CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術活用委員会活動報告

暗号鍵管理ガイダンスWG活動報告

2025年7月25日

暗号技術活用委員会 委員長
（産業技術総合研究所 フェロー／横浜国立大学 上席特別教授） 松本　勉
暗号鍵管理ガイダンスWG　主査
（立命館大学 教授） 上原　哲太郎

目次

1. 暗号技術活用委員会　概要

2. 暗号技術活用委員会　2024年度の活動概要と2025年度の活動計画
   - 暗号鍵管理ガイダンスPart 2の作成
   - クラウドにおける鍵管理ガイダンスの検討
   - 暗号技術活用委員会　2025年度活動計画

3. 暗号鍵管理ガイダンスWG　2024年度の活動概要
   クラウド鍵管理ガイダンスWG　2025年度の活動計画
   - 暗号鍵管理ガイダンスPart 2の作成
   - クラウド鍵管理ガイダンスWG　2025年度活動計画

目次

1. 暗号技術活用委員会　概要

2. 暗号技術活用委員会　2024年度の活動概要と2025年度の活動計画
- 暗号鍵管理ガイダンスPart 2の作成
- クラウドにおける鍵管理ガイダンスの検討
- 暗号技術活用委員会　2025年度活動計画

3. 暗号鍵管理ガイダンスWG　2024年度の活動概要
クラウド鍵管理ガイダンスWG　2025年度の活動計画
- 暗号鍵管理ガイダンスPart 2の作成
- クラウド鍵管理ガイダンスWG　2025年度活動計画

CRYPTREC活動体制（2024年度）

暗号技術検討会

① CRYPTREC暗号のセキュリティ及び信頼性確保のための調査・検討
② CRYPTREC暗号リストの改定に関する調査・検討
③ 関係機関と連携した暗号技術の普及による情報セキュリティ対策の推進検討・提言

暗号技術評価委員会

① 暗号技術の安全性及び実装に係る監視及び評価
② 新世代暗号に係る調査
③ 暗号技術の安全な利用方法に関する調査

暗号技術調査WG （耐量子計算機暗号）

暗号技術活用委員会

① 暗号の普及促進・セキュリティ産業の競争力強化に係る検討
② 暗号技術の利用状況に係る調査及び必要な対策の検討
③ 暗号政策の中長期的視点からの取組の検討

暗号鍵管理ガイダンスWG

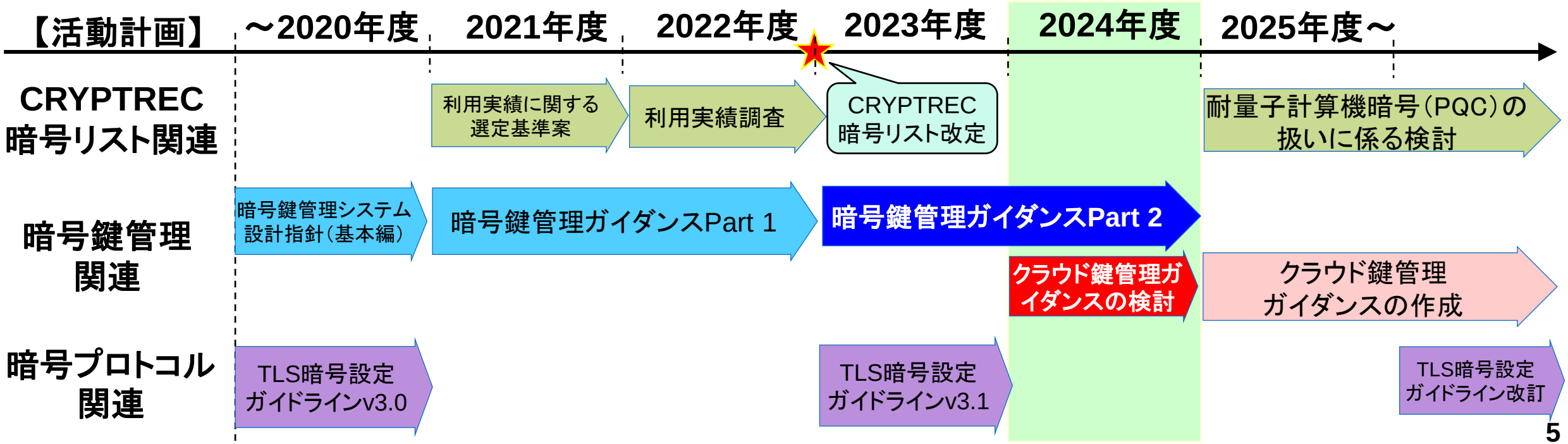
暗号技術活用委員会の活動目的

【活動目的】

暗号技術活用委員会は、**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**を行うものとする。

具体的には、実運用におけるセキュリティ確保の観点から、以下の対象を取り扱う。

- 暗号アルゴリズムの利用及び設定に関する運用マネジメント
- 暗号プロトコルの利用及び設定に関する運用マネジメント
- その他、情報システム全体のセキュリティ確保に有用な暗号に関わる運用マネジメント



目次

1. 暗号技術活用委員会　概要

2. 暗号技術活用委員会　2024年度の活動概要と2025年度の活動計画
- 暗号鍵管理ガイダンスPart 2の作成
- クラウドにおける鍵管理ガイダンスの検討
- 暗号技術活用委員会　2025年度活動計画

3. 暗号鍵管理ガイダンスWG　2024年度の活動概要
クラウド鍵管理ガイダンスWG　2025年度の活動計画
- 暗号鍵管理ガイダンスPart 2の作成
- クラウド鍵管理ガイダンスWG　2025年度活動計画

暗号技術活用委員会委員（2024年度）

CRYPTREC Cryptography Research and Evaluation Committees

（注）2025年3月末時点

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　上席特別教授
委員	上原　哲太郎	立命館大学　教授
委員	垣内　由梨香	Microsoft corporation　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セキュリティ株式会社　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　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　サイバーセキュリティ事業本部長
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	順天堂大学　准教授
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

