暗号鍵管理ガイダンス Part 2

～暗号鍵管理システム設計指針の理解を助ける副読本～

Ver. 1

作成

CRYPTREC
Cryptography Research and Evaluation Commitees

発行

IPA 独立行政法人情報処理推進機構
セキュリティセンター

本書は、以下の URL からもダウンロードできます。

「暗号鍵管理ガイダンス」
https://www.ipa.go.jp/security/crypto/guideline/ckms.html

CRYPTREC GL-3005-1.0

暗号鍵管理ガイダンス

Part 2

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

目次

【修正履歴】

修正日	修正内容
2025.4.25	第 1 版公開

1 はじめに

1.1 位置づけ

企業や個人の管理する情報を保護するために暗号アルゴリズムが広く利用されている。各暗号アルゴリズムは、それぞれの情報が必要とする機密性、完全性、認証を提供する目的で利用される。

デジタル庁と総務省、経済産業省は、暗号技術に関する有識者で構成される CRYPTREC 活動を通して、電子政府で利用される暗号技術の評価を行っており、2023 年 3 月に「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」を改定した。CRYPTREC 暗号リストは、安全性、実装性能及び市場における利用実績を踏まえ、「電子政府推奨暗号リスト」、「推奨候補暗号リスト」及び「運用監視暗号リスト」で構成される。

CRYPTREC 暗号リスト（電子政府推奨暗号リスト）：
https://www.cryptrec.go.jp/list.html

実際、「政府機関のサイバーセキュリティ対策のための統一基準（令和 5 年度版）[1]」（令和 5 年 7 月 4 日、サイバーセキュリティ戦略本部。以下、「統一基準」という）では、政府機関における情報システムの調達及び利用において、図 1-1 のとおり、CRYPTREC 暗号リストのうち「電子政府推奨暗号リスト」に記載された暗号アルゴリズムを原則的に利用するように記載されている。このように、セキュアな暗号アルゴリズムの選択に関しては電子政府推奨暗号リストを活用する等により、比較的容易に満たすことができる。

しかしながら、実際のシステムがセキュアに動作し続けるためには暗号アルゴリズム自体がセキュアであるだけでは不十分である。統一基準でも暗号鍵の管理手順を定めることになっているように、データが保護される期間中、その暗号アルゴリズムが使用する暗号鍵もセキュアに管理されている必要がある。もし、暗号鍵がセキュアに管理されていなければ、管理が不十分な点を悪用した何らかの手段で暗号鍵が漏えいする可能性があり、その漏えいした暗号鍵を使ってシステムへの侵入、機密データの窃取や改ざん、なりすましなどが行われる。

一般に、暗号鍵管理の脆弱性を突く攻撃方法のほうが、セキュアな暗号アルゴリズム自体を解読するよりもはるかに容易な攻撃方法である。また、漏えいまでは至らなくても、暗号鍵にデータ不整合等が発生すればシステムエラーの原因となり、業務が停止するなどの悪影響が発生する場合もある。実際、セキュアな暗号アルゴリズムを利用していても、不十分な暗号鍵管理が原因となって、数多くのインシデントが発生している。

[1] 内閣サイバーセキュリティセンター（NISC）, https://www.nisc.go.jp/pdf/policy/general/kijyunr5.pdf

7.1.5 暗号・電子署名

遵守事項

(1) 暗号化機能・電子署名機能の導入

(a) 情報システムセキュリティ責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の全ての措置を講ずること。

(ア) 要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性 の有無を検討し、必要があると認めたときは、当該機能を設けること。

(イ) 要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を 行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機 能を設けること。

(b) 情報システムセキュリティ責任者は、**暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」に基づき**、情報システムで使用する暗号及び電子署名のアルゴリズム及び鍵長並びにそれらを利用した安全なプロトコルを定めること。また、その運用方法について実施手順を定めること。

(c) 情報システムセキュリティ責任者は、機関等における暗号化及び電子署名のアルゴリズム、鍵長及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な公的な公開鍵基盤が存在する場合はそれを使用するなど、目的に応じた適切な公開鍵基盤を使用するように定めること。

図 1-1　政府機関のサイバーセキュリティ対策のための統一基準（抜粋）

さらに、暗号鍵管理はうまく利用すると、大規模なデータ管理をセキュアに実現することも可能になる。例えば、クラウドサービスなど、外部の第三者にデータを預ける場合であっても、それらのデータを暗号化し、そのときの暗号鍵管理を利用者側が実施することで、クラウドサービス事業者に対しても機密性を維持できる。また、データセンターや大規模な記録メディアなどに保存されたデータで、物理的な破砕によるデータの完全削除を実現することが困難なケースでは、暗号鍵の破壊によって当該鍵で暗号化されたデータを事実上復号できなくすることでそれらのデータが完全に削除されたとみなす暗号化消去（Cryptographic Erase）といった方法を実現することもできる。

このような背景のもと、CRYPTREC では暗号鍵管理に関するガイドライン／ガイダンスを作成している。

- 暗号鍵管理システム設計指針（基本編）[2]
- 暗号鍵設定ガイダンス[3]

[2] https://www.cryptrec.go.jp/op_guidelines.html
[3] https://www.cryptrec.go.jp/op_guidelines.html

- 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[4]

このうち、「暗号鍵管理システム設計指針（基本編）」（以下、「設計指針」と呼ぶ）は、暗号鍵管理システム（以下、「CKMS (Cryptographic Key Management System)」という）を設計・構築・運用する際に参考すべきドキュメントとして作成されたものであり、「暗号鍵管理についての技術的内容」について解説している。具体的には、あらゆるユースケースにおける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事項一覧を提供し、CKMS 設計時に考慮すべきトピックス及び設計書等に明示的に記載する要求事項を示している。これは、CKMS の包括的な設計指針であり、CKMS 設計時に考慮すべきトピックス及び設計書等に明示的に記載する要求事項を列挙した NIST SP 800-130「A Framework for Designing Cryptographic Key Management Systems」をベースに作成されている。

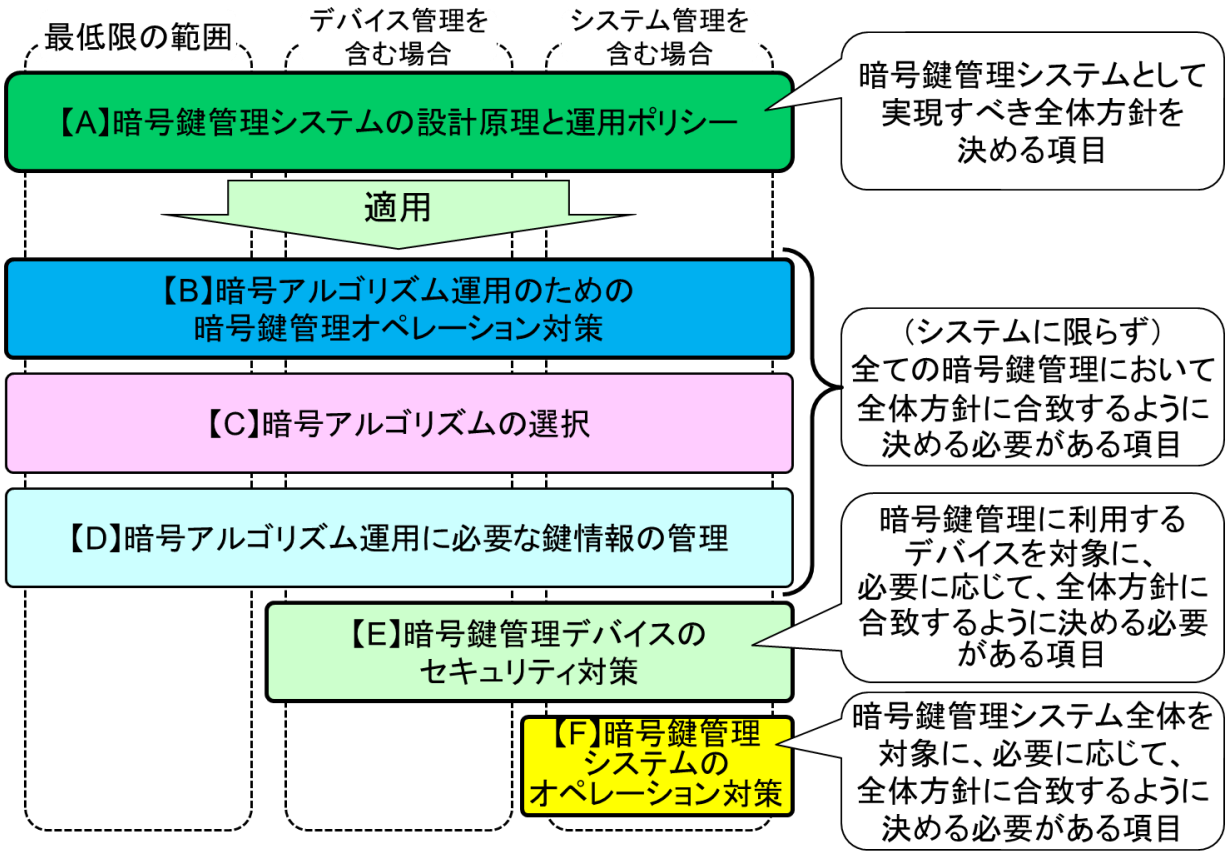


図 1-2　暗号鍵管理における目的別分類関係（「暗号鍵管理システム設計指針」より）

本書である「暗号鍵管理ガイダンス」は、「設計指針」で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して書かれたものである。本ガイダンスは Part 1 と Part 2 の 2 部構成となっている。

[4] https://www.cryptrec.go.jp/list.html

ガイダンス Part 1（2023 年 5 月発行）では、図 1-2 において、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の【B】、【C】、【D】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。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ことに留意されたい。

ガイダンス Part 2（本書）では、図 1-2 における【A】、【E】、【F】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。【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。【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、【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。【E】や【F】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 1-2 における【A】から【F】は、それぞれ順に「設計指針」の 4 章から 9 章に対応している。これらの「設計指針」の 4 章から 9 章についてはガイダンス Part 1 及び Part 2 においてより詳細を解説している[5]が、「設計指針」の 1 章から 3 章にイントロダクションとして記載されている内容については本ガイダンスに十分な記載をしていない。特に、「設計指針」の 2 章「暗号鍵管理の在り方」及び 3 章「本設計指針の活用方法」については、暗号鍵管理に責任を有するあらゆる担当者を想定読者とした内容であり、「設計指針」に基づいて CKMS を検討する際の基本的な事項を説明している。本ガイダンスと併せて「設計指針」の該当章を参照いただきたい。

上記のように、本ガイダンス Part 2 は、「設計指針」及びガイダンス Part 1 と併せて利用することを想定している。また、「暗号鍵管理システム設計指針（基本編）チェックリスト[6]」を利用する際には、以降に説明するトイモデルの記載例が参考となる。

1.2 想定読者

「設計指針」の 4 章以降に対する想定読者と同様であり、主として CKMS 設計者を想定読者としている。

1.3 構成

本ガイダンス Part 2 は、4 章で構成されており、章立ては以下のとおりである。

1 章は「はじめに」として、本ガイダンスの位置づけや想定読者を説明し、さらに本ガイダンスにおいて、各章の理解を助けるために設定した簡単なシステム（トイモデル）について説明する。トイモデルは、そこで設定された構成や運用条件などを踏まえて各章における項目に対する記載例を示すために導入したものである。

---

[5] 本書の 2 章以降において灰色枠内で囲った箇所は、「設計指針」該当部分の記載内容を転記したものである。

[6] IPA, https://www.ipa.go.jp/security/crypto/guideline/ckms.html

【トイモデルにおける注意】

ここでのトイモデルの構成や運用条件は、これらの内容と各々の項目における記載例との対応関係が“理解しやすくなる”ように設けたものであり、これらの内容を“推奨しているわけではない”ことに十分に注意されたい。

2 章は「暗号鍵管理システムの設計原理と運用ポリシー」における項目についての解説・考慮点を記載し、トイモデルでの記載例を示す。

同様に、3 章では「暗号鍵管理デバイスへのセキュリティ対策」における項目についての解説・考慮点を記載し、トイモデルでの記載例を示す。

最後に、4 章では「暗号鍵管理システムのオペレーション対策」における項目についての解説・考慮点を記載し、トイモデルでの記載例を示す。

なお、「設計指針」に述べているように、本ガイダンスにおいて各節のトピックスで対象とする Framework Requirements の目的を「①、②、…」として記載している。CKMS 設計者は、この目的及びそれに続く解説に照らし合わせて、個々のトピックスが今回設計する CKMS で検討する必要がある範囲であるかどうかの判断を行う。対象範囲と判断すれば Framework Requirement ごとにどのような対応をとるかを決定する。一方、対象範囲外と判断すればそのように判断した理由を明記したうえで当該 Framework Requirement は「対象外」として除外する。

さらに、対象範囲と判断した Framework Requirement であっても、ベンダから商用既製品として調達するデバイスやコンポーネントについては機能要件を定めることでよく、その機能の詳細に関わるものは、CKMS 設計者や調達者がその仕組みまでを確認するのではなく、ベンダに情報提供を求めることでよい。ベンダからの情報提供が得られないものは対象外としてもよい。

1.4 トイモデル

本書における CKMS のトイモデルは、図 1-3 に示す、IoT 製品向けに公開鍵証明書を発行するプライベート CA システムとする。ここでの IoT 製品としては家電製品を想定する。

このシステムの CKMS の設計範囲は、図 1-3 のとおり、CA サーバ、HSM（Hardware Security Module）[7]、及びルータまでとする。プライベート CA の主要機能は、IoT 製品向け証明書の発行及び証明書の失効処理である。IoT 製品利用者にとって、証明書のトラストアンカーは本プライベート CA となる。

CKMS の提供機能に関わる IoT 製品や製造工場内の機器と動作の概要を説明する。CKMS 外部の IoT 製品向け証明書管理端末は、プライベート CA に対して CSR（Certificate Signing Request）による IoT 製品向け証明書の発行の送出、及び証明書の失効要求の送出を行う。IoT 製

[7] HSM を利用しない CA システムを構築することも可能である。その場合は、HSM に代わる暗号鍵の保護に関する様々な対応が求められるため、本ガイダンスでは HSM を利用するトイモデルとした。

品向け証明書管理端末とプライベート CA は同じ IoT 製品の製造工場内に存在し、工場の計算機ネットワークに接続されている[8]。

IoT 製品の製造時に、プライベート CA は IoT 製品向け証明書管理端末からの要求を元に証明書を発行する。ここで、IoT 製品の ID 発番及びプライベート鍵生成を伴う ID 管理がプライベート CA 外部の IoT 製造環境で行われ、証明書の IoT 製品への埋め込みは製造工場内で行われる。

市場出荷後の IoT 製品は、当該製品の利用者の設定によってインターネット接続され、利用者のスマートフォン内の専用アプリから IoT 製品ハブを経由して当該製品の動作状態のセンシング及び設定や動作に関わる制御が行われる。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[9]。

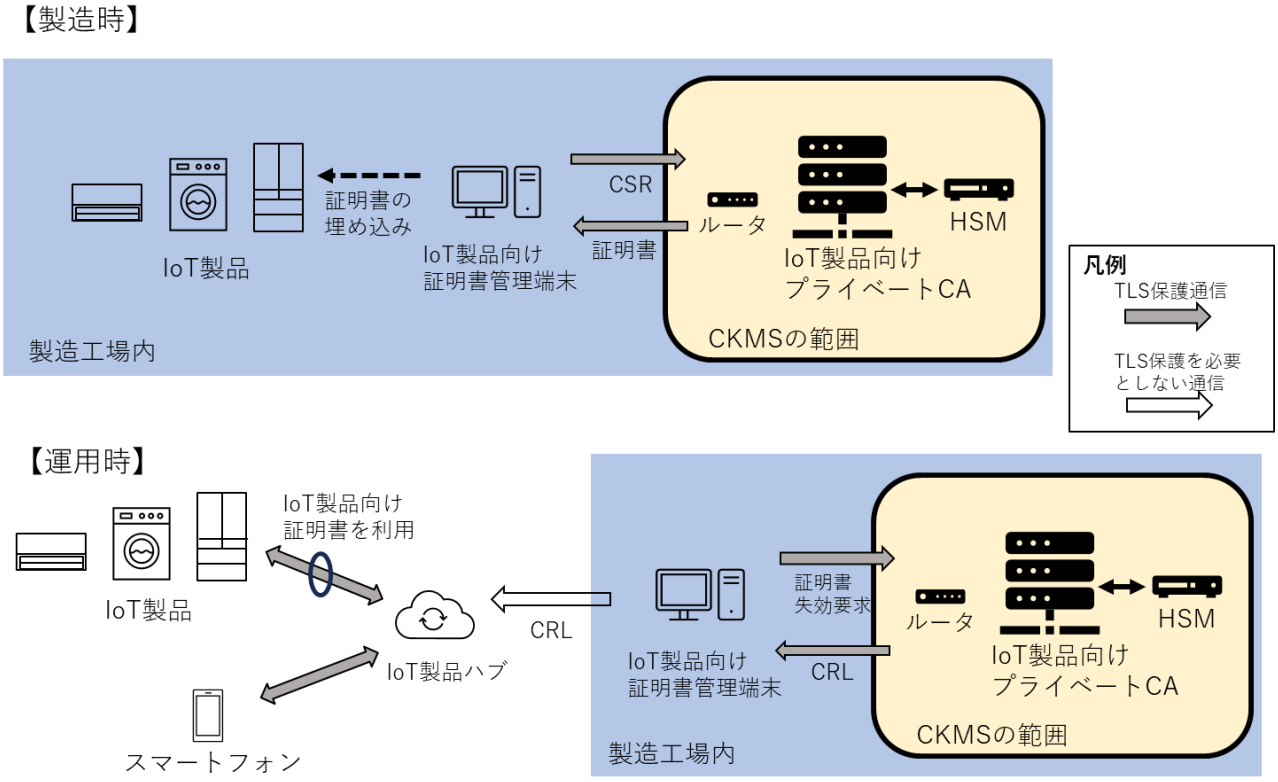


図 1-3 トイモデル（プライベート CA）の概要

出荷後の当該製品の運用中にセキュリティに関わる重大な事故が発生した場合や製品リコール時などに証明書の失効処理を行う場合がある。失効処理の対象となる IoT 製品の ID 管理も製造

[8] ASP（Application Service Provider）やクラウドサービス（SaaS）として CA 機能が提供される場合もあるが、本トイモデルではオンプレミスにプライベート CA を構築する想定であることに注意されたい。

[9] これらの通信の確立においては、IoT 製品及びスマートフォンアプリが IoT 製品ハブを認証するための情報や、IoT 製品ハブがスマートフォンの利用者を認証するための情報を用いることになるが、それらの情報を管理する機能は今回の CKMS 機能に含まれない。

工場内の環境で行われ、プライベート CA は IoT 製品向け証明書管理端末からの要求を元に CRL（Certificate Revocation List）を発行する。CRL は IoT 製品向け証明書管理端末から IoT 製品ハブに送られ、利用者は IoT 製品ハブにおいて証明書の失効状況を確認できる。

IoT 製品向け証明書管理端末とプライベート CA 間の証明書発行及び証明書失効に関わる通信は TLS を利用し、CSR や失効要求情報の改ざん防止及び送信元の認証が実施される。

以上から、本 CKMS が扱う鍵情報として、CA 証明書生成用の署名鍵・検証鍵、IoT 製品向けに生成された証明書が該当する。また、プライベート CA が IoT 製品向け証明書管理端末との通信を行う際の TLS 通信に用いられるサーバ証明書及びプライベート鍵も本 CKMS が扱う鍵情報に含まれる。ただし、本ガイダンスにおけるトイモデル記載例では、HSM で管理されている CA 証明書生成用の署名鍵を利用して発行される、IoT 製品向け証明書に関わる部分に注目している。プライベート CA と IoT 製品向け証明書管理端末との間の TLS 通信に必要となるサーバ証明書及びプライベート鍵については、当該プライベート鍵の保護に関わる事項の記載を省略している。

1.5 検討体制

本ガイダンス Part 2 は、2023 年度及び 2024 年度 CRYPTREC 暗号鍵管理ガイダンス WG において作成された。

表 1-1 暗号鍵管理ガイダンス WG の構成（2025 年 3 月時点）

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 CPL 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

2 暗号鍵管理システム（CKMS）の設計原理と運用ポリシー

本章の目的・趣旨

本章は、「設計指針」の 4 章に記載されている要求事項（各節での灰色枠内で示している内容）について解説したものである。

CKMS として実現すべき全体方針を取り決める項目（項目 A.01～A.69）を集めている。ここには、主に以下のような項目を含んでいる。

- CKMS をどのような方針（ポリシー）で運用するのか。そのために、どういった機能を用意しなければならないのか
- CKMS 参加者（責任者／管理者／運用者／ユーザ）が誰でどういった権限を有しているのか
- CKMS の構築環境や実現目標はどういったものか
- 適合しなければならない法規制や標準化等があるのか。あるならどういったものか
- 将来的な移行対策を準備しておく必要があるか。あるならどういった準備をするか

ここでの項目の検討結果が、他の章における項目での具体的な技術的選択や精緻化などに当たっての条件として適用される。

2.1 CKMS セキュリティポリシー

解説・考慮点

本節は、SP 800-130 の 4.3 節、4.4 節、4.5 節に記載されている事項について解説したものである。

CKMS は、CKMS を使用しているそれぞれの組織の目標をサポートするやり方で設計されなければならず、またそれぞれの組織が有するポリシー群とも整合させる必要がある。そのうちのいくつかのポリシーは CKMS の設計及び使用に影響を及ぼすため、まず CKMS 設計における設計原理と運用ポリシーを整理する必要がある。これは、CKMS セキュリティポリシーとして定義される。

① CKMS の設計にあたって、CKMS セキュリティポリシーを作成しなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.01	FR4.1	CKMS 設計は、実行するために設計した設定可能なオプションとサブポリシーを含む CKMS セキュリティポリシーを明記しなければならない。	4.3 節

A.02	FR4.2	CKMS 設計は、CKMS セキュリティポリシーが CKMS によってどのように実行されるのか（例えば、ポリシーが要求する保護を提供するために使用されるメカニズム）を明記しなければならない。	4.3 節

解説・考慮点

CKMS セキュリティポリシーは、情報管理ポリシー及び情報セキュリティポリシーに従ってデータを保護するために、CKMS がサポートしなければならないデータ、並びに鍵情報を保護するためのルールを規定するものである。
CKMS の設計にあたって、項目 A.01 は CKMS セキュリティポリシーを作成することを、A.02 はその CKMS セキュリティポリシーに明記すべき内容及びその実現・利用方法について明確化することを要求したものである。具体的には、以下のようなことが求められる。

- CKMS で使用される全ての鍵情報の機密性、完全性、可用性、及びソース認証（source authentication）を保護するためのルールを定める。
  - 鍵ライフサイクル全体にわたってカバーされなければならない。
  - CKMS が使用できる全ての暗号メカニズム及び暗号プロトコルの選択を含むこともある。
- 組織のより高位レベルのポリシー群（情報管理ポリシー及び情報セキュリティポリシー）と定めたルールが整合している必要がある。
- CKMS セキュリティポリシーに沿ってデータの保護を実行するために、いつどのようにセキュリティ機能が使用されるのかを文書化する。
- 教育・トレーニング等を通じて、各種ポリシーを役員・従業員が容易に理解して自らの役割及び責任を正しく実行できるように書かれるべきである。

なお、CKMS 設計において、CKMS セキュリティポリシーを適切にサポートしているか、又はサポートするように設定できるかどうかを保証・確認するのは、CKMS を使用する組織の責任である。

【参考】

- 情報管理ポリシーに明記すべき要件には、以下のようなものがある。
  a) 収集又は作成する情報、及び管理方法
  b) 情報を獲得及び利用するための高レベルの目標
  c) ポリシーに対する組織上の管理ルール及び責任
  d) 情報管理上の義務を実行するために要求される認可
  e) 認可されない開示（窃取）、改ざん、又は破壊に対して保護が必要な情報（保護対象の情報）のカテゴリ
  f) ポリシーを作成し、その実装と利用を管理するための権限を誰に与えるかのルール

- 情報セキュリティポリシーに明記すべき要件には、以下のようなものがある。

a) 機微と考えられる情報（保護対象の情報）のカテゴリ
b) 情報に関連するインパクトレベル
c) 情報に対する現時点で予測されている潜在的なリスク
d) 必要な保護を行うための方法
e) 情報を収集、保護及び配付するためのルール

