREC暗号リストから参照しなくてもよいのではないか。

高木構成員：参照するとした場合、例えば耐量子計算機暗号の場合は公開鍵に注をつけて、こうしたガイドラインがあるため、量子コンピュータに対する安全性については参照してくださいといったことを記載するということか。きちんと検討した方がよいのではないか。

松本勉座長：例えば、現行のCRYPTREC暗号リストは、前文もなく、いきなり電子政府推奨暗号リストというのがあってという感じになっている。最初に、何か解説みたいなものがあれば、このリストはこういうもので、それ以外のものについては他の文書があるということが書ける。

宇根構成員：CRYPTREC暗号リストから参照するとなると、他のガイドラインも引っ張ってこないと平仄がとれないのではないか。その点を含めて検討する必要がある。

事務局（総務省）：ガイドラインが多くある中で、埋もれないようにという意図がある。その点では、統一基準群での記載による周知なども考えられる。

松本勉座長：少なくともパラメータについては、ここを見てくださいというため現行のCRYPTREC暗号リストを変える必要がある。その他のガイドラインについては、ここにあるということをわざわざ書かなくてもよいのではないか。現行のCRYPTREC文書の解説のような、どのように見てどのように使うかといったものがあってもいいのかもしれない。

事務局（総務省）：Webサイト上でそのような解説を記載することも一つの方法。ただ、CRYPTREC暗号リストを閲覧する際に、そうした解説を見ずにリスト本体のPDFだけを見る人が結構いて、その場合には書き込まないとガイドラインの存在がわからないのではないかという懸念があった。

松本勉座長：PDFをURLから直接行けないようにすればよいのではないか。

満塩構成員：資料のp.6に統一基準の記載が抜粋されているが、「電子政府推奨暗号リスト」は遵守事項として記載されており、これは、即利用してくださいという話かと思う。一方、ガイドラインにしようとしている耐量子計算機暗号とか軽量暗号や高機能暗号は、「即」ではなくもう少し待ってもよい雰囲気だと理解している。ガイドラインの場所に置くぐらいでよいのではないか。

松本勉座長：耐量子計算機暗号等のガイドラインについては、CRYPTREC暗号リストから参照という形でなくてよいということとしたい。「また、当該文書の重要性がわかるよう、 CRYPTREC暗号リストから参照する方針とする。」という部分は削除するのが簡単だが、ガイドラインを目立つようにせよという趣旨はある。

宇根構成員：CRYPTREC暗号リストのどこかにフットノートをつけて、リストを利用する際には、各種ガイドラインがあるため、それらを参照してくださいと入れればよ

いのではないか。

松本勉座長：全てのガイドラインを対象とするのであれば、Webページを見よという形か。

宇根構成員：その理解である。

國廣構成員：ガイドラインが将来増えてくることを考えると、CRYPTREC暗号リストは真に重要でなければ触らない方がよい。頻繁に変わるものを、本来変わらないものにつけることはあまりよくない。

事務局（総務省）：例えば、CRYPTREC暗号リストの前に１枚紙を入れ、全体の在り方やガイドライン等をまとめることもあるのではないか。「はじめに」のように１枚目をつけ、２枚目から本体が始まるイメージである。

松本勉座長：そのような体系になっていると、見た人も必ず理解できるかと思う。

事務局（総務省）：p.13の記載ぶりについても、「重要性がわかるよう取りまとめるものとする」という旨に変更して報告することとしたい。

（３）その他

高木構成員：量子超越性の報道があり、問合せも多く来ている。報道関係者にも説明したが、先ほども議論があったように、誤解を招くような質問もある。記事について丁寧に添削したとしても、なかなかうまく伝わらない状況。

　報道発表があった際に、CRYPTRECとして、例えば注意喚起などで國廣構成員の技術的な内容を説明するなど、何かできないか。

國廣構成員：従来、注意喚起について、どういうタイミングで、何を実施してきたのか。

事務局（NICT）：注意喚起については、2015年の暗号技術検討会で承認されたフローがある。おおまかに３類型あり、１つ目は、世の中に大きな影響があるものやCRYPTREC暗号リストに実用的な攻撃があった場合にはすぐに注意喚起を出すというもの。２つ目は、期限は限らないが、委員会の中でしっかりと検討した内容を出していくというもの。３つ目は、毎年のCRYPTRECレポートの中で、参照できるドキュメントとして残すというもの。枠組みとしては、注意喚起を出すスキームは整っている。

松本勉座長：コンテンツさえしっかりするのであれば、また、事実誤認がなく、誤解が生じにくい表現をとって、あまり長くなくまとめられるのであれば注意喚起を出せる。本日の國廣構成員の解説は非常に良かったが、これを正しく理解できるよう文書化する作業は大変か。

國廣構成員：分量によるかと思う。

松本勉座長：１ページ程度でよいのではないか。

満塩構成員：読者的視点としては、資料３のp.1の２ポツ目にある重要な指標を理解してもらうことはよいと思う。その上で、今どこにいるのかが分かれば、一般的に時間がかかることは理解してもらえると感じた。

國廣構成員：量子ビット数に関しては、比較的わかりやすく指標も出ているが、ノイズに関しては明確な記載も少ない。

満塩構成員：目標値は書けないにしても、こういったものが重要なパラメータだという認識がない。量子ビット数だけではなく、ここも重要だということが我々の理解だと認識している。

國廣構成員：IBMが「量子ボリューム」という指標を掲げており、量子ビット数やノイズ

を掛け合わせたようなものである。ただ、個社の話でもあり記載ぶりについては考えたい。

宇根構成員：高木構成員としては、量子超越性に関する解説をうまくテキスト化したような注意喚起をCRYPTRECとして出したいということか。

高木構成員：暗号に与える影響が実際どれくらいなのかを伝えたい。

宇根構成員：その前提として、このようなパラメータが重要といった話も当然しないといけないということか。

松本勉座長：その理解である。そのため、量子超越性というよりは、むしろ暗号にどのような影響があるかという観点が重要である。

量子コンピュータが暗号に与える影響について、わかりやすい資料を１枚程度で作成するということとしたい。これは来年度というわけではなく、できるだけ早くということ理解した。注意喚起の資料作成に当たっては、関係者で相談したい。

６．３．閉会

事務局から本日の議事概要の確認、及び量子コンピュータが暗号に与える影響に関する注意喚起の作成については別途メール等連絡する旨の説明が行われた。

以上