２０１４年度　第２回暗号技術検討会　議事概要

１．日時　平成２７年３月２７日（金）　１０：００～１１：５０

２．場所　経済産業省別館１階　１０４各省庁共用会議室

３．出席者（敬称略）

構成員：今井秀樹（座長）、今井正道、上原哲太郎、太田和夫、岡本栄司、岡本龍明、金子敏信、国分明男、佐々木良一、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、向山友也

オブザーバ：奥山剛、中村武英（村田利見 代理）、江森久子（野口宣大 代理）、佐久間明彦（大村周一郎 代理）、岩下守男（鯨井佳則 代理）、岩永敏明（和泉章 代理）、平和昌、寶木和夫、伊藤毅志、竹内英二、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　南俊行、赤阪晋介、筒井邦弘、中村一成

経済産業省　大橋秀行、上村昌博、中野辰実、室井佳子

４．配布資料

（資料番号）

資料１	2014 年度 暗号技術評価委員会活動報告
資料１別添１	2014 年度 暗号技術調査 WG（暗号解析評価）活動報告
資料１別添２	離散対数問題の困難性に関する調査
資料１別添３	格子問題等の困難性に関する調査
資料１別添４	2014 年度 暗号技術調査 WG（軽量暗号）活動報告
資料１別添５	暗号技術調査 WG（軽量暗号）報告書（案）
資料２	2014 年度 暗号技術活用委員会活動報告
資料２別添１	暗号普及促進・セキュリティ産業の競争力強化に向けた課題分析と見解
資料２別添２	SSL/TLS 暗号設定ガイドライン
資料２別添３	SSL/TLS 暗号設定ガイドラインチェックリスト
資料２別添４－１	暗号技術参照関係の俯瞰図（全体像）
資料２別添４－２	暗号技術参照関係の俯瞰図
資料２別添５	標準化提案におけるノウハウ・課題・基本的な情報の整理
資料３	CRYPTREC 暗号リストの注釈の一部変更について
資料３別添	CRYPTREC 暗号リストの変更案
資料４	2014 年度 暗号技術検討会報告書（案）

資料５	暗号技術検討会における小グループの設置について（案）
資料６	2015 年度 暗号技術評価委員会活動計画（案）
資料７	2015 年度 暗号技術活用委員会の活動について（案）
参考資料１	2014 年度　第１回暗号技術検討会議事概要
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
参考資料３	2014 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、経済産業省の大橋審議官から開会の挨拶が行われた。

参考資料３に基づき、暗号技術検討会事務局よりオブザーバの交代（(警察庁）佐藤氏→村田氏、(一般社団法人日本情報経済社会推進協会）亀田氏→竹内氏及び構成員の欠席（渡辺構成員）について説明が行われた。

２　議事

（１）2014 年度　暗号技術評価委員会活動報告について

資料１から資料１別添５に基づき、暗号技術評価委委員会事務局より説明が行われた。質疑応答は以下のとおり。原案どおり承認された

〇質疑応答

今井座長：軽量暗号に関してこれほど多くの内容を取りまとめた報告書は世界で初めてではないか。今後、IoT のあらゆる面で軽量暗号が重要になってくると思うが、どのような場面で軽量暗号が使用できるかしっかり示すことは意義深い。この報告書は既に公開されているのか。

暗号技術評価委員会事務局:まだ公開されていない。今回の暗号技術検討会の審議の後、4 月以降に誤植等の修正を行った上で、CRYPTREC の HP で公開する。

（２）2014 年度　暗号技術活用委員会活動報告について

資料２から資料２別添５に基づき、暗号技術活用委員会事務局より説明が行われた。質疑応答は以下のとおり。原案どおり承認された。

〇質疑応答

松尾構成員：標準化 WG の報告において、公開できない情報があるとのことだが、実際はそのような公開できない情報こそが重要だったりする。今後標準化活動を行う人に、これらの情報を提供する方法は考えているのか。

暗号技術活用委員会事務局：標準化団体の国内委員会等のコンタクト先を掲載することで、対応したい。

佐々木構成員：暗号ライブラリ市場が縮小しているというのは、おっしゃるとおりだと思う。しかし、軽量暗号は半導体への利用が想定されているなど、ライブラリ製品以外への広がりが期待できるのではないか。この動きは産業化に結びつくのか、あるいは、結びつけるにはどうしていったらよいと考えているか。軽量暗号については、どのくらい暗号強度があればリスクを許容可能なのかを示していかないと、利用が進ま

ないのではないかと危惧している。

暗号技術活用委員会事務局：軽量暗号の安全性評価については、暗号技術評価委員会が担当しているが、暗号技術活用委員会として議論のポイントとなったのは、資料２別添１の 16 頁にも記載している点である。日本は各社が全て独自技術で競争しようとするが、米国はある程度のレイヤーで区切りをつけ、共通化すべき部分は共通化している。日本で製品化が進むかどうかは、共通化すべき部分を共通化していくようまとめることができるかどうかにかかっている。