暗号鍵管理ガイダンスWG委員（2024年度）

CRYPTREC Cryptography Research and Evaluation Committees

（注）2025年3月末時点

主査	上原　哲太郎	立命館大学　教授
委員	泉　雅明	シスコシステムズ合同会社　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　フェロー
委員	垣内　由梨香	Microsoft corporation　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　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　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　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　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　課長代理
委員	満塩　尚史	順天堂大学　准教授

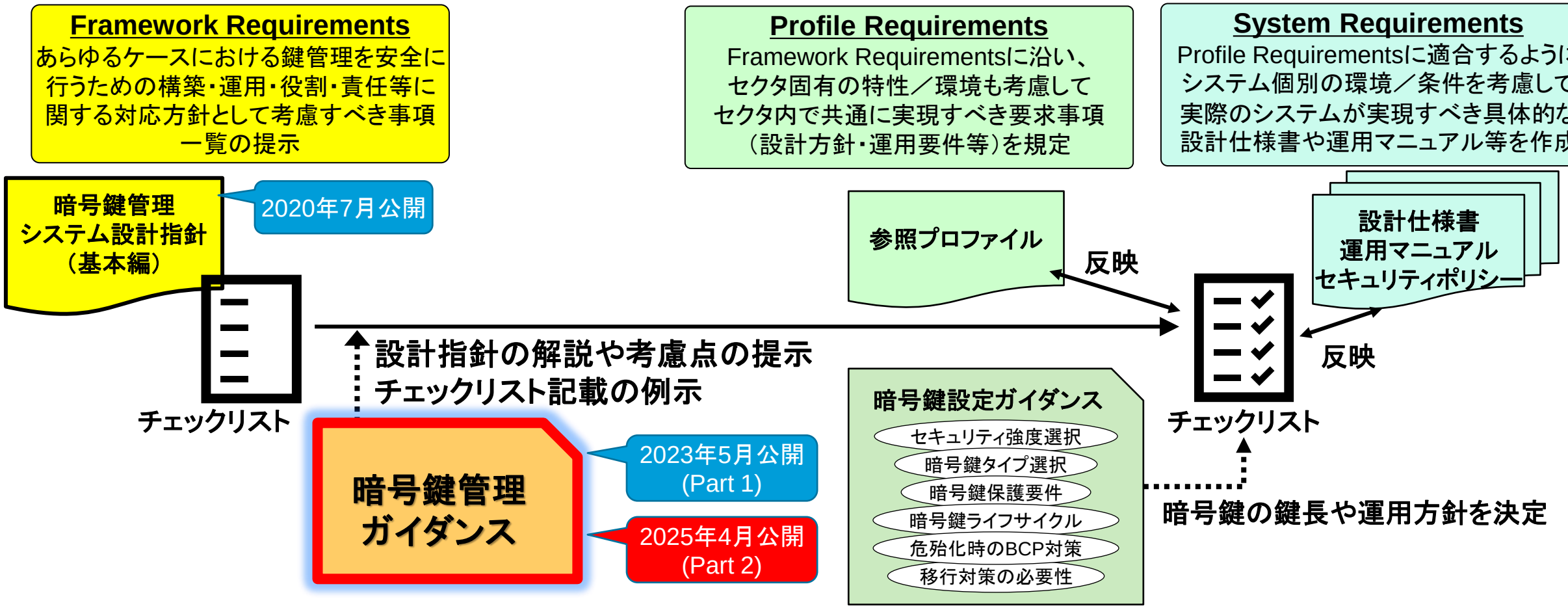
2024年度の活動概要

- 「暗号鍵管理ガイダンスPart 2」の作成
  - 暗号鍵管理ガイドラインの拡充を目的として、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、「暗号鍵管理ガイダンス」を作成。
  - 2023年度に発行した「暗号鍵管理ガイダンスPart 1」でカバーしていない項目を解説した「暗号鍵管理ガイダンスPart 2」を作成。
  - 本活動は暗号鍵管理ガイダンスWGにて実施。

- クラウドにおける鍵管理ガイダンスの検討
  - 新ガイドライン/ガイダンスの候補として「クラウドにおける鍵管理」をテーマに、ガイダンスの作成方針・記載上のポイントなどを検討。

「暗号鍵管理ガイダンスPart 2」の作成

■ 暗号鍵管理が必要なシステムの設計者向けに、暗号鍵管理の設計において考慮すべき点を解説するガイダンス
- 「暗号鍵管理ガイダンスPart 1（2022年度作成）」に記載していない章を解説
- 詳細は暗号鍵管理ガイダンスWG活動報告（上原主査）にて紹介



「クラウドにおける鍵管理ガイダンス」の検討：作成方針

【目的】

- 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が増加している。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のセキュリティに関して、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（CKMS: Cryptographic Key Management System）を適切に選択・構築・運用することで、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、クラウド環境での安全な暗号技術の運用を促進する。
- クラウドサービスにおける鍵の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。
  基本的な事項の解説にも重点を置く。
- クラウドサービス利用時を想定したCKMS設計に関わる「暗号鍵管理システム設計指針（基本編）」の解説書と位置づけるものとする。

