2009年度第2回暗号技術検討会　議事概要

１．日時　平成22年3月16日（火）　9：30～10：50

２．場所　経済産業省別館8階　825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）、宇根 正志、太田 和夫、岡本 栄司、岡本 龍明、加藤 義文、金子 敏信、国分 明男、武市 博明、松井 充、松本 勉、松本 泰

オブザーバ：木本 裕司、初川 泰介（高橋 浩二代理）、松本 和人（橋本 敏代理）、水野 伸太郎（中野 正康代理）、馬場 啓晴（江原 健志代理）、郡司 久（田中 正幸代理）、小貫 卓也、井上 幹邦、松本 裕悟（坂下 圭一代理）、米子 房伸（篠田 陽一代理）、大塚 玲、矢島 秀浩、亀田 繁、岸本 博之

暗号方式委員会事務局：松尾 真一郎

暗号実装委員会事務局：山岸 篤弘

暗号運用委員会事務局：田中 秀磨

暗号技術検討会（CRYPTREC）事務局：

総務省　河内 正孝、古賀 康之、梶原 亮

経済産業省　富田　健介、山田 安秀、下里 圭司

４．配付資料

資料２－１	2009年度第1回暗号技術検討会議事概要（案）
資料２－２	暗号技術検討会2009年度報告書（案）
資料２－３－１	2010年度暗号方式委員会活動計画（案）
資料２－３－２	2010年度暗号実装委員会活動計画（案）
資料２－３－３	2010年度暗号運用委員会活動計画（案）

参考資料１	暗号技術検討会　構成員・オブザーバ名簿
参考資料２	CRYPTREC シンポジウム 2010 -応募暗号説明会- 配付資料

５．議事概要

１．開会

事務局から開会の宣言があり、経済産業省の富田審議官から開会の挨拶があった。

オブザーバの交代について報告があった。

２．議事

（１）2009 年度第 1 回暗号技術検討会議事概要（案）の確認

資料 2-1 に基づき、暗号技術検討会事務局から 2009 年度第 1 回暗号技術検討会議事概要(案)の確認が行われた。

（２）電子政府推奨暗号リストの改訂に向けた進捗状況

資料 2-2 第 3 章に基づき、暗号方式委員会事務局から電子政府推奨暗号リストの改訂に向けた進捗状況について説明があった。その後の質疑応答で以下の発言があった。

今井座長：暗号技術の公募を行なって 6 件の応募があった。これは前回のときよりもだいぶ少ないが、今回はカテゴリを絞ったのでまずまずの応募状況であったと言えるのではないか。また、いただいたご意見というところでは、パネルの時に出てきたご意見のみを記載しており、合同委員会での意見は掲載されていないという理解でよいか。

暗号方式委員会事務局：そのとおり。

辻井顧問：エンティティ認証で、無限ワンタイムパスワードについての議論は逆説的で印象深かった。ID・パスワードをちゃんとやろうとすると、結局は公開鍵暗号に関する議論に帰着するということか。一昨年の 6 月、福田総理大臣の頃に、NISC から、公開鍵暗号を使っているから電子政府の普及が遅いという意見があったが、乱暴だという印象を持っていた。今回の暗号技術の応募について、公開鍵暗号が利用されているのは公募要項がそのようになっているからという理解でよいか。

暗号方式委員会事務局：エンティティ認証については、事務局選出のものに公開鍵暗号を使用しているものも電子署名を利用しているものもある。今回の提案されている方式は、世の中で使われているものの１つとして理解している。公募要領では、公開鍵暗号を使用したものでも、共通鍵暗号を使用したものでも提案していただけるような書き方にしている。

松本勉構成員：シンポジウムの時と比較して、暗号利用モードのカテゴリに事務局選出暗号技術が 2 つ追加されており、賛同する。これから 2 年間の評価に入るということだが、評価の途中で、事務局選出暗号技術を追加することもありえるのか。

暗号方式委員会事務局：基本的には考えていない。

松本勉構成員：基本的にはないということは了解した。しかし、緊急を要する場合には別途考える必要がある。

今井座長：応募暗号の中には、8 月までに国際会議に出す予定になっているものが 2 件あり、この 2 件は途中で落ちてしまう可能性もあるという理解でよいか。

暗号方式委員会事務局：そのとおり。

（３）暗号技術検討会 2009 年度報告書（案）について

資料 2-2 に基づいて、暗号技術検討会事務局から暗号技術検討会２００９年度報告書（案）の全体構成についての 説明が行われた。構成員から特段のコメントはなく了承された。

①暗号方式委員会活動報告

資料 2-2 第 4 章に基づき、暗号方式委員会事務局から暗号方式委員会活動報告が行われた。その後の質疑応答で以下の発言があった。

金子構成員：疑似乱数生成については、互換性維持の観点からリストに入れようというように聞こえたが、そもそも必要なのか。

暗号方式委員会事務局：互換性維持の必要性が少ないため、リストには入れず、リストガイドで実装仕様を定めるということである。

②暗号実装委員会活動報告

資料 2-2 第 5 章に基づき、暗号実装委員会事務局から暗号実装委員会活動報告が行われた。特段の質疑応答はなかった。

③暗号運用委員会活動報告

資料 2-2 第 6 章に基づき、暗号運用委員会事務局から暗号運用委員会活動報告が行われた。その後の質疑応答で以下の発言があった。

今井座長：暗号運用委員会は今年度に立ち上がったもので、扱う内容が難しいため苦労しているようだが、リストを本当に使ってもらえるものにするために必要な検討を行っていただいているものと認識している。

