２０１３年度　第１回暗号技術検討会　議事概要

１．日時　平成２５年７月５日（金）　１４：００～１５：３５

２．場所　経済産業省本館４階　商情局第１会議室

３．出席者（敬称略）

構成員：今井 秀樹（座長）、岡本 栄司、岡本 龍明、金子 敏信、国分 明男、武市 博明、近澤 武、中山 靖司、松井 充、松尾 真一郎、松本 勉、松本 泰、向山 友也、渡辺　創

オブザーバ：伊藤 毅志、奥山 剛、亀田 繁、木村 和仙、平 和昌、寶木 和夫、西村 敏信

暗号技術評価委員会事務局：盛合 志帆（独立行政法人情報通信研究機構（ＮＩＣＴ））

暗号技術活用委員会事務局：神田 雅透（独立行政法人情報処理推進機構（ＩＰＡ））

暗号技術検討会事務局：

総務省　吉田 靖、山碕 良志、村上 聡、飯田 恭弘、吉田 丈夫、橋本 直樹

経済産業省　富田 健介、上村 昌博、中谷 順一、室井 佳子

４．配布資料

（資料番号）	（資　料　名）
資料１－１	2013 年度　暗号技術検討会開催要綱（案）
資料１－２	暗号技術検討会の公開について（案）
資料２	2012 年度　暗号技術検討会報告書（案）
資料３	暗号技術評価委員会　活動計画（案）
資料４	暗号技術活用委員会　活動計画（案）
資料５	CRYPTREC の暗号アルゴリズム仕様書について
参考資料１	2012 年度　第３回　暗号技術検討会議事概要
参考資料２	今後の検討課題に関する方針
参考資料３	2013 年度　暗号技術検討会及び関連委員会の体制
参考資料４	2013 年度　暗号技術検討会　構成員・オブザーバ名簿

５．議事概要

１　開会

暗号技術検討会事務局から開会の宣言があり、総務省の吉田政策統括官から開会の挨拶。

参考資料４に基づき、構成員及びオブザーバの交代等の説明（辻井 重男顧問が昨年度をもって勇退、上原 哲太郎構成員が新任、持麾構成員→向山構成員、（内閣官房情報セキュリティセンター）三角氏→奥山氏、（総務省）栗原氏→稲垣氏、濱島氏→増田氏、宮地氏→篠原氏、（財務省）石田氏→郷氏、（法務省）河合氏→佐藤氏、（厚生労働省）代田氏→三富氏、（経済産業省）鈴木氏→辻本氏、（独立行政法人情報処理推進機構）笹岡氏→伊藤氏、（公益財産法人金融情報システムセンター）鈴田氏→西村氏）。上原 哲太郎構成員、太田 和夫構成員、佐々木 良一構成員、本間 尚文構成員は欠席。

２　議事

（１）2013 年度 暗号技術検討会開催要綱等について【承認事項】

資料１及び資料１－２に基づき、2013 年度暗号技術検討会開催要綱及び暗号技術検討会の公開について暗号技術検討会事務局から説明。質疑は以下のとおり。原案どおり承認。座長として今井構成員を選任。

○質疑応答

松本（勉）構成員：資料が速やかに公開されることはよいことである。暗号技術評価委員会、暗号技術活用委員会の各委員会の資料等の公開については、各委員会で定めるのか。

暗号技術検討会事務局：各委員会の初回の会合で決定する。

（２）　2012 年度 暗号技術検討会報告書（案）について【承認事項】

資料２に基づき、2012 年度 暗号技術検討会報告書（案）について暗号技術検討会事務局から説明。質疑等なし。原案どおり承認。

（３）　暗号技術評価委員会 活動計画（案）について【承認事項】

資料３に基づき、暗号技術評価委員会 活動計画（案）について暗号技術評価委員会事務局から説明。質疑は以下のとおり。原案どおり承認。

〇質疑応答

今井座長：注意喚起レポートは委員会で審議せずに発出することもあり得るのか。

暗号技術評価委員会事務局：緊急性を要する場合や次の委員会まで時間が空く場合は電子メールによる審議を経て実施する。

松本（勉）構成員：「リストガイド」から「ガイドライン」となった理由は何か。今後はガイドラインに統一するのか。

暗号技術評価委員会事務局：名称には特段の意図はない。今後はガイドラインに統一する。

松本（勉）構成員：「ガイドライン」だと従うべきという義務的なニュアンスがあるように思うが、本質的には問題ない。

寳木オブザーバ：軽量暗号に関して ISO/IEC の動きが進んでいる。ISO/IEC の活動と関連づけるのか。

暗号技術評価委員会事務局：標準化が進んでいた軽量暗号の ISO/IEC の規格は既に出版されており、新しく軽量ハッシュ関数についてのパートが 10 月から ISO/IEC で標準化が始まることになった。次の ISO/IEC の改定の際に提案できればと考えている。

松本（勉）構成員：更に軽量なものも議論の対象とするのか。

暗号技術評価委員会事務局：そういったものも検討に含めたいと考えているが、WG 委員の意見を聞きながら定義について決定したいと考えている。

（４） 暗号技術活用委員会 活動計画（案）について【承認事項】

資料４に基づき、暗号技術活用委員会 活動計画（案）について暗号技術活用委員会事務局から説明。質疑は以下のとおり。

〇活動計画全般について

暗号技術検討会事務局：小改定のスパンを３年としたので、２年間で調査・検討する方針とした。ただし、２年間も要するのでは遅すぎるという意見もあり得るのではないかとも考えるがどうか。

