CRYPTREC Report 2023

令和 6 年 3 月

独立行政法人情報処理推進機構
国立研究開発法人情報通信研究機構

「暗号技術活用委員会報告」

目次

はじめに

本報告書は、デジタル庁、総務省及び経済産業省が主催する暗号技術検討会の下に設置され、独立行政法人情報処理推進機構及び国立研究開発法人情報通信研究機構が共同で運営する暗号技術活用委員会の 2023 年度活動を報告するものである。

暗号技術活用委員会は、電子政府の安全性及び信頼性を確保し国民が安心して電子政府を利用できる環境を整備するため、暗号利用に関するセキュリティ対策の推進、暗号技術の利用促進に向けた環境整備を主に担当する委員会である。2015 年度に、暗号技術活用委員会の活動目的の軸足を、「暗号技術を主軸とした検討」から「情報システムのセキュリティ確保に寄与する暗号技術等に係る成果物の提供」に移すことに定義し直し、2016 年度から新たな目的に基づいて活動している。特に、実運用におけるセキュリティ確保の観点から、運用面でのセキュリティマネジメントに関するガイドライン群の作成に注力している。

2023 年度は、「TLS 暗号設定ガイドライン」のアップデートを行った。既発行の「TLS 暗号設定ガイドライン」は TLS を利用する際の有用な運用ガイドラインとして広く利用されているが、利用環境と技術環境の変化に伴って記載内容の見直しを行った。現在のガイドラインの策定以降に実施した、CRYPTREC 暗号リストの改定、及び「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」の策定を反映したことが特徴である。

また、安全な暗号利用のためには暗号鍵管理が重要であることを踏まえ、2021 年度から設置した暗号鍵管理ガイダンスワーキンググループにて「暗号鍵管理システム設計指針（基本編）」をより活用しやすくするためのサポート文書の作成を行っている。この目的で 2022 年度に発行した「暗号鍵管理ガイダンス Ver.1.0」にて記載を見送った部分の拡充を 2024 年度に完成させる予定であり、記載すべき内容の整理を進めた。

今年度の成果をもとに、TLS における暗号設定や暗号鍵管理などが適切に行われ、安全な暗号利用が促進されることによって、情報システムのセキュリティ確保の底上げ、暗号の普及促進・セキュリティ産業の競争力強化に繋がり、より安心・安全な情報化社会の実現に結び付くと期待している。

末筆ではあるが、本活動に様々な形でご協力下さった委員の皆様、関係者の皆様に対して深く謝意を表する次第である。

2024 年 3 月

暗号技術活用委員会 委員長　松本 勉

本報告書の利用にあたって

本報告書の想定読者は、一般的な情報セキュリティの基礎知識を有している方である。例えば、電子署名や GPKI[1]システム等、暗号関連の電子政府関連システムに関係する業務に従事している方などを想定している。しかしながら、個別テーマの調査報告等については、ある程度の暗号技術の知識を備えていることが望まれる。

本報告書は、2023 年度の暗号技術活用委員会の活動内容と成果概要を記述した。

2022 年度以前の CRYPTREC Report は、CRYPTREC 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、及び独立行政法人情報処理推進機構）が共同で運営する下記の Web サイトから参照できる。

https://www.cryptrec.go.jp/
CRYPTREC 報告書

本報告書ならびに上記 Web サイトから入手した CRYPTREC 活動に関する情報の利用に起因して生じた不利益や問題について、本委員会及び事務局は一切責任をもっていない。

本報告書に対するご意見、お問い合わせは、CRYPTREC 事務局までご連絡いただけると幸いである。

【問合せ先】 info@cryptrec.go.jp

[1] GPKI：Government Public Key Infrastructure（政府認証基盤）

委員会構成

暗号技術活用委員会（以下「活用委員会」という。）は、図 1 に示すように、デジタル庁、総務省及び経済産業省が共同で運営する暗号技術検討会の下に設置され、独立行政法人情報処理推進機構（以下「IPA」という。）と国立研究開発法人情報通信研究機構（以下「NICT」という。）が共同で運営している。

活用委員会は、電子政府の安全性及び信頼性を確保し国民が安心して電子政府を利用できる環境を整備するため、暗号利用に関するセキュリティ対策の推進、暗号技術の利用促進に向けた環境整備を主に担当する委員会である。

なお、活用委員会と連携して活動する「暗号技術評価委員会」も暗号技術検討会の下に設置され、NICT と IPA が共同で運営している。

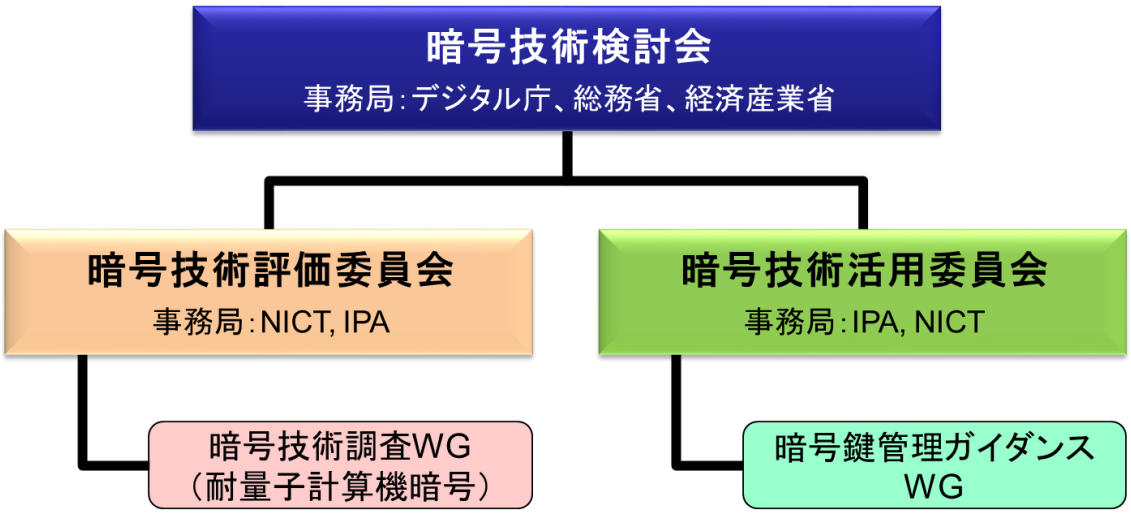

図 1　2023 年度の CRYPTREC の体制

委員名簿

暗号技術活用委員会

委員長	松本 勉	横浜国立大学 教授
委員	上原 哲太郎	立命館大学 教授
委員	垣内 由梨香	マイクロソフト株式会社 セキュリティプログラムマネージャー
委員	菊池 浩明	明治大学 教授
委員	佐藤 直之	SCSK 株式会社 シニアプロフェッショナルコンサルタント
委員	佐藤 雅史	セコム株式会社 主幹研究員
委員	須賀 祐治	株式会社インターネットイニシアティブ シニアエンジニア
委員	田村 裕子	日本銀行 企画役
委員	手塚 悟	慶應義塾大学 教授
委員	寺村 亮一	GMO サイバーセキュリティ by イエラエ 執行役員
委員	三澤 学	三菱電機株式会社 グループマネージャー
委員	満塩 尚史	デジタル庁 セキュリティアーキテクト
委員	山口 利恵	東京大学 准教授
委員	渡邊 創	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 副研究センター長

