２０１５年度　第１回暗号技術検討会　議事概要

１．日時　平成 27 年 10 月５日（月）　10:00～12:00

２．場所　経済産業省本館 17 階　第１特別会議室

３．出席者（敬称略）

構成員：松本勉（座長）、今井正道、宇根正志、太田和夫、岡本栄司、金子敏信、佐々木良一、近澤武、手塚悟、松井充、松浦幹太、松本泰、向山友也、渡邊創

オブザーバ：太田裕介（坂本三郎　代理）、平和昌、寳木和夫、竹内英二、中村武英（村田利見　代理）、西島学（溝口浩和　代理）、西村敏信、橋本壮司（中山隆介　代理）、橋本敬史、頓宮裕貴、松永一義、松本静香（篠原俊博　代理）、吉岡達宏（木村和仙　代理）

暗号技術評価委員会事務局：盛合志帆（国立研究開発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、大森一顕、筒井邦弘、丸橋弘人、今野孝紀

経済産業省　前田泰宏、瓜生和久、上坪健治、中野辰実、中村博美

４．配付資料

（資料番号）	（資料名）
資料１－１	「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	「CRYPTREC の在り方に関する検討グループ」における議論結果報告書
資料３	暗号技術検討会における「重点課題検討タスクフォース」の設置について（案）
資料４	2015 年度　暗号技術検討会活動計画
資料５	2015 年度暗号技術評価委員会の活動について（案）
資料５別添	64 ビットブロック暗号 MISTY1 の安全性について
資料６	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２回暗号技術検討会議事概要
参考資料２	2015 年度　暗号技術評価委員会活動計画
参考資料３	2015 年度　暗号技術活用委員会活動について（案）
参考資料４	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、総務省の南政策統括官から開会の挨拶が行われた。参考資料４に基づき、暗号技術検討会事務局より構成員及びオブザーバの交代（(東京大学）今井先生、(一般財団法人ニューメディア開発協会）国分様、(独立行政法人情報通信研究機構）松尾様、(日本銀行）中山様→（日本銀行）宇根様、(東京工科大学）手塚先生、(東京大学）松浦先生)、オブザーバの交代（(法務省）野口様→坂本様、(外務省）大村様→松永様、(財務省）武田様→中山様、(厚生労働省）鯨井様→橋本様、(経済産業省）和泉様→橋本様、(独立行政法人情報処理推進機構）伊藤様→頓宮様、（総務省）増田様の辞退）及び構成員の欠席（上原構成員、本間構成員、岡本龍明構成員）について説明が行われ、新たに構成員に加わった方々から挨拶があった。

２　議事

（１）2015 年度暗号技術検討会　開催要綱案等について

資料１－１及び１－２に基づき、「暗号技術検討会開催要綱（案)」及び「暗号技術検討会の公開」について事務局より説明が行われた。質疑はなし。原案のとおり承認された。構成員の互選により、座長として松本勉構成員を選任した。

（２）「CRYPTREC の在り方に関する検討グループ」における議論結果について

資料２に基づき、事務局より説明が行われた。

○質疑応答

佐々木構成員：今後の IoT 社会では完全に安全であると言い切ることは出来ない。現実的にはレベル別のセキュリティの在り方の議論が必要であり、リスク評価の観点が必要である。

松本座長：確かに、例えば消費電力がかかるからといってセキュリティを低くして良いのか、ということになる。うまくバランスを取ることが大事。

宇根構成員：システムのセキュリティ要件のまとめ方は非常に難しいため、CRYPTREC 成果物が仕様書へ反映することを意識したものになることは良い。ユーザはどういう情報が必要なのかというところをヒアリングなどにより把握することが大切。また、鍵管理においても、例えば証明書が失効した際の入替え方法など、システムのライフサイクルを予め仕様書の段階から考慮しておかないと、コスト面で問題となる。

（３）「重点課題検討タスクフォース」の設置について

資料３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。原案どおりに承認された。

○質疑応答

佐々木構成員：既存のプロトコルの普及戦略についても検討内容として入れてほしい。例えば最近巷で話題のなりすまし対策における S/MIME 普及の検討や DNSSEC 等である。S/MIME は最初の認証に課題があるなど、一般への普及には困難があるが、マイナンバー制度の始まりをトリガーとして個人認証をしっかりしてほしい。

松本座長：重点課題検討タスクフォース又は、暗号技術活用委員会など、どの検討会で受け取るべきかを含めて検討したい。

宇根構成員：重点課題検討タスクフォースで決定した方向性はその後どうなるのか。

暗号技術検討会事務局：各委員会の活動計画へ反映し、次回検討会で報告する予定。

（４）2015 年度　暗号技術検討会活動計画について

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。原案のとおり承認された。

（５）2015 年度暗号技術評価委員会活動計画（案）について

資料５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。質疑応答は以下のとおり。原案のとおり承認された。

○質疑応答

金子構成員：計算量がこれぐらいだから問題が無い、というのは研究者には理解できるが、一般人もそうであるかと言われれば違う。暗号技術調査 WG（暗号解析評価）で作成している「処理能力の予測図」を参照することにより、ある時点で、1024 ビットなら NG だが、2048 ビットなら大丈夫、といった判断ができるように、MISTY1 などの共通鍵暗号系の解析にかかる計算量についても、例えば 2 の 108 乗の場合から 2 の 100 乗となった場合、計算機の処理能力が現状これぐらいだから大丈夫だ、あるいは危ない、というラインが一般人にもわかるような予測図などの表現を考えてほしい。

暗号技術評価委員会事務局：こういった表現を明快にすることは軽量暗号の受け入れにもつながる。評価委員会として検討したい。

（６）2015 年度暗号技術活用委員会活動計画（案）について

資料６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。原案のとおり承認された。

○質疑応答

宇根構成員：SSL/TLS ガイドラインについて、非常に参考になった。感謝している。引き続きやっていただきたい。アルゴリズムの実績調査について、重点課題検討タスクフォースの検討結果を踏まえて行うとのことであるが、クラウド等において処理されるデータの機密性やプライバシーを確保する技術として高機能暗号が今後活用される場面が増えると思うが、これは活用委員会のスコープに含まれるのか。

暗号技術活用委員会事務局：実績調査はあくまでも CRYPTREC 暗号リストの改定の際に行われるものであり、高機能暗号は実績調査の対象には含まれない。しかし御指摘の点は、重点課題検討タスクフォースで行う予定の新しいニーズ調査での重要なテーマになりうると認識している。

3　閉会

経済産業省の前田審議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２回暗号技術検討会は３月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。

以上