２００７年度第３回暗号技術検討会　議事概要

１．日時　　平成２０年3月２５日(火)　１０：００～１２：００

２．場所　　経済産業省別館１０階　１０２０共用会議室

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、太田 和夫、岡崎 宏、岡本 栄司、岡本 龍明、加藤 義文、金子 敏信、国分 明男、櫻井 幸一、佐々木 良一、苗村 憲司、畠山 有子（松井充代理)、松本 勉、松本 泰

オブザーバ：伊藤 毅志、内藤 伸悟、小松 聖（中井川 禎彦代理)、藤井 信英（塚田 桂祐代理)、沼田 知之（相澤 哲代理)、荒木 美敬（菊田 豊代理)、森 規昭（田中 正幸代理)、佐藤 勉、和泉 章、武田 仁己、安井 哲也（篠田 陽一代理)、山田 安秀、亀田 繁、郡山 信

暗号技術監視委員会事務局：山村 明弘、松尾 真一郎

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：

経済産業省　　三角 育生、下田 裕和、小野塚 直人、花田 高広

総務省　　松本 正夫、田中 宏、荻原 直彦、増子 喬紀、山﨑 浩史

４．配付資料

資料３－１　２００７年度第２回暗号技術検討会議事概要（案）

資料３－２　暗号技術検討会２００７年度報告書（案）

資料３－３　暗号モジュール試験及び認証制度における技術審議委員会からの要望書に対する回答（案）

資料３－４　電子政府推奨暗号リストの見直しについて（案）

資料３－５　電子署名及び認証業務に関する法律の施行状況に係る検討会への回答

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　暗号技術監視委員会　委員名簿

参考資料３　暗号モジュール委員会 委員名簿

５．議事概要

１．開会

今井座長より開会の宣言があり、松本総務省大臣官房技術総括審議官より挨拶があった。

２．議事

（１）２００７度第２回暗号技術検討会議事概要（案）の確認

事務局より資料３－１の確認が行われた。

（２）２００７年度暗号技術検討会報告書（案）について

① 暗号技術監視委員会　活動報告

資料３－２に基づき、暗号技術監視委員会事務局から説明が行われた。

主な質疑については以下のとおり。

辻井顧問：大変すばらしい報告書（特にリストガイド）を作っていただいたと思う。今後アメリカのようにわが国の民間分野に電子政府推奨暗号を広めて行くには、組織間の連携の強化と成果の共有が必要と思う。その解決手段としてリストガイドの活用があればと思う。

岩下構成員：今回のリストガイドは大変良い資料だと思うが、電子政府推奨暗号リストの中でも、相対的により安全であろうと思われる、より厳しいセキュリティ基準を適用したものを使うことを推奨するように読めてしまう。また、電子政府推奨暗号リストとリストガイド、２つの基準をどのように適用するという説明をされるのか。

暗号技術監視委員会事務局：基本的にリストガイドは現在のリストより踏み込んだ内容になっている。ただしそれを強制するように定めるつもりはなく、推奨する立ち位置にある。設計上・実装上等の制約で従来の鍵長の暗号を利用せざるを得ない場合もあり得るためである。

松本勉構成員：特に公開鍵暗号ＷＧには精力的な評価をしていただき、新しい規格を参照できる形にあるいは置き換えていただき感謝している。

苗村構成員：リストガイドへの記述対象技術の分類方法が従来の推奨暗号リストのそれと比較して良く、役に立つと思う。一方で、ハッシュ関数 SHA-1 の取扱が、電子署名法で推奨するハッシュ関数についての議論の方向性と今回のリストガイドの記載内容で異なっていてわかりにくい。

暗号技術監視委員会事務局：現状の規格上または実装上の点で SHA-1 を選択せざるを得ないので、この使い方については問題ないということでリストガイドに掲載している場合がある。実装上の問題を議論した上で問題が確認されなければ、追認という意味で掲載していると考えていただくのが妥当と思う。