（所属：2024 年 3 月末時点）

オブザーバー

高木 浩光	内閣官房内閣サイバーセキュリティセンター
水野 邦俊	内閣官房内閣サイバーセキュリティセンター
宮崎 俊一	内閣官房内閣サイバーセキュリティセンター
高橋 元	内閣官房内閣サイバーセキュリティセンター
泉 雅巳	内閣官房内閣サイバーセキュリティセンター[2024 年 2 月から]
千葉 亮輔	デジタル庁 デジタル社会共通機能グループ
桜田 啓介	デジタル庁 デジタル社会共通機能グループ[2023 年 7 月まで]
弓 智宏	デジタル庁 デジタル社会共通機能グループ[2023 年 7 月まで]
稲見 唯睦	デジタル庁 デジタル社会共通機能グループ
武井 亮	デジタル庁 デジタル社会共通機能グループ
當波 孝明	デジタル庁 デジタル社会共通機能グループ[2023 年 7 月から]
河合 直樹	総務省 サイバーセキュリティ統括官室

荒木 友愛　　総務省 サイバーセキュリティ統括官室
重信 真也　　総務省 サイバーセキュリティ統括官室[2023 年 9 月から]
榎 聡美　　総務省 サイバーセキュリティ統括官室
澤田 知子　　経済産業省 商務情報政策局[2023 年 7 月まで]
塚本 大介　　経済産業省 商務情報政策局[2023 年 9 月まで]
味木 耕平　　経済産業省 商務情報政策局[2023 年 9 月から]
和平 悠希　　経済産業省 商務情報政策局[2023 年 7 月まで]
加藤 優一　　経済産業省 商務情報政策局[2023 年 7 月から]
木下 誠　　外務省 大臣官房 情報通信課
金井 貴洋　　外務省 大臣官房 情報通信課[2023 年 6 月から]
椛木 隆慎　　防衛省 整備計画局情報通信課
酒匂 直也　　防衛省 整備計画局情報通信課
藤本 大輔　　防衛省 整備計画局情報通信課
大矢 政基　　防衛省 整備計画局情報通信課[2024 年 2 月まで]
工藤 康男　　防衛省 整備計画局情報通信課[2024 年 2 月から]
井上 智樹　　警察大学校
黒澤 敦　　警察大学校[2023 年 6 月まで]
増田 伊智也　警察大学校[2023 年 7 月から]

事務局

独立行政法人情報処理推進機構（高柳大輔、中野美夏、神田雅透、新保淳、伊藤忠彦、松﨑博子、白岩裕子）
国立研究開発法人情報通信研究機構（盛合志帆、篠原直行、小川一人、吉田真紀、黒川貴司、金森祥子、青野良範、伊藤竜馬、大久保美也子）

第1章　2023 年度活動内容

1.1. 活動内容

活用委員会では、情報システム全般のセキュリティ確保に寄与することを目的として、暗号の取り扱いに関する観点から必要な活動を行っている。

2023 年度の活動概要は以下の通りである。

（1） 暗号鍵管理ガイダンスの拡充

暗号鍵管理ガイドラインの拡充を目的として進めていた暗号鍵管理ガイダンスについて、2021 年度・2022 年度に引き続いて暗号鍵管理ガイダンス WG を設置し、2022 年度発行版では記載を見送った部分の拡充を行う。2022 年度版の内容見直しも含め、2024 年度完成を目標とする。

（2） 暗号利活用のための新たなガイダンスの作成

2022 年度の活用委員会での議論を踏まえて、暗号利活用に向けた有用なガイダンステーマを一つ又は二つ選定し、新たなガイダンスの作成に着手する。おおむね 2 年程度での完成を想定して執筆作業を行う。

[2023 年度完成を目指すガイドライン／ガイダンス]

- TLS 暗号設定ガイドラインのアップデート

[おおむね 2024 年度完成を目指すガイドライン／ガイダンスの候補]

同種のガイドライン／ガイダンスを作成している団体／組織などとの連携（リエゾン、joint WG）も含めて体制を検討し、新たなガイドライン／ガイダンスを作成する（以下は候補例）。

- クラウドにおける鍵管理ガイダンス（例えば、日本クラウドセキュリティアライアンス（CSA））
- 暗号化消去ガイダンス（例えば、データ適正消去実行証明協議会（ADEC））
- 認証についてのガイダンス（例えば、FIDO アライアンス、OpenID ファウンデーション）

1.2. 開催状況

2023 年度に開催された暗号技術活用委員会での審議概要は表 1 のとおりである。

表 1　2023 年度暗号技術活用委員会　開催概要

回	開催日	議案
第一回	2023 年 7 月 11 日	● 2023 年度暗号技術活用委員会活動計画について ● 2023 年度暗号鍵管理ガイダンス WG 活動計画について ● TLS 暗号設定ガイドライン改訂について
メール	2024 年 1 月 12 日～ 2 月 15 日	● TLS 暗号設定ガイドライン改訂案 v3.1 のメール審議
第二回	2024 年 3 月 5 日	● TLS 暗号設定ガイドライン改訂内容について ● 2023 年度暗号鍵管理ガイダンス WG 活動報告 ● Triple DES に関する扱いについて ● 2023 年度暗号技術活用委員会活動報告案について

第2章　成果概要

2.1. TLS 暗号設定ガイドラインの改訂

【改訂の背景】

現在の「TLS 暗号設定ガイドライン（Ver3.0.1）」の公開（2020 年 7 月）以降、CRYPTREC では CRYPTREC 暗号リストの改定、及び「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（以降「強度要件設定基準」と表記）」の策定が行われた。

具体的には、CRYPTREC 暗号リストの改定により、IANA TLS registry に登録されている EdDSA と ChaCha20-Poly1305 が電子政府推奨暗号に、3-key Triple DES が運用監視暗号に、RC4 が CRYPTREC 暗号リスト外（削除）にそれぞれ位置付けられた。

また、現在の「TLS 暗号設定ガイドライン（Ver3.0.1）」の作成時点では、強度要件設定基準が発行されていなかったため、「鍵長」を用いた設定要件を行っていた。この設定要件上の一番の問題は、「鍵長 256 ビット（以上）」としている関係上、楕円曲線パラメータ「Curve25519」を使用する鍵交換方式「X25519」の採用を難しく（事実上禁止）している面である。しかし、強度要件設定基準が発行されたことにより、「X25519」も、「P-256」同様、「128 ビットセキュリティ」としての強度があると認められることとなった。このため、TLS 暗号設定ガイドラインについても、「鍵長」基準から「ビットセキュリティ」基準への変更を行うことにより、「X25519」の採用が許容できるようになり、より実用性を増すことにつながることになる。

【改訂に向けた検討項目】

上記の CRYPTREC 暗号リストの改定及び強度要件設定基準の策定に加え、3 年間の TLS に関連する IETF での動向・規格化や技術環境の変化なども踏まえて、主に以下の観点での議論を行い、必要な改訂を行うこととした。

<u>確実に改訂する項目</u>

① 設定要件について、「鍵長」基準から「ビットセキュリティ」基準に変更（チェックリストを含む）

- 「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」についての概要を追記（2.6.2「異なる暗号アルゴリズムにおける安全性の見方」の改訂）

② 2020 年 2 月以降の期間に「プロトコルバージョン」「サーバ証明書」「暗号スイート（暗号アルゴリズム）」に関連して発行された RFC の追記（2.7「SSL/TLS の利用環境の変化」の改訂）

