２００６年度第1回暗号技術検討会
議事概要

1．日　時：平成１８年7月7日（水）１０：００～１１：４０

2．場　所：経済産業省本館2西8共用会議室

3．出席者：今井座長、岩下構成員、太田構成員、岡崎構成員、岡本(栄司)構成員、
岡本(龍明)構成員（代理）、加藤構成員、金子構成員、苗村構成員、松井構成員、
松本(勉)構成員、松本(泰)構成員

4．配付資料

資料１－１　「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　２００５年度第2回暗号技術検討会議事概要（案）
資料１－４　CRYPTREC 運営方針（案）
資料１－５　SHA-1 の安全性に関する見解
資料１－６　各国の推奨暗号・標準暗号に関する海外調査報告
資料１－７　２００６年度 CRYPTREC 活動計画（案）
資料１－８　２００６年度暗号技術監視委員会活動計画（案）
資料１－９　２００６年度暗号モジュール委員会活動計画（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
参考資料4　電子政府推奨暗号リスト上の個別暗号の危殆化に係る対策スキーム（イメージ）
参考資料5　暗号モジュール試験及び認証(JCMVP)制度の創設について
参考資料6　暗号技術検討会　２００５年度報告書
参考資料7　CRYPTREC Report 2005

5．議事概要

（1）開会と挨拶

事務局が開会を宣言した後、西川経済産業省大臣官房審議官（商務情報政策局担当）から挨拶があった。

（2）「暗号技術検討会」開催要綱について

事務局から資料１－１について説明を行い、了承された。

（3）暗号技術検討会の公開について

事務局から資料１－２について説明を行い、了承された。

（4）座長の選任

構成員の互選により今井構成員が座長として選出され、今井座長から着任の挨拶があった。
事務局から、2005年度に引き続き2006年度も辻井構成員(当日欠席)に顧問を依頼する旨を提案し、了承された。

（5）２００５年度第2回暗号技術検討会議事概要（案）の確認

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

⑹ CRYPTREC 運営方針（案）について

事務局から資料１－４について説明を行い、了承された。

⑺ SHA-1 の安全性に関する見解について

事務局から、資料１－５の審議経過等について、次のとおり説明を行った。

-昨年度のＳＨＡ－１の安全性評価に関する検討の過程で、ＣＲＹＰＴＲＥＣとしての見解を示す文書に関しては、電子政府システムを所管する政府関係者にもわかりやすい表現にすべき等の要望があった。

-この要望を踏まえ、資料１－５について、６月２８日の暗号技術監視委員会のメール審議決定を経て、６月３０日にＮＩＳＣへ説明を行った。

・構成員から、衝突発見に要する時間の目安 462 年が果たして現実的な脅威となりうるのか、SHA-1 のことを知らないユーザーの立場に立った説明は、重要であるとの意見があった。

・構成員から、CRYPTREC の活動に代表されるように、我が国の暗号技術のポテンシャルは一定のレベルに保たれている一方、暗号政策の体制整備についても、今回の SHA-1 の危殆化対策を契機として、平時から政府における安全な暗号の利用を図るべく、しっかりしたものとして欲しいとの意見があった。

・オブザーバの NISC 立石参事官から、SHA-1 の危殆化対策については、政府としてどの暗号を使っていくべきか現場で混乱が生じないように移行方法を検討すること、また、危殆化が生じていない平時から安全な暗号の利用と危殆化対策を検討するための体制づくりが必要との認識が述べられ、今後 CRYPTREC からの情報をもとに、暗号の利用形態を把握した上で、関係府省と相談しながら、必要な検討を進める旨の説明があった。

⑻ 各国の推奨暗号・標準暗号に関する調査報告

暗号技術監視委員会事務局から、資料１－６に基づき、各国の推奨暗号・標準暗号に関する海外調査報告があった。

・各構成員から、各国が独自に行っている評価の内容や、ドイツの暗号リストが引用する SAGA（規格）のドキュメント、暗号アルゴリズムを利用するドメイン環境（無線 LAN、SSL 通信等）毎の分析の必要性についての意見等があり、引き続きさらなる海外調査が必要、との指摘があった。

⑼ 活動報告等の説明

事務局から、資料１－７、資料１－８及び資料１－９に基づいて、本年度の活動計画について説明を行い、了承された。

⑽ 暗号モジュール試験及び認証制度の創設について

暗号モジュール委員会事務局から、参考資料5に基づき、暗号モジュール委員会の成果を活用してコモンクライテリア（CC）制度を拡充・補完する暗号モジュール試験及び認証制度(JCMVP 制度)の創設について説明があった。

・構成員から、JCMVP 制度で評価される暗号モジュールには、電子政府推奨暗号リスト以外に、今後業界にて策定が見込まれる標準暗号リストも利用され得ることについての発言があり、暗号モジュール委員会事務局から補足説明があった。

⑾ 閉会

・松本総務省大臣官房技術総括審議官からの挨拶の後、閉会した。

以上