佐々木構成員：今回は、各分野において標準があり選択の余地がない場合は、その範囲で最善のものを使用する形で説明して、そこに CRYPTREC が推奨するものが全く入っていないようなものがあったら、それはやめていこうという形で作成した。

苗村構成員：例えば鍵導出関数としての SHA-1 を、推奨ではないものの使用を可とすることが書いてあるが、これはたぶん SHA-1 の使用について境界線を明確にされているのだと思う。使う側でこういう組合せで良いと書いているが、ハッシュ関数という目で見ると、SHA-1 はどのような場面で今後使えるのか、それがこの資料ではわかりにくい。今後とも積極的に導入していいものとして鍵導出関数では OK ということになっているのか、そういう整理をされたのか知りたかった。

暗号技術監視委員会事務局：鍵のスタンスで言うと、現状の CRYPTREC での評価結果に従う形で掲載しているので、それを追認する形になっている。今年度出す版については、最終的に FIX しているわけではないので、正確な記述を追加していくこと、次年度以降の改訂においてポリシーをより明確にしていくことを進めていきたいと考えている。

松本勉構成員：「改ざん検知・時刻保証」においては、SHA-1 の使用不可という風に記載して、細かい点で苗村構成員の御懸念の点は考慮している。

今井座長：「電子署名を用いたタイムスタンプ方式」でも同様の記述がある。一方、KPMについてはどうなっているか？
松本勉構成員：KPMは大丈夫です。
今井座長：そうならば、少しわかりやすいようなコメントを入れてほしい。
松本勉構成員：資料３－３は、何日付の回答になるのか？
暗号技術監視委員会事務局：出来るだけ速やかに今日付でお返しする。
今井座長：これで問題がなければの話しである。前回の暗号技術監視委員会から是正されわかりやすくなっている。
暗号技術検討会事務局：前回の暗号技術監視委員会の時に提出した図と比較して、「現在」「JCMVP要望」「CRYPTREC」での検討結果の表示を修正した。
苗村構成員：詳細が未確認のため、何かあったら検討会終了までに報告する。

② 暗号モジュール委員会　活動報告
資料３－２に基づき、暗号モジュール委員会事務局から説明が行われた。
主な質疑については以下のとおり。

今井座長：SASEBOは、電力解析実験用装置としてのみならず色々使えるのか。
暗号モジュール委員会事務局：SASEBOは、INSTACと同じように現在配布しているものはFPGAを使用しているので、対抗策（カウンターメジャー）の開発等で使っていただくことが可能と思う。現在、産総研の情報セキュリティ研究センターで互換性のあるLSIを開発し、それを搭載したボードの開発が可能との報告が上がっている。
今井座長：サイドチャネル攻撃においては、一時的な故障を利用した手法（フォールトインダクションアタック）が今後おそらく非常に強力になりその対策が重要になってくると思われるが、それにも対応できるということか。
暗号モジュール委員会事務局：対応できる。SASEBOには様々な入力が可能になっており、例として、外部から動作クロックを供給することが可能。クロックにノイズを入れたり、電源も外から供給できるので、そこにノイズを入れることも可能である。
今井座長：もう一点。こういったことを非常に積極的にやっていただいているが、FIPSへの影響は？
暗号モジュール委員会事務局：暗号モジュール委員会・電力解析実験WG及びINSTACの活動が反映されたと考えているが、FIPS140-3は正式に電力解析攻撃・電磁波解析攻撃に対するRequirementが追加されている。それに耐えうる試験要件・運用要件については今後NISTと共同して研究を進めるということで動いている。