- SSL Pulse によるデータ修正（2.7「SSL/TLS の利用環境の変化」の改訂）

③ 8.「ブラウザを利用する際に注意すべきポイント」の改訂
- サポート終了バージョンの削除
- サポート終了時期の更新
- 設定画面／設定方法の改訂（必要があれば）

<u>基準変更の要否についての検討項目</u>

a. 2.5「本ガイドラインでの暗号アルゴリズムに対する考え方」の内容
- サーバ証明書で利用する暗号アルゴリズムに対する考え方
- 暗号スイートで利用する暗号アルゴリズムに対する考え方
- DH(E)/ECDH(E)での鍵長設定についての注意

b. 3.1「実現すべき設定基準の考え方」の内容

c. 4.「推奨セキュリティ型の要求設定」の内容
- 【プロトコルバージョンの遵守項目】／【プロトコルバージョンの推奨項目】
- 【サーバ証明書の遵守項目】
- 【暗号スイートの遵守項目】／【暗号スイートの推奨項目】

d. 5.「高セキュリティ型の要求設定」の内容
- 【プロトコルバージョンの遵守項目】
- 【サーバ証明書の遵守項目】
- 【暗号スイートの遵守項目】／【暗号スイートの推奨項目】

e. 6.「セキュリティ例外型の要求設定」の内容
- 【プロトコルバージョンの遵守項目】／【プロトコルバージョンの推奨項目】
- 【サーバ証明書の遵守項目】
- 【暗号スイートの遵守項目】／【暗号スイートの推奨項目】

<u>内容の変更・改訂の必要性についての検討項目</u>

(ア) 2.2「プロトコルバージョンごとの安全性の違い」の内容
(イ) 7.「TLS を安全に使うために考慮すべきこと」の内容
(ウ) 8.3「ブラウザ利用時の注意点」の内容
(エ) 9.「その他のトピック」の内容
(オ) 2.1「TLS の概要」の内容

(カ) コラム

【コラム①】常時 HTTPS 化に伴う留意点

【コラム②】サーバ証明書の自動発行・更新プロトコル

【コラム③】サーバ証明書解析からフィッシングサイトを見つけ出せるか？

【コラム④】TLS ではフィッシングが防げない？－TLS で守られる限界を知ろう

【コラム⑤】ローカルネットワークでの HTTPS 通信問題

(キ) 「サーバ設定編」の内容

(ク) 「暗号スイートの設定例」の内容

【改訂内容】

検討を踏まえ、今回改訂した「TLS 暗号設定ガイドライン v3.1」に対する主な改訂内容を表 2 にまとめる。

表 2　TLS 暗号設定ガイドラインの主な改訂内容

<table>
<tr><th>項目</th><th>改訂内容概要</th></tr>
<tr><td>「鍵長」基準から「ビットセキュリティ」基準への変更</td><td>強度要件設定基準に従い、現行版（v3.0.1）の鍵長をそのままビットセキュリティ基準に置き換えた。また、利用する楕円曲線は、強度要件設定基準に記載のものから選択することを明記した。

<table>
<tr><th>セキュリティ強度</th><th>楕円曲線の種類</th></tr>
<tr><td>128 ビットセキュリティ</td><td>P-256, B-283, K-283, W-25519, Curve25519, Edwards25519</td></tr>
<tr><td>192 ビットセキュリティ</td><td>P-384, B-409, K-409, W-448, Curve448, Edwards448</td></tr>
<tr><td>256 ビットセキュリティ</td><td>P-521, B-571, K-571</td></tr>
</table>

また、セキュリティ例外型の DH／DHE の 1024 ビット鍵長は、対応するビットセキュリティ基準が存在しないため、鍵長表現のままとした。</td></tr>
</table>

CRYPTREC 暗号リスト改定等を踏まえた TLS での利用を推奨／禁止する暗号アルゴリズムの更新	改定された CRYPTREC 暗号リストによりリストの位置づけが変更されたアルゴリズム、及び 3 年間の TLS に関連する IETF での動向・規格化や技術環境の変化などにより変更が必要と考えるアルゴリズムについて、以下のように改訂する。 ● サーバ証明書における DSA の利用推奨を削除する ● サーバ証明書における RSA-PSS を「推奨セキュリティ型」および「高セキュリティ型」の利用推奨に追加する ● EdDSA はサーバ証明書、暗号スイートともに利用推奨をしない ● 暗号スイートでの利用禁止暗号アルゴリズムに SM2（署名）、SM3、SM4 を追加する ● なお、ChaCha20-Poly1305、3-key Triple DES、RC4 については、今回の CRYPTREC 暗号リスト改定内容を考慮した対応がすでになされているため、今回のガイドライン改訂にあたっては対応不要である
「セキュリティ例外型」の取り扱い	移行を明確に促す観点から移行期限を明記した以下の表現に強化する。 「本ガイドラインで記載されているセキュリティ例外型の設定内容は、2029 年度を目途とした改訂時に終了させる予定である。速やかに推奨セキュリティ型への移行を完了させるべきである。」
DHE の強度設定について推奨要件の改訂要否	以下のように改訂する。 ● 「高セキュリティ型」は 112 ビットセキュリティから 128 ビットセキュリティ以上に変更する ● 「推奨セキュリティ型」は変更しない（112 ビットセキュリティのまま） ● 「セキュリティ例外型」は変更しない（鍵長 1024 ビットのまま）。このようにした理由は、設定内容を変更させるよりも「推奨セキュリティ型への変更」に誘導するほうがよいうえ、このタイミングで設定内容を見直すと、設定内容を変更しさえすれば「セキュリティ例外型の継続利用」をむしろ容認したかのように誤解される恐れがあるため

暗号スイートに係るその他の要件	● CCM_8 の備考の記載について、暗号スイートの優先順位をつけるべきほどのセキュリティ上の差があるとは言い切れないものの、IETF としては CCM を推奨指定しており、CCM_8 はそうではないので、「CCM の縮退版なので、CCM が利用できるのであれば、CCM を利用することが望ましい」に修正する ● 「DHE の鍵長を明示的に設定できない製品を利用する場合には、DHE を含む暗号スイートは選定すべきではない。」では、例えば 1024 ビットであっても設定が変更できるなら許容するとも読めるので、意図を明確化するために、高セキュリティ型及び推奨セキュリティ型については、「DHE の鍵長を明示的に**適切に**設定できない製品を利用する場合には、DHE を含む暗号スイートは選定**してはならない**。」に修正する
その他	その他の主な改訂内容として以下のものがある。 ● 「Certificate Transparency」に関する節の追加 ● 「ブラウザを利用する際に注意すべきポイント」について、Microsoft、Google、Mozilla、Apple の各ブラウザの最新情報を反映 なお、IoT の普及という観点から組み込み系に向けた補足ドキュメントを検討してはどうかとの意見があったが、本ガイドラインの主たる読者層とは対象が異なると想定されることから、今後の新規ガイドラインの作成や拡充の候補として検討することになった。

2.2. 暗号鍵管理ガイダンスの拡充

2022 年度に完成させた「暗号鍵管理ガイダンス Ver.1.0」の追補との位置づけとして、2023 年度は、「暗号鍵管理システム設計指針（基本編）」に記載された項目でありながら記載を見送った部分について章・節ごとに記載予定の概要について審議した。特に、「暗号鍵管理システム（CKMS）の設計原理と運用ポリシー」及び「暗号鍵管理デバイスへのセキュリティ対策」の 2 つの章について記載すべき事項をダイジェスト形式で整理した。