- CKMS セキュリティポリシーに明記すべき要件には、以下のようなものがある。

a) ポリシーを適用する組織名称
b) ポリシーを承認／変更する権限を有する人（人物、役職、又は役割）
c) ポリシーに明記され、コントロールされる情報のインパクトレベル
d) 提供される主要なデータ及び暗号鍵／メタデータの保護処理（データ秘匿性、データ完全性、ソース認証）
e) サポートできるセキュリティ処理（例：個人の説明責任、個人のプライバシー、可用性、匿名性、連結不可能性、観測不可能性）
f) 暗号鍵及び関連付けられたメタデータに対する制限の影響及び取り扱い
g) 各々のインパクトレベル及び各々の保護サービスで利用されるアルゴリズム及び全ての関連パラメタ
h) 利用される各々の暗号アルゴリズムに対する鍵情報の期待される最大許容暗号鍵有効期間（この期間を超えて同一の鍵情報（暗号鍵やメタデータ）が利用され続けてはならない）
i) 暗号鍵及び関連付けられたメタデータによって保護される各々の情報インパクトレベルに対するユーザ／役割及びソース認証の受け入れ可能な方法
j) 各々の情報インパクトレベルに応じた鍵情報に対するバックアップ、アーカイブ及び復元要求
k) サポートされる役割
l) 各々のインパクトレベルに対する鍵情報に対するアクセスコントロール及び物理的セキュリティ要件
m) 鍵情報を復元する手段とルール
n) 機微データ、及び鍵情報を保護する際の利用される通信プロトコル

CKMS の設計にあたって、項目 A.01 は CKMS セキュリティポリシー（CKMS のセキュリティを確保するための指針）を明文化することを要求している。CKMS セキュリティポリシーは CKMS の設計前に定めておくことが好ましいが、仮に CKMS が暗黙的なセキュリティポリシーに基づいて設計されていた場合、そのセキュリティポリシーを後からでも明文化することを項目 A.01 は要求している。

セキュリティポリシーは、当該システムを運用する主体により、その主体の事情に合わせて策定されるものであり、どの程度の粒度で規定するかは運用主体が決定するものとなる。セキュリティポリシーの作成方法についての文書も少ないながら存在し、RFC 3647（Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework）はその１つとなる。もっとも、RFC 3647 は CA のセキュリティポリシーに関する一般的なフレームワ

ークを記載するものであり、必ずしもその記載に則ってセキュリティポリシーを作成する必要はない。例えば、自社向けの小規模な CKMS に対して、簡略化したセキュリティポリシーを作成することは許容される。また、NIST SP 800-57 Part 2 には、組織が暗号鍵管理のポリシー（Key Management Policy）を作成する際に検討する内容とセキュリティポリシーを実現するための文書（Key Management Practice Statement）に書くべき内容のガイドが含まれている。

項目 A.02 はその CKMS セキュリティポリシーに明記された内容が、どのように実現されるかを記載したものとなる。例えば、セキュリティポリシーに「FIPS 140-2 レベル 3 を満たす HSM を FIPS モードで利用すること」と記載されていた場合に、具体的にどのメカニズム（暗号アルゴリズムや認証手法等）を、どのように利用するかを記載する。例えば、暗号アルゴリズムの標準名や、処理内容を記した仕様書等が存在する場合はその仕様書を指定する。ただし、項目 A.02 は詳細な仕様までを求めるものではなく、セキュリティポリシーを実現するためのメカニズムを概要レベルで記載することで良い。

《トイモデルと記載例》

本節のトイモデルは 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.01	当該 CKMS のセキュリティポリシーは RFC3647 に基づくパブリック CA の CP（Certificate Policy）や CPS（Certification Practice Statement）を参考に作成した。 セキュリティポリシーは<URI>に保存されている。
A.02	本プライベート CA において証明書や CRL に付与する署名の鍵生成や署名処理は、管理区域内に設置された FIPS 140-2/-3 の認証を取得した HSM によって実行する。管理区域への入室は CKMS 管理者権限のあるメンバに制限する。証明書の発行処理や失効処理の要求送出は CKMS 利用者権限のあるメンバに制限する。（以下略） CKMS メカニズムの仕様書は<URI>に保存されている。

② CKMS セキュリティポリシーは、他のセキュリティポリシーや組織の様々なポリシーに依存することがあるので、それらを意識しなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.03	FR4.4	CKMS 設計は、CKMS セキュリティポリシーをサポートする他の関連するセキュリティポリシーを明記しなければならない。	4.4 節
A.04	FR4.5	CKMS 設計は、CKMS 設計によってサポートされるポリシーと、その設計によってどのようにサポートされるのかの要約を明記しなければならない。	4.5 節

解説・考慮点

高位レベルのポリシー群（情報管理ポリシー及び情報セキュリティポリシー）以外にも、CKMS セキュリティポリシーをサポートする別のセキュリティポリシー（例：コンピュータセキュリティポリシー）があったり、CKMS セキュリティポリシー以外のセキュリティポリシー（例：CKMS モジュールセキュリティポリシー）が存在したりする可能性がある。

CKMS の設計にあたって、項目 A.03 は CKMS セキュリティポリシーをサポートする別のセキュリティポリシー（もしあれば）の情報について、A.04 は CKMS の適切でセキュアな運用を実行するために要求される CKMS セキュリティポリシー以外のセキュリティポリシー（もしあれば）の情報について明確化することを要求したものである。

上記①の解説・考慮点にも記載されているように、CKMS を運用する組織には CKMS セキュリティポリシー以外に様々なセキュリティに関わるポリシーが存在するのが一般的である。例えば、組織が取り扱う情報全般に対する情報管理ポリシー、組織内の情報セキュリティの維持管理に関わる情報セキュリティポリシー、さらに組織内のコンピュータシステムにおける全般的なセキュリティ対策などを定めたコンピュータセキュリティポリシーなどが該当する。これらのポリシーは階層構造などの依存関係を持って、相互に矛盾なく規定される。

CKMS セキュリティポリシーもこれらのポリシーとの関係を意識して定める必要がある。CKMS からみてより上位に位置づけられるポリシー（より汎用的なポリシー）もあれば、CKMS からみてより下位のポリシー（より具体的なポリシー）もある。上位のポリシーが変更された場合には、下位のポリシーの変更が必要となる可能性がある。

項目 A.03 及び A.04 はこうした CKMS 以外の関連するセキュリティポリシーを CKMS から見た依存関係を含めて一通り整理することを要求するものであり、項目 A.03 は CKMS セキュリティポリシーに依存する下位のセキュリティポリシーのリストを、項目 A.04 は関連する上位のセキュリティポリシーのリストを明らかにすることを要求している。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。本モデルでは、IoT 製品のセキュアな製造及びセキュアな運用などの管理手順を定めたポリシーが「IoT 製品製造管理及び運用管理ポリシー」として明文化されていることを想定している。同ポリシーにおける IoT 製品向け証明書の発行及び失効管理に関わるセキュリティポリシーを詳細化したものが当該 CKMS セキュリティポリシーとして位置づけられる。

一方、IoT 製品の製造時や運用時のセキュリティポリシーとプライベート CA のセキュリティポリシーとの間には、次のような依存関係があることに注意が必要である。プライベート CA のセキュリティポリシーに依存して IoT 製品のセキュアな製造や運用が担保されるが、逆に IoT 製品の製造や運用におけるセキュリティはプライベート CA のセキュリティには影響を及ぼさない。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.03	当該 CKMS セキュリティポリシーの下位に位置づけられるポリシーには以下のものがある。 ● HSM セキュリティポリシー
A.04	当該 CKMS セキュリティポリシーの上位に位置づけられるポリシーには以下のものがある。 ● 情報管理ポリシー ● 情報セキュリティポリシー ● コンピュータ及びネットワークセキュリティポリシー ● IoT 製品製造管理及び運用管理ポリシー

③ CKMS セキュリティポリシーが CKMS 内に電子的に保管され自動的に処理される場合には正しい処理が行われるように注意をしなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.05	FR4.3	CKMS 設計は、CKMS セキュリティポリシーのあらゆる自動化部分についてどのように曖昧さのない表形式又は形式言語（例えば XML、ASN.1）で表現されているのかを明記しなければならない。CKMS の自動化されたセキュリティシステム（例えば table driven 又は syntax-directed software mechanisms）がそれらを実行できるようにするためである。	4.3 節

解説・考慮点

CKMS セキュリティポリシーが自動処理される場合、その内容が正しく処理されるように正確に表現されていなければならない。

項目 A.05 は、CKMS の設計にあたって、CKMS セキュリティポリシーが自動処理される場合の CKMS セキュリティポリシーの表現手法について明確化することを要求したものである。なお、自動処理される部分がなければ対象外の項目である。

例えば、X.509 証明書においては「証明書ポリシー拡張」が存在し、拡張を閲覧することにより対象となる主体に対応するポリシーを確認することが可能となる。その拡張を参照して、所定のポリシーを満たすか否かの判断が自動的に行われるような場合は、その旨を記載することとなる。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.05	当該 CKMS のセキュリティポリシーは、RFC 5280 に規定された X.509 v3 証明書の証明書ポリシー拡張にて、ポリシー識別子が ASN.1 DER 形式で記載される。証明書の検証処理において、当該拡張部のポリシー識別子の確認処理が実行される。

2.2 情報管理ポリシー等からの要求事項

解説・考慮点

本節は、SP 800-130 の 4.6 節、4.7 節に記載されている事項について解説したものである。

CKMS の設計にあたっては、CKMS セキュリティポリシーよりも上位のポリシー群から要求される事項が存在する場合がある。本節では、そのような上位のポリシー群から要求されることが多い事項を取り上げる。

① 機微な情報を管理するために、「個人の説明責任（Personal accountability）」について情報管理ポリシー等の要求事項に記載される場合には、どのように対応するかを決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.06	FR4.6	CKMS 設計は、個人の説明責任（personal accountability）が CKMS でサポートされるかどうか、及びどのようにサポートされるかを明記しなければならない。	4.6 節

解説・考慮点

「個人の説明責任」とは、ユーザが機微な情報にアクセスした行為が正当なものであることを保証することである。そのために、認可された範囲でのみ機微な情報にアクセスできることや、認可されないアクセスを検知・防御・管理者に通報することなどの機能を実現することが求められる。

項目 A.06 は、CKMS の設計にあたって、そのような機能を備えるかどうか、また備えるとすればどのように実現するのか明確化することを要求したものである。

個人の説明責任が要求される代表的な場面としては、監査及びリスクマネジメントがあげられる。例えば、複数の個人が行った一連のプロセスで事故や障害等が発生し、それらのインシデントが何かの個人のミス又は不適切な操作に起因する可能性が疑われるような状況において、各個人が自身の行った行動について説明を求められることがありうる。CKMS がその説明責任に応えることが可能となるように設計されているのであれば、その点について記載するべきというのが項目 A.06 の趣旨となる。また、より上位のポリシー等で説明責任が要求された場合も、項目 A.06 を参照することで、CKMS において説明責任を実現しているか否かの判断をすることができる。

個人の説明責任を果たす機能の具体例には、適切なアクセスコントロールの実施を可能とする設定ファイルやログファイル等が含まれる。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.06	当該 CKMS 設計は個人の説明責任をサポートする機能を備える。 CA サーバ及び HSM に対する各種処理の実行は、それぞれのアクセスコントロールによって権限を持つエンティティに制限されている。また、それらの各種処理やアクセスコントロールの設定及び変更の処理は、改ざん困難な実行ログに、実行時のエンティティ ID と共に記録される。

② エンティティに対するプライバシーの提供、関連法令の遵守、又はセキュリティ強化のために、「匿名性」「連結不可能性」「観測不可能性」（のいずれか）の保証について情報管理ポリシー等に記載される場合には、どのように対応するかを決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.07	FR4.7	CKMS 設計は、CKMS でサポートできる匿名性、連結不可能性（unlinkability）、及び観測不可能性（unobservability）に関するポリシーを明記しなければならない。	4.7 節
A.08	FR4.8	CKMS 設計は、どの CKMS トランザクションが匿名性保護を提供している、又は提供可能であるのかを明記しなければならない。	4.7.1 節
A.09	FR4.9	CKMS 設計は、匿名性の保証を提供する場合、CKMS トランザクションの匿名性保証をどのように達成するのかを明記しなければならない。	4.7.1 節
A.10	FR4.10	CKMS 設計は、どの CKMS トランザクションが連結不可能性（unlinkability）保護を提供している、又は提供可能であるのかを明記しなければならない。	4.7.2 節
A.11	FR4.11	CKMS 設計は、CKMS トランザクションの連結不可能性（unlinkability）をどのように達成するのかを明記しなければならない。	4.7.2 節
A.12	FR4.12	CKMS 設計は、どの CKMS トランザクションが観測不可能性（unobservability）保護を提供している、又は提供可能であるのかを明記しなければならない。	4.7.3 節

A.13	FR4.13	CKMS 設計は、CKMS トランザクションの観測不可能性（unobservability）をどのように達成するのかを明記しなければならない。	4.7.3 節

解説・考慮点

以下のセキュリティ特性はいずれもプライバシー保護に効果があるものである。

- 匿名性：パブリックなデータを所有者と関係付けることができないことを保証
- 連結不可能性：情報処理システムにおいて 2 つ以上の関連する事象を互いに関係付けることができないことを保証
- 観測不可能性：観測者がトランザクションに関係する当事者の識別子（ID）を特定又は推定することができないことを保証

項目 A.07～A.13 は、CKMS の設計にあたって、匿名性、連結不可能性、観測不可能性といったセキュリティ特性を実現するプライバシー保護機能を備えるかどうか、また備えるとすればどのように実現するのか明確化することを要求したものである。

なお、システムが扱う情報の種類によってはプライバシーを提供することが適切ではない場合もあり得る。そのようなシステムに対しては、「プライバシー保護機能を提供してはならない」という選択を行うことも容認される。

これらの要件は、典型的には個人情報保護法や GDPR 等の法令準拠の観点で CKMS に求められ得る。匿名性はトランザクションに関わる主体を特定することが困難な性質であり、連結不可能性は複数のトランザクションが同一の主体に関わるものであることを当人以外が判定することが困難な性質であり、観測不可能性はトランザクション自体を当人以外が観測することが困難な性質を指す。

CKMS がこれらの性質を持つことが可能であれば、その旨を明示し（項目 A.07）、その性質がどのように達成されるかを明記しなければいけない(項目 A.08-A.13)。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。当該 CKMS が発行する証明書には対象となる IoT 製品の ID が記載されるが、この ID がどのように割り振られるか、及び ID や証明書をどのように利用するかは、本 CKMS のスコープ外となる。そのため、IoT 製品の ID 自体を保護する機能（匿名性、連結不可能性、観測不可能性）についても当該 CKMS のスコープ外である。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.07	当該 CKMS 設計は、匿名性、連結不可能性、及び観測不可能性をサポートしない。
A.08	当該 CKMS 設計は、トランザクションの匿名性保護を提供しない。
A.09	対象外である。
A.10	当該 CKMS 設計は、連結不可能性保護を提供しない。

A.11	対象外である。
A.12	当該 CKMS 設計は、観測不可能性保護を提供しない。
A.13	対象外である。

2.3 ドメインのセキュリティポリシー

2.3.1 セキュリティドメイン

解説・考慮点

「設計指針」4.3.1 節では、セキュリティドメイン及びそのポリシー（セキュリティドメインポリシー）を以下のように説明している。

> セキュリティドメインとは、同じドメインのセキュリティポリシー下で運用されるエンティティ／CKMS の集合のことである。互いに信頼するエンティティが同じセキュリティドメインに属しているとき、両者はドメインのセキュリティポリシーが要求する保護を提供しながら鍵情報を交換できる。
> ドメインのセキュリティポリシーが要求する保護の保証には、以下を含む。
> - 鍵情報（暗号鍵やメタデータ）を認可されない開示（窃取）から保護すること
> - 鍵情報（暗号鍵やメタデータ）の認可されない改変（改ざん）から保護すること
> - アプリケーションに要求された際の鍵情報（暗号鍵やメタデータ）のソース（送信者）及びディスティネーション（受信者）を確認できること
>
> このようなセキュリティドメインの例には、公開鍵証明書を発行する PKI がある。

2.3.2 異なるセキュリティドメイン間での鍵情報の交換

① 異なるセキュリティドメイン間で鍵情報の交換が必要な場合には、それができるためのルールを決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.14	FR4.15	CKMS 設計は、同等だが異なるセキュリティ保護を提供するとみなせる他のセキュリティドメインに属するエンティティ間での鍵情報（暗号鍵及びメタデータ）の交換を許可する設計仕様を明記しなければならない。	4.9.1 節
A.15	FR4.16	CKMS 設計は、鍵情報（暗号鍵やメタデータ）を異なるセキュリティドメインに属するエンティティ間で共有するときに実施されるソース認証ポリシー（source authentication policy）とデスティネ	4.9.2 節

		ーション認証ポリシー（destination authentication policy）を明記しなければならない。	
A.16	FR4.17	CKMS 設計は、鍵情報（暗号鍵やメタデータ）を異なるセキュリティドメインに属するエンティティ間で共有するときに実施される機密性と完全性のポリシーを明記しなければならない。	4.9.2 節
A.17	FR4.18	CKMS 設計は、他のセキュリティドメインのエンティティと通信するときに要求される保証要件を明記しなければならない。	4.9.2 節
A.18	FR4.19	CKMS 設計は、ドメイン間通信が許可される前に他のドメインのセキュリティポリシーのレビューと検証をサポートするかどうか、またどのようにサポートするのかを明記しなければならない。	4.9.3 節
A.19	FR4.20	CKMS 設計は、弱いポリシーを持つセキュリティドメインのエンティティとの通信がもたらす潜在的なセキュリティに関する影響をどのように検知、防止、又はエンティティに警告するのかを明記しなければならない。	4.9.3 節

解説・考慮点

2 つのエンティティが異なるセキュリティドメインに属しているとき、それらのエンティティは異なるドメインのセキュリティポリシーの下で運用されているため、交換した鍵情報に対して同等の保護を提供することができない可能性がある。

そのため、提供されるセキュリティ保護に関して、それぞれのセキュリティドメインに責任を持つオーソリティ（authority）が他方のセキュリティポリシーを自分自身のポリシーと同等であるかどうかを判断し、互いのエンティティが同等（ただし、同一ではなく異なる場合もある）のセキュリティポリシーであると承認した場合、他方のドメインに属するエンティティともデータ共有が可能となる。もし弱いセキュリティポリシーを持っているセキュリティドメインであると判断した場合には、あらゆる潜在的な危殆化の影響を軽減するために、鍵情報の交換を制限又は拒否することもある。

なお、共有した鍵情報は、他の同等のセキュリティドメインとも共有され得る（第三者共有）と認識しておく必要がある。

項目 A.14～A.19 は、CKMS の設計にあたって、異なるセキュリティドメイン間での鍵情報の交換が必要な場合に、互いのセキュリティポリシーの検証方法や、鍵情報を交換するための手順等を明確化することを要求したものである。なお、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の項目である。

異なるセキュリティドメイン間で鍵情報を交換する場合は、本節で述べるような様々な配慮が必要となる。そのため、その必要性が特にない場合においては、異なるセキュリティドメイン間での鍵交換を行わない、又は禁止することが一般的なアプローチとなる。

一方で、多数のステークホルダが関与するセキュリティシステムを、多様な用途に利用する場合においては、異なるセキュリティドメイン間での鍵情報の交換が必要となることもある。その場合における CKMS 設計では、本節に記載するような検討が必要となる。

なお、一般に、異なるセキュリティドメイン間で情報を交換する場合は、以下の順番で処理を行う。ここで、ベースラインとなるセキュリティ要件の簡単な例としては、各業界団体におけるセキュリティ規範等が挙げられる。

1） 情報交換の対象となるセキュリティドメイン間で、ベースラインとなるセキュリティ要件を規定し、その規定を守ることに合意する。
2） 上記対象となる各セキュリティドメインが、ベースラインとなるセキュリティ要件を満たすことを確認する。
3） 上記セキュリティ要件を満たしたドメイン間で情報の交換を行う。

日本の政府認証基盤 GPKI（Government Public Key Infrastructure）は本節に該当する事例であり、GPKI ではセキュリティドメインが異なる様々な CA に対して相互接続を行うためのブリッジ CA を設けている。GPKI ではブリッジ CA が行政機関の CA と民間の CA 等の信頼関係を仲介し、ブリッジ CA と個々の CA 間で相互認証の証明書を発行する。異なるドメインのエンティティ間で情報交換を行う際は、自ドメインの CA を起点に、相互認証されたブリッジ CA 及び相手方 CA を含む証明書チェーンによって相手方証明書の正当性を確認し、対向するエンティティの署名を検証して署名者の認証を行うことができる。ブリッジ CA は相互認証先の CA が満たすべき要件を相互認証基準として定めており、相互認証先の CA がこの基準に準拠することが要求されている。

項目 A.14 には、異なるセキュリティドメイン間で情報の交換を許可しない場合はその旨を記載し、許可する場合は情報交換のための設計仕様を記載する。項目 A.14 で設計仕様を記載した場合は、項目 A.15 から A.21 により詳細な情報を記載する。項目 A.15 では情報の送信元と受信先をどのようなポリシーで認証するかを記載し、項目 A.16 では交換する時に実施される（交換情報の）機密性と完全性保護のためのポリシーを記載し、項目 A.17 では要求される保証要件、項目 A.18 ではいかに相手のポリシーのレビューを行うか、項目 A.19 では通信相手のポリシーが弱い場合にどうするかを記載する。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。当該 CKMS は、単一のセキュリティポリシーのもとで、単一の企業により運用されている。そのため、項目 A.14 に記載のとおり、他のセキュリティドメインとの情報共有をサポートしないことを念頭に設計されているものとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.14	当該 CKMS 設計は他のセキュリティドメインとの情報共有をサポートしない。
A.15	対象外である。
A.16	対象外である。
A.17	対象外である。

A.18	対象外である。
A.19	対象外である。

② ドメインのセキュリティポリシーの変更が設定可能なシステムであり、その変更が機能の範囲内であっても、あらゆるポリシーの変更は実行前にドメイン管理者が必ず承認するなど、予め変更ルールを決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.20	FR4.26	CKMS 設計は、異なるドメインのセキュリティポリシー及び異なるアプリケーションをサポートするように、鍵情報（暗号鍵やメタデータ）の管理機能を設定することができるかどうか、及びどのように設定するのかを明記しなければならない。	4.9.7 節
A.21	FR4.27	CKMS 設計は、異なるセキュリティドメイン間のエンティティ同士との通信に適応するために、再設定によるドメインのセキュリティポリシーの変更をサポートしているかどうか、及びどのようにサポートできるかを明記しなければならない。	4.9.7 節

解説・考慮点

ドメインのセキュリティポリシーは、時々、改訂・更新されることが望ましい。

しかし、異なるセキュリティドメイン間での鍵情報の交換が認められている場合、別のセキュリティドメインが改訂・更新したドメインのセキュリティポリシーが、承認されている元のセキュリティポリシーと整合的ではない可能性があり得る。そのため、ドメインのセキュリティポリシーの変更が設定可能であっても自由に変更できるようにすべきではなく、変更前にドメイン管理者の承認を必要とするなど、予め決められた変更ルールに従って変更すべきである。

CKMS の設計にあたって、項目 A.20 は異なるセキュリティドメイン間でのセキュリティポリシーをサポートするように鍵管理機能が設定可能であるか、可能であるならばどのように設定するのか明確化することを、また A.21 ではセキュリティポリシーの変更に伴う再設定が可能であるか、可能であるならばどのように再設定するのか明確化することを要求したものである。これらも、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の項目である。

上記のように、本節は単なるドメインのセキュリティポリシーの変更に関わる項目ではなく、異なるセキュリティドメイン間での鍵情報の交換を行うために、互いのセキュリティポリシーを（動的に）変更することを可能とするかどうかに関わる項目であることに注意すべきである。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。当該 CKMS は、単一のセキュリティポリシーのもとで、単一の企業により運用されている。

そのため、A.14 にも記載のとおり、他のセキュリティドメインとの情報共有をサポートしないことを念頭に設計されているものとする。したがって、本節は対象外である。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.20	対象外である。
A.21	対象外である。

2.3.3 マルチレベルのセキュリティドメインポリシーを持つセキュリティドメインとの鍵情報の交換

① マルチレベルのセキュリティドメインをサポートする場合には、それができるためのルールを決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.22	FR4.21	CKMS 設計は、マルチレベルのセキュリティドメインをサポートするかどうかを明記しなければならない。	4.9.5 節
A.23	FR4.22	CKMS 設計は、サポートするセキュリティドメインのそれぞれのレベルを明記しなければならない。	4.9.5 節
A.24	FR4.23	マルチレベルのセキュリティドメインをサポートしている場合、CKMS 設計は、それぞれのセキュリティレベルに属する鍵情報（暗号鍵及びメタデータ）の分離をどのように保持しているのかを明記しなければならない。	4.9.5 節
A.25	FR4.24	CKMS 設計は、鍵情報（暗号鍵及びメタデータ）のアップグレード又はダウングレードをサポートするかどうか、及びどのようにサポートするのかを明記しなければならない。	4.9.6 節
A.26	FR4.25	CKMS 設計は、アップグレード又はダウングレード機能をどのようにドメインオーソリティ（domain authority）に制限しているかを明記しなければならない。	4.9.6 節

