2020年度 第１回 暗号技術検討会 議事概要

１．日時

令和２年６月19日（金）10:00～12:00

２．場所

オンライン開催

３．出席者（敬称略）

構成員：松本勉（座長）、今井正道、上原哲太郎、宇根正志、太田和夫、高木剛、近澤武、
手塚悟、本間尚文、松井充、松本泰、向山友也、渡邊創

オブザーバ：川崎明彦（一ノ瀬宏昭代理）、矢田晴之（三原祥二代理）、管野学（吉田和彦代理）、
千葉英之、服部直樹（篠原辰夫代理）、野口和久（澁谷弘一代理）、
西城泰裕（坂本秀敬代理）、荒木弘二（田平浩二代理）、林巧（中野宏和代理）、
大橋洋一、久保田実、花岡悟一郎（寶木和夫代理）、瓜生和久、大澤昭彦、
戸田裕之

事務局：（総務省(MIC)）二宮清治、赤阪晋介、梅城崇師
（経済産業省(METI)）三角育生、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) 「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」の検討状況及び活動について
(2) 2019年度暗号技術評価委員会 活動報告について
(3) 2019年度暗号技術活用委員会 活動報告について
(4) XTSの推奨候補暗号リストへの追加について
(5) 運用監視暗号リストからの削除ルール及びRC4の取扱いについて
(6) 暗号技術検討会 2019年度 報告書（案）について
(7) 2020年度暗号技術評価委員会 活動計画について

５．配付資料

資料１	議事次第・配付資料一覧
資料２－１	「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」の検討状況について
資料２－２	「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」の活動について
資料３	2019年度暗号技術評価委員会 活動報告
資料３別添１	現在の量子コンピュータによる暗号技術の安全性への影響
資料３別添２	暗号利用モードXTSについて
資料３別添３	2019年度暗号技術調査WG（暗号解析評価）活動報告
資料４	2019年度暗号技術活用委員会 活動報告
資料４別添１	EdDSAに関する安全性評価の必要性について
資料４別添２	暗号鍵管理システム設計指針（基本編）概要

資料４別添３　TLS暗号設定ガイドライン概要
資料５　　XTSの推奨候補暗号リストへの追加について
資料６　　運用監視暗号リストからの削除ルール及びRC4の取扱いについて
資料７　　暗号技術検討会　2019年度　報告書（案）
資料８　　2020年度暗号技術評価委員会 活動計画(案)
参考資料１　暗号技術検討会　開催要綱（構成員・オブザーバ名簿）
参考資料２　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

事務局から開会の宣言があり、総務省の二宮審議官から開会の挨拶が行われた。その後、事務局より、初めてのオンライン開催となったことから開催要綱を改訂して旨の説明がなされた。

また、本会合の議事(1)から(6)までについては、感染症対応等の影響により2019年度内に開催できなかった暗号技術検討会にて報告・審議予定であった案件であり、形式上、2020年度の第１回検討会として開催している旨の説明がなされた。

６．２．議事

(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」の検討状況及び活動について

資料２－１及び資料２－２について事務局より説明が行われ、資料２－２については原案のとおり決定された。主な質疑内容は以下のとおり。

太田構成員：暗号が危ないという報道がされることがあるが、資料によれば、量子ビット数だけでなく周辺状況を踏まえても、現状の量子コンピュータによって現在使用されている暗号技術が解かれるには、まだかなり余裕があるということであった。こうした内容を情報発信していくことが重要である。

高木構成員：その点に関しては、本年２月にCRYPTREC 暗号技術評価委員会からの注意喚起として、量子超越に対するCRYPTRECの見解となるものをWebサイト上で公表している。

宇根構成員：ゲート型だけではなくアニーリング型の量子コンピュータについても、素因数分解問題に適用する研究も出てきており、タスクフォースのスコープとして検討する必要がある。

事務局(MIC)：量子コンピュータの動向については、ゲート型に限らずアニーリング型を含めてフォローしていきたい。

本間構成員：資料２－１ではゲート型の方が脅威となり、素因数分解された最大の数は21とある。一方、アニーリング型を模倣したものでも素因数分解ができたという論文が出ており、必ずしもゲート型が優れていると言い切るのは危険ではないか。

高木構成員：CRYPTRECの暗号解析WGでアニーリング型の動向も把握しており、素因数分解記録はアニーリング型のほうが大きいということも承知している。ただし、アニーリング型はShorのアルゴリズムのように多項式時間で解けるものではなく、より大きなビットを素因数分解するには指数関数的にゲート数が増大するためスケールせず、理論的に脅威はないと認識している。

向山構成員：総務省が意見募集している「IoT・5Gセキュリティ総合対策2020」において、「大規模な量子コンピュータの実用化により、現在の公開鍵暗号が容易に解読されるおそれがあることを踏まえ」とあるが、先ほどの議論ではまだ容易には解読でき

