2024年度 第1回暗号技術検討会 議事概要

1. 日時

令和7年3月25日（火） 9:00～11:00

2. 場所

経済産業省本館17階第2特別会議室及びオンライン開催

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、國廣昇、高木剛、田村裕子、
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

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（代理出席）

総務省 自治行政局 マイナンバー制度支援室長（代理出席）

法務省 民事局 商事課長（代理出席）

外務省 大臣官房 情報通信課長（代理出席）

財務省 大臣官房 文書課 業務企画室長（代理出席）

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）

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

個人情報保護委員会事務局 参事官（代理出席）

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 首席研究員

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：デジタル庁デジタル社会共通機能グループ

総務省サイバーセキュリティ統括官室

経済産業省商務情報政策局サイバーセキュリティ課

暗号技術評価委員会事務局

暗号技術活用委員会事務局

4. 議事

- (1) 2024 年度暗号技術評価委員会 活動報告について【報告】
- (2) CRYPTREC 暗号リスト仕様書の参照先変更について【報告】
- (3) 耐量子計算機暗号ガイドライン／調査報告書の更新について【承認】
- (4) 「量子コンピュータが共通鍵暗号の安全性に及ぼす影響」に関する外部評価報告書（案）について【承認】
- (5) 2024 年度暗号技術活用委員会 活動報告について【報告】
- (6) 暗号鍵管理ガイダンス（Part 2）について【承認】
- (7) 耐量子計算機暗号（PQC）への対応について【承認】
- (8) 2025 年度暗号技術評価委員会活動計画（案）について【承認】
- (9) 2025 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 2024 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	2024 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	CRYPTREC 暗号リスト仕様書の参照先変更
資料 3 - 4	2024 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
（別紙）耐量子計算機暗号ガイドライン／調査報告書の更新
（別紙 1）CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）（案）
（別紙 2）2023 年度外部評価報告書（ASCON 標準化動向）
資料 3 - 5	量子コンピュータが共通鍵暗号の安全性に及ぼす影響に関する技術動向調査
（別紙）2024 年度外部評価報告書（量子コンピュータが共通鍵暗号の安全性に及ぼす影響）（案）
資料 4 - 1	2024 年度 暗号技術活用委員会 活動報告
資料 4 - 2	2024 年度暗号鍵管理ガイダンス WG 活動報告
資料 4 - 3	暗号鍵管理ガイダンス（Part 2）の概要
資料 4 - 4	暗号鍵管理ガイダンス（Part 2）
資料 5	耐量子計算機暗号（PQC）への対応について
資料 6	2025 年度暗号技術評価委員会活動計画（案）
資料 7	2025 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 2024 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、経済産業省奥家大臣官房審議官（商務情報政策局担当）及びデジタル庁楠デジタル社会共通機能グループ長より開会の挨拶が行われた。

6. 2. 議事

松本座長により以下の議事が進行し審議が行われた。

(1) 2024 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 について暗号技術評価委員会事務局より説明が行われ、特段の質疑はなかった。

(2) CRYPTREC 暗号リスト仕様書の参照先変更について【報告】

資料 3 - 3 について暗号技術評価委員会事務局より説明が行われ、特段の質疑はなかった。

(3) 耐量子計算機暗号ガイドライン／調査報告書の更新について【承認】

資料 3 - 4 について暗号技術評価委員会事務局より説明が行われ、原案のとおり承認された。

(4) 「量子コンピュータが共通鍵暗号の安全性に及ぼす影響」に関する外部評価報告書（案）について【承認】

資料 3 - 5 について暗号技術評価委員会事務局より説明が行われ、指摘事項への対応を前提とした上で承認された。指摘事項への対応については座長一任とされた。

主な質疑は以下のとおり。

（吉田構成員）資料 3 - 5（本書）P4 の表 2 において、「古典・量子攻撃モデルでの SHA2 と SHA3 に対する衝突攻撃の比較」が記載されているが、攻撃の計算量に関して何か情報等あるか。

（暗号技術評価委員会事務局）攻撃の計算量に関して具体的な数値は算出していない。

（渡邊構成員）資料 3 - 5（本書）P6 の表 4 において、計算時間や量子メモリが記載されているが、どのように読めばいいか。また、単位についてはどうなるか。

（暗号技術評価委員会事務局）著者に確認し、対応については座長一任とさせていただく。

（田村構成員）資料 3 - 5（本書）P7 の表 5 の「現在」において、「…384 ビットや 512 ビットのものを用いた方が無難であると考えられる。」と記載されているが、「無難である」との記載は読者を混乱させるため、「望ましい」等の記載に変更出来ないか。

（暗号技術評価委員会事務局）著者に確認し、対応については座長一任とさせていただく。

- (5) 2024 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 について暗号技術活用委員会事務局より説明が行われ、特段の質疑はなかった。
- (6) 暗号鍵管理ガイダンス (Part 2) について【承認】
資料 4 - 2、4 - 3 及び 4 - 4 について暗号技術活用委員会事務局より説明が行われ、原案のとおり承認された。
- (7) 耐量子計算機暗号 (PQC) への対応について【承認】
資料 5 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。
主な発言等は以下のとおり。
(松井構成員) 世の中の動きを見ているとスピード感も必要。産業界からも期待が非常に高い。CRYPTREC でできることは移行方針の検討等ではなくテクニカルな部分だが、その中でできることに取り組むべき。
(國廣構成員) FIPS203、FIPS204、FIPS205 の安全性評価・実装性能評価を先行して進めることについて賛成であり、その旨を対外的に示すことは非常に重要。
(松本構成員) 移行には相当の期間が必要。計画的な移行をどのように進めるかは CRYPTREC の範疇を超えるが、CRYPTREC としてできることについて、具体的なタイムラインの設定を検討すべき。
(高木構成員) CRYPTREC においてはこれまで候補リストから推奨リストへ引き上げる際に、当該暗号の普及実績を確認していたが、PQC については同様の対応はなじまないため、普及を待たずに推奨リストに掲載することも検討すべき。
- (8) 2025 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 について暗号技術評価委員会事務局より説明が行われ、原案のとおり承認された。
- (9) 2025 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 について暗号技術活用委員会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 2024 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、本日の議論を反映し、構成員へメール確認することとした上で承認された。
- (11) その他
特になし。

6. 3. 閉会

総務省山内サイバーセキュリティ統括官から閉会の挨拶が行われた。

以上