暗号鍵管理ガイダンスの位置づけと想定読者

暗号鍵管理ガイダンスの位置づけ及び想定読者は次のとおりである。これらは同ガイダンス Ver.1.0 と同じである。

ガイダンスの位置づけ

- 暗号鍵管理機能を持つシステム設計者向けのガイダンスを作成する。このガイダンス

は 2020 年に発行した「暗号鍵管理システム設計指針（基本編）」に記載された各検討項目（Framework Requirement：以降 FR）をより詳細に解説した副読本である

- 「暗号鍵管理システム設計指針（基本編）」に記載された各検討項目の解釈に役立つ、検討項目の背景や補足事項、実システムでの設計において検討項目に基づいた要求事項を含めるかどうかの判断材料などについて解説する
- 暗号鍵管理システムのシンプルなモデル（トイモデル）を例示し、トイモデルにおける各検討項目への対応例を説明することで、各検討項目の内容や思想の理解を促進する

想定読者

- 暗号鍵管理機能を持つシステムの設計者

暗号鍵管理ガイダンス拡充部分の章構成

今回作成中の暗号鍵管理ガイダンス拡充部分は、「暗号鍵管理システム設計指針（基本編）」の章構成に対応して表 3 のとおりである。なお、下表はガイダンス拡充分を別冊とした場合の章構成であり、2022 年度発行済のガイダンス Ver.1.0 にマージするか別冊とするかは 2024 年度の執筆状況を踏まえて決定する。

表 3　暗号鍵管理ガイダンスの章構成

暗号鍵管理システム設計指針（基本編）	暗号鍵管理ガイダンス Ver.1.0（2022 年度発行）	暗号鍵管理ガイダンス拡充分（別冊時）
1. はじめに	1. はじめに	1. はじめに
2. 暗号鍵管理の在り方	（1 章に集約）	（1 章に集約）
3. 本設計指針の活用方法	（1 章に集約）	（1 章に集約）
4. 暗号鍵管理システム（CKMS）の設計原理と運用ポリシー		2. 暗号鍵管理システム（CKMS）の設計原理と運用ポリシー
5. 暗号アルゴリズム運用のための暗号鍵管理オペレーション対策	2. 暗号アルゴリズム運用のための暗号鍵管理オペレーション対策	
6. 暗号アルゴリズムの選択	3. 暗号アルゴリズムの選択	
7. 暗号アルゴリズム運用に必要な鍵情報の管理	4. 暗号アルゴリズム運用に必要な鍵情報の管理	
8. 暗号鍵管理デバイスへのセキュリティ対策		3. 暗号鍵管理デバイスへのセキュリティ対策

9. 暗号鍵管理システム（CKMS）のオペレーション対策		4. 暗号鍵管理システム（CKMS）のオペレーション対策

2023 年度は、「暗号鍵管理システムの設計原理と運用ポリシー」及び「暗号鍵管理デバイスへのセキュリティ対策」について、記載すべき内容をダイジェスト形式で整理した。整理した主な概要は以下のとおりである。

議論の詳細については、【別紙】暗号鍵管理ガイダンス WG 活動報告を参照されたい。

① トイモデル

暗号鍵管理システムのシンプルなモデル（トイモデル）を例示し、それに対する各検討項目への対応例を説明するためのモデルとして、「暗号鍵管理システムの設計原理と運用ポリシー」及び「暗号鍵管理デバイスへのセキュリティ対策」の節に記載するトイモデルを、IoT 製品向けのプライベート CA システム（図 2）とすることに決定した。

トイモデルで扱う「プライベート CA システム」の構成

- CKMS の範囲を CA サーバと HSM までとする
- プライベート CA システムは IoT 製品（家電想定）向けに公開鍵証明書の発行及び証明書の失効管理に使われる CRL の発行を行う
- 証明書のトラストアンカーはプライベート CA である
- IoT 製品向けの ID 管理、プライベート鍵生成、発行された証明書の機器埋め込みは工場内で行う
- IoT 製品は運用時にネット接続され、スマホ内専用アプリから IoT 製品ハブ経由でセンシングや制御が行われる。証明書は専用アプリと IoT 機器の接続（TLS での認証と秘匿通信確立）に利用される

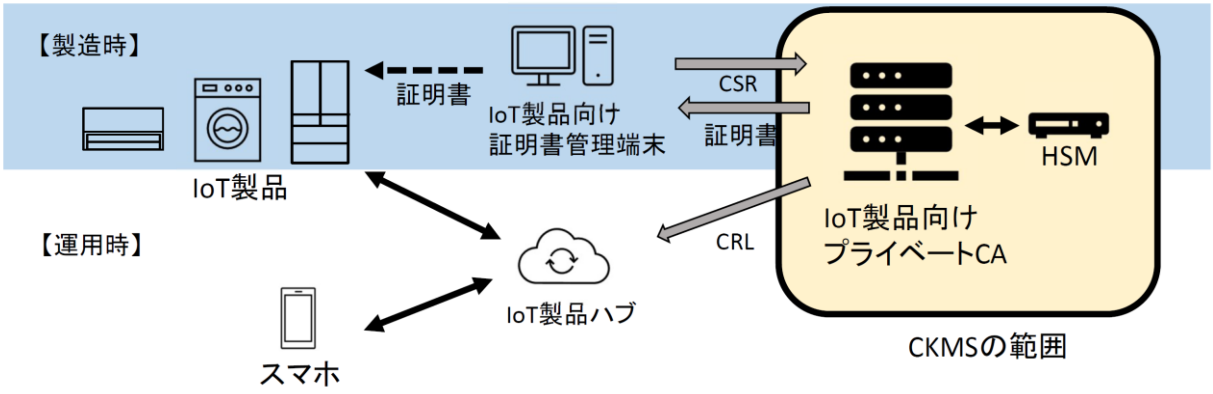

図 2　トイモデルで扱う「プライベート CA システム」の構成図

② 「暗号鍵管理システムの設計原理と運用ポリシー」に記載する「解説・考慮点」の主な概要（表 4）

表 4 「暗号鍵管理システムの設計原理と運用ポリシー」での「解説・考慮点」の主な概要

節番号	FR 番号	「解説・考慮点」の説明概要
4.1 節 CKMS セキュリティポリシー	A.01-A.05	セキュリティポリシーとは CKMS が実現するセキュリティ機能や運用方針の概要を定めたものである。CKMS を利用するシステムや CKMS が構築される IT 環境のポリシーなどと矛盾がないことが前提である。
4.2 節 情報管理ポリシー等からの要求事項	A.06	個人の説明責任が求められるケース（監査、リスクマネジメントの観点）を想定して CKMS でのサポートメカニズムを記載する
	A.07-A.13	匿名性、連結不可能性、観測不可能性のサポート有無とサポートする場合のメカニズムを記載する。一般に、匿名性、連結不可能性、観測不可能性を要求するのは特殊なケースである。
4.3 節 ドメインのセキュリティポリシー	A.14-A.19	異なるセキュリティドメイン間での鍵情報の交換がなければ対象外である。GPKI は異なるセキュリティドメイン間での鍵交換の事例である。
	A.22-A.26	マルチレベルのセキュリティドメインでの鍵情報の交換がなければ対象外である。一般に、マルチレベルのセキュリティドメインでの鍵情報の交換は特殊なケースである。
4.4 節 CKMS における役割と責任	A.27-A.28	CKMS の運用に関わるエンティティを定め、エンティティに割り当てる役割と実行できる鍵情報の管理機能へのアクセス権（権限）を定義する
	A.29-A.31	不必要な権限の割り当てや権限の分離が不十分な場合、内部犯行を誘発するリスクがある
4.5 節 CKMS の構築環境及び実現目標	A.32	CKMS を構成する主要なデバイスおよびコンポーネントの一式を定める
	A.33-A.36	CKMS が要求する時刻の精度や利用する権威時刻ソース、第三者タイムスタンプの要求有無を定める
	A.39-A.42	初期及び将来を想定してユーザ数や CKMS 性能面の目標、負荷増大時の対応策を定める
	A.43-A.46	CKMS 内デバイスや CKMS 間の相互運用を可能とするため、インタフェース、プロトコル、コマンド仕様を定める
	A.47-A.50	使いやすいユーザインタフェースを検討し、ヒューマンエラーを防止する