ないということであり、整合をとったほうがよい。
事務局(MIC)：御指摘を踏まえ、脚注を加える等により正確な表現としていく。
松本泰構成員：「大規模な量子コンピュータの実用化」という表現があるが、現状の「実用化」は、必ずしも公開鍵暗号を解く方向ではなく、誤りがあってもよいような実用化が進んでいるためミスリードがあるのかと思う。
事務局(MIC)：タスクフォースを設置したときの文言を引用したものだが、不正確に捉えられるようであれば修正をしていきたい。

(2) 2019年度暗号技術評価委員会 活動報告について
(3) 2019年度暗号技術活用委員会 活動報告について

資料３及び資料４について事務局より説明が行われた。主な質疑内容は以下のとおり。

宇根構成員：量子コンピュータが共通鍵暗号の安全性に及ぼす影響に関する外部評価の調査報告についても重要と考えるが、公表タイミングはどうなっているか。
事務局(NICT)：数ヶ月以内には公開する予定である。
宇根構成員：TLS暗号設定ガイドラインについてはいつ頃公表予定か。
事務局(IPA)：７月上旬を目途に公表予定である。

近澤構成員：TLS暗号設定ガイドラインについて、概要資料のp.8に「利用禁止暗号」として具体的なアルゴリズムが出ているが、ガイドラインとして公表された際にISO規格を明示的に排除してよいのかという点が気になった。
事務局(IPA)：概要資料のp.8の図そのものはガイドラインには掲載していないが、高セキュリティ型、推奨セキュリティ型、セキュリティ例外型の各セクションにおける利用禁止暗号は明示している。また、利用禁止暗号については、その考え方についてもガイドライン中に明確に示している。

(4) XTSの推奨候補暗号リストへの追加について

資料５について事務局より説明が行われ、注釈の記載方法については座長一任とした上で原案のとおり決定された。主な質疑内容は以下のとおり。

宇根構成員：条件１で「利用用途はNIST SP800-38Eの規格に沿ったストレージデバイス」とあるが、単なるストレージデバイスではなくNIST SP800の規格に沿ったものという限定をかけているのか、それとも一般的なストレージデバイスはNIST SP800の規格に沿ったものという意味か、どちらであるのか。
事務局(NICT)：NIST SP800-38E規格に限定されたものということである。
松本座長　：「規格に沿った」という表現は「暗号化」と「ストレージデバイス」のどちらに係っているのか。
上原構成員：XTSというのは、ストレージデバイスの暗号化にしか使えないようなブロック暗号であって、その「規格に沿った」が係るところは、「ストレージデバイスの暗号化」全体に係るという理解をしている。
松本座長　：その理解であり、その意味で抵抗なく読めるかどうかが宇根構成員の懸念かと思う。ストレージデバイスの暗号化が、NIST SP800-38Eに規定されているもの以外にもあり、そうした中で特定のものに限っているのかどうかがわかりにくい。
宇根構成員：その通り。ストレージデバイスの規格かと思ったが、そうでないとわかった。

松本座長　：条件である注釈の記載ぶりについては事務局と検討し、最終的にメールで御報告するという形で進めさせていただきたい。
宇根構成員：それで問題ない。
松本座長　：XTSを推奨候補暗号リストに追加すること自体についてはどうか。
宇根構成員：追加すること自体は賛成である。

上原構成員：地方自治体でハードディスクの消去が十分でなかったために情報漏えいした事件を受け、自治体の情報セキュリティガイドラインとして、デバイスの記録情報を消去してから廃棄するといった要件が議論されている。その際、暗号化されたデバイスの破棄であれば、鍵の消去がなされていればよいとしたとき、暗号化とは何かというものがここで関係してくるかと思う。つまり、XTSでブロック暗号化されたストレージは、適切な暗号化がされた状態と定義できる。
こうした話はホットトピックであり、CRYPTRECとして適切な暗号化方法を決めた後、更にこれを活用する意味で、暗号化データの消去とは何かを定義していくという次のフェーズがあると理解している。
松本座長　：民間団体でそのような定義をしているところもあると認識している。今後、必要に応じて検討項目としていきたい。

(5) 運用監視暗号リストからの削除ルール及びRC4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、原案のとおり決定された。特段の質疑はなかった。

(6) 暗号技術検討会 2019年度 報告書（案）について

資料７について事務局より説明が行われ、本日の議論を踏まえた修正版を議事概要と併せて確認することとした上で承認された。特段の質疑はなかった。

(7) 2020年度暗号技術評価委員会 活動計画について

資料８について事務局より説明が行われ、原案のとおり承認された。主な質疑内容は以下のとおり。

宇根構成員：２ページ目の暗号技術調査ワーキンググループの活動に関して、「Shorの量子アルゴリズムによる現代暗号への脅威に関する調査」とあるが、具体的にはどのようなものを想定されているか。
事務局(NICT)：素因数分解問題と離散対数問題に対する評価を行うことを想定している。

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。

また、事務局から、暗号技術活用委員会の2020年度の活動計画については別途メール審議を行う予定であること、及び次回の暗号技術検討会は翌年３月頃の開催を予定しており、詳細については別途連絡する旨の説明が行われた。

以上