CRYPTREC Report 2024

令和 7 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 2024 年度の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。

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おり、2024 年度は「暗号鍵管理ガイダンス Part 2」を作成した。2023 年に発行した「暗号鍵管理ガイダンス Part 1」及び 2024 年度作成の「暗号鍵管理ガイダンス Part 2」は、「暗号鍵管理システム設計指針（基本編）」で記載が求められる項目を検討する際に明記する事項や考慮点などを解説している。両ガイダンスによって「暗号鍵管理システム設計指針（基本編）」の全ての項目をカバーした。

また、近年はクラウドサービスを活用して情報システムを構築するケースが増えており、そのようなシステムでは暗号鍵管理が今まで以上に重要になる。そこで、クラウドサービスで利用する暗号鍵管理システムに特化したガイダンスについて検討を開始した。2025 年度より新たなワーキンググループを設置して当該ガイダンスの作成を本格的に開始する予定である。

2024 年度の成果をもとに、暗号鍵管理が適切に行われ、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ことを期待している。

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。

2025 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、2024 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。

2023 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負わない。

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。

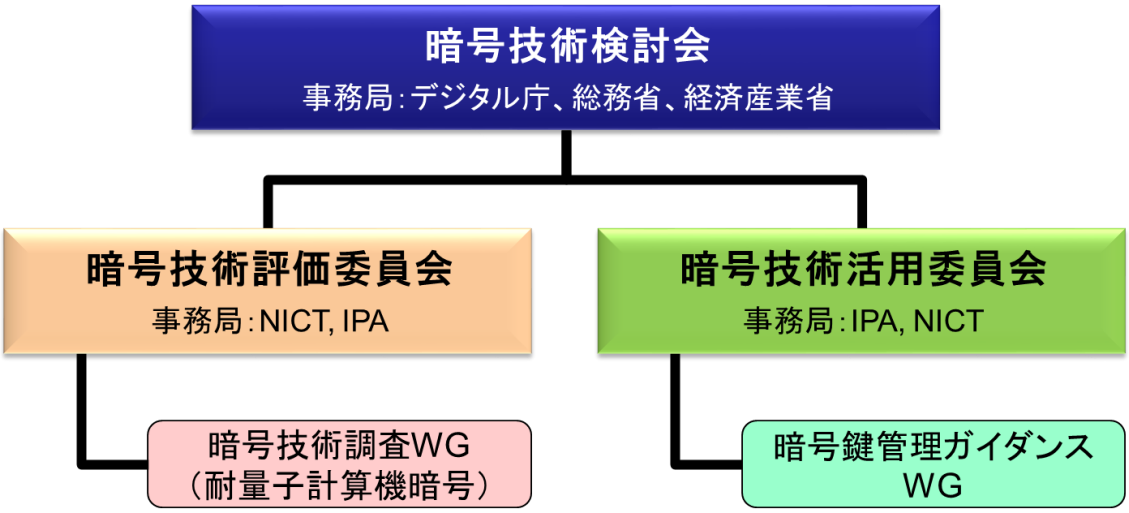

図 1　2024 年度の CRYPTREC の体制

委員名簿

暗号技術活用委員会

委員長	松本 勉	産業技術総合研究所 フェロー 横浜国立大学 先端科学高等研究院 上席特別教授
委員	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	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	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	佐藤 直之	SCSK セキュリティ株式会社 コンサルティング本部 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 IS 研究所 デジタルプラットフォームディビジョン 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 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	田村 裕子	日本銀行 金融研究所 情報技術研究センター 企画役
委員	手塚 悟	慶應義塾大学 グローバルリサーチインスティテュート 特任教授
委員	寺村 亮一	GMO サイバーセキュリティ by イエラエ株式会社 上席執行役員 CMO サイバーセキュリティ事業本部 本部長
委員	三澤 学	三菱電機株式会社 情報技術総合研究所 情報ネットワークシステム技術部 グループマネージャー
委員	満塩 尚史	順天堂大学 健康データサイエンス学部 健康データサイエンス学科 准教授
委員	山口 利恵	東京大学 大学院情報理工学系研究科 ソーシャル ICT 研究センター 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：2025 年 3 月末時点）

暗号鍵管理ガイダンス WG

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 東日本公共・法人システムズエンジニアリング ソリューションズエンジニアリング第 1 ソリューションズエンジニア
委員	漆嶌 賢二	GMO グローバルサイン株式会社 事業企画部 フェロー
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 常務取締役 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 ２係 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 ソリューション事業本部 セキュリティ&ネットワーク事業部 サイバーセキュリティ統括部 課長代理
委員	満塩 尚史	順天堂大学 健康データサイエンス学部 健康データサイエンス学科 准教授

（所属：2025 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
松井 裕介	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
北井上 礼樹	デジタル庁 デジタル社会共通機能グループ
渡辺 良光	デジタル庁 デジタル社会共通機能グループ
山之上 隆広	デジタル庁 デジタル社会共通機能グループ
水野 美紀	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
内藤 めい	総務省 サイバーセキュリティ統括官室
市川 和秀	総務省 サイバーセキュリティ統括官室
川村 航太	総務省 サイバーセキュリティ統括官室
見次 正樹	経済産業省 商務情報政策局
加藤 優一	経済産業省 商務情報政策局
味木 耕平	経済産業省 商務情報政策局
木下 誠	外務省 大臣官房 情報通信課
黛 大輔	防衛省 整備計画局
椛木 隆慎	防衛省 整備計画局
樋田 雄士	防衛省 整備計画局
太和田 隆弘	警察大学校
増田 伊智也	警察大学校