	A.51-A.53	どのような商用既製品を利用してどのようなセキュリティ機能を実行するかを定める
4.6 節 標準／規制に対する適合性	A.54-A.55	暗号アルゴリズム、暗号モジュール、セキュリティ認証などの標準への準拠性を明確にする
	A.57	CKMS が使用される国家・地域の法的規制を明確にする。欧州のサイバーセキュリティ法、中国のデータセキュリティ法、各国のデータ規制などが関係する。
4.7 節 将来的な移行対策の必要性	A.58-A.61	CKMS は暗号アルゴリズムのセキュリティライフタイムを超えたサービス提供や、危殆化により、暗号アルゴリズムの置き換えが必要になる。そのため、複数の暗号アルゴリズムや異なる鍵長をサポートするケースも多い。
	A.62-A.69	技術の進歩をウォッチすると共に、予め潜在的な脅威に対する影響評価の実施を推奨する

③ 「暗号鍵管理デバイスへのセキュリティ対策」に記載する「解説・考慮点」の主な概要（表 5）

表 5 「暗号鍵管理デバイスへのセキュリティ対策」での「解説・考慮点」の主な概要

節番号	FR 番号	「解説・考慮点」の説明概要
8.1 節 鍵情報へのアクセスコントロール	E.01-E.04	暗号モジュールの各機能の実行を認可されたエンティティに限定する。実行権を管理するアクセスコントロールシステム（ACS）は暗号モジュールと連動して動作する
	E.05	ACS によるエンティティ識別、認証、認可の粒度や機能を明確にする
	E.07-E.20	暗号モジュールとは、暗号境界内で暗号処理を実行するハードウェアもしくはソフトウェアの集合である。暗号境界内で利用される暗号鍵の保護機能を有する
	E.08-E.14	暗号モジュールへの鍵情報の入出力を平文形式で行うことは望ましくない。出力は暗号化して行うことが望ましく、主に外部での保管（バックアップなど）目的である
	E.21	鍵情報の入力を人間が行う場合、その正確さとセキュリティ面の問題がある。こうした入力がない場合は対象外である

	E.22-E.25	マルチパーティコントロールを利用する機能を明確にする。暗号鍵分割（K out of N 秘密分散）やマルチパーティ機能をベンダに確認する
8.2 節 セキュリティ評価･試験	E.26-E.34	いずれもシステムレベルの試験項目であるが、特に暗号モジュール（HSM など）にも関連するものはベンダテスト、機能テスト、セキュリティテスト、環境テスト、セルフチェックテスト、第三者テストである
	E.26-E.34	FIPS140 などの認証試験で上記テストをカバーするものが多い
8.3 節 暗号モジュールの障害時の BCP 対策	E.35	暗号モジュールはセルフテスト機能を備えることが望ましい。FIPS140-2/-3 の要件に動作前や条件付きのセルフテスト機能がある
	E.37	回復可能なエラー発生時のセルフテストを含む回復の手順、回復困難なエラー発生時の暗号モジュールの交換手順（鍵情報のバックアップや破壊を含む）を明確にする

2.3. Triple DES 等の取り扱いについて

NIST が Triple DES を規定していた SP 800-67 Revision 2 を 2023 年 12 月 31 日に（予定通り）廃止したことに伴い、暗号技術検討会事務局からの Triple DES の取り扱いについての意見聴取の依頼に対し、暗号技術活用委員会としては検討の結果、以下のように回答した。

【Triple DES の扱いに対する意見】

- 現時点では、「運用監視暗号リスト」からの削除を検討する必要性はない
- 現時点では、「運用監視暗号リスト」の条件である「互換性維持以外の目的での利用は推奨しない。」が実質的かつ十分な制約になっており、特段の利用制限を付加する必要性もない
- 「SP 800-67 Revision 2 が 2023 年 12 月に廃止されたが、それ以外は、運用監視暗号リストに移行した時点での状況とほとんど変わっていないため、Triple DES の位置づけに変更はない。」との注釈を付記する

【上記意見に至った理由】

① 廃止理由が、安全性が著しく低下したわけではなく、NIST のスケジュールに基づく動きであること

② 利用実績調査結果からは依然として極めて高い実装率であること

③ すでに運用監視暗号リストに掲載されており、互換性維持以外の目的での利用が推奨されていないこと

④ NIST も、Triple DES ですでに暗号化されたデータに対する処理は引き続き許容していること

⑤ 「電子政府推奨暗号リスト」に掲載されている DSA は、現在の FIPS PUB 186-5 では廃止されているが、FIPS PUB 186-5 になるときに削除すべきとの議論はなかったこと

【運用監視暗号リスト掲載のアルゴリズムの取り扱いに対する意見】

- 運用監視暗号リスト掲載の暗号アルゴリズムは、新規に極力使用しないように促していく活動を積極的に進めるべきである。

【DSA の扱いに対する意見】

- 今回、Triple DES の取り扱いについて検討することになった理由が「SP 800-67 Revision 2 が廃止された」ことが契機になっていると承知している。その場合、上記⑤に記載の通り、DSA も「現在の FIPS PUB 186-5 では廃止されている」ことから、Triple DES との注釈と同様の注釈を追記すべきではないか。

第3章　今後に向けて

2024 年度は、暗号鍵管理ガイダンス WG にて検討中の暗号鍵管理ガイダンスを完成させる予定である。また、暗号利活用のための新たなガイダンスとして、クラウド利用者が留意すべき鍵管理を解説することを目的とする「クラウドにおける鍵管理ガイダンス」の作成に着手する計画である。おおむね 2 年程度での完成を想定している。

【別紙】

2023 年度　暗号鍵管理ガイダンス WG 活動報告

1.　2023 年度の活動内容

1.1.　活動背景と目標

CRYPTREC では、情報システム設計者やシステム調達者が暗号の利活用を適切に行うためのガイドライン作成を進めており、暗号鍵管理ガイダンス WG では暗号鍵管理が必要なシステムの設計者向けに、暗号鍵管理システム（CKMS：Cryptographic Key Management System）の設計において考慮すべき事項を解説したガイダンスの作成を行っている。本 WG では、2020 年度に発行した「暗号鍵管理システム設計指針（基本編）」の副読本として 2021-2022 年度で「暗号鍵管理ガイダンス Ver.1.0」を作成した。

しかしながら、同ガイダンス Ver.1.0 は、あらゆる暗号鍵管理システムにおいて検討が必要となる共通項目に絞って解説を行ったものであり、「暗号鍵管理システム設計指針（基本編）」に記載された項目のすべてをカバーしたものではない。このため、同ガイダンス Ver.1.0 でカバーしなかった項目についてガイダンスの拡充を行い、2024 年度の公開を目指す。

