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）、持麾 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、鈴田 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、山碕 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（竇木構成員→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→竇木氏）。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。

〇評価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。

〇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：例え話をするなら、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ィア。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。

〇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。

〇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。

〇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。

〇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

総務省の山碕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