２００７年度第２回暗号技術検討会　議事概要

１．日時　　平成１９年１１月２０日(火)　１６：３０～１８：００

２．場所　　経済産業省本館２階　東３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、松井充、松本勉、松本泰

オブザーバ：伊藤毅志、内藤伸悟、中井川 禎彦、塚田桂祐、相澤哲、菊田豊、田中正幸、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

暗号モジュール委員会事務局：山岸篤弘

暗号技術検討会事務局：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　田中宏、荻原直彦、川崎光博、山﨑浩史

４．配付資料

資料２－１　　２００７年度第１回暗号技術検討会議事概要（案）

資料２－２－１　暗号モジュール委員会　中間報告

資料２－２－２　電力解析実験WG　中間報告

資料２－３－１　暗号技術監視委員会　中間報告

資料２－３－２　暗号技術調査WG（リストガイド）　中間報告

資料２－３－３　リストガイド対象技術　一覧

資料２－３－４　電子政府推奨暗号リストガイド目次（案）

資料２－３－５　暗号技術調査WG（公開鍵暗号）　中間報告

資料２－４－１　暗号技術仕様の変更手順について（案）

資料２－４－２　参照先概念図

資料２－５－１　電子政府推奨暗号リストの改訂に向けた検討に関する中間報告

資料２－５－２　改訂案の概念図

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　暗号モジュール委員会　委員名簿

参考資料３　電力解析実験WG　構成員名簿

参考資料４　暗号技術監視委員会　委員名簿

参考資料５　暗号技術調査WG　委員名簿

５．議事概要

（１）開会

今井座長より開会の宣言が行われた。

（２）２００７度第１回暗号技術検討会議事概要（案）の確認

事務局より資料２－２－１の確認が行われた。

（３）暗号モジュール委員会　中間報告

資料２－２－１及び２－２－２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：今回のFIPS140-3の改訂において、特に重要なところがあれば教えて頂きたい。

暗号モジュール委員会事務局：FIPS140-3 で設定されているサイドチャネル攻撃に対するセキュリティ要件に対して、INSTACとの合同委員会にて検討を行い、セキュリティ要求条件を別紙２－２－１のとおり範囲を広げるよう提案した部分が大きな点だと思う。

松本(勉)構成員：物理的には壊さず、内部から漏れ出る情報を観測し、中の鍵を推定する攻撃（ノンインベーシブアタック）については、ＩＣチップやＩＣカード、携帯端末において侮れないものであり、以前より日本から是非内容に入れるべきであると言っていた。今回 FIPS140-3 において、FIPS140-2 では注意事項だったものが、明確に要件として新たに入ったことは評価できることであると思う。ただ、要求事項とするならもっとしっかり検討すべきであると日本から意見したが、NIST側ではサイドチャネル攻撃に対応することが難しいとの見解があり消極的であった。そのため、あまり強く言い過ぎて、全く対応しないということは避けるよう対応した。

（４）暗号技術監視委員会（リストガイドWG含む）中間報告

資料２－３－１から資料２－３－５に基づき、暗号技術監視委員会事務局から説明があった。

主な質疑については以下のとおり。

今井座長:今回ご提案頂いたリストガイドについては、いいものができるのではないかと期待している。是非頑張っていただきたい。

太田構成員：公開鍵暗号WGの構成員において、前年度までは因数分解の安全性をテーマとして扱っていたが、この度テーマ変更があったため、P.25のとおり、構成員の変更をさせて頂いた。

今井座長：構成員の変更については、この前の暗号技術監視委員会で承認されたのか。

太田構成員：そうである。

加藤構成員：リストガイド対象技術ということで、インターネットに関することも色々と出ているので、中身がまとまった時点で、可能ならば、インターネットプロバイダー協会等の業界団体に説明会や紹介をして頂ければと思う。

