2010年度第1回暗号技術検討会　議事概要

１．日時　平成22年12月17日（金）　10：00～12：00

２．場所　経済産業省別館10階　1028会議室

３．出席者（敬称略）

構成員：今井 秀樹（座長）、岡本 栄司、岡本 龍明、加藤 義文、国分 明男、櫻井 幸一、
佐々木 良一、松本 勉、寶木 和夫、武市 博明、苗村 憲司、松井 充、松本 泰、
米山 正夫

オブザーバ：木本 裕司、丸林 夏彦 （高橋 浩二代理）、松宮 志麻（澤田 稔一代理）、
浦船 利幸（高地 圭輔代理）、浦上 哲朗（山崎 重孝代理）、
馬場 啓晴（江原 健志代理）、荒木 美敬（中前 隆博代理）、
石井 貴光（寺岡 光博代理）、本間 陽也（田中 正幸代理）、
西 正弘（松原 徳和代理）、山中 豊（山本 雅亮代理）、
坂下 圭一、高橋 幸雄、渡辺 創、亀田 繁、鈴田 信

暗号方式委員会事務局：大久保美也子

暗号実装委員会事務局：山岸 篤弘

暗号運用委員会事務局：神田 雅透

暗号技術検討会（CRYPTREC）事務局：

総務省　武井 俊幸、中野 正康、水野 伸太郎、佐々木 伸行、谷岡 大祐

経済産業省　富田 健介、山田 安秀、森川 淳、池西 淳

４．配付資料

資料１－１	2010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	2009年度第２回暗号技術検討会議事概要（案）
資料３－１	政府機関における暗号アルゴリズム危殆化に備えた緊急対応計画
資料３－２	急激な安全性の低下時における暗号技術検討会及び各委員会の役割について（案）
資料４－１	暗号方式委員会活動報告
資料４－２	暗号実装委員会活動報告
資料４－３	暗号運用委員会活動報告
資料５	CRYPTREC用語の英語名称について
参考資料１	暗号技術検討会構成員・オブザーバ名簿及び各委員会構成員名簿
参考資料２	2010年度暗号技術検討会活動計画

５．議事概要

１．開会

事務局から開会の宣言があり、総務省の武井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。また、本年度検討会において今井座長の選任、辻井顧問の指名があった。(今井座長より、辻井顧問は本検討会は欠席だが事前に内諾を得ている旨、説明があった。)

２．議事

（１）2009 年度第 2 回暗号技術検討会議事概要（案）の確認

資料 2 に基づき、暗号技術検討会事務局から 2009 年度第 2 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掲載暗号危殆化時の対応について

資料 3-1 に基づき、内閣官房情報セキュリティーセンター木本参事官より、政府機関における暗号アルゴリズム危殆化に備えた緊急対応計画について説明があった。その後、暗号技術検討会事務局から資料 3-2 に基づき、危殆化時における対応の提案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。

佐々木構成員：大筋では問題ないと思う。内容にまで入ったときに、例えば公開鍵暗号系、ハッシュ系においては、新しい暗号方式を使うだけではなく、過去の存在する署名付き文書等に対する対策についても説明しないといけない。どういう形でやっていくのか。事前に公開鍵暗号系については、危殆化したときは文書をどこかで管理していて、新しい署名する等対応策を決めておかないと、対応が遅れることと心配している。運用についてはどういう考えか。

暗号技術検討会事務局：運用については、政府の緊急時対応計画があるので、緊急時の度合いによって、どういう場合に発動するか NISC で決めることだが、運用委員会の方でも一般的な技術の観点から発動が各委員会の役割に応じて何を進めていくか今後の検討を頂けたらと思っている。

今井座長：重要な話しであると思う。検討会で議論すべきことはどういう方向性を取るのが良いのかをこの検討会においてリコメンドする。どういう対処するのかについて、いろんな要素が絡んでくる。基本的には運用委員会で検討して頂き、その他の委員会で必要事項について議論せざるを得ない。

松本(勉)構成員：資料 3-2 の 2 ページの図 1 の情報伝達フロー図について、これの検討はいつするのか。今行うのか。

暗号技術検討会事務局：このフローは、エクセルの表が完成した後に、どのように情報を流すべきか並行して検討を行う。

松本(勉) 構成員：論文等からありえるが、例えば、他の国で関連する暗号技術を政府が使うのをやめた場合、またニュースで流れた場合も方式委員会で事実関係を調査する形になるのか。これで対応しきれるのかがよく分からない。別紙の表の方を考えてから全体の流れが決まるのか。

暗号技術検討会事務局：このようなものを作りたいというイメージであり、決定したというものではない。

今井座長：重要な議題である。今後、それぞれの委員会で十分精査していただいて、情報交換が必要。この流れを最終的に案として作って頂き、次回の検討会で最終的に決める。今の段階で他にコメントを頂いておくようなことはあるか。

