# ２００７年度第１回暗号技術検討会　議事概要

１．日時　　平成１９年６月１５日(金)　１０：３０～１１：５０

２．場所　　経済産業省別館１０階１０２８共用会議室

３．出席者　今井座長、辻井顧問、岩下構成員、岡崎構成員、岡本（栄司）構成員、岡本（龍明）構成員、加藤構成員、国分構成員、松井構成員、松本（勉）構成員、松本（泰）構成員

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　　２００６年度第２回暗号技術検討会議事概要（案）
資料１－４　　CRYPTREC 運営方針（案）
資料１－５－１　２００７年度 CRYPTREC 活動計画（案）
資料１－５－２　電子政府推奨暗号リストの改訂に関する検討について（案）
資料１－６―１　２００７年度暗号技術監視委員会活動計画（案）
資料１－６－２　国際会議等の報告
資料１－７　　２００７年度暗号モジュール委員会活動計画（案）

参考資料１　政府機関における暗号利用に関する取組状況
参考資料２　暗号技術検討会　構成員・オブザーバ名簿
参考資料３　暗号技術監視委員会　委員名簿
参考資料４　暗号モジュール委員会　委員名簿
参考資料５　暗号技術検討会　２００６年度報告書
参考資料６　CRYPTREC Report 2006

５．議事概要

（１）開会

・今井座長の開会の宣言後、西川経済産業省審議官より挨拶があった。

（２）「暗号技術検討会」開催要綱について

・事務局より資料１－１について説明を行い、了承された。

（３）暗号技術検討会の公開について

・事務局より資料１－２について説明を行い、了承された。

（４）座長の選任

・構成員の互選により今井構成員が座長として選出され、今井座長から着任の挨拶があった。
・事務局から、２００６年度に引き続き２００７年度も辻井構成員に顧問を依頼する旨を提案し、了承された。

（５）２００６年度第２回暗号技術検討会議事概要について

・事務局より資料１－３について説明し、意見がある場合は後日事務局あてに連絡をいただくこととした。

（６）CRYPTREC 運営方針について

・事務局より資料１－４について説明を行い、了承された。

（７）CRYPTREC 活動計画について

・NISC 伊藤参事官より、政府機関における暗号利用に関する取組状況について、参考資料１に基づいて説明があった。

（岩下構成員）政府機関の暗号の利用状況の洗い出しには賛成だが、確認の仕方を「SHA-1 利用の有無」ではなく、「使っているハッシュ関数の種類」を聞く形にしてはどうか。具体的には SHA-1 よりも脆弱性がある MD5 がある。MD5 は電子政府推奨暗号ではないので GPKI 等では使われていないはずだが「パーツ」として使われている可能性はある。SHA-1 について聞くのであればこれを機会に、長期・短期の用途の観点も踏まえ、より脆弱性のある暗号の洗い出しをしてはどうか。

（NISC 伊藤参事官）基礎調査に、用途についても盛り込むことを検討する。

・事務局より資料１－５－１および資料１－５－２について説明を行った。

（松本勉構成員）スケジュールについて、第２回暗号技術検討会の開催は秋の予定であるが、リストの暗号の仕様等の修正など急ぎの対応を要する事項については、今年度末までに結論を出すのではなく、第２回のときには既に（対応の方向性に関する）結論が出るという形で進めてほしい。

（藤田課長補佐）具体的な問題点等を、早急に把握して検討したい。

（松本勉構成員）できれば８月末までに状況把握を終え、９月中に結論を出すぐらいにしてもらいたい。

（今井座長）難しい面もあるが、今年度この問題をかなり急いで実施する必要性は事務局も十分認識しているし、その要望もあるので、かなり早いペースでやっていただけると期待している。

（８）暗号技術監視委員会活動計画

・暗号技術監視委員会事務局より資料１－６－１及び１－６－２に基づいて説明を行い、了承された。

（９）暗号モジュール委員会活動計画

・モジュール委員会事務局より資料１－７に基づいて説明があった。

（今井座長）FIPS140-3 は、CMVP にどのように反映されているのか？

（モジュール委員会事務局）CMVP については、ドラフトの開示から約１年半で FIPS として成立している。日本もこれに追随する形になろうが、試験要件をどれだけ早期に策定できるかが鍵であり、当委員会として貢献していきたい。試験要件が確立しなければ試験ができなくなるので、早期に準備だけは進めたい。

