２００５年度第２回暗号技術検討会　議事概要

１．日時　　平成１８年3月３０日(木)　１４：００～１５：２０

２．場所　　経済産業省本館２階東３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(龍明)構成員、加藤構成員、金子構成員、国分構成員、
櫻井構成員、宝木構成員、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２－１　２００５年度第１回暗号技術検討会議事概要（案）
資料２－２　２００５年度暗号技術検討会報告書（案）
資料２－３　各国の推奨暗号・標準暗号に関する海外調査（中間報告）
資料２－４　暗号の危殆化に係るスキーム（イメージ）
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

５．議事概要

（１）開会

・今井座長の開会の宣言後、松本総務省大臣官房技術総括審議官より挨拶があった。

（２）２００５年度第１回暗号技術検討会議事概要（案）の確認

・事務局より資料２－１について確認を行い、了承された。

（３）暗号技術監視委員会活動報告

・監視委員会事務局より資料２－２（３章）及び資料２－３に基づいて説明があった。また、今井座長より、ＳＨＡ－１に関する検討について、補足説明が求められ、事務局より資料２－４に基づいて暗号危殆化に係る政府の検討状況の説明があった。
・今井座長より、近い将来ＳＨＡ－１の衝突が見つかるのは確実であるため、監視委員会で引き続き検討を行うとともに、なるべく早急に情報発信等の措置について決定すべきであるとの意見があった。

・構成員より、資料２－２の表１３にある「２６９回」との記述は「2^{69}回」であるとの指摘があり、事務局で修正を行うことになった。

（４）暗号モジュール委員会活動報告

・モジュール委員会事務局より資料２－２（４章）に基づいて説明があった。
・構成員より、３４ページのＤＥＳの失効に伴う予算措置に関する記述に関連し、暗号の危殆化によるシステムの移行にあたっては、運用者側の事情にも配慮するとともに、真の危険性等について、うまく周知をしていくことが大事であるとの意見があった。
・今井座長より、モジュール委員会は ISO や NIST の文書翻訳作業をやっているが、我が国の成果についても紹介すべきであるとの意見があり、これに対してモジュール委員会事務局より、INSTAC-8 を用いたサイドチャネルアタック攻撃の実験報告が徐々に出てきているとの回答があった。
・構成員より、３９ページの、「INSTAC-8 を用いた」は、「INSTAC-8 に準拠して作られたボードを用いた」に書き直すべきとの指摘があり、事務局で修正を行うことになった。
・構成員より、３７ページにある翻訳物の扱いについて、「非公開」とあるのを「当面非公開」とするべきであるとの意見があり、事務局で修正を行うことになった。

（５）今後のＣＲＹＰＴＲＥＣ活動について

・事務局より資料２－２（５章）及び資料２－４に基づいて説明があった。
・構成員より、ＨＰＫＩに関する会議で、厚生労働省がＣＲＹＰＴＲＥＣの存在をよく認識していなかったとの意見があり、事務局から今後もＣＲＹＰＴＲＥＣの周知に努めたいとの回答があった。
・構成員より、報告書の最初の方に、ＣＲＹＰＴＲＥＣの成果についても触れたらどうかとの意見があり、事務局で修正を行うことになった。

（６）２００５年度暗号技術検討会報告書について

・事務局より資料２－２に基づいて、２００５年度暗号技術検討会報告書（案）の構成等について説明があった。
・構成員より、ＲＳＡの安全性評価について質問があり、事務局より今年度はＳＨＡ－１の検討を優先して行ったが、ＲＳＡのセキュリティパラメータに関しては、来年度検討していくとの回答があった。
・本会合における指摘を踏まえた具体的な修正については座長一任として、２００５年度暗号技術検討会報告書（案）は承認された。

（７）その他

・事務局より、来年度第１回会合は平成１８年５月頃を予定している旨の通知があ

った。

・西川経済産業省商務情報政策局審議官及び今井座長より挨拶があったのち、閉会した。

以　上