【想定読者】

- 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】

- IaaSもしくは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。

「クラウドにおける鍵管理ガイダンス」の検討：記載上のポイント

- Point1: クラウド鍵管理サービスの分類

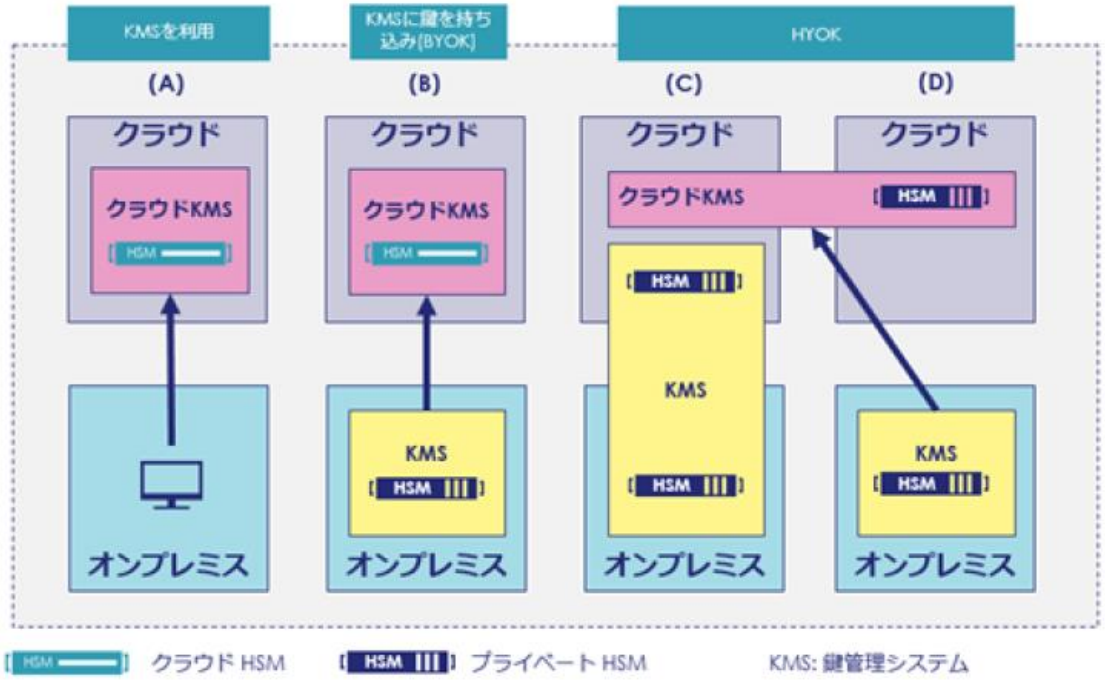
  クラウドサービスプロバイダ（CSP)が提供する鍵管理サービスを体系化し、ユースケースに応じてどのような鍵管理サービスを利用すべきかを判断できる情報を提供する。

- Point2: クラウド鍵管理サービスに関わる責任共有

  クラウド鍵管理サービスの種類に応じてCSPとの責任共有の原則となる考え方を整理する。
  前提として、クラウドサービスの種類（IaaS、PaaS、SaaS）に応じた鍵管理サービスの選択に係る制約も整理する。

- Point3: 「暗号鍵管理システム設計指針（基本編）」のFramework Requirement（FR）視点での整理

  クラウドサービス利用時も暗号鍵管理システムの全体として検討すべきことは変わらないが、クラウドサービスの利用によって利用者が重点的に検討すべきことは変わる。
  どういう項目に重点が置かれるかを「暗号鍵管理システム設計指針（基本編）」のFRの視点で整理する。



出典:「Cloud Data Protection バージョン1.0」, CSAジャパン, 2021年8月

暗号技術活用委員会 2025年度の活動計画

- 耐量子計算機暗号の扱いに係る検討
  - 昨今の耐量子計算機暗号の移行をめぐる社会的動向が、技術的側面からだけでなく、産業育成観点も含めた政策的側面を持って定められ、実行されている可能性が高いことを踏まえ、以下の検討を行う。
    - ✓ **「PQCへの移行（方針）」の政策的側面からのとりまとめ**
      「PQCへの移行（方針）」を検討する際の素材としてもらうため、各国政府・公的機関等がどのような政策やガイドラインを発行し、どのように産業界等に影響を与えているのかを整理する。
    - ✓ **「PQC専用にCRYPTREC暗号リストでの取扱いルール」を変更すべきかどうかの検討**
      CRYPTREC暗号リストにおけるPQCの位置づけ、特にPQC専用に「CRYPTREC暗号リストでの取扱いルール」を変更すべきかどうかを検討し、暗号技術活用委員会としての見解を取りまとめる。

- クラウドにおける鍵管理ガイダンスの作成
  - 暗号鍵管理ガイドラインの拡充活動の一環として、クラウドサービスを利用したシステム構築を対象とした暗号鍵管理ガイダンスの作成を目標に、クラウド鍵管理ガイダンスWGを設置する。

CRYPTREC活動体制（2025年度）

暗号技術検討会

① CRYPTREC暗号のセキュリティ及び信頼性確保のための調査・検討
② CRYPTREC暗号リストの改定に関する調査・検討
③ 関係機関と連携した暗号技術の普及による情報セキュリティ対策の推進検討・提言

暗号技術評価委員会

① 暗号技術の安全性及び実装に係る監視及び評価
② 新世代暗号に係る調査
③ 暗号技術の安全な利用方法に関する調査

暗号技術調査WG （耐量子計算機暗号）

暗号技術活用委員会

① 暗号の普及促進・セキュリティ産業の競争力強化に係る検討
② 暗号技術の利用状況に係る調査及び必要な対策の検討
③ 暗号政策の中長期的視点からの取組の検討

クラウド鍵管理ガイダンスWG

暗号技術活用委員会委員（2025年度）

CRYPTREC Cryptography Research and Evaluation Committees

（注）2025年5月時点

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　上席特別教授
委員	上原　哲太郎	立命館大学　教授
委員	垣内　由梨香	日本マイクロソフト　リスクマネージャー
委員	菊池　浩明	明治大学　教授
委員	佐藤　直之	SCSKセキュリティ株式会社　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	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長
委員	三澤　学	三菱電機デジタルイノベーション株式会社　グループマネージャー
委員	満塩　尚史	順天堂大学　准教授
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部門長

クラウド鍵管理ガイダンスWG委員

CRYPTREC Cryptography Research and Evaluation Committees

（注）2025年5月時点

主査	上原　哲太郎	立命館大学　教授
委員	漆嶌　賢二	GMOグローバルサイン株式会社　フェロー
委員	垣内　由梨香	日本マイクロソフト　リスクマネージャー
委員	菊池　浩明	明治大学　教授
委員	税所　達朗	さくらインタネット株式会社　特務
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	中島　智広	アマゾン ウェブ サービス ジャパン合同会社　Sr. Specialist Solutions Architect, Security
委員	畠中　亮	デジタル庁　ユニット長
委員	舟木　康浩	タレスDIS株式会社　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　課長代理
委員	満塩　尚史	順天堂大学　准教授