暗号技術監視委員会事務局：了。

今井座長：せっかくいいものができあがりそうなので、是非お願いしたい。

（５）暗号技術仕様の変更手順について

事務局より資料２－４－１、暗号技術監視委員会事務局より２－４－２に基づき説明があった。主な質疑は以下のとおり。

今井座長：JCMVP より要望書がきているので、JCMVP の技術委員長の立場から、松本委員にご意見いただきたい。

松本(勉)構成員：P.38 の暗号技術監視委員会事務局案は DSA の仕様参照先に、現在の ANSI X9.30:1 だけでなく、NIST の FIPS 186-2 を追加するというもの。これでは、政府推奨暗号リストに ANSI X9.30:1 が残るので、ANSI X9.30:1 が JCMVP に持ち込まれた場合、試験をして認証する体制をとる必要があり、結局一つのアルゴリズムに、種類の違う暗号モジュールの仕様が二つ存在することを許すことになる。そもそも、これが良くないというのが当初の JCMVP の意見である。さらに、ANSI の仕様は、FIPS の仕様よりも古く、メンテナンスもされていない状況。移行措置ということで、古いバージョンを残すということはわかるが、２つの仕様が同時に両方オーソライズされているのはおかしい。いつ一本化するのかということを合わせて、検討頂かないと困る。ECDSA については、要望もれである。

今井座長：実例を見ながら、事務局からの暗号技術の変更手順の提案についてご議論頂きたい。政府推奨暗号リストについては、当初かなり厳しいルールを決めており、容易にリストの変更をすることができないものだった。これはリスト策定の段階で、次々に仕様を変えられては困ってしまうので、きちんと一つに決めたいという意図があった。しかし、５年経ち状況は変わってきている。国際標準等の対応も求められており、柔軟に対応する必要がある。このような状況を受け、事務局側で、暗号技術仕様の変更手順について提案頂いたので、これについてご意見いただきたい。

苗村構成員：基本的に、リストに柔軟性を持たせていくことには賛成である。ただ、P.27 の中で、記述について３点ほど意見させて頂きたい。1.(2)において、「第三者による改変が行われた場合」と記述があるが、提案者側がある程度自主的に変更せざる得ない場合もあるため、「第三者」という記述は不要ではないか。同 1.(2)において、IEEE は公的機関ではないので、削除した方がいいのではないか。IEEE を入れると ANSI も入れろという話になり、ややこしいことになる。同 1.(4)の「電子政府推奨暗号の安全性に影響を与えない範囲」とあるが、これは「安全性を悪化（劣化）させない範囲」という意味だと思うので、文言を検討頂ければと思う。

暗号技術監視委員会：了。

佐々木構成員：今回の変更については問題ないと思う。ただ、古いバージョンで既に製品が存在するものや、現在開発中のものについては、いつまで仕様を認めるのか問題になると思う。事務局側では、製品の開発や市場の状況等の情報は把握しているのか。

暗号モジュール委員会事務局：DSA については、そこまで詳しい情報が出てきていないので、把握できていない。ただし、DSA は電子署名法の中で使われているが、民間の公的個人認証基盤を含めて、DSA をサポートする認証局は存在ないと認識している。そのため、DSA については、変更があっても影響はそれほどないと思っている。PSEC-KEM については、公式に製品を出しているのは１社ある。また、P.28 3.(5)にある互換性維持方策は絶対必要になってくるので、維持していかなくてはいけない。脆弱性に相当するパッチ情報の公開方法を出していかなくてはいけない。

苗村構成員：既に製品がある場合、標準に基づいて作った製品が、ある日手続きの変更により標準でなくなってしまうとなると、利害が出てくるので、気をつける必要がある。単に仕様の変更とするのか、移行期間を設け、ある時点から古いバージョンをとめるのかなど方法はいろいろとあり、検討の余地はあるかと思う。