（１０）その他

（辻井顧問）ＣＲＹＰＴＲＥＣの守備範囲ではないと思うが、統一基準（第２版）の鍵管理・電子署名関係について、個人情報保護法で過剰反応が問題となっているということで、情報が流出しても電子政府推奨暗号で暗号化された情報は漏えいとみなさないこととしてはどうかという話を以前にもこの場で申し上げたが、アメリカでは適切に暗号化された情報の流出について漏えいとみなさない州が２４ある。経済産業省が最近出したガイドラインでも「高度な暗号」を使用した場合に漏えいとはしない方向としていると思う。統一基準でも、暗号鍵の管理については認証局対策はできているが利用者

対策はできていない。暗号アルゴリズムがよくても鍵管理が不十分ではいけない。ＥＣＯＭさんで検討していると聞いたが今後どうされるのか？

（松本泰構成員）確かに運用面での鍵管理については、認証局向けはきちんと対策しているが利用者向けはまだまだである。ＥＣＯＭとしても現時点で特に鍵管理に係る取り組みは行っていない。ＣＲＹＰＴＲＥＣとして考えていくべきではないか。

（今井座長）ＣＲＹＰＴＲＥＣとして初めはアルゴリズムのみの検討であったがモジュールの対策も開始したのであり、暗号に係る検討として今後は鍵管理まで含めて考えていく必要があるかも知れない。この問題については、暗号技術監視委員会でも検討する。

（岩下構成員）懸念事項として、電子政府推奨暗号リストと ISO/SC27 等で標準化作業を行う暗号の関係がある。ISO 18033 シリーズでは、これまでは公的機関による評価を受けたものが標準とされているが、最近は、カナダ、韓国、ロシア、中国など、十分な評価を経ずに標準化提案をしてくる傾向にある。そのため、従来と比べてセキュリティリスク的にみると、ISO が（標準への採用基準の面で電子政府推奨暗号と比べて）甘いといえる。ただし、TBT 協定等を含めて、国際標準と国内ルールの違いがさまざまな問題を起こす可能性がある。今後は、利用者側で両者の関係を理解・把握する必要がある。

（今井座長）電子政府推奨暗号リストのあり方を検討する際に、このことを含めて事務局を中心に検討することになると思う。我々は評価した上で標準化しなければならないと考えるが、WTO との絡みもあり、それらを考慮することになるだろう。

（松本勉構成員）SHA-1 移行の指針について、「RSA の安全性低下についても」とある。暗号の安全性の相対的な低下への対策として、SHA-1 の危殆化は既に議論されてきているが RSA1024bit についても昨年の検討会で議論に上がり、予測では2010年に危機を迎えるおそれがあることを確認している。同時に、楕円曲線暗号もビット数が決まっているので同じ状況になるが、今回の検討対象に含まれるのか？米国 CMVP では同じ対象が 2010 年には外される動きがある。

（伊藤参事官）まずは SHA-1、RSA1024bit についてみて、それから他の暗号方式に対応していく予定である。

（松本勉構成員）国内の各セクターの考えもあるが、外国からみた視点でも併せて検討してほしい。

（伊藤参事官）世界の動きも見ながら、政府としてどうすべきかを考えていく。

（松本泰構成員）時間軸・保証レベルと鍵長（鍵の長さ）の関係について、使途で鍵長を分けるべきでは。また電子政府の調達と異なり、民間のアルゴリズムの変更は強制力が働かないので困難が予想され、ＩＴ戦略上、総合的な対策が必要では。

（伊藤参事官）まずは政府において SHA-1 の移行計画を策定し、民間ではその動きを追えればと考えている。

・事務局より、次回会合は平成１９年秋頃を予定している旨の通知があった。

・松本総務省大臣官房技術総括審議官より挨拶があったのち、閉会した。

以　上