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、鷲見拓哉、新保淳、伊藤忠彦、白岩裕子、川名優香）

国立研究開発法人情報通信研究機構（井上大介、青野良範、伊藤竜馬、大久保美也子、小川一人、金森祥子、黒川貴司、篠原直行、田村千代、吉田真紀）

第1章　2024 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。

2024 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、2020 年に発行した「暗号鍵管理システム設計指針（基本編）（以降「設計指針」と表記）」の副読本として、「暗号鍵管理ガイダンス」を作成する。本活動は暗号鍵管理ガイダンス WG にて実施する。具体的には、2021 年度から 2022 年度にかけて作成した「暗号鍵管理ガイダンス Ver.1.0」ではカバーできていない項目について、同ガイダンスの拡充を行う。2024 年度の完成を目標とする。

（2） クラウドにおける鍵管理ガイダンスの検討

以下のテーマに関する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。

- クラウドにおける鍵管理ガイダンス

  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。

1.2. 開催状況

2024 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　2024 年度暗号技術活用委員会　開催概要

回	開催日	議案
メール審議	2024 年 6 月	● 2024 年度暗号鍵管理ガイダンス WG 活動計画の審議
第一回	2024 年 10 月 28 日	● 2024 年度暗号技術活用委員会活動計画の確認 ● 2024 年度暗号鍵管理ガイダンス WG 活動計画の確認 ● 暗号鍵管理ガイダンス WG 進捗報告 ● クラウドにおける鍵管理ガイダンスについて

第二回	2025 年 3 月 4 日	● 2024 年度暗号鍵管理ガイダンス WG 活動報告及びガイダンス案の審議 ● クラウドにおける鍵管理ガイダンスについて ● 2024 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. 暗号鍵管理ガイダンスの拡充

2022 年度に作成した「暗号鍵管理ガイダンス Ver.1.0」において記載を見送った部分について追補版となるガイダンスを執筆した。追補版はガイダンス Ver.1.0 の分冊に相当するため、ガイダンス Ver.1.0 を「暗号鍵管理ガイダンス Part 1」、今年度執筆した追補版を「暗号鍵管理ガイダンス Part 2」と呼ぶこととした。

以下にガイダンス Part 2 の概要をまとめる。

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 Part 1 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「設計指針」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
- 「設計指針」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を解説する
- 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 Part 2 の章構成

暗号鍵管理ガイダンス Part 1 及び Part 2 の章構成は、「設計指針」の章構成に対応して表 2 のとおりである。

表 2　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 Part 1（2023 年 5 月発行）	暗号鍵管理ガイダンス Part 2（2024 年度執筆）
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の設計原理と運用ポリシー		2. 暗号鍵管理システム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のオペレーション対策		4. 暗号鍵管理システムのオペレーション対策

ガイダンス Part 1（2023 年 5 月発行）では、暗号鍵管理システム（Cryptographic Key Management System: CKMS）の利用環境に関わらず検討する必要がある項目のうち、「設計指針」の 5 章から 7 章に該当する項目に関して、項目の概説及びその記載例を提供している。これら「設計指針」の 5 章、6 章、7 章の項目は、図 2 の【B】、【C】、【D】にそれぞれ対応する。これらの項目は「狭義」の意味での暗号鍵管理に相当するものである。これらは CKMS を設計する場合だけでなく、暗号アルゴリズムを使ったアプリケーション等を利用する場合なども含めて、全ての暗号鍵管理に対して検討が必要となる項目である。

ガイダンス Part 2（2024 年度執筆）では、「設計指針」の 4 章、8 章、9 章に該当する項目に関して、項目の概説及びその記載例を提供している。これら「設計指針」の 4 章、8 章、9 章の項目は、図 2 の【A】、【E】、【F】にそれぞれ対応する。Part 2 の 2 章（＝図 2 の【A】）は CKMS の利用環境に関わらず検討する必要がある項目のうち、CKMS の全体方針を定める項目である。Part 2 の 3 章（＝図 2 の【E】）は CKMS に利用するデバイス管理を含む場合に検討すべき項目であり、Part 2 の 4 章（＝図 2 の【F】）は CKMS のシステム管理を含む場合に検討すべき項目である。Part 2 の 3 章や 4 章までを含む場合、