1.2.　暗号鍵管理ガイダンス WG の委員構成及び開催状況

暗号鍵管理ガイダンス WG の委員構成は表 1-1 のとおりである。また、2023 年度の開催状況は表 1-2 のとおりである。

表 1-1 暗号鍵管理ガイダンス WG 委員構成

主査	上原　哲太郎	立命館大学　情報理工学部　情報理工学科　教授
委員	泉　雅明	シスコシステムズ合同会社 公共・法人システムズエンジニアリング システムズアーキテクト
委員	漆嶌　賢二	GMO グローバルサイン株式会社　事業企画部 部長
委員	垣内　由梨香	Microsoft Corporation　セキュリティレスポンスチーム セキュリティプログラムマネージャー
委員	菅野　哲	GMO サイバーセキュリティ by イエラエ株式会社 取締役 CTO of Development
委員	菊池　浩明	明治大学　総合数理学部　先端メディアサイエンス学科　教授

委員	小林　浩二	パナソニック オートモーティブシステムズ株式会社 開発本部プラットフォーム開発センター セキュリティ開発部　開発２課　係長
委員	須賀　祐治	株式会社インターネットイニシアティブ セキュリティ本部セキュリティ情報統括室　シニアエンジニア
委員	舟木　康浩	タレス DIS ジャパン株式会社 クラウドプロテクション&ライセンシング データプロテクション事業本部 セールスエンジニアマネージャ
委員	程吉　英仁	株式会社 NTT データグループ システム技術本部　サイバーセキュリティ技術部　課長代理
委員	満塩　尚史	デジタル庁 戦略・組織グループ　セキュリティ危機管理チーム セキュリティアーキテクト

（2024 年 2 月 15 日現在）

表 1-2　暗号鍵管理ガイダンス WG 開催状況

回	開催日	議事概要
第一回	2023 年 10 月 16 日	■ 2023 年度 WG 活動計画の確認 ■ 「暗号鍵管理デバイスへのセキュリティ対策」の記載概要に関する審議 ■ 「暗号鍵管理システム（CKMS）の設計原理と運用ポリシー」の記載概要に関する審議
第二回	2024 年 2 月 15 日	■ 第一回審議内容に係る対応方針に関する審議 ■ 「暗号鍵管理システム（CKMS）の設計原理と運用ポリシー」の記載概要に関する審議

2.　成果概要

2.1.　活動概要

2022 年度に完成させた「暗号鍵管理ガイダンス Ver.1.0」の追補との位置づけとして、2023 年度は表 1-2 内の議事概要のように、「暗号鍵管理システム設計指針（基本編）」に記載された項目でありながら記載を見送った部分について章・節ごとに記載予定の概要について審議した。特に、「暗号鍵管理システム（CKMS）の設計原理と運用ポリシー」及び「暗号鍵管理デバイスへのセキュリティ対策」の 2 つの章について記載すべき事項をダイジェスト形式で整理した。

暗号鍵管理ガイダンスの位置づけと想定読者

暗号鍵管理ガイダンスの位置づけ及び想定読者は次のとおりである。これらは同ガイダンス Ver.1.0 と同じである。

ガイダンスの位置づけ

- 暗号鍵管理機能を持つシステム設計者向けのガイダンスを作成する。このガイダンスは 2020 年に発行した「暗号鍵管理システム設計指針（基本編）」に記載された各検討項目（Framework Requirement：以降 FR）をより詳細に解説した副読本である
- 「暗号鍵管理システム設計指針（基本編）」に記載された各検討項目の解釈に役立つ、検討項目の背景や補足事項、実システムでの設計において検討項目に基づいた要求事項を含めるかどうかの判断材料などについて解説する
- 暗号鍵管理システムのシンプルなモデル（トイモデル）を例示し、トイモデルにおける各検討項目への対応例を説明することで、各検討項目の内容や思想の理解を促進する

想定読者

- 暗号鍵管理機能を持つシステムの設計者

暗号鍵管理ガイダンス拡充部分の章構成

暗号鍵管理ガイダンス拡充部分は「暗号鍵管理システム設計指針（基本編）」の章構成に対応して下表のとおりである。なお、下表はガイダンス拡充分を別冊とした場合の章構成であり、2022 年度発行済のガイダンス Ver.1.0 にマージするか別冊とするかは 2024 年度の執筆状況を踏まえて決定する。

暗号鍵管理システム設計指針（基本編）	暗号鍵管理ガイダンス Ver.1.0（2022 年度発行）	暗号鍵管理ガイダンス拡充分（別冊時）
1. はじめに	1. はじめに	1. はじめに
2. 暗号鍵管理の在り方	（1 章に集約）	（1 章に集約）
3. 本設計指針の活用方法	（1 章に集約）	（1 章に集約）
4. 暗号鍵管理システム（CKMS）の設計原理と運用ポリシー		2. 暗号鍵管理システム（CKMS）の設計原理と運用ポリシー

5. 暗号アルゴリズム運用のための暗号鍵管理オペレーション対策	2. 暗号アルゴリズム運用のための暗号鍵管理オペレーション対策	
6. 暗号アルゴリズムの選択	3. 暗号アルゴリズムの選択	
7. 暗号アルゴリズム運用に必要な鍵情報の管理	4. 暗号アルゴリズム運用に必要な鍵情報の管理	
8. 暗号鍵管理デバイスへのセキュリティ対策		3. 暗号鍵管理デバイスへのセキュリティ対策
9. 暗号鍵管理システム（CKMS）のオペレーション対策		4. 暗号鍵管理システム（CKMS）のオペレーション対策

2.2. 「暗号鍵管理システム（CKMS）の設計原理と運用ポリシー」の章

本年度の WG で主に議論した概要は以下のとおりである。

① 本章に記載するトイモデル

本章に記載するトイモデルについて検討を行い、IoT 製品向けのプライベート CA システム（図 1）とすることに決定した。

トイモデルで扱う「プライベート CA システム」の構成

- CKMS の範囲を CA サーバと HSM までとする
- プライベート CA システムは IoT 製品(家電想定)向けに公開鍵証明書の発行及び証明書の失効管理に使われる CRL の発行を行う
- 証明書のトラストアンカーはプライベート CA である
- IoT 製品向けの ID 管理、プライベート鍵生成、発行された証明書の機器埋め込みは工場内で行う
- IoT 製品は運用時にネット接続され、スマホ内専用アプリから IoT 製品ハブ経由でセンシングや制御が行われる。証明書は専用アプリと IoT 機器の接続(TLS での認証と秘匿通信確立)に利用される

