2008年度第1回暗号技術検討委員会　議事概要

１．日時　平成20年7月4日（金）　10：00～11：30

２．場所　総務省8階　第1特別会議室

３．出席者（敬称略）

構成員：今井 秀樹（座長）、辻井 重男（顧問）、岩下 直行、岡本 龍明、国分 明男、佐々木 良一、宝木 和夫、武市 博明、酒井 康行（松井 充代理）、松本 勉、松本 泰

オブザーバ：伊藤 毅志、大橋 一夫（高橋 浩二代理）、宮田 拓司（中井川 禎彦代理）、山西 浩仁（相澤 哲代理）、佐久間 明彦（菊田 豊代理）、風間 広幸（田中 正幸代理）、山田 一彦（佐藤 勉代理）、和泉 章、武田 仁己、安井 哲也（篠田 陽一代理）、大蒔 和仁、山田 安秀、亀田 繁、岸本 博之

暗号技術監視委員会事務局：田中 秀磨

暗号モジュール委員会事務局：山岸 篤弘

暗号技術検討会（CRYPTREC）事務局：

総務省　河内 正孝、田中 宏、荻原 直彦、川崎 光博、梶原 亮、齊藤 修啓

経済産業省　木村 雅昭、三角 育生、黒田 俊久、下里 圭司、花田 高広

４．配付資料

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1-3　2007年度第3回暗号技術検討会議事概要（案）

資料1-4-1　2008年度暗号技術検討会（CRYPTREC）活動計画（案）

資料1-4-2　2008年度暗号技術監視委員会活動計画（案）

資料1-4-3　2008年度暗号技術監視委員会運用方針（案）

資料1-4-4　2008年度暗号モジュール委員会活動計画（案）

資料1-4-5　2008年度電力解析実験WG活動計画（案）

資料1-4-6　2008年度暗号モジュール委員会運用方針（案）

資料1-5　電子政府推奨暗号リスト改訂骨子（案）

資料1-6-1　メール審議結果報告

資料1-6-2　JCMVPからの要望に対する回答

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　暗号技術検討会　2007年度報告書

参考資料3　CRYPTREC report2007

参考資料４　電子政府推奨暗号の利用方法に関するガイドブック

５．議事概要

（１）開会

木村経済産業省大臣官房審議官より開会の挨拶があった。

（２）暗号技術検討会の開催要綱（案）について

暗号技術検討会の開催要綱について、資料 1-1 に基づき暗号技術検討会事務局から説明があり、承認された。

（３）暗号技術検討会の公開（案）について

暗号技術検討会の公開について、資料 1-2 に基づき、暗号技術検討会事務局から説明があり、承認された。

（４）座長、顧問の選任について

座長の選任、顧問の指名があり、今井座長、辻井顧問が選任された。

（５）2007 年度第 3 回暗号技術検討会議事概要（案）の確認

資料 1-3 に基づき、暗号技術検討会事務局から 2007 年度第 3 回暗号技術検討会議事概要（案）の確認が行われた。

（６）2008 年度の活動計画（案）について

資料 1-4-1、1-4-2、1-4-3、1-4-4、1-4-5 及び 1-4-6 に基づいて、暗号技術検討会事務局、暗号技術監視委員会事務局および暗号モジュール委員会事務局から説明が行われた。引き続いて、各委員会について質問、意見が交わされた。質疑の概要は以下のとおり。

ア　暗号技術検討会

今井座長：資料 1-4-1 について、今年度の昨年度と違う点は電子政府推奨暗号リスト改訂に関する調査検討を具体化させていくことだが、(3) の項目以外で変わっていることは。

暗号技術検討会事務局：(3) 以外は特に変更はなく、引き続き行うこととしている。

今井座長：スケジュールでは、本検討会の開催は現時点では 3 回ということになっている。もちろん途中でメール審議等が入ることもある。今年度は公募の方針についてパブリックコメントを求めるということで、その対処等で審議回数が増える可能性はある。

