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４回）
議事概要

１．日時
令和３年３月３日（水）10:00～12:00

２．場所
オンライン会議（Webex）

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：伊藤公平（慶應義塾大学）、
木村誠一郎（内閣官房内閣サイバーセキュリティセンター）、
藤原辰悟（警察庁）、岡野孝子（警察大学校）、多賀文吾（警察大学校）、
原嶋美緒（総務省）、朝山直木（法務省）、佐久間明彦（外務省）、
村上匠（外務省）、野口和久（財務省）、山上孝祐（財務省）、
坂本秀敬（文部科学省）、野口信（厚生労働省）、林巧（経済産業省）、
椛木隆慎（防衛省）、柏原陽（個人情報保護委員会事務局）、
花岡悟一郎（国立研究開発法人産業技術総合研究所）
事務局：（総務省）高村信、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、篠原直行、高安敦、青野良範
（独立行政法人情報処理推進機構（IPA））神田雅透

４．議事
（１）本年度の検討内容等について
（２）量子コンピュータに関する動向等について
（３）量子コンピュータに対する暗号技術の動向等について
（４）CRYPTREC暗号リストでの推奨候補暗号リストの取扱いについて
（５）その他

５．配付資料
資料１　これまでの議論と本年度の検討内容について
資料２　量子コンピューティング最前線
資料３　耐量子計算機暗号の動向等について
資料４　量子コンピュータにおける素因数分解の評価について
資料５　量子コンピュータにおける離散対数問題の求解実験について
資料６　CRYPTREC暗号リストでの推奨候補暗号リストの取扱いについて
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）

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）本年度の検討内容等について

資料１について事務局より説明が行われた。主な質疑応答は次のとおり。

宇根構成員：３ページ目の１番で「暗号技術評価委員会にてガイドライン作成検討中」という点について、耐量子計算機暗号に関しては、安全性や性能・処理速度はNISTを中心にやっているかと思うが、これに加えて、Open Quantum Safeプロジェクトであったり、TLS1.3に組み込む暗号ライブラリのプロトタイプをつくったり、そうした動向も、このガイドラインに含めていくということか。

事務局（NICT）：はい。事務局としては拾えるものはまず拾うという方針。ただ、このガイドラインについては、ＷＧを立ち上げることが必要かと考えており、具体的にはそのＷＧの意向に従う予定。

宇根構成員：アメリカでの標準化というものがあると思うが、今後、耐量子計算機暗号の利用や実装に関する動向を見ていく上では、プロトタイピングであるとか実際に実験した場合の評価であるとか、そうしたところも重要になってくると思う。そうした産学の欧米での検討等も、調査のスコープに入れ、ＷＧで検討いただけるとありがたい。

事務局（NICT）：承知した。

國廣構成員：４ページ目に「（Ｐ）」とあるが何を意図しているか。

事務局（総務省）：ペンディングの「Ｐ」で、明確にこの時期にこれが出来上がると言っているようなものではないという意図。詳細については別途開催される暗号技術評価委員会でも議論されるかと思うが、22年度中の完成を目指している。

（２）量子コンピュータに関する動向等について

資料２について慶應義塾大学の伊藤教授より説明が行われた。主な質疑応答は次のとおり。

高木構成員：Quantum volumeに関して伺いたい。CRYPTRECでは、ムーアの法則を使って、スーパーコンピュータの計算能力がどれくらい伸びるかということで、暗号の安全性を評価している。Quantum volumeが毎年倍々で伸びていくということだが、その見通しというのは、伊藤先生の視点からどのようなものか。

伊藤教授：おそらく加速していくと思う。逆に言えば、この倍々だと、使えるようでいて大して使えない。というのは、今年、７つの量子ビットで７段の深さのコンピューティングが正確に行えるということだとすると、それだけではまだ足りない。実際にHoneywellは、Quantum volumeを何万レベルにできると言っているし、競争が相当激しくなっている。さらに、Quantum volumeというのは、普通のコンピュータで検証できることが前提となっているので、Quantum volumeという指標自体も、ある時点では、例えば３年ぐらいしたら使えなくなる可能性もあるのかと思っている。

國廣構成員：Quantum volumeについて、「高精度計算が可」とある「高精度」ということが重要かと思うが、どの程度の高精度をイメージしているのか。

伊藤教授：Quantum volumeというのは、古典コンピュータのシミュレーションに対して、この程度の範囲に入っていれば合格、例えば８割以上だったら合格といったような考え方でやっている。

