２０１２年度　第２回暗号技術検討会　議事概要

１．日時　平成２４年１２月１１日（火）　１４：００～１５：４５

２．場所　経済産業省本館２階　２東３共用会議室

３．出席者（敬称略）

構成員：今井 秀樹（座長）、辻井 重男（顧問）、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、本間　尚文、松井 充、松尾 真一郎、松本 勉、松本 泰、持麾 裕之、渡辺　創

オブザーバ：三角 育生、羽室 英太郎、村田 莉衣奈（栗原 利男代理）、中山 紀雄（濱島 秀夫代理）、金城 裕隆（宮地 毅代理）、佐藤 真紀子（河合 芳光代理）、楢木野 由善（中村 耕一郎代理）、冨士池 俊英（石田 清代理）、中島 誠（田中 正幸代理）、浜田 和之（代田 雅彦代理）、岩永 敏明（鈴木 晴光代理）、木村 和仙、平 和昌、寶木 和夫、笹岡 賢二郎、亀田 繁、鈴田 信

暗号方式委員会事務局：盛合 志帆（独立行政法人情報通信研究機構（ＮＩＣＴ））

暗号実装委員会事務局：大熊 建司（独立行政法人情報処理推進機構（ＩＰＡ））

暗号運用委員会事務局：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　阪本 泰男、山碕 良志、村上 聡、上原 哲太郎、飯田 恭弘、吉田 丈夫、橋本 直樹

経済産業省　永塚 誠一、上村 昌博、守谷 学、中谷 順一、守山 速飛

４．配布資料

（資料番号）	（資　料　名）
資料１	2012 年度 第１回 暗号技術検討会議事概要（案）
資料２	2012 年度 暗号方式委員会、暗号実装委員会及び暗号運用委員会 第１回 合同委員会の概要
資料３	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）（案）
資料４―１	電子政府推奨暗号リスト（CRYPTREC 暗号リスト）策定の流れの確認
資料４－２－１	【安全性評価・実装評価】判定結果
資料４－２―２	【安全性評価・実装評価】における安全性評価（暗号方式委員会）
資料４－２―３	【安全性評価・実装評価】における実装性能評価（暗号実装委員会）
資料４－３	【条件適合性評価】評価Ａ判定結果
資料４－４	【条件適合性評価】評価Ｂ判定結果
資料４－５	総合評価の判定（案）
資料５	パブリックコメントの実施方法について
資料６	今後の検討課題の整理について
参考資料１	選定基準一覧表（総合評価）
参考資料２	次期電子政府推奨暗号リスト策定スキーム
参考資料３	電子政府推奨暗号リスト（現行リスト）
参考資料４	2012 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

事務局から開会の宣言があり、総務省の阪本政策統括官から開会の挨拶。

参考資料４に基づき、オブザーバの交代の説明（(総務省自治行政局住民制度課）高原氏→宮地氏、（防衛省）坂下氏→木村氏、（独立行政法人情報通信研究機構）高橋氏→平氏)。太田構成員及び佐々木構成員は欠席。

２　議事

（１）第１回暗号技術検討会議事概要（案）の確認

資料１に基づき、検討会事務局から説明。質疑等なし。原案どおり承認。

なお、今後は迅速な議事概要の確定に向けて、メール審議の承認をもって議事概要の確認とすることを暗号技術検討会事務局が提案し承認された。

（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）（案）（以下、「リスト案」）について【承認事項】

資料２に基づき、第１回合同委員会の概要について、資料４－１に基づき、電子政府推奨暗号リスト（CRYPTREC暗号リスト）策定の流れについて、暗号技術検討会事務局から説明。

資料４－２－１から資料４－２－３に基づき、安全性評価及び実装評価の判定結果について、暗号方式委員会及び暗号実装委員会から、資料４－３及び資料４－４に基づき、条件適合性評価（評価Ａ、評価Ｂ）の判定結果について、暗号運用委員会から説明。