「広義」の意味での暗号鍵管理に相当する内容となる。

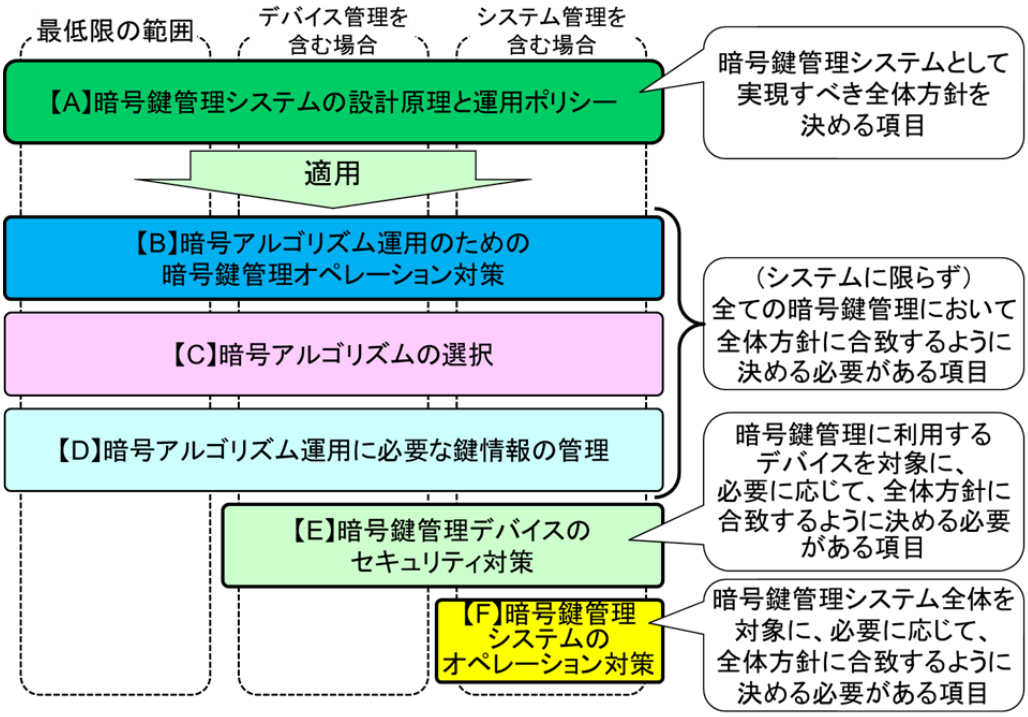

図 2　暗号鍵管理における目的別分類関係（「設計指針」の図 2-4 より）

暗号鍵管理ガイダンス Part 2 の記載概要

暗号鍵管理ガイダンス Part 2 の目次構成は以下のとおりである。

1　はじめに
- 1.1　位置づけ
- 1.2　想定読者
- 1.3　構成
- 1.4　トイモデル
- 1.5　検討体制

2　暗号鍵管理システムの設計原理と運用ポリシー
- 2.1.　CKMS セキュリティポリシー
- 2.2.　情報管理ポリシー等からの要求事項
- 2.3.　ドメインのセキュリティポリシー
- 2.4.　CKMS における役割と責任

各章の記載概要は以下のとおりである。

1 章は、イントロダクションとして、ガイダンス Part 2 の位置づけについて、「設計指針」やガイダンス Part 1 との関係を含めて記載した。また、ガイダンス Part 2 におけるトイモデルとして設定した「IoT 機器（家電製品を想定）向けに公開鍵証明書を発行するプライベート CA システム」の概要を説明した。

2 章は、「設計指針」での「暗号鍵管理システムの設計原理と運用ポリシー」における検討項目について解説・考慮点を記載した。本章は CKMS として実現すべき全体方針に関わる検討項目であり、ガイダンス Part 2 の以降の章やガイダンス Part 1 の各章における検討項目は、本章の検討結果と整合をとって定めることになる。CKMS のセキュリティポリシー、CKMS に関わるエンティティの定義、CKMS を構成するデバイスやコンポーネントの一覧、CKMS での実現目標、CKMS に関わる法規制や標準化技術、将来的な移行対策などの検討項目から構成される。トイモデルとしてプライベート CA のセキュリティポリシーや運用の想定例を設定して、各検討項目の対応例を説明した。

3 章は、「設計指針」での「暗号鍵管理デバイスへのセキュリティ対策」における検討項目について解説・考慮点を記載した。本章は、CKMS におけるセキュアな暗号鍵管理・保管の中核となる暗号鍵管理デバイスへのアクセスコントロールに対する検討事項、暗号鍵管理デバイス内の暗号モジュールに対する検討項目、暗号鍵管理デバイス及び CKMS のセキュリティ評価・試験に関する検討項目、暗号鍵管理デバイスにおける障害

発生時の BCP 対策に関わる検討項目などで構成される。トイモデルとして、プライベート CA で用いるハードウェア・セキュリティモジュールに関わる具体例として各検討項目の対応例を説明した。

4 章は、「設計指針」での「暗号鍵管理システムのオペレーション対策」における検討項目について解説・考慮点を記載した。本章は、CKMS における物理的セキュリティコントロール及びコンピュータシステムやネットワークにおけるセキュリティコントロールとそれらが危殆化した場合の BCP 対策、システム及びデバイスの開発プロセスやセキュリティメンテナンスに関わる検討項目、セキュリティアセスメントに関わる検討項目、CKMS 全体に関わる災害・障害発生時の BCP 対策などの検討項目で構成される。トイモデルとして、プライベート CA の設置環境や入退室管理、プライベート CA を構成するサーバシステムでのセキュリティコントロール、セキュリティアセスメントにおける実施項目、プライベート CA の災害復旧対策等を想定して各検討項目の対応例を説明した。

2.2. クラウドにおける鍵管理ガイダンスの検討

新たなガイダンスとして「クラウドにおける鍵管理ガイダンス（仮称）」を設定し、委員会での議論を通じて作成方針を検討した。

① 目的・想定読者・スコープについて

作成目的

本ガイダンス作成の目的について以下のように整理した。

クラウドサービスを活用して効率的に情報システムを構築することは政府機関、民間企業を問わず一般的になっている。一方で、クラウドサービスの活用には、クラウドサービスに預けた情報が漏洩すること、設定不備やクラウドサービスにおける障害波及のリスクがあること、等のオンプレミスとは異なる懸念事項も生じる。クラウドサービスにおける暗号鍵管理システムを適切に選択・構築・運用することによって、そうした懸念事項に対処できる部分がある。クラウドサービスにおける暗号鍵管理の仕組みや注意事項を解説したガイダンスを作成し、クラウド環境で安全に暗号を運用するための一つの解説書とする。

