2008 年度第 3 回暗号技術検討会　議事概要

１．日時　平成 21 年 3 月 27 日（金）　10：00～11：10

２．場所　経済産業省本館 2 階　西 8 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、岡本 龍明、
加藤 義文、金子 敏信、国分 明男、佐々木 良一、宝木 和夫、武市 博明、苗村 憲司、
高島 克幸（松井 充代理）、松本 勉、松本 泰

オブザーバ：伊藤 毅志、高橋 浩二、松本 和人（橋本 敏代理）、平野 友貴（新井 孝雄代理）、
山西 浩仁（江原 健志代理）、荒木 美敬（菊田 豊代理）、
郡司 久（田中 正幸代理）、井上 幹邦、武田 仁己、米子 房伸（篠田 陽一代理）、
大塚 玲、亀田 繁、垣内 兵輔（岸本 博之代理）

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：

経済産業省　三角 育生、下里 圭司、花田 高広

総務省　河内 正孝、田中 宏、荻原 直彦、梶原 亮、齊藤 修啓

４．配付資料

資料３－１	２００８年度第２回暗号技術検討会議事概要（案）
資料３－２	２００８年度暗号技術検討会報告書（案）
資料３－３	暗号技術公募要項（案）に関するメール審議結果について
参考資料	暗号技術検討会　構成員・オブザーバ名簿
	暗号技術監視委員会　委員名簿
	暗号技術調査ＷＧ　委員名簿
	暗号モジュール委員会　委員名簿
	電力解析実験ＷＧ　委員名簿

５．議事概要

１．開会

今井座長から開会の宣言があり、総務省の河内総括審議官から挨拶があった。

事務局からオブザーバの追加及び交代について報告があった。

２．議事

（１）2008 年度第 2 回暗号技術検討会議事概要（案）の確認

資料 3-1 に基づいて、暗号技術検討会事務局から 2008 年度第 2 回暗号技術検討会議事概要（案）の確認が行われた。

（２）CRYPTREC シンポジウム 2009 開催報告

資料 3-2 の 3.5 節に基づいて、暗号技術監視委員会事務局から CRYPTREC シンポジウム 2009 の開催報告が行われた。

（３） 2008 年度暗号技術検討会報告書（案）について

資料 3-2 に基づいて、暗号技術検討会事務局から暗号技術検討会報告書（案）の全体構成並びに 1 章及び 2 章について説明が行われた。構成員から特段の意見、コメントはなかった。

資料 3-3 に基づいて、暗号技術検討会事務局から暗号技術公募要項（案）に関するメール審議について説明が行われた。その後の質疑応答で以下の発言があった。

宝木構成員:サイドチャネル攻撃等に対する評価は例えば米国の NIST による SHA-3 の公募でも要求されていない対応である。これを評価するということは我が国独自のアプローチであり、これはこれでよいと思う。ただ、公募要項がちょっと分かりにくい。Xilinx 社製のハードウェアは応募者が用意する必要が出てくるので、持っていない会社は予算を請求して購入することになると思うが、サイドチャネル攻撃は必須でないと書かれていると、大義名分が立ちにくいのではないかという心配がある。結局のところ、サイドチャネル攻撃に対する評価は必須ではないと書いてあるが、サイドチャネル攻撃への耐性は実装したものを出さないと審査段階でかなり不利になるものと理解すればよいのか。

監視委員会事務局：サイドチャネル攻撃に対して必須ではないと記載されているというのは、要項案 11 ページの「サイドチャネル攻撃の評価」のところに、「本公募では必須でありませんが」と書いてあるというご指摘だと思うが、これは 6.3 の自己評価書に関係するものである。サイドチャネル攻撃に対する安全性評価の詳細が決まるのが 2010 年度末であり、自己評価書を提出しなければならない 2009 年度末の時点では書けないものであることから、必須ではないとしている。評価や測定をすること等については必須となっている。実際にどのような形で評価するかという点についてはまだ検討段階である。もう一つの Xilinx 社に限定しているという点については、テストベクトル等を取るためにサンプルコード等の提出をお願いしている。動作確認を行うために、事務局で用意しているのが Xilinx 社のものという意味。サイドチャネル攻撃の評価を行うハードウェアが Xilinx 社製のものだという意味ではない。