目次

1. 暗号技術活用委員会　概要

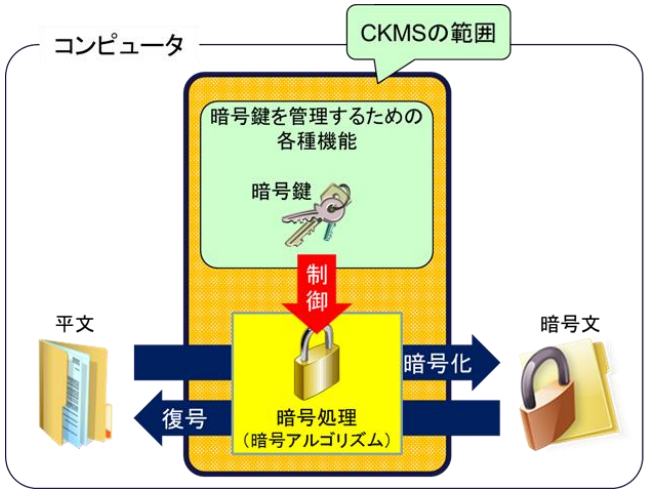
2. 暗号技術活用委員会　2024年度の活動概要と2025年度の活動計画
   - 暗号鍵管理ガイダンスPart 2の作成
   - クラウドにおける鍵管理ガイダンスの検討
   - 暗号技術活用委員会　2025年度活動計画

3. 暗号鍵管理ガイダンスWG　2024年度の活動概要
クラウド鍵管理ガイダンスWG　2025年度の活動計画
   - 暗号鍵管理ガイダンスPart 2の作成
   - クラウド鍵管理ガイダンスWG　2025年度活動計画

「暗号鍵管理システム設計指針（基本編）」とは

あらゆる分野／領域の暗号鍵管理システム（CKMS）を対象に
暗号鍵管理を安全に行うための構築・運用・役割・責任等に関する
対応方針として考慮すべき検討事項（Framework Requirements）を網羅的にカバーする指針

- イントロダクション：「鍵管理」の在り方／考え方の解説
- 技術的な中身： NIST SP800-130*の理解を深める利用手引き
  - NIST SP800-130の Framework Requirements を『暗号鍵管理における目的に応じた』対象範囲に分類・整理することによって検討すべき項目の目的や必要性を明確化
    - NIST SP800-130：A Framework for Designing Cryptographic Key Management Systems



- セキュリティ要求事項は定義せず、特定のセキュリティ機能を義務づけない
  - どのように要求事項に対応するか → 設計者に委ねられる
  - 対応方針が適正かどうかの判断　→ 運用管理者や調達責任者が行う

「暗号鍵管理ガイダンス」とは

「暗号鍵管理システム設計指針（基本編）」の解説書

- 「設計指針（基本編）」に基づいて暗号鍵管理プロファイルを作成するためのガイダンス
- 暗号鍵管理で必要となる検討項目について、シンプルなモデル（トイモデル）を例示して説明

Framework Requirements
あらゆるケースにおける鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として考慮すべき事項一覧の提示

Profile Requirements
Framework Requirementsに沿い、セクタ固有の特性／環境も考慮してセクタ内で共通に実現すべき要求事項（設計方針・運用要件等）を規定

System Requirements
Profile Requirementsに適合するようにシステム個別の環境／条件を考慮して実際のシステムが実現すべき具体的な設計仕様書や運用マニュアル等を作成

暗号鍵管理
システム設計指針
（基本編）

2020年7月公開

参照プロファイル

反映

設計仕様書
運用マニュアル
セキュリティポリシー

反映

チェックリスト

設計指針の解説や考慮点の提示
チェックリスト記載の例示

チェックリスト

暗号鍵管理
ガイダンス

2023年5月公開
(Part 1)

2025年4月公開
(Part 2)

暗号鍵設定ガイダンス

- セキュリティ強度選択
- 暗号鍵タイプ選択
- 暗号鍵保護要件
- 暗号鍵ライフサイクル
- 危殆化時のBCP対策
- 移行対策の必要性

暗号鍵の鍵長や運用方針を決定

「暗号鍵管理ガイダンス」の概要

■ 位置づけ

- 「暗号鍵管理システム設計指針（基本編）」を詳しく解説し、記載が求められる項目について検討する際の**有用な副読本**となることを目的とする。
  具体的には、「暗号鍵管理システム設計指針（基本編）」で記載されている項目に関して、各検討項目についての**解説・考慮点を具体的に説明**する。
- 理解を助けるため、**シンプルなモデル（トイモデル）を例示**し説明する。
  - トイモデルを用いた説明では、鍵管理における**要求や思想が理解できるような記載**を行う。
    （**※“推奨しているわけではない”ことに注意**）