解説・考慮点

マルチレベルのセキュリティドメインとは、2 つの分離された保護レベルを有しているセキュリティドメインのことである。マルチレベルのセキュリティドメインに属するエンティティは、異なったセキュリティレベルで運用しているドメインに属するエンティティからの鍵情報（暗号鍵やメタデータ）を処理できるようになる。

マルチレベルのセキュリティドメインに属するエンティティは、2 つ（以上）の保護レベルを区別し、異なる保護レベルの鍵情報（暗号鍵やメタデータ）が互いに混同されないことを保証しなければならない。

また、保護レベルを変更するアップグレード（低セキュリティの鍵情報を高セキュリティの鍵情報として扱う）／ダウングレード（高セキュリティの鍵情報を低セキュリティの鍵情報として扱う）ともに、提供される保護レベルが異なることからセキュリティ上何らかのリスクが発生する。例えば、アップグレードは低レベルドメインからの鍵情報（暗号鍵やメタデータ）を高レベルドメイン側が受け入れるということであるから、当該鍵情報（暗号鍵やメタデータ）のソース及び信頼性に確信を持っている場合にのみ行うべきである。一方、ダウングレードは低レベルのセキュリティしか提供されないことから、送付する鍵情報（暗号鍵やメタデータ）に対して低レベルの保護でもよいと判断された場合に限り実行すべきである。

CKMS の設計にあたって、項目 A.22～A.24 はマルチレベルのセキュリティドメインをサポートするか、サポートするならばどのように運用するのか明確化することを、また A.25 と A.26 はアップグレード／ダウングレードが可能であるか、可能であるならばどのようなルールの下で行うのか明確化することを要求したものである。これらは、マルチレベルのセキュリティドメインを設置しなければ対象外の項目である。

図 2-1 のセキュリティドメイン D（ピンク色部分）内のドメインセキュリティポリシーのように、単一のセキュリティドメインポリシーが、異なるセキュリティレベルのドメインと情報交換を行うために、複数のレベルのセキュリティをサポートする場合がある。そのようなケースの例として、扱う情報を機密レベル１、機密レベル２、機密レベル３、等に分けるようなポリシーが該当する。このように複数のポリシーで管理された情報を分離し、異なるセキュリティレベルを持つドメインと情報を交換する場合、マルチレベルのセキュリティドメインに関する記載（項目 A.22 から A.26）を行うこととなる。

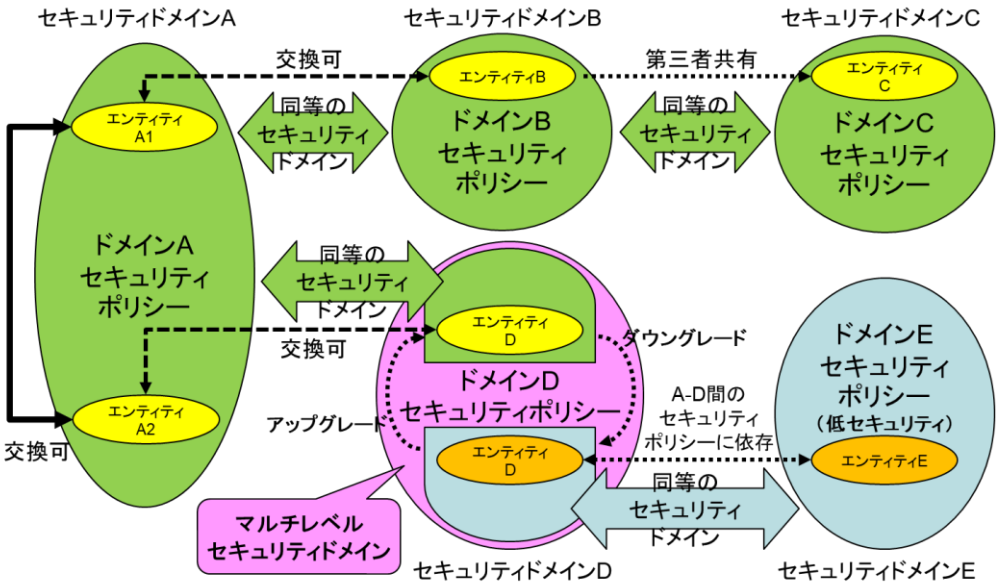


図 2-1　セキュリティドメインとセキュリティポリシーの関係

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。当該 CKMS は、単一のセキュリティポリシーのもとで、単一の企業により運用されている。そのため、項目 A.14 にも記載のとおり、他のセキュリティドメインとの情報共有をサポートしないことを念頭に設計されているものとする。したがって、マルチレベルのセキュリティドメインはサポートしておらず、本節の項目は対象外となる。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.22	対象外である。
A.23	対象外である。
A.24	対象外である。
A.25	対象外である。
A.26	対象外である。

2.4　CKMS における役割と責任

① CKMS 参加者（責任者／管理者／運用者／ユーザ）には、それぞれの役割に応じて定義された特定の認可が必要であり、その役割の責任を果たすために、鍵情報を管理する一連の機能への必要なアクセスだけが提供されなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.27	FR5.1	CKMS 設計は、CKMS に用いられているそれぞれの役割と責任、及びそれぞれの役割にどのようにエンティティが割り当てられるのかを明記しなければならない。	5 章
A.28	FR5.2	CKMS 設計は、CKMS に用いられているそれぞれの役割を満たしているエンティティが使用できる鍵情報（暗号鍵及びメタデータ）の管理機能（SP 800-130、6.4 節を参照）を明記しなければならない。	5 章
A.29	FR5.3	CKMS 設計は、どの役割が役割分離を必要とするのかを明記しなければならない。	5 章
A.30	FR5.4	CKMS 設計は、役割分離を必要とする役割に対してその分離がどのように保持されるのかを明記しなければならない。	5 章
A.31	FR5.5	CKMS 設計は、セキュリティ違反が認可された役割を実行する個人（内部者）によるのか、認可された役割がない人（外部者）によるのかを特定するための全ての自動化された対策を明記しなければならない。	5 章

解説・考慮点

本節は、CKMS 参加者（責任者／管理者／運用者／ユーザ）への権限付与の在り方について取り扱う。

CKMS の運用に関与するのは典型的には人間であるが、個々人に割り当てられる役割は異なり、そのために必要となる権限も異なる。CKMS 参加者に不必要な権限を与えることはインシデント発生時の原因究明の妨げになったり、場合によっては内部犯行を誘発する原因となったりする等、CKMS のセキュリティを低下させる方向に作用する。

責任とは、与えられた権限を適正に利用することであり、そのために付随する行為を含む。例えば、説明責任を果たすための操作ログの取得やセキュリティ維持・向上のためのセキュリティ教育の受講などがある。

CKMS における役割には以下のようなものがある。ただし、これらは例であり、CKMS によってはこれら全ての役割が必要となるわけではなく、またこれら以外の役割が定義されても構わない。最低限、CKMS 全体の最終責任を負う「システムオーソリティ」、CKMS の現場責任者に位置付けられる「システム管理者」及び「暗号責任者」、CKMS 運用から独立して監査を行う「監査責任者」、並びに「CKMS ユーザ」の役割定義が必要である。

なお、個人と役割は必ずしも一対一対応するものではない。ある役割が複数の個人に割り当てられることもあるし、ある一個人に対して複数の役割が割り当てられることもある。

a) システムオーソリティ
b) システム管理者
c) 暗号責任者
d) ドメインオーソリティ
e) 鍵管理者
f) 鍵所有者
g) CKMS ユーザ
h) 監査責任者
i) 登録エージェント
j) 鍵復元エージェント
k) CKMS オペレータ

CKMS での不正を防止・検知するために、システム的には、それぞれの役割を実行するために必要な範囲内での適切なアクセスコントロールを定める必要がある。

加えて、例えば監査と運用責任といった利益相反するような複数の役割に関しては、同時に両方の役割が割り当てられる個人がいないように、役割分離を行うべきである。また、長期の不正使用の可能性を最小化するために、役割を交代で割り当てることが望ましい。

CKMS の設計にあたって、項目 A.27 は CKMS でサポートする全ての役割及びそれぞれの役割にどのエンティティを割り当てるのか明確化し、A.28 でそれらの役割を実行するために採用するアクセスコントロールの手段を明確化することを要求したものである。

A.29 及び A.30 は、一個人に複数の役割を割り当てる場合にどのようにそれらの役割を混同せずに実行するのか明確化することを要求したものである。

A.31 は、不正が発覚した際の監査のための対策、特に有権限者の不正か否かを判定するための対策について明確化することを要求したものである。

「設計指針」には、役割として上記の 11 種が例示されている。これらの役割が担う責任と権限については SP 800-130 の 5 章を参照されたい。

一般に役割の数が増えるほどより細やかなシステム運用が可能となる一方、オペレーションコストは増加する。CKMS 設計者は、扱う情報の重要性とオペレーションコストのバランスを考慮しつつ、上記 11 種の役割に代表される、システム運用に必要な役割を決定する。限られた影響しか持たない暗号鍵の管理におけるオペレーションコストを下げるために 2、3 種程度の役割のみを利用することもあれば、資産価値の高い情報を扱うためにより多くの役割に分離することもある。

役割を決める際の基本的な考え方は、その役割に求められる職務をもとに責任を規定した上で、その職務を遂行するために必要な最小限の権限を与えることである。

項目 A.27 では、規定した役割とその責任、及び役割を割り当てるエンティティの条件や割り当て方法を明記する。項目 A.28 には、所定の役割が割り当てられたエンティティが使用可能な、鍵情報の管理方法を明記する。例えば、暗号化して鍵情報を管理する場合は暗号化方法を明記し、

署名により鍵情報の完全性を確保する場合は署名方法を明記する。

一人に複数の役割を割り当てることもあるが、その場合でも分離すべき役割については、同一人物に割り当てることがないようにすべきである。例えば、日常的な操作を行う役割と管理や監査をする役割は、異なる人物に割り当てることが望ましい。これにより、それらの役割を持つ人員のグループ同士で、内部不正を相互に牽制することが可能となり、内部不正のリスクが低下する。項目 A.29 は、このような分離すべき役割を明記する。項目 A.30 では、その分離方法を明記する。

項目 A.31 では、情報漏洩などのセキュリティ違反が、どの役割を割り当てられた個人により発生したのか、または外部者により発生したのかを特定する方法を明記する。これにより、情報漏洩が発生した場合においても、役割における個人の説明責任（項目 A.06）が明確になる。このことは、操作ミスや悪意のある挙動から情報漏洩を防ぐことにもなる。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.27	責任者（システムオーソリティ）、管理者（システム管理者及び暗号責任者）、利用者（CKMS ユーザ）、監査者（監査責任者）の役割が存在する。 ● 責任者は、当該 CKMS の日々の運用が的確なのか確認を実施する。責任者は CA システムの責任者としての権限を持ち、その権限により操作ログの取得が可能である。本システムの運用を担当している部署の管理責任者が担当する。 ● 管理者は、当該 CKMS の正常運用に関わるデバイス（CA サーバ、HSM、ルータ）の設定、運用、管理、メンテナンスに責任を持つ。本システムの運用を担当している部署に所属する責任者以外のメンバが担当する。 ● 利用者は、当該 CKMS のサービスを利用して IoT 製品向けの証明書発行手続き及び証明書の失効手続きを行う。IoT 製品の製造や顧客対応を担当する部署に所属するメンバが担当する。 ● 監査者は、当該 CKMS の監査を実施する。本システムの操作ログ、運用ログの閲覧が可能である。社内の内部監査メンバが担当する。外部監査時には内部監査メンバが事前に取得したログ情報を利用して対応する。
A.28	● 管理者は、CA 署名鍵の生成、更新、破棄が可能である。また、HSM 内部の鍵情報のバックアップ・アンド・リストアが可能である。ただし、これらの HSM 内部の鍵情報の操作には HSM 管理者としての権限が必要となる。当該権限の操作はマルチパーティコントロールがされているため、管理者 2 名以上の権限が必要である。管理者はこれに加えて、CA サーバやルータのアクセスコントロールの設定も可能である。 ● 利用者は、CA 署名鍵を使用した証明書発行、CA 署名鍵を使用した証明書の失効処理の要求送出が可能である。 ● 責任者及び監査者は、操作ログ、運用ログの取得と閲覧が可能である。

A.29	A.27 に挙げたそれぞれの役割は分離する。
A.30	A.27 のそれぞれの役割は、CA サーバの OS である Linux のユーザ管理機構により分離する。
A.31	CA サーバにおける証明書発行及び証明書失効アプリケーションのログ、Linux の操作ログ及び HSM の操作ログによりセキュリティ違反者の特定が可能である。

2.5 CKMS の構築環境及び実現目標

解説・考慮点

本節は、SP 800-130 の 2.10 節、3.1 節、3.2 節、3.4 節、3.5 節、6.2 節、7 章に記載されている事項について解説したものであり、CKMS をどのような実現目標を踏まえてどのように構築するのかといった全体像を取り扱う。

2.5.1 構築環境

① 鍵情報を保護、管理及び確立するために利用するデバイス及びコンポーネントの一式を明確化しなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.32	FR2.5	CKMS 設計は、CKMS の全ての主要なデバイス（例えば、メーカ、モデル、バージョン）を明記しなければならない。	2.10 節

解説・考慮点

項目 A.32 は、CKMS の設計にあたって、どのようなデバイスやコンポーネントで鍵情報の保護や管理等が行われるか明確化することを要求したものである。例えば、認証された暗号モジュールを利用するなどがある。
なお、コンポーネントとは CKMS を構成するために必要とするハードウェアやソフトウェア、あるいはファームウェアという意味であり、デバイスとは特定の目的を供するコンポーネントの組み合わせを意味する（プロセッサ、通信メディア、ストレージユニットなど全てが該当）。

項目 A.32 が要求するような、CMKS が使用するデバイスを明記することは、例えば特定のデバイスに脆弱性が発見された場合に有用な情報となる。CKMS の管理者はその情報を利用することで、CKMS が当該脆弱性の対象となるデバイスを利用しているか否かを確認することができる。デバイスやソフトウェアに脆弱性が発見された場合には、迅速な対応が求められることも多く、デバイス名のみでなく、使用するソフトウェアのバージョンなども予め明記しておくことが望ましい。

これらの情報は、インベントリ管理、ベンダのサポート契約管理、リプレイス計画の策定、第三者監査などにおいても有用である。さらに、CKMS の機能拡張や増強、将来的な移行対策の検

討においてもこれらの情報は参照される。

当該 CKMS で利用されるソフトウェアやハードウェアの管理台帳が存在し、それを利用することで必要な情報を閲覧可能であれば、その管理台帳へのリンクを記載することで良い。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。本モデルでは、プライベート CA が担当するのは CA の機能のうち、IA（Issuing Authority）と VA（Validation Authority）の機能である。RA（Registration Authority）の機能は CKMS 外部の IoT 製品向け証明書管理端末が担っている。以下の項目 A.32 では上記を想定している。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.32	本プライベート CA システムの構成要素となるデバイスには、CA サーバ、HSM、ルータがある。また、CA サーバ上で動作するコンポーネントには CA ソフトウェアがあり、このソフトウェアによって IA（Issuing Authority）及び VA（Validation Authority）の機能を実現する。 これらのデバイスとソフトウェアのシステムインベントリは<URI>に保存されている。

② 様々な CKMS トランザクションや鍵情報で使用される日時について、正確でかつ Network Time Protocol（NTP）サーバのように権威ある情報源を元にすることが要求される場合のルールを決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.33	FR6.9	CKMS 設計は、システムで使用される日時に要求される正確さと精度を明記しなければならない。	6.2.1 節
A.34	FR6.10	CKMS 設計は、要求される正確さを達成するためにどの権威時刻ソース（authoritative time source）を使用するかを明記しなければならない。	6.2.1 節
A.35	FR6.11	CKMS 設計は、要求される正確さを達成するためにどのように権威時刻ソース（authoritative time source）を使用するかを明記しなければならない。	6.2.1 節
A.36	FR6.12	CKMS 設計は、どの日付、時刻、及び機能が信頼される第三者タイムスタンプ（trusted third-party time stamp）を要求するかを明記しなければならない。	6.2.1 節

解説・考慮点

トランザクションや鍵情報で使用される日時は重要な意味を持つため、正確である必要がある。また、場合によっては、信頼される第三者機関が提供するメカニズムによって日時の正確性を客観的に担保することが必要なこともある。

CKMS の設計にあたって、項目 A.33 は CKMS で使用される日時にどの程度の正確性が要求されるのか明確化することを要求したものである。また、具体的な達成手段として、A.34 及び A.35 は日時の正確性をどのような手段で達成するのか、A.36 は第三者機関によるタイムスタンプをどのように使うのか明確化することを要求したものである。なお、タイムスタンプを利用しなければ A.36 は検討対象外である。

項目 A.33～A.36 は、CKMS で使用する日時に関する項目である。暗号鍵のメタデータには一般に日時が含まれ（例えば、鍵生成日、活性化日、有効期限や失効日、更新予定日など）、日時は CKMS において暗号鍵のライフサイクル管理に利用される重要な要素である。要求される日時の精度はシステムによって異なるため、CKMS で要求される日時の正確さと精度、その実現手段について、権威時刻ソースを含めて明確にすることを求めている。

適切に時刻が管理されておらず、例えば、新しいポリシーに準拠できないとの理由で CKMS の内部時刻を巻き戻して過去のポリシーと時刻で処理を行うことが可能であれば、ポリシー変更の実効性は失われることとなる。このように日時の精度以前に内部時刻の巻き戻しを可能としないことを必要とする場面は多い。

システムによっては、信頼できる第三者機関によるタイムスタンプサービスを利用して、対象となるデータが確かにその日時に存在したことの客観的なエビデンスを必要とすることも考えられる。項目 A.36 は第三者タイムスタンプを必要とする場合の項目である。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。要求する時刻の精度や権威時刻ソースの使用例については、あくまで仮想的な設定であり、ここに記載した設定は必ずしも一般的なものではないことに注意されたい。また、項目 A.34 での「信頼できる NTP サーバ」について、実際には具体的な NTP サーバを記載することになるが、本書では具体的な記載を省略した。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.33	当該 CKMS において証明書の発行や証明書の失効に利用する日時情報は、A.34 記載の権威時刻ソースとの誤差が 10 秒以内であることを必要とする。
A.34	国内の「信頼できる NTP サーバ」を権威時刻ソースとして使用する。
A.35	当該 CKMS の CA サーバ及び HSM は、NTP によって上記権威時刻ソースとの時刻合わせを実施する。
A.36	当該 CKMS では、信頼される第三者タイムスタンプを要求する機能は無い。

2.5.2　実現目標

解説・考慮点

CKMS は、特定の目標を達成するために設計されるべきである。望ましいレベルのセキュリティを提供してアプリケーションと使用する組織のニーズを満たし、手頃なコストで、運用への負の影響が最小限になることを同時に満たすように機能するセキュリティメカニズム一式を規定する。そのためには、使用するセキュリティプロトコル標準（例：TLS、IKE、SSH、CMS）における鍵情報の安全な生成、配付、保管及び保護といった“セキュリティ”視点での実現目標だけでなく、本節で示すような視点での実現目標についても CKMS 設計で考慮する必要がある。

CKMS は利用する上での目的があり、その目的のために CKMS 設計は、暗号処理や認証処理に加えてアプリケーションやネットワークの性能も考慮して設計する必要がある。それにより、CKMS の処理がアプリケーションやネットワークに与える影響を最小限にすることができ、またアプリケーションやネットワークの特性を考慮して暗号アルゴリズムや暗号利用モードを選択することができる。

① CKMS を運用するネットワーク視点での実現目標を定めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.37	FR3.1	CKMS 設計は、それが機能する通信ネットワークに関しての目標を明記しなければならない。	3.1 節

解説・考慮点

項目 A.37 は、CKMS の設計にあたって、通信バックボーンを形成するネットワークへの影響がどの程度までなら許容できるのか明確化することを要求したものである。それには以下のような観点がある。

- ネットワークの効率性及び信頼性
- ネットワークサイズ及びスケーラビリティ
- ネットワークの特性

ネットワークの信頼性は、例えば有線 LAN を想定するのか、モバイル環境を想定するかで大きく異なる。ネットワークサイズやスケーラビリティは CKMS を利用するエンティティの規模や利用頻度に影響を及ぼす。

例えば、ネットワークの特性の 1 つの指標に誤り率がある。暗号技術は、秘匿と認証に関わる機能を提供するが、ネットワークの誤り率は、それぞれの暗号技術に対して次のような影響を与えることとなる。秘匿に関わる処理では、特定のケース（CTR や OFB などの暗号利用モードとストリーム暗号）を除いて通信路でのビット誤りが、復号結果においてブロックサイズにまで増大する性質がある。また、認証に関わる処理であるメッセージ認証（HMAC や CMAC など）、認

証暗号（GCM や CCM など）及びデジタル署名では、通信路で 1 ビットでも誤りがあれば検証時に認証エラーが発生する。従って、特に認証に関わる処理を伴う場合は、通信路誤りの影響を低減できる誤り制御を行うことが必要となる。

これらを考慮して CKMS の設計において、運用するネットワークにどのような想定をおくかを定めることを要求している。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。以下に記載した証明書の生成に関わる遅延時間の要求値は、あくまで仮想的なものであることに注意されたい。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.37	証明書の生成は、IoT 製品向け証明書管理端末とプライベート CA 間で工場内ネットワークでの通信が利用される。IoT 製品の生産ラインと連動してオンラインで証明書を生成する必要はないが、年間の IoT 製品の生産台数の計画から、 IoT 製品向け証明書管理端末が CSR を送信後に対応する証明書を受信するまでの処理が 5 秒以内に実施される必要がある。HSM における署名付与の処理は十分に高速であるので、この処理時間がネットワークに関わる要求値となる。 なお、証明書の失効に関わる CRL の伝達に関しては 1 時間以内の遅延は許容される。

② アプリケーションでの CKMS 視点での実現目標を定めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.38	FR3.2	CKMS 設計は、それがサポートすることを意図しているアプリケーションを明記しなければならない。	3.1 節

解説・考慮点

サポートするアプリケーションを踏まえ、単一のアプリケーションに特化して暗号鍵管理機能と緊密統合する CKMS にするのか、多くのアプリケーションを包含して暗号鍵管理機能をできるだけ共有化する汎用的な CKMS にするのかを選択して設計するのが一般的である。
項目 A.38 は、CKMS の設計にあたってどちらの方法の CKMS が有利であるのかを判断するために、どれだけのアプリショーンをサポートするのか明確化することを要求したものである。

項目 A.38 では、当該 CKMS がどのようなアプリケーションをサポートすることを意図しているか明記する。ここで、サポートするアプリケーションは単一とは限らず、目的の異なる複数のアプリケーションをサポートする場合もある。CKMS 設計において、サービス対象とするアプリケーションを定義することを求めている。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.38	本プライベート CA のアプリケーションには次の 2 つがある。これらのアプリケーションは専用のプログラムによって IoT 製品管理端末によって実行される。 ● 証明書発行アプリケーション：IoT 製品の製造時の処理 ● 証明書失効アプリケーション：IoT 製品の出荷後、IoT 製品運用中の処理

③ CKMS に対するユーザニーズの視点での実現目標を定めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.39	FR3.3	CKMS 設計は、意図するユーザ数とそれらのユーザに課する責任を一覧にしなければならない。	3.1 節

解説・考慮点

項目 A.39 は、CKMS の設計にあたって、CKMS をどのようなユーザが利用するのか明確化することを要求したものである。なお、それらの事項はニーズとして顕在化しているとは限らないので、潜在的なニーズについても検討することが必要である。それには以下のような観点がある。

- 初期及び将来のユーザ数
- 利用目的
- 利用環境（場所、時間等）
- ユーザの能力・前提条件（ユーザに課す知識・責任等）

上記の項目は、システムの前提条件に関わる事項であり、CKMS 設計において明確にすべきである。サービスの継続と共に大きく変化する可能性がある事項については、特に注意が必要となる。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。以下に記載した担当者の人数については、仮想的な数字である。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.39	証明書発行及び署名書の失効の各処理要求は、専用のプログラムによって CKMS 利用担当（項目 A.27 の利用者の役割に該当）が送出する。CKMS 利用担当はプログラムの操作に習熟している必要がある。担当者は、当初は 10 名程度であり、今後 10 年間で最大 100 名程度である。