岩下構成員：仮称を付けるか付けないかということについては私のコメントだが、回答について

は了解した。リストガイドのところには仮称がついていないので、それは正式名称だが、その他の 3 つはこれから名称の変更の可能性もありうるということで仮称を付けているということだと思う。しかしある意味で決めの問題であると思うし、紹介する際にいちいち仮称を付けろと言われるのは、引用する人たちにとっても大変だと思うので、できるだけ早い段階で仮称が取れるようにした方がよい。

今井座長：名称については、確かに皆さんにご意見を求めてもなかなかいい案が出てこない。また、色々出てきても色々問題もあるということでそう簡単にもいかないが、できればなるべく早く決めていきたい。

これでメール審議の件はお認めいただいたということで、前回の検討会の議論も踏まえて、これをもって公募要項の案を外して公募要項としたい。この公募要項でこれから公募を行うこととしたい。

① 電子政府推奨暗号リスト改訂に向けた活動について

資料 3-2 の 3 章に基づいて、暗号技術監視委員会事務局から電子政府推奨暗号リスト改訂に向けた活動についての説明が行われた。構成員から特段の意見、コメントはなかった。

② 暗号技術監視委員会　活動報告について

資料 3-2 の 4 章に基づいて、暗号技術監視委員会事務局から暗号技術監視委員会の活動報告が行われた。その後の質疑応答で以下の発言があった。

今井座長：MD5 に関しては「その他」のところに書いてあるのか。

監視委員会事務局：そのとおり。

今井座長：監視活動の方も非常に精力的にやっていただいて、報告書を見ると世界の最先端の状況が非常によく分かるものになっている。監視委員会委員にも努力していただいている。

③ 暗号モジュール委員会　活動報告について

資料 3-2 の 5 章に基づいて、暗号モジュール委員会事務局から暗号モジュール委員会の活動報告が行われた。その後の質疑応答で以下の発言があった。

今井座長：最終データの形式の統一化について、暗号モジュール委員会委員長の松本構成員から補足をお願いしたい。

松本勉構成員：サイドチャネル攻撃は装置の上で暗号アルゴリズムを動かした時に問題になるものなので、実際に暗号のチップやボードがないと測定できない。アタック側からすると、そういう装置から出てきた電力や電磁波の波形を記録した上で、それを分析して鍵を割り出すことを考える。その際、ハードウェアの部分については、例えば企業の研究所では社内で計測したデータを社外に出すことは基本的に困難。しかし、外部から計測したデータであれば、会社や大学で自分たちが持っている解析の方法で試して相互に比較することができる。あるいは外部にデータを出してよい大学などが、そのような形でデータを提供すれば色々なところで比較実験、計算機実験ができる。ボードの部分については SASEBO 等の標準的に使われる

ものを我が国で作ることができたが、次の段階としてデータの流通ができるようにしようということで検討していて、このような結果になっている。

今井座長：暗号モジュール委員会の活動は世界的にも極めてユニークで、ある意味で世界をリードする活動をしている。精力的に活動していただいたと思っている。

④ 今後の CRYPTREC 活動について

資料 3-2 の 6 章に基づいて、暗号技術検討会事務局から今後の CRYPTREC 活動について説明が行われた。その後の質疑応答で以下の発言があった。

今井座長：体制の見直しについてはこれから議論を始めるところだが、これからは、使用実績の評価など、従来までとは違う調査を行う必要がある。今の体制のままでうまくやっていけるのかという問題があり、体制の見直しを行うもの。

岩下構成員：今後の活動について、ここに書かれた案は望ましい方向なので進めていただきたいが、そもそも監視委員会の任務というのは電子政府推奨暗号リストに掲載されているものの監視であって、掲載されていないものは監視の対象ではない。ただ実際には世の中を見ると、昨年末の MD5 騒動では、こんなにたくさんの MD5 が未だに使われているということが改めてよく分かった。逆にあのようなインシデントがあったからこそ CRYPTREC の報告書に書いてもらって世間が認識するところになったが、それがなければ延々と使われていたのではないかということを心配している。MD5 は危ないから使用を止めるべきであると言われ始めたのは 10 年以上前の話であるし、2-key triple DES にしても、最初の電子政府推奨暗号リストには載っていないので、それについては CRYPTREC の責任では全くないと思うが、組み込まれているものやツールの一部に入っているものはなかなか消えていない。かつて DES を止めて Triple DES に変えようとした時には、色々な標準を見直したが、いくら見直しても、モグラ叩きのように実はここでも使っていたという例がたくさん出てきた。そういう意味ではなかなか難しいが、推奨するものとは別に、推奨しないというか、使用するべきではないものについても、こまめにきちんと言っておかないと見逃されてしまうのではないか。理論的にアタックされたというものから後になると暗号学者的には面白くないので誰も見ないけれども、むしろ実装屋にとっては暗号学的にアタックされたということよりも、例えば RC4 のように本当に破られてしまうものが出るかどうかということの方が切実な問題である。これについては、フォローがなかなかされないという問題はあると考える。ここは、おそらく CRYPTREC の電子政府推奨暗号リストのメンテナンスの責任ではないが、そこをどう考えていくかというのが先ほどの、使用実績を調べるということと重なる部分があると思うので、一緒に検討していただきたい。