イ　暗号技術監視委員会

今井座長：安全性評価を行う体制について検討する時、これまでは WG を使っていたが、これを新たに検討するというのはどういうことか。

暗号技術監視委員会事務局：WG でやるか、事務局である程度、評価の体制をまとめてから審議するか、フレキシブルにやれる方法がないか考える。

ウ　暗号モジュール委員会

佐々木構成員：暗号アルゴリズムでは、基本的に脆弱性が見つかればそのままオープンにする仕組みだったと思うが、暗号モジュール等に関する脆弱性が見つかった場合の公表の仕方の方針は考えているのか。

暗号モジュール委員会事務局：暗号モジュール委員会で脆弱性の届出を受け付ける訳ではない。脆弱性に関しては IPA の中で行っている「暗号モジュール試験及び認証制度」の中で確認を行い、欠陥がないかチェックしている。欠陥がある物に関しては認証を出さないとか、修正を求めるという対応をとっている。一方、市場に出回っている製品のモジュールに脆弱性が指摘される可能性はあるが、それへの対応はできていない。今後の宿題としたい。

今井座長：暗号アルゴリズムに欠陥があった場合の対応については、学会で公開されるなどはっきりしている。具体的な製品に実装された暗号に欠陥があったという場合は､それがソフトウェアなら IPA が中心となって一応の体制ができている。それと同じようなものがいずれは必要であろう。オープンにしないというのはまずいし、かといって具体的な脆弱性までオープンにするのは影響が大きいのではないか。

暗号モジュール委員会事務局：ソフトウェアなら比較的早く対応できる。ハードウェアでは、ファームウェアで修正が効く場合はソフトウェアと同じような対応ができるが、それ以外の場合は作成のし直し等が必要で時間がかかる。今の体制で対応するのは難しく、ペンディングにしている状況。

松本勉構成員：暗号技術検討会で何をどこまで検討すべきかということから議論する必要がある。現在は、電子政府推奨暗号リストがあって、暗号アルゴリズムについては定められている。それに対して、暗号アルゴリズムを実装した暗号モジュールについては統一基準の中で認証されたものを使用することが望ましい、というオプショナルな扱いになっている。一旦認証されたものに関して問題があるということであれば、その制度の中で判断できるが、世の中一般に出回っているものについて、脆弱性を指摘した場合にどうするべきかということをこの検討会でどこまで議論すればいいのかということを考える必要がある。先程の佐々木構成員の話は、誰かがそのような情報をコントロールしなければなら

ないということでは。

佐々木構成員：オープンにするまでに一定の対策期間をとるべきだと考える。最初は審査機関が対応する話であり、それ以外が行うかについては課題になるのでは。しかし、ここがやらなければ誰もやらない話なので、何らかのことは考えた方がよい。

今井座長：松本構成員の言う通り。CRYPTREC の座長としてではなく暗号研究家としてＩＰＡにはお願いしたい。いずれにせよこのようなことをどこかで検討しなければならない時期に既に来ている。総務省及び経産省で検討するべきだが、これを CRYPTREC でやるべきか否かについては議論が必要。

岩下構成員：難しいのは、何が暗号モジュールかということ。もちろん学問的には暗号モジュールを定義することができるが、使う人が暗号モジュールと考えなければ、暗号モジュールの問題だと認識してくれない。アルゴリズムに関してはクリアだと思うが、暗号を使っている製品は山ほどある。例えば、建物の鍵となる IC カードにも何らかの暗号が使われているはずだが、電子政府推奨暗号リストに入っている暗号か、実装は大丈夫なのかという話になると、ちゃんとチェックをされていることは恐らくないだろう。一方で、全ての暗号が電子政府推奨暗号リストに載っているものでなければならないかというと、それはアプリケーションによる。この点には注意しなければならない。アプリケーションの要請するセキュリティに対応するアルゴリズムが実装できているかというところからの評価が必要。この場合、アルゴリズム面からの検討に加えてアプリビジネスの意見を聞く必要もある。オランダやイギリスでは 48 ビットなどの暗号を用いた詐欺が横行しているが、一旦問題になると国を挙げて調査をする事態になる。問題になる前にどういうことになるか考えるのが必要。電子政府推奨暗号を使っていないのであれば、そもそも暗号モジュールの評価の基準に入らないものが多いだろうが、そういうものについてどう考えるのかも考えなければならない。

