２００６年度第２回暗号技術検討会　議事概要

１．日時　　平成１９年３月２７日(火)　１４：００～１６：００

２．場所　　経済産業省本館２階東３共用会議室

３．出席者　今井座長、辻井顧問、岩下構成員、太田構成員、岡崎構成員、
加藤構成員、金子構成員、佐々木構成員、苗村構成員、
松井構成員（代理)、松本（勉）構成員、松本（泰）構成員

４．配付資料

資料２－１　２００６年度第１回暗号技術検討会議事概要（案）
資料２－２　２００６年度暗号技術検討会報告書（案）
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

・今井座長の開会の宣言後、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）２００６年度第１回暗号技術検討会議事概要（案）の確認

・資料２－１について本検討会終了後でも修正意見がある場合は、３月２８日（水）までに、事務局あて電子メール等で連絡いただくこととした。

（３）暗号技術監視委員会活動報告

・監視委員会事務局より資料２－２（３章）に基づいて説明があった。

（構成員）Ｐ１３の図２について、１年で計算するのに、１００万個のＣＰＵが必要とのことであるが、一般人には、まだまだ大丈夫だという印象を持たれるのではないか。

（構成員）いつその計算量が利用可能になるかの情報が重要である。図３にそれが書いてある。

（構成員）全体を読めばわかるが、そこだけ読まれると、誤解されやすい。

（今井座長）図３は非常に重要なので、図２の位置にもってきてほしい。

（構成員）ＲＳＡの評価を行って頂きたいと前から申し上げてきたこともあり、今回評

価をしたとのことで大変有り難い。また、一般読者がどう思うか、いわゆるアウトリーチの観点が重要と思う。例えば、Ｐ１８の公開鍵の指数 e に関して、e=3 では不十分というように、省庁やベンダにとってわかりやすくする必要がある。
（今井座長）アウトリーチについては、来年度の課題になるかと思うが、事務局で考えていってほしい。e=3 に関する岩下構成員の意見は報告書に入れてほしい。

（構成員）公開鍵暗号ＷＧとして図３にハードウェア実装の線を入れていたが、消したのはなぜか。
（事務局）ＷＧでは、ソフトウェア評価とハードウェア評価を行ったと承知しているが、前者については、用いられるスーパーコンピュータのコストについてある程度の参考情報が示される一方、後者については、実装に関するコストの議論も行っているが、十分なデータを提供するに至っていないため両者を同列に扱うのもどうかと考え、検討会の報告書としては、図３からはハードの線を外し、評価結果の概要をＰ２１に加筆した。

（４）暗号モジュール委員会活動報告
・モジュール委員会事務局より資料２－２（４章）に基づいて説明があった。

（構成員）Ｐ３１にある「非侵襲」とは一般的な用語か。
（モジュール委員会事務局）invasive の訳である。分野によって、非破壊、非侵入、非侵襲という訳がある。報告書は INSTAC で使用している非侵入に統一したい。また、２００７年度は全体的に揃えていけるようにする。

（構成員）電子政府推奨暗号は統一基準で参照されているが、実装に関する要求条件はどのようになるのか。
（内閣官房）実装に関する要求条件も統一基準に盛り込む方向で検討しているところ。
（今井座長）実装で破られることの方が多いので、是非検討してほしい。

（構成員）電子政府推奨暗号リストに載っている暗号で、例えばＤＳＡについて言えば、抱き合わせにしている乱数の生成機構が、電子政府推奨暗号リストで参照しているものと、その後ＦＩＰＳになったものとで若干違っている。現実的には、新たに実装を行う場合、最新のものが実装されるので、電子政府推奨暗号リストと違ってきてしまい、認証の際に問題になってくる。
（今井座長）たしかに整理しなければならない状況にある。全面見直しは時間がかかる。それまでは運用でカバーが必要で、来年度はそういうことについて検討が必要。
（構成員）ＲＣ４についても気になっているところ。

（５）今後のＣＲＹＰＴＲＥＣ活動について

・事務局より資料２－２（５章）に基づいて説明があった。
（今井座長）さきほどのＤＳＡのパラメータに関する松本構成員の意見を５．４にいれてほしい。

（構成員）現場では、ハッシュ関数を使っているかどうかも知らない場合が多い。非常に多くの認証でまだＭＤ５が使われているのが実情である。暗号化すらされないで使用されている場合もある。きちんと使われているかどうか、定期的に確認していく必要がある。また、ベンダの人ときちんと議論をするとどこまで言うべきか見えてくると思う。
（構成員）ＣＲＹＰＴＲＥＣは世の中の情勢にも配慮した上で暗号を選定したはずで、そのような暗号には、全て注釈をつけている。
（構成員）　５．３と５．４の整合性について考えなくてはならない。５．３にあるようにリストの暗号の仕様は変えないとする原則に沿わない例外の扱いを考える必要がある。原則を変える必要はないが、当面緊急にやるべきものをどう扱うか考える必要がある。
（構成員）本当に活用していくという観点でいくと、リストをどのような形のものにすべきなのか、リストの発注者は誰なのかなど考えていく必要がある。ＮＩＳＣが設立された等、当初の環境と変わってきているので、体制やアクションプランについて早く 明確にすることが必要である。事務局で調整してほしい。
（構成員）ＣＲＹＰＴＲＥＣの宣伝も必要ではないか。国立大学用セキュリティポリシでは電子政府推奨暗号リスト以外に、当該大学で開発され安全性の確認された新暗号を使用することも許されている例がある。
（構成員）文科省や医療機関のシステムを所管する厚労省からもオブザーバを入れる必要がある。

（７）その他
・内閣官房より、暗号危殆化に対する体制整備について、ユーザの声を聞きながら、検討を進めていくための体制作りを行うことをセキュアジャパン２００７に明記したいとの説明があった。
・事務局より、来年度第１回会合は平成１９年５～６月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及び今井座長より挨拶があったのち、閉会した。

以　上