2020年度 第２回 暗号技術検討会 議事概要

１．日時

令和３年３月30日（火）10:00～11:30

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）、上原哲太郎、宇根正志、太田和夫、高木剛、近澤武、本間尚文、
松井充、松浦幹太、松本泰、向山友也、渡邊創

オブザーバ：木村誠一郎（内閣官房：中野美夏代理）、今西玄（警察庁：吉田和彦代理）、
原嶋美緒（総務省行政管理局：千葉英之代理）、
細川敬太(総務省自治行政局:三橋一彦代理)、服部直樹(法務省:篠原辰夫代理)、
佐久間明彦（外務省：渡邊滋代理）、山上孝祐（財務省：大野由希代理）、
西城泰裕（文部科学省：坂本秀敬代理）、寺島誠司（厚生労働省：釜石英雄代理）、
大平浩之（経済産業省：柳澤智也代理）、大橋洋一（防衛省）、
柏原陽（個人情報保護委員会：赤阪晋介代理）、
久保田実（国立研究開発法人情報通信研究機構）、
花岡悟一郎（国立研究開発法人産業技術総合研究所）、
大澤昭彦（一般財団法人日本情報経済社会推進協会）、
戸田裕之（公益財団法人金融情報システムセンター）

事務局：(総務省(MIC)) 田原康生、藤野克、高村信、梅城崇師
(経済産業省(METI)) 江口純一、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) 2020年度暗号技術評価委員会 活動報告について
(3) 2020年度暗号技術活用委員会 活動報告について
(4) 暗号技術検討会 2020年度 報告書（案）について
(5) その他

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	CRYPTREC暗号リストの３リスト構成について
資料３	2020年度 暗号技術評価委員会 活動報告
資料３別添１	監視状況報告
資料３別添２	ディジタル署名EdDSAの安全性評価結果(外部評価)
資料３別添３	2020年度 暗号技術調査WG（暗号解析評価）活動報告

資料３別添４　仕様書の参照先の変更について
資料３別添５　ガイドラインに関する今後の方針について
資料４　2020年度 暗号技術活用委員会 活動報告
資料５　暗号技術検討会 2020年度 報告書（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、総務省の田原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。

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。

宇根構成員：暗号技術活用委員会で詳細が議論される予定となっている利用実績調査について、次は2022年との理解だが、その結果は公表されるのか。
事務局(IPA)：アンケート先は特定できないようにした集計値としてのデータは公開する。
宇根構成員：2022年の結果を公表し、推奨候補暗号リストに掲載している暗号のどれが使われていないが分かれば、５年後に同じ状況であればその暗号は削除されると分かる。どの暗号が使われていないか分かれば、削除を想定してシステム開発に利用でき、システム更改のタイミングで排除することもできるのではないかと思っている。
太田構成員：資料２－１の3.3の項目について、Shorのアルゴリズムではなく、Groverのアルゴリズムを使うと共通鍵暗号の鍵やハッシュ関数の衝突を見つけることができる。20年程前に研究したが、NMRのコンピュータで実現が早いのではないか、と言われた。現状、どうなっているのか知りたい。NICTなどで実験できる環境あるのであれば、取り組まれてはどうか。
高木構成員：GroverのアルゴリズムがAESにも影響を及ぼすことは、昨年度の暗号解析WGでも検討し報告している。実験結果はないという認識だがどうか。
事務局(NICT)：事務局としてもGroverのアルゴリズムを用いた実験は行っていないという認識。

(2)　2020年度暗号技術評価委員会 活動報告について

資料３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：耐量子計算機暗号のガイドラインはハイブリッドモードも含めるのか。
事務局(NICT)：ハイブリッドモードをガイドラインに含めるかどうかも含めて次年度に検討予定。

(3)　2020年度暗号技術活用委員会 活動報告について

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。

高木構成員：鍵長ガイドラインは2021年度に最初のものができるという理解で良いか。また、そこから５年ごとか。

事務局(IPA)：最初の公開はそのとおり。その後は、遅くとも、そのタイミングまでに内容を再確認する予定という意味。

高木構成員：NISTは2031年から128ビットセキュリティといっている。５年刻みの場合、NISTの周期と合うのか。

事務局(IPA)：何年刻みにするかわからないが、例えば、2030年まで、2031～2040年、2041～2050年というように年で区切るということが考えられる。この区切りについては検討中。なお、再確認というは、年刻みを見直すということではなく、該当年の内容を再確認するという意味。

高木構成員：ガイドラインの公表から何年という記載ではなく、何年から何年まで、という記載ぶりと理解した。ビットセキュリティの決め方は難しいと思うが、刻み幅はどうするのか。

事務局(IPA)：112・128・192・256ビットの４種類は決まっている。160や224を公開鍵暗号等の関係で入れる必要があるかどうかは暗号技術活用委員会で検討予定。

(4)　暗号技術検討会 2020年度 報告書（案）について

資料５について事務局より説明が行われ、本日の議論結果について追記することとした上で承認された。特段の質疑はなかった。

(5)　その他

その他全体を通じて以下の質疑が行われた。

松本(泰)構成員：CRYPTRECの活動は個々がとても深く、それぞれ意義があると認識している。しかし、活動の全体が見えにくい。CRYPTRECの活動のうち、暗号リストはわかりやすいが、それ以外の活動は一般に説明が難しい。活動のビッグピクチャーを示して活動意義を示すことや、活動の抜けがないか議論していくことも必要ではないか。世の中にとっての説明にもなる。暗号技術がなぜ社会にとって重要なのかの理解につながればよい。

松本(勉)座長：報告内容や審議事項も多岐に渡っている。全体の理解が進むよう来年度しっかり進めていきたい。

６．３．閉会

経済産業省の江口サイバーセキュリティ・情報化審議官から閉会の挨拶が行われた。

また、事務局から、次回の暗号技術検討会は別途連絡する旨の説明が行われた。