④ CKMS に対する将来的なスケーラビリティの視点での実現目標を定めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.40	FR3.14	CKMS 設計は、CKMS のパフォーマンス特性を明記しなければならない。それには、実装された機能とトランザクションのタイプによる処理可能な平均及びピーク時の負荷と、その負荷がかかったときの機能とトランザクションのタイプごとの応答時間を含む。	3.5 節
A.41	FR3.15	CKMS 設計は、増大する負荷要求に応じてシステムを拡張するために、サポートされ使うことができる技術を明記しなければならない。	3.5 節
A.42	FR3.16	CKMS 設計は、増大する負荷要求に対応して CKMS を拡張できる範囲を明記しなければならない。これは、追加される負荷、負荷に対する応答時間、及びコストの観点で表現しなければならない。	3.5 節

解説・考慮点

CKMS の設計にあたって、項目 A.40～A.42 は、将来的なニーズ増大の負荷に CKMS がどの程度まで耐えられるか明確化することを要求したものである。特に、A.40 はパフォーマンス観点で、A.41 及び A.42 はスケーラビリティ観点での項目である。
なお、それらの事項はニーズとして顕在化しているとは限らないので、潜在的なニーズについても検討することが必要である。

CKMS 設計において、パフォーマンスや将来的なスケーラビリティに関わる要求を定めることを求めている。項目 A.42 は CKMS の拡張時に採用できる方法及び拡張の限界やコストについて検討するものである。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。以下に記載した生産台数や証明書の生成に関わる処理時間は、あくまで仮想的なものであることに注意されたい。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.40	本プライベート CA システムは、単体の処理性能としては 50msec 以内に証明書発行及び証明書失効の処理が可能である。
A.41	IoT 製品の生産台数が増大し、証明書発行要求が増大した場合は、CA サーバ及び HSM の増設による並行処理によって対応可能である。
A.42	本プライベート CA による証明書の発行を必要とする IoT 製品の初期生産台数は 100 万台／年、今後の 10 年間で最終的に 1,000 万台／年まで増加する可能性がある。また、失

	効処理を必要とする証明書は、当初は最大 1,000 件／年、今後の 10 年間で 1 万件／年まで増加する可能性がある。 このように、今後 10 年間で 10 倍程度の生産台数増加を想定しているため、10 台の並行処理を可能とするようシステム設計する。1 台の CA システムでは、1 秒間に 20 件の証明書発行の処理が可能であり、10 台の並行処理を行った場合は、1 秒間に 200 件の証明書発行の処理が可能となる。

2.5.3 システム間の相互運用の必要性

① 複数のシステム間で相互運用しようとする場合のルールを決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.43	FR7.1	CKMS 設計は、デバイスのインタフェース間の相互運用性の要求事項がどのように満たされるかを明記しなければならない。	7 章
A.44	FR7.2	CKMS 設計は、サポートすることを意図しているアプリケーションとの相互運用に必要な標準、プロトコル、インタフェース、サポートする処理（service）、コマンド、及びデータフォーマットを明記しなければならない。	7 章
A.45	FR7.3	CKMS 設計は、相互運用性を意図している他の CKMS との相互運用に必要な標準、プロトコル、インタフェース、サポートする処理（service）、コマンド、及びデータフォーマットを明記しなければならない。	7 章
A.46	FR7.4	CKMS 設計は、アプリケーションと他の CKMS に対する全ての外部インタフェースを明記しなければならない。	7 章

解説・考慮点

複数のシステム間で相互運用しようとする場合には、インタフェースの詳細な仕様を有することでのみ達成可能である。 CKMS の設計にあたって、項目 A.43～A.46 は、相互運用しようとする場合の条件やインタフェース等について明確化することを要求したものである。

CKMS がサポートするアプリケーションの拡張やデバイスの置き換え、他の CKMS との相互運用を可能とするために、外部インタフェースやプロトコル、コマンドの仕様を明確にする必要がある。デバイスのインタフェース、アプリケーションのプロトコル・コマンド、CKMS 間の標準プロトコルなどが本節の項目の対象となる。

項目 A.43 は CKMS 内のデバイスの交換や増設、より高機能もしくはより高性能なデバイスへの置き換えなどを念頭に、インタフェース仕様を明確にしておくことを求めている。

項目 A.44 は CKMS が提供するサービスの対象となるアプリケーションとの相互運用に関わる内容であり、項目 A.45 は他の CKMS との相互運用に関わる内容である。これらの項目 A.44 から A.46 はいずれも CKMS がその外部と連携して動作する上で定義されるインタフェース、通信プロトコル、API などを一通り整理することを求めるものであり、対象とするアプリケーションや外部 CKMS の変更や拡張などを検討する際に必要な情報である。

一般にこれらのインタフェースは、対象となる CKMS が将来においてどの程度の拡張性が見込めるかを想定した上で定義される。それらの検討の成果物としてネットワーク図、データフロー図、アーキテクチャ図等が存在する場合は、それらのドキュメントをこれらの項目で参照することが望ましい。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。本プライベート CA のアプリケーションは、IoT 製品向けに証明書を発行する IoT 製品製造時のサービスと、IoT 製品向けに発行した証明書の失効処理を行う IoT 製品運用時のサービスの 2 つであり、項目 A.44 と A.46 はそれらを前提に記載している。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.43	当該 CKMS を構成するデバイスには CA サーバ、HSM、ルータがある。CA サーバとルータ間は TCP/IP で接続する。CA サーバと HSM は LAN ケーブルで接続され、HSM の API は PKCS #11 に基づいている。 デバイス間の通信様式はネットワーク図に記載されている。ネットワーク図は<URI>に保存されている。
A.44	証明書発行要求である CSR は PKCS #10、証明書及び CRL のフォーマットは RFC 5280 の各仕様及びプロトコルに従う。 データフォーマット、コマンドなどのアプリケーションとの相互運用に関わる要件はアーキテクチャ図に記載されている。アーキテクチャ図は<URI>に保存されている。
A.45	当該 CKMS は他の CKMS との相互運用を想定していないので、対象外である。
A.46	当該 CKMS は、同一社内に存在する IoT 製品向け証明書管理端末より、項目 A.44 に記載の証明書の発行及び証明書の失効要求を受け、その処理を実施する。これ以外に外部の機器や CKMS との通信は行わない。

2.5.4 ユーザインタフェースの重要性

① ユーザインタフェース（特に習熟していないユーザに対しての）を検討しなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.47	FR3.10	CKMS 設計は、システムへの全てのユーザインタフェースを明記しなければならない。	3.4.1 節

A.48	FR3.12	CKMS 設計は、ユーザインタフェースの設計原理を明記しなければならない。	3.4.2 節
A.49	FR3.13	CKMS 設計は、システムに設計された全てのヒューマンエラー防止又はフェールセーフ機能を明記しなければならない。	3.4.2 節
A.50	FR3.11	CKMS 設計は、提案されたユーザインタフェースの使いやすさに関する､あらゆるユーザ受け入れテストの結果を明記しなければならない。	3.4.1 節

解説・考慮点

CKMS の利用にあたって最も重要な条件は、習熟していないユーザにとって分かりやすくかつ誤りなく安全にシステムを使わせることである。その際、ほとんどのユーザは暗号セキュリティのエキスパートではなく、かつセキュリティは一般に最優先の目的ではないので、使用しているセキュリティ機能の目的を十分に理解していない可能性が高いことに留意しておくべきである。
このため、習熟していないユーザに対するユーザインタフェースほど精錬されたものを用意すべきである。透過的なセキュリティを実現する一方、以下のような確立された使いやすいユーザインタフェースの設計原理を踏まえるべきである。

- 正しい操作を行うことが直感的で容易である
- 誤った操作を行うことが困難である
- 誤った操作を実行したときの回復が直感的で容易である

また、ユーザの技量に適応したユーザインタフェースは、習熟していないユーザをガイドすることができる一方、エキスパートには効率的なショートカットを使い、ステップバイステップのガイダンスを迂回できる。

CKMS の設計にあたって、項目 A.47 は、どのようなユーザインタフェースをサポートするのか明確化することを要求したものである。A.48 及び A.49 は、具体的なユーザインタフェースの設計指針・要求事項の明確化であり、どのように設計するのか明確化することを要求したものである。
A.50 はユーザインタフェースの使いやすさについての評価に関するものであり､評価を実施した際にはその結果を付けるように要求したものである。評価を実施していなければ対象外である。

項目 A.47 では CKMS で使用される全てのユーザインタフェースを把握できるよう、論理・物理問わずに全てを記述する。CKMS では CUI や GUI 以外の物理インタフェース（トークン、ピン・エントリー・デバイスなど）を使用していることも多いが、それらも余さずに記録することが重要となる。

項目 A.48 及び A.49 に記載する事項は、商用既製品であればマニュアルなどに記載されていることもあり、その場合はマニュアル類を参照することで良い。自社開発によるソフトウェアが存

在する場合には、ユーザインタフェースを整理し、それらの情報を利用者向けの教育資料やユーザマニュアルに記載する必要がある。それらの文書を参照すると共に、ユーザインタフェースの設計原理などを整理する。

項目 A.50 については、ユーザのベータテストや QA リストなどの各種テストの結果にユーザインタフェースに関わる内容があれば記載する。これらのテスト結果は、以降に変更を加える際に変更してよい箇所と変更が望ましくない箇所の把握にも利用できる。

一般に、社内に UI・UX を担当する人員が存在する場合は、それらの人員が一元的にユーザインタフェースの設計や管理を行うことで、効率良く統一性のある設計を達成することができる。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。ここでは項目 A.48 から A.50 について、社内で開発した、IoT 製品向け証明書管理端末から本プライベート CA に処理要求を送出するプログラムのユーザインタフェースに絞って検討を行ったことを想定して記載例を作成した。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.47	当該 CKMS のサービスを利用するプログラムのユーザインタフェースは、社内担当者向けのユーザマニュアルに記載している。また、CA ソフトウェアや HSM のセットアップ及び設定変更に関わるユーザインタフェースはそれぞれの製品に固有のマニュアルに記載されている。
A.48	当該 CKMS のサービスを利用するプログラムのユーザインタフェースの設計原理は、社内の UI 設計ガイドに基づいている。
A.49	当該 CKMS のサービスを利用するプログラムでは、使用できるコマンドは最小限に抑えられており、誤操作の可能性は低い。
A.50	当該 CKMS のサービスを利用するプログラムは、操作に習熟した社内の担当者が利用することを想定しているため、ユーザインタフェースに関わる評価を行っていない。

2.5.5 商用既製品の活用

① 商用既製品を活用する場合は、どのように CKMS の目標を満たすのかを検討しなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.51	FR3.4	CKMS 設計は、CKMS で使用される商用既製品を明記しなければならない。	3.2 節
A.52	FR3.5	CKMS 設計は、商用既製品によってどのセキュリティ機能が実行されるのかを明記しなければならない。	3.2 節

A.53	FR3.6	CKMS 設計は、CKMS の目標を満たすために商用既製品をどのように設定し拡張するかを明記しなければならない。	3.2 節

解説・考慮点

商用既製品は、入手、運用及び保守のためのコストが特定顧客用にカスタム設計、製造された製品より安いことが多い。その一方、多数の顧客の“最小公倍数”的な要求を満たすように設計し製造されているので、セキュリティ要求を完全には満たさない可能性もある。したがって、拡張性と拡充性を許容しサポートしている商用既製品が望ましい。
CKMS の設計にあたって、項目 A.51～A.53 は、CKMS のセキュリティ機能部分に商用既製品を採用する場合に、どのような商用既製品を使い、その商用既製品でどのセキュリティ機能を実行し、セキュリティ要求を満たすためにどのような設定をするのか明確化することを要求したものである。

項目 A.51 及び A.52 は、当該 CKMS において、どのような商用既製品が何をするために用いられているのかを把握するために記載するものである。既にシステムインベントリ、ネットワーク図、データフロー図等が存在するのであれば、それらに記録されていることも考えられ、それらを引用することもできる。これらの情報は、商用既製品のアップグレードを行う際のマイグレーション準備、他社製品への置き換え、同等製品の追加配備による処理能力の増強等を行う際に非常に有用な情報となる。

商用既製品の中には、自社開発では取得が困難なセキュリティ認証を既に取得しているものもある。そうした製品を利用することで、セキュリティポリシーが定める鍵管理機能の具現化や監査要件などを満たす手続きが簡素化されることもある。例えば、FIPS 140-2/-3 レベル 3 もしくは ISO/IEC 15408 EAL4+などのセキュリティ認証を取得した製品の採用により、鍵情報の管理に関する大半の要求を満たせる場合がある。加えて、商用既成品の中には有償のサポート等を提供しているものも多く、技術支援や最新動向の把握をワンストップで行えることは大きな利点となる。

本節の項目 A.51 から A.53 は CKMS において商用既製品を採用しない場合は対象外となる。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.51	次に挙げる商用既製品を利用している。ハードウェア製品としては、サーバ、HSM、ルータであり、ソフトウェア製品としては CA ソフトウェア、Linux OS である。 上記の詳細は、システムインベントリに、メーカと型番、バージョン番号を含めて記載されている。システムインベントリは<URI>に保存されている。

A.52	商用既製品によって実行されるセキュリティ機能は次のとおりである。HSM によって、CA 鍵による証明書への署名付与、CA 鍵による CRL への署名付与、CA 署名鍵の管理が行われる。CA ソフトウェアによって、鍵のメタデータ管理を含むプライベート CA 機能の全体制御が行われる。 当該 CKMS に利用されている商用既製品を含むすべての機器の主な役割、それら機器の配置は、ネットワーク図及びデータフロー図に記載されている。ネットワーク図及びデータフロー図は<URI>に保存されている。
A.53	HSM 及び CA ソフトウェアの適切な設定については、それぞれの製品のセットアップマニュアルに記載されている。当該 CKMS を設定する手順は、これら製品のセットアップマニュアルに基づいた社内の設定管理プロセスによって管理されている。また、設定内容の変更を行う手順はセットアップマニュアルに基づいた変更管理プロセスによって管理されている。 設定変更には、CA ソフトウェアや HSM における設定メニュー内の設定項目の変更からソフトウェアアップデートによる機能修正、機能変更や機能拡張、さらには CA 署名における鍵長の変更など様々なものがある。これらの全てのケースについて変更管理プロセスに一連の実施手順が承認フローを含めて示されている。

2.6 標準／規制に対する適合性

解説・考慮点

本節は、SP 800-130 の 3.3 節、4.8 節に記載されている事項について解説したものであり、CKMS 設計における外的な制約条件となりうるルール等について取り扱う。

① CKMS が使用される地域・国家の法律、ルール及び規制に従わなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.54	FR3.7	CKMS 設計は、CKMS に使用される連邦政府標準（注：米国の場合）、国内標準、及び国際標準を明記しなければならない。	3.3 節
A.55	FR3.8	CKMS に使用されるそれぞれの標準に対して、CKMS 設計は、どの CKMS デバイスが標準を実装しているのかを明記しなければならない。	3.3 節
A.56	FR3.9	CKMS に使用されるそれぞれの標準に対して、CKMS 設計は、標準への適合がどのように検証されるか（例えば、第三者試験プログラムによって）を明記しなければならない。	3.3 節

A.57	FR4.14	CKMS 設計は、CKMS が使用されることを意図する国名や地域名、及び CKMS が実行することを意図する際のあらゆる法的規制を明記しなければならない。	4.8 節

解説・考慮点

標準を使用することは、相互運用性と競争の促進、及び製品又は実装における信頼性を高めることが多い。特に、適合性認証プログラムがある場合、CKMS が正しく実装されていることのさらなる信頼性が得られる。
一方、セキュリティに関して CKMS が使用される地域・国家によって適用される法律等が異なるため、国際的に使用できるように設計される CKMS の場合、各国の制限に従うことができる十分な柔軟性を持っているべきである。

CKMS の設計にあたって、項目 A.54 及び A.55 は CKMS がどのような標準に適合しているのか明確化することを要求したものであり、A.56 及び A.57 は CKMS が使用される地域・国家によって適用される各国の法律・ルール・規則等に準拠していることを明確化するものである。

項目 A.54～A.57 は CKMS で使用されている国内・国際標準を把握するためのものである。CKMS には多数のモジュールが存在し、標準の対象が大規模な複合モジュールとなる可能性もあれば、小規模なサブモジュールとなる可能性もある。また、それぞれのモジュールの標準の対象となる領域は、通信プロトコル、ファイルフォーマット、ハードウェア、ソフトウェア、適合性認証プログラム等、多岐に渡り得る。

項目 A.54～A.57 では、CKMS に含まれるモジュールが準拠する標準や仕様書、ポリシー等を記載することになる。システムインベントリ、ネットワーク図、データフロー図、アーキテクチャ図、システムの仕様書などにデバイスやモジュールごとに準拠する標準や第三者認証が記載されていれば、それを引用することも可能となる。監査要件がある場合は、ポリシーに記載されることもある。

項目 A.57 はポリシーや利用規約、契約書の類に記載されているのが一般的であり、それらとの整合性を意識して記載されるべきである。

CKMS に関連する暗号技術や暗号製品、暗号利用システムに関わる標準を以下に例示する。暗号アルゴリズム及び暗号鍵長に関する国内標準には、電子政府推奨暗号リスト（CRYPTREC)、暗号強度要件（アルゴリズム及び鍵長）設定基準（CRYPTREC）がある。また、暗号モジュールや暗号製品・システムに関わるセキュリティ認証の国内・国際標準の具体例として、ISO/IEC15408 に基づく IT セキュリティ評価制度（日本では JISEC、欧州では EUCC)、FIPS 140-2/-3 に基づく暗号モジュール認証（CMVP、日本では JCMVP)、日本での政府情報システムにおけるクラウドサービスの評価認証制度 ISMAP などがある。さらに、2024 年 8 月に経済産業省が公表した「IoT 製品に対するセキュリティ適合性評価制度構築方針」に基づいて構築されたセキュリティ要件適合評価及びラベリング制度（JC-STAR）がある。

法的規制についてはその具体例として、欧州のサイバーレジリエンス法、中国のサイバーセキ

ュリティ法などに加え、各国のデータ規制（欧州では GDPR 等）などがある。また、国内の電子署名法も暗号技術に関連した法令である。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.54	当該 CKMS は以下の暗号アルゴリズム及び暗号鍵長の基準に準拠する。 ● 電子政府推奨暗号リスト（CRYPTREC） ● 暗号強度要件（アルゴリズム及び鍵長）設定基準（CRYPTREC） また、当該 CKMS は、X.509 形式の証明書を発行する CA 機能を含み、その CA 機能は、ITU-T X.509 及び RFC 5280 及びそれらに関連する標準に準拠する。 HSM は FIPS 140-2/-3 レベル 3 の CMVP 認証を取得した製品を利用する。 当該 CKMS が準拠している標準の一覧はセキュリティポリシーに記載されている。
A.55	当該 CKMS では、HSM において、項目 A.54 に記載の暗号アルゴリズム及び暗号鍵長の基準に準拠した設定がなされており、暗号モジュール認証を取得している。また、CA サーバ上で動作する CA ソフトウェアにおいて CA 機能に関わる標準に準拠している。 上記のデバイスやコンポーネントごとに準拠している標準はシステムインベントリ及びアーキテクチャ図に記載されている。それらのファイルは<URI>に保存されている。
A.56	項目 A.54 に記載のように、当該 CKMS で利用する HSM は FIPS 140-2/-3 レベル 3 の CMVP 認証を取得している。本プライベート CA の新規システム構築時及びリプレイス時に有効な CMVP 認証を取得していることを要件とし、ベンダから提供された認証書により確認する。
A.57	当該 CKMS は当社国内の工場内のみでの運用が想定されているので、日本国の法律以外は適用されない。この旨はセキュリティポリシーに記載されている。

2.7　将来的な移行対策の必要性

解説・考慮点

本節は、SP 800-130 の 7 章、12 章に記載されている事項について解説したものである。
長期の利用が想定されている CKMS の場合には、システム的に長期にわたる CKMS のセキュリティライフタイムを持つように設計・実装されるべきであるため、移行戦略があることが望ましい。その際、円滑な移行には、少なくとも 2 つの暗号アルゴリズム（異なった鍵長であるかもしれない）の利用を同時にサポートする機能が要求されることが多い。なお、異なった暗号アルゴリズムによって保護されるデータのセキュリティは最も弱い暗号アルゴリズムを上回らないことにも留意すべきであり、可能な限り素早く移行することが最善である。

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。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.58	FR7.5	CKMS 設計は、新規の、相互運用可能な、同等のデバイスへの移行のための全ての対策を明記しなければならない。	7 章
A.59	FR7.6	CKMS 設計は、暗号アルゴリズムのアップグレード又は置き換えのために提供されるあらゆる対策を明記しなければならない。	7 章
A.60	FR7.7	CKMS 設計は、暗号アルゴリズムの移行期間中に、どのように相互運用性をサポートするかを明記しなければならない。	7 章
A.61	FR7.8	CKMS 設計は、暗号アルゴリズムと鍵長の使用をネゴシエーションするプロトコルを明記しなければならない。	7 章

解説・考慮点

CKMS が保護する情報に見込まれるライフタイムと同じかそれ以上のセキュリティライフタイムを持つか、もしくはより強固なアルゴリズム及びより長い鍵長に将来移行するための移行戦略がある暗号アルゴリズムだけを利用しなければならない。
項目 A.58～A.61 は、CKMS の設計にあたって、CKMS の移行戦略を実行するためにどのような仕組みや機能を予めサポートしておくか明確化することを要求したものである。

上記のように、CKMS 設計はそれによる保護の対象となるシステムやそのデータのライフタイムをカバーすべく、十分なセキュリティライフタイムを備えた暗号アルゴリズムを採用することとなる。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の変更は、予め設定していた鍵長や暗号アルゴリズムのライフタイムを超える場合の他に、運用中の暗号アルゴリズムが予期せぬ危殆化をした結果、当初の設計よりも早く鍵長や暗号アルゴリズムの変更が必要となる場合もある。

暗号アルゴリズム及びその鍵長のセキュリティライフタイムについては、「暗号強度要件（アルゴリズム及び鍵長）設定基準」（CRYPTREC）を参照するとよい。

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。

通信データの保護や通信時の認証に関わる状況において暗号アルゴリズムを変更する場合は、全ての関連する機器やソフトウェアを一斉に変更するような場合を除いて、各機器やソフトウェアが通信相手と利用する暗号アルゴリズムや鍵長に関して合意することが可能であるようにその通信プロトコル設計がなされている必要がある。また、データ秘匿の目的で暗号化された上で保

存されているデータや署名が付与されて保存されているデータについては、汎用的な解決方法は存在しないものの、移行後の暗号アルゴリズムや鍵長による暗号化や署名付与を適用し直す、暗号学的タイムスタンプを実施する、暗号以外の手段（例えば物理的保護）によって秘匿データや署名データを安全に保管するなどの対策が存在する。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。当該 CKMS での暗号処理は HSM が担っているため、HSM における鍵長や暗号アルゴリズムの置き換え、及び HSM の移行が検討事項となる。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.58	当該 CKMS で利用する HSM について、鍵情報のバックアップ・アンド・リストア処理をサポートする製品への移行においては、鍵情報の転送を伴う移行が可能となる。鍵情報のバックアップ・アンド・リストア処理がサポートされない HSM 製品に移行する場合は、新たな鍵の生成を伴う新規セットアップを行うこととなる。
A.59	当該 CKMS で利用する HSM 選定においては、将来の移行を想定して、署名アルゴリズムと鍵長については、128 ビットセキュリティ（ECDSA P-256 及び SHA-256）及び 192 ビットセキュリティ（ECDSA P-384 及び SHA-384）を選択可能な製品を採用する。署名アルゴリズムの選択は CA ソフトウェアの設定によって行う。 運用中に署名アルゴリズムに危殆化が生じて署名アルゴリズムのアップグレードが必要になった場合は、次のいずれかの方法によって対応する。 192 ビットセキュリティの署名アルゴリズムへの切り替え、HSM ベンダにより提供される更新ファームウェアのサポート範囲内での署名アルゴリズムの更新や鍵長の変更、より強度の高い署名アルゴリズムをサポートした HSM 製品への置き換え、など。
A.60	当該 CKMS は、鍵長の更新以外の暗号アルゴリズムの移行をサポートする構成とはなっていない。暗号アルゴリズム自体の移行が必要となった場合は、CKMS 全体もしくは HSM を含むサブモジュールを再設計して、新たな CKMS として運用を行うこととなる。
A.61	当該 CKMS において、証明書生成や失効処理に利用可能な署名アルゴリズム及び鍵長は、CA サーバにおいて設定されている。また、TLS は利用する暗号アルゴリズム及び鍵長のネゴシエーションを行う機能を備えている。

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。

項目	FR 番号	Framework Requirements の内容	SP 800-130
A.62	FR12.1	CKMS 設計は、システムに実装されたそれぞれの暗号アルゴリズムの想定されるセキュリティライフタイムを明記しなければならない。	12 章