資料４－５に基づき、総合評価の判定（案）について、暗号技術検討会事務局から説明。質疑等なく原案どおり承認され、総合評価による更なる絞り込みは不要と決定。

資料３に基づき、リスト案の体裁等について、暗号技術検討会事務局から説明。質疑等なく、リスト案は体裁等を含めて、原案どおり承認された。

○リスト案の体裁等に係る発言

暗号技術検討会事務局：この体裁にはいくつか込めた思いがある。大きな更新として表題を変えたこと、また、リストを３つに分けたこと。「電子政府推奨暗号リスト」はその説明の末尾に書かれているとおり、利用を推奨するものである。「推奨候補暗号リスト」は利用も認められるという記述で電子政府推奨暗号リストと差別化した。また、「運用監視暗号リスト」は直ちに危険ではないが監視が必要なものである。今後、本リストが使われていくことが必要であり、NISCの政府機関統一管理基準にどう落とし込んでいくのか関係者と調整していく必要がある。

今井座長：NISC の政府機関統一管理基準には、電子政府推奨暗号リストが参照されることとなるのではないか。

資料５に基づき、パブリックコメントの実施方法について、パブリックコメント開始希望日を含めて、暗号技術検討会事務局から説明。質疑等なく、原案どおり承認。

〇パブリックコメントの実施方法に係る発言

暗号運用委員会事務局：パブリックコメントの実施に合わせて、利用実績調査の報告書を IPA ウェブサイトに掲載する予定である。

（３） 今後の課題について【討議事項】

資料６に基づき、今後の検討課題の整理について、暗号技術検討会事務局から説明。

〇今後の検討課題についての討議

辻井顧問：今までの精密な議論に感謝。暗号化された個人情報はもちろん個人情報には違いないが、どこまでを個人情報と言うのかは議論していくべき。クラウドコンピューティングにおける秘密分散について議論があり、秘密分散された情報は個人情報かどうかの議論も出てくるだろう。つまり、０＋０＝１になりうるため、この議論が必要。個人情報保護法では、秘密分散された１つ１つも個人情報である、という整理だが、それで良いのかという議論もある。また、阪本政策統括官も冒頭の挨拶において指摘されたとおり、プライバシーと個人情報活用との両立の話も重要である。

今井座長：単体の情報では個人を特定できなくても、例えばインターネット検索で調べるとそれらの情報がつながることもあるだろう。確かにどこまでを個人情報とするかは難しい。技術で何とかなる部分は CRYPTREC としても考えていく必要がある。

寶木オブザーバ：NIST で公募されている SHA-3 について CRYPTREC としてどうするのか。

今井座長：事務局としてはどう考えているのか。

暗号技術検討会事務局：CRYPTREC で評価し、政府でどう共有するかを考えなくてはいけない。事務局としても米国政府の動きも見ているし、これから具体的な対応を考えていく必要がある。

今井座長：小改訂をフレキシブルに行ってほしい。

近澤構成員：IPA と NIST の定期会合で得た情報によると、SHA-3 のドラフトは来年９月頃に出るようである。

松本（泰）構成員：暗号化された個人情報は、暗号化鍵で復号できるので個人情報であることには変わりないとして、では「暗号化鍵」の破棄は、個人情報の破棄になるのかということを明確にする必要があるのではないか。米国

においては、NIST が発行しているデータ破棄のガイドライン案において、こうした暗号化鍵の破棄によるデータ破棄が示されている。暗号化鍵の破棄を証明するには鍵管理を明確にする必要があるが、こうした対応のやり方を示す必要があるのはないか。

暗号技術検討会事務局：制度の人は技術が不得手で、技術の人は制度が不得手ということが多い。その間を埋めることが重要である。従来、個人情報か否かという０か１かの議論が主流を占めてきたが、そうでない形にどうもっていくかということで、本検討会のような技術的な場で、何が可能で何が不可能か、個人情報についての０か１かでない確率的な考え方などについての議論もしていかないといけないだろうと考えている。

今井座長：正にそのとおりである。事務局としても、多くの構成員と協力して、今後の検討課題について整理して欲しい。なお、「耐量子暗号」という訳語は再考してほしい。

（４） その他

暗号方式委員会事務局から、CRYPTREC シンポジウム 2013 の開催について、2013 年 3 月 26 日（火）にコクヨホールで午前 10 時から開催予定であることが周知された。

（５） 閉会

経済産業省の永塚商務情報政策局長から閉会の挨拶。

暗号技術検討会事務局から、第３回暗号技術検討会は 2013 年 2 月 22 日（金）15:00～17:00 に開催予定であることを周知。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