暗号技術検討会
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）

令和元年１２月２４日
１０：００～１２：００
総務省（中央合同庁舎２号館）
１１階　１１０１会議室

議事次第

１　開会

２　議題

（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

３　閉会

配付資料一覧

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）

資料１

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２回）
議事概要（案）

１．日時
令和元年９月６日（金）10:00～12:00

２．場所
経済産業省別館11階　1111各省庁共用会議室

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：岩田哲、徳永竜一、久山純也、岡野孝子、足立直、内山諒子、荒木美敬、
土本雄介、野口信、林巧、藤森英俊、中村佳憲、衛門愛子、花岡悟一郎
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、盛合志帆
（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）耐量子計算機暗号の扱いについて
（３）軽量暗号の動向について
（４）軽量暗号等の扱いについて
（５）その他

５．配付資料
資料１　第１回会合議事概要（案）
資料２　耐量子計算機暗号の扱いについて
資料３　岩田先生提出資料
資料４　軽量暗号等の扱いについて

６．議事概要
６．１．開会
松本勉座長から開会の宣言があり、岩田オブザーバの出席について説明があった。

６．２．議事
（１）前回議事概要の確認について
資料１の第１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、宇根構成員より、同構成員も著者の一人として令和元年８月30日に公表された日本銀行金融研究所のディスカッションペーパー「量子コンピュータによる脅威を見据えた暗号の移行対応」について説明が行われた。主な質疑は以下のとおり。
松本泰構成員：P27の図表A-1に、鍵長2048ビットのRSA暗号が量子コンピュータによって解読されうる時期の試算がある。CRYPTRECにおいても議論のたたき台になる

のではないか。

高木構成員：第１回会合で「Interface」を引用して「量子コンピュータの規模予測」を示したが、この図は更に傾斜を考慮して考えたものか。

宇根構成員：然り。既存の資料を活用し、誤り訂正能力も含めて場合分けして作成したものである。ワーストケース側に寄せた試算である。

国廣構成員：誤り率としている0.5%・0.01%は何を指しているか。

宇根構成員：誤り率は、既存の量子ゲート型コンピュータで発生している0.5%程度の場合と、既存論文で今後の目標とされている0.01%を設定している。なお、量子ビット数の増加に伴い誤り率が上昇すると考えられるが、ワーストケースとして誤り率の上昇は発生しないこととしている。

国廣構成員：量子ビット数以外にも計算時間などの指標もありえるため、量子ビット数だけに絞るのはよくないのではないか。

宇根構成員：どのように考えていくべきか引き続き検討していきたい。

満塩構成員：暗号移行の話として、「アクセス制御の強化」とは、アクセス制御を強化することか、それともアクセス制御を正確に使うということか。

宇根構成員：ICカードによる入退室管理システムなどで使用されている場合には、耐量子計算機暗号に切りかえて強化することを強化と呼んでいる。

一方で、バイオメトリクスの場合などで既存の技術を活用して運用を手厚くするという方法もありえると考えている。

満塩構成員：その意味では、適切にアクセス制御を利用するという趣旨か。

宇根構成員：然り。そのような場合もある。

満塩構成員：文書中にある「暗号処理部」とは何か。

宇根構成員：ランタイムで情報を読み出しながら処理する状況を想定している。ランタイム部分に問題があると、そもそも暗号システムの処理結果が信頼できないものになってしまうため、問題は大きいという考察である。

高木構成員：マイクロソフト社の「Open Quantum Safeプロジェクト」は、先週開催されたNISTの2nd PQC標準化会議でも議論になったハイブリッドシステムのことか。まだNISTの標準がないが、マイクロソフトが中心であるため、マイクロソフト派以外の人は使用しないといった問題はないか。

宇根構成員：ハイブリッドスキームについては、これをうまく組み込むことができれば、大規模量子コンピュータが実現する前から従来暗号と耐量子計算機暗号の両方で処理をすすめることができるため安心できるということである。

マイクロソフト社は一部の暗号ライブラリで先行して活動しているが、IEEEで標準化されRFCになっているハッシュベースの署名をNISTも今年中に標準に組み込む予定である。

マイクロソフト社の活動も、アマゾン等の主要ベンダーも参加し、Open SSL、Open SSH、Open VPNが対象になっている。実装性もそれなりにあると見込んでいる。

（２）耐量子計算機暗号の扱いについて

資料２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。

高木構成員：耐量子計算機暗号は量子コンピュータに対して安全だが、RSA暗号と楕円曲線暗号は量子コンピュータが大規模化すると安全ではなくなる。このため利用者視点として、量子コンピュータに対する安全性は考えない従来のリスト

と、量子コンピュータ時代の安全性を考えたリストとを分けることは良いアイデア。

今のCRYPTRECの暗号リストは、実用化や使用状況も考慮されるため、2023年の段階で普及している状況がなければ、リストではなく、ガイドラインにすることも良いアイデアである。

松井構成員：量子コンピュータの動向以上に、耐量子計算機暗号も今後の議論や攻撃手法の研究等によりどのようになるかわからない。リスト改定時に耐量子計算機暗号がリストとして載せる段階にはないかもしれないため、幾つかの可能性の一つとしてリスト群があるというフレキシブルな考えも必要である。

松本勉座長：資料中に「暗号リストと併せてリスト群として提示」とあり、「リスト群」とすると全てが「リスト」だと誤解されかねないが、この意味するところは、CRYPTREC暗号リストではなくて、ガイドライン等の別の文書とするということか。

事務局（総務省）：御認識のとおり、リスト群というのは語弊があるかもしれない。

松本勉座長：要するにサポーティングドキュメントのように、重要な資料であることが分かるように周知するといった趣旨かと思う。その意味で「リスト群」という言葉が使われており、ガイドライン等の中身をどうするかはこれからの検討。

宇根構成員：ガイドライン等の別の文書で扱うかどうかについては、何らかの形で文書としてまとめユーザーに示すようにすることが適切。

３ページの我が国における耐量子計算機暗号の開発・標準化については、研究が不十分な部分もあり、また、安全性等の検証にはまだ時間を要する状況。NISTの会議でも慎重に進めていく必要があるとなっており、CRYPTRECとしても慎重に検討する必要がある。量子コンピュータによって従来暗号が破られる状況がすぐに来るわけではないため、それまでに移行がスムーズにできるような体制を構築しておくことが重要。その意味で、ハイブリッドスキームのような観点でのサポーティングドキュメントの検討も有用ではないか。

国廣構成員：ガイドライン等の別の文書として扱うことについては、それが適当と思う。

耐量子計算機暗号の開発・標準化については、標準化というとCRYPTRECと関係がないようにみえる。国として何か考えること、やりたいことがあっての記載なのか。

事務局（総務省）：国として具体的な実施策が裏にあるものではなく、今回のタスクフォースにおいて、CRYPTREC暗号リストだけではなく、耐量子計算機暗号全体を見据えた幅広な議論を願って記載したものである。

事務局（NICT）：NISTから耐量子計算機暗号の標準化について、Round 2だけではなくRound 3まで実施することが発表になった。最速スケジュールだと2022年にはドラフト版が出る想定であったが、これにより２年は延びると想定されるため、CRYPTREC改定時期を考えるとガイドラインとする方針は適切かと思う。