今井座長：必ずということではないものの、こういうことを考えられるのは CRYPTREC しかない。検討会、監視委員会、及びモジュール委員会の活動計画は総意で承認で良いか。

（異議なし）

（７）電子政府推奨暗号リスト改訂骨子（案）について

資料 1－5 に基づいて、事務局より暗号リスト骨子（案）について説明が行われた。質疑の概要は以下のとおり。

今井座長：昨年度議論があったが、ライトウェイトの暗号をどうするかという話はどう

なったか。

暗号技術監視委員会事務局：ライトウェイトは新しいカテゴリを作るという方向ではなく、同じスペックなら実装性能が今より高いということで、例えば「暗号技術公募の基本方針」における、(2)(a)応募可能な暗号技術の条件の中で、「既にリストに掲載されている暗号技術と同カテゴリに属する暗号技術については、それらの暗号技術よりも安全性及び実装性において優れた暗号技術であること。」という観点から公募するという方向。

今井座長：(b)に、「個別のシステムやアプリケーションの仕様に依存しない、汎用的な暗号技術であること。」とあるが、これには矛盾しないのか。

暗号技術監視委員会事務局：矛盾しないと考える。ただしミューチップのように極めてライトウェイトなものはシステムやアプリケーションの面であまりに範囲が絞られ、電子政府で推奨すべきものとは違うと考える。

佐々木構成員：表１にある公募カテゴリと別紙にある技術分類について。技術分類は公募カテゴリとして実施するのか。それとも、公募カテゴリに基づいて、今後の推奨リストを作っていくということか。

暗号技術監視委員会事務局：カテゴリは固定かという質問だと思うが、カテゴリを変えようということ。4 節の「暗号技術公募の基本方針」(1) 公募対象のカテゴリの決め方というところでは、例えば ID ベース暗号等の、リストに含まれていないがこれから標準化が見込まれると思われる技術は、将来的にはカテゴリを新たに作って公募を行うことになると考えられる。

佐々木構成員：暗号はこれでいいが、ハッシュ、鍵共有等はどうするのか。どこかに含まれているという認識か。

暗号技術監視委員会事務局：現在あるハッシュ関数や鍵共有などはそのまま載せることにする。

佐々木構成員：そうすると最終的な政府推奨暗号リストの分類としては、公開鍵・共通鍵・その他という形になるのか。

暗号技術監視委員会事務局:技術カテゴリとの整合性という問題もある。例えば CRYPTREC の技術カテゴリは ISO 等の技術カテゴリと一致していない。国際戦略（国際標準化）の面で不利になるのではという指摘もある。技術カテゴリの整合性の問題はこれから監視委員会で議題として挙げる。

佐々木構成員：変えていくというのは悪くないと思うが、カテゴリでカバーしきれず、公募されず積み残しとなる項目があるとまずい。

松本勉構成員：ハッシュは公募しないという案だと思う。公募とは別に、ハッシュのファミリーについては再編した形でそのまま電子政府推奨暗号リストに載せることはありうる。

暗号技術監視委員会事務局：今のハッシュで SHA-2 ファミリーがあるが、これはそのま

ま引き続き、再編した形で載せる。

岩下構成員：1-5-表 1 で、ブロック暗号自体は 128 ビットにしようという提案は良い。しかし、暗号利用モードと製品仕様コードで 64 ビット暗号をカテゴリに入れているのはなぜか。