暗号モジュール委員会事務局：ご指摘の問題点については了解した。本件については、検討させて頂きたい。

今井座長：２つの暗号モジュールを参照先とすることはできるが、ただ、松本構成委員の意見があった

とおり、それでは混乱を招く可能性もあるので、いずれは一つにした方が望ましい。ただ、しばらくは両方を参照先として、リストにいれておくこともできると思う。

苗村構成員：２つに互換性があるのならば問題はないと思う。

今井座長：互換性は必要。

松本(勉)構成員：ISO の規格になっているものの、それが間違っているものがある。ISO の規格は変更するにしても時間がかかる。現実世界では、それは一斉参照されていないが、それを参照しなくてはならないとなったときに、どう対応したら良いかという問題が出てくる。今回の事務局の変更案については、なし崩し的にどんなものでもリストに入らないようになっていて、いいと思っている。今後、どの程度の変更を許容するのか、本リストについては他の仕様に頼る部分あるのでその参照先の仕様が変わったときにリストをどう変更していくのかなど、そのつどアドホック的に考える必要もあると思うが、大方針については考えておく必要がある。

今井座長：事務局から提案頂いた変更案に示されたルールを元に、実際のポリシーについて検討する必要があるということだが。

松本(勉)構成員：具体的に言うと、アメリカでは、全部 FIPS で自律的に動いており、ISO は全く関係ない。ISO、CRYPTREC、FIPS 等それぞれ連動する規格が違うので、対応する側も時間がかかってしまう。

今井：ISO の規格がそのままリストに載るわけではなく、我々はきちんと評価をした上でリストにのることになっている。

松本(勉)構成員：現在、電子政府暗号リストでは、擬似乱数生成器は例示でしかない。ISO では ISO19790 という擬似乱数生成器の標準があり、JIS の規格のセキュリティ要求事項となっている。JCMVP が従うルールである JIS では、擬似乱数生成器については、ISO の規格しか許さないとしているので、JCMVP では擬似乱数生成器については ISO で定めたものしか参照を許されないことになる。本来なら各国の事情に合わせて承認するアルゴリズムを決めてもいいとなっているはずである。CMVP のルールでは、CMVP で擬似乱数生成器を定めればいいとなっている。JCMVP でも JCMVP で定めた擬似乱数生成器を使える形になるのが本来の姿だと個人的には思う。これに関しては、関係者がおかしいと意見をいっているが、ISO 等では、もう十分審議を尽くして定めたものだから、そう簡単にかえることはできないといわれる。ところが、その ISO にはバグがあり、そのまま実装することはできない。原因は、ISO が ANSI の古い規格に基づいていることによる。NIST では、ANSI の新しい規格に基づいているので、米国では一切問題ないが、我が国では、ISO に従わなくてはならず、それぞれの仕様が異なる等問題があり困った状態。暗号モジュールを支援する立場でいうと、うまく対処できる方針を暗号検討会で出していただければ、現場で対処しやすくなる。リストも活きてくると思う。

今井座長：時間もないので、今回の会では、変化する技術動向に対応するためにも、今回の変更手続きについては、ご承諾いただきたい。実際の対応については、個別に問題については個々に議論していかなくてはいけないと思う。

事務局：今回の手続きについては、ご承諾いただきたい。佐々木構成員よりご指摘のあった、並存期間や一本化の時期、ポリシーについては、次回の検討会までに検討させて頂きたい。

太田構成員：P.27 2（1）に、暗号技術仕様管理者とあるが、これは参照先（リンク先）の管理者のことか。そうすると CRYPTREC 事務局では管理できないということを意味しているのかと思うが、松本構成員等の事例を考えると、ある推奨技術については、事務局で管理者をおかなくてはならないこともありうる。

暗号技術監視委員会事務局：そのとおりである。ご指摘の点については、次の議題である今後の暗号リスト仕様の維持・管理の仕方で議題検討させていただきたい。

苗村構成員：ISO の規格のバグの話について、内容にもよるが、ISO はフレキシブルに対応できる。バグの指摘を文書で提出すると、国際会議とは無関係に、変更する権限がＷＧのコンビナーにあたえられている。私はその担当者でもある。ただ、多くの場合、意見が違うことがあるので、国際会議で対応する必要がでる。バグの訂正については、今の具体的な問題について合意ができれば、四月の京都会議で実施的に決めることができる。バグの訂正ならば、そんなに何ヶ月や何年も掛からない。