松本(勉)構成員：検討事項（案）に、３つの委員会が書かれている。どういう流れで対処するか。左側の電子政府にあるのか、他の部分にこれをしてくださいという流れがあると思うが。というのがあると思うが、そこの部分については、誰がどう考えるのか。すなわち何かイベント、予兆があると、CRYPTREC で監視しているので、これをしてくださいと CRYPTREC 外部から何かアクションがあると思うが、そこも併せて検討しないといけないと思う。

暗号技術検討会事務局：外部からの情報提供についてはあると思うが、委員会として検討すべきと思われる項目について、各委員会にトリガー案を検討してもらって、対応可能か議論していただく。

今井座長：そういうことも含めて各委員会で検討していただく。

（３）本年度の各委員会の活動報告

資料 4-1～3 に基づいて、各委員会の 2010 年度活動報告についての 説明が行われた。

①暗号方式委員会活動報告

資料 4-1 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。

特段の質疑応答は無かった。

②暗号実装委員会活動報告

資料 4-2 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。

その後の質疑応答で以下の発言があった。

今井座長：この委員会と ISO との国内委員会との関係はどうなっているのか。

暗号実装検討会事務局：暗号実装委員会である松本委員長から SC27 の WG3 の委員として CRYPTREC としてまとめたコメント案を提出している。

③暗号運用委員会活動報告

資料 4-3 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：リスト構成というのは、何が良くなって何が悪くなるということを表しているのか。

暗号運用委員会事務局：分けたことで、分かりやすくなっているか。どのような点が明確になると分かりやすくなるかと聞いている。

松本(勉)構成員：この外部ヒアリング候補案の備考欄はどういう意味か。

暗号運用委員会事務局：他のカテゴリでノミネートされている企業を２重に説明する必要があるので、外させていただいている。サーバーだとＮＥＣ、富士通、日立とか備考に書かれているが、SIer の方でメインに対応している。

松本(勉)構成員：電子政府推奨暗号リストの考え方に対するシナリオについて、評価軸がＡ～Ｆまであげられているが、電子政府側、あるいは暗号技術検討会側サイドとしてのコスト、もしくは CRYPTREC を運用していく上でのコストあると思うが、この評価軸の中に入っているのか。この軸の研究体制に入っているのか。

暗号運用委員会事務局：CRYPTREC としての評価体制の明確に対象にあがったものではない。

松本(勉)構成員:シナリオ１のレーダーチャートにおいてセキュリティ研究体制の影響というのは、大きく２つの方向にあると思う。国内の企業の研究者が体制を保ってないといけないという部分がある。人的パワーを活用して、CRYPTREC がいろいろな評価を行ってきた。これが手薄になってしまうという、セキュリティ体制の影響が中心にあると思う。

暗号運用委員会事務局：そういう影響は考慮していない。

松本(勉)構成員：運用面ではセキュリティ研究体制として CRYPTREC の評価が無くなる。２つくらい分けないといけないのではと思う。このことは CRYPTREC として、または日本として、暗号を評価できる人のきちんと確保しなければいけない　　政策的な視点として政策的判断が必要。業界の体制を論じるところにつながる重要なところであると思う。

今井座長：シナリオの４つについて、もう一つ軸が入る可能性があるとは思うが、これについて他に意見はないか。

苗村構成員：CRYPTREC の存在そのものについて、体制が存在することによって日本の中で暗号技術の安全性評価をする能力が備わったことは事実。存続する可能性を高めることをあってもいいのではないか。レーダーチャートを見ると安全評価が論点になっているのは当たり前で、国内で、評価体制を維持できるかということが重要。Ａの評価結果が低くなるのではないか。評価軸のＡを変えたらどうかと思う。

今井座長：今日は結論を出すということではなくてご意見を頂くとして。

櫻井構成員：研究者育成という立場から議論するなら、日本の暗号技術でハッシュ関数を研究する体制が少ない。日本が発表している論文等のデータを出していただければ説得あると思う。

今井座長：確かに国際会議の場において、日本の発表が減ってきている事実はあると思う。その辺をどう考えるか。

寶木構成員：SC27 のベルリン会合で暗号アルゴリズムの ISO の標準化については、きっちり評価すべきではという意見が ECRYPTⅡから出た。SC27 委員長から、日本の CRYPTREC のことが言及された。日本としての国際標準への対応について CRYPTREC を軸に考える時期である。

今井座長：今までは暗号研究者からの発言が多かったが、ユーザーの立場からの意見はいかがか。シナリオ１～４のどれが良いか各委員からコメントお願いしたい。

米山構成員：シナリオ２か３が個人的には良い。

松本(泰)構成員：ユーザーの立場からすると、シナリオ１か２が良いのではないか。そもそも対象となる暗号技術とは何を指しているのか。実際に使われている暗号は何かを明確にした方