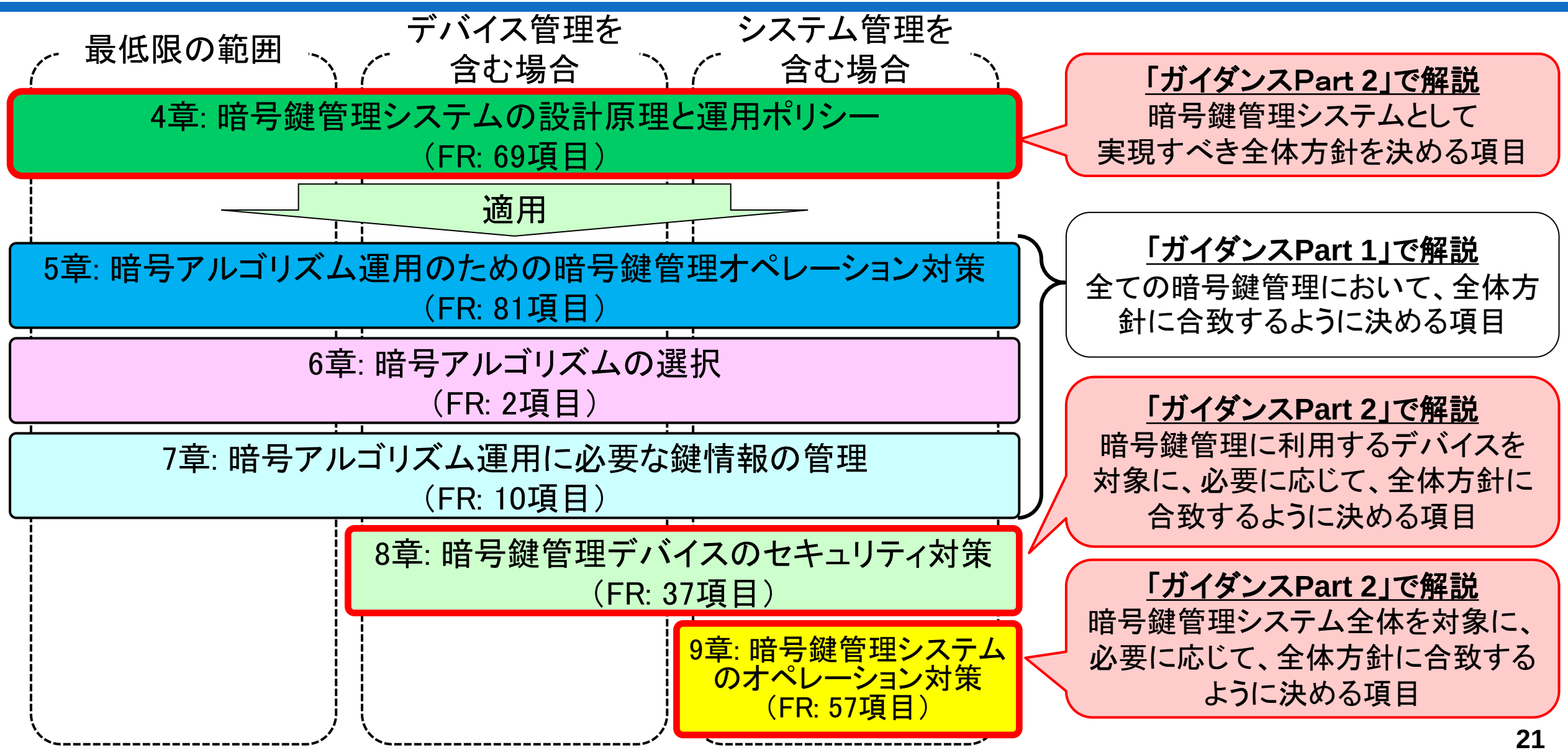
■ 想定読者

- 暗号鍵管理機能を有するシステムの設計者

■ 構成

- 「Part 1（2022年度作成）」と「Part 2（2024年度作成）」の分冊構成

「暗号鍵管理システム設計指針（基本編）」の構成及びガイダンスとの対応

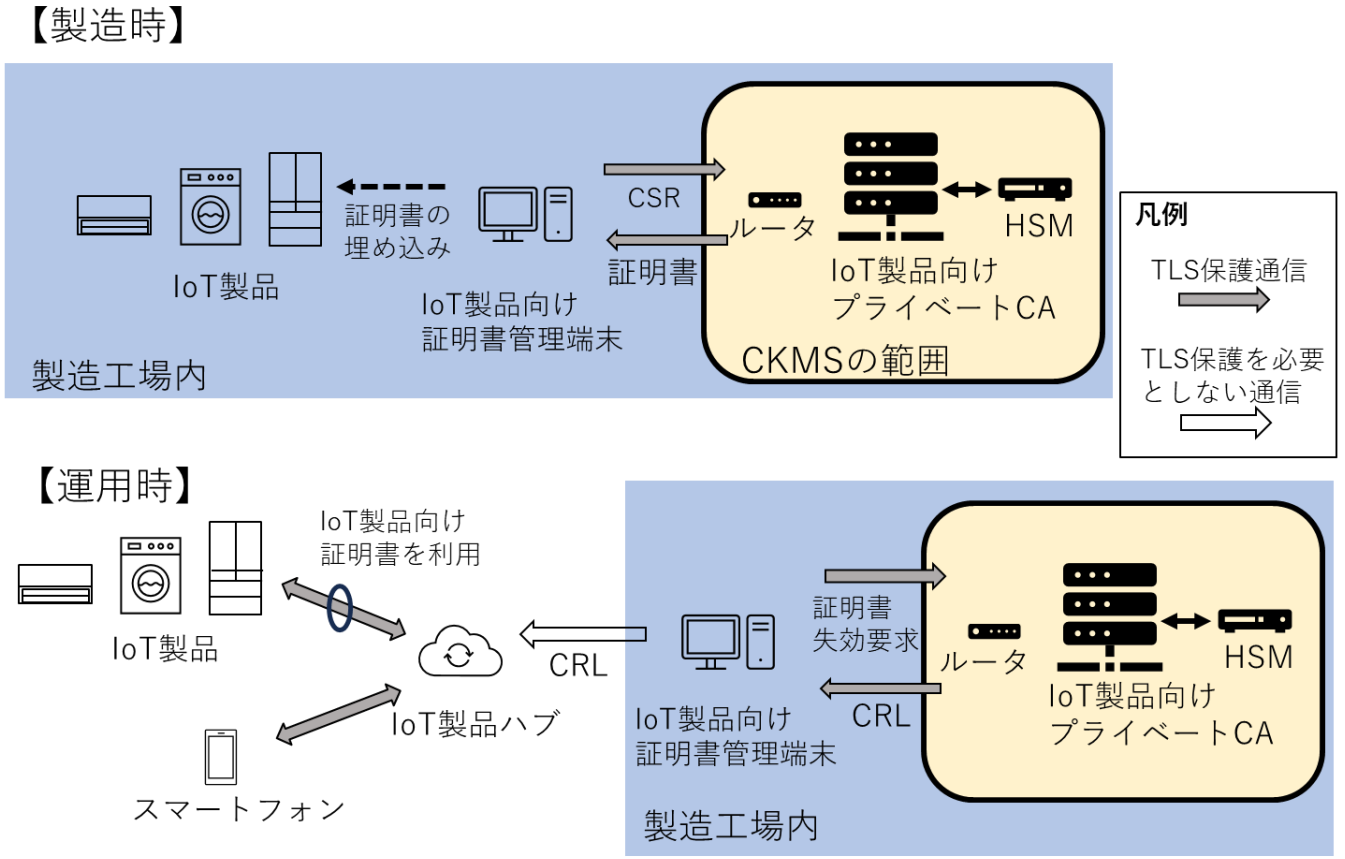


[Part 2] トイモデル（1.4節）

- IoT製品（家電想定）向けのプライベートCAシステムを設定。
  CKMSの範囲はCAサーバ、HSM（Hardware Security Module）、ルータとする。

