

## 2012年度 第1回暗号技術検討会 議事概要

1. 日時 平成24年8月2日(木) 16:00~18:00

2. 場所 経済産業省 本館 2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)、太田 和夫、岡本 栄司、岡本 龍明、金子 敏信、国分 明男、武市 博明、近澤 武、中山 靖司、本間 尚文、松井 充、松尾 真一郎、松本 勉、島岡 政基(松本 泰代理)、持麿 裕之

オブザーバ: 三角 育生、松本 淳平(羽室 英太郎代理)、大平 利幸(栗原 利男代理)、濱島 秀夫、佐藤 真紀子(河合 芳光代理)、佐久間 明彦(三澤 康代理)、中島 誠(田中 正幸代理) 浜田 和之(代田 雅彦代理)、岩永 敏明(鈴木 晴光代理)、坂下 圭一、高橋 幸雄、寶木 和夫、笹岡 賢二郎、亀田 繁、鈴木 信

暗号方式委員会事務局: 盛合 志帆(独立行政法人情報通信研究機構(NICT))

暗号実装委員会事務局: 大熊 建司(独立行政法人情報処理推進機構(IPA))

暗号運用委員会事務局: 神田 雅透(独立行政法人情報処理推進機構(IPA))

暗号技術検討会事務局:

総務省 佐藤 文俊、山崎 良志、村上 聡、上原 哲太郎、飯田 恭弘、鮫島 清豪

経済産業省 永塚 誠一、上村 昌博、森川 淳、守山 速飛

4. 配付資料

(資料番号)

(資料名)

資料1-1	2012年度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	2011年度第2回暗号技術検討会議事概要(案)
資料1-4	次期電子政府推奨暗号選定のための評価基準案について (暗号運用委員会)
資料1-5-1	次期電子政府推奨暗号選定のための「安全性評価」判定案及び「評価B」「総合評価」に関する評価項目について(暗号方式委員会)
資料1-5-2	次期電子政府推奨暗号選定のための「実装評価」判定案及び「評価B」「総合評価」に関する評価項目について(暗号実装委員会)
資料1-6	今後の検討課題の整理について
参考資料1	電子政府推奨暗号リスト
参考資料2	2012年度 暗号技術検討会構成員・オブザーバ名簿
参考資料3	次期電子政府推奨暗号リスト策定スキーム

## 5. 議事概要

### 1 開会

事務局から開会の宣言があり、経済産業省の永塚商務情報政策局長から開会の挨拶。

参考資料1に基づき、構成員及びオブザーバの交代等の説明（寶木構成員→渡辺構成員、（内閣官房情報セキュリティセンター）木本氏→三角氏、（厚生労働省）川上氏→代田氏（警察庁）、岡本氏→羽室氏、（経済産業省）藤原氏→鈴木氏、（独立行政法人産業技術総合研究所）渡辺氏→寶木氏）。佐々木構成員及び松本（泰）構成員（島岡氏が代理出席）が欠席。

### 2 議事

#### （1）2012年度暗号技術検討会開催要綱等について

資料1-1及び資料1-2に基づき、検討会事務局から説明。質疑等なし。原案どおり了承。  
開催要綱に基づき、今井座長の選任、座長による辻井顧問の指名があった。

#### （2）2011年度第2回暗号技術検討会議事概要の確認

資料1-3に基づき検討会事務局から説明。質疑等なし。原案どおり了承。

#### （3）次期電子政府推奨暗号選定のための評価基準案について（暗号運用委員会）

資料1-4に基づき、次期電子政府推奨暗号選定のための評価基準案について、暗号運用委員会事務局から説明。

##### ○評価A及び評価Bに係る質疑応答

金子構成員：評価B中「調達コスト低減を図るハードルの低さ」の評価は、評価A中「市販製品での採用実績」の評価の内容は同一ではないか。

暗号運用委員会事務局：評価B中の「市販製品の採用実績」は8つの評価項目の一であり、その評価基準を50%と提案している。一方で、評価B中の「調達コスト低減を図るハードルの低さ」の評価基準は10%と提案しており、閾値が異なる評価である。