CRYPTREC では、NIST SP 800-130（A Framework for Designing Cryptographic Key Management Systems）に基づいて CKMS を設計する際の解説書として「暗号鍵管理システム設計指針（基本編）」及び「暗号鍵管理ガイダンス」を発行しており、今回作

成する解説書は、これらの CRYPTREC 文書を補強する位置づけにもなる。

上記の目的でガイダンスを作成することの意義について、クラウドサービスプロバイダ（CSP）や政府系プラットフォームの構築者にヒアリングしたところ、そもそもクラウドサービスにおける鍵管理にどのような事項があり、誰がそれを管理するのかといった内容について、利用者や SI 事業者の理解が十分でないとの意見をいただいた。そこで、上記の目的に加えて、まずは鍵管理における基本的な事項の解説に重点を置くこととした。

想定読者

本ガイダンスの想定読者は以下とした。

- クラウドサービスを利用した情報システムの構築者（SI 事業者）、運用者、利用者

スコープ

本ガイダンスのスコープについて以下のように整理した。

IaaS や PaaS のクラウドサービスを利用して、情報システムのプラットフォーム構築を行うケースを対象に、どのような鍵管理サービスを利用者に提供すべきかをターゲットとする。暗号機能による保護の対象は、クラウドサービスに預けたデータ及び鍵情報の機密性と完全性の確保、並びに暗号化消去とする。

上記のスコープは、クラウドにおける鍵管理には多様な対象が含まれ、例えば CSP の IaaS 上に SaaS 事業者が介在する形態もあるので、議論が発散しないようにスコープを定義すべきであるとの意見を踏まえて設定したものであり、クラウドサービスプロバイダ、SI 事業者、政府系プラットフォームの構築者にヒアリングした結果を参考にした。ただし、最初からスコープを狭くしすぎるのは適当でないとの意見もあり、スコープの妥当性については継続して検討することとした。

② 記載内容のポイントについて

本ガイダンス記載内容のポイントとなる事項について、以下の点を設定した。

- クラウド鍵管理サービスの分類

CSP が提供する鍵管理サービスを体系化し、ユースケースに応じてどのような鍵管理サービスを利用すべきかを判断できる情報を提供する。

上記に関して、CSP が提供する鍵管理サービスとして、「クラウドネイティブ暗号化」、「BYOK（Bring Your Own Key）」、「HYOK（Hold Your Own Key）」、「BYOE（Bring

Your Own Encryption）」と呼ばれる分類がある[2]が、必ずしも明確な定義は与えられていない。本ガイダンスではこれらの用語に定義を与える代わりに、鍵管理サービスの分類軸となる項目を明確にして鍵管理サービスを分類することとした。

- クラウド鍵管理サービスに関わる責任分界について

クラウドサービス利用時の鍵管理システムに関わる CSP との責任分界について、クラウド鍵管理サービスの種類に応じて原則となる考え方を整理する。その際、クラウドサービスモデル（IaaS、PaaS、SaaS）に依存する部分があるかについても現状を整理する。

上記のクラウドサービスモデルに依存する部分については、SI 事業者にヒアリングした中で、クラウドネイティブ暗号化と BYOK は IaaS、PaaS、SaaS の全てにおいて概ね利用できるが、HYOK や BYOE は適用できるクラウドサービスが限定されているとの見解をいただいた。

- 暗号鍵管理ガイダンス（NIST SP 800-130）の Framework Requirement との関係

暗号鍵管理ガイダンスにおいて解説している検討項目（Framework Requirement）について、クラウドサービス利用時はどのように検討されるべきかを記載する。現在の暗号鍵管理ガイダンスでは、オンプレミスに構築した CKMS をトイモデルに設定して検討項目への対応例を記載しているため、クラウドサービスを利用した場合に重点的に検討すべき項目や対応例がどのように変わるかを説明する。

上記に関しては NIST SP 800-130 の検討項目の中で、暗号鍵のライフサイクル管理（鍵の生成、ローテーション、破棄など）、暗号鍵の保管方法、暗号鍵へのアクセス制御を重点的に検討すべき項目の候補と考えている。

③ 作成スケジュールおよび検討体制

本ガイダンスの作成にあたって、2025 年度より WG を新しく設置することとした。WG 委員として CSP、SI 事業者・SaaS 事業者、クラウド HSM ベンダ、クラウドサービス利用者、大学や関連団体などの有識者にそれぞれ参画いただき、事務局を中心に委員の知見をまとめる形でガイダンス作成を進める。

作成スケジュールについては、WG の任期である 2 年間で遅くとも本ガイダンスの作成を行う。ただし、技術やサービスの進展が早い領域であり、計画は柔軟に捉えることとす

[2] 例えば、「Cloud Data Protection、バージョン 1.0」、日本クラウドセキュリティアライアンス（2021 年 8 月）。

る。ガイダンスに含める内容を明確にして作成を進めると共に、本ガイダンスに続いて検討すべき内容についても並行して議論していく。

第3章　今後に向けて

2025 年度は、新たなガイダンスである「クラウドにおける鍵管理ガイダンス（仮称）」について WG を設置し、ガイダンス作成を本格的に開始する予定である。

また、分冊構成とした暗号鍵管理ガイダンスについて合冊化の検討や、同ガイダンス作成中に「設計指針」記載内容に対して修正意見があった事項の対応については今後の課題事項とする。

