2008 年度第 2 回暗号技術検討会　議事概要

１．日時　平成 20 年 11 月 7 日（金）　10：00～11：30

２．場所　経済産業省別館 11 階　第 1120 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 栄司、岡本 龍明、加藤 義文、国分 明男、松井 充、松本 勉

オブザーバ：伊藤 毅志、大橋 一夫（高橋 浩二代理）、松本 和人（橋本 敏代理）、小野 吉昭（井上 知義代理）、山西 浩仁（相澤 哲代理）、荒木 敬美（菊田 豊代理）、郡司 久（田中 正幸代理）、根本 健治（山田 一彦代理）、井上 幹邦、武田 仁己、米子 房伸（篠田 陽一代理）、大塚 玲、山田 安秀、亀田 繁、岸本 博之

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　田中 宏、荻原 直彦、梶原 亮、齊藤 修啓

４．配付資料

資料 2-1　2008 年度第 1 回暗号技術検討会議事概要（案）

資料 2-2-1　暗号技術監視委員会　中間報告

資料 2-2-2　リストガイド WG　中間報告

資料 2-2-3　ID ベース暗号 WG　中間報告

資料 2-3-1　暗号モジュール委員会　中間報告

資料 2-3-2　電力解析実験 WG　中間報告

資料 2-4　「電子政府推奨暗号リストの改訂に関する骨子（案）」に対する意見募集の結果及び意見に対する考え方（案）

資料 2-5-1　電子政府推奨暗号リストの改訂のための暗号技術公募要項（案）に係る評価の考え方について

資料 2-5-2　電子政府推奨暗号リストの改訂のための暗号技術公募要項（案）

資料 2-6　暗号技術公募の周知を目的としたイベントの開催について（案）

参考資料 1　「電子政府推奨暗号リストの改訂に関する骨子（案）」に対する意見募集

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　暗号技術調査ワーキンググループ　委員名簿

参考資料 5　暗号モジュール委員会　委員名簿

参考資料 6　電力解析実験ワーキンググループ　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った。

事務局よりオブザーバが交代したことの報告があった。

（２）2008 年度第 1 回暗号技術検討会議事概要（案）の確認

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

（３）暗号技術監視委員会　中間報告について

資料 2-2-1、2-2-2 及び 2-2-3 に基づいて、暗号技術監視委員会事務局から説明が行われた。その後の質疑応答で以下の発言があった。

岡本栄司構成員：ID ベース暗号及びペアリング技術については、関連した研究の進展を考慮し、是非検討を進めてほしい。

（４）暗号モジュール委員会　中間報告について

資料 2-3-1 及び 2-3-2 に基づいて、暗号モジュール委員会事務局から説明が行われた。その後の質疑応答で以下の発言があった。

松本構成員：今年度の暗号モジュール委員会の活動は、国際標準に関係する部分及び暗号技術監視委員会との関係（リスト改訂に関連した実装評価）が主となっている。電力解析実験 WG では具体的な成果（実験データフォーマットの統一化）があり公表している。今後は、実機を有さなくてもデータ解析で貢献できる組織との連携を図りたい。これまで、セキュリティと関わっていることから、企業内のルールによりデータを公表しにくいという問題があったが、解決に向かっている。

（５）電子政府推奨暗号リストの改訂に関する骨子（案）に対する意見募集の結果等について

資料 2-4 に基づいて、暗号技術検討会事務局より説明が行われた。事務局より、資料 2-4 の内容については検討会の了解が得られ次第、今月中に報道発表する予定である旨の説明があった。

（６）「電子政府推奨暗号リストの改訂のための暗号技術公募要項（案）」について

資料 2-5-1 に基づいて暗号技術検討会事務局及び暗号技術監視委員会事務局から説明が行われた。質疑の概要は以下のとおり。

今井座長：要項案（資料 2-5-2）の説明は。

暗号技術監視委員会事務局：具体的な要項案は資料 2-5-2 になるが、その概要をまとめたものが資料 2-5-1 になり、今の説明と重複するので省略した。エンティティ認証についての技術仕様と、実装評価については修正を要する点が残っている。また、要項案 2 ページのリスト改訂概念図における（仮称）

も、公表時には名称を確定させる必要がある。これについては構成員の皆様のアイディアをいただければと思う。また、パブコメへの回答を受けて、15 ページの知的財産権項目について修正している。

岡本龍明構成員：エンティティ認証について、理想的なプリミティブを組み合わせてつかうものを想定しているようだが、ゼロ知識証明などを用いるようなものは範疇になるか？

暗号技術監視委員会事務局：そのとおり。

岡本龍明構成員：Dolev-Yao モデルのみを仮定した攻撃への耐性のみについて評価しているが、フォーマルメソッドではないやり方で安全性証明をするものを入れないというのはあり得るのか。

