# ２０１４年度　第１回暗号技術検討会　議事概要

１．日時　平成２６年１０月９日（木）　１４：００～１５：０５

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、国分明男、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、渡辺創

オブザーバ：奥山剛、根本農史（佐藤正明 代理）、村田莉衣奈（稲垣浩 代理）、江森久子（野口宣大 代理）、大村周一郎、村田秀樹（武田一彦 代理）、田中正幸、濱田和之（鯨井佳則 代理）、岩永敏明（和泉章 代理）、木村和仙、平和昌、寶木和夫、伊藤毅志、亀田繁、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

経済産業省　大橋秀行、上村昌博、中野辰実

４．配布資料

（資料番号）

| | |
|---|---|
| 資料１－１ | 2014 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 | 2014 年度 暗号技術検討会活動計画 |
| 資料３ | 2014 年度 暗号技術評価委員会活動中間報告 |
| 資料３別添 | 監視状況報告 |
| 資料４ | 暗号技術活用委員会の活動状況 |
| | |
| 参考資料１ | 2013 年度 第 2 回暗号技術検討会議事概要 |
| 参考資料２ | 2014 年度 暗号技術評価委員会活動計画 |
| 参考資料３ | 2014 年度 暗号技術活用委員会活動計画 |
| 参考資料４ | 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５ | 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、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５に基づき、暗号技術検討会事務局より構成員の交代（(一般社団法人情報通信ネットワーク産業協会）武市構成員→今井構成員)、オブザーバの交代（(財務省）郷氏→武田氏、(厚生労働省）三富氏→鯨井氏、(経済産業省）辻本氏→和泉氏）及び構成員の欠席（佐々木構成員）について説明が行われた。

２　議事

（１）2014 年度　暗号技術検討会　開催要綱等について

資料１－１及び１－２に基づき、「2014 年度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、座長として今井秀樹構成員を選任した。今井座長より、座長代理として松本勉構成員が指名された。

（２）2014 年度　暗号技術検討会活動計画

資料２に基づき、事務局より説明が行われた。質疑はなし。前回検討会において承認された本活動計画について、改めて確認した。

（３）暗号技術評価委員会の活動に関する中間報告

資料３及び資料３別添に基づき、暗号技術評価委員会事務局より説明が行われた。

〇質疑応答

今井座長：RC4 の注釈変更は、なるべく RC4 を使ってもらいたくないというメッセージを意図しているという理解でよいか。

暗号技術評価委員会事務局：そのとおり。

上原構成員：「（１）④ 推奨候補暗号リストへの新規暗号（事務局選出）の追加」に関連して、現在 RC4 が使用できなくなったことによってストリーム暗号の有力な選択肢が存在していないところ、国産暗号アルゴリズムの国際標準化の推進に係る取組も実施するのか。

暗号技術評価委員会事務局：事務局としての取組に加え、暗号技術活用委員会のもとに標準化推進ワーキンググループが設置されており、これらの活動とも連携し推進していく。

寶木オブザーバ：軽量暗号に関する技術公募は実施しないということだが、ISO で標準化が進んでいることと関係があるのか。

暗号技術評価委員会事務局：当面の目標として CRYPTREC が技術公募まで行う段階にないと判断したもの。ISO で標準化が進んでいることと直接の関係はない。

松尾構成員：軽量暗号については、既に ISO で標準化されて何年かたっているが、利用が進んでいない。CRYPTREC として、国内でどういったアプリケーションで使用していくのか、どのように利用を促進していくのか、といった点についてどのような議論を行っているのか。

暗号技術評価委員会事務局：暗号技術調査ワーキンググループ（軽量暗号）の今年度報告書に、アプリケーションについても記載していく。

松尾構成員：具体的にどのようなアプリケーションが挙げられているのか。

暗号技術評価委員会事務局：委員からの意見としては、リアルタイム性が求められる用途として「メモリの暗号化」、「自動車の安全に関わる部分」などがあった。

（４）暗号技術活用委員会の活動状況

資料４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。

〇質疑応答

松本（泰）構成員：「① 暗号の普及促進・セキュリティ産業の競争力強化に係る検討」及び「② 暗号政策の中長期的視点からの取組の検討」に関して、「暗号」はサービス提供者側の競争力強化に必要なコア技術であると認識している。国産暗号、暗号アルゴリズムといった枠組にとらわれず広い意味での暗号技術と、産業競争力や課題解決との関係性について整理された方が良いと考えるが、この点についてどう考えるか。また、電子政府向けという従来の CRYPTREC の範囲を越えて、産業の領域まで広げていくことについて、どのように考えているのか。

松本（勉）暗号技術活用委員会委員長：暗号アルゴリズム以外の、暗号プロトコル等の広い意味での暗号技術についても、本来 CRYPTREC で取り扱われるべき。しかし、どのように取り扱うかという点について今年度の暗号技術活用委員会で検討しているところであるが、数年間模索を続けている大変難しい課題であると認識している。

今井座長：今年度の暗号技術活用委員会において、課題をある程度整理した形で出してもらえるのか。

暗号技術活用委員会事務局：アプリケーションとの連携という観点からの整理は難しいと感じている。諸外国の動向という点については、まず制度面・体制面がどうなっているのか、調査を行った段階である。

今井座長：広く暗号技術について検討することは重要である。上手く進めていけば産業競争力の強化にも繋がる可能性がある。今後の検討課題である。

今井座長：近年、国際標準化を行う場も増えており、標準化推進ワーキンググループの委員だけで全てをカバーすることは難しいのではないか。

暗号技術活用委員会事務局：標準化推進ワーキンググループに担当の委員がいない分野についてはカバー出来ていないが、まずは比較的重要と思われる分野について俯瞰図を作成し、将来的に拡張していくことも検討する。

（５）その他

〇質疑応答

松本（勉）構成員：現在法案審議が進んでいるサイバーセキュリティ基本法について、法案が成立した場合に、政府における暗号技術の取扱はどのように変化すると考えられるのか。

暗号技術検討会事務局：まず本法案は議員立法である。政府として立法趣旨を推察した場合、サイバー攻撃が益々増加する中、政府として積極的に対策を講じることを示すものである。暗号技術は、セキュリティ対策を講じる際の手段として重要であると考える。

今井座長：近年、量子コンピュータについて話題に上ることが多い。最近話題になった量子アニーリングに基づく計算法について、ご説明願えないか。

松井構成員：現時点で暗号技術の安全性を脅かすような手法ではない。素因数分解を容易に行えるような量子コンピューティングは、技術的に大変難しい。

国分構成員：暗号技術を輸出する場合、諸外国の規制などにも影響を受けると考えられるので、CRYPTREC としてもグローバルな視点をより強く意識した方が良いのではないか。

暗号技術活用委員会事務局：諸外国では、安全保障の観点を含めて暗号を取り扱っており、輸出できたとしてもその国に入り込んでいけるかどうかは別の問題といった状況である。

３　閉会

経済産業省の大橋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、2014 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