2018 年度 暗号技術検討会 議事概要

1. 日時

平成 31 年 3 月 29 日（金）10：00～11：30

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（座長）、上原哲太郎、宇根正志、太田和夫、岡本龍明、高木剛、
近澤武、酒井康行（松井充代理）、松浦幹太、松本泰、向山友也、渡邊創

オブザーバ：一ノ瀬宏昭、岡田崇志（三原祥二代理）、佐々木駿（吉田和彦代理）、
足立直（小高久義代理）、寺田麻倫（阿部知明代理）、小野田和靖
（宮崎拓也代理）、土本雄介（髙橋良明代理）、西城泰裕（竹田和彦代理）、
佐藤誠一（原口剛代理）三島崇（中野宏和代理）、二宮勉、庭田椋介
（下井善博代理）、宮崎哲弥、大澤昭彦、栗田学（和田雅昭代理）

事務局：（総務省）竹内芳明、泉宏哉、赤阪晋介、豊重巨之、吉永勇輝
（経済産業省）三角育生、土屋博英、稲垣良一、飯山貴啓
（国立研究開発法人情報通信研究機構（NICT））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）　2018 年度 暗号技術評価委員会 活動報告について
（２）　2018 年度 暗号技術活用委員会 活動報告について
（３）　次期 CRYPTREC 暗号リストの改定に向けた検討について
（４）　「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」の設置について
（５）　暗号技術検討会　2018 年度　報告書（案）について

5. 配付資料

資料１	議事次第・配付資料一覧
資料２	暗号技術検討会　構成員・オブザーバ名簿
資料３	2018 年度 暗号技術評価委員会 活動報告
資料３別添１	2018 年度 暗号技術調査 WG（暗号解析評価）活動報告
資料３別添２	耐量子計算機暗号の研究動向調査報告書（案）
資料４	2018 年度 暗号技術活用委員会 活動報告
資料４別添	鍵管理システム設計指針（基本編）　ドラフト素案
資料５	次期 CRYPTREC 暗号リストの改定に向けた検討について
資料５別添	「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」の

設置について（案）
資料６　暗号技術検討会　2018 年度　報告書（案）
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

暗号技術検討会事務局から開会の宣言があり、総務省の竹内サイバーセキュリティ統括官から開会の挨拶が行われた。その後、暗号技術検討会事務局より、今井構成員、手塚構成員、本間構成員及び松井構成員が欠席である旨の連絡がなされた。

6.2. 議事

（１） 2018 年度 暗号技術評価委員会 活動報告について

資料３及び別添に沿って、暗号技術評価委員会事務局より報告が行われた。主な発言は以下のとおり。

松本座長　：（予測図の更新について）確かに、量子計算機の素因数分解に対する有効性を見るのはまだ難しい段階だと思う。

（２） 2018 年度 暗号技術活用委員会 活動報告について

資料４及び別添に沿って、暗号技術活用委員会事務局より報告が行われた。主な質疑は以下のとおり。

宇根構成員：鍵管理に関する成果は網羅的にまとまっており、役立つだろう。ドラフト版の公表は秋頃になるのか。
事務局　：７月に開催される CRYPTREC シンポジウムにてドラフト版を公表予定。
松本座長　：７月のシンポジウムではどのようなレベルのものをドラフトとして公表するのか。
事務局　：どこまで文書化できるかによるが、Word 形式のものを想定している。ただ、実際には文量が多く、すべての文書化は難しいと考えている。資料４別添９ページ目以降はパワーポイントで、８ページまでの説明を文書に起こしていくイメージで進めたいと思う。
松本座長　：資料４別添の４ページにある俯瞰図について、このような流れで考えた場合、例えば米国の Profile Requirements のようなものが、公表されていないだけで日本にも存在したりしないのか。俯瞰図一番右側の System Requirements は日本でも作られていると思うが。

事務局　　：そこまでは調べられていない。

松本座長　：Profile Requirements は業界によっては存在していると思うが、抜け漏れがないように、このような体系的な整理が必要になるだろう。

宇根構成員：金融業界では、フレームワークやプロファイルを精緻化するのは有用だと考える。金融業界においても鍵管理についてざっくりと整理したものはあると思うが、鍵管理を体系的にどのように実施すべきかを整理する取組は非常に重要。金融業界では、これまでも CRYPTREC の鍵管理リストガイドを参照しているので、今回の取組も非常に有用だと思う。

松本構成員：鍵管理ガイドラインの話は、非常に複雑な話になっているが、これは暗号技術の世の中での使われ方が大きく変化していることに起因していると認識している。これまでは情報システムの中で暗号技術は使われてきたが、今は情報システムだけでなく、インダストリーの中でも使われるように変わってきた。現在、一番暗号技術が組み込まれようとしている分野に自動車分野がある。車の中の各 ECU に暗号技術が組み込まれようとしており、車の仕組み自体にパラダイムシフトが起きている。これからは、数百億個の IoT デバイスにも暗号技術が組み込れていくことも考えられ、こうしたことに対応した暗号鍵管理の在り方が必要になるだろう。

仮想通貨の場合も然り、暗号鍵管理の仕方次第で約 600 億の被害が発生した。一つの暗号鍵が数百億の価値と結び付く時代でもある。世の中の変化や、どのように暗号技術が使われているかが理解できないと、暗号技術における暗号鍵管理が必要性も理解いただけないだろう。Society5.0 における暗号技術では、世の中の変化や技術の使われ方を把握し、今までとは違う暗号鍵管理の考え方が必要だと考える。