③ 今後のCRYPTREC活動について
資料３－２及び資料３－４に基づき、暗号技術検討会事務局から説明が行われた。
主な質疑については以下のとおり。

今井座長：「新しい暗号技術の公募の考え方」の「④安全性に関して評価方法、評価基準および評価体制が整備されているあるいは整備が見込めること」というのはどういう意味か？
暗号技術監視委員会事務局：基本的には、暗号技術を公募するときに、評価技法がある程度合意が得られているようなものを目指すことである。
松本勉構成員：評価は、公募時期を決め、そのときに来た暗号を「安全性・実装性能評価（評価委員会）」で行う。一方で多種多様かつ変化する国際標準については、評価する必要性の有無を「いつ」「誰が」「どこで」判断するのかについて詰める必要がある。次に、評価した後で製品化・利用実績の有無を見るとあるが、安全性について評価する以上、多数の応募暗号があった場合、無償で全てを評価するのは無理がある。評価して役に立ちうるものを選択する必要がある以上、製品化・利用実績がないものは評価しないというふうに順番を変えるべきではないか。関連して、資料３－４の５頁の「新しい暗号技術の公募の考え方」にある「応募可能な暗号

技術の条件」としての「現状で広く利用されている技術であること。あるいは 2013 年時点で広く利用される見込がある技術であること」の記載と、今回の 2013 年の改定に向けて考えたときに、３頁の図はいつから実施することになるのか？最後に、CRYPTREC 推奨暗号リスト（仮称）というふうに全体をどう表すのかについて名前をつけることには賛成だが、「～リスト」が多数あって非常に紛らわしい。表記の変更を検討願いたい。

CRYPTREC 事務局：評価委員会について。公募の定期的実施と国際標準の採用では、評価委員会の検討サイクルが違ってくると思われる。現時点では具体的内容が議論しきれていないので、「評価委員会」と記載した。評価体制については今後事務局で検討したいと考えている。公募と国際標準を取り入れる場合は、それぞれで評価体制を考える必要があると思う。次に、製品化の有無を評価実施の可否判断基準とする点について。確かに効率の良い手順を選ぶ必要があり、今回は考え方を示すため複雑な書き方をした。効率の良い評価手順を選ぶ点では、松本勉構成員の御意見のとおりとするのが簡単と思う。最後に、資料３－４の図が有効になる時期は 2013 年の改訂時からで、その想定で書いている。また、リストの名称はあくまでも仮称である。御意見をいただければ、事務局で相談して提示する。

松本勉構成員：了解。このあたりの確定をいつごろとしていけばいいのか御意見を伺いたい。私は、姿は来年度中にでも公表できるような形にして、先ずは全体像を示す必要があると考えるが。

CRYPTREC 事務局：この図については、今後さらに基本的スケジュールを含めて検討を行い、来年度の早い内にパブリックコメントを行い、それを踏まえて確定させていきたいと考えている。

松本勉構成員：2009 年度に広報する時点では確定していることでよろしいか。

CRYPTREC 事務局：はい。

岩下構成員：いくつかコメントしたい。１点目として、電子政府推奨暗号リストを制定してから 10 年目に新たな形になるので、これまでの CRYPTREC の活動を総括した上で次のプロジェクトを考えるべきと思う。その際、現在のリストがどのくらい有効に使われているのか、費用対効果の面での反省に基づいて次のリストを作るべきだと思う。具体的には、現在のリスト策定時には数を絞らないというアプローチを取った。その結果として推奨した暗号の使用頻度、その評価に対する費用対効果を考えた上で、次回どうすべきかを考えるべき。もし有効に利用されている暗号が限定的であれば、最終的にリストに掲載するものは数を絞るのがいいと思うので御検討いただきたい。２点目として、資料３－４の３頁の図の中で、公募条件を決める際に外形基準をどうするのか、ポリシーとして早めに決めておく必要があるのではないかと考える。その場合、今回のリストガイドが策定されれば電子政府推奨暗号リストとリストガイドとの間でいわば「並」と「上」の形の二重構造が出来るが、それをこの図の中で想定されているのか、それとも、2013 年の時点では両者はフラットな構造になっているのか。３点目は、資料３－４の５頁の中にある「アプリケーションに依存しない、汎用的な技術を選択すること」について。確かに CRYPTREC の理念からするとその方が望ましいと思うが、一方でアプリケーションとの紐付けをリストの中で活用することの可能性を考えた方がいいのではないか。最後に、推奨暗号に危殆化が発見された場合には「互換性維持暗号リスト」に移行するとあるが、その際は ISO 等の国際標準をただしていくルートがあればいい。現状では、国際標準を使うしかなく、問題があるものを排除するという方向で何らかの仕組みが必要と考える。