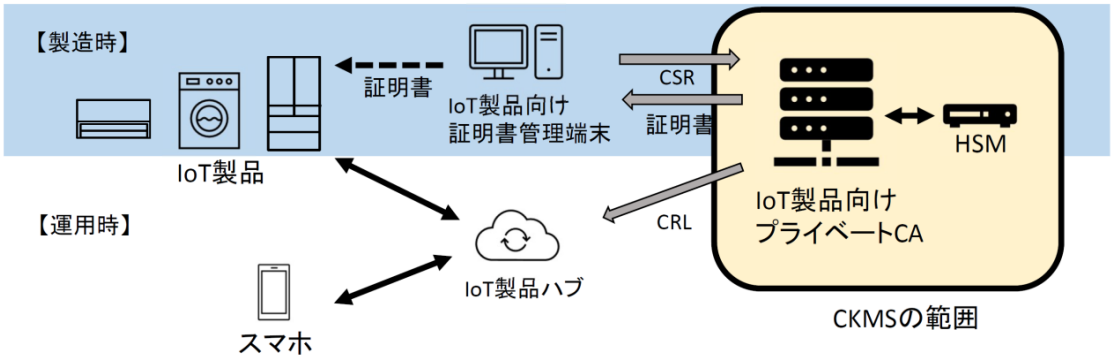

図 1　トイモデルで扱う「プライベート CA システム」の構成図

②　異なるセキュリティドメイン間での鍵情報の交換についての論点

異なるセキュリティドメイン間およびマルチレベルのセキュリティドメインを持つセキュリティドメインとの鍵交換の事例として、GPKI、マイナンバーカードの JPKI 及び民間活用、e シールについて該当する可能性を議論した。その結果、GPKI はセキュリティレベルの同等性を確認する事例であるがマルチレベルではないこと、マイナンバーカードの民間活用や e シールはマルチレベルのドメインポリシーを持つがドメインレベルが異なる相互の鍵交換を行う事例ではないことを確認した。

以上を踏まえ、GPKI を異なるセキュリティドメイン間での鍵交換の事例とし、マルチレベルのセキュリティドメイン間での鍵交換の事例は記載しない方針とした。

③　解説・考慮点の記載概要

本章に記載する「解説・考慮点」の主な概要について以下のように取りまとめた。

節番号	FR 番号	「解説・考慮点」の説明概要
4.1 節 CKMS セキュリティポリシー	A.01-A.05	セキュリティポリシーとは CKMS が実現するセキュリティ機能や運用方針の概要を定めたものである。CKMS を利用するシステムや CKMS が構築される IT 環境のポリシーなどと矛盾がないことが前提である。
4.2 節 情報管理ポリシー等からの要	A.06	個人の説明責任が求められるケース（監査、リスクマネジメントの観点）を想定して CKMS でのサポートメカニズムを記載する

求事項	A.07-A.13	匿名性、連結不可能性、観測不可能性のサポート有無とサポートする場合のメカニズムを記載する。一般に、匿名性、連結不可能性、観測不可能性を要求するのは特殊なケースである。
4.3 節 ドメインのセキュリティポリシー	A.14-A.19	異なるセキュリティドメイン間での鍵情報の交換がなければ対象外である。GPKI は異なるセキュリティドメイン間での鍵交換の事例である。
	A.22-A.26	マルチレベルのセキュリティドメインでの鍵情報の交換がなければ対象外である。一般に、マルチレベルのセキュリティドメインでの鍵情報の交換は特殊なケースである。
4.4 節 CKMS における役割と責任	A.27-A.28	CKMS の運用に関わるエンティティを定め、エンティティに割り当てる役割と実行できる鍵情報の管理機能へのアクセス権（権限）を定義する
	A.29-A.31	不必要な権限の割り当てや権限の分離が不十分な場合、内部犯行を誘発するリスクがある
4.5 節 CKMS の構築環境及び実現目標	A.32	CKMS を構成する主要なデバイスおよびコンポーネントの一式を定める
	A.33-A.36	CKMS が要求する時刻の精度や利用する権威時刻ソース、第三者タイムスタンプの要求有無を定める
	A.39-A.42	初期及び将来を想定してユーザ数や CKMS 性能面の目標、負荷増大時の対応策を定める
	A.43-A.46	CKMS 内デバイスや CKMS 間の相互運用を可能とするため、インタフェース、プロトコル、コマンド仕様を定める
	A.47-A.50	使いやすいユーザインタフェースを検討し、ヒューマンエラーを防止する
	A.51-A.53	どのような商用既製品を利用してどのようなセキュリティ機能を実行するかを定める
4.6 節 標準／規制に対	A.54-A.55	暗号アルゴリズム、暗号モジュール、セキュリティ認証などの標準への準拠性を明確にする

する適合性	A.57	CKMS が使用される国家・地域の法的規制を明確にする。欧州のサイバーセキュリティ法、中国のデータセキュリティ法、各国のデータ規制などが関係する。
4.7 節 将来的な移行対策の必要性	A.58-A.61	CKMS は暗号アルゴリズムのセキュリティライフタイムを超えたサービス提供や、危殆化により、暗号アルゴリズムの置き換えが必要になる。そのため、複数の暗号アルゴリズムや異なる鍵長をサポートするケースも多い。
	A.62-A.69	技術の進歩をウォッチすると共に、予め潜在的な脅威に対する影響評価の実施を推奨する

④　トイモデルでの説明の記載概要

本章に記載する「トイモデルでの説明」の主な概要について以下のように取りまとめた。

節番号	FR 番号	トイモデルにおける説明概要
4.1 節 CKMS セキュリティポリシー	A.01-A.02	パブリック CA の CP（Certificate Policy）と CPS（Certification Practice Statement）を参考にセキュリティポリシーを作成する
	A.03-A.04	情報管理ポリシー、情報セキュリティポリシー、HSM セキュリティポリシーが関連するポリシーである
4.2 節 情報管理ポリシー等からの要求事項	A.06	個人の説明責任の要求について、アクセス制御・認可とログ管理によって対応する
	A.07-A.13	匿名性、連結不可能性、観測不可能性は要求事項にない
4.3 節 ドメインのセキュリティポリシー	A.14-A.19	プライベート CA はシングルポリシーであり、「異なるセキュリティドメインとの鍵交換」は対象外である
	A.22-A.29	マルチレベルのセキュリティドメインポリシーをサポートするエンティティは存在しないため、対象外である
4.4 節 CKMS における役割と責任	A.27-A.28	役割と権限を次とする。責任者及び監査者 : 各種ログの閲覧； CA 及び HSM 管理者 : CA 署名鍵の生成・更新・破棄、鍵のバックアップ&リストア、CA 設定の管理； ユーザ : 証明書発行・証明書失効処理の要求及び証明書・CRL の受信
	A.29	責任者、監査者、CA 及び HSM 管理者、ユーザの各権限は兼任できないものとする

4.5 節 CKMS の構築環境及び実現目標	A.32	CA サーバ、HSM、ルータが主要なデバイスであり、CA ソフトウェアが主要なコンポーネントである
	A.33-A.36	国内の信頼できる NTP サーバによる時刻を用い、時刻精度は msec レベルである。第三者タイムスタンプは不要である
	A.38-A.39	証明書及び CRL の発行は専用のプログラムによって品質管理部門の習熟したメンバーが実施する
	A.40-A.42	証明書の発行対象となる IoT 製品は 100 万台/年の生産量であり、CRL は最大約 500 台/年の規模である。今後 10 年間で 10 倍程度の生産台数増加を想定。証明書及び CRL 発行処理のトランザクションはシーケンシャル処理で 1sec 以内を要求。負荷増大には CA サーバ及び HSM 増設で対処する
	A.43-A.46	HSM の API は PKCS#11、証明書発行要求は PKCS#10、証明書及び CRL の形式は RFC5280 に従う
	A.47	運用時のユーザは習熟した担当者であり、ユーザインタフェースでのヒューマンエラー防止は重要でない
	A.51-A.52	商用既製品としてサーバ（OS 及び CA ソフトウェアを含む）、HSM、ルータを利用する。HSM によって証明書や CRL への CA 署名付与、CA 署名鍵の管理を実施。CA ソフトウェアによって鍵のメタデータ管理や全体制御を行う
4.6 節 標準／規制に対する適合性	A.54-A.56	HSM 搭載の署名アルゴリズムは CRYPTREC 暗号リストに従い、HSM は FIPS140-2/-3 レベル 3 に準拠した製品を運用開始時及びリプレイス時に採用する
	A.57	サービス対象の IoT 機器は国内に閉じた運用であり、考慮すべき法的規制はない
4.7 節 将来的な移行対策の必要性	A.59-A.63	将来の移行を想定して、署名アルゴリズムと鍵長は 128bit セキュリティ（ECDSA P-256, SHA-256 : ライフタイムは 2040 年まで）と 192bit セキュリティ（ECDSA P-384, SHA-384 : ライフライムは 2070 年まで）を用意する