- プライベートCAシステムはIoT製品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。
  IoT製品は、製品向けに発行された証明書を利用してIoT製品ハブとの通信を確立し、スマートフォン内の専用アプリもIoT製品ハブと別途通信を確立する。
  これら2つの通信をIoT製品ハブが仲介することにより、IoT製品とスマートフォン間の保護された通信が実現される。



[Part 2] 2章　暗号鍵管理システムの設計原理と運用ポリシー

CKMS設計において実現すべき全体方針を定める

- 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

→ CKMSのセキュリティポリシー
（CKMSセキュリティポリシー、他の関連するセキュリティポリシー）

- 2.4 CKMSにおける役割と責任
- 2.5 CKMSの構築目標及び実現目標
- 2.6 標準・規制に対する適合性

→ CKMSの概要設計
（エンティティと権限の定義、構築目標、関連する標準・規制）

- 2.7 将来的な移行対策の必要性★

→ 将来の移行対策
（暗号アルゴリズムや鍵管理デバイスの移行、技術の進歩に起因する課題評価）

★：記載概要を後続シートでピックアップ

2.7 将来的な移行対策の必要性

① 使用中の暗号アルゴリズムは、必要なときに拡張又は置き換えができるように実装することを検討しておかなければならない。
② 技術の進歩に起因する潜在的な脅威についても考慮しておかなければならない。(暗号アルゴリズムに対する攻撃，鍵確立プロトコルに対する攻撃，デバイスに対する攻撃，量子コンピュータ)

「設計指針」の見出し（FRの目的）

解説・考慮点

① 採用した暗号アルゴリズムのセキュリティライフタイムを超えてCKMSサービスを提供する必要がある場合には、鍵長の変更や暗号アルゴリズムの変更が要求される。
鍵長や暗号アルゴリズムをより強度の高いものに移行するための具体的な方法としては、予め複数の鍵長や暗号アルゴリズムをサポートした製品を採用する、暗号製品のベンダが提供するソフトウェアアップデートによって移行する、及び暗号処理を担う製品自体を置き換えるなどが存在する。

② 長期の利用が想定されるCKMSでは、採用した暗号技術に対して新たな攻撃が発見される等の理由により、当初想定していた以上のペースでセキュリティ強度の低下が生じる可能性がある。
長期の利用が想定されるCKMSでは、関連し得る技術の進歩を常に監視すると共に、潜在的な脅威への備えをしておく必要がある。
具体的には、上記に挙げる4つの脅威を例とする潜在的な脅威が現実となった場合の影響評価等を予め実施することを推奨する。

トイモデルでの記載例

② 当該CKMS設計において、CKMS及び各サブモジュールは極力シンプルに作られており、外部アプリケーションとの依存関係も極めて少ない。
暗号解読可能な量子コンピュータの実現可能性が高まった場合には、耐量子計算機暗号アルゴリズムをサポートしたHSM及びそれを含むCKMSへの置き換えを検討する。

② 当該CKMSの設計時のライフタイムは10年である。
この期間で暗号解読可能な量子コンピュータが実現されることは、現在の技術水準、及び、これまでの量子コンピュータの発展状況に鑑みると、非常に困難と考えられる。
また、そのような量子コンピュータの実現を仮定した場合でも、本IoT製品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、過去の通信データを保存しておき後で解読する「ハーベスト攻撃」特有の脅威は小さい。

[Part 2] 3章　暗号鍵管理デバイスへのセキュリティ対策

暗号鍵管理デバイス（暗号モジュール）に対する検討項目を定める

- 3.1 鍵情報へのアクセスコントロール
  - アクセスコントロールシステム★
  - 暗号モジュール
  - 人間による入力のコントロール
  - マルチパーティコントロール