金子構成員：電子政府推奨暗号リストの位置づけについてディスカッションしていただきたい。例えば、電子政府で暗号を使う場合はリストに掲載された暗号技術の利用をマストにするのか、それとも選べるようにするのか。マストにするのであれば、暗号の数は少ない方が良い。

今井座長：その話はこの場だけでは決められないので、NISC にもご意見を頂きたい。

木本オブザーバ：電子政府推奨暗号リストについては、各府省で CRYPTREC の議論を参考にさせていただいているところ。数を絞り込むことに関しては、調達の支障にならないようにという観点も考えて策定する必要があるのではないか。技術的な観点からは、CRYPTREC のご意見を参考にさせていただきたいと考えているので、引き続き審議をお願いしたい。

松本勉構成員：電子政府推奨暗号リストは外国から見ても理解可能にしておくべきであると考えるが、英訳をする予定はあるのか。アクセシビリティは重要で、日本でしっかりやっているということを外国からも見えていた方が良い。

（４）今後の CRYPTREC 活動について

資料 2-2 第 7 章、資料 2-3-1、資料 2-3-2 及び資料 2-3-3 に基づき、暗号技術検討会事務局及び各委員会事務局から今後の CRYPTREC 活動について説明があった。その後の質疑応答で以下の発言があった。

辻井顧問：公開鍵暗号はこれからの社会の基盤となるはずである。韓国においては、2003 年に盧武鉉氏が大統領に就任した時に、国家的課題の 1 つとして、電子政府の推進が挙げられ、積極的に推進されるようになった。日本では、公開鍵暗号を使っていることが問題なのではなくて、電子政府が全体最適化の観点から政府のインフラとして捉えられていないことが問題であると考える。電子政府は国民の基盤として重要であり、これを ID とパスワードでやろうとすると公開鍵暗号を使う必要が生じてくるので、全体最適化の中に CRYPTREC の活動を位置付けていただくことを諸官庁にお願いしたい。

宇根構成員：リストガイドについて、鍵管理と等価安全性についてはどのような検討を行なうのか。

暗号方式委員会事務局:鍵管理と等価安全性については別々のものだと考えていただきたい。ISO、FIPS 等でも鍵管理について記載されているが、使う人にとっては分かりにくいものもあるので、分かりやすいガイドとしてまとめていきたい。等価安全性の方は NIST から出ているものをベースとして、どれだけのものを出せるかということを含め、今後、検討を行ってまいりたい。

松本泰構成員：鍵管理については、そもそも暗号方式委員会のタスクなのか疑問がある。一般論として、3 つの委員会全てに関係するものであると考える。例えば、暗号化された個人情報の扱いの問題は、鍵管理のプラクティスが無いことに起因している。これは鍵の運用の問題だと言える。

暗号方式委員会事務局：辻井顧問からも検討のご要望があったように、暗号技術を使うことと鍵管理とはセットだと考えているので、リストガイドという形でまとめようとしている。

今井座長：鍵管理についてはリストガイドで記述するということで、リスト自体に組み込むことはないということか。

暗号方式委員会事務局：そのとおり。

今井座長：鍵管理は根本的に重要であるが、適用先のアプリケーションに大きく依存するものであるため、統一的なことを書けるのか。CRYPTREC としては、電子政府の安心・安全を守るという観点で、実装等についても扱い始めたところなので、鍵管理についても同様の観点で、まずリストガイドから入って行くということ。

辻井顧問：鍵管理については、クラウドの時代になるとますます重要になると考える。

暗号運用委員会事務局：鍵管理はプラクティス寄りなので暗号実装委員会や暗号運用委員会で扱うべきだという意見もあったが、まずは暗号方式委員会で頭出しを行なって、暗号実装委員会や暗号運用委員会に展開していくという形を考えている。

松本泰構成員：共通鍵暗号と公開鍵暗号では、その鍵管理の考え方の違いがある。韓国のように公開鍵による認証基盤が広く利用されるためには、共通鍵暗号と公開鍵暗号の

鍵管理の違いなどがもっと理解される必要がある。

今井座長：韓国では官主導で電子政府を強力に推進していたが、暗号については国産のものを適当に使っている。この部分については、CRYPTREC のある日本の方が進んでいると考える。

金子構成員：サイドチャネル攻撃の話があったが、ハードウェアのサイドチャネル攻撃しか検討対象としていないようにも聞こえたので、ソフトウェアのサイドチャネル攻撃についても忘れずに検討を行っていただきたい。

暗号実装委員会事務局：ご指摘の点は認識しており、ソフトウェアのサイドチャネル攻撃についても検討を行なっていきたい。

宇根構成員：等価安全性について、重要なのは SSL の使い方である。SSL の適切な使い方について、可能であれば検討していただきたい。

松井構成員：暗号運用委員会の利用実績の調査は、難しいものであると考える。暗号技術としてはオープンなものであっても、個別の製品としてはクローズなものもある。特に電子政府に利用されているものは官公庁との間で守秘義務がかかっていることもあり、アンケートを取っても答えにくいところもあるのではないか。こういう調査を行なうのであれば、暗号を作っている側だけではなく、運用している側にも聞いてみるのも一案ではないか。

（５）その他

事務局から、構成員の外国への情報発信を行うべきという指摘を踏まえ、必要な情報の英訳について検討したいので、場合によっては、次回の検討会の前にメールで連絡等をさせていただくこともありえるので、ご協力をお願いしたい旨発言した。

３．閉会

総務省の河内総括審議官から閉会の挨拶があった。

事務局から、次回会合の日程、場所等については別途連絡する旨、連絡があった。

以上