A.63	FR12.2	CKMS 設計は、CKMS の運用に悪影響を与えることなしに、暗号アルゴリズムのどの副関数（例えば、HMAC の副関数として使うハッシュ関数）が、類似だが暗号学的に改良されている副関数にアップグレード又は置き換えを行うことができるかを明記しなければならない。	12 章
A.64	FR12.3	CKMS 設計は、どの鍵確立プロトコルがシステムによって実装されているかを明記しなければならない。	12 章
A.65	FR12.4	CKMS 設計は、システムに実装されているそれぞれの鍵確立プロトコルの想定されるセキュリティライフタイムを、採用されている暗号アルゴリズムの想定されるセキュリティライフタイムの観点から、明記しなければならない。	12 章
A.66	FR12.5	CKMS 設計は、CKMS デバイスへの外部からのアクセスが許容されている範囲を明記しなければならない。	12 章
A.67	FR12.6	CKMS 設計は、CKMS デバイスへの全ての許可された外部アクセスがどのようにコントロールされるかを明記しなければならない。	12 章
A.68	FR12.7	CKMS 設計は、CKMS の暗号アルゴリズムに対する量子コンピュータによる攻撃のような、新しい技術の発展の影響に抵抗又は軽減するために採用している機能を明記しなければならない。	12 章
A.69	FR12.8	CKMS 設計は、CKMS の暗号に対する量子コンピュータによる攻撃の、現在知られている影響を明記しなければならない。	12 章

解説・考慮点

長期の利用が想定されている CKMS の場合には、CKMS がセキュアでなくなるかもしれない技術の進歩に起因する潜在的な脅威についても考慮すべきである。

以下に 4 つの潜在的な脅威の例を挙げる。項目 A.62～A.68 は、CKMS の設計にあたって、それぞれの脅威に対する現時点で採用されている対策技術（及び対策の限界）について明確化することを要求したものである。なお、潜在的な脅威はこれら 4 つに限るものではない。

- 暗号アルゴリズムに対する新しい攻撃
  もともと暗号アルゴリズムには想定されるセキュリティライフタイムがある。また、時間が経過するにつれ、そのセキュリティライフタイムを短縮する新しい攻撃が発見される可能性もある。暗号アルゴリズムがセキュアでなくなった場合、最終的には、暗号アルゴリズムを完全にアップグレード又は置き換える必要がある。その場合、暗号アルゴリズムは、（当該アルゴリズム以外の）残りの実装への著しい影響なしで置き換え又はアップグレードができるような方法が望ましい。
- 鍵確立プロトコルに対する新しい攻撃
  CKMS のセキュリティは、暗号アルゴリズムの安全性のほか、鍵確立段階での対称鍵の安全性にも依存する。しかしながら、鍵確立プロトコルのセキュリティ評価は、暗号アルゴ

リズムに対して行われるのと同じ程度で評価されることはめったになく、数年間使用された後に弱点が発見されることが少なくない。
しかも、一旦広く使用されるようになると当該プロトコルをアップグレードすることは困難であることも多い。

- CKMS デバイス／アクセスコントロールに対する新しい攻撃
  認可されない当事者が CKMS の外部から CKMS デバイスへアクセスすることを、現実的な範囲で最大限防止しなければならない。CKMS のセキュリティが依存するアクセスコントロールメカニズムは、要求に応じて、最新の攻撃を実行したりアップグレードしたりして定期的にレビューされるべきである。
- 新しい計算機技術の発展
  現状の脅威で最も高い関心が払われているものは、暗号鍵を復元するのに十分な能力を持つ量子コンピュータの発展である。

上記のように、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。そのため、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。

暗号アルゴリズムに対する新しい攻撃や新しい計算機技術の発展（特に暗号解読可能な量子コンピュータによる影響）については、CRYPTREC の発信する「注意喚起情報」が参考になる。また、CKMS デバイスに対する新しい攻撃については、デバイスベンダからの情報入手が原則となるため、有償のサポート契約を結ぶことを推奨する。

なお、暗号アルゴリズムのセキュリティライフタイムについては「暗号強度要件（アルゴリズム及び鍵長）設定基準」（CRYPTREC）を参照するとよい。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

A.62	本 CKMS で実装される暗号アルゴリズムは以下となる。これらのアルゴリズムは証明書や CRL への署名付与や IoT 製品向け証明書管理端末との間の TLS 通信において用いられる。 ● ECDSA（P-256, P-384） ● SHA-256、SHA-384 ● AES128、AES256 ● ECDH（P-256, P-384） 「暗号強度要件（アルゴリズム及び鍵長）設定基準（CRYPTREC）」によると、上記アルゴリズムのセキュリティライフタイムは以下のとおりである。

	● 128 ビットセキュリティ：ECDSA(P-256)、SHA-256、AES128、ECDH(P-256)。これら のセキュリティライフタイムは 2040 年まで ● 192 ビットセキュリティ：ECDSA(P-384)、SHA-384、ECDH(P-384)。これらのセキュリティライフタイムは少なくとも 2070 年までは有効 ● 256 ビットセキュリティ：AES256。このセキュリティライフタイムは少なくとも 2070 年までは有効
A.63	ECDSA に利用するハッシュ関数（副関数に相当）である SHA-256 もしくは SHA-384 に危殆化が生じた場合は ECDSA の標準文書に従って対応する。具体的には、同等のハッシュ長のダイジェストを生成する SHA-3 アルゴリズムなどに置き換えることが対応の候補となる。利用する HSM 製品において、代替となる安全なハッシュ関数への置き換えが可能であればそれを検討するが、置き換えができない場合は HSM 自体の置き換えを検討する。
A.64	当該 CKMS では TLS1.3 を IoT 製品向け証明書管理端末との通信に利用する。TLS1.3 における鍵確立には ECDH(P-256)を利用する。
A.65	「暗号強度要件（アルゴリズム及び鍵長）設定基準（CRYPTREC）」によると、TLS1.3 で利用する鍵確立アルゴリズム ECDH(P-256)のセキュリティライフタイムは 2040 年までである。
A.66	当該 CKMS では外部からの直接のアクセスは許可されていない。遠隔地から外部ネットワークを経由してアクセスを行う場合は、所定の VPN エンドポイントを経由し、社内ネットワークへの接続が許可された後に CKMS へ接続する必要がある。
A.67	当該 CKMS へ外部からアクセスを行うには、施設や管理区域への入退出管理、もしくはネットワークセキュリティコントロール及びコンピュータシステムのセキュリティコントロールを経由する必要がある。さらに、HSM 自体が備える HSM 内に保管される鍵に対するアクセスコントロールを介することになる。 なお、HSM において外部アクセスから鍵を保護する機能は、サイドチャネル攻撃や故障利用攻撃などの非侵襲攻撃の進化によって危殆化する可能性がある。そのため、リスク分析等を行った結果、HSM における鍵の保護機能を強化する必要が生じた場合には、より強固な耐性を備えた HSM への移行を検討するものとする。
A.68	本 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。これは、暗号の置き換えが必要な場合において、CKMS 全体または HSM を含むサブモジュール単位での置き換えを想定しているためである。 さらに、モジュールの置き換えの容易性を確保するために、商用既製品の利用を想定し、CKMS の外部接続や HSM との接続には標準的な API を採用し、暗号アルゴリズムも CRYPTREC 暗号リストに記載される標準的なものから選定している。 上記のような構成のため、（量子コンピュータを含む）新たな技術の進展によって当該 CKMS が危殆化する場合においても、新たな技術に対抗可能な暗号技術をサポートした CKMS への置き換えを比較的容易に実現することが期待できる。 上記のような思想のもと、暗号解読可能な量子コンピュータ（CRQC：Cryptographically

	Relevant Quantum Computer）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（PQC：Post-Quantum Cryptography）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。
A.69	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（本書を執筆した 2025 年時点の状況）。 また、仮に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。 さらに、項目 A.68 のように当該 CKMS は、PQC をサポートした CKMS への置き換えを比較的容易に実現可能と期待できる。 以上から、量子コンピュータによる暗号解読のリスクに関しては、そのような量子コンピュータの実現の兆候に気づいてからの対応で十分と考える。

3 暗号鍵管理デバイスへのセキュリティ対策

本章の目的・趣旨

本章は、「設計指針」の 8 章に記載されている要求事項（各節での灰色枠内で示している内容）について解説したものである。

本章の記載内容は、暗号鍵を管理するための個々のデバイスに対して、必要に応じて検討する項目（E.01～E.37）をまとめたものであり、主に以下のような検討項目を含んでいる。

- アクセスコントロールシステム／暗号モジュールを利用する際に、それらが有するべき機能や運用方法などはどういったものか
- デバイスのセキュリティ確認のためにどのようなセキュリティ評価試験を実施するか

本章の検討項目は、暗号鍵の管理・保管を実際に行う個々のデバイスを対象としており、「広義」の意味での暗号鍵管理に相当するものの一つである。また、アクセスコントロールシステムと暗号モジュールは暗号鍵のセキュアな管理を行うための主要なコンポーネントであることから、本章でまとめて解説する。

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。

項目	FR 番号	Framework Requirements の内容	SP 800-130
E.01	FR6.88	CKMS 設計は、エンティティ、ACS（アクセスコントロールシステム）、機能ロジック、及びそれらの間の接続の配置を示すことで CKMS のトポロジーを明記しなければならない。	6.7.1 節
E.02	FR6.89	CKMS 設計は、適切な操作を保証するために実装されている鍵管理機能に対する制限を明記しなければならない。	6.7.1 節
E.03	FR6.90	CKMS 設計は、鍵管理機能へのアクセスがどのように認可されたエンティティを制限しているかを明記しなければならない。	6.7.1 節
E.04	FR6.91	CKMS 設計は、鍵管理機能へのアクセスを制御するための ACS とそのポリシーを明記しなければならない。	6.7.1 節
E.05	FR6.92	CKMS 設計は、少なくとも以下を明記しなければならない： a) エンティティの粒度（例：人、デバイス、組織） b) エンティティが識別されているかどうか、及びその方法 c) エンティティが認証されているかどうか、及びその方法 d) エンティティの認可が検証されているか、及びその方法	6.7.1 節

		e) それぞれの鍵管理機能のアクセスコントロール	
E.06	FR6.93	CKMS 設計は、CKMS セキュリティポリシーを適応、実装、施行するための ACS の能力を明記しなければならない。	6.7.1 節

解説・考慮点

CKMS のセキュリティは、鍵情報の管理機能の適切なシーケンスと実行に依存する。そのため、鍵情報の管理機能が認可されたエンティティの要求（呼び出し）への応答としてのみ実行されること、及びその他の制限事項が全て満たされていることを保証することが必要である。
アクセスコントロールシステムは、暗号モジュールと連動して、鍵情報への適切なアクセスをコントロールするために動作する。
CKMS の設計にあたって、項目 E.01～E.06 は、アクセスコントロールへの要求事項を明確化することを求めたものである。E.01 及び E.06 はアクセスコントロールの構成や性能、E.02 は機能のコントロール、E.03 はエンティティの認証・認可、E.04 及び E.05 はアクセス条件を対象としている。

上記のように、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。

ACS は暗号処理の実行主体である暗号モジュールと連動するため、暗号モジュール及び ACS を含む CKMS 全体のトポロジーと処理フローを定める必要がある(項目 E.01)。図 3-1 は SP 800-130 の 6.7.1 節に例示された CKMS のトポロジーである。

ここで暗号モジュールとは、FIPS 140-2/-3 で定義されているように、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。暗号モジュールは、暗号境界内で利用される暗号鍵の保護機能を備えている。

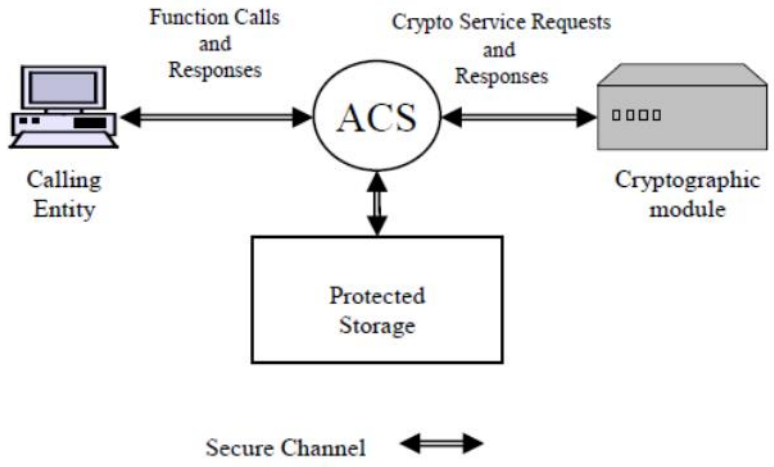


図 3-1　CKMS のトポロジー例（SP 800-130 から引用）

項目 E.02 は暗号モジュールなどの鍵管理機能の実行に対する制限を ACS と絡めて定義することを求めており、項目 E.03 は特にエンティティとの対応付けに関してエンティティ認証、認可の機能を定義することを求めている。また、項目 E.04 は暗号モジュールなどの鍵管理機能へのアクセスをコントロールする ACS が従うポリシーを定めることを求めている。

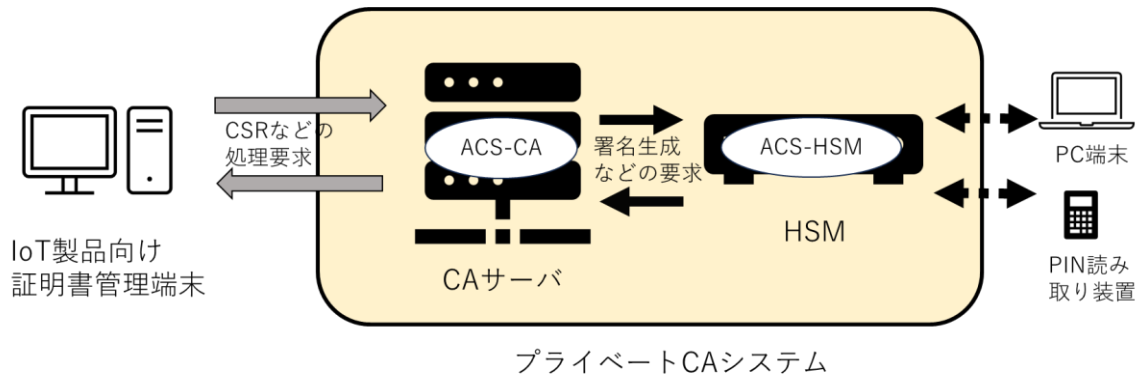
項目 E.05 は ACS におけるエンティティの粒度や識別方法、認証の方法、認可された鍵管理機能を明確にすることを定めており、ACS の本質的な部分である。

項目 E.06 は CKMS 全体のセキュリティポリシーの変更に際して、ACS ポリシーの変更がどの程度可能であるか、ACS ポリシーの更新に関わる手順を定めることを要求している。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

E.01	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 のトポロジーは図 3-2 を参照。 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 3-3 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。  **図 3-2　ACS の配置**

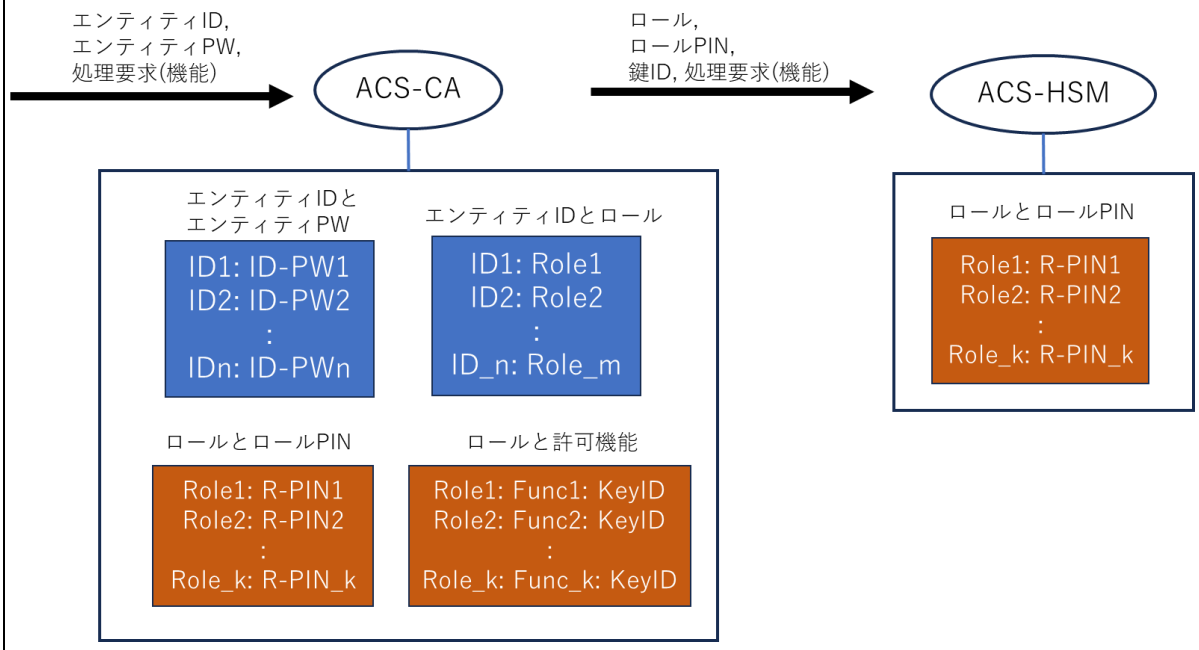


図 3-3　ACS に関わる処理フロー

E.02	HSM の機能である、署名鍵生成機能、署名生成機能、署名鍵の更新機能、署名鍵の破棄機能、署名鍵のバックアップ機能、HSM ログのアーカイブ機能のそれぞれの実行は権限を有するエンティティでなければ実施できない。
E.03	CKMS 利用担当(証明書の作成、失効処理の実行)、CKMS 管理担当(CA 鍵の生成、更新、破棄、バックアップ、HSM ログのアーカイブ)、監査者(HSM ログの閲覧)をそれぞれの鍵管理機能に対して認可されたエンティティとする。これら機能の実行権限の設定、認証や認可が ACS-CA 及び ACS-HSM によって管理される。
E.04	各エンティティは個人単位で識別・認証され、設定したロールに基づき認可された権限(E.03 に記載)を実行できる。ACS の設定や更新を行う場合、CKMS 管理担当が CA サーバ及び HSM の管理者権限を取得して設定を変更する。
E.05	a) CA サーバにおける ACS-CA でのエンティティの粒度は個人単位である。また、HSM における ACS-HSM でのエンティティの粒度はロール単位である。 b) CA サーバにおけるエンティティはエンティティ ID によって識別される。HSM ではロールによって識別される。 c) CA サーバにおけるエンティティの認証はエンティティパスワードによる。また、HSM におけるロールの認証はロール PIN による。ただし、HSM の管理者権限の認証では PIN に加えて複数の USB ドングルを専用の PIN 読み取り装置に接続する必要がある。HSM 管理者権限の取得に関わる認証処理は、マルチパーティコントロールが適用されている（E.23 記載例を参照）。 d) 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及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。 e) CA サーバの管理者権限に関わる機能、操作ログ閲覧及び操作ログアーカイブの各機能のアクセスコントロールは ACS-CA によって管理されている。一方、HSM の管理者権限に関わる機能、HSM の操作ログ閲覧及び操作ログアーカイブの各機能のアクセスコントロールは ACS-HSM によって管理されている。それ以外の各種機能のアクセスコントロールは ACS-CA と ACS-HSM の双方によって管理されている。
E.06	CKMS セキュリティポリシーを変更する場合、CA サーバ内の ACS-CA 及び HSM 内の ACS-HSM の更新が必要となる場合がある。ACS の更新を行う場合、CKMS 管理担当が CA サーバ及び HSM の管理者権限を取得して設定を変更する。更新後にはそれぞれの更新内容が整合していることを確認する。

3.1.2 暗号モジュール

① 暗号モジュールセキュリティポリシーを定めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
E.07	FR8.19	CKMS 設計は、以下を含む、使用する暗号モジュール及びそれぞれのセキュリティポリシーを特定しなければならない： a) それぞれのモジュールの実装形態（ソフトウェア、ファームウェア、ハードウェア、又はハイブリッド） b) それぞれのモジュールの完全性を保護するために使用されるメカニズム c) それぞれのモジュールの暗号鍵を保護するために使用される物理的及び論理的メカニズム d) それぞれのモジュール（セキュリティ機能を含む）で実行された第三者試験と検証、及びそれぞれのモジュールで使用される保護措置	8.4 節

解説・考慮点

一般にコンピュータは暗号鍵への十分な保護を提供するようには設計・実装されていない。実際、同じコンピュータ上にセキュリティが検証されていないソフトウェアが含まれていることから、当該コンピュータ上の暗号ソフトウェアでは物理的に保護されていること及び信頼できないソフトウェアによる攻撃から論理的に保護されていることが重要である。

その対策の一つとして、暗号モジュールの利用がある。暗号モジュールは、暗号境界内に実装される暗号ベースのセキュリティ機能全てを包含しており、実装形態はハードウェア、ソフトウェア、ファームウェアを問わない。

暗号モジュールの目的は、実装されたセキュリティ機能の完全性と鍵情報の保護を行うことであり、暗号モジュールセキュリティポリシーに従って、改ざんや窃取から物理的及び論理的に保護するように作られている。このため、CKMS では、暗号モジュールを使用して暗号鍵を生成し、保管、使用及び保護を行うことが望ましい。
ただし、暗号モジュールが提供するセキュリティ機能や保護レベル等は、暗号モジュールセキュリティポリシーに大きく依存することに留意されたい。

項目 E.07 は、CKMS の設計にあたって、暗号モジュールへの要求事項を暗号モジュールセキュリティポリシーの形で明確化することを求めたものである。暗号モジュールは、E.07 で定めたセキュリティポリシーに則って利用しなければならない。

上記のように、多くの汎用的なコンピュータは暗号鍵の十分な保護を提供するような設計や実装はされていない。実際に、暗号処理を実行するコンピュータ上にセキュリティ面で十分な検証がされていないソフトウェアが動作する場合、ソフトウェア自身の脆弱性をついた攻撃によって暗号鍵のセキュリティに影響が及ぶことがある。他方で、暗号モジュールは汎用的なコンピュータから暗号鍵を保護しながら暗号処理を実行することができる。暗号モジュールの実装形態はハードウェア、ソフトウェア、ファームウェアと様々であるが、典型的なものにハードウェア・セキュリティ・モジュール（HSM）が存在する。

暗号モジュールはそれ自身のセキュリティポリシーに従って構成されており、暗号モジュール内に実装されているセキュリティ処理機能の完全性保護及び保管されている暗号鍵の保護が実現される。暗号モジュールが備える保護機能の強度は、暗号モジュールの実装形態や保護機能として利用されるメカニズムに依存する。暗号モジュールのセキュリティポリシーの実例は NIST の CMVP 認証の検証済み製品のサイトでも参照できる。

暗号モジュールを対象とした第三者試験には FIPS 140-2/-3 や ISO/IEC 15408 がある。FIPS 140-2/-3 では暗号モジュールのセキュリティについてレベルが定義されている。ただし、レベルの値が大きいほど厳格な環境条件の整備が要求されるなど運用コストの上昇が想定されるため、利用ケースに応じた適切なレベルを選定することが望ましい。また、ISO/IEC 15408 では評価保証レベルが定義されており、レベルの値が大きいほど認証試験においてドキュメントや実装内容、開発環境などのより広い範囲をより厳密に評価したことを表している。

項目 E.07 は CKMS で採用する暗号モジュールに対して、そのセキュリティポリシーについて実装形態、セキュリティ機能の完全性保護メカニズム、暗号鍵の保護メカニズム、第三者認証の観点でそれぞれ明確化することを求めている。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

HSM 製品のセキュリティポリシーを確認し、CKMS セキュリティポリシーと整合したモジュール内での鍵管理、鍵保護、暗号処理の各機能を備えたデバイスを採用するものとする。第三者試験として FIPS 140-2/-3 レベル 3 の認証取得を要件とし、本プライベート CA の新規構築時及びリプレイス時に FIPS 140 認証が有効な製品を採用するものとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

E.07	a) HSM はハードウェアによって暗号機能を実装した暗号モジュールである。本 CKMS のセキュリティポリシーが定める各種の暗号アルゴリズムや乱数生成機能を備えた HSM 製品を選定する。 b) 本プライベート CA システムで利用する HSM は、暗号アルゴリズムや乱数生成機能の正常動作を検査するセルフテスト機能を備える。HSM の電源投入時や暗号機能の動作前、あるいは要求したタイミングでセルフテスト機能を実行する。 c) 本プライベート CA システムで利用する HSM は暗号鍵を保護するための物理的メカニズムとして、物理的なタンパー攻撃の検知機能と検知した場合のタンパー応答機能を備える。さらに、サイドチャネル攻撃や故障利用攻撃などの非侵襲攻撃に対する緩和策を備えている。論理的メカニズムとして、アクセス制御機能に基づいたエンティティの認証・認可の機能、さらに鍵情報を外部と入出力する場合に暗号学的保護によって解読や改ざんを防止する機能を備えている。 d) 第三者試験として FIPS 140-2/-3 レベル 3 の認証取得を要件とする。本プライベート CA の新規構築時及びリプレイス時に、FIPS 140 認証が有効な HSM 製品を採用する。