【別紙】

2024 年度　暗号鍵管理ガイダンス WG 活動報告

1.　2024 年度の活動概要

1.1. 活動目的と活動概要

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 年度から 2022 年度にかけて「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かった。

本年度は、ガイダンス Ver.1.0 において記載を見送った部分について追補版のガイダンスを執筆した。分冊構成としたため、ガイダンス Ver.1.0 を「暗号鍵管理ガイダンス Part 1」、今年度執筆した追補版を「暗号鍵管理ガイダンス Part 2」と呼ぶこととした。

1.2. 暗号鍵管理ガイダンス WG の開催状況

2024 年度の暗号鍵管理ガイダンス WG の開催状況は表 3 のとおりである。

表 3　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	2024 年 7 月 30 日	■ 2024 年度 WG 活動計画の確認 ■ 「暗号鍵管理システムのオペレーション対策」の記載概要に関する審議 ■ ガイダンス執筆方針及びレビュー計画に関わる審議
メール審議	2024 年 8 月 ～10 月	■ 「暗号鍵管理デバイスへのセキュリティ対策」ドラフトのレビュー（7/30～9/13） ■ 「暗号鍵管理システムの設計原理と運用ポリシー」ドラフトのレビュー（10/1～11/1）
第二回	2024 年 11 月 18 日	■ 「暗号鍵管理デバイスへのセキュリティ対策」ドラフトの審議

		■ 「暗号鍵管理システムの設計原理と運用ポリシー」ドラフトの審議
メール審議	2024 年 11 月～2025 年 1 月	■ 「暗号鍵管理システムのオペレーション対策」ドラフトのレビュー（11/20～1/17） ■ 「はじめに」ドラフトのレビュー（12/5～1/17）
第三回	2025 年 1 月 22 日	■ 「はじめに」ドラフトの審議 ■ 「暗号鍵管理システムのオペレーション対策」ドラフトの審議 ■ ガイダンス全体に関わる審議
メール審議	2025 年 1 月～2 月	■ ガイダンスの最終レビュー（1/27～2/14）

2. 成果概要

2.1. 暗号鍵管理ガイダンス Part 2 の位置づけと章構成

暗号鍵管理ガイダンス Part 2 の位置づけは次のとおりである。これらは同ガイダンス Part 1 と同一である。

暗号鍵管理ガイダンス Part 2 の位置づけ

- 暗号鍵管理機能を持つシステムの設計者向けのガイダンスである。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 Part 2 の章構成

暗号鍵管理ガイダンス Part 2 の構成は「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 4 のとおりである。

表 4　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 Part 1（2023 年 5 月発行）	暗号鍵管理ガイダンス Part 2（今年度執筆）
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の設計原理と運用ポリシー		2. 暗号鍵管理システム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のオペレーション対策		4. 暗号鍵管理システムのオペレーション対策

2.2. 「はじめに」の章

本年度の WG で議論した事項の概要は以下のとおりである。

① トイモデルについて

本ガイダンスにおけるトイモデルは IoT 製品向けのプライベート CA システム（図 3）を設定した。本ガイダンスの各章において同一のトイモデルを扱うこととした。

トイモデルで扱う「プライベート CA システム」の概要

- CKMS の範囲を CA サーバ、HSM（Hardware Security Module）、ルータまでとする
- 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

- 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 製品は運用時にインターネット接続され、スマートフォン内専用アプリから IoT 製品ハブ経由で状態の監視や制御が行われる。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