國廣構成員：誤り訂正をしないぐらい高精度かと思ったのだが。

伊藤教授：そういうわけではない。我々はIBMを使っているが、Google、IonQ、Honeywell

などを使っていく人がいるということは、この指標のみならず全体として実感する人が必要だということを感じている。

満塩構成員：100原子超分子や1,000原子超分子の計算では、ハードウェアに加えて、ソフトウェアと協調した子育てが必要だという説明があった。我々として、ハードウェアのところを注目していればいいのか、プログラム言語であるとかソフトウェアの影響はまだそんなにはないということか、そのあたりの感覚を教えてほしい。

伊藤教授：量子の世界をどうやって量子で表せるかということは、量子力学的、物理的な考察もいろいろ入ってきて、それがアルゴリズムになっていくので、その工夫が上手にできていくと、アルゴリズム的な工夫で、飛躍的に良くなっていく。ただ、それをどうやって指数関数的な発展に結びつけていくかということは、ハードウェアの発展にも頼らなければいけないので、そことのインタープレイだと思っている。

（３）量子コンピュータに対する暗号技術の動向等について

資料３から資料５までについて事務局より説明が行われた。主な質疑応答は次のとおり。

松井構成員：資料５について、離散対数問題の研究があまりないのは、まだ研究者がそちらに目が向いてないのか、それとも離散対数問題ならではの難しさがあるのか。

事務局（NICT）：おそらく暗号の人間としては目が向いており、量子デバイスの専門家からすると向いていなかったのではないかと思う。ただ実際にやってみて分かったことは、離散対数問題ならではの後処理の部分に、かなり素因数分解と違う難しさがあり、アルゴリズム的に結構難しいことをしなければいけないので、そこが量子の方には難しくハードルが高かったのではないかと思う。

宇根構成員：今回、離散対数問題を考えられたわけだが、ECDLPも同じような感じだと考えてよいか。

事務局（NICT）：はい。基本的に回路の設計としてはほぼ同じで、ECDLPに関わる楕円曲線の点の加算を行うところだけが違うことになる。

松本勉座長：ECDLPだと、一番小さい例を作ろうとしても、今回出てきたようなサイズではできないと思うので、多分、実験的にやるのはもう少し先でないと難しいのではないか。

事務局（NICT）：そのとおりだと思う。ECDLPの場合だと、おそらく掛け算と、剰余つきの除算も入ってしまうので、かなり回路が複雑になり、一番小さいインスタンスでも今すぐにできるようなものではないとは思う。

高木構成員：Quantum volumeに代わるものがあったほうがいいということだが、どういったものが暗号の評価に適するという、何か候補みたいなものはあるか。

事務局（NICT）：今のところ、候補と呼ばれるようなものはなく、量子コンピュータの様々な実験、暗号以外でも実験はされているので、そうした論文で成功したということをどうやって定量的に評価しているのかを調査している段階。

高木構成員：CRYPTRECでスーパーコンピュータの性能を指標にしているが、そのような何か指標をうまく暗号に持ってこられるものがないかということは課題ということか。

事務局（NICT）：そのとおり。それができれば、ある程度は将来予測ができるようになる

と思うが、まだ解決されておらず大きな課題。

國廣構成員：Quantum volumeはあくまでもデバイスの評価。古典の場合も、スーパーコンピュータがどれくらいの精度で伸びるかという、あくまでも計算機性能の話であって、どのような問題を取り扱うかということまでは加味していない。なので、暗号の予測ができるものが果たして必要なのか、よく分からない。

事務局（NICT）：研究集会で発表した資料をベースにしているので個人的な感想も入ってしまっているが、離散対数を計算する能力を測ることに特化した指標を作ることができれば、それをもとに暗号解読の能力を測るための指標に拡張できるのではないかという趣旨。

國廣構成員：ある意味、我々の立場からすると、汎用の量子計算機は必要ではなくて、離散対数問題専用の量子計算機があればよく、その指標があればいいということか。

事務局（NICT）：そのとおり。

國廣構成員：資料３で、RainbowとGeMSSのアタックが出てきているという話があったが、これはどれくらいクリティカルなものなのか。

事務局（NICT）：詳細は確認中だが、セキュリティーパラメータが変わるのは仕方なさそうである。NISTの候補から落ちるかどうかについては、それならほかの格子ベース方式ももっとチェックしないといけないのではないかという意見も出ており、新たな攻撃の提案によってRainbowとGeMSSが消えるというところまではまだ言えないとは思う。

國廣構成員：とりあえずRainbowとGeMSSはパラメータを変えることによって、ファイナリストのままであるけれども、その一方で一応リスクヘッジのために、SPHINCSをファイナリストに上げようかという議論もあるということか。