② 鍵情報の暗号モジュールへの入出力のための機能及び制限を決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
E.08	FR6.58	CKMS 設計は、どのように、どのような状況で鍵情報（暗号鍵及びメタデータ）が暗号モジュールに入力されるか、入力される形式、及び入力に用いられる手段を明記しなければならない。	6.4.19 節
E.09	FR6.59	CKMS 設計は、（必要ならば）どのように入力された鍵とメタデータの完全性及び機密性が入力時に保護され検証されるかを明記しなければならない。	6.4.19 節
E.10	FR6.60	CKMS 設計は、どのように、どのような状況で鍵情報（暗号鍵及びメタデータ）が暗号モジュールから出力されるか、及び出力される形式を明記しなければならない。	6.4.20 節
E.11	FR6.61	CKMS 設計は、どのように出力された鍵とメタデータの機密性及び完全性が暗号モジュールの外部で保護されるかを明記しなければならない。	6.4.20 節

E.12	FR6.94	CKMS 設計は、平文での対称鍵又はプライベート鍵が暗号モジュールに入力又は出力される状況を明記しなければならない。	6.7.2 節
E.13	FR6.62	プライベート鍵、対称鍵、又は機密のメタデータが暗号モジュールから平文形式で出力される場合、CKMS 設計は、鍵情報（暗号鍵及びメタデータ）が提供される前に、呼び出しエンティティを認証するかどうか、及びどのように認証するかを明記しなければならない。	6.4.20 節
E.14	FR6.95	いかなる暗号モジュールにおいても、平文での対称鍵又は平文のプライベート鍵が入力又は出力される場合には、CKMS 設計は、平文鍵がどのように暗号モジュールの外部で保護され、制御されるかを明記しなければならない。	6.7.2 節
E.15	FR6.96	いかなる暗号モジュールにおいても、平文での対称鍵又は平文のプライベート鍵が入力又は出力される場合には、CKMS 設計は、そのような動作がどのように監査されるかを明記しなければならない。	6.7.2 節

解説・考慮点

暗号モジュールは、平文形式の暗号鍵への物理的保護を提供し、平文形式のまま暗号鍵が露出しないようにしている。このため、人間が平文形式の対称鍵又はプライベート鍵を見る必要が全くない暗号モジュールを使用する CKMS は、より透過的でよりセキュアである。また、暗号モジュールから出力される場合には、出力前に暗号鍵に暗号学的保護が適切に適用されなければならない。

CKMS の設計にあたって、項目 E.08 は暗号モジュールに鍵情報を入力するための条件を明確化することを、E.09 は入力される鍵情報の完全性と機密性を保護するための方法を明確化することを要求したものである。一方、E.10 は暗号モジュールから鍵情報を出力するための条件を明確化することを、E.11 は出力される鍵情報の完全性と機密性を保護するための方法を明確化することを要求したものである。
E.12～E.15 は対称鍵やプライベート鍵などが平文形式で入出力される場合の要求事項を明確化することを求めたものである。E.12 は平文形式で対称鍵やプライベート鍵などの入出力を行うための条件を、E.13 はエンティティ認証の手法を、E.14 は暗号モジュール外での保護方法を、E.15 は監査方法をそれぞれ明確化することを求めたものである。

上記のように、一般に暗号モジュールは、平文形式の暗号鍵への物理的保護を提供し、平文形式のまま暗号鍵が外部に露出しないようにしている。さらに、暗号モジュールは、その内部で対称鍵やプライベート鍵と公開鍵のペアを生成する機能を備えている。従って、暗号モジュールの外部に暗号鍵の出力を一切行わないように運用するのがよりセキュアといえるが、実際には暗号モジュールの故障対策や置き換えのために暗号鍵を外部に出力する機能や、外部から暗号鍵を入力する機能が必要となることもある。

このように、暗号モジュールにおける入力機能は、ひとつ又は複数の暗号鍵及び関連付けられたメタデータを、実使用の準備のために暗号モジュールに入力するために使用する。また、暗号モジュールにおける出力機能は、ひとつ又は複数の暗号鍵及び関連付けられたメタデータを、外部での使用もしくは保管（バックアップやアーカイブ）のために暗号モジュールから出力するために使用する。ここで、暗号モジュールから暗号鍵やメタデータを出力する場合、出力する鍵情報に対して暗号学的保護である機密性及び完全性の保護処理が適切に適用される必要がある。

外部にある鍵情報の保護は暗号学的保護により論理的に実現されるが、その暗号学的保護は元となる鍵暗号化鍵や鍵ラッピング鍵の管理状況に依存することには留意すべきである。また、レガシーシステムへの対応など何らかの理由により、平文状態で暗号鍵の入出力を許容する場合には、外部での平文状態での暗号鍵の保護がどのように実現されるかによって CKMS のセキュリティレベルに大きな影響が及ぶ可能性がある。E.12～E.15 に暗号モジュール外部への平文状態での暗号鍵の入出力に関わる FR が並んでいるのは、このためである。暗号モジュールで利用する対称鍵やプライベート鍵などの機密性保護を要する鍵に対して平文形式での入出力を行わない場合には、E.12～E.15 は検討対象外としてよい。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

E.08	本 CKMS では、CA プライベート鍵は原則として利用する HSM 内で生成するが、HSM のリプレイスや障害発生に備えて、HSM は鍵のバックアップ・アンド・リストアの機能を有している。鍵情報の入力は USB インタフェースに専用のストレージモジュールを接続して行われ、入力形式は HSM ベンダの独自仕様である。鍵情報の入力は、HSM のリプレイス時に、従来の HSM で使用していたプライベート鍵を新規の HSM でリストアして使用する場合などに行われる。
E.09	利用する HSM に外部から鍵情報を入力する場合、PKCS #11 API によって暗号化されて行われ、外部もしくは入力の過程における鍵情報の解読や改ざんから保護される。入力された鍵情報の完全性は HSM 内で検証する。
E.10	利用する HSM は、内部の CA プライベート鍵を含む鍵情報を外部に出力する機能を備える。本機能は鍵情報のバックアップ・アンド・リストアのためのものである。出力形式を含めて、バックアップ・アンド・リストア機能の詳細は HSM ベンダの独自仕様である。
E.11	利用する HSM から鍵情報を外部に出力する場合、PKCS #11 API によって暗号化されて行われ、外部での鍵情報の解読や改ざんから保護される。外部での保護レベルは、外部出力時に利用された鍵ラッピング鍵（key wrapping key）の管理に依存する。
E.12	本 CKMS で利用する HSM は署名用プライベート鍵の平文状態での入出力を行えないように設定されている。そのため、対象外である。

E.13	本 CKMS で利用する HSM は平文状態での署名用プライベート鍵、及び機密のメタデータの出力を行えないように設定されている。そのため、対象外である。
E.14	本 CKMS で利用する HSM は署名用プライベート鍵の平文状態での入出力を行えないように設定されている。そのため、対象外である。
E.15	本 CKMS で利用する HSM は署名用プライベート鍵の平文状態での入出力を行えないように設定されている。そのため、対象外である。

③ 暗号モジュールの危殆化に対する BCP 対策を定めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
E.16	FR6.109	CKMS 設計は、暗号モジュールの中身への物理的及び論理的アクセスがどのように認可されたエンティティに制限されるかを明記しなければならない。	6.8.4 節
E.17	FR6.110	CKMS 設計は、暗号モジュールの危殆化からの回復のために使用される方法を明記しなければならない。	6.8.4 節
E.18	FR6.111	CKMS 設計は、どの非侵襲攻撃がシステムで使用される暗号モジュールによって軽減されるかを記載し、どのように軽減が実行されるかの記載を提供しなければならない。	6.8.4 節
E.19	FR6.112	CKMS 設計は、非侵襲攻撃に脆弱であるあらゆる暗号モジュールを明記しなければならない。	6.8.4 節
E.20	FR6.113	CKMS 設計は、可能性のある非侵襲攻撃によって起きる脆弱性を受け入れる原則を明記しなければならない。	6.8.4 節

解説・考慮点

暗号モジュールの危殆化は、当該暗号モジュールに保持されている対称鍵及びプライベート鍵の危殆化の可能性を伴う。結果として、機密性の喪失、完全性の喪失、又は認証能力の喪失につながり得る。

暗号モジュールの危殆化の原因には、暗号モジュール内の暗号鍵へ直接アクセスする物理的手段、又は暗号モジュール内の暗号鍵についての知識を何らかの外部からの操作によって得る非侵襲的手段がある。
物理的手段に対する保護を提供するためには、認可されないアクセスが許可されない場所、又は認可されないアクセスが速やかに検出されるような仕組みがあるところで暗号モジュールは運用されるべきである。非侵襲的手段に対する保護を提供するためには、暗号モジュールの使用を信頼されるユーザに制限する、又は（特定の）非侵襲的手段による攻撃を防止するように設計された暗号モジュールを利用すべきである。

実際に暗号モジュールの危殆化又は危殆化の疑いがあった場合には、通常運用に戻る前に当該暗号モジュールをセキュア状態に再確立する必要がある。特に暗号モジュールの修理又は交換を行った場合には、セキュリティ状態の確認とともに機能確認のためのテストも行わなければならない。

CKMS の設計にあたって、項目 E.16 はエンティティ認証の手法を明確化することを、E.17 は危殆化が検知された後にどのような BCP[10]対策を行うかを明確化することを要求したものである。
E.18 は非侵襲的手段に対する事前対策を明確化することを、E.19 及び E.20 は対策の限界を明確化することを要求したものである。これは、あらゆる非侵襲的手段に対して完璧な対策を行うことはコスト的にも技術的にもほぼ不可能であることに原因がある。つまり、非侵襲的手段の種類によって、事前対策による被害軽減策がとられている部分と、残存リスクとして対策を取らない（あるいは不十分な対策である）部分とに予め整理しておくことに主眼がある。

上記のように、暗号モジュールの危殆化により、当該暗号モジュールに保持されている対称鍵及びプライベート鍵が危殆化する。その結果、CKMS が実現すべき機密性の喪失、完全性の喪失、又は認証能力の喪失につながり得る。

暗号モジュールの危殆化の原因には、暗号モジュール内の暗号鍵へ直接アクセスする物理的攻撃、及び、暗号モジュールの外部からの操作によって得られる暗号鍵に関わる情報を利用して最終的に暗号鍵を推定する非侵襲攻撃などがある。物理的攻撃は暗号モジュールの筐体などの囲いを除去する作業を伴うが、非侵襲攻撃はそうした作業を必要としない。ここで、非侵襲攻撃の具体例にはサイドチャネル攻撃と故障利用攻撃がある。代表的なサイドチャネル攻撃としては、暗号モジュールにおける暗号処理中の消費電力の変動を観測する電力解析と暗号処理の処理時間の変動を観測するタイミング攻撃などが知られている。また、故障利用攻撃としては、レーザ照射や電源グリッチ挿入などの外乱を与えることで暗号処理の結果を誤らせたデータを得て、正常な処理データとの差分を利用する差分故障解析などが知られている。緩和策が全くとられていない場合に、一度の処理データの観測だけで秘密鍵が判明するような攻撃もある。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

E.16	本 CKMS を収めた施設にはアクセス制御があり、利用する HSM への物理的攻撃及び非侵襲攻撃を実行可能な主体はアクセス制御を通過した主体に限定される。
E.17	まず、危殆化の要因が、HSM の物理的防御に関わるものか非侵襲攻撃への防御に関わるものかを明確にする。さらに、リスク評価を行って緩和策や対策の必要性、及び鍵更新の

[10] BCP: Business Continuity Plan（事業継続計画）。

	必要性を判断する。緩和策には、HSM を収容するエリアへのアクセスコントロールの見直しによって、アクセス可能な主体をより信頼できるメンバに限定すること等がある。対策は、より強固な防御機能を備えた HSM への置き換えとなる。ファームウェア更新によって防御を強化できる場合もある。なお、リスク評価の結果、鍵更新を必要とする場合は HSM 内で新たな鍵の生成を行い、それ以外はバックアップしておいた鍵をリストアする。
E.18	利用する HSM は内部に実装されている暗号処理機能に対して、サイドチャネル攻撃（DPA 及び SPA と呼ばれる電力解析）や故障利用攻撃（DFA）といった非侵襲攻撃の耐性を備えている。証明書及び CRL に付与する ECDSA 署名の生成処理において耐性がある。耐性を実現する具体的な緩和策は HSM ベンダのプロプライエタリ情報である。
E.19	利用する HSM は非侵襲攻撃に対する耐性を有している。ただし、非侵襲攻撃の種類や進化によって緩和策が有効でない場合もあり、HSM ベンダが提供する注意喚起情報を監視する必要がある。
E.20	利用する HSM は非侵襲攻撃への耐性を備えるが、非侵襲攻撃の進化によって現行の緩和策を破る手法が発見されるリスクはある。そうした場合でも多層防御として本 CKMS を収めた施設へのアクセス制御やアカウント権限管理等があり、非侵襲攻撃を実行可能な主体は多層防御を通過した主体に限定される。そのため、本 CKMS 全体でのリスクは低減される。また、非侵襲攻撃による HSM の危殆化が判明した場合は、対象となる非侵襲攻撃への耐性を強化した暗号処理 FW への更新やより強固な緩和策を備えた HSM への置き換えによってリスクの低減を図る。

3.1.3　人間による入力のコントロール

① 鍵情報の入力を人間に求める場合の要求事項を決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
E.21	FR6.97	それぞれの鍵とメタデータの管理機能に対し、CKMS 設計は、全ての人間による入力パラメタ、そのフォーマット、及び入力が行われないときに CKMS が取るアクションを明記しなければならない。	6.7.3 節

解説・考慮点

暗号鍵又は機微なメタデータの入力を人間に求める場合、それらの入力の正確さ（場合によってはセキュリティも）が担当する人間に依存する。また、必要な時に人間が適切に動いてくれるかどうかもわからない。一方、必要なときに CKMS が自動的に実行できるのであれば、そのシステムはユーザにとってより透過的になり、よりセキュアになる可能性がある。
項目 E.21 は、CKMS の設計にあたって、鍵情報の入力を人間に求める場合の要求事項を明確化することを求めたものである。

上記の「暗号鍵及び機微なメタデータ」とは、暗号鍵そのもの、鍵情報の生成に利用可能な情報、及び暗号鍵に紐づくメタ情報とする。暗号モジュール自体は堅牢であっても、人間による暗号鍵及び機微なメタデータの入力が存在する場合、その入力の正確さの課題やセキュリティ面の問題があり、リスク要因となる。人間による入力の具体例としては、人間の操作をエントロピー源として、鍵生成時のシードの一部を入力するケースが挙げられる。

人間による鍵情報の入力としては様々なケースがあるが、ここでは人間の関与によって入力あるいは生成された鍵情報の一部に影響が及ぶかどうか、あるいは、入力処理のほとんどが機械化（自動化）して行われ人間が関与する処理はごく一部に過ぎないかどうか（例えば、鍵情報の記憶された媒体をアタッチする操作のみであれば人間の関与は少ない）、によって項目 E.21 の該否を判断するとよい。

項目 E.21 は人間による鍵情報の入力を求める場合の入力パラメータ・フォーマット、入力が行われないときの CKMS のふるまいを明確にすることを求めている。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

一般に HSM 製品の利用においては項目 E.21 に該当するケースがないことが望ましい。しかしながら、HSM 製品を利用するユースケースの中には、マルチパーティコントロールによって分割した鍵コンポーネントを HSM に入力する際に、人間がキーボードから鍵コンポーネントを入力する運用事例がある。そのような運用を行う場合には項目 E.21 を検討対象とすべきである。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

E.21	本プライベート CA では該当するケースはないので対象外。

3.1.4 マルチパーティコントロール

① 暗号鍵管理機能を実行するために複数のエンティティの協力を必要とする場合の概要を明確化しなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
E.22	FR6.98	CKMS 設計は、マルチパーティコントロール（multiparty control）を要求する全ての機能を明記し、それぞれの機能に対して k と n を規定しなければならない。	6.7.4 節
E.23	FR6.99	それぞれのマルチパーティ機能に対して、CKMS 設計は、なぜ n 個中任意の k 個のエンティティで望む機能を有効にできるが k-1	6.7.4 節

		個のエンティティでは有効にできないのかを示すあらゆる既知の論拠（論理、数学）を引用又は明記しなければならない。	

解説・考慮点

ある種の暗号鍵管理機能を実行するために複数のエンティティの協力を必要とする場合に利用する一手法であり、当該機能を実行する前に、n 人中 k 人のエンティティが ACS で認証・認可されることを要求する。暗号鍵管理機能の中でも高度に機微な機能が対象となる。
CKMS の設計にあたって、項目 E.22 はマルチパーティコントロールで管理される機能及び利用条件を明確化することを、E.23 は採用する方式の安全性を明確化することを要求したものである。

マルチパーティコントロールは複数のエンティティの協力によって、ある種の処理を実行可能とする機能である。ここで、n エンティティのうち任意の k エンティティ以上の協力が得られれば所定の処理を実行できるが、k エンティティ未満の協力下では処理を実行できない。

マルチパーティコントロールは、機微な権限の取得や高度な管理を要する鍵情報の分散管理に利用されることが多い。例えば、管理者権限のエンティティ認証・認可やマスター鍵/鍵導出鍵のバックアップ・アンド・リストアに利用される。ここで暗号鍵自体をマルチパーティコントロールによって分割する場合は次の②の項目 E.24 と E.25 にも該当する。

なお、一般にマルチパーティコントロールの実現メカニズムは、対象機器やシステムを構築するベンダのプロプライエタリ情報である。従って、マルチパーティ機能の原理説明に関わる項目 E.23 を CKMS 要件とするかどうかはシステム設計者や調達者が判断し、CKMS 要件とする場合はベンダに説明を要求することとなる。その際、メカニズムの説明は原理を説明する論文へのポインタ情報程度でもよい。

マルチパーティコントロールで管理される機能がない場合には本節の FR は対象外である。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

本トイモデルにおけるマルチパーティコントロールは HSM により提供される。HSM により提供されるマルチパーティコントロールの実現メカニズムの内容は、一般に HSM ベンダのプロプライエタリ情報である。ここでは HSM ベンダによる説明が得られたケースを想定して E.23 の例を記載した。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

E.22	本 CKMS では利用する 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使用

	する。その際、CKMS 管理担当の中で HSM 管理者として予め登録した 3 エンティティのうち 2 エンティティの認証を必要とする。 本 HSM 内の鍵情報のバックアップ・アンド・リストアを実施する場合には HSM の管理者権限を必要とするように設定されている。
E.23	本 CKMS で利用する HSM では次のメカニズムによってマルチパーティコントロールを実現している。予め Shamir の秘密分散（2 out of 3）により、管理者権限取得のための認証情報が 3 つの share に分割され、異なる USB ドングルに格納される。各エンティティは USB ドングルを順次接続した上で、USB ドングルのアクティベート PIN を入力することにより、share が HSM に転送され、HSM 内で集まった share 群から認証情報が復元される。

② 暗号鍵を鍵分割する場合の概要を明確化しなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
E.24	FR6.100	CKMS 設計は、鍵分割技術を使用して管理される全ての鍵を明記しなければならず、またそれぞれの技術に対して n と k を明記しなければならない。	6.7.5 節
E.25	FR6.101	使用しているそれぞれの（k, n）鍵分割技術に対して、CKMS 設計は、鍵分割がどのように行われ、なぜ n 個中任意の k 個の分割鍵で鍵を構成できるが k-1 個の分割鍵では鍵に関する情報を何ら提供しないのかを示すあらゆる既知の論拠（論理、数学）を明記しなければならない。	6.7.5 節

解説・考慮点

CKMS の設計にあたって、項目 E.24 は鍵分割で管理される対象の暗号鍵及び鍵分割の利用条件を明確化することを、E.25 は採用する方式の安全性を明確化することを要求したものである。

本節の①に記載したように、マルチパーティコントロールの一形態として鍵分割がある。n 個の分割鍵（share）のそれぞれが n 人のエンティティに割り当てられ、そのうち任意の k 人のエンティティが協力しない限り元の暗号鍵が構成できない仕組みである。ここで k 人未満のエンティティの協力（すなわち k-1 個以下の share）では元の暗号鍵の情報は一切得られない（すなわち share が全くない状態と情報理論的に情報量が変わらない）ことが特徴である。

鍵分割によるマルチパーティコントロールが効果を発揮するためには分割鍵の管理を適正に行うことが重要である。例えば、複数の分割鍵を一人のエンティティが利用できるような状況にあってはならないし、分割鍵へのアクセス権限を持つエンティティ間で結託が行われるような状況があってはならない。

鍵分割は、多くの他の暗号鍵を保護し、その危殆化が深刻な悪影響をもたらすようなマスター鍵/鍵導出鍵のバックアップ・アンド・リストアを実施するために、分割鍵を暗号モジュールに入出力する場面で使用されることが多い。

本節の①と同様に、一般に鍵分割の実現メカニズムは、対象機器やシステムを構築するベンダのプロプライエタリ情報である。従って、鍵分割機能の原理説明に関わる項目 E.25 を CKMS 要件とするかどうかはシステム設計者や調達者が判断し、CKMS 要件とする場合はベンダに説明を要求することとなる。その際、メカニズムの説明は原理を説明する論文へのポインタ情報程度でもよい。

鍵分割技術を利用して管理される暗号鍵がない場合には検討対象外である。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

E.24	本 CKMS で利用する 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使用する。その際、E.23 に記載のように認証情報の分割に暗号鍵分割に相当する手法を利用するが、分割対象は暗号鍵ではないため、E.24 は対象外である。
E.25	E.24 と同じ理由により、E.25 は対象外である。

3.2 セキュリティ評価・試験

解説・考慮点

本節は、SP 800-130 の 9.1 節から 9.7 節に記載されている事項について解説したものである。

セキュリティ評価・試験におけるテストスイートに合格することの価値は、選択したテストケースの包括性及び代表性に直接関連する。一方、全ての可能性の組み合わせ数よりはるかに少ない有限個のケースに限定されるため、デバイス又はシステムが全てのケースにおいて正しい又はセキュアであることを保証しないことに留意されたい。
調達者又はユーザは、どのテスト結果を必要とするのかを事前に決める必要がある。さらに提供されたテスト結果をレビューし受入可能かどうかを判断するのか、事前に満たすべき条件を指示しておくのか決めておくべきである。

本節の各テストの概要は SP 800-130 の該当節も参照されたい。SP 800-130 の該当節の記載では、ここでのテスト対象が CKMS 全体なのか、CKMS の構成要素であるデバイスなのかがあいまいであるが、原則としていずれも CKMS 全体を対象としたテスト項目と捉えるのが良い。ただ

し、テスト項目の中でデバイスでのテストを実施すれば十分と判断できるものや、デバイスでのテスト結果をベンダに要求すべきと判断するものはデバイスでのテスト項目として実施する。

暗号モジュールに相当するデバイスを対象にテストを実施する場合には、本節のテスト項目のうち①ベンダテスト、③機能テスト及びセキュリティテスト、④環境テスト、⑤セルフチェックテスト、⑦第三者テストを選定するとよい。なお、一般に、FIPS 140-2/-3 や ISO/IEC 15408 などのセキュリティ認証を取得済の暗号モジュールであれば、これらのテストは認証取得時の試験によって満たしていると判断するのも妥当である。

① ベンダテストの実施概要を明確化しなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
E.26	FR9.1	CKMS 設計は、システムで実行され合格した非プロプライエタリベンダテストを明記しなければならない。	9.1 節

解説・考慮点

ベンダが自ら実施するテストである。テストの技術及び仕様は、ベンダによるプロプライエタリ情報と見なされることが多く、一般に公開されない。
項目 E.26 は、CKMS の設計にあたって、調達者又はユーザがレビュー可能なベンダテストの実施概要を明確化することを要求したものである。

調達側としては、非プロプライエタリな情報で提供可能なテスト結果の有無をベンダに確認することが本 FR の対応となる。なお、FIPS 140-2/-3 や ISO/IEC 15408 などのセキュリティ認証を取得した製品であれば認証時の試験内容で十分と判断することもできる。一方、セキュリティ認証を取得していない製品を採用する場合や、特に確認の必要なテスト内容がある場合には、ベンダに相談すべきである。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

E.26	利用する HSM は FIPS 140-2/-3 レベル 3 のセキュリティ認証を取得しており、認証時の試験によって本件に相当するテストはカバーされていると考え、対象外とする。

② 相互運用性テストの実施概要を明確化しなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
E.27	FR9.3	CKMS が他のシステムとの相互運用性を主張する場合、CKMS 設計は、その主張を検証するために実行し合格したテストを明記しなければならない。	9.3 節
E.28	FR9.4	CKMS が他のシステムとの相互運用性を主張する場合、CKMS 設計は、相互運用性に必要な、あらゆる構成設定（configuration settings）を明記しなければならない。	9.3 節

