2023 年度　第 1 回暗号技術検討会　議事概要

１．日時

令和 6 年 3 月 26 日（火）

２．場所

オンライン開催

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 長官官房 技術企画課 情報セキュリティ対策室長
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 サイバー整備課 AI・サイバーセキュリティ政策調整官
国立研究開発法人情報通信研究機構 執行役/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首席研究員
独立行政法人情報処理推進機構 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) 2023 年度暗号技術評価委員会 活動報告について【報告】
(2) 軽量暗号に関する外部評価報告書（案）及び CRYPTREC 暗号技術ガイドライン（軽量暗号）（案）について【承認】
(3) 2023 年度暗号技術活用委員会 活動報告について【報告】
(4) TLS 暗号設定ガイドライン（案）について【承認】
(5) Triple DES 等の取り扱いに係る暗号技術活用委員会からの意見について【報告】
(6) CRYPTREC 暗号リストの更新について【承認】
(7) 電子署名法特定認証業務の暗号基準の改正スケジュールについて【報告】
(8) 2024 年度暗号技術評価委員会活動計画（案）について【承認】
(9) 2024 年度暗号技術活用委員会活動計画（案）について【承認】
(10) 暗号技術検討会 2023 年度 報告書（案）について【承認】
(11) その他

５．配付資料

資料１　議事次第・配付資料一覧
資料２　暗号技術検討会 開催要綱（構成員・オブザーバ名簿）
資料３－１　2023 年度 暗号技術評価委員会 活動報告
資料３－２　監視状況報告
資料３－３　2023 年度暗号技術調査ワーキンググループ（耐量子計算機暗号）活動報告
資料３－４　軽量暗号に関する技術動向調査
（別紙１）2023 年度外部評価報告書（ASCON 実装性能評価）
（別紙２）2023 年度外部評価報告書（ASCON 標準化動向）
資料３－５　CRYPTREC 暗号技術ガイドライン（軽量暗号）の更新について
（別紙）CRYPTREC 暗号技術ガイドライン（軽量暗号）（案）
資料４－１　2023 年度 暗号技術活用委員会 活動報告
資料４－２　TLS 暗号設定ガイドライン（案）の概要
資料４－３　TLS 暗号設定ガイドライン（案）
資料４－４　Triple DES 等の取り扱いに係る暗号技術活用委員会からの意見
資料５－１　CRYPTREC 暗号リストの更新について
資料５－２　CRYPTREC 暗号リスト（案）
資料６－１　電子署名法特定認証業務の暗号基準の改正スケジュールについて
資料６－２　特定認証業務の基準の改正スケジュールについて（案）

資料７　　2024 年度暗号技術評価委員会活動計画（案）
資料８　　2024 年度暗号技術活用委員会活動計画（案）
資料９　　暗号技術検討会 2023 年度 報告書（案）

６．議事概要

６．１．開会

事務局から開会の宣言があり、総務省山内サイバーセキュリティ統括官より開会の挨拶が行われた。

６．２．議事

(1) 2023 年度暗号技術評価委員会 活動報告について【報告】
資料３－１及び資料３－２について事務局より説明が行われ、軽微な修正を行うよう指示があった。

(2) 軽量暗号に関する外部評価報告書（案）及び CRYPTREC 暗号技術ガイドライン（軽量暗号）（案）について【承認】
資料３－４について事務局より説明が行われ、吉田構成員のコメントへの対応を含めた案とすることについて承認された。主な質疑内容は以下のとおり。
吉田構成員：Ascon の標準化に関して３節の表にあるように、Ascon は認証暗号モードとハッシュモードという２つのモードがサポートされているというところが一つ特徴的だが、IETF で今、標準化が検討されているという報告があったが、こちらは認証暗号モードとハッシュモードの２つとも標準化を検討されているということでよろしいか。もしそういう情報があれば、書いていただけると非常によいかなと思う。
事務局（NICT）：承知した。記載するようにする。直接の担当ではないため、分かり次第、検討会の構成員の皆様に共有させていただく。

(3) 2023 年度暗号技術活用委員会 活動報告について【報告】
資料４－１について事務局より説明が行われ、特段の質疑はなかった。

(4) TLS 暗号設定ガイドライン（案）について【承認】
資料４－２及び資料４－３について事務局より説明が行われ、資料４－３について原案のとおり承認された。

(5) Triple DES 等の取り扱いに係る暗号技術活用委員会からの意見について【報告】
資料４－４について事務局より説明が行われ、特段の質疑はなかった。

(6) CRYPTREC 暗号リストの更新について【承認】
資料５－１及び資料５－２について事務局より説明が行われ、資料５－２について原案のとおり承認された。

(7) 電子署名法特定認証業務の暗号基準の改正スケジュールについて【報告】

資料６－１及び資料６－２について事務局より説明が行われ、特段の質疑はなかった。

(8) 2024 年度暗号技術評価委員会活動計画（案）について【承認】

資料 7 について事務局より説明が行われ、原案のとおり承認された。

(9) 2024 年度暗号技術活用委員会活動計画（案）について【承認】

資料 8 について事務局より説明が行われ、原案のとおり承認された。

(10) 暗号技術検討会 2023 年度 報告書（案）について【承認】

資料 9 について事務局より説明が行われ、軽微な修正を行うことを前提とした上で承認された。

(11) その他

特になし。

６．３．閉会

経済産業省上村サイバーセキュリティ・情報化審議官及びデジタル庁楠統括官から閉会の挨拶が行われた。

以上