事務局（NICT）：はい。文献を見ていると、このRound 3は実装性能などを重視して絞っている印象があり、そのため鍵長を大きくすると実装性能が落ちることになるので、ファイナリストとしてRainbowやGeMSSはどうなのかと物言いがついているのだと思う。なので、もう一度全体的に、格子や符号や多変数なども、詳細な安全性評価を行い、セキュリティーレベルを達成するための鍵長を精査しないといけないという議論が進んでいると思っている。

高木構成員：RainbowとGeMSSは、私の方でも研究しているが、Rainbowに関しては、多項式時間のアタックがあったわけではなくて、ランク攻撃という指数軸が少し下がったということ。ただし、Rainbowのチームは、メモリが非常に必要なので、パラメータを変えなくても、その攻撃は影響がないということも主張していて、そこは今議論が分かれているところ。GeMSSは、HFEv-という問題のマイナスモディファイヤーが効かないということで、こちらはかなりクリティカルな話になっていると思う。

高木構成員：資料５について、重要だと思うので、もう一度話したいのだが、先ほどスーパーコンピュータの話が出てきたが、スーパーコンピュータをなぜCRYPTRECで採用しているかというと、LINPACKという線形代数を解く計算問題が、数体ふるい法の計算問題に近いだろうということで、非常に相性が良いということで採用している。量子コンピュータでも、LINPACKのような問題コンテストが始まれば採用できるかと思った。

宇根構成員：資料４の９ページ目で、素因数分解アルゴリズムのパラメータごとの比較を示していたが、ページ下の「[GE19]による共通の設定」として示された数値は、量子コンピュータを考えたときには、現状この程度は実現できるだろうという意味で妥当な設定だと理解してよいか。

事務局（NICT）：現在の量子コンピュータでこれらの数値が実際に達成されているかはわからないが、このくらいを見積もっていれば妥当な線だろうという設定になっていると思う。

（４）CRYPTREC暗号リストでの推奨候補暗号リストの取扱いについて

資料６について事務局より説明が行われた。主な質疑応答は次のとおり。

松本勉座長：まず、２ページ目、「推奨候補暗号リスト自体は維持することでよろしいのではないか」という点について、異論はあるか。

松本勉座長：異論ないということで、確認した。

松本勉座長：続いて、推奨候補暗号リストからの移行ルールを明確化すべきではないかということで、３ページ目、「②推奨候補暗号リスト」から、「①電子政府推奨暗号リスト」に移行するルールについて意見をいただきたい。

高木構成員：５年ごとの利用実績調査について、全ての方式を調査するのは大変なので、電子政府推奨暗号リストにしようとする候補に関して調査するということでよいか。

事務局（IPA）：利用実績調査については、アルゴリズム名は既に書いてあり、使っている、使っていないをチェックしてもらう形式のアンケートを実施する。そのため、アルゴリズムを絞ったから簡単になる、多いから複雑になるということはなく、全部のリストのアルゴリズムを載せることを想定している。なお、委員会に提示して評価をする段階では、結果を絞り込んで提示する可能性はある。

満塩構成員：推奨候補暗号リストから削除することも考えると、ある程度網羅的な調査にならざるを得ないかと思う。現状の推奨候補暗号リストは、最初に掲載されたのは何年になるのか。

事務局（総務省）：推奨候補暗号リストという構成にしたのは2013年になるが、CRYPTREC暗号リストとして暗号技術が掲載されたのは最初の2003年になる。今年は2021年であり、18年間掲載されていることになる。

松本勉座長：まず、網羅的な調査について、アンケートをどこに聞くかということに対する網羅性をどう考えるかという問題はあるかと思うが、CRYPTREC暗号リストに掲載されているものを全部調べることはそれほどコストがかからないという発言もあり、そのとおりかと思う。

そして削除する件については、この後で議論したいと思う。まず、「②推奨候補暗号リスト」から「①電子政府推奨暗号リスト」への移行に関しては、利用実績があれば移すことが妥当であろうということで、具体的な方法として、５年ごとの調査は必ず行い、エマージングな状況が起きた場合には、それも救えるようにするために２番目の項目（その他、普及していることが明らかな場合）があるということと理解。

さらに質問はあるか。

松本泰構成員：利用実績調査は過去にも実施しているかと思うが、暗号技術が様々なところで使われており、重要になっていると感じている。今まではＩＴシステムにおける暗号技術だったが、IoTやサイバーフィジカルシステムなど使われる場面が相当変わってきており、そうしたところに対して、いつまで使いたいかとか、例えば機器に組み込む場合にどのくらいの期間使いたいかとか、そのあたりも併せて調査してもらえると、基礎資料になるのではないかと期待している。

松本勉座長：調査をする際に、今のような視点に対する回答が得られるように工夫するとよいのではないかということと理解。それでは、「②推奨候補暗号リスト」から「①電子政府推奨暗号リスト」への移行について、方針に賛同いただける方は、挙手ボタンをお願いしたい。
皆様、挙手をいただいたので、提案のとおりとしたいと思う。