解説・考慮点

2 つ以上のデバイスを相互接続し、互いに運用することができるかどうかのテストである。ただし、個々のデバイスの内部機能自体をテストしているわけではないので、その機能が正しく動作することを検証しているとは限らない。テスト対象デバイスと保証ベースラインデバイスが異なる組織によって独立に設計・実装されていれば、このテストはより信用できる。
CKMS の設計にあたって、項目 E.27 は、相互運用性テストの実施概要を明確化することを、E.28 は相互運用するための要求条件を明確化することを求めたものである。

相互運用性テストの一般的な形式は、対向接続試験である。SP 800-130 には、テスト対象装置（device under test）と保証ベースライン装置（assured baseline device）との相互運用をテストすることにより、テスト対象装置の正常動作を確認するケースが示されている。

暗号モジュールなどのデバイスレベルのテストは、それを利用する上位のシステムとの間で API の機能テストを実施することが一般に行われており、次の③の機能テストと捉えることができる。

本ガイダンスにおいて相互運用性テストとは、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（ゴールデンデバイスと呼ばれることもある）との接続試験を行うものとして解釈することとする。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

本 CKMS の直接の連携先は IoT 製品向け証明書管理端末に限定される。ここで証明書管理端末向けに提供するサービスは IoT 製品向けの証明書発行及び証明書の失効に関わる CRL の生成である。これらのサービスに関わるプロトコルは単純であるため、本 CKMS の提供するサービス自体は機能レベルのテストとして実施することができ、本ガイダンスでの解釈に該当する相互運用性テストを実施する必要はない。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

E.27	本 CKMS では相互運用性テストに相当する特段のテストを実施する必要はなく、非該当とする。

E.28	同上

③ 機能テスト及びセキュリティテストの実施概要を明確化しなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
E.29	FR9.7	CKMS 設計は、システムで実行された機能テスト及びセキュリティテスト、並びにそのテスト結果を明記しなければならない。	9.6 節

解説・考慮点

機能テストとはある機能の実装が正しく動作することを検証するテストであり、セキュリティテストとはある機能の実装がセキュアに機能することを検証するテストである。このため、暗号アルゴリズムの実装が正しく機能する（機能テストに合格）一方で、暗号処理中の電力消費の変動等が暗号鍵の危殆化につながり得ると判定（セキュリティテストに不合格）することがある。
ペネトレーションテストは特別な種類のセキュリティテストである。ペネトレーションテストのエキスパートチームが攻撃シナリオを開発して、ペネトレーション成功のリスクを評価する。初期運用開始前及び大規模変更後の運用再開前にペネトレーションを実施し、発見されたあらゆる課題に事前に対処すべきである。なお、スコープには、人的、設備及び手続きを含むべきである。
項目 E.29 は、CKMS の設計にあたって、機能テスト及びセキュリティテストの実施概要を明確化することを要求したものである。

機能テストは、CKMS の適切な動作を保証するために様々なレベルで実施される。これには、個々のデバイスやコンポーネントなど、CKMS の構成要素レベルでのテスト及び CKMS 全体が提供する機能レベルでのテストが含まれる。これらのテストは、システム開発における単体試験、結合試験及び総合試験に対応しており、個々の機能からシステム全体の統合的な動作までを評価することを目的とする。

セキュリティテストは、システムや実装の堅牢性を評価し、機密性・完全性・可用性といったセキュリティ要件を満たしているかを確認するための重要なプロセスである。このテストでは、暗号鍵やパスワードなどの秘匿すべき情報が、権限のないエンティティから適切に保護されているかを検証する。また、暗号鍵、プログラムコード、権限設定情報など、保護すべきデータが改ざんから適切に保護されているかを評価する。

セキュリティテストを実施する際には、どのような攻撃を想定するか、利用する解析手法やツールを明確に定義することが求められる。攻撃者のスキルレベルは、初歩的な IT エンジニアから国家レベルの専門家集団まで幅広く存在し、保護対象の資産価値に応じて想定する攻撃者像を設定する必要がある。この攻撃者像に基づいて、要求されるセキュリティレベルが大きく変化する。

ペネトレーションテストは、こうした攻撃者を想定したセキュリティテストの代表的な方法であり、専門家チームが対象システムに実際に侵入を試み、攻撃が成功する可能性を評価する。こ

のプロセスでは、攻撃者のスキル、使用するツール、攻撃に要する時間、攻撃手順といった要素を定量的に採点し、防御能力をスコアリングする場合もある。外部機関にペネトレーションテストを依頼する場合、コストや時間がかかることが多いため、設計情報を活用した簡易的な内部テストで代替するケースもある。

また、ペネトレーションテスト以外にも脆弱性診断の様々な手法が存在する。例えば、静的解析ツールを使用してプログラムコードの脆弱性を検出する方法や、ファジングを用いて異常なデータ入力への耐性を評価する方法がある。ファジングは、通信プロトコルだけでなく、ファイル形式、API（アプリケーションプログラミングインタフェース）、CLI（コマンドラインインタフェース）、OS やデバイスドライバなど、広範な対象に適用される手法である。これにより、入力検証の不備やエラーハンドリングの欠陥を検出できる。

一方で､暗号アルゴリズムそのものや､暗号を利用したセキュリティプロトコル全体の解析は、セキュリティテストには通常含まれない。これらの要素については、業界で推奨されている方式であるか、選定時に既知の脆弱性が報告されていないかを確認することで対応する。

調達するデバイスの機能テスト及びセキュリティテストについては、ベンダに提供可能な情報を確認することが項目 E.29 の対応となる。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

E.29	● 利用する HSM の機能試験の結果及び実装の堅牢性に関わるテスト結果について、ベンダに提供可能な情報を確認する。 ● 本プライベート CA のシステムレベルの機能テストとして、結合試験、総合試験の結果を報告書で確認する。 ● 本プライベート CA のセキュリティテストとして、プログラムコードの脆弱性診断を含むセキュリティテスト仕様書を作成し、内部で実施したテスト結果を報告書にまとめる。

④ 環境テストの実施概要を明確化しなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
E.30	FR9.8	CKMS 設計は、CKMS が使用される設計上の環境条件を明記しなければならない。	9.7 節
E.31	FR9.9	CKMS 設計は、CKMS デバイスで実行された環境テストの結果を、設計上の条件を超えたストレスをデバイスに与えた時の全てのテストの結果も含めて、明記しなければならない。	9.7 節

解説・考慮点

デバイスやシステムに対して特定の利用環境（例えば、温度範囲及び電圧範囲）を仮定することが多い。この場合、当該デバイスやシステムはその利用環境用に構築され、決められた範囲内でのみテストされる。もし範囲外の利用環境で当該デバイスやシステムが使用されると、セキュアな運用が失われる可能性がある。 CKMS の設計にあたって、項目 E.30 は設計上の利用環境条件を明確化することを、E.31 は環境テストの実施概要を明確化することを要求したものである。なお、E.31 では、設計上の利用範囲外の環境でのテストを実施した場合にはその結果も含めることを要求していることに留意されたい。ただし、利用範囲外の環境でのテスト結果が悪かったとしても、それ自体に問題があるわけではない。

環境テストは、温度や供給電圧などの環境条件を変えたときの CKMS の挙動を検査するものである。一般に環境条件は設計上の動作可能範囲として定められており、その範囲で正常な動作を行うこと、セキュアに機能することが確認できれば良い。

項目 E.31 は設計上の環境条件を超えた場合のテスト結果に関わる FR である。FIPS140-3 レベル 3 の物理セキュリティには環境故障保護(Environment Failure Protection)の機構を備えるか、環境故障試験(Environment Failure Test)に合格することの要件があり、これらが相当する。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

E.30	本 CKMS を構成する各デバイスの仕様上の環境条件に基づいて、CKMS として設計上の環境条件を定める。
E.31	利用する HSM は FIPS 140-3 レベル 3 の認証を取得した製品であり、セキュリティポリシーによって HSM の環境条件を超えた場合の保護機構もしくは試験結果を確認する。

⑤ セルフチェックテストの概要を明確化しなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
E.32	FR9.5	CKMS 設計は、設計者によって作成及び実装された全ての自己テスト、及びそれが正しい動作を検証する対象の CKMS 機能を明記しなければならない。	9.4 節

解説・考慮点

セルフチェックテストとは、完全性及びセキュリティ障害に対してデバイスが自分自身を定期的にテストする機能である。

項目 E.32 は、CKMS の設計にあたって、セルフチェックテストの概要を明確化することを要求したものである。

セルフチェックテストの例として、FIPS 140-2/-3 において要件としている自己テスト機能があり、動作前自己テストと条件自己テストを要求している。動作前自己テストでは電源投入時やリセット直後にファームウェア完全性のテストを実施する。条件自己テストでは暗号アルゴリズムを最初に利用する前に暗号アルゴリズム自己テストの実施が要求される他に、公開鍵・プライベート鍵ペアを生成した際に鍵ペア整合性テストの実施などが要求される。

汎用的な PC において実施されるブート時に起動するソフトウェアの完全性を検査するセキュアブート処理もセルフチェックテストに該当する。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

E.32	● 本プライベート CA のサーバはセキュアブート処理により、電源投入時やリセット後にロードするファームウェアやプログラムコードを検証する。 ● 採用する HSM のセキュリティポリシーを参照して、搭載されている自己テストの内容と各自己テストが実施される条件を確認する。

⑥ スケーラビリティテストの実施概要を明確化しなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
E.33	FR9.6	CKMS 設計は、今までにシステムで実行された全てのスケーラビリティ分析及びテストを明記しなければならない。	9.5 節

解説・考慮点

プロセスが増大する負荷に適応してデバイスやシステムの処理能力を拡大する必要があるため、与えられた時間内で処理するトランザクション数又は取り扱うユーザ数が劇的に増加したときにデバイスやシステムがどのように反応するかを見極めるために行うテストである。デバイスやシステムが完全に運用される前にスケーラビリティの問題を認識して、必要な負荷軽減策を検討するために行われる。 項目 E.33 は、CKMS の設計にあたって、スケーラビリティテストの概要を明確化することを要求したものである。

項目 E.33 は CKMS のシステムレベルのスケーラビリティテストに関わる FR である。一般に負荷テストと呼ばれる。CKMS の負荷が増大した場合にどこがボトルネックとなるか、高性能なデバイスへの更新やデバイスの増設で対処可能かを予めテストすることを求めている。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

E.33	本プライベート CA を構成するサーバや HSM、ネットワーク機器などをモジュール化した設計とし、負荷の分散を可能としておく。ロードテストやストレステストを実施し、ピーク性能の確認や負荷の集中による障害発生時の回復作業を確認する。

⑦ 第三者テストの概要を明確化しなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
E.34	FR9.2	CKMS 設計は、CKMS 又はデバイスが今までに合格した全ての第三者テストプログラムを明記しなければならない。	9.2 節

解説・考慮点

ベンダが自身のテスト手順のなかで欠陥を見逃していないことの信頼性を提供するために第三者によって行われるテストのことである。
項目 E.34 は、CKMS の設計にあたって、第三者テストの概要を明確化することを要求したものである。

暗号標準や推奨事項への製品適合の検証プログラムとして、ISO/IEC 15408 認証、FIPS 140-2/-3 認証（CMVP 認証）、CAVP 認証等が代表例である。これらの認証を取得した製品は CCRA や NIST のサイトで検索可能である。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

E.34	本プライベート CA システムで採用する HSM は FIPS 140-2/-3 レベル 3 認証を取得した製品である。ベンダに対して認証書やセキュリティポリシーの提供を依頼する。

3.3　暗号モジュールの障害時の BCP 対策

解説・考慮点

暗号モジュールには、セキュリティ機能、鍵情報（暗号鍵やメタデータ）など、CKMS のセキュリティを確保するための様々な情報が内包されている。このため、暗号モジュールが障害を起こすことは CKMS のセキュアな運用ができなくなることを意味する。本節では、暗号モジュールに障害が発生した場合の対策を取り扱う。

暗号モジュールの障害は CKMS の運用に影響を及ぼし、さらには CKMS がサービスを提供するシステムの機能不全や情報喪失につながるおそれがある。

① 暗号モジュール障害発生時における BCP 対策を定めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
E.35	FR10.8	CKMS 設計は、モジュールのエラー検知及び完全性検証のために、それぞれの暗号モジュールがどの自己テストを使用するかを明記しなければならない。	10.6 節
E.36	FR10.9	CKMS 設計は、それぞれの暗号モジュールがどのように検知したエラーに応答するかを明記しなければならない。	10.6 節
E.37	FR10.10	CKMS 設計は、障害が起こった暗号モジュールの修理又は交換の方策を明記しなければならない。	10.6 節

解説・考慮点

暗号モジュールは、ハードウェア、ソフトウェア又はファームウェアの障害を検知するために適切に組み込まれたテスト機能を備えるべきである。テストの結果、暗号モジュールがエラー状態にある間は、機微なデータが暗号モジュールから出力されるべきではない。

CKMS の設計にあたって、項目 E.35 は暗号モジュールの障害検知のために組み込まれたテストに関する概要について明確化することを、E36 は障害を検知した時に直ちに取るべき対応策を明確化することを、E.37 は復旧に向けて障害が検知された後にどのような BCP 対策を行うかを明確化することを要求したものである。
なお、E.37 については、E.17 と同様、通常運用に戻る前に当該暗号モジュールをセキュア状態に再確立する必要がある。エラーが回復可能なものであるならば、暗号モジュールを再起動した後、通常処理を続行する前に全てのパワーアップセルフチェックテストを実施してエラーが解消されたことを確認しなければならない。また、暗号モジュールの修理又は交換を行った場合には、セキュリティ状態の確認とともに機能確認のためのテストも行わなければならない。

暗号モジュールに対するセルフテスト（自己テスト）機能として FIPS 140-2/-3 では以下に示すことを要件としている。暗号モジュールの自己テストとして、動作前自己テスト及び条件自己テストがあり、暗号モジュールはこれらの自己テストを実行して成功か失敗かを判定する。自己テストに失敗した場合はエラー状態に遷移し、エラーインジケータが出力される。エラー状態では暗号処理やデータ出力を行うことはできない。

暗号モジュールが再起動をしてもセルフテストによるエラー状態から回復しない場合は暗号モジュールを交換することとなる。そうした状況に備えて、暗号モジュール内の鍵情報のバックアップを事前に取得しておくべきであり、交換後の暗号モジュールへの鍵情報のリストアやエラー状態となった暗号モジュールの廃棄処理などの手順を定めておくべきである。

本節の FR は上記のような FIPS 140-2/-3 の要件を満たす暗号モジュールを念頭にしたものと捉えると理解しやすい。

なお、暗号モジュールの汎用的な BCP 対策として、CKMS がサービスを提供するシステムの要件に合わせて、暗号モジュールの提供ベンダと適切な保守契約を結ぶことを推奨する。こうした保守契約がないと、ベンダから最新のファームウェアが提供されないことや暗号モジュールに不具合が発生した際の回復がベンダのサポートがないために実行できない等の事態が懸念されるためである。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

E.35	本プライベート CA システムで利用する HSM は FIPS 140-2/-3 レベル 3 認証を取得しており、実装されている暗号処理に関わるセルフテスト機能を備えている。セルフテストには動作前自己テストと条件自己テストの両テストを備えている。
E.36	本 HSM はセルフテストでエラーを検知した場合はエラー状態となり、エラーインジケータが出力される。エラーインジケータとして処理要求に対して応答不能コードが返される。エラー状態では暗号に関わるデータ出力や暗号処理を行えない。
E.37	● 本 HSM がエラーを出力した場合、HSM 管理者は HSM の再起動により、エラー解除を試みる。エラー状態から回復しない場合は、HSM の初期化、破壊などマニュアル記載の HSM 廃棄に関わる手続きを実施する。 ● 予め HSM 障害時の対応を想定して HSM 内の鍵情報のバックアップを作成しておく。HSM のエラーが回復しない場合は、新たな HSM をセットアップし、バックアップした鍵情報をリストアして、新たな HSM に交換する。 ● HSM ベンダと障害時の対応を踏まえた保守契約を締結しておき、障害発生時にベンダサポートを受けられるようにしておく。

4 暗号鍵管理システム（CKMS）のオペレーション対策

本章の目的・趣旨

本章は、「設計指針」の 9 章に記載されている要求事項（各節での灰色枠内で示している内容）について解説したものである。

CKMS 全体に対して、必要に応じて検討する項目（F.01～F.57）を集めている。ここには、主に以下のような検討項目を含んでいる。

- CKMS 全体に対する包括的なセキュリティ対策（物理的対策、マルウェア対策、脆弱性対策、侵入防御対策、システム監査など）をどうするか
- CKMS 全体のセキュリティアセスメントをどのように実施するか
- CKMS への危殆化・障害・災害発生時の BCP 対策をどのように準備するか

ここでの検討項目も「広義」の意味での暗号鍵管理に相当するものの一つであり、CKMS 全体を対象としている。個々の暗号鍵管理のためではなく、システムとしての暗号鍵管理が正常に機能するようにするための検討項目になっており、CKMS 全体のオペレーション対策や物理的な対策を含めた総合的な対応を対象としたシステム設計を行う場合に検討する必要がある。

4.1 CKMS へのアクセスコントロール

解説・考慮点

本節は、SP 800-130 の 8.1 節、8.2 節、8.3 節に記載されている事項について解説したものである。
アクセスコントロールには、セキュリティ境界において、認可されたエンティティのみがセキュリティ境界内部に入れるようにするための門番としての役割がある。これらが、暗号モジュールやセキュリティ境界内部の CKMS デバイス等と連携して CKMS のセキュリティを確保している。本節では、セキュリティ境界内部の CKMS デバイス等をセキュアに保つためのアクセスコントロールの方法について取り扱う。

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。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.01	FR8.1	CKMS 設計は、それぞれの CKMS デバイスと意図する目的を明記しなければならない。	8.1 節

F.02	FR8.2	CKMS 設計は、CKMS コンポーネントを含むそれぞれのデバイスを保護するための物理セキュリティコントロールを明記しなければならない。	8.1 節
F.03	FR6.120	CKMS 設計は、全ての CKMS コンポーネント及びデバイスがどのように認可されない（不正な）物理アクセスから保護されるかを明記しなければならない。	6.8.8 節
F.04	FR6.121	CKMS 設計は、CKMS がどのように認可されない（不正な）物理アクセスを検知するかを明記しなければならない。	6.8.8 節

解説・考慮点

CKMS では、コンポーネント、デバイス及び CKMS 内に含まれる機微なデータの窃取及び改ざん、又はハードウェアやソフトウェアの改ざんから保護するため、CKMS コンポーネント及びデバイスは物理的に保護されるべきである。それらのセキュリティの重要性に応じて、一つ以上の物理的保護メカニズムが選択される。

CKMS の設計にあたって、項目 F.01～F.04 は、CKMS コンポーネント及びデバイス等に対する物理セキュリティの要求事項を明確化することを求めたものである。F.01 は CKMS デバイスの利用環境・場所や利用目的、F.02 はコンポーネント及びデバイスに対する保護手段についての検討項目であり、SP 800-130、8.1 節に保護手段の参考例が掲載されている。F.03 及び F.04 は保護手段の運用条件に関する検討項目である。

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。

上記のように、SP 800-130、8.1 節には施設や収容エリアへの物理アクセスに関わる保護メカニズムや物理的侵入の検知メカニズムが例示されている。

施設に関わる物理セキュリティの要件や基準について、以下のような文献が参考になる。

- 「データセンター　セキュリティ　ガイドブック」、日本データセンター協会
- 「金融機関等コンピュータシステムの安全対策基準・解説書」、金融情報システムセンター

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。CKMS を収容するエリアや CKMS を構成するデバイスに関わる物理的保護については、CKMS の利用や運用に関わるエンティティに物理アクセスを制限するように構築されるが、建物や施設全体は

CKMS に関わらない従業員も入構が許可されるので、物理アクセスを許可する範囲が段階によって異なる性質がある。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。図 4-1 に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示す。各保護エリアにアクセスするために必要となるクレデンシャル（認証用の識別情報）を白矢印に示しており、エリアごとに異なるクレデンシャルが必要となるように設計されている。

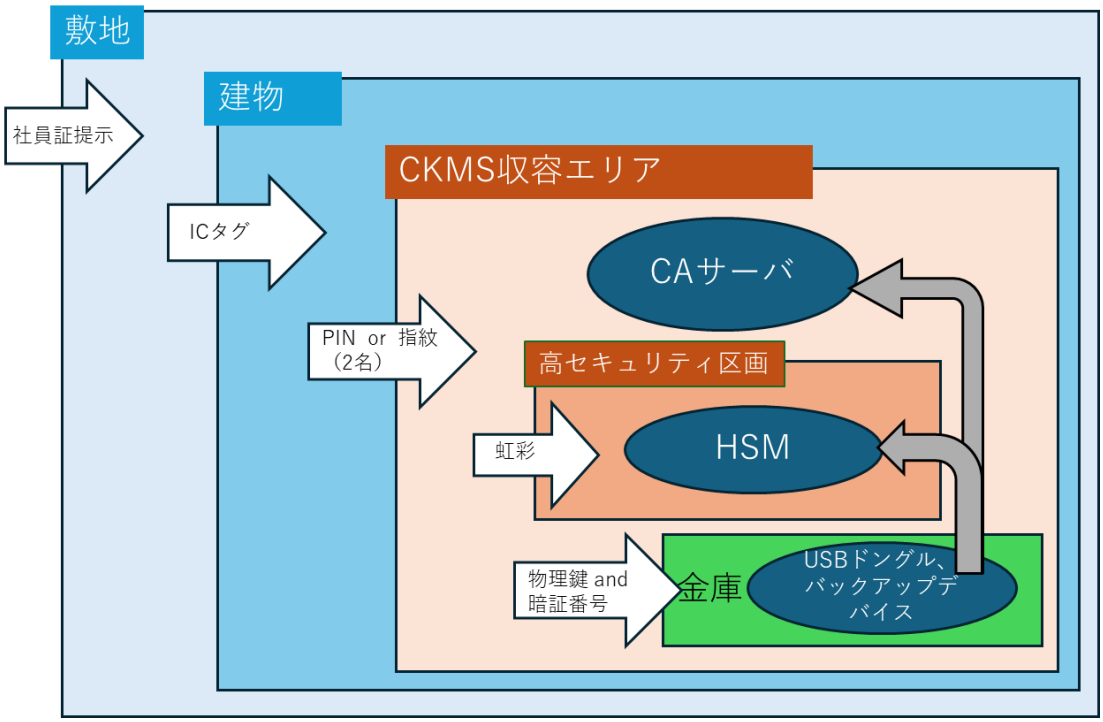


図 4-1 トイモデルにおける物理アクセスコントロール

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.01	当該 CKMS を構成する HSM、CA サーバ、さらに、HSM 内鍵情報のバックアップ用デバイス、及び HSM の管理者権限取得に必要となる USB ドングルは物理的保護を必要とする。
F.02	当該 CKMS では、物理的アクセスコントロールとして、敷地のフェンスと警備員、建物と CKMS を収容した部屋（図 4-1 の CKMS 収容エリア）の入退室管理機能、HSM を収容したラック扉（図 4-1 の高セキュリティ区画）の施錠機能、HSM の管理者権限取得に必要な USB ドングルや鍵情報のバックアップ用デバイスを保管した金庫がある。 さらに、暗号モジュールの物理的保護メカニズムとして FIPS 140-2/-3 レベル 3 の HSM における筐体の物理的保護がある。
F.03	F.02 に記載した物理的アクセスコントロールについて、敷地内にアクセスするには敷地

	入り口での社員証提示、建物に入る際は社員証内タグによるドア開錠、CKMS 収容エリアへの入室には PIN もしくは指紋認証による入り口扉の開錠、HSM を収容したラック扉の開錠には虹彩認証、USB ドングルやバックアップデバイスを保管した金庫の開錠には暗証番号及び物理鍵がそれぞれ必要である。ここで、CKMS 収容エリアの入り口扉の開錠には、内部不正の相互監視を主たる目的として複数名での入室認証を必要とする。また、メンテナンスや監査などの目的で部外者を CKMS 収容エリアに入室させる場合には、PC やスマートフォンなどの情報機器の持ち込みを含めて事前登録を必要とし、敷地入り口で警備員が確認する。
F.04	CKMS 収容エリアの入り口や室内には監視カメラが設置され、不審者を警備員が監視している。また、暗証番号の不一致が一定回数連続した場合には不審なアクセスとして警備員に通知される。