暗号技術監視委員会事務局：入れないわけではないが、目安として記載した。

岡本龍明構成員：あくまでも目安であり、must ではないのか。

暗号技術監視委員会事務局：must にしたい。

岡本龍明構成員：あまりこれに強制しすぎるとよくない。直接しなければならないものを排除する理由は。

暗号技術監視委員会事務局:評価手法が固まっていないところについては、排除しているところ。

太田構成員：Dolev-Yao モデルに限定するのは不自然。特に電子署名ベースで作成したエンティティ認証の場合は、このモデルは不適切のはず。

暗号技術監視委員会事務局：限定しているわけではない。目安として記載している。

太田構成員：Dolev-Yao モデルはそれ以外の安全性証明よりも安全性が高いというようなことがわかっていればいいが。

暗号技術監視委員会事務局：例えばブロック暗号においても安全性評価基準を記載しているが、記載した攻撃手法は一例に過ぎず、これ以外の評価はしないわけではない。

太田構成員：少なくとも「など」といった表記を追加すべき。

暗号技術監視委員会事務局：そのような記述にする。

太田構成員：記載方式について、理想的に安全とか仮定できないと思うが、実際にあるものを推奨するしかないと思うが、切り分けをどうするか。

暗号技術監視委員会事務局：実際に評価してみないと判断できない部分があるため、現時点では明確に定義するのは適切ではないと考えている。

太田構成員：少なくとも、理想的な部品を使えるという前提ではあるという認識でよいか。

暗号技術監視委員会事務局：御認識のとおり。

岩下構成員：公募案にあるリスト改訂概念図では、公募時の評価によって（候補リストか推奨リストかに）振り分けることになっている。今回の公募では、利用実績の有無についても同時に判断するという理解でよろしいか。

暗号技術監視委員会事務局：今回公募してくるものは、基本的に利用実績はない。しかし現リストにあるものや国際標準となっているものは利用実績があると思われるので、調査に関しては 2012 年度に実施することを考えている。

岩下構成員：ここでは、利用実績に関する部分は保留として、安全性・実装性を評価するという判断で要項案を作成されたのか。

暗号技術監視委員会事務局：現時点で議論してきたのは安全性・実装性に関する部分。製品化・利用実績・普及度合いについての判断基準についての議論は十分でないため、今回の報告では省いている。

岩下構成員：要項案では新リストを「2013 年に使用開始予定」としつつ、公募対象要件として「2012 年度末までに製品化予定」となっている。さらに、公募対象を評価結果により推奨候補リストか推奨暗号リストに振り分けるという大きな負担がある。さらに今回のパブコメ回答を踏まえながら要項案にある提出書類を見ると、利用実績、見込みを確認するのに必要な情報がないように見受けられる。現リスト記載分についても利用の見込について判断する必要があり、議論が必要になるのではないか。

暗号技術監視委員会事務局：前回 2000・2001 年も同様の議論はあったが、曖昧になってしまった。今回はその点のルールは厳格化したい。

今井座長：エンティティ認証に関する評価内容については再検討するように。

辻井顧問：具体的提案とは異なるが、電子認証が今後需要として大きくなってくると思われるので、これを背景に含めて考えていただければと思う。

太田構成員：資料 2-5-1 の最終ページにある「安全性」について。暗号プリミティブを評価する手法として「モデルチェッカ」等のツールの使用を必須とするのは、肝心のチェッカにバグがあった場合等のツールの信頼性を考慮するとハードルが高すぎるのではないか。

暗号技術監視委員会事務局：エンティティ認証については再検討して、次回の暗号技術監視委員会で御議論をお願いする予定である。

太田構成員：ただ、要項案そのものは良く出来ているので、この方向で進めていただければと思うが、さらに踏み込んで検討していただければと思う。

松本構成員：今回の改訂で「リストを活用する」としているが、応募者・評価者のみががんばるだけでは駄目である。安全性・実装性で優れているのみならず調達の容易性も必要ではないか。あと、資料 2-5-2 にもあるが、例えば「候補リスト」から「推奨暗号リスト」への移行の際に設けるハードルは簡単に認めるのかそれとも非常に優れたもののみなのか、どの程度を考えているのか。

暗号技術監視委員会事務局：現時点では高めのハードルを考えている。今後検討・議論した上で来年 2 月のワークショップで周知する予定である。

今井座長：最初の公募時に出てきた様々な問題点を考慮して、今回は新しいやり方を打ち立てている。それ自体は評価できるものの煮詰まっていない点もある。今後決定していくことになるが、ある程度の相場感は要項に示しておくべき。提出書類には、今後の利用に関するものを含めるのか。

暗号技術監視委員会事務局：事業予定表の提出を求めることが考えられるが、そうすると応募に対するハードルが高くなってしまう。さらに検討する。

この後今井座長より、今回の審議内容を反映した上で次回の暗号技術監視委員会（12 月 19 日）で検討すること、その結果について暗号技術検討会のメール審議を実施した上で確定させ、その内容を来年 2 月のイベントで公表していきたい旨の発言があり、本件に関する質疑は終了した。

（７）暗号技術公募の周知を目的としたイベントの開催について

資料 2-6 に基づいて暗号技術監視委員会事務局から説明があり、了承された。

（８）その他

暗号技術検討会事務局より、資料 2-4「電子政府推奨暗号リストの改訂に関する骨子（案）」に対する意見募集の結果及び意見に対する考え方（案）及び資料 2-5-2 電子政府推奨暗号リストの改訂のための暗号技術公募要項（案）について、追加の意見がある場合は 11/14 までに暗号技術検討会事務局まで連絡をいただきたい旨の発言があった。

（９）閉会

暗号技術検討会事務局より、次回会合については来年３月の開催を予定しており、詳細については別途連絡する旨、連絡があり、今井座長からの閉会の挨拶で終了した。

以上