松本泰構成員：2023年は、耐量子計算機暗号が実用的に利用できるようになっているかどうかに係らず非常に微妙な時期。RSA2048に相当する112bitセキュリティ暗号について、NISTのロードマップでは2030年には128bitセキュリティ暗号に移行すべきとしており、2023年というのは暗号を10年程度の保証をするとしたときに移行を始める時期。これを何らかの形で示す必要がある。データのライフサイクルも長くなっており、また、暗号がフレームワーク化しており

アルゴリズムが取り替えられるようなアーキテクチャが重要になっており、CRYPTREC暗号リストの立場を示さないと混乱するのではないか。

松本勉座長：現行のCRYPTREC暗号リストについて、耐量子計算機暗号をどのように位置付けるかという話と、現行リストに掲載された暗号をどのように移行するかという話は分けて考える必要がある。後者については、CRYPTRECの次期暗号リストに必要な情報を入力することが望ましいと思うが、耐量子計算機暗号については、別立てのガイドラインとすることが適当と考える。

ただし、日常的に耐量子計算機暗号の使用が必要となった場合は、電子政府推奨暗号リストに位置付けられるものと理解している。

高木構成員：2023年のリスト改定の際に、2030年以降のRSA2048移行について、耐量子計算機暗号への移行や鍵長の増加などについて、世界的な動きとともにリストに明記して利用者に示すことがよいのではないか。

また、CRYPTREC暗号リストへの掲載有無によって、企業の暗号開発への注力の度合いも変わるようであるので、日本の産業で使われるものは、ガイドライン等の形でも掲載し、状況にあわせて正式なリストに入れるような体制にしていくことは重要。

学術界としては、NISTのRound 2でも幾つかの攻撃手法が提案されており、標準化されたからといって未来永劫安全なわけではない。CRYPTRECでは監視体制のための人材もいるため、耐量子計算機暗号についての安全性を長期的に検討していく体制を維持していくことは非常に重要。

松本勉座長：2030年の移行については、民間でも準備がなされているかと思うが、それをCRYPTREC暗号リストの中でどのように位置付けるかは重要。

満塩構成員：NISTの動向も含めてサマリー的なものを整備するのがよいのではないか。

暗号移行について、従来はITシステムを５年程度で更改してきたため、そこで動く暗号アルゴリズムをどのように構築するかという話であったが、近年はクラウド利用が前提になりつつあり、開発もアジャイルやDevOpsといった方法で、暗号を切り替える部分が変わっていると感じている。これを踏まえた暗号移行の研究を始めてはどうか。また、量子コンピュータも自前で保有するというよりは、クラウド的に利用することが先行することも考えられ、その意味でもクラウドを意識したガイドラインの整備を考えてはどうか。

岩田オブザーバ：我が国における耐量子計算機暗号の開発・標準化について、量子コンピュータによって共通鍵暗号技術を突破できるものがあるという例示が報告されており、公開鍵だけでなく共通鍵についてもフォローしていくことが必要。

松本勉座長：AESはどうなるのか。

岩田オブザーバ：最近は、AESの安全性は思ったより低下しないといった論文が出ており、鍵長を倍にすれば使えるような認識である。

松本勉座長：AES-256を使用するのが現実的か。

岩田オブザーバ：AES-256があったとして、それを使用してどのようにデータを認証していくかは別の話であり、そのような点も含めて研究が進んでいくかと思う。

高木構成員：今年度の暗号解析WGで、共通鍵暗号に対する量子コンピュータの耐性の調査を実施している。

国廣構成員：暗号解析WGでは、こうした場合は安全ではないという形で、どうすれば安全かという形までは議論が進みそうになく、長期的視点で見ていくことにな

る。

高木構成員：その議論を踏まえて、2023年のリスト改定時に、共通鍵暗号に対しても量子コンピュータがどのような影響があるかを記述すべきである。

宇根構成員：満塩構成員からクラウドの話があったが、金融機関でもクラウドを使用する場合はどのように考えれば良いのか等の疑問が出ている。先ほどのディスカッションペーパーはオンプレミス環境が前提だが、クラウドは重要な論点である。

松本勉座長：今回の議論としては、耐量子計算機暗号については今後も動向をウォッチする必要があり、次期改定においては、暗号解析WGで検討した結果等も盛り込む必要があること。

　また、耐量子計算機暗号については、ガイドライン等の別文書として取り扱うが、リスト本体から参照するなど何らかの形でその文書が重要だとわかる形式をとること。

　それから、2030年やその先といった長期的な課題についても、CRYPTRECとしてどう考えていくかを考えていかなければならないこと。

　そして、移行として、現在のCRYPTREC暗号リストは、仕様は参照しているが、パラメータまでは特定しないところもあるため、具体的にどのように考えるか参考になる情報も入れる必要がある。

（３）軽量暗号の動向について

資料３に沿って、岩田オブザーバより説明が行われた。主な意見等は次のとおり。

国廣構成員：軽量だから２の64乗でもよいわけでなく、112乗ないと議論に乗れないというように、高い安全性が要求されていることに驚いた。

宇根構成員：サイドチャネル攻撃耐性がDesign Requirementsとなっているが、処理時間が一定ということか。電力消費量一定みたいなことまで可能なのか。

岩田オブザーバ：そのような保護がしやすい設計をとるということがある。また、リンケージ・レジリエントというキーワードで、例えばモード等でデータ処理する際に中間状態の一部が敵の手に渡ったとしてもある程度の安全性が保たれる設計を目指しているというものがある。

宇根構成員：IoT機器等で使用すると、長期間使用し続けなければならないことがある。そうした大量のデータ処理についても、NISTでは考慮しているのか。

岩田オブザーバ:NISTでは、２の50乗バイト以上の暗号が処理できるよう規定しており、想定している大部分のユースケースはこの処理量で対応可能と考えられている。

松本泰構成員：軽量暗号はIoTで利用される暗号技術として非常に重要。一方で、例えばLightweight applicationsといったときに、これが具体的に何を指すのかという共通コンセンサスは簡単に得られるものではない。また、IoT機器では省電力対応のため、小さなデータの送信時に128ビット暗号よりも送信時間が半分で済む64ビット暗号が、省電力対応の観点から欲しい場合もある。CRYPTRECの活動範囲としてはこうした応用層の話は見えにくく、CRYPTRECでそこまで含めたコンセンサスが得られるものを作ることは難しいのではないか。

岩田オブザーバ：2017年にCRYPTRECで軽量暗号のガイドラインを作成した際に、想定する軽量暗号のユースケースを幾つか例示している。

松本勉座長：CRYPTRECでの取扱いについては次の議事で議論する。

国廣構成員：CAESARとNISTの標準化の関係はどのようになっているのか。

岩田オブザーバ：CAESARは学術コミュニティ手動であり、ポートフォリオに選ばれた何かの標準になるというわけではない。

　また、CAESARは2014年に応募締切であったが、当時はユースケース分類がなく、AsconとACORNはLightweight applicationsとして提案されたわけではない。その意味では、NISTとしてもLightweightをするに機は熟したと判断した可能性はある。なお、AsconはNISTに提案されているが、ACORNは提案されていない。理由は不明である。

事務局（NICT）：NISTから発表されたRound 2候補から見えてくる、選定ポリシーのようなものはあるか。

岩田オブザーバ：初期不良が指摘されたアルゴリズムは選ばれていない。また、コメントが出ても収束していないものや議論中のものは残っている。NISTが選定した背景を今後コメントするとしているのでそれを待ちたい。

