2022年度　第1回暗号技術検討会　議事概要

１．開催日時

令和５年２月27日（月）から令和５年３月８日（水）

２．開催方法

電子メールによる検討

３．出席者（敬称略）

構成員：松本勉（座長)、阿部正幸、石井義則、上原哲太郎、太田和夫、高木剛、田村裕子、近澤武、手塚悟、本間尚文、松井充、松浦幹太、松本泰、向山友也、吉田博隆、渡邊創

オブザーバー：

内閣官房内閣サイバーセキュリティセンター 内閣参事官（政府機関総合対策担当）
個人情報保護委員会事務局 参事官
警察庁 情報通信局 情報管理課 情報セキュリティ対策官
総務省 自治行政局 住民制度課長
総務省 自治行政局 住民制度課 マイナンバー制度支援室長
法務省 民事局 商事課長
外務省 大臣官房 情報通信課長
財務省 大臣官房 文書課 業務企画室長
文部科学省 大臣官房 政策課 サイバーセキュリティ・情報化推進室長
厚生労働省 大臣官房参事官（サイバーセキュリティ・情報システム管理担当）
経済産業省 産業技術環境局 国際電気標準課長
防衛省 整備計画局 情報通信課 AI・サイバーセキュリティ推進室長
国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所長
国立研究開発法人産業技術総合研究所 サイバーフィジカルセキュリティ研究センター 高機能暗号研究チーム長
独立行政法人情報処理推進機構 技術本部セキュリティセンター長
一般財団法人日本情報経済社会推進協会 デジタルトラスト評価センター 副センター長
公益財団法人金融情報システムセンター 監査安全部長

事務局：デジタル庁
総務省
経済産業省

国立研究開発法人情報通信研究機構
独立行政法人情報処理推進機構

４．議事

（１）公募提案暗号の自主取下げ要望に対する取り扱いルールの策定並びに「ECDSA、ECDH 及び SC2000」の取扱いについて【承認】
（２）CRYPTREC 暗号リストの改定について【承認】
（３）意見募集の実施方法及びその後の対応について【承認】

５．配付資料

資料１	議事次第・配付資料一覧
資料２	公募提案暗号の自主取下げ要望に対する取り扱いルールの策定並びに「ECDSA、ECDH 及び SC2000」の取扱いについて（案）【承認事項】
資料３	今次の CRYPTREC 暗号リスト改定（旧“全面改定”）に至る主な経緯
資料４－１	CRYPTREC 暗号リストの改定について（案）【承認事項】
資料４－２	CRYPTREC 暗号リスト（現行）
資料４－３	CRYPTREC 暗号リスト（改定案）
資料５	意見募集の実施方法及びその後の対応について（案）【承認事項】
参考資料１	電子政府推奨暗号リスト掲載への推薦候補案について
参考資料２	暗号アルゴリズム利用実績調査報告

６．議事概要

（１）公募提案暗号の自主取下げ要望に対する取り扱いルールの策定並びに「ECDSA、ECDH 及び SC2000」の取扱いについて【承認】
特段の質疑は無く、原案の通り承認された。

（２）CRYPTREC 暗号リストの改定について【承認】
特段の質疑は無く、原案の通り承認された。

（３）意見募集の実施方法及びその後の対応について【承認】
特段の質疑は無く、原案の通り承認された。

以上