（3） 次期 CRYPTREC 暗号リストの改定に向けた検討について　　及び

（4） 「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」の設置について

資料５及び別添に沿って、事務局より説明が行われた。主な質疑は以下のとおり。

宇根構成員：タスクフォースの設置に賛成。耐量子計算機暗号に対する技術的な検討についても賛成。両委員会で出た意見の中で、量子計算機の性能が今後どうなるか予想ができないことはそのとおりだが、だからと言って、時間が経つとリスクも移行のコストも上がると思う。

金融業界でも耐量子計算機暗号に注目している。量子コンピュータが現実のものになると金融システムで使用している暗号も総入れ替えとする必要があるが、現実的には、金融システムの暗号を総入替えするのには少なくとも 10 年はかかると見ている。早めの対応が必要。また、各金融機関で一斉に暗

号を入れ替えようとすると、それらに対応するためのベンダーの人手不足によって暗号の入れ替えにかかる期間が延びる可能性があるほか、工数の単価が上昇し暗号の入れ替えにかかるシステム対応の費用が増加する可能性がある。対応には何が必要か早めに検討する必要がある。こうした事情は、電子政府においても同様ではないだろうか。どういう順番で何が必要になるか、余裕をもって対応できるようにタスクフォースで議論頂きたい。

松本構成員：宇根構成員は入替えに 10 年と言われたが、私は 10 年では無理で 20 年、30 年かかると見ている。PQC は移行問題が一番の肝。RSA1024 からの移行も 10 年くらいかかっており、PQC への移行は、それとは比較にならないくらい時間がかかると考えている。移行のための標準化も必要になると思う。
タイトルでは「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」とあるが、その前に Society5.0 時代の暗号技術を考えるべきでないか。IoT デバイス向けの軽量暗号も必要ではないか。それも重たい問題だと考えている。2000 年代の暗号リストは、客観的に評価された暗号アルゴリズムを定着させることが目的だった。今は、多様に利用される暗号技術をどう整理するかが重要だと考える。

松本座長　：タスクフォースの検討事項の中に「その他新たな暗号技術の動向」と入っているので、スコープとしては松本構成員の意見も入っていると思う。他方、タイトルが量子コンピュータだけではないだろうという点は、確かに、耐量子計算機暗号を使わなければいけないという前提であればこう名付けているが、移行に 10 年、20 年かかるという見通しの一方で、資料３別添の現状の量子コンピュータの素因数分解の性能を見ると、先の予想が全く付かない。最終的に耐量子計算機暗号への移行は必要ないという見解に至る可能性もある。そういう情勢で、どこまで耐量子計算機暗号の対応を検討するのか、またその検討にどれほど投資できるかということも考えなくてはいけないので、こういうタスクフォースを作らざるを得ない。

宇根構成員：安全性のためには RSA の鍵長を更に伸ばすと言う意見もあって、それから耐量子計算機暗号に移行するというのもあると思う。CRYPTREC 暗号リストの使われ方にも関係するが、金融分野では、安全性が客観的に評価されていない独自暗号を排除するためにも CRYPTREC 暗号リストが参照されている。逆にリストに載っていないと金融業界では使われないことが少なくない。そのような状況であるので、CRYPTREC 暗号リストに耐量子計算機暗号が載っていないと、金融業界としても、採用すべき暗号の検討対象外になってしまうと考えられる。耐量子計算機暗号を暗号リストに掲載することは、選択肢を増やしておくという意味があると思う。利用期間の長いシステムや、多くの関係機関と調整する必要があるシステムは、暗号の移行に期間がより

必要となるので、暗号リストに耐量子計算機暗号を掲載してあるとよいのではないか。

高木構成員：資料で RSA2048 は 2030 年まで可能、その先は、危殆化予想図にも関係するが鍵の長さをどうするかを書いてはどうか。

宇根構成員：来年度の検討の中で考えていくということか。

松本座長　：本件は審議事項であるので、タスクフォースを設置してよいか結論を出したいが、設置してよろしいか。異論無しとして、本件は承認させていただく。

（5） 2018 年度 暗号技術検討会 報告書（案）について

資料 6 に沿って、事務局より説明が行われた。主な質疑は以下のとおり。

松本座長　：骨子としては 10 ページが重要、それ以外の部分はこれまでに両委員会から報告された内容が組み込まれていると承知。

松浦構成員：今回のポイントは 10 ページとのことだが、タスクフォースの検討事項としては「（2）その他新たな暗号技術の動向等（軽量暗号や秘密計算に利用される準同型暗号等）を踏まえた検討等」も重要だと考える。先ほど自動車の例が出たが、既に大きな産業だけではなくて、本検討中に大きく成長する産業についても考える必要があって、プリミティブな暗号リストの使われ方が広がるだけではなく、成長産業において使われている技術に暗号技術を取り入れようという動きも増えるだろう。ブロックチェーンはまさにその一つであり、これまでの署名を使わず、新しい暗号技術を使うという話である。研究者の間では高機能暗号と呼んでいる暗号技術も数多くあるが、新たに暗号技術として出てくるものは CRYPTREC としてどこまで対応するか検討が必要になる。タスクフォース名に入れるのは難しいと思うが、タスクフォースの説明には（2）も重要だと記載すべき。後々、タスクフォースが設置された経緯について参照されることもあるので。

松本座長　：文言を調整して盛り込んでいただきたい。これはいつまでに確定させる必要があるのか。意見を出すのはいつまで許されるか。

事務局　　：本日の議論を踏まえて事務局で案文を作った上で、再度審議を行いたい。1 週間程度で確定させたい。

松本座長　：提示されたスケジュールを踏まえ、意見があればそれまでに提出し、修正されるという前提で本件を承認していただけるか。
皆様にも修正された文書はご確認いただくが、最終的には座長と事務局で確定したい。

6.3. 閉会

経済産業省の三角審議官から閉会の挨拶が行われた。

以上