

2010年度第2回暗号技術検討会

メール審議の結果について（報告）

平成22年度第2回暗号技術検討会については、「2010年度暗号技術検討会開催要綱」第5項の（6）の規程に基づき、緊急やむを得ない事情により、座長の下承のもと、会合に代え電子メールによる審議を平成23年3月18日から3月25日までの間に実施。

このため、同規程に基づき、ここに当該審議の結果を報告する。

1 審議事項

(1) 電子政府推奨暗号リスト掲載暗号危殆化時の対応について

【審議の対象（電子メールで配布した資料）】

資料番号	資料名等
資料2-2	「急激な安全性の低下時における CRYPTREC の対応について（案）」
資料2-4	「暗号技術検討会2010年度報告書（案）」のうち、「4. 電子政府推奨暗号リスト掲載暗号危殆化時の対応について」

(2) 暗号技術検討会2010年度報告書（案）について

ア 電子政府推奨暗号リストの改訂に向けた進捗状況

【審議の対象（電子メールで配布した資料）】

資料番号	資料名等
資料2-4	「暗号技術検討会2010年度報告書（案）」のうち、「3. 電子政府推奨暗号リストの改訂」（「3. 3. 電子政府推奨暗号リストに関する考え方」を除く。）

イ 各委員会活動報告について

【審議の対象】

資料番号	資料名等
資料2-4	「暗号技術検討会2010年度報告書（案）」のうち、

	「４．暗号方式委員会活動報告」、「５．暗号実装委員会活動報告」及び「６．暗号運用委員会活動報告」
--	--

２ 審議結果

(1) 電子政府推奨暗号リスト掲載暗号危殆化時の対応について

提出された意見の要旨	対応状況
資料 2-2 の 6 枚目のスライドにおける「今後検討が必要となる課題」の各項目の末尾の括弧内記載事項の趣旨が、その委員会で検討が必要なのか、その委員会から提示されたのか不明確。	別紙のとおり資料を修正しました。
資料 2-2 の 3 枚目のスライドにおいて、「暗号実装委員会」列の「想定検討期間」行の記載事項が誤植。	

(2) 暗号技術検討会 2010 年度報告書（案）について

特段の意見等はなかったため、原案どおり了承されたものとする。

３ 特記事項

重要であるため審議事項とされていない「次期電子政府推奨暗号リストに関する考え方」については、今暗号検討委員会において、継続審議する。

【特記事項の対象（電子メールで配布した資料）】

資料番号	資料名等
資料 2-3-1	「電子政府推奨暗号リストの在り方について」
資料 2-3-2	「電子政府推奨暗号リストの考え方の明確化に向けた論点整理」
資料 2-3-3	CRYPTREC アンケート集計結果概要(2011 年 3 月 8 日現在)
資料 2-4	「暗号技術検討会 2010 年度報告書（案）」のうち、「３． ３． 電子政府推奨暗号リストに関する考え方」