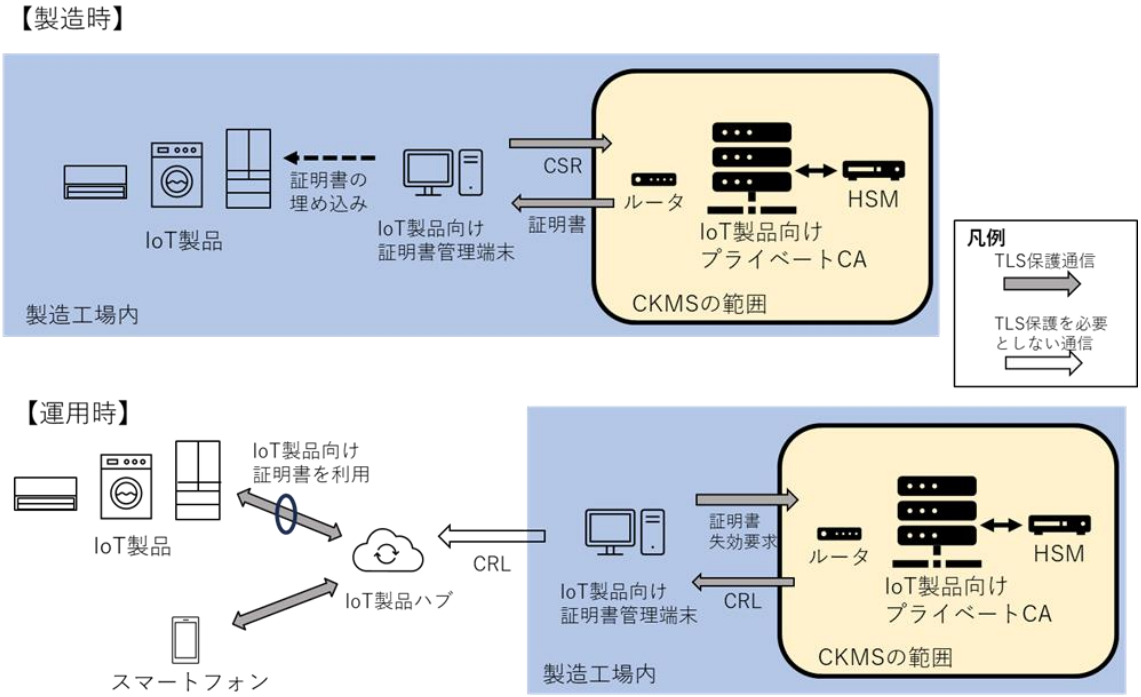

図 3　トイモデル（プライベート CA システム）の概要図
（「暗号鍵管理ガイダンス Part 2」の図 1-3 より）

トイモデルに関して、今回は CA 秘密鍵の管理に HSM を利用しているが、同様のシステムを設計する際に HSM を導入しないといけないと読者に誤解を与えないかとの意見があった。これに対して、HSM 以外の選択肢もあるが、その場合は HSM に代わる秘密鍵の保護に関する様々な対応が必要になることを注記した。また、トイモデルはあくまで FR の説明のための参考例であり、この内容を推奨しているわけではないことの注意が本文に書かれていることを確認した。

2.3.　「暗号鍵管理システムの設計原理と運用ポリシー」の章

本年度の WG で議論した事項の概要は以下のとおりである。

① セキュリティポリシーと準拠する規格・標準の関係について

CKMS セキュリティポリシーに関して、CKMS を運用する組織に存在する様々なセキュリティに関わるポリシーとの依存関係を整理する FR がある。

CKMS より上位に位置づけられるポリシー及び CKMS より下位のポリシーについて例示を行った際に、上位ポリシーの例として、製品規格のセキュリティポリシー、NIST SP 800-57 Part 2（鍵管理セキュリティポリシー）、IoT 製品に対するセキュリティ適合性評価制度構築方針（経済産業省）を追加してはどうかとの意見が出された。このことを契機に、「セキュリティポリシー（2.1 節）」と「準拠すべき標準・規格（2.6 節）」の関係を整理した。

セキュリティポリシーは準拠すべき規格を元に各組織で定める性格のものとするのが適当であると判断し、製品規格や IoT 製品に対するセキュリティ適合性評価制度構築方針は「準拠すべき標準・規格（2.6 節）」の具体例として記載した。また、NIST SP 800-57 Part 2 は組織が暗号鍵を安全に管理するためのベストプラクティスを提供し、鍵管理セキュリティポリシーの策定に役立つガイド文書に相当する内容と捉え、「セキュリティポリシー（2.1 節）」の解説・考慮点にその旨を記載した。

② 実現目標の記載例について

「CKMS の構築環境及び実現目標（2.5 節）」において、ネットワーク性能やパフォーマンス特性などの目標値を整理することが求められる。

トイモデルの想定事例として、IoT 製品に証明書を埋め込む生産ラインでの性能要求から CKMS（プライベート CA）での証明書の発行処理におけるネットワーク性能及びパフォーマンス性能の目標値を規定していたが、証明書は事前に発行しておき、製造工程で製品に証明書を埋め込む処理は発行処理とは分れるのが一般的ではないかとの指摘があった。指摘のような運用が一般的と考えられることから、IoT 製品の生産ラインと連動してオンラインで証明書を発行する必要はないが、年間の生産台数の計画から証明書発行に関わるパフォーマンスが規定されるものとして事例をまとめた。

2.4. 「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 で議論した事項の概要は以下のとおりである。

① トイモデルにおけるアクセスコントロールシステム（ACS）について

「鍵情報へのアクセスコントロール（3.1 節）」において、鍵情報へのアクセスコントロールへの要求事項を整理する FR がある。

トイモデルにおけるアクセスコントロールシステムの想定事例では、CA サーバにおける ACS と HSM における ACS を連携させて構成するものとした。このうち、HSM の ACS に関わる

エンティティ認証、及び権限認可について、製品事例として以下の情報提供があった。

- HSM 製品は一般に PKCS #11 ベースのユーザ管理となっており、セキュリティ・オフィサー（HSM の管理者ロール）とクリプト・オフィサー（HSM 内の鍵生成や鍵利用を行うアプリケーションにおいて利用するユーザのロール）で HSM にログオンする
- HSM 管理者権限の取得などに利用するインタフェースとして、汎用 PC のシリアル接続や SSH 接続をサポートしている
- HSM 内の署名鍵を利用して署名付与を実施する際の処理概略は以下のとおりとなる。
  1. CA アプリケーションから HSM に対してクリプト・オフィサーの PIN で認証
  2. CA アプリケーションは利用する鍵の名称を指定して、鍵の探索を HSM に対して依頼し、HSM から鍵のオブジェクト・ハンドルを取得
  3. CA アプリケーションはオブジェクト・ハンドルを指定して、提供するデータへの署名処理を HSM に対して依頼