4.1.2 コンピュータシステムセキュリティコントロール

① OS に対するセキュリティの要求事項を決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.05	FR8.3	CKMS 設計は、それぞれの CKMS デバイスに対して、全てのセキュアな OS の要求事項（いかなる必要な OS 設定も含む）を明記しなければならない。	8.2.1 節
F.06	FR8.4	CKMS 設計は、下記のどの堅牢化機能が CKMS によって実行されているかを明記しなければならない： a) 全ての必須でないソフトウェアプログラムとユーティリティをコンピュータから削除する b) 危殆化を受けやすいシステム機能及びアプリケーションに対するアクセスコントロールに最小権限の原則を適用する c) 危殆化を受けやすいシステム及びアプリケーションのファイルとデータに対するアクセスコントロールに最小権限の原則を適用する d) ユーザアカウントを合理的な運用に必要なだけに制限する、すなわち、もはや必要のないアカウントは無効化又は削除する e) 最小権限の原則でアプリケーションを動作させる f) 全てのデフォルトパスワード及びデフォルト鍵をそれぞれ強力なパスワード及びランダムに生成された鍵で置き換える g) システムの運用に必要でないネットワークサービスを無効化又は削除する	8.2.1 節

		h) システムの運用に必要でない全ての他の処理（service）を無効化又は削除する i) リムーバブルメディアを無効化する、又はリムーバブルメディアにおける自動実行機能を無効化しメディア挿入時の自動マルウェアチェック機能を有効にする j) システム運用に必要でないネットワークポートを無効化する k) オプションのセキュリティ機能を適切に有効化する l) セキュアにする他の設定オプションを選択する	
F.07	FR8.5	CKMS 設計は、OS の正しいインスタンス化を保証する BIOS 保護機能を明記しなければならない。	8.2.1 節

解説・考慮点

セキュアな OS はセキュアなコンピュータシステムの基礎であり、それなしにコンピュータシステム上でプログラム及びデータのセキュリティを保証することができない。
CKMS の設計にあたって、項目 F.05～F.07 は、CKMS デバイス等に搭載される OS に対するセキュリティの要求事項を明確化することを求めたものである。これには、OS 自体のセキュリティだけでなく、当該 OS 上で動作するソフトウェアやユーザ等の管理に対する要求事項も含む。SP 800-130、8.2.1 節にセキュリティ機能の参考例が掲載されている。

CKMS はコンピュータデバイス上に構築され、コンピュータデバイス上の OS によって、コンピュータ上のエンティティ認証とアカウント管理、各種操作に対する権限管理やプロセス管理、ソフトウェアコードのインテグリティチェック、ソフトウェアアップデート時のアップデートコードの署名検査、操作ログの管理、など様々なセキュリティコントロールに関わる機能が提供される。本節は CKMS が動作するコンピュータ環境におけるセキュリティコントロールのうち、OS によって実施される内容を整理することを求めている。

なお、IoT 向けの小規模デバイスなどで OS がないデバイスや、ファームウェアの更新やソフトウェアの追加を不可とするよう機能が制限されたデバイスもある。そのように機能が限定されたコンピュータデバイスでは本節の項目の多くが非該当となる。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.05	当該 CKMS では CA サーバ上の Linux OS において CKMS のエンティティ管理と権限管理などのセキュリティコントロールが行われる。

F.06	当該 CKMS の CA サーバ上の Linux OS によって次の堅牢化設定を行う。 a) CA としての機能を稼働させるために必須ではないアプリケーションを削除する b) システム機能及びアプリケーションに最小権限の原則を適用する c) ファイルとデータに最小権限の原則を適用する d) ユーザアカウントは CKMS のエンティティに限定する。不要なアカウントは無効化または削除する。また、sudo による管理者権限を持つアカウントを限定し、それらのアカウントで実行可能なコマンドを制限する f) 十分なエントロピーを確保できるように、パスワードの長さや複雑さ、及び鍵に関わる規則を設け、デフォルトのパスワード及び鍵を置き換える g) CKMS の運用に不要なネットワークサービスを無効化または削除する h) CKMS の運用に不要な他の処理を無効化または削除する i) CA サーバにおいて USB メモリなどのリムーバブルメディアの無効化または自動実行機能を無効化する j) 不要なネットワークポートを無効化する k) SELinux、AppArmor などのオプションのセキュリティ機能を有効化する l) SSH の設定強化、ルートログインの無効化、システムのアップデートなど、その他のセキュリティ設定オプションを有効化する
F.07	当該 CKMS の CA サーバのブート時にはセキュアブート処理を実施する。ROM 内ブートローダから BIOS、OS、CA アプリケーションの起動において実行コードのインテグリティチェックを行う。

② デバイスに対するセキュリティの要求事項を決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.08	FR8.6	CKMS 設計は、それぞれの CKMS デバイスに必要なセキュリティコントロールを明記しなければならない。	8.2.2 節
F.09	FR8.7	CKMS 設計は、堅牢化の基となるデバイス／CKMS のセキュリティ設定要求事項及びガイドラインを明記しなければならない。	8.2.2 節

解説・考慮点

CKMS を構成する各々のデバイスに対して、認可されない使用から自らを保護するように設計されているか、外部から適用される保護が必要である。
CKMS の設計にあたって、項目 F.08 及び F.09 は、CKMS デバイス等に対するセキュリティの要求事項を明確化することを求めたものである。SP 800-130、8.2.2 節にセキュリティ機能の参考例が掲載されている。

CKMS デバイスにはそれをコントロールするホスト OS と独立したセキュリティコントロールを備えるものがある。本節はそのようなデバイスにおけるセキュリティコントロールの内容やデバイスの堅牢化に関わる機能を定めることを求めている。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.08	当該 CKMS を構成するデバイスのセキュリティコントロールには HSM で実施されるものがある。HSM 上の OS において HSM 内の処理に関わるユーザ認証と権限管理が実施される。また、HSM におけるイベントログ情報が取得される。
F.09	上記 F.08 の HSM における堅牢化に関わるセキュリティ設定については HSM の設定マニュアルに記載されている。

③ マルウェア感染防止に対する要求事項を決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.10	FR8.8	CKMS 設計は、CKMS デバイスに対する以下のマルウェア防御能力を明記しなければならない： a) ウイルス対策ソフトウェア。アンチウイルススキャン、ソフトウェア更新、及びウイルスシグネチャデータベース更新を開始する時間周期及びイベントの指定を含む。 b) スパイウェア対策ソフトウェア。アンチスパイウェアスキャン、ソフトウェア更新、及びウイルスシグネチャ更新を開始する時間周期及びイベントの指定を含む。 c) ルートキット検出及び防御ソフトウェア。ルートキット検出、ソフトウェア更新、及びシグネチャ更新を開始する時間周期及びイベントの指定を含む。	8.2.3 節
F.11	FR8.9	CKMS 設計は、OS 及び CKMS アプリケーションソフトウェアに対する以下のソフトウェア完全性チェックの情報を明記しなければならない： a) ソフトウェア完全性がインストール時に検証される場合、検証がどのように実行されるかを記載する b) ソフトウェア完全性が定期的に検証される場合、検証が実行される頻度を記載する	8.2.3 節

解説・考慮点

データやファイル等をネットワーク（特に、保護されていないネットワーク）等を通して受信する CKMS デバイスは、受信した情報のマルウェア感染防止のための対策をすべきである。CKMS の設計にあたって、項目 F.10 及び F.11 は、CKMS デバイス等へのマルウェア感染防止に対する要求事項を明確化することを求めたものである。

上記のように、CKMS コンピュータシステムにおけるマルウェア感染の防御機能を定めることを求めている。ネットワークやリムーバブルメディアからマルウェアが持ち込まれる可能性があり、マルウェア（ウイルス、スパイウェア、ルートキット検出など）の検知ツールを利用するなどの緩和策がある。また、OS やアプリケーションソフトのインテグリティチェックもそれらのコードへのマルウェア感染の検出に有効である。

意図した相手と意図した通信しか行わず、通信内容も暗号学的に保護されている場合には外部からネットワーク経由でマルウェアが侵入する可能性は低減できるが、マルウェアの侵入経路は多様であることに注意すべきである。例えば、外部から持ち込まれたリムーバブルメディアや PC 端末が侵入口となり得ること、CKMS に関わるエンティティが悪意を持って感染させることなどもあり得る。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.10	当該 CKMS の CA サーバが定常的に通信を行うのは外部の IoT 向け証明書管理端末のみであるが、多層防御の一つとしてマルウェア検出ツールを CA サーバで動作させる。a)ウイルス、b)スパイウェア、c)ルートキットのいずれに対しても検出力を備えたツールである。シグネチャの更新はツールベンダの更新サイクルに依存する。
F.11	当該 CKMS の CA サーバのセキュアブート処理において、起動時に OS と CA アプリケーションはインテグリティチェックが実施される。また、OS と CA アプリケーションに対するソフトウェアパッチが配信され、コードにパッチを適用する際にはソフトウェアパッチのインテグリティチェックが実施される。

④ 監査機能に対する要求事項を決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.12	FR8.10	CKMS 設計は、サポートされている監査可能イベントを明記し、それぞれのイベントは固定されているか選択可能であるかを示さなければならない。	8.2.4 節

F.13	FR8.11	それぞれの選択可能な監査可能イベントに対し、CKMS 設計は、イベントを選択する能力を持つ役割を明記しなければならない。	8.2.4 節
F.14	FR8.12	それぞれの監査可能イベントに対し、CKMS 設計は、記録されるデータを明記しなければならない。	8.2.4 節
F.15	FR8.14	CKMS 設計は、システムファイルの改変又はアクセスコントロールリストのようなセキュリティ属性のあらゆる改変について検知や防止をするため､危殆化を受けやすいシステムファイルに対するシステム監視要求事項を明記しなければならない。	8.2.4 節
F.16	FR8.13	CKMS 設計は、CKMS の正しい運用及びセキュリティを評価するために､どの自動化ツールが提供されているかを明記しなければならない。	8.2.4 節

解説・考慮点

CKMS では、イベント、イベントの発生日時、及びイベントを発生させたエンティティの識別子（ID）又は役割を検知及び記録することによって、セキュリティ関連イベントを監査すべきである。そのためには、監査管理者に対して可能な限り速やかに調査すべきあらゆる異常なイベントを検知し報告するとともに、監査の完全性が保証できるように監査ログの改ざんから保護されることが必要である。
また、セキュリティ設定共通化手順（Security Content Automation Protocol；SCAP）に規定されているような自動評価ツールは、現在のステータス及びコンピュータシステムの完全性の評価に有効な手段であり、システムファイル又はそれらのアクセスコントロール属性の改変、データファイルの完全性及び機密性の侵害等を検知し、警告及び監査イベントを発する監視ツールとしても利用できる。

CKMS の設計にあたって、項目 F.12～F.15 は、監査機能に対する要求事項を明確化することを求めたものである。F.16 は SCAP を利用する場合に SCAP に対する事項を明確化することを要求したものである。SCAP を利用しない場合には、F.16 は検討対象外である。

異常な操作や処理の検出や解析にイベントログが利用される。イベントログを利用した監査機能について明確にすることを求めている。汎用 OS には一般にイベントログとして取得する対象のイベントや監視報告に関わるコマンドやツールが提供されている。アプリケーションプログラムにもアプリケーションに関わるイベントのログ機能を備えるものがある。

セキュリティ設定共通化手順（Security Content Automation Protocol；SCAP）は米国 NIST が策定した情報セキュリティ対策の自動化と標準化を実現する技術仕様群である。脆弱性対応で利用される CVE（Common Vulnerabilities and Exposures：共通脆弱性識別子)、CVSS（Common Vulnerability Scoring System：共通脆弱性評価システム)、CPE（Common Platform Enumeration：共通プラットフォーム一覧）に加えて、CCE（Common Configuration Enumeration：共通セキュリティ設定一覧）や OVAL（Open Vulnerability and

Assessment Language：セキュリティ検査言語）等も標準仕様として含まれる。SCAP については IPA のサイトに概説がある[11]。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.12	当該 CKMS では、CA サーバの Linux OS においてユーザ管理、アプリケーション管理、堅牢化に関わる設定管理(F.06 に記載)などのイベントログを監査対象とする。また、CA ソフトウェアにおいて証明書の発行や失効処理に関わるイベントログが監査対象として利用できる。さらに、HSM でも操作ログや実行処理のログが取得され、監査対象となる。これらの監査対象のログは選択可能である。
F.13	上記 F.12 に記載したイベントログの選択は、CA サーバについては CKMS 管理者、HSM については HSM 管理者が実施できる。HSM 管理者は CKMS 管理者のうち HSM 管理者としてアサインされた担当者であるが、マルチパーティコントロールがされており、1 名では権限を取得できない。
F.14	上記 F.12 に記載したイベントログとして記録されるデータには、実行者、時刻、処理対象及び処理内容が含まれる。具体的なデータ形式は管理マニュアルを参照。
F.15	上記 F.12 に記載したイベントログのうち、ユーザ管理、特にアクセス権限管理に関わるイベントはリアルタイムでの監視対象とし、イベント発生時に CKMS 管理者及び CKMS 責任者に通知されるように設定する。
F.16	当該 CKMS では脆弱性情報に関わる CVSS や CVE を参照するが、自動化ツールは利用しない。本項目は対象外である。

4.1.3 ネットワークセキュリティコントロール

① セキュリティ境界をコントロールするためのネットワークセキュリティコントロールデバイスに対する要求事項を決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.17	FR8.15	CKMS 設計は、CKMS によって採用される境界保護メカニズムを明記しなければならない。	8.3 節
F.18	FR8.16	CKMS 設計は、以下を明記しなければならない： a) 使用されるファイアウォールのタイプとファイアウォールを介して許可されるプロトコル。それぞれのプロトコルタイプの発信元（source）と宛先（destination）を含む	8.3 節

[11] セキュリティ設定共通化手順 SCAP 概説、https://www.ipa.go.jp/security/vuln/scap/scap.html

		b) 使用される侵入検知・防止システムのタイプ。ログ及びセキュリティ侵害対応の機能を含む	
F.19	FR8.17	CKMS 設計は、CKMS デバイスをサービス拒否（DoS）攻撃から保護するために使用される方法を明記しなければならない。	8.3 節
F.20	FR8.18	CKMS 設計は、使用されるそれぞれの方法がどのようにサービス拒否攻撃から保護するかを明記しなければならない。	8.3 節

解説・考慮点

ネットワーク化された CKMS デバイスへの外部からの攻撃を防護するためには､それら CKMS デバイスをセキュリティ境界内部に配置するとともに、ファイアウォール及び侵入検知・防御システム等のネットワークセキュリティコントロールデバイスをいくつか組み合わせてセキュリティ境界内部を保護する必要がある。そのため、ネットワークセキュリティコントロールデバイスは物理的にセキュアな場所に配置され、セキュアな操作に必要なユーザアカウント及びネットワークサービスのみを提供すべきである。
また、CKMS デバイスへの DoS/DDoS 攻撃は CKMS のサービス提供が停止することにつながる可能性があるので、DoS/DDoS 攻撃を防止することも必要である。

CKMS の設計にあたって、項目 F.17 及び F.18 は、セキュリティ境界をコントロールするためのネットワークセキュリティコントロールデバイスに対する要求事項を明確化することを求めたものである。F.19 及び F.20 は DoS/DDoS 攻撃への対策のための要求事項を明確化することを求めたものである。

上記のように、CKMS へのネットワーク経由の侵入や攻撃を防御するために利用するネットワーセキュリティコントロールのメカニズムを明確にすることを求めている。具体的なメカニズムには SP 800-130 に例示されているように、ファイアウォール、フィルタリングルータ、仮想プライベートネットワーク（VPN)、侵入検知システム（IDS)、侵入防止システム（IPS）などがある。これらの機能に加えてディープ・パケット・インスペクションによるアプリケーションレベルでのパケットの検査や外部からの脅威インテリジェンスの活用などの機能を加えたネクスト・ジェネレーション・ファイアウォールと呼ばれる製品もある。

境界コントロール型の防御は、内部ネットワークは安全な領域として外部ネットワークとの接続点での防御に注力するものであるが、内部ネットワークに持ち込まれるデバイスに様々なものがあるなど侵入経路が多様化しており、クラウドサービスの普及などにより物理的なネットワーク境界が明確でなくなっている場合がある。このような状況で、従来のシグネチャベースやフィルタリングルールでは検知できない脅威も存在する。マルウェアに感染し外部からコントロールされている内部ネットワークの端末や、内部犯によるデータ窃取がその一例である。そのような不正行為を試みるトラヒックの振る舞いを定常時・非定常時の差分などから検知して対処する Network Detection and Response（NDR）というカテゴリの製品も登場している。NDR では人工知能や機械学習を用いて異常なふるまいを検知しており、従来の攻撃方法を分析してシグネチャをアップデートする手法の欠点であったゼロデイ攻撃に対するアプローチにもなる。

関連した動向として、従来の内部ネットワークは安全という考え方に基づかないセキュリティアーキテクチャとして Zero Trust Architecture（ZTA）が提唱されている。SP 800-207 に基本的な概念が整理されており、ZTA では必要最小限のアクセス権のみを付与することでリソースを制限し、暗黙的に信頼が付与される状況を無くすことでリソースが保護され、さらに継続的な状態評価を実施することを目標としている。

実際のネットワーク構成やセキュリティモデルを踏まえて、それに適したネットワークコントロールを実現するように留意されたい。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.17	当該 CKMS では、ネットワークセキュリティコントロールデバイスとして、フィルタリング機能を搭載したルータを利用する。さらに、侵入検知用に IDS を利用する。また、緊急時に外部からシステム管理を行えるように VPN を設置する。
F.18	当該 CKMS で利用するファイアウォールと侵入検知システムは以下のように設定する。 a) ファイアウォールはルータのパケットフィルタリング機能で実現する。通信パケットの発信元と宛先は CA サーバと IoT 製品向け証明書管理端末、及びシステム管理用に予め登録した PC 端末に限定する。 b) 侵入検知システム（IDS）は、CA サーバ上で稼働させるホスト型を利用する。
F.19	当該 CKMS において、DoS/DDoS 攻撃対策に関わるメカニズムは F.18 に記載のフィルタリング機能を搭載したルータ及び IDS である。
F.20	当該 CKMS において、DoS/DDoS 攻撃対策は、ルータにおいて予め設定したアドレス以外から送受信したパケットを遮断すること、CA サーバ上の IDS で予め設定した正常なアクセスパターン以外の通信を検知すること、の 2 つのメカニズムによる。

4.2 システム保証

解説・考慮点

本節は、SP 800-130 の 9.8 節に記載されている事項について解説したものである。
本節で取り扱うシステム保証とは、CKMS で利用するコンポーネント及びデバイスがそもそもセキュアなものであり、不正な組み込みがされていないことを保証するためのプロセスである。

本節で検討される項目は、CKMS 全体やその構成要素であるデバイスやコンポーネントの開発環境やメンテナンスに関わるセキュリティを保証するために検討すべきものである。特に CKMS の開発工程において考慮すべき項目は「製品セキュリティ」と呼ばれる活動と共通するものがある。例えば、「脆弱性対処に向けた製品開発者向けガイド（IPA）」に開発工程における脆弱性の混

入を抑えるための施策が書かれている。また、FIPS 140-2 には暗号モジュールに対するセキュリティ要件として、設計保証（Design Assurance）の項目があり、その中に構成管理、配送、開発の小項目がある。これらの要件が本節に関わるものと考えられる。

CKMS の構築において、システム開発を委託した SI 業者、及びデバイスやコンポーネントの調達先であるベンダに対して適切な保守契約を締結して、運用後のメンテナンスにおけるセキュリティ維持のサポート手段を確保することが望ましい。

① 構成管理に関する要求事項を決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.21	FR9.10	CKMS 設計は、以下を明記しなければならない： a) 構成制御の下に置かれているデバイス（ソースコード、スクリプト実装、実行コード、ファームウェア、ハードウェア、文書、及びテストコードを含む） b) 構成制御の下でコンポーネント及びデバイスへの認可された変更だけが行われたことを保証するための保護要求事項（例えば、形式的認可及び適切な記録保持）	9.8.1 節

解説・考慮点

構成管理は、製品への認可されていない又は意図しない変更によってセキュリティが低下せず、かつ機能的欠陥が取り込まれることがないことを保証するための手法である。
項目 F.21 は、CKMS の設計にあたって、管理対象や構成変更方法等、構成管理に関する要求事項を明確化することを求めたものである。

上記のように、CKMS の要素となるデバイスやコンポーネントに対して、構成管理の対象とするものを定めることを要求している。構成管理を適切に実施して製品を開発したり、保守を行ったりするのはベンダ側の対応事項であるが、利用者側でも利用するデバイスやコンポーネントの型番やファームウェアバージョンを管理することは重要である。これらの情報は、CKMS の運用中に発見された脆弱性情報や欠陥などが対象のデバイスやコンポーネントに該当するものかどうか、該当する場合にファームウェア更新などによる機能更新を実施すべきかどうかを迅速に判断して対処することに利用される。

また、自社開発のソフトウェアに対しては社内で構成管理を行うことが必要となる。なお、暗号モジュールに関する構成管理について、FIPS 140-2 では小節を設けて簡単に要件が記載されている。

構成管理に関連して SBOM（Software Bill of Materials：ソフトウェア部品表）の利活用が注目されている。OSS（Open Source Software）の利用が拡大するなどソフトウェアのサプライチェーンが複雑化している中で、SBOM の活用によってソフトウェアの脆弱性管理を効率化することが期待されている。SBOM については経済産業省が手引書を公開している。

- 「ソフトウェア管理に向けた SBOM の導入に関する手引」、経済産業省

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。このトイモデルでは、CA システム自体は社内でシステム構築を行うが、サーバ、HSM、ルータなどのデバイス及び CA ソフトやサーバ OS などのソフトウェアコンポーネントは外部から調達した製品を利用することを想定している。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.21	当該 CKMS における構成管理の対象を以下のように定める。 a) 構成管理の対象は、サーバ、HSM、ルータ、CA ソフトウェア、サーバ OS である。特に、ソフトウェアコンポーネントである CA ソフトウェアとサーバ OS は脆弱性が発見される可能性が比較的高く、バージョン情報を元に脆弱性情報の監視を行う。 b) 上記のデバイスやコンポーネントに対してファームウェア更新などによってバージョンが変更された場合は、システムインベントリの管理情報を適切に更新する。

② セキュアな配送に関する要求事項を決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.22	FR9.11	CKMS 設計は、以下を含む、CKMS で使用される製品のセキュアな配送[12]の要求事項を明記しなければならない： a) 配送プロセス中に製品がタンパー（tamper）されていない、又はタンパーされたことが検知されることを保証するための保護要求事項 b) 配送プロセス中に製品が交換されていない、又は交換されたことが検知されることを保証するための保護要求事項 c) 要求されていない配送が検知されることを保証するための保護要求事項 d) 製品の配送が差し止め又は遅延していない、及び差し止め又は遅延が検知されることを保証するための保護要求事項	9.8.2 節

解説・考慮点

CKMS で使用される製品には、セキュアな配送の保証（受領した製品が間違いなく注文した製品であり、改ざんされていないこと）が必要である。

[12] 「暗号鍵管理システム設計指針（基本編）」では「セキュアな配付」と表記されている。SP 800-130 では secure delivery となっており、CKMS で利用するデバイスやコンポーネントなどの製品が対象とすると「セキュアな配送」と表記するのが適当と考え、本書ではそのように表記した。

項目 F.22 は、CKMS の設計にあたって、セキュアな配送を保証・確認するための要求事項を明確化することを求めたものである。

上記のように、CKMS の要素であるデバイスやコンポーネントの配送においても製品のすり替えや改ざんがされていないことを確認できることが望ましい。本節の対象となるのはハードウェア製品やメディアに記録したソフトウェア製品である。物理的な製品梱包における開封検知の仕組みや初期起動に必要な鍵情報を別送するなどの手段をベンダ側で実施していることがある。また、製品の配送状況のトラッキングを可能とするサービスなども関連する。CKMS 設計側ではベンダに実施可能な手段を確認するのが基本的な対応となる。

なお、暗号モジュールに関するセキュアな配送について、FIPS 140-2 では小節を設けて配送とインストール、初期化について簡単に要件が記載されている。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.22	a) 当該 CKMS で調達する HSM、サーバ、ルータについて配送上のセキュリティ対策をベンダ側で用意しているかを確認する。例えば、製品梱包におけるタンパーシールや初期起動に必要な鍵情報の配送方法など。 b) 上記と同様。 c) 上記と同様。 d) 製品配送の差し止めや遅延の確認は購買管理システムによって行う。

③ 開発環境及びメンテナンス環境におけるセキュリティに関する要求事項を決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.23	FR9.12	CKMS 設計は、以下を含む、CKMS の開発環境及びメンテナンス環境におけるセキュリティ要求事項を明記しなければならない： a) 物理セキュリティ要求事項 b) 開発者、試験者、及び保守員に対する身分照会及びバックグラウンドチェックのような人的セキュリティ要求事項 c) 複数人員（multi-person）による制御、及び