　傾向としては、暗号学的置換に基づくものが有力のように見え、認証暗号とハッシュ関数との橋渡しが容易であるという点が挙げられる。

高木構成員：NISTのDesign Requirementsにおいて実装性能等があったが、ハードウェア・ソフトウェアのテスト環境をNISTは指定しているのか。

岩田オブザーバ：指定している。CAESARでGMUがハードウェア評価用のプラットフォームを出しており、これに準じたものを使うとしている。ソフトウェアも名前が挙がっていたように思う。

高木構成員：サイドチャネル攻撃耐性についてはどうか。

岩田オブザーバ：提案者やコミュニティに任されているかと思う。

松本勉座長：CAESARは必ずしも軽量暗号だというわけではなく、認証暗号というカテゴリで公募して進んできて、その中には軽量性のあるものも入っている。その一部はNISTの軽量暗号標準化プロジェクトにも応募されているということか。

岩田オブザーバ：その理解である。CAESARポートフォリオの中でAsconという暗号がNISTのRound2にも残っている。

（４）軽量暗号等の扱いについて

資料４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。

＜軽量暗号について＞

松井構成員：「軽量暗号とはそもそも何か」の議論が難しい。

NISTでもAESベースのものが結構あるが、AESのモードを工夫して軽量にしている。一方でAESは128ビットブロック暗号として既にCRYPTREC電子政府推奨暗号リストに掲載されている。AESのモード次第で軽量暗号になるとすれば、軽量暗号の定義付けをどのように考えていくのか、公的な文書としてどのように考えるのかは難しく、議論が必要。

松本勉座長：2017年に軽量暗号のガイドラインを作成した際は、AESを基準としてそれに比べて何らかの点で軽量性があるということだったかと理解している。

岩田オブザーバ：そのとおりであり、電力等でAESより優位性があるものを軽量暗号と呼んでいた。また、ブロック暗号単体で話す場合はよいが、実際に使用する場合はブロック暗号単体として利用するわけではないため、松井構成員が述べられたような齟齬が生じる。

松本勉座長：軽量性をどのように取り扱うかという議論が必要との指摘であり、その通りかと思う。

松本泰構成員：「安全性を一部トレードオフした」という記載があるが、トレードオフではなく、何らかの制約の下で安全性を確保したものが軽量暗号であるとの認識。

松本勉座長：個々に状況が異なるが、「安全性を確保した」というと、制約がない場合に比べて保証や確認の手厚さが劣るのではないか。

岩田オブザーバ：先ほどのNISTのDesign Requirementsをみても要求自体のレベルが非常に高く、一概に安全性が損なわれているとは思えない。

利用環境が制限されているため、一般的なリストとは変えることは選択肢としてはあり得る。ただ、安全性のトレードオフは、該当するものとしないものとがある。

事務局（NICT）：NISTのDesign RequirementsはCRYPTREC暗号リストとしても参考になる。

松本勉座長：CRYPTRECにおいて軽量暗号の定義をする際に、ほかのアクティビティとして出ている基準等はとても参考となる。

現行の暗号リストには、想定しているアプリケーションであるだとか、データ取扱に関する要件は入っておらず、個々の暗号について安全性や利用実績を見ている。軽量暗号については、政府調達等でも使用されるものについて、どれを選んだらよいかという参考になる情報が整理されていることが重要。

次期改定リストに軽量暗号というカテゴリがいきなり入るということではなく、現行のリストとは別立てで整理する議論が望ましい。その際、現行の「ガイドライン」だと単なる参考文書のようにも見えるため、位置付けを議論する必要がある。

高木構成員：現行の暗号リストとは設計思想や安全性の評価指標が違うため、軽量暗号が非常に普及したとしても、セキュリティと使用環境をセットにして明示し、セキュリティが通常とは異なるということがわかるように別リストとしたほうがよい。

宇根構成員：先ほどの軽量暗号の定義が難しいという点については同意見。

現行のリストにおいて軽量なものであれば、電子政府推奨暗号リストに64ビットブロック暗号はなく、推奨候補暗号リストはMISTY1等があるといったように当て込みは可能であるが、利用者側の要求条件等は別文書にするほうが現実的である。

松本勉座長：リストへの位置付けについて幾つか御意見を頂戴した。耐量子計算機暗号も同様であるが、対象を多くすれば、それだけ評価体制も整えなければならず、投入できるリソースも含めて検討していく必要がある。

＜高機能暗号について＞

國廣構成員：高機能暗号については、従来のリストのようにリストアップすることは難しい。新しい方式が日々提案され、改良もされている。このタイミングで特定のものをリストに挙げて固定化することは難しく、方式を決め打ちにすることは現状にそぐわないのではないか。

満塩構成員：軽量暗号や高機能暗号について、利用者側視点からは、ユースケースや制約がわかればよい。現行のリストだとそうした点ができていない理解であり、そこをどのようにわかりやすく書けるかがポイントになる。

宇根構成員：高機能暗号のキラーアプリケーションは、既存の暗号でも実現できなくはないが、高機能暗号の使用によって、ユーザビリティやコスト的な有効性が高まる等の話になるのかと思う。そうすると、既存のシステムを構築し直してまでコスト的にメリットがあるのか、使い勝手が良くなるのか等の内容になるため、個別の事象に特化しないと議論が深まらない。現時点では、様々なケースで議論を深めないとリストの取扱いについて議論するのは難しい印象がある。

松本勉座長：高機能暗号についても研究が盛んに行われており、耐量子計算機暗号より先に高機能暗号が普及する印象を持っている。耐量子計算機暗号についての議論は着々と進める必要はあるが、高機能暗号についても利用が一気に広まるまでに関連ドキュメントの整備を進めておく必要がある。

松井構成員：高機能暗号はアルゴリズムよりも更に上位レイヤーの概念。これをCRYPTREC暗号リストの観点からどのように捉えるかは非常に難しい観点。応用側によっているからこそ価値のある高機能暗号について、高機能暗号とは何かといった議論から深めていく必要がある。

松本泰構成員：耐量子計算機暗号も軽量暗号も高機能暗号も同様だが、CRYPTREC暗号リスト以外は使用不可とすることが、暗号技術を利用したイノベーションを阻害する可能性が出てくることが大きな問題。その点について、どのようにバランスを取るかがCRYPTREC暗号リストに望まれている。

高木構成員：高機能暗号が普及して使われ始めたときに、どの程度安全なのかをCRYPTRECで議論することは非常に価値がある。その結果についてどのような形になるかわからないが、発表することで、安心して使ってもらえるようになる。

６．３．閉会

事務局から次回は12月頃の開催を予定しており、詳細な日程、場所等については、別途連絡する旨の説明が行われた。

以上

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

筑波大　國廣　昇

量子超越性

quantum supremacyとは？

J. Preskillにより提唱
(Quantum Computing and the Entanglement Frontier, 2012)
the day when well controlled quantum systems can perform tasks surpassing what can be done in the classical world

何らかの意味で古典計算ではできないことが量子計算でできることになる.
直後の文章
One way to achieve such “quantum supremacy” would be to run an algorithm on a quantum computer which solves a problem with a super-polynomial speedup relative to classical computers,
but
there may be other ways that can be achieved sooner, such as simulating exotic quantum states of strongly correlated matter.