上記を踏まえて、ACS 関連のトポロジー（図 4）と ACS に関わる処理フロー（図 5）を下図のとおりにまとめた。

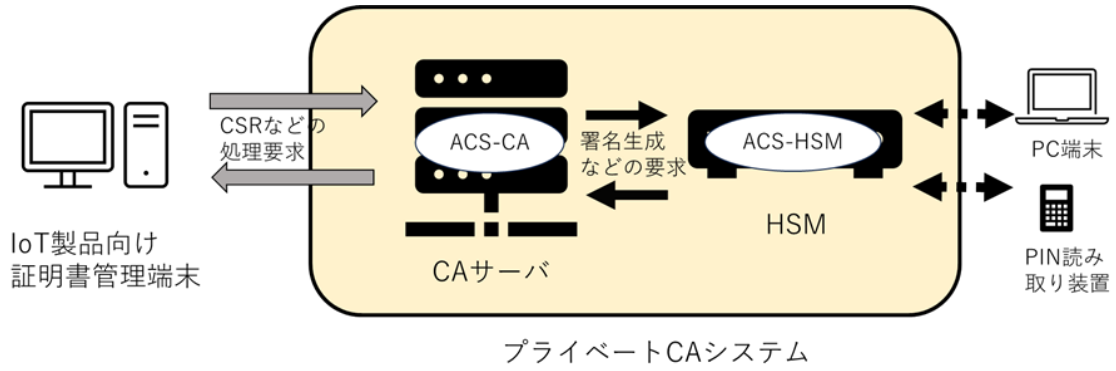

図 4　ACS の配置（「暗号鍵管理ガイダンス Part 2」の図 3-2 より）

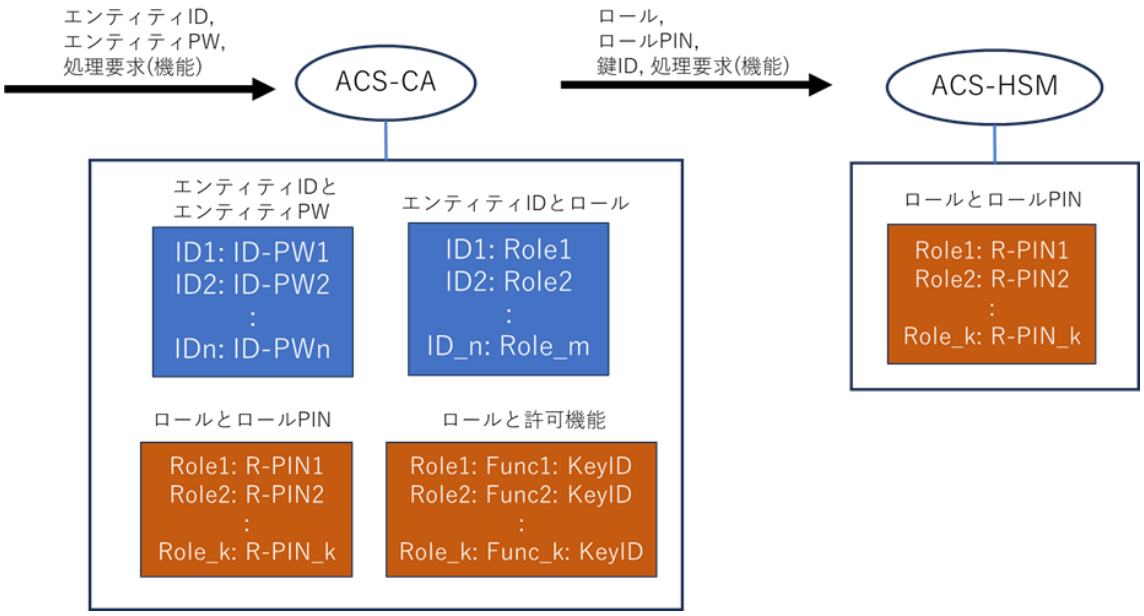

図 5　ACS に関わる処理フロー（「暗号鍵管理ガイダンス Part 2」の図 3-3 より）

CKMS のエンティティ、ACS、機能ロジックなどの接続配置については以下のとおりに記載した。

CA サーバ内の ACS-CA が要求を送出した利用者を識別・認証し、認証結果に応じて利用者に割り当てられた役割（ロール）の実行許可を与える。CA サーバは HSM に対して処理の依頼を利用者に代わって送出し、HSM から受け取った処理結果を利用者に返す。ここで、HSM 内の ACS-HSM は CA サーバのロールを認証して処理の実行を許可する。ACS に関わる処理フローは図 2-3 を参照。
一方、HSM 管理者の識別・認証は、CA サーバ内の ACS-CA を介さずに HSM 内の ACS-HSM によって行われる。その際、HSM に専用の PIN 読み取り装置を接続して認証処理を行う。また、HSM への管理用コマンドの送信には PC 端末から HSM がサポートしている方式（例えば、シリアル接続や SSH 等）で接続して処理を行う。

また、エンティティへの権限認可による署名付与の処理手順については以下のとおりに記載した。

CA サーバ及び HSM においてエンティティはロールベースで権限が付与される。ACS-CA にはエンティティの ID ごとに対応するロールを管理するデータベースがあり、さらにロールと許可された鍵管理機能および当該処理に利用する鍵 ID の対応を管理するデー

タベースがある。ACS-HSM では、PKCS #11 仕様に基づいてロールや鍵を管理しており、ACS-HSM で認証された利用者は、利用可能な鍵を検索して署名処理などを実行する。

② 相互運用性テストについて

「セキュリティ評価・試験（3.2 節）」の中に相互運用性を主張する際のテストの明確化に関わる FR がある。トイモデル（プライベート CA）が提供する機能は証明書の発行処理と証明書の失効処理における CA 署名の付与のみであり、通信相手は社内の証明書管理端末に限定される。さらに、プロトコルも単純であるため、トイモデルの記載例では相互運用性テストに相当するテストは不要で、API レベルの機能テストや結合テストで十分であると記載していた。