暗号技術監視委員会事務局：現在 64 ビットブロック暗号として MISTY と Triple DES が入っているが、それがなくなるのかという話になる。64 ビット暗号が必要でなくなれば外してもよいが、現時点ではなくならない状況なので入れている。しかし新しく公募する状況ではないため、公募はしていない。

松本勉構成員：2 ページ図 1、現在のリストに掲載されている暗号はどこからスタートするのか。

暗号技術監視委員会事務局：同ページに「現リストに掲載されている暗号技術については、安全性の再評価を行った上で推奨暗号候補リスト（仮称）へ登録し、製品化の状況・技術の利用状況により電子政府推奨暗号リスト（仮称）へ登録するかの決定を行う。」と書かれているとおりとする。

松本勉構成員：次ページの（2）推奨暗号候補リスト（仮称）の部分にもそのように記述しておかないと矛盾するのではないか。「市場において利用実績が十分でない普及段階にある暗号技術が登録されているリスト。」と書いてあるので、初期値はそれに限らないということを言っておかなければならない。

今井座長：アルゴリズムとして完璧ではないと。入れておいた方がよい。

岩下構成員：3 ページ目の（1）電子政府推奨暗号リストについて、WTO/TBT 協定との関係はどこまで遵守しなければならないのか、またどうすれば遵守したということになるのか。例えば ISO とは違うリストになるはずだが、厳密に言えば TBT 協定違反にも見える。

暗号技術監視委員会事務局：この場で検討していただきたい。

今井座長：CRYPTREC 主催のイベントとは。

暗号技術監視委員会事務局：これまでの CRYPTREC の活動の総括、推奨暗号リストが変わるということでニーズが変わってきたということとその背景、公募要領等について、シンポジウムのような形で行いたい。

松本勉構成員：公募開始から締切りの期間は。

暗号技術監視委員会事務局：公募開始とは応募書類の受付という意味。アナウンスは 2008 年第 4 四半期に行い、イベントの時に公募要領を発表する。書類受付が 2009 年の第 3 四半期ということ。前回はアナウンスから締切までの期間が短かったので、今回は長く設定する予定。

今井座長：公募開始というのは誤解を招く表現なので、公募受付開始等、表現は適当に変えるべき。微修正はあるが、本件は了承したということでよろしいか。

（異議なし）

（８）その他

ア　NISC からの報告

NISC 伊藤参事官：CRYPTREC から、SHA-1 危殆化についてご指摘があった。それについての政府間の検討状況を報告する。政府における SHA-1、RSA1024 の利用について昨年度から検討を進め、今年 4 月、内閣官房長官をヘッドとする情報セキュリティ政策会議において「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」が決定した。今後政府でどのように新しいアルゴリズムに円滑に移行するか検討し、2013 年度末までに政府機関については情報システムを新しいアルゴリズムに段階的に移行する。この指針の中で、急激な安全性低下に対し、緊急避難的対応をどうするかについても検討することにしている。現在 NISC では具体的に段階的な移行の中身について、各省庁を集めた連絡会議で検討しているところ。この中で、急激に危殆化が進んだ場合の対応が緊急の課題となっている。ぜひ、CRYPTREC でも検討してほしい。これまで移行指針の検討に CRYPTREC にも協力していただいて感謝している。

イ　メール審議結果報告

荻原推進官：今年 3 月に JCMVP への回答書について、議論していただいたが、直後に参照する仕様書にミスがあったという連絡があり、4 月 14 日に訂正版の提出があった。このため、暗号技術監視委員会及び本検討会において改めてメール審議をしていただき、問題ないという判断をいただいた。資料 1-6-2 にあるように、事務局から 6 月 10 日付けで JCMVP に回答を提出し、本日配布した 2007 年度報告書 p23 の該当部分に経緯を書き込んでいる。

（９）次回開催予定

事務局より、次回会合については今秋の開催を予定しており、詳細については別途連絡する旨、連絡があった。

以上