

2022年度 第2回 暗号技術検討会 議事概要（案）

1. 日時

令和5年3月30日（木）9:00～11:00

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、松本泰、向山友也、吉田博隆、渡邊創

オブザーバ：

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）

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

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

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

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

4. 議事

- (1) 2022年度暗号技術評価委員会 活動報告について【報告】
- (2) CRYPTREC暗号技術ガイドライン（耐量子計算機暗号）及び CRYPTREC暗号技術ガイドライン（高機能暗号）について【承認】
- (3) 2022年度暗号技術活用委員会 活動報告について【報告】
- (4) 暗号鍵管理ガイダンスについて【承認】
- (5) 「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」（案）に対する意見募集に寄せられたご意見に対するデジタル庁、総務省及び経済産業省の考え方（暗号技術検討会事務局案）並びにCRYPTREC暗号リストの改定版（暗号技術検討会事務局案）について【承認】
- (6) 2023年度暗号技術評価委員会活動計画（案）について【承認】
- (7) 2023年度暗号技術活用委員会活動計画（案）について【承認】
- (8) 暗号技術検討会 2022年度 報告書（案）について【承認】
- (9) 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 2022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 2022年度暗号技術評価委員会 電子メールによる審議とその結果
- 資料3-4 2022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3-5 CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）
- 資料3-6 2022年度暗号技術調査ワーキンググループ（高機能暗号）活動報告
- 資料3-7 CRYPTREC 暗号技術ガイドライン（高機能暗号）
- 資料3-8 軽量暗号に関する技術動向調査報告（外部評価）
- 資料3-9 CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）及び CRYPTREC 暗号技術ガイドライン（高機能暗号）について
- 資料4-1 2022年度 暗号技術活用委員会 活動報告
- 資料4-2 暗号鍵管理ガイダンスワーキンググループ活動報告
- 資料4-3 暗号鍵管理ガイダンス概要について
- 資料4-4 暗号鍵管理ガイダンス
- 資料5-1 CRYPTREC 暗号リストの改定について
- 資料5-2 「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」（案）に対する意見募集に寄せられたご意見並びにそれらに対するデジタル庁、総務省及び経済産業省の考え方（暗号技術検討会事務局案）
- 資料5-3 CRYPTREC 暗号リスト（改定版）（暗号技術検討会事務局案）
- 資料5-4 CRYPTREC 暗号リスト（現行版）
- 資料6 2023年度暗号技術評価委員会活動計画（案）
- 資料7 2023年度暗号技術活用委員会活動計画（案）
- 資料8 暗号技術検討会 2022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、デジタル庁楠統括官及び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) 2022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について事務局より説明が行われ、特段の質疑は無かった。
- (2) CRYPTREC暗号技術ガイドライン（耐量子計算機暗号）及び CRYPTREC暗号技術ガイドライン（高機能暗号）について【承認】
資料3-5、資料3-7及び資料3-9について事務局より説明が行われ、資料3-5及び資料3-7について原案のとおり承認された。特段の質疑は無かった。
- (3) 2022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、特段の質疑は無かった。
- (4) 暗号鍵管理ガイダンスについて【承認】
資料4-3及び資料4-4について事務局より説明が行われ、資料4-4について原案のとおり承認された。特段の質疑は無かった。
- (5) 「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」（案）に対する意見募集に寄せられたご意見に対するデジタル庁、総務省及び経済産業省の考え方（暗号技術検討会事務局案）並びにCRYPTREC暗号リストの改定版（暗号技術検討会事務局案）について【承認】
資料5-1、資料5-2及び資料5-3について事務局より説明が行われ、資料5-2及び資料5-3について原案のとおり承認された。特段の質疑はなかった。
- (6) 2023年度暗号技術評価委員会活動計画（案）について【承認】
資料6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。特段の質疑はなかった。
- (7) 2023年度暗号技術活用委員会活動計画（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。特段の質疑はなかった。
- (8) 暗号技術検討会 2022年度 報告書（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、本日の結果を踏まえた軽微な修正を行うことを条件として承認された。
- (9) その他
特になし。

6. 3. 閉会

経済産業省の上村サイバーセキュリティ・情報化審議官から閉会の挨拶が行われた。

また、事務局から、暗号技術検討会 2022年度 報告書（案）の修正版及び第2回暗号技術検討会 議事概要（案）について後日送付する旨の説明が行われた。

以上