松本（勉）構成員：スピード感が大事であることは同感であるが、課題抽出から対応まで２年ほどを要する課題もあるのではないか。

暗号技術検討会事務局：じっくり検討する必要があるものと、そうではないものがあると思うので、切り分けないとスピード感がなくなるのではないかということを気にしている。

松本（勉）構成員：その通りであり、その点は留意しておく必要がある。

〇運用ガイドラインについて

岡本（栄）構成員：今までに CRYPTREC で行ってきた内容とは大分異なるように感じる。電子政府推奨暗号リストに入っていても推奨されないものが出るのか。

暗号技術活用委員会事務局：例えば SSL のサイファースイートに含まれており、CRYPTREC 暗号リストに掲載されていてもほとんど製品に実装されていない場合は外れる可能性がある。また、暗号を実装するために複雑なコマンドラインを使用しないと実装できないものを外す、あるコマンドラインで実装しようとすると推奨できない組合せが入ってしまったとしても、対処できる場合は運用上の観点から使用する、といったことはありうる。

岡本（栄）構成員：推奨候補暗号リストや運用監視暗号リストから入ることもあるのか。

暗号技術活用委員会事務局：（使用の要件を付した上で）ありうる。

今井座長：こういったものが出てきた理由は IPA のマニュアルが非常に大きなインパクトを与えたことである。CRYPTREC 暗号リストに掲載しただけではなかなか利用されないという現状がある。ある程度現実に妥協する形となるが、安全性はきちんと確保していくものである。

岡本（栄）構成員：CRYPTREC の活動と分けないと整合性がとれないのではないか。

松本（勉）構成員：一方で、運用ガイドラインが CRYPTREC の活動とリンクしていないと、利用者から見るとばらばらに見えてしまい困るのではないか。したがって CRYPTREC の枠内で行い、しっかりと内容を見ていく方がよいのではないか。

今井座長：電子政府推奨暗号リストの活用を推進するという意味では、こういった方法もあり得るのではないか。まず CRYPTREC の傘の下で実施してみて、その中身を検討会でも確認する方法が良いと思う。その上で議論すれば良いのではないか。ところで、この運用ガイドラインの作成作業での成果について、電子政府推奨暗号リストへのフィードバックは行うのか。

暗号技術活用委員会事務局：対象を SSL/TLS 等に限定することを考えていたため、フィードバックはまでは想定していない。

金子構成員：「運用ガイドライン」という名称が良くない。「SSL/TLS 運用ガイドライン」と限定したらどうか。また、技術ガイドラインと運用

ガイドラインの違いも分かりにくい。さらにベースラインとレッドラインという２つの概念が登場しており、説明を難しくしている。

暗号技術活用委員会事務局：ベースラインとレッドラインは同じ意味で使用している。

暗号技術検討会事務局：事務局内でもガイドラインの違いについて議論があった。今後の進め方としては、両委員会で作成したガイドラインは、相互に関連することから、事前に両委員会で案を作った段階でそれぞれの認識と合致することを確かめながら進め、今井座長のご発言のとおり出来上がったものを CRYPTREC のクレジットで出すべきかどうかについて、この検討会で確認していただく必要があると考えている。

岡本（栄）構成員：SSL/TLS といった限定があるならば、向いていないものがあることも分かるが、やはりリスト上で推奨暗号ではない暗号を、運用ガイドライン上では推奨する可能性があるということに違和感がある。

岡本（龍）構成員：このガイドラインは電子政府を対象としていると考えて良いか。つまり、民生品は対象外と考えて良いか。

暗号技術検討会事務局：そのとおりである。ただ、民間においても参照されればなお良いと考えている。

今井座長：様々な意見があると思うので、この場で言い切れなかった意見は事務局あてメール頂きたい。最終的な判断は座長に一任して頂きたいが、ガイドラインについては、この検討会でチェックする機会は必ず設けるようにする。

（５） CRYPTREC の暗号アルゴリズム仕様書について【承認事項】

資料５に基づき、CRYPTREC の暗号アルゴリズム仕様書の更新について暗号技術評価委員会事務局から説明。以下の質疑を踏まえて軽微な修正を行うこととなるが、ほぼ原案どおり承認。

〇質疑応答

金子構成員：KCipher-2 に日付がついていないのはなぜか。

暗号技術評価委員会事務局：公募提案時に入手した仕様書にリンクさせているため、そのままの名称となっている。

金子構成員：日付は必要ではないのか。

暗号技術評価委員会事務局：入れるようにしたい。

松本（勉）構成員：仕様書がいつの時点のものなのかが分かることが重要であるため、その他の仕様書についても日付を入れるようにすべきではないか。

暗号技術評価委員会事務局：整理して一意に特定できるようにしたい。

松本（勉）構成員：また、リストの改正を踏まえ、JCMVP の方で CRYPTREC の仕様書を改めて引用したいと思ったが、更新されておらず困っているとも聞いている。この仕様書の更新について、対処する必要があるだろう。

暗号技術評価委員会事務局：できれば正式に JCMVP の方から要望の文書が欲しい。

松本（勉）構成員：了解した。仕様書の更新についてのルールを作成することも近々の課題となるだろう。

金子構成員：資料４の４ページ中に、「トレードマーク」とカタカナで書かれている部分があるが、これは正しいのか。

暗号技術評価委員会事務局：RSA 社からの提出された文章のまま引用しているが、確認する。

３　閉会

経済産業省の富田商務情報政策局局長から閉会の挨拶。

暗号技術検討会事務局から、次回暗号技術検討会の時期、場所等の詳細については、別途連絡する旨が説明された。

以上