CRYPTREC 事務局：まず CRYPTREC の活動を総括することは有意義と思うので、事務局でも相談していきたい。また、電子政府推奨暗号リストの数を絞ることも含めて、具体的な方針についても事務局で検討を深めたい。外形基準についてはパブリックコメントを準備する中で詰めていきたい。公募のカテゴリについては事務局の中で議論している。国際標準については、危殆化したもの、推奨候補リストに入ったものいずれについても積極的に反映させていく動きは重要と考えている。資料３－４の３頁の図で線は入れていないが意識して議論している。

太田構成員：２点確認したい。資料３－４の３頁の図の実行時期について 2013 年との発言があったが、これを 2009 年に有効としてほしい。この全体イメージは 2013 年に推奨暗号リストを提示する際のプロシージャーとして使うべき。２点目は資料３－４の５頁の最後、条件として「国

際標準化機関によって既に国際標準化されていること。あるいは、国際標準化の見込が立っていること」がある。今後公募に応じる人の意識に標準化の話しを含めるからだと思うが、これを公募の要件と課すのは厳しいのではないか。評価され推奨暗号リストに残ったものが国際標準にされやすくなるようなということがあってもいいのではないかと考える。

CRYPTREC 事務局：１点目について。公募段階から資料３－４の３頁の図の内容で動いてはという意見だが、2013 年は公募が終わって新しい電子政府推奨暗号がスタートする年であり、そのときはこの図が完成している。

太田構成員：現在電子政府推奨暗号リストに載っている暗号は、次の評価時には互換性維持暗号リストや推奨暗号候補リストに移っていることもあり得るのか？

CRYPTREC 事務局：ありえる。次に国際標準について。国際標準化という流れがある中で公募を行うわけで、現在の書き方では厳しいので、事務局の方で検討して、改めて審議をお願いしたい。

今井座長：書き方については安全性のところも含めて少し工夫するように。

松本勉構成員：暗号モジュール委員会の来年度以降の活動内容をみると、暗号モジュールについての重要性、実装までみたセキュリティは非常に重要であることは間違いないが、その中身が「国際標準規格化への貢献」だけなのか。体制が色々と整ってきたので、今後の暗号モジュール委員会の活動について、来年度は見直してよりよい体制に進むべきと考える。

暗号モジュール委員会事務局：暗号モジュール委員会を設立したときから周辺環境が変化している。今回の資料には従来通りの活動方針を記載したが、書き直さなければならないという認識はある。今後の方針として、一つは国際規格（FIPS140-3）であり、電力実験解析 WG でデータを集めて FIPS に提案していくこと。「国際標準等の標準規格を基にした日本における暗号モジュールのセキュリティ要件の原案の作成」は削除しても良いのではと考えている。この点は最終の報告書案作成までに詰めていく。

今井座長：検討していくということか？

松本勉構成員：検討して、今後の体制を盤石にするつもりである。

今井座長:さらに御意見がある場合は事務局までお寄せ頂ければと思う。いただいた御意見を尊重して、引き続き CRYPTREC 活動を推進していきたいと思う。

④　その他

資料３－２に基づき、暗号技術検討会事務局から今年度の暗号技術検討会報告書案について、これまでの議論で触れていない部分の説明があり、これまでに出た修正意見を含める形で暗号技術検討会報告書案は承認された。

（３）その他

資料３－５に基づき暗号技術検討会事務局から、３月上旬に実施した暗号技術検討会メール審議の結果について説明を行った。また、CRYPTREC のホームページのドメイン名が、「cryptrec.jp」から「cryptrec.go.jp」に変更したこと、及び来年度第１回の暗号技術検討会は５月または６月頃を予定しており、時間・場所等は後日改めて連絡するとの報告を行った。

３．閉会

今井座長より挨拶があり終了した。

以　上