素因数分解

今回の実験

Googleによるアナウンス

Nature誌に，量子超越を達成したことをアナウンス．
論文自身は，Nature誌に2019年10月23日に公開

概略：

- 古典計算機では，10,000年かかるタスクを，
- 開発した量子計算機（Sycamore processor）では200秒で可能．

Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505–510 (2019)

対象とする問題

Random Quantum Circuitからのサンプリング

- 53量子ビット
- 20 cycles (1qubit operation （ランダムに選択）
  then 2qubit operation)

この量子回路からの出力系列を考える.

実機（ Sycamore）を用いると,

- 200秒で終了
- fidelity (忠実度) =0.2%

fidelityの定義：Cross-Entropy
1. ノイズがない理想的な量子回路からの出力
2. 実際の量子計算機 (Sycamore)からの主力
3. 古典計算機を用いたシュミレーション
1との距離をfidelityとして定義．1<-> 2と2<->3を比較

fidelity=1 <=> 完全に理想的な量子回路をシミュレート
fidelity=0 <=> 完全にランダムな系列を主力

実際の量子計算機は，ノイズがあるので，理想的な分布からは
離れた分布になる．
古典計算機では，指数関数時間が必要なので，近似を行っている．

今回の実験では，0.2% = $2*10^{-3}$

(参考)サンプリングアルゴリズム

理想の分布が与えられた状況下で,
理想の分布と近い分布を，高速に出力するアルゴリズム

性能評価：
理想的な分布との距離（忠実度）を導入し，同一の忠実度
を達成するのに必要な計算時間で比較

例)
格子暗号における離散ガウス分布
Rejection samplingなど

今回の場合では,

- 理想的な分布＝ランダム量子回路からの出力分布
- 距離＝理想的な分布と出力分布とのクロスエントロピー

古典計算機を使う場合の評価

- Schrodinger-Feynmanアルゴリズム（最も効率的なアルゴリズム）を使用.
- 小規模な数値計算および理論的な評価式を用いて，外挿.

同じfidelityを達成するのにスパコンを用いると，10,000年かかると推定

量子超越は達成したのか？

Googleによる主張

- 実機を用いた場合：200秒
- 最速のアルゴリズム，スパコンを用いた場合：10,000年

これにより，量子超越を達成したと主張

IBMによる反論

- 10,000年は最悪の場合の見積もり
- ストレージ周りの制御を適切に行うことにより，2.5日で十分だと主張.

暗号の安全性に関する影響

今回の実験は,
- 53量子ビットの量子計算機
- ノイズあり
- 用いた量子ゲートは，1500個程度

2048ビットの素因数分解を行うのに必要なリソース
ノイズが全くないという理想的な環境下でも,
- 4098量子ビット，量子ゲート数は，10^13程度，もしくは
- 6146量子ビット，量子ゲート数は，10^12程度.

大きなギャップがあり，暗号の安全性への影響はほぼないと言える.

Googleの論文中にも,
realizing the full promise of quantum computing (using Shor's algorithm for factoring, for example)still requires technical leaps to engineer fault-tolerant logical qubits

まとめ

- 今回の実験は，NISQ (Noisy Intermediate-Scale Quantum) 計算機の実現に向けた第一歩と考えるべき
- 誤り訂正は組み込まれていない.
- これを契機に量子計算機の研究開発が加速すると予想されるため，動向を継続的に注視する必要がある.
- 特に，量子誤り訂正機能の有無は常に意識して注視する.

CRYPTREC
Cryptography Research and Evaluation Committees

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

令和元年１２月２４日
CRYPTREC事務局

第１回会合での議論①

＜量子コンピュータについて＞

- ✓ 暗号解読ができるような（大規模でノイズの少ない）量子コンピュータ※の実現時期は見えていない。
  - ※ 素因数分解された最大の数は「21」であるが、その数に特化した方法で計算しており汎用的な素因数分解を実施したものではない。（暗号解読のためには、汎用的な方法により、数百桁程度の素因数分解が必要）
- ✓ 量子コンピュータの性能は、「量子ビット数」、「ノイズ（誤り）」※、「演算可能回数」※が重要な指標。
  - ※ 古典コンピュータには計算誤りの発生時に訂正する機能があり、何年も計算させ続けられるが、量子コンピュータでは誤り訂正の実現の難易度が高く、現在は誤り訂正をせずに計算を行う必要がある。そのため、コヒーレンス時間（状態が保たれている時間；現状はミリ秒程度）の中で計算を終わらせる必要があり、演算可能回数も制限されている。
- ✓ 量子ビット数は公表されているが、ノイズ等はあまり公表されないため、計算性能に関する将来予測は困難。
- ✓ そもそも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見込まれているため、公表されている量子ビット数の動向を確認し続けることが妥当。
- ✓ ノイズがある場合※でも、化学や金融の分野では活用できる想定だが、現状のノイズは暗号解読のための素因数分解に活用できる水準ではない。
  - ※ NISQ（Noisy Intermediate-Scale Quantum Computer）。Google社、IBM社、Intel社等が開発している。

第１回会合での議論②

＜耐量子計算機暗号（PQC）について＞

- ✓ 現在の暗号を使い続けながら、量子コンピュータに対しても準備をしておくことが必要。
- ✓ 大規模システムの更改には10年以上を要することもあり、データのライフサイクルも踏まえた議論も必要。
- ✓ SHA-1等の危殆化に備えSHA-3が作られたがほとんど使われていない。PQCについても実際にどの暗号方式が残っていくかという点に留意が必要。
- ✓ PQCの利用は、アプリケーションによって使用アルゴリズムを切り替えるようになる可能性も高いのではないか。
- ✓ 公開鍵暗号は、アプリケーションが広まったため活用も広まった。 PQCを活用すると従来の暗号に比べてデータサイズが大きくなってしまうため、高機能暗号としてアプリケーションを広げ、それが耐量子性も持っているというような形が有効。

第２回会合での議論①

＜量子コンピュータについて＞

- ✓ 量子コンピュータによって従来暗号が破られる状況はすぐには到来しない。
- ✓ NISTでのPQCの標準化はRound3まで実施する模様。

＜CRYPTREC暗号リストにおけるPQCの位置づけについて＞

- ✓ CRYPTREC暗号リストは、利用実績や普及見込みも考慮したものであるため、PQCに関してはガイドライン等の別文書にすることが適当。
  （日常的にPQCを使用することが必要となった場合は、暗号リスト本体に位置付けられる。）
- ✓ 利用者視点としても、量子コンピュータに対する安全性を考えない従来のリストと、量子コンピュータ時代の安全性を考えたPQCに関する文書とを分けることは適当。
- ✓ PQCに関する文書は、CRYPTREC暗号リスト本体から参照するなどして、重要性がわかるものとすべき。

＜PQCに関する文書について＞

- ✓ NIST等の他のアクティビティが実施している取組も参考にしていくことが適当。
- ✓ 公開鍵暗号方式だけでなく、共通鍵暗号方式に対する影響についても言及すべき。

第２回会合での議論②

＜軽量暗号・高機能暗号等について＞

- ✓ 現行のCRYPTREC暗号リストは、利用環境によらない暗号技術自体の安全性や利用実績を見ている。一方で、軽量暗号や高機能暗号では、利用するアプリケーションやデータ取扱に関する要件が限定される。
- ✓ そのため、軽量暗号等については、現行のCRYPTREC暗号リストとは別立てで整理することが適当。
- ✓ 軽量暗号について、現行ガイドラインは単なる参考文書のようにも見えるため、位置付けの整理が必要。
- ✓ CRYPTREC暗号リスト以外は使用不可となると、暗号技術のイノベーションを阻害する可能性があるため、バランスを取る必要。

