

2021年度 第1回 暗号技術検討会 議事概要

1. 日時

令和4年3月30日（水）14:00～16:00

2. 場所

オンライン開催

3. 出席者（敬称略）

構成員：高木剛（座長代理）、上原哲太郎、宇根正志、太田和夫、近澤武、手塚悟、本間尚文、松浦幹太、松本泰、向山友也、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）
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) 暗号技術検討会 開催要綱の改定について【報告】
- (2) 2021年度暗号技術評価委員会 活動報告について【報告】
- (3) 2021年度暗号技術活用委員会 活動報告について【報告】
- (4) 利用実績による選定基準について【承認】
- (5) 暗号強度要件に関する設定基準について【承認】
- (6) 暗号鍵設定ガイダンスについて【承認】
- (7) CRYPTREC暗号リストの改定について【承認】
- (8) 暗号技術検討会 2021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 | 2021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 | デジタル署名EdDSAの評価結果について |
| 資料 3－4 | 2021年度暗号技術調査WG（耐量子計算機暗号）活動報告 |
| 資料 3－5 | 2021年度暗号技術調査WG（高機能暗号）活動報告 |
| 資料 3－6 | 軽量暗号に関する技術動向調査について |
| 資料 3－7 | 軽量暗号ガイドライン更新方針 |
| 資料 4 | 2021年度 暗号技術活用委員会 活動報告 |
| 資料 5 | 利用実績による選定基準（案） |
| 資料 6－1 | 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準概要 |
| 資料 6－2 | 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準 |
| 資料 7－1 | 暗号鍵設定ガイダンス概要 |
| 資料 7－2 | 暗号鍵設定ガイダンスについて |
| 資料 8－1 | CRYPTREC暗号リストの改定について |
| 資料 8－2 | デジタル署名EdDSAの推奨候補暗号リストへの追加について |
| 資料 8－3 | CRYPTREC暗号リスト改訂案 |
| 資料 8－4 | CRYPTREC暗号リスト（現行） |
| 資料 9 | 暗号技術検討会 2021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、総務省の巻口サイバーセキュリティ統括官及びデジタル庁楠統括官から開会の挨拶が行われた。

6. 2. 議事

(1) 暗号技術検討会 開催要綱の改定について

資料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。

(2) 2021年度暗号技術評価委員会 活動報告について

資料3-1について事務局より説明が行われ、特段の質疑はなかった。

(3) 2021年度暗号技術活用委員会 活動報告について

資料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。

(4) 利用実績による選定基準について【承認】

資料5について事務局より説明が行われ、資料5について原案のとおり承認された。主な質疑内容は以下のとおり。

近澤構成員：クローズドなシステムで使われているアルゴリズムは利用実績の対象外とするものの電子政府システムで使われているものは例外、とのことだが、電子政府システムで使われているアルゴリズムは公開されているのか。

事務局（IPA）：一部公開されているものもあるが、内部システムはほぼ公開されていない。関係省庁から情報提供いただいて事務局で判断することを想定している。

近澤構成員：不公平が生じないように進めてほしい。

宇根構成員：今回は推奨候補暗号リストから電子政府推奨暗号リストへの格上げの議論と認識しているが、推奨候補暗号リストの掲載ルールはこれまで通りか。

事務局（IPA）：然り。推奨候補暗号リストには、委員会や事務局の推薦を受けて暗号技術検討会で評価対象にすると決定したアルゴリズムについて暗号技術評価委員会で安全性及び実装性の評価を行った上で追加する。

宇根構成員：色々な暗号が使われており、急速に普及が進むケースもあるが、リストへの掲載が間に合うのか。

事務局（IPA）：暗号技術評価委員会や暗号技術活用委員会の委員からの提案に基づき、暗号技術検討会で評価対象にすると決定し、暗号技術評価委員会で安全性及び実装性の評価を行った上でリストに載せたこともある。随時ご提案いただければ、推奨リストへの掲載に向けた評価対象として検討する。

(5) 暗号強度要件に関する設定基準について【承認】

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、資料6-2について原案のとおり承認された。主な質疑内容は以下のとおり。

高木構成員：これらの資料は公開するのか。

事務局（IPA）：資料6-2は公開する。資料6-1は政府向けの概要資料として作ったものなので、

公開するかは検討する。公開する際はVer1.0にする。

高木構成員：ビットセキュリティの鍵長などはどのように決めたのか。SP800-57などを参照しているのであれば、参照先を明示したほうがよいのではないか。

事務局（IPA）：資料6-2の2.2節とAppendixに参考情報を記載している。

高木構成員：利用期間の区分の10年区切りはどうやって決めたのか。諸外国の例だと違う切り方もあるので、経緯を記載すべきではないか。

事務局（IPA）：例えばNISTでは～2030/2031～と分かれているが、今回の区切り案は暗号技術活用委員会の合意で作成した。

高木構成員：かなり先のことも書いてあるので、ムーアの法則も踏まえて、見直せるようにしておく必要があるのでは。

事務局（IPA）：5年ごとに利用可・容認等の中身を見直す。10年の区切りは変えない。

宇根構成員：いちばん後ろが2070年とあるが、その先はどうなるのか。例えばセンシティブなデータを量子コンピュータの脅威に備えながら長期保存するニーズはあるのではないか。むしろ2040年など短期間で切り、その後はロールオーバーして新しい暗号に移行させていく、という方法もあるのではないか。

事務局（IPA）：行政文書の保存期間は無期限を除けば最長30年となっており、2070年まで書けばしばらくはカバーできるだろうという趣旨で利用期間を決定した。量子コンピュータのリスクは認識しているが、現時点ではあえて対象外としている。なお、量子コンピュータのリスクが高まった場合には移行計画の中で判断してもらう。

(6) 暗号鍵設定ガイダンスについて

資料7-1及び資料7-2について事務局より説明が行われ、資料7-2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。

(7) CRYPTREC暗号リストの改定について

資料8-1について事務局より説明が行われ、資料8-3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。

(8) 暗号技術検討会 2021年度 報告書（案）について

資料9について事務局より説明が行われ、本日の議論結果について追記することとした上で承認された。特段の質疑はなかった。

(9) その他

その他全体を通じて以下の質疑が行われた。

宇根構成員：量子コンピュータの脅威については先ほど説明があったが、鍵共有の手段として、耐量子計算機暗号の他に量子鍵配送（Quantum Key Distribution）がある。国内でも研究開発が進んでおり、量子鍵配送の装置が実用化されているほか、実証実験も行われている。量子コンピュータに耐性のある鍵共有の方式として、量子鍵配送は、耐量子計算機暗号の代替となりうる技術であると思うが、量子鍵配送の位置づけをどのように考えているか。

事務局（METI）：現時点でははっきりとは申し上げられないが、検討は必要と認識している。

6. 3. 閉会

経済産業省の江口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、次回の暗号技術検討会は別途連絡する旨の説明が行われた。

以上