松本構成員：擬似乱数生成器については、技術的に安定しているバージョンに ISO のアルゴリズムのスペックを合わせるという形での修正要求を出せば、対処いただけるとのことだと思う。複数の擬似乱数生成器を許すことや、各国事情に応じて追加するということはできない。

苗村：そう。バグに限る。

今井座長：今回の変更手順についてはお認めいただけるか。

（異議なし）

今井座長：それでは、変更手順（１）～（４）については、ご承諾いただいたこととさせていただく。DSA 等について、今回決められた手順を基に、どう具体的に進めていくかは暗号技術監視委員会で議論頂くことになるがよいか。

暗号技術監視委員会：参照先については、技術的な話ではなく、制度的な問題だと思う。どのようなポリシーで決めるかという大方針は本検討会で決めていただきたい。

今井座長：DSA でいうと、事務局案では、従来の ANSI と FIPS の両方を参照先とする提案であるが、松本構成員から一本化の指摘もある。もちろん一本化した方が望ましいことは間違いないが、電子署名法の事情等により２つの参照先とする必要があるとの提案である。これら意見についてどうか。

暗号技術監視委員会事務局：SEC の場合は、リスト作成時に応募者がいたので、固持した部分がある。

今井座長：ECDH については SEC の提案があり参照先としている。もともと公募で提案していただいて採用している部分もあるので、提案者のものをいきなり外すのはなかなか難しいというのが事務局の意見だと思う。

今井座長：現実では、ECDH については日本で使われているのか。

モジュール委員会事務局：使われているものはない。

今井座長：それでは、現時点では、提案者においても問題はないのは事実だと思う。公募して決めているので、提案者を尊重することも重要だが、現実的な面を考えて、特に支障がないものは一本化するという方針でどうか。

（コメントなし）

今井座長：方針としては、特に支障がないものは一本化することにして、その他詳細については、事務局、暗号技術監視委員会で決めていただきたい。

事務局、暗号技術監視委員会事務局：了。

金子構成員：P.32 の＜お願い＞とあるが、これについてはいかがするのか。

暗号モジュール委員会事務局：２０１０年の移行については、事務局で案を作成し回答させて頂く。後ほどメールで回覧する。

太田構成員：Ｐ３８の事務案において、矢印が点線となっているが、どういう意味か。

暗号技術監視委員会事務局：追加という意味で、実線と解釈いただいて問題ない。

（６）電子政府推奨暗号リストの改訂に向けた検討に関する中間報告
事務局より資料２－５－１及び２－５－２に基づき説明を行った。主な質疑は以下のとおり。

今井座長：本件については、案の段階であり、今回は結論を出すのではないとのこと。公募をする方向で進むとのことだが、これら案についてご意見を頂きたい。

佐々木構成員：暗号リストの改訂でスキームの大きな流れはこのような感じだと思う。以前も言ったが、暗号が危殆化していくような場合は、アルゴリズムだけの問題ではない。いろいろな形で検討していかなくてはならないが、この検討が十分できているとはいえない。暗号が危殆化した場合の影響は非常に大きいと思っている。これに対する検討を少なくとも日本全体としては、早めに検討する必要があると思っている。CRYPTREC が担当するかは別として、今日暗号の施策に関係する人がここに集まっているので、全体としてどう対処するか、検討する場を作ってご検討頂きたい。次回の暗号技術検討会で、検討の状況の報告があるといいと思っている。
事務局：次回３月に第３回を予定している。本件については、事務局で一度預からせて頂いき、ポンチ絵等を出して説明していきたい。
佐々木構成員：是非お願いする。検討を CRYPTREC に閉じないで、例えばNISC も含めた対応も必要だと思う。