＜我が国における耐量子計算機暗号の開発・標準化について＞

- ✓ PQCについての安全性を長期的に検討していく体制を維持していくことが重要。
- ✓ PQCへの移行がスムーズにできるよう、十分な体制構築や参考となる文書の検討が必要。
- ✓ CRYPTREC暗号リストへの掲載有無によって、企業の暗号開発への注力の度合いも変わるのであれば、我が国の産業で使用されるものは、状況にあわせて組み込んでいくことが必要。

＜その他＞

- ✓ 現在のCRYPTREC暗号リストはパラメータを特定しないが、この取り扱いについても検討する必要。
- ✓ PQCへの移行や鍵長の増加等のほか、2030年頃のRSA2048の移行※についても、利用者に示していくことが有用であり、CRYPTREC暗号リストの中でどのように位置づけるかは重要。

※ RSA2048に相当する112bit暗号について、NISTのロードマップでは2030年には128bit暗号に移行すべきとしている。

本会合での論点

論点１　現行リストの在り方について（2023年目途の改定に当たって）

- 論点１－１　リスト構成について
- 論点１－２　技術分類について
- 論点１－３　暗号技術の公募について

論点２　暗号技術のパラメータについて

論点３　暗号リストの今後の改定について

論点４　CRYPTRECの文書体系について

論点1-1　リスト構成について

CRYPTREC暗号リストは、①電子政府推奨暗号リスト※1　②推奨候補暗号リスト※2　③運用監視暗号リスト※3　の３リスト構成となっており、この構成を維持すべきか。

※1　CRYPTRECにより安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。
※2　CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト。
※3　実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったとCRYPTRECにより確認された暗号技術のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。

✓ 安全性及び実装性能が確認された暗号技術を推奨するための「①電子政府推奨暗号リスト」、及び、危殆化等により推奨すべきではなくなった暗号技術を周知するための「③運用監視暗号リスト」については、その性質から引き続き利用することが望ましいのではないか。

＜参考：政府機関等の対策基準策定のためのガイドライン（平成30年度版）（平成30年7月25日 内閣官房 内閣サイバーセキュリティセンター）＞
6.1.5 暗号・電子署名＜遵守事項＞
(1) 暗号化機能・電子署名機能の導入
(b) 情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「**電子政府推奨暗号リスト**」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、以下の事項を含めて定めること。
(ア) 職員等が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「**電子政府推奨暗号リスト**」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。
(イ) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「**電子政府推奨暗号リスト**」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。
(ウ) 暗号化及び電子署名に使用するアルゴリズムが**危殆化した**場合又はそれを利用した安全なプロトコルに**脆弱性が確認された場合**を想定した緊急対応手順を定めること。
(エ) 暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定めること。

論点1-1　リスト構成について（続き）

- ✓ 以下の状況を踏まえ、「②推奨候補暗号リスト」については、その意義・必要性について十分な検討が必要ではないか。
  - 現行リスト改定の際に「②推奨候補暗号リスト」を含めた３リスト構成としたのは、国産暗号技術の普及展開を促進することもその目的の一つ※であるが、３リスト構成とした意図が十分に活用されている状況とは言いがたい。
    ※2011年度第1回暗号技術検討会資料3-2
  - 一方、「②推奨候補暗号リスト」は、（利用実績等が十分でないものの）安全性及び実装性能が確認されていることから、将来的に「①電子政府推奨暗号リスト」に載る可能性がある暗号アルゴリズムの受け皿としての機能もある。
  - 現状の「②推奨候補暗号リスト」には、将来的に普及することが予想され「①電子政府推奨暗号リスト」に載る可能性がある暗号技術と、掲載から十分な期間を経てもあまり普及したとは言えない暗号技術とが混在している。
  - 「②推奨候補暗号リスト」から暗号技術を削除する際の基準や手続きが定まっていない。
- ✓ ３リスト構成については、望ましいあり方について、引き続き検討が必要ではないか。

論点1-2　技術分類について

各リストにおける暗号技術の技術分類について、現在の構成※を維持すべきか。

※　公開鍵暗号（署名・守秘・鍵共有）／共通鍵暗号（64ビットブロック暗号・128ビットブロック暗号・ストリーム暗号）／ハッシュ関数／暗号利用モード（秘匿モード・認証付き秘匿モード）／メッセージ認証コード／認証暗号／エンティティ認証

✓ 以下の状況を踏まえ、次期CRYPTREC暗号リストの技術分類については、現在の構成を維持してはどうか。

- 耐量子計算機暗号並びに軽量暗号及び高機能暗号については、第２回会合において現行のCRYPTREC暗号リストとは別文書とすることとした。
- 現行の技術分類における暗号技術については、十分成熟しており、現時点で特筆すべき動きはない。
- 現行のCRYPTREC暗号リストにおいても、改定後に必要に応じて技術分類の変更を行っている※。

※　平成30年3月29日付けで「認証暗号」の技術分類を追加する変更を実施。
2013年の「改定」後に実施してきたCRYPTREC暗号リストの修正は「変更」とし、2023年目途に実施しようとしている「改定」と分けて取り扱う。

論点1-3　暗号技術の公募について

各リストにおける暗号技術について、改定に当たって公募を実施すべきか。

- ✓ 以下の状況を踏まえ、今般のCRYPTREC暗号リストの改定に当たって、暗号技術の公募を行わない方針としてはどうか。
  - 現行の技術分類における各暗号技術については、十分成熟しており、現時点で特筆すべき動きはない。
  - 現行のCRYPTREC暗号リストにおいても、改定後に必要に応じて暗号技術の掲載内容の変更を行っている※ 。

※　平成30年3月29日付けで「ChaCha20-Poly1305」を追加する変更を実施。

論点２　暗号技術のパラメータについて

CRYPTREC暗号リストにはパラメータが規定されていないが、パラメータを規定する必要はないか。

- ✓ 以下の状況を踏まえ、CRYPTREC暗号リストは、引き続き、推奨する暗号技術（アルゴリズム）を規定するものとして用い、CRYPTREC暗号リストから推奨パラメータを規定する別の文書（新規作成）を参照する構成としてはどうか。
  - これまで、CRYPTRECでは、推奨する暗号アルゴリズムをCRYPTREC暗号リストにより示してきたが、パラメータについては積極的な提示は行ってこなかった。
  - 他方、米国では、NIST SP800-57やSP800-131A等において、推奨パラメータを示している。
  - 危殆化対策としての安全なシステム構築や計画的な暗号技術の移行を促進するために、推奨パラメータを明示することは有用。
  - 推奨パラメータは、利用環境や技術の進展に依存するほか、さらには相互接続性などを踏まえて検討を行う必要がある。

論点３　暗号リストの今後の改定について

2003年に「電子政府推奨暗号リスト」を作成し、2013年に現行のCRYPTREC暗号リストとして改定を行い、今般、2023年を目途とした改定作業を行っているが、今後も10年単位での改定※を行うのか。

