2005年度第１回暗号技術検討会
議事概要

１．日　時：平成１７年１０月１２日（水）１０：００～１２：００

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、辻井顧問、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、加藤構成員、金子構成員、苗村構成員、松井構成員（代理)、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
資料１－２　暗号技術検討会の公開について
資料１－３　2004年度第３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　CRYPTREC 2005年度活動計画（案）
資料１－６　暗号技術監視委員会活動報告
資料１－７　暗号モジュール委員会活動報告
資料１－８　電子政府推奨暗号に関する調査結果

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　政府機関の情報セキュリティ対策のための統一基準
参考資料５　CRYPTRECホームページ

５．（１）開会

今井座長の開会の宣言後、岩田経済産業省大臣官房審議官（商務情報政策局担当）より挨拶があった。

（２）「暗号技術検討会」開催要項

事務局より、資料１－１に基づ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

事務局より、資料１－２に基づいて説明を行い了承された。

（４）2004年度第３回議事概要（案）

事務局より、資料１－３に基づいて前回議事概要の確認を行い了承された。

（５）運営方針（案)、活動計画（案）の説明

事務局より、下記資料に基づいて説明を行い了承された。

資料１－４　CRYPTREC運営方針（案）
資料１－４－１「暗号技術検討会」運営方針（案）
資料１－４－２「暗号技術監視委員会」運営方針（案）
資料１－５　CRYPTREC2005年度活動計画（案）

・構成員より、暗号のユーザーの立場からの意見として、現在の電子政府推奨暗号リストは暗号アルゴリズムの情報しか掲載されていないので、公開鍵との対応関係などの情報をわかりやすくしてはどうかとの意見があった。

・構成員より、アメリカは FISMA 法により、政府が FIPS に基づき製品を調達することが規定されており、日本においても、CRYPTREC の場から、暗号の調達に関する提案ができる仕組みを取り入れるべきとの意見があった。

・構成員より、電子政府推奨暗号リストには SHA-1 の使用期限やビット長と鍵の対応関係等の情報が必要との意見があった。

・経済産業省より、情報セキュリティ政策会議において策定中の「政府機関の情報セキュリティ対策のための統一基準」について紹介があり、統一基準においても CRYPTREC が位置付けられているが、政府における暗号利用の方策等を今後内閣官房と協力して検討していく旨説明があった。

・今井座長より、電子政府推奨暗号リストの見直し等について、暗号技術検討会やワーキンググループで討議すべき内容であり、各委員に対しても今後、ご協力頂く事になる旨説明があった。

（６）活動報告等の説明

事務局より、下記資料に基づいて、活動報告、中間報告等の説明を行った。

資料１－６　2005 年度暗号技術監視委員会活動報告
資料１－６－１　2005 年度暗号技術ＷＧ（署名・認証技術調査）中間報告
資料１－６－２　同ＷＧ（ハッシュ関数・暗号利用モード調査）中間報告
資料１－６－３　同ＷＧ（疑似乱数生成系調査）中間報告
資料１－６－４　MD-5 等に関する見解
資料１－６－７　国際会議等の報告
資料１－７　暗号モジュール委員会活動報告について説明

・構成員より、FIPS 140-3 の動向について、日本からのコメントも反映されて洗練されたものになってきたが、発行は当初予定よりも遅れ気味である旨説明があった。

（７）審議案件

事務局より、資料１－６－５に基づいて、電子署名法の指針の改訂に係る意見として、SHA-1 しか利用できなかったものを、SHA-256、SHA-384、SHA-512 まで拡張する内容の説明を行い了承された。

事務局より、資料１－６－６に基づいて、NIST が 3-Key Triple DES が十分な安全性を持たなくなったとして FIPS 46-3 を廃止し、SP 800-67 を発行したことにより、電子政府推奨暗号リストの注釈を修正する旨説明を行い了承された。

（８）調査結果の説明

事務局より、下記資料に基づいて、調査結果の説明を行った。

資料１－８　電子政府推奨暗号に関する調査結果
資料１－８－１　各府省の電子政府システムにおける暗号利用状況等に関する調査結果について
資料１－８－２　電子政府推奨暗号の提案元に対する電子政府推奨暗号の製品化状況に関するアンケート調査結果について

・構成員より、アンケート調査は、我が国における暗号アルゴリズムの使用状況が分かる唯一の貴重な調査であり、継続的な調査を希望する旨、意見があった。

（９）閉会

・松本総務省大臣官房技術総括審議官及び今井座長より挨拶があった後、閉会した。

以上