今井座長：確かに CRYPTREC に対する要望というのは最近になって幅が広くなってきている。それこそ MD5 に対しても何かしらコメントを出さなければならなくなったということもあるわけで、CRYPTREC の任務は、必ずしも電子政府推奨暗号リストのメンテナンスだけということではないのかもしれない。そういったことも含めて体制の見直しが必要と考えている。

監視委員会事務局：岩下構成員の意見は貴重だと思うが、もともと CRYPTREC は、応募された暗号に対して何か言うという立場で、応募されていない暗号に対して否定するようなことは言わ

ないという精神を持っていた。とは言え、安全性を損なうという状況は無視できないため、個人的な考えでは、リストガイドで注意喚起を行うことを考えている。

辻井顧問：電子政府の問題というのは電子政府だけで閉じなくて、一般論として官民連携が非常に大事。特に CRYPTREC の場合は、CSR、社会貢献を考えて少しスコープを広げていけるといい。

今井座長：おそらく、それが我々に対する社会からのリクエストであると考える。

松本泰構成員：電子政府ガイドライン作成検討会のセキュリティ分科会の座長を辻井先生が務められているが、その中で認証の保証レベルという考え方を取り入れようとしている。電子政府の認証基盤に関して、これまでは暗号を使った最高のセキュリティを目指してきたが、それだけでは電子政府はなかなか普及せず、コストやユーザビリティ等に関する観点も求められている。こうした中、暗号の使われ方自身も、適切な使われ方とは何かという観点をもう少し追求しないと、現実の世界と乖離してしまう可能性がある。岩下構成員の言うとおり、現実の世界では MD5 が今でも数多く使われている。特に、認証局のルート証明書は MD5 や MD2 が多い。このようなことを無視して、SHA-1 から SHA-2 への移行を指示しても、署名を付すこと自体を止めるという方向に動いてしまうことも考慮される必要がある。それから電子政府の中でも、アクセスの多様化という話がある。IC カードや PC だけではなく、携帯電話や地デジなど、そういうものが使えないかという話である。SSL 証明書の業界では、今は EV 証明書というセキュリティの高い証明書への移行を促す動きがあるが、その中で、例えば RSA1024 のルート証明書や MD5 のルート証明書を止めていく動きがある。しかし、日本特有の問題だが、特に携帯では今でも 1024 ビットの RSA しか使えないから移行できないという問題がある。、また、地デジは、現時点において、RSA1024 ビットのルート証明書しか入っていないものが数多く出荷されている。この場での議論とギャップを感じるため、このようなギャップを埋める動きについては CRYPTREC でもやっていかなければならないと考える。

今井座長:そういったことも何らかの形で CRYPTREC の活動の中に入っていくこともありうるということで、検討していただきたい。

佐々木構成員：今後 CRYPTREC の活動を行う上で、特にリスト改訂を行っていく上ではかなりのお金がかかる。前回 2000 年頃にリストを作った時に比べて暗号人口はかなり減ったし、当時は自己負担でもやっていこうという動きは高かったが、状況は変わってきて、自己負担だけでやっていける時代ではなくなってきている。そういう意味で色々な予算措置が必要であるので、関係者にはお願いしたい。

今井座長：大変ありがたいご意見。その点はぜひよろしくお願いしたい。

３．閉会

経済産業省の木村審議官の代理で、三角室長から閉会の挨拶があった。

事務局から、来年度の第 1 回検討会は 6 月頃を予定している旨の連絡があり、今井座長からの閉会の宣言により会合が終了した。

以上