※2013年の「改定」後に実施してきたCRYPTREC暗号リストの修正は「変更」とし、2023年目途に実施しようとしている「改定」と分けて取り扱う。

- ✓ CRYPTREC暗号リストの内容については、常に危殆化等の監視を行うとともに、必要に応じて新規の暗号技術を加えるなどの変更を行っている。
- ✓ 2023年目途の改定以後は、10年単位での改定と期限を切らずに、必要に応じて改定を行うこととしてはどうか。
- ✓ また、改定の必要性の判断については、暗号技術や諸外国の動向を踏まえ、改定後５年※以内を目途に（以後５年以内ごとに）、技術検討会において判断することとしてはどうか。

※前回の改定では、枠組み等の検討開始から改定まで５年程度を要している。

論点４　CRYPTRECの文書体系について

これまでの議論を踏まえ、CRYPTRECの発行する文書の体型はどのようにあるべきか。

- ✓ 耐量子計算機暗号等に係る文書については、GLに位置付けてはどうか。
- ✓ 推奨パラメータに係る文書については、LSの下に位置付けてはどうか。

（参考）現行の分類

CRYPTREC文書

- CRYPTREC暗号
  - CRYPTREC暗号リスト（LS）
- 年次報告書
  - 暗号技術検討会/各委員会報告書（RP）
- 注意喚起
  - 注意喚起レポート（ER）
- ガイドライン
  - 暗号技術ガイドライン（GL）
    - 「CRYPTREC暗号技術ガイドライン(軽量暗号)」
  - 暗号運用ガイドライン（GL）
- 技術報告書
  - 外部評価報告書（EX）
  - 暗号技術関連の調査報告（TR）
    - 「耐量子計算機暗号の研究動向調査報告書」リストガイド
- 会議資料
  - 暗号技術検討会/グループ/タスクフォース資料（MT）

暗号技術検討会への報告について

暗号技術検討会については、次の内容を報告する方針としてはどうか。

- ✓ 2023年目途のCRYPTREC暗号リストの改定について、現行の３リスト構成の在り方については引き続き検討が必要であるものの、技術分類については現行のものを踏襲し、公募は行わない方針とする。
- ✓ 耐量子計算機暗号、軽量暗号、高機能暗号は、CRYPTREC暗号リストには含めず、それぞれ別の文書とする。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。
- ✓ 推奨される暗号のパラメータについて、CRYPTREC暗号リストから参照する形で別の文書としてまとめる方針とする。
- ✓ これらの新たな文書も含め、CRYPTREC暗号リストを含むCRYPTRECの文書の位置付けを整理する。
- ✓ 量子コンピュータや耐量子計算機暗号の状況をフォローするため、及び引き続き継続検討とした内容の議論を行うため、2020年度以降も本タスクフォースの継続設置を提案する。

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）

平成２５年３月１日
総　　務　　省
経　済　産　業　省

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

技術分類		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64 ビットブロック暗号(注2)	該当なし
	128 ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード(注13)	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
認証暗号		該当なし
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

[1] 総務省政策統括官（情報セキュリティ担当）及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、総務省及び経済産業省における施策の検討に資することを目的として開催。

[2] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

（注1） 「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」（平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成25年 3 月 1 日 現在）

（注2） CRYPTREC暗号リストにおいて、64 ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注4） 初期化ベクトル長は 96 ビットを推奨する。

（注13） 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て、「認証暗号」として使うことができる。

推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術[3]のリスト。

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM(注5)
共通鍵暗号	64 ビットブロック暗号(注6)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128 ビットブロック暗号	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
		SC2000
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01(注7)
ハッシュ関数		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128(注12)
		SHAKE256(注12)
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード(注14)	該当なし
メッセージ認証コード		PC-MAC-AES
認証暗号		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-4

（注5） KEM (Key Encapsulating Mechanism) – DEM (Data Encapsulating Mechanism) 構成における利用を前提とする。

（注6） CRYPTREC暗号リストにおいて、64 ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注7） 平文サイズは 64 ビットの倍数に限る。

（注12） ハッシュ長は 256 ビット以上とすること。

（注14） 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て、「認証暗号」として使うことができる。

[3] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったとCRYPTRECにより確認された暗号技術[4]のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5(注8)(注9)
	鍵共有	該当なし
共通鍵暗号	64 ビットブロック暗号(注15)	3-key Triple DES
	128 ビットブロック暗号	該当なし
	ストリーム暗号	128-bit RC4(注10)
ハッシュ関数		RIPEMD-160
		SHA-1(注8)
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード(注16)	該当なし
メッセージ認証コード		CBC-MAC(注11)
認証暗号		該当なし
エンティティ認証		該当なし

（注8） 「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1 及び RSA1024 に係る移行指針」（平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成25年 3 月 1 日 現在）

（注9） SSL 3.0 / TLS 1.0, 1.1, 1.2 で利用実績があることから当面の利用を認める。

（注10） 互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。SSL/TLS での利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。

（注11） 安全性の観点から、メッセージ長を固定して利用すべきである。

（注15） CRYPTREC暗号リストにおいて、64 ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注16） 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て、「認証暗号」として使うことができる。

[4] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

変更履歴情報

変更日付	変更箇所	変更前の記述	変更後の記述
平成27年 3月27日	（注１０）	128-bit RC4 は、 SSL(TLS1.0 以上)に限定して利用すること。	互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。SSL/TLS での利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。
平成28年 3月29日	推奨候補 暗号リスト （技術分類： ハッシュ関数）	該当なし	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256(注12)
	（注１２）	[新規追加]	ハッシュ長は 256 ビット以上とすること。
平成29年 3月30日	推奨候補 暗号リスト （技術分類： ハッシュ関数）	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256(注12)	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE128(注12) SHAKE256(注12)
平成30年 3月29日	（注２） （注６）	より長いブロック長の暗号が利用できるのであれば、128 ビットブロック暗号を選択することが望ましい。	CRYPTREC暗号リストにおいて、64 ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。
	（注１５）	[新規追加]	
	電子政府推奨 暗号リスト （技術分類： 共通鍵暗号）	3-key Triple DES(注3)	該当なし
	（注３）	3-key Triple DES は、以下の条件を考慮し、当面の利用を認める。 １）NIST SP 800-67 とし	[削除]

		て規定されていること。 ２）デファクトスタンダードとしての位置を保っていること。	
	運用監視暗号リスト（技術分類：共通鍵暗号）	該当なし	3-Key Triple DES（注１５）
	電子政府推奨暗号リスト	［技術分類の新設］	技術分類：認証暗号 暗号技術：該当なし
	推奨候補暗号リスト		技術分類：認証暗号 暗号技術： ChaCha20-Poly1305
	運用監視暗号リスト		技術分類：認証暗号 暗号技術：該当なし
	（注１３） （注１４） （注１６）	［新規追加］	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て、「認証暗号」として使うことができる。
	電子政府推奨暗号リスト（見出し）	名称	暗号技術
	推奨候補暗号リスト（見出し）		
	運用監視暗号リスト（見出し）		