佐々木構成員：民間企業が自らまとまるという方法もあると思うが、CRYPTREC でも検討を行っているため、連携していく道もあるのではないか。

暗号技術活用委員会事務局：暗号技術はロイヤリティフリーが多いため、企業にとって国産暗号を推進するメリットは少ない。しかし、国によっては国産暗号の普及を国が主導して成功している例もある。そこで仮説として、国産暗号の普及が、国にとっても企業にとってもメリットがあり、Win-Win の関係を構築していることが成功の秘訣ではないかと考えている。その仮説に至る具体的な考え方は、資料２別添１の 13～14 頁に記載しているとおり。

暗号技術評価委員会事務局：軽量暗号の安全性に不安を感じている人はいると思う。来年度に作成するガイドラインにおいて、同じ鍵でどれくらいの暗号ならリスクを許容できるのかということを示していきたいと考えている。また、来年度の暗号技術評価委員会では、軽量暗号の普及について、標準化の観点も含めて検討する。

佐々木構成員：国産暗号の普及促進のみを強く言いすぎることも良くないと思うが、せっかく良い暗号アルゴリズムがあるのだから普及させていきたい。現在、一番芽が出そうだと考えているのが軽量暗号である。

（３）CRYPTREC 暗号リストの注釈の一部変更について

資料３及び資料３別添に基づき、暗号技術検討会事務局より説明が行われた。質疑はなし。原案どおり承認された。

（４）2014 年度　暗号技術検討会報告書（案）について

資料４に基づき、暗号技術検討会事務局より説明が行われた。質疑はなし。本日の議事内容を反映させた上で、本日の議事概要とともにメールで最終的な確認を行うこととして承認された。

（５）暗号技術検討会における小グループの設置について

資料５に基づき、暗号技術検討会事務局より説明が行われた。質疑応答は以下のとおり。原案どおり承認された。

〇質疑応答

松尾構成員：資料４の暗号技術検討会の報告書（案）にもあるとおり、重要なのは日本の安全な ICT 基盤の確立であると思う。そこで、安全な ICT 基盤とは何なのか、その中で CRYPTREC が発揮できる強みとは何か、JCMVP 等の制度との連携も含めて検討すべき。

佐々木構成員：産業育成についてもう少し検討していただきたい。国として国産の暗号アルゴリズムを１つは持っていないといけないという事が正しいのかどうかということを含めて小グループで議論していただきたい。

松本（勉）構成員：これまで策定してきた CRYPTREC 暗号リストは、暗号アルゴリズムが中心であるが、もっと暗号プロトコルとその実装まで、CRYPTREC がカバーしていく必要があるのではないか。

今井座長：暗号プロトコルについては、CELLOS とも上手く連携していく必要がある。先日、メディカル ICT で医薬品や医療機器を自国で評価・認証することが重要という話があった。暗号分野においては、まさに CRYPTREC がそういった活動を担っている。人材育成についても、人を増やすことが重要。人が増えれば、評価・認証にかかる時間も短縮される。即応性の観点も重要である。

（６）2015 年度　暗号技術評価委員会活動計画（案）について

資料６に基づき、暗号技術評価委員会事務局より説明が行われた。質疑はなし。原案どおり承認された。

（７）2015 年度　暗号技術活用委員会の活動について

資料７に基づき、暗号技術活用委員会事務局より説明が行われた。質疑応答は以下のとおり。原案どおり承認された。

〇質疑応答

松本（泰）構成員：暗号技術評価委員会の 2015 年度の計画にある新技術に関する調査について、どういった暗号技術が今後求められるようになるかという観点からの調査も必要ではないか。例えば、マイナンバーであれば、プライバシー保護技術に関連した暗号技術が有用になると考えられるし、IoT における暗号技術の利用というのも今後進展が期待できる分野と考えられる。そういった暗号研究者にモチベーションを与えるような調査も実施していただきたい。

上原構成員：運用ガイドラインの検討準備についてだが、SSH に関しては、つい最近 CSIRT 協議会がガイドラインを策定している。既に策定されているものに対して、政府が別

の動きをすると現場が混乱する可能性があるので、ガイドラインのテーマは既存のものとなるべく重複しないよう検討していただきたい。

暗号技術活用委員会事務局:既存のテーマと重複しないように、事前準備で確認を行う。

３　閉会

総務省の南政策統括官から閉会の挨拶が行われた。

暗号技術検討会事務局から、2015 年度第 1 回暗号技術検討会は夏頃の開催を予定しており、詳細な日程、場所等については、別途連絡する旨の説明が行われた。

今年度限りでの CRYPTREC からの退任にあたり、今井座長から挨拶が行われた。

以上