	A.69	暗号解読可能な量子コンピュータが実現された場合、IoT機器運用時の TLS が危殆化する可能性があるが、本 IoT機器で保護する通信内容はリアルタイムで意味を持つ情報であり、ハーベスト攻撃特有のリスクは小さい

2.3. 「暗号鍵管理デバイスへのセキュリティ対策」の章

本年度の WG で主に議論した概要は以下のとおりである。

① 本章に記載するトイモデル

本章に記載するトイモデルとして､図 1 のプライベート CA におけるハードウェア･セキュリティモジュール（HSM）を対象とすることに決定した。

② HSM での鍵の入出力機能について

HSM における鍵の入出力機能、障害対策や可用性確保のための鍵情報のクローン機能及びバックアップ&リストア機能について議論した。HSM で利用するプライベート鍵は HSM 内で生成することが原則であるが、既存の秘密鍵をインポートするニーズがあり鍵の入力機能を備えた製品があること、PKI では HSM のクローンではなく鍵情報のバックアップ&リストアを利用するのが一般的であること、鍵情報のバックアップ&リストアは PKCS#11 に従った API であるが HSM ベンダの独自仕様として機能提供されることを確認した。これらをトイモデルでの説明に反映することとした。

③ HSM でのセキュリティ評価・試験について

HSM でのセキュリティ評価・試験に関わる情報提供について議論した。HSM ベンダのセキュリティ評価･試験の情報提供は FIPS140 認証取得のセキュリティポリシーや製品マニュアルの範囲が原則であり、ベンダテストやペネトレーションテストの結果は提供していないことを確認した。その結果、セキュリティ評価･試験は FR 要求内容の説明の追加に加えて、FIPS140 などのセキュリティ認証で FR が要求するテストにカバーできるものが多いことを補足する方針とした。

④ 「解説・考慮点」の記載概要

本章に記載する「解説・考慮点」の主な概要について以下のように取りまとめた。

節番号	FR 番号	「解説・考慮点」の説明概要
8.1 節 鍵情報へのアクセスコントロール	E.01-E.04	暗号モジュールの各機能の実行を認可されたエンティティに限定する。実行権を管理するアクセスコントロールシステム（ACS）は暗号モジュールと連動して動作する
	E.05	ACS によるエンティティ識別、認証、認可の粒度や機能を明確にする
	E.07-E.20	暗号モジュールとは、暗号境界内で暗号処理を実行するハードウェアもしくはソフトウェアの集合。暗号境界内で利用される暗号鍵の保護機能を有する
	E.08-E.14	暗号モジュールへの鍵情報の入出力を平文形式で行うことは望ましくない。出力は暗号化して行うことが望ましく、主に外部での保管（バックアップなど）目的である
	E.21	鍵情報の入力を人間が行う場合、その正確さとセキュリティ面の問題がある。こうした入力がない場合は対象外である
	E.22-E.25	マルチパーティコントロールを利用する機能を明確にする。暗号鍵分割（K out of N 秘密分散）やマルチパーティ機能をベンダに確認する
8.2 節 セキュリティ評価・試験	E.26-E.34	いずれもシステムレベルの試験項目であるが、特に暗号モジュール（HSM）にも関連するものはベンダテスト、機能テスト、セキュリティテスト、環境テスト、セルフチェックテスト、第三者テストである
	E.26-E.34	FIPS140 などの認証試験で上記テストをカバーするものが多い
8.3 節 暗号モジュールの障害時の BCP 対策	E.35	暗号モジュールはセルフテスト機能を備えることが望ましい。FIPS140-2/-3 の要件に動作前や条件付きのセルフテスト機能がある
	E.37	回復可能なエラー発生時のセルフテストを含む回復の手順、回復困難なエラー発生時の暗号モジュールの交換手順（鍵情報のバックアップや破壊を含む）を明確にする

⑤　「トイモデルでの説明」の記載概要

本章に記載する「トイモデルでの説明」の主な概要について以下のように取りまとめた。

節番号	FR 番号	トイモデルにおける説明概要
8.1 節 鍵情報へのアクセスコントロール	E.01	ACS は CA サーバと HSM の 2 段階があり、HSM の ACS は HSM 内に設けられている
	E.03	HSM 管理者権限、HSM 利用者権限、HSM 監査者権限がある
	E.04-E.05	各エンティティは個人単位で識別・認証され、設定した役割に基づき認可された権限を実行できる
	E.08-E.15	CA プライベート鍵は原則として HSM 内で生成する。バックアップ&リストアのために HSM 内の鍵情報の入出力機能がある。PKCS#11 の API によって暗号化して外部出力する
	E.21	HSM 内鍵情報のバックアップ&リストアに人間が介在する。本機能の HSM のエラー処理を確認する
	E.22	HSM の管理者権限の取得にマルチパーティコントロールを利用する
8.2 節 セキュリティ評価・試験	E.29-E.32, E.34	HSM のセキュリティ評価に関わる次の評価結果を HSM ベンダに要求する：機能試験とセキュリティ試験の結果、環境試験の評価結果、セルフチェックテストの内容と実施タイミングの説明、FIPS140-2/-3 レベル 3 の認証書
	E.26-E.34	システムレベルの試験内容はセキュリティ試験仕様書にまとめ、試験報告書の試験結果を確認する
8.3 節 暗号モジュールの障害時の BCP 対策	E.35	HSM は暗号処理のセルフテスト機能を備える
	E.37	予め HSM 障害時の対応を想定して鍵情報のバックアップを取得しておく。HSM の再起動を繰り返してもエラーが回復しない場合は HSM の入れ替えと鍵情報のリストアを実施する

3. 今後に向けて

2024 年度は、2022 年度に取りまとめを行わなかった拡充部分について、残る「暗号鍵管理システム（CKMS）のオペレーション対策」の章を今年度と同様の形式で記載概要として整理する。その上で、記載概要をもとにガイダンス文書の執筆を進め、暗号鍵管理ガイダンスの拡充を完了する予定である。

CRYPTREC Report 2022
(暗号技術活用委員会報告　CRYPTREC RP-3000-2022)

発行日　2023年6月30日 第1版（印刷版）
発行者
・〒113-6591
東京都文京区本駒込二丁目28番8号
独立行政法人情報処理推進機構
(セキュリティセンター 技術評価部 暗号グループ)
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
2-28-8 HONKOMAGOME, BUNKYO-KU
TOKYO, 113-6591 JAPAN

・〒184-8795
東京都小金井市貫井北町四丁目2番1号
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 セキュリティ基盤研究室)
NATIONAL INSTITUTE OF
INFORMATION AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI, KOGANEI
TOKYO, 184-8795 JAPAN