参考

2011年度第1回暗号技術検討会資料3-2（抜粋）

電子政府推奨暗号リストの考え方の明確化に向けた論点整理

暗号運用委員会事務局

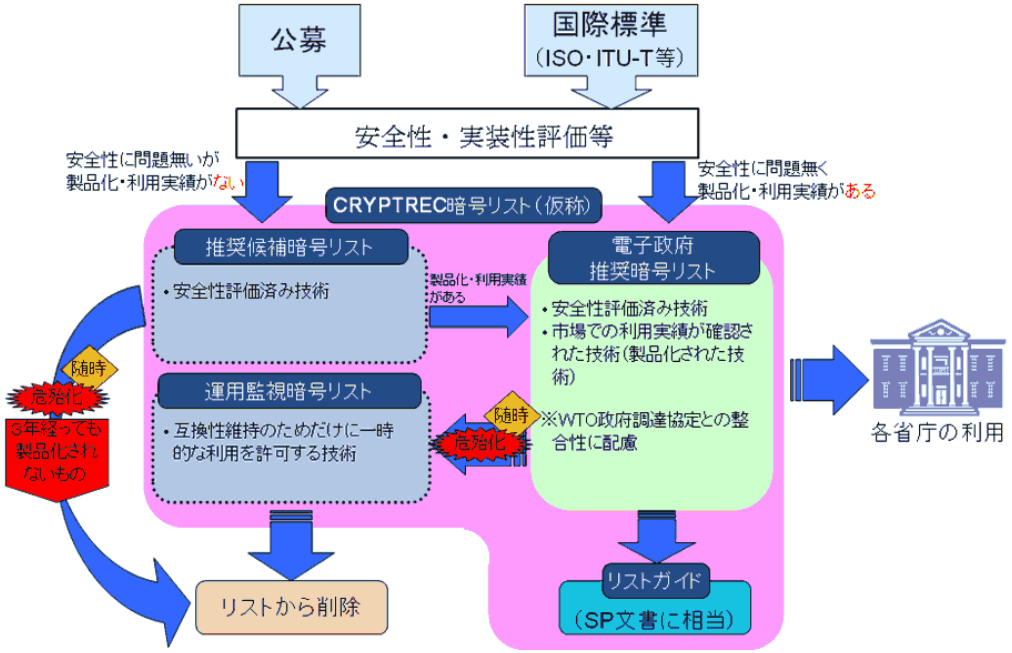
電子政府推奨暗号リストの考え方の明確化の必要性

- 「電子政府推奨暗号リスト」と「推奨候補暗号リスト」の差異をどのように考えるかが不明確だったのではないか
  - 「市場において利用実績が十分」が意味する目的が明確ではない

    ⇒　製品化・利用実績の「ある・ない」の基準についてコンセンサスがない
  - 暗号研究者・暗号学界の意見は反映されても、実際に暗号製品を作っているベンダの意見が反映される仕組みがなかったのではないか

    ⇒　ビジネス展開を実際に担う産業界とのコンセンサス作りが不十分だったのではないか

市場における製品化・利用実績等に関する評価の考え方を決める上で、「電子政府推奨暗号リスト」と「推奨候補暗号リスト」とに与える役割を明確にする必要がある



電子政府推奨暗号リストの考え方の明確化に向けて

- 電子政府推奨暗号リストに「何を求める」のか

  ⇒ それぞれの設定意図を参考に4つのシナリオを設定

シナリオ			推奨リスト例	シナリオの設定意図
No. 1	実際に利用されている暗号だけを電子政府推奨暗号に選定	実際に利用されている暗号だけを電子政府推奨暗号リストに限定することでリストの有効性を高めるために**「現状の調達容易性（利用実績）」を主たる判断材料**としたうえで、有力な標準化規格で必須実装に指定されているなどの「純技術的なその他要件」を考慮	米国政府標準暗号のみ	調達容易性の観点から、特定の暗号アルゴリズムが政府システムにおいて広く利用されている実態を考慮
No. 2	国際標準化・製品化促進の手段として電子政府推奨暗号リストを活用	「安全性」、「現状の調達容易性（利用実績）」、「将来的な調達容易性（利用実績）」の見通しを踏まえつつ、電子政府推奨暗号リストの掲載個数を限定したうえで、提案暗号の普及展開をどのように進めるべきかといった**「非技術的なその他要件」を最大限加味**	米国政府標準暗号＋国産暗号（1 or 少数）	米国政府標準暗号以外の暗号は国際標準化や規格化、製品化からも排除される流れが強まっている点を考慮。 提案暗号に対する国としてのバックアップの明確化
No. 3	一定期間経過後の利用実績不振による電子政府推奨暗号からの降格	当初は電子政府推奨暗号リスト入りさせるが、一定期間経過後の普及状況を厳格に判定する**「将来的な調達容易性（利用実績）」を重要視**	短期的にはシナリオNo. 4。中長期的にはシナリオNo. 1, 2, 4のいずれにもなりうる	提案暗号の普及展開を強力に実施するモチベーションを応募企業に持たせる一方、一定期間経過後の普及展開が思わしくない提案暗号には電子政府推奨暗号リストから降格してもらうルールを新たに導入
No. 4	政府調達の選択肢としての提示	電子政府推奨暗号リストと推奨候補リストとの区分は**「安全性」を主たる判断基準**として行うことにより、現状とほぼ同様の構成	現状とほぼ同様	「調達容易性」を判断することは難しいうえ電子政府推奨暗号リストの掲載個数を削減することによる効果も定かではない点、ならびに暗号研究体制に与えるマイナス影響を考慮

電子政府推奨暗号リストの考え方に対する評価

- 各シナリオを実施した時のメリット・デメリット・留意点の洗い出し

  ⇒　評価軸ごとにメリット・デメリット・留意点を洗い出した後、評価点を採点

≪評価軸≫

A)「安全性」に関する検討項目
推奨暗号の安全性評価の充実度や危殆化に伴う影響・対策有無、等

B)「調達容易性」に関する検討項目
実利用されている暗号との相関度やベンダロックインの懸念有無、等

C)「標準化・規格化等への影響」に関する検討項目
国際標準化（ISO/IEC等）や規格化（IETF等）策定に与える影響、等

D)「提案暗号（国産暗号）の利用促進」に関する検討項目
提案暗号（国産暗号）をサポートするモチベーションや政策支援効果、等

E)「セキュリティ研究体制への影響」に関する評価項目
新暗号開発へのモチベーションや国内セキュリティ研究体制への影響、等

F)「CRYPTREC活動成果」に関する評価項目
CRYPTRECリストの位置づけやCRYPTREC活動成果の対外的効果、等

≪評価点≫

4：メリットのほうがかなり多い
3：どちらかといえばメリットのほうが多い
2：どちらかといえばデメリットのほうが多い
1：デメリットのほうがかなり多い

※ 評価点は、審議過程で抽出されたメリット・デメリットの個数ではなく、メリット・デメリットの効果の大きさで判断
※ 評価点は、解決すべき問題点への対策が実施されたとしての前提で判断（対策が実施されない場合は評価点が変わることがある）