これに対して、相互運用性テストが不要であることはなく、ローカル環境やフィールドにおいて CKMS 提供機能の動作試験を行うものが該当するのではないかとの意見があった。委員の間でもどのようなテストが相互運用性テストに相当するかの見解が必ずしも一致していない状況を認識したので、本文書における相互運用性テストの解釈を記載することとした。具体的には、NIST SP 800-130 該当節の記載から、CKMS レベルで他の CKMS との連携をテストするケースや保証ベースライン装置のようなゴールデンサンプルとの接続試験を行うものが相互運用性テストに該当する旨を追記した。

2.5. 「暗号鍵管理システムのオペレーション対策」の章

本年度の WG で議論した事項の概要は以下のとおりである。

① トイモデルにおける物理セキュリティコントロールについて

「CKMS へのアクセスコントロール（4.1 節）」において、CKMS デバイスやコンポーネントを保護するために設けられる物理的なセキュリティコントロールを明確にする FR がある。

当該項目に関して、複数の物理アクセスコントロールの境界があり、敷地や建物、CKMS 収容エリアなどのレイヤによって求められる物理セキュリティの強度が異なること、さらにスイスチーズモデルのようにレイヤ間で多層防御が有効に働き、複数のレイヤを貫通するような欠陥がないことを示せるとよいとの指摘があった。指摘を踏まえて、トイモデルにおける想定事例を図 6 のとおりにまとめた。各領域へのアクセスに必要となる認証情報がそれぞれ異なり、同一の認証情報によって複数の領域へのアクセスが可能とならないように設計していることを示した。

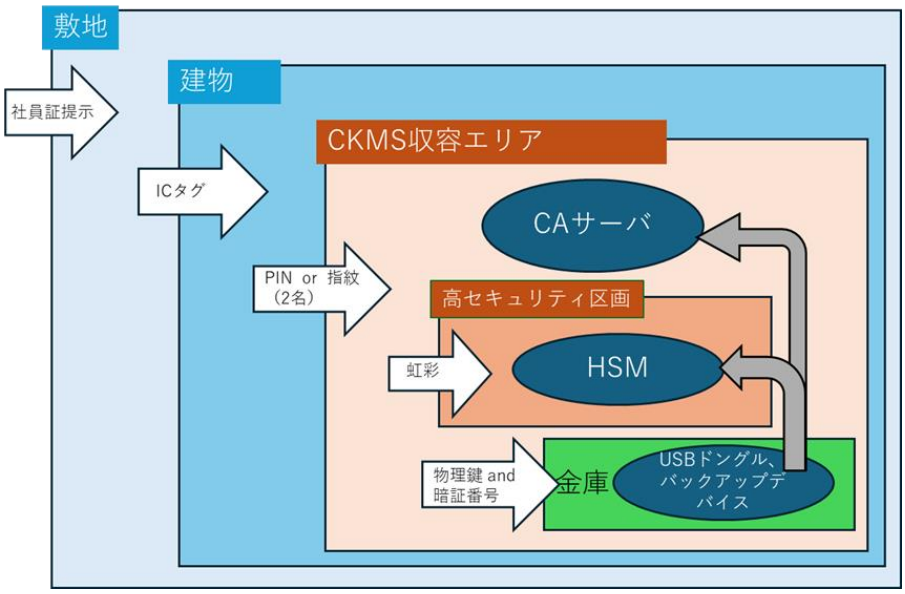

図 6　トイモデルにおける物理アクセスコントロール
（「暗号鍵管理ガイダンス Part 2」の図 4-1 より）

②　トイモデルにおける災害復旧対策について

「CKMS 設備への障害・災害発生時の BCP 対策（4.5 節）」において、CKMS 設備における物理的損害が発生した場合の復旧対策を明確にする FR がある。地震及び水害などの自然災害や火災及び事故などの人為災害をも想定した内容であり、災害復旧対策と呼ばれる検討項目である。CKMS 運用の価値と機微度にふさわしいレベルでの対策を講じることが原則であり、トイモデルではどのような対策を想定するのが妥当かを議論した。

トイモデルは IoT 製品の製造拠点に設けられたプライベート CA を CKMS としており、災害復旧対策の基準は IoT 機器の製造設備と同等とするのが妥当であろうとなった。また、一般に IoT 製品の製造拠点は、現地生産等を目的に分散して設けられていることが多く、ある拠点がダウンしても他の拠点が製造をカバーすることができ、自ずと災害復旧対策にもなる。今回の CKMS のレベルで災害復旧の目的で複数サイトを用意することは現実的ではないとの意見があった。

議論を踏まえて、CKMS の災害復旧対策を目的としたプライベート CA の冗長化は行わず、障害対策として CA サーバのディスク冗長化、予備デバイスの準備、HSM 内の鍵情報を含むバックアップ取得と保管を実施する事例とした。ここで、バックアップ情報は災害復旧の目的で他の製造拠点にも保管するものとした。

3. 今後に向けて

「暗号鍵管理システム設計指針（基本編）」の副読本である「暗号鍵管理ガイダンス」を作成する活動は今年度で終了する。暗号鍵管理ガイダンス Part 1 と Part 2 を合冊化するかどうかについては、今後のガイダンス読者の反応などに鑑みて判断する予定である。

執筆した暗号鍵管理ガイダンスにおいて設定したトイモデルは、オンプレミスに構築する CKMS を想定したが、近年はクラウドサービスを活用してシステム構築をするケースが増加している。クラウドサービスを活用した環境における暗号鍵管理のガイダンスを作成することは今後の課題である。

CRYPTREC Report 2024
(暗号技術活用委員会報告　CRYPTREC RP-3000-2024)

発行日　2025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