辻井顧問：前回の暗号技術監視委員会で、佐々木構成員より、「今の研究費ではなく、いつまでになにをやるべきかという視点で考える必要がある」との意見があり納得した。何かあったときの社会的なシミュレーションの研究をやる必要があるではないかと思う。日本全体でいろいろな部分を検証しておく必要がある。

事務局：電子署名法も担当している。来月から電子署名法のあり方の検討会を年度末にかけて計画している。現状では、電子署名法の告示で SHA１や RSA 等を規定しているが、SHA2 を今回の告示の中に含めていくことを検討する予定である。その際、その根拠を CRYPTREC で示していただけるとありがたい。
今井座長：技術的な面はもちろん CRYPTREC で出てくると思う。
事務局：電子署名法では１８事業者がおり、そこからエンドユーザーまでいくと結構な数がいるので、マイグレーションの期間が必要。そうなると移行時期の目標をアナウンスする必要もあり、直感的にはそろそろまずい時期と考えている。技術的な時期的なものを、目安として提示していただけると電子証明法においてもありがたいと思う。
今井座長：佐々木構成員の意見は、さらに電子署名法にはその他にもいろいろと問題があるので、それらを安全に移行できるようなスキームを作っていく必要があり、それを検討頂きたいということだと思う。
佐々木構成員：既にある署名、長期署名、ライセンスなど、移行の際の対応や、移行の際の公的根拠、具体的な手法をいったいどうするのかなど、現実に暗号の問題は迫ってきている。そのような問題を全体的に検討して課題明確にし、そのうち CRYPTREC として、どの部分を対応していくのかを決めたほうがよい。CRYPTREC として担う部分を明確化にし、検討の場を早く作ってもらいたいと思っている。
今井座長：同じような意見は出ているが実際には動いていないようなので、是非WG等を作って、検討いただきたい。特に RSA1024 は実際に問題となりつつある。是非検討の場を設けていただき、具体的に動いて頂きたい。

岩下構成員：そもそも CRYPTREC が政府推奨暗号リストをつくったとき、１２８ビットの共通カギ等を採用したが、これはビット数を上げると製品がないという理由があった。リストを国際標準であり市場に製品があるものという基準で選んでいくと、長期に使えるものはなかなか市場にない。そうだとすると、今市場に出回っているものをある程度だめだと言わないと、長期使えるものは出てこないと思う。ビット数については、NIST もある程度線を引いているが、日本では、調整が簡単にはできない。そのような中で、全体的なポリシーをきちんと決め、その範囲内で何をやるかということを言わないと、全体的にぐらつくリスクがある。そのへんについても、この検討会で検討することが重要である。

岡本構成員：P.44 の概念図において、候補リストに入ったものは少なくても３年間おかれると読めるが、そうなのか。３年間も候補リストに入れておくのは長すぎるのではないかと思う。

事務局：そういう意味でつくったが、本資料はあくまでたたき台として提出している。今後、期間等も含め検討していく。

金子構成員：資料２－５－２によると、５年ごとに公募して暗号リストに追加され、一旦リストに入り、製品として販売し続ければ、CRYPTREC と外国の研究者が問題を指摘しない限り、リストに残っているような印象を受ける。５年ごとの公募という形をとるならば、既にリストにのっているものについても、簡単なレポート等を出して頂きたい。

事務局：ご指摘についてはもっともであり、図として抜けていた。既にリストにあるものの評価も、継続的にチェックが必要と考えている。

今井座長：その他、ご意見あればメールで事務局に連絡頂きたい。

（７）その他

NISC 伊藤参事官より、「SHA-1 の安全性低下への政府機関における対応について」前回会合以降の暗号利用に関する取組状況について説明があった。

（８）閉会

事務局より、次回会合は平成２０年３月頃を予定しており、詳細については、別途事務局より連絡がある旨の通知があった。

以　上