- 各シナリオを実施する時に解決すべき問題点の明確化

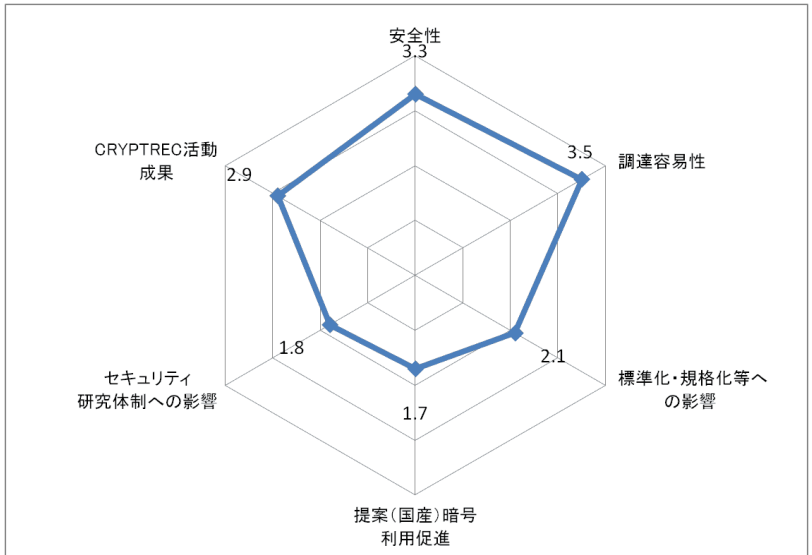
  ⇒　各シナリオを実施する上で考慮しなければならない問題点への対策検討

- 搭載暗号アルゴリズムの選定プロセスの実態をアンケート調査

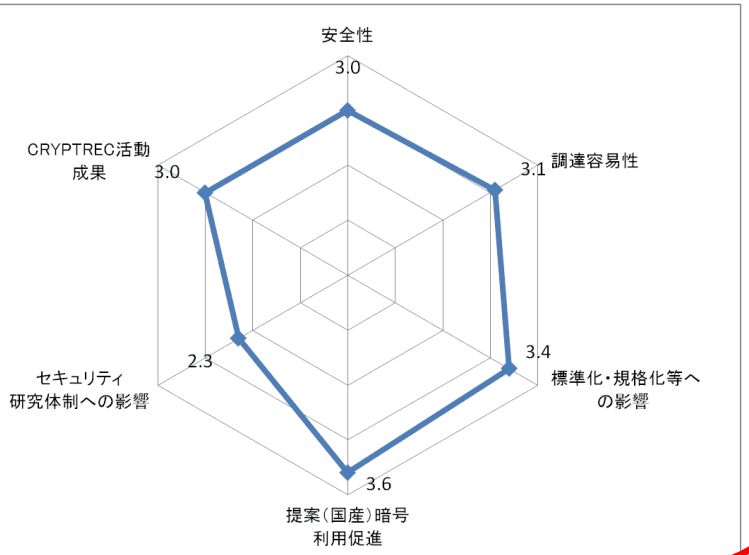
  ⇒　特徴的なメリット・デメリットの抽出や評価点を検討するうえでの基礎情報

評価点比較のまとめ（報告書（案）7.2.4参照）

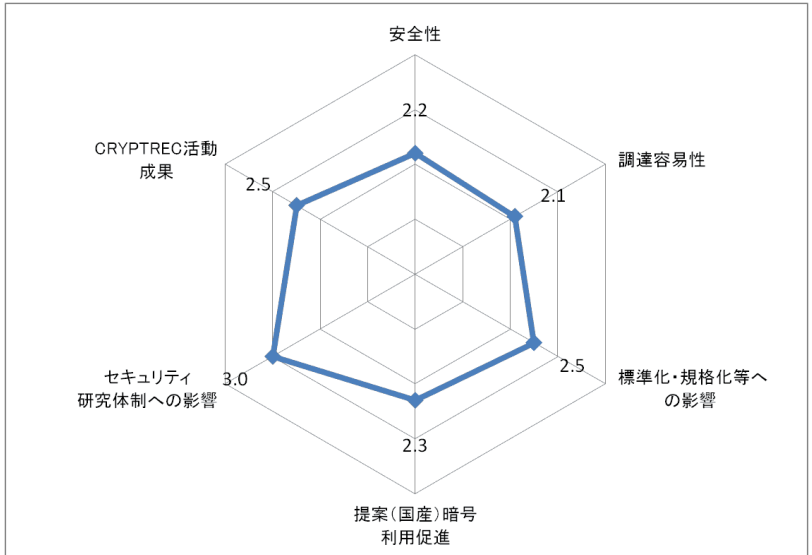
【シナリオ1（実際に利用されている暗号だけを選定）】



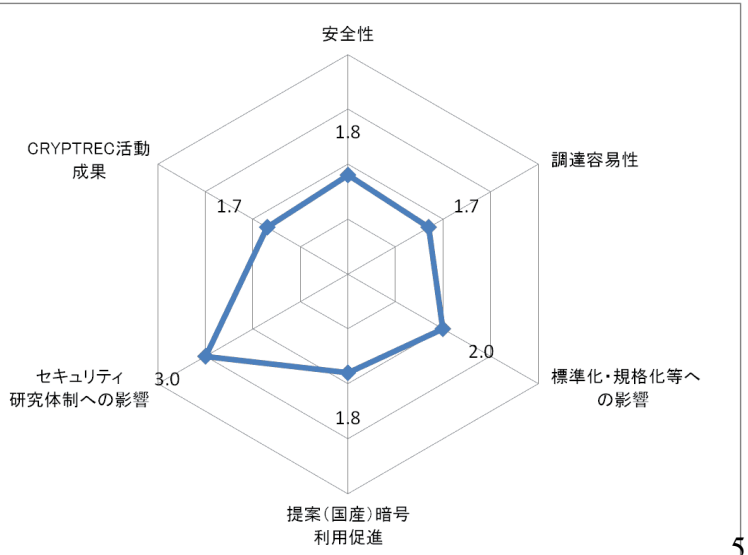
【シナリオ2（標準化・製品化促進の手段として活用）】



【シナリオ3（利用実績不振による降格ルール導入）】



【シナリオ4（政府調達の選択肢としての提示）】



各シナリオを実施する時に解決すべき問題点と対処策案

シナリオ	推奨リスト例	解決すべき問題点	問題点への対処策（案）
No. 1	米国政府標準暗号のみ	①民間で技術者を抱えられなくなる ⇒ 暗号評価、監視が出来なくなる	暗号研究者の公的機関における雇用が必要 （安全な暗号を公的に評価・監視する体制）
No. 2	米国政府標準暗号＋国産暗号（1 or 少数）	①民間で技術者を抱えられなくなる ⇒ シナリオNo. 1よりも顕在化が早いかもしれない ②国産暗号の絞り込みが大変 ③絞り込んだとして本当に使われるのか ⇒ 絞り込むことによるメリットを生かせないとやる意味がない	① 暗号研究者の公的機関における雇用が必要 （安全な暗号を公的に評価・監視する体制） ② 国産暗号が使われるように振興する目的であることを明確化 ②-1 パテントフリー等の実施 ②-2 推奨リストから外れた組織へのフォロー ②-3 ISO等、標準化機関とのリエゾン関係構築 ③ プロトコル等へ展開（注力先の変更）
No. 3	短期的にはシナリオNo. 4。中長期的にはシナリオNo. 1, 2, 4のいずれにもなりうる	①現状と変わらない可能性が高い ⇒ 最終的にいずれシナリオNo. 1やシナリオNo. 4になるのではないか ⇒ 推進する産業政策的意義は少ない ②現状のまま継続してもいずれ民間企業で暗号研究者を抱えられなくなるのではないか ⇒ 気がついたときには、暗号評価、監視をするための体制が構築できなくなっている事態も想定される	未検討（意見出ず）
No. 4	現状とほぼ同様	①現状と変わらないと思われる ⇒ 推進する産業政策的意義が説明できない ②現状のまま継続してもいずれ民間企業で暗号研究者を抱えられなくなるのではないか ⇒ 気がついたときには、暗号評価、監視をするための体制が構築できなくなっている事態も想定される	未検討（意見出ず）