今井座長：現実には50%の水準を達成することは難しいことから、評価Bにおいて評価Aとは異なる評価項目が設置されていると認識している。

金子構成員：評価A中「市販製品での採用実績」と評価B中「市販製品での採用実績」の評価基準は同一か。

暗号運用委員会事務局：同一である。

金子構成員：評価B中「調達コスト低減を図るハードルの低さ」と「市販製品での採用実績」の両方の評価基準を満たすこともありえるか。

暗号運用委員会事務局：50%以上の採用実績があった場合には、両方が評価基準を満たしたものと認められる。

##### ○総合評価に係る質疑応答

今井座長：評価Aを充足してルート①を通過した暗号技術と、評価Aで不十分とされたが評価Bを通過してルート②③を通過した暗号技術を、公平にどう評価するか、という案だと認識している。

金子構成員：ルート①だと50%で加点、ルート②③だと10%で加点ということか。

暗号運用委員会事務局：総合評価に到達した暗号技術は、評価A及びBは完了しており、改めて各暗号技術の実力を判断する。例えば、「市販製品での採用実績」の満点が30点だとすると、ルート①を通過した暗号技術は満30点、ルート②③の暗号技術は採用実績に応じて20点又は10点となる。

金子構成員：異なる基準ではない、との理解で良いか。

暗号運用委員会事務局：採用実績を評価する場合には、同一の評価軸上の評価である。

金子構成員：通過するルートによって、満点が異なることに違和感がある。

暗号運用委員会事務局：ルートにかかわらず満点を同一にするためには、各評価項目の採点を二つのルートで変えて調整する必要がある。議論はあったが、説明が難しいものと思料する。

今井座長：例え話をすれば、事務局案は経験豊富な大先生と若い研究者を同一に評価して良いのか、ということだと考えている。若い人は将来性に係る60点を含めて、評価するというアイデア。各評価項目の詳細な配点については、今後検討していくことになる。

#### ○利用実績調査に係る質疑応答

金子構成員：64ビットブロック暗号のカテゴリについては、調査する必要性はあるのか。安全性に照らして、カテゴリがなくなるのではないのか。

暗号運用委員会事務局：カテゴリに関する判断がまだ示されていない以上、利用実績としては調査する。

暗号技術検討会事務局：64ビットブロック暗号のカテゴリの取扱いについては、今後検討する。

今井座長：カテゴリごとに運用監視暗号とする可能性があるかと認識している。

#### (4) 次期電子政府推奨暗号選定のための評価基準案について（暗号方式委員会・暗号実装委員会）

資料1-5-1に基づき、暗号方式委員会事務局から暗号方式委員会での検討事項について説明。  
また、資料1-5-2に基づき、暗号実装委員会から暗号実装委員会での検討事項について説明。

#### ○暗号方式委員会検討事項に係る質疑応答

今井座長：暗号方式委員会において、電子情報通信学会論文誌等の論文掲載についても評価すべきとの意見があったのではないか。

暗号方式委員会事務局：「論文誌」として、評価対象となる。

#### ○暗号実装委員会検討事項に係る質疑応答

今井座長：実装性能の比較対象の「標準的な暗号技術」とは何か。

暗号実装委員会事務局：応募者が提案し、実装委員会がその正当性を判断することとしている。

今井座長：事務局選出暗号についてはどのように措置するか。

暗号実装委員会事務局：事務局が提案することになるが、同様に実装委員会がその正当性を判断することとなる。

○評価基準全体に係る質疑応答

金子構成員：応募者や、できれば広く世の中に、今回の評価基準を公開すべきではないのか。

今井座長：今後の検討事項だと考えている。暗号運用委員会委員長の松本先生、暗号実装委員会委員長の本間先生から一言ずつ今回の評価基準案についてお伺いしたい。

松本構成員：暗号の利用実績を評価基準にするにあたって、いかに客観性・透明性のある基準とするか、暗号運用委員会において侃々諤々の議論があった。その上で、最も適切だと考える案を本検討会に提案していると自負している。

本間構成員：暗号実装委員会においても多くの議論があった。実装性能に関しては、数値で各暗号技術を比較することが難しい性質を持っている。その上で、今回の検討会へ付議する案を検討してきた。

今井座長：暗号方式委員会委員長としては、論文数の判断等、議論を要したところもあるが、しっかりまとめてきたものと認識している。

以上の質疑応答の後、今井座長から発議があり、(3)及び(4)の議題については、原案どおり了承されたものと確認された。

(5) その他

資料1-6について暗号技術検討会事務局から説明。追加課題等があれば、次回の検討会開催までの期間に、事務局宛に提出することが確認された。

3 閉会

総務省の山崎情報セキュリティ対策室長から閉会の挨拶。

検討会事務局から、第2回検討会については11月下旬頃に開催する予定を連絡。詳細な日程については、別途調整する旨が示された。

以上