} 鍵情報へのアクセスコントロール及び暗号モジュールによる保護

- 3.2 セキュリティ評価・試験
  - 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

} CKMSシステム及びデバイスに対するセキュリティ評価・試験

- 3.3 暗号モジュール障害時のBCP対策

} 障害発生に対する検知・回復

★：記載概要を後続シートでピックアップ

3.1　鍵情報へのアクセスコントロール

3.1.1 アクセスコントロールシステム

① アクセスコントロールへの要求事項を決めなければならない。

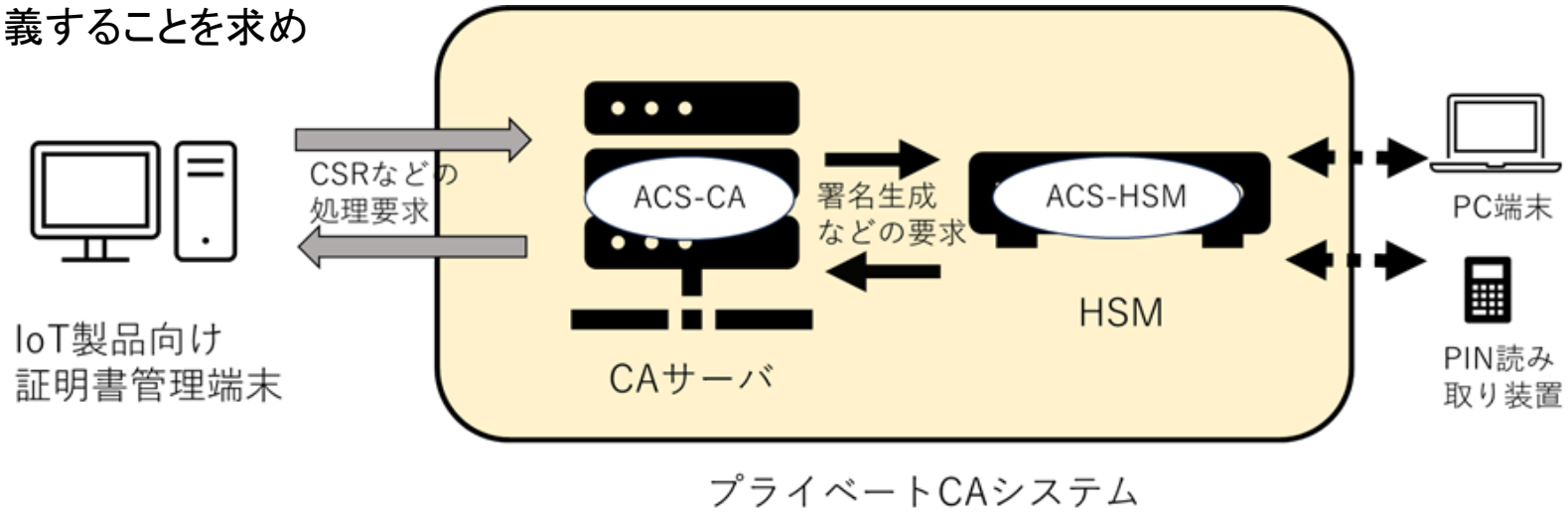
「設計指針」の見出し（FRの目的）

解説・考慮点

- CKMSのセキュリティは、鍵情報の管理機能が適切に設定され、認可されたエンティティからの要求のみに対応して鍵情報を利用した各種処理が実行されることによって担保される。
  アクセスコントロールシステム（ACS）はエンティティの認証や認可された処理の実行許可を与える機能モジュールであり、本節はCKMSが備えるACSを定義することを求めている。

トイモデルでの記載例

- 本プライベートCAシステムにおけるACSはCAサーバとHSMの2つ（ACS-CAとACS-HSM）がある。
  ACSのトポロジーは下図を参照。



3.1　鍵情報へのアクセスコントロール（続き）

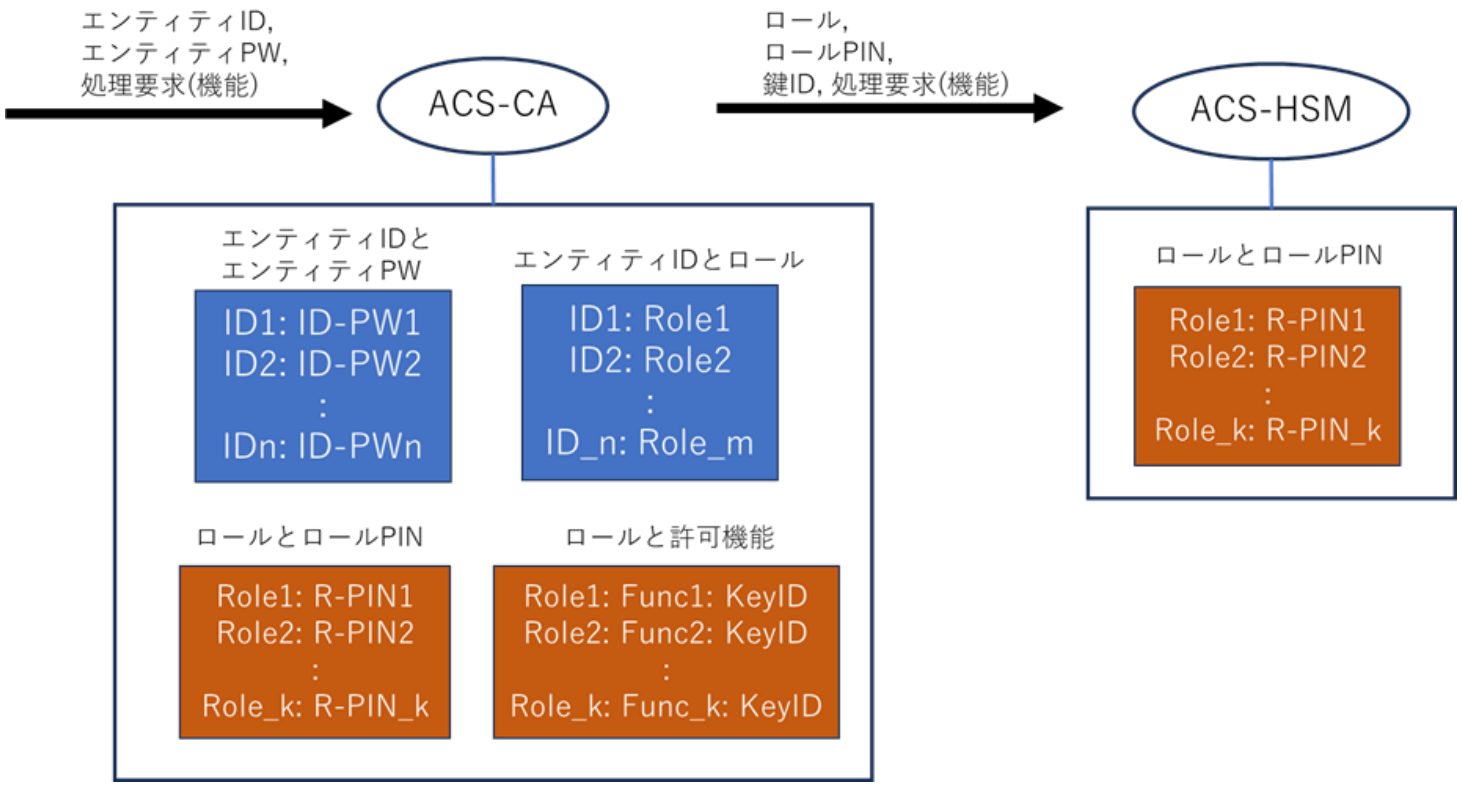
3.1.1 アクセスコントロールシステム（続き）

① アクセスコントロールへの要求事項を決めなければならない。

「設計指針」の見出し（FRの目的）

トイモデルでの記載例

- 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右図を参照。
- 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。