が良い。

松井構成員：強い意見は無いが、確認させて頂きたい。

苗村構成員：この資料 4-3 の中で、４つのシナリオを挙げること自身は大いに良い。この中からどうするかを選択する考え方も良いと思うが、シナリオ１の下の本シナリオの意図に書いてあることは誤解を招くのではと感じたのでコメントする。2000 年暗号輸出規制緩和以降として、米国についての記載があるが、製品化は確かにその通りだと思うが、国際標準化は正しくない。米国政府標準は、おそらく RSA は入らないと思う。ここで言いたいのが、TripleDES がそうだというのであればその通りだが、これはおかしい。AES の場合は、暗号規制とは無関係にもともと欧州で開発されたものであるから米国が規制することは出来なかったはず。誤解を招く文章であると思う。参考資料１の中でも、RSA を推奨と書いてあるが、RSA を国の政府調達で推奨している国は無いのではないか。事実は、米国政府は非常に高い評価能力を持っている。その結果、AES のように欧州で開発されたものを採用して、それを積極的に調達に利用している。民間でも普及している。それとは別に RSA のように民間の努力で普及した。そういう中で日本はどうするのかという時に、アメリカの政府と同じように評価し、日本独自のものを出すのかが問われている。誤解に基づいて、どれかのシナリオを選ばれるのはどうかと思うし、専門家の皆さんに確認をしていただきたい。要するに欧州は、暗号の技術開発の力もあるし、評価能力も持っている。アメリカは、開発能力もあるし、評価能力と体制もある。日本は、開発能力は間違いなくあるが、評価能力はようやく上がってきた。欧米が選んだものを採用することにして、コストが減るけども評価体制がなくなるがそれが日本にとって良いことなのかどうか。欧米の評価能力に依存するかどうか。

暗号運用委員会事務局：国際標準化に関しては、ISO ではなく、ここでは IETF、IEEE などをイメージしている。

武市構成員：リストが長くなるというのは選択肢が増える一方、絞っていく方向では使われるのかという疑問がある。シナリオ３はある意味で興味ある。

寶木構成員：議論が産業全般、国だけの調達だけでなくてとなりますと、アンケートも広く使われていて、携帯電話とか放送とかにも使われている。電子政府推奨暗号リストに掲載されていない暗号も使われている事実もある。それから、国際標準化と言いましたが、基本的には良い技術がフェアに決められることが、一番日本にとってハッピーである。製造業界、研究者の間であると思う。現実では、ナショナリティをあげて、必ずしもフェアでない暗号標準が入ってきているという現状であるので、それをなるべく阻止して、我が国としては良い技術がナンバー１になるという形を推奨すべき。シナリオ２をメインで考えている。

松本(勉)構成員：暗号技術は少なくして、競争力のある暗号技術を育てていくことが良い。シナリオ２が良いと思う。

佐々木構成員：とりまとめの立場からどれが良いとは言い難いが、シナリオ３は幅が広い。やり方によっては、シナリオ２にもシナリオ４にもなり得る。シナリオ３になってもやるべきことはたくさんある。

櫻井構成員：４つのシナリオは面白いと思うが、今後どれを選択すればどうなるというシミュレーションを出してもらうのが良い。人材育成の観点から、そういう軸でシミュレーションを

やれば選びやすくなる。国際標準化に関しては、米国以外の国ではAESを使わないという自国のものだけ使う国があったりする。ヨーロッパのものも採用したりする国もあるので、データを整理した方が情報としては参考になると思う。

国分構成員：私は暗号技術ではなく、ICカードの開発で電子政府システムを作るという立場で座っている。ヨーロッパのICカードメーカーとの間で、チップのレベルで非常に高度な高機能なものを作るとなると高くなる。客は暗号の強度とかはあまり評価しなく、コストで判断したりするのだが、ICカードがたくさんある中で、暗号がやぶられると世界的に大変なことになるので、シナリオにおいては、あまり使われない暗号がリストに掲載されていても、掲載されているだけになるので、使われるもの、実績があるもの、これからメジャーになっていくものが入っていれば良いのではないかと思う。シナリオ２で考えていくのが良いと思う。

岡本(龍)構成員：先ほど苗村構成員の意見にも関連するが、アメリカの連邦政府の公開鍵暗号に関しては、聞いた話しだとRSAじゃなくて、楕円曲線暗号を電子政府調達暗号として今後は進めていく方針と聞いている。理由はいろいろあって鍵サイズの問題。だから、圧倒的に民間の使用はRSAが９割近く。民間で使われているから政府で使用する暗号にするというのではなく、今後望ましいかという観点から楕円曲線暗号を選んだと聞いたことがある。アンケートをとると今使われているもの、RSAが良いというわけでは無いと思う。何のためにCRYPTREC委員会があるか。CRYPTRECの専門家としての観点が強調されてもいいのではないか。良いリストを作るというよりも、政府調達暗号で使ってはいけないもの。悪いものだけ使われないことに対する排除するという考え方があっても良いのではないかと思う。現在使われているものに流されるのは良くないと思う。

岡本(栄)構成員：シナリオ４は安全性だけというのは無いと思う。シナリオ１こちらは今までの実績。シナリオ２と３を合わせた感じが良いと思う。

暗号技術検討会事務局から、資料4-3参考資料2に基づいて、ISO/IEC JTC1/SC27における暗号アルゴリズム規格に関する状況について説明があった。

（４）CRYPTRECの英語名称について

資料5に基づき、暗号技術検討会事務局から報告があった。特段の質疑応答等は無かった。

３．閉会

経済産業省の富田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