松本勉座長：続いて、「②推奨候補暗号リスト」からの削除について、CRYPTREC暗号リスト掲載から20年を超えた後に実施する最初の利用実績調査までに十分な利用実績が確認できなかった場合に削除する。利用実績調査は直近でいつ行うことになるのか。

事務局（IPA）：令和４年、2022年に実施する予定。CRYPTREC暗号リストができたのは2003年であるので、2022年だと20年は超えておらず、2022年の調査で削除されるものはない。その次の2027年の調査で、初めて削除に該当するアルゴリズムが出てくるかどうかというところ。

宇根構成員：20年という期間は長いのではないか。５年ごとの利用実績調査で「①電子政府推奨暗号リスト」に上がるので、削除も同じように、５年ごとの利用実績調査で利用実績が確認できなければ、リストから削除というほうが自然ではないか。調査工数を減らす観点からもシンプルになる。
また、例えば推奨候補暗号リストに掲載されているものは昔からのものもあり、ベンダーの立場からすると掲載されている限りは政府で使われているかもしれないのでサポートを続けないといけないということで、コストになっているのではないか。

事務局（総務省）：まず、５年ごとの利用実績調査という観点だが、利用実績調査は５年ごとであり、推奨候補暗号リストへの掲載タイミングによっては、掲載の１年後になるかもしれないし、４年後になるかもしれないので、必ずしも掲載から５年間が確保されるわけではない点がある。また、そもそも20年にした理由としては、暗号技術が「①電子政府推奨暗号リスト」に上がる可能性があるものは、できる限り残したほうがよいと考える一方で、20年経過すると暗号の世代としてかなり古くなっているということがある。過去の暗号技術の例を見ても、20年を超えた上で発展していくというものも、なかなか想像しにくいということで、20年という期間を設定した。

事務局（IPA）：普及の度合いを考えると５年は短すぎる気がする。実際にアルゴリズムができて、ある程度認知され、標準化や規格化が始まり、その後に実装が始まるので、それを考えると、最初のスタートだけで５年ぐらいかかり、その後の５年が実際の普及期に入るかということで、最低10年は、普及するかどうか判断のためには必要かと思っている。20年ではなく15年かという議論はあるかもしれないが、10年より短いというのはないのではないか。

松本勉座長：そのほか宇根構成員の御意見で、既に掲載されているものについて責任があり、出し元がもうやめたいというようなこともあるのかと考えたが、その場合、次の次の利用実績調査なので７年後になってしまうということ。このあたり、御意見いただければと思うがどうか。

松井構成員：基本的な方針としては、これでよいかと思う。「②推奨候補暗号リスト」の意義としては、もちろん「①電子政府推奨暗号リスト」に上がる候補であるという位置づけとともに、実際問題として現在使われているものにお墨つきを与えているという、そうした側面もあるかと思う。例えばベンダーがもうやりたくないというものは削除すればよいと思うが、削除となると、その暗号は使うなと国が言っているという、かなり強いメッセージを発することになるので、それなりの慎重さも必要かと思う。

実際に暗号技術活用委員会で具体的な議論がされることになるかと思うが、ある種の慎重さというか、柔軟性というか、そうしたものをもってやることが重要であり、そうした運用としてできるのであれば、20年か15年かという議論はあるかもしれないが、基本的には記載された方針でよいと思う。

松本勉座長：柔軟性は、例えばどういう点か。

松井構成員：例えば利用実績が何％とかデジタルに決めてそれ以下を落とすという、ある意味公平性という観点からきっちりとしたものを決めがちだが、どうしてもそうしてしまうと、実際に使われているものを見落としていることにならないかということを少し心配しているという意味。

松本勉座長：何を持って利用実績とするかという判断について、慎重に検討すべきだという御意見だと承った。そのほか、御意見はあるか。

満塩構成員：方針自体への意見ではないが、参考資料のCRYPTREC暗号リストを見ていると、いつから掲載されているか、いつ頃落ちそうかがわかると、現場の例えばレビューや助言をする立場からはありがたい。

松本勉座長：御意見に感謝。それでは、「②推奨候補暗号リスト」から削除することに関する方針について、御賛同いただける方は、挙手ボタンをお願いしたい。

御賛同いただけたと判断する。

（５）その他

暗号技術検討会への今年度の取組報告については、電子メールで確認いただいた上で、意見取りまとめに関しては座長一任で取りまとめることとなった。

６．３．閉会

事務局から本日の議事概要の確認については別途メール等連絡する旨の説明が行われた。

松本勉座長から開会の宣言があった。

以上