[Part 2] 4章　暗号鍵管理システムのオペレーション対策

暗号鍵管理システム全体に対する多層防御などの検討項目を定める

- 4.1 CKMSへのアクセスコントロール
  - 物理セキュリティコントロール★
  - コンピュータシステムセキュリティコントロール
  - ネットワークセキュリティコントロール
- 4.2 システム保証
  - 構成管理、配送、開発及びメンテナンス環境、欠陥修正能力

} CKMS全体に対する包括的なセキュリティ対策

- 4.3 セキュリティアセスメント
  - 完全アセスメント、定期的レビュー、追加アセスメント、メンテナンス

} CKMS全体のセキュリティアセスメント

- 4.4 CKMSへのアクセスコントール危殆化時のBCP対策
- 4.5 CKMS設備への障害・災害発生時のBCP対策

} CKMS全体への危殆化・障害・災害発生に対する検知・回復

★：記載概要を後続シートでピックアップ

4.1 CKMSへのアクセスコントロール

4.1.1 物理セキュリティコントロール

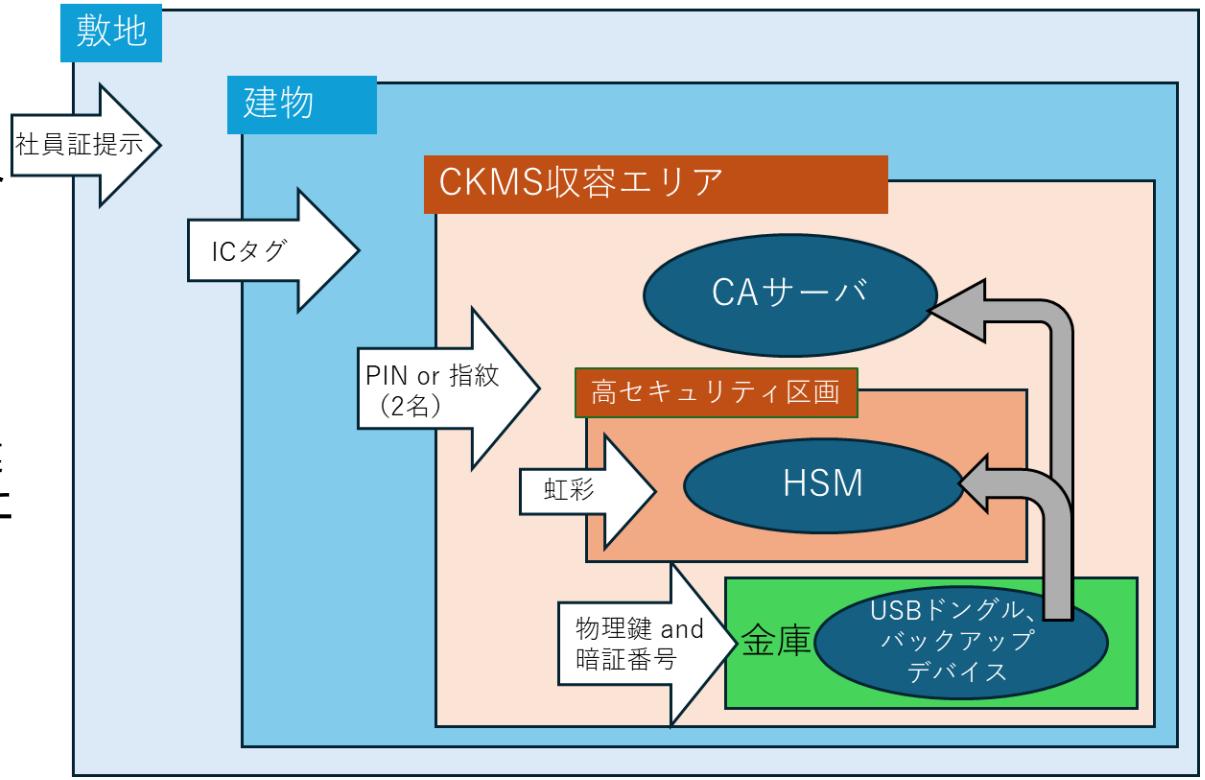
① CKMSコンポーネント及びデバイスに対する物理セキュリティの方法を決めなければならない。 **「設計指針」の見出し（FRの目的）**

解説・考慮点

- CKMSにおける物理的セキュリティ保護メカニズムを整理することを要求している。
  CKMSを構成するデバイスやコンポーネントの盗難やすり替え、物理的攻撃による改ざん、物理的攻撃による内部の機微な情報へのアクセスなどを防ぐために物理的保護が実施される。
  暗号モジュール自体が物理的保護メカニズムを備えている場合もあるが、多層防御としてCKMS全体を収容する施設（ファシリティ）としての物理的保護メカニズムも構築される場面が多い。
- 一般に施設レベルの物理的セキュリティ保護メカニズムとして、複数の段階の保護が設けられる。
  ある段階の物理的保護を解除するための認証情報や物理的鍵により、複数の段階の物理的保護を解除できることがないように保護メカニズムを構築することが重要である。

トイモデルでの記載例

- トイモデルで実施されている物理アクセスコントロールを下図に示す。



クラウド鍵管理ガイダンスWG 2025年度の活動計画

- 活動目的と目標
  - 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「クラウド鍵管理ガイダンス」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ことを活動の目的とする。
  - 遅くとも2026年度末までにガイダンスの完成を目標とする。
  - 本ガイダンスに続いて検討すべき内容も並行して議論する。

- 2025年度活動計画：クラウドにおける鍵管理ガイダンスの骨子作成
  - 2025年度はクラウドサービスとして提供される鍵管理システムを理解するために必要な知識を整理する。
  - ガイダンスの目次案を定め、記載の骨子となる資料を作成する。

おわりに

■ 2024年度暗号技術活用委員会／暗号鍵管理ガイダンスWGの活動報告・成果物

- CRYPTREC Report 2024　暗号技術活用委員会報告
  https://www.cryptrec.go.jp/report/cryptrec-rp-3000-2024.pdf

- 暗号鍵管理ガイダンスPart 2
  https://www.cryptrec.go.jp/report/cryptrec-gl-3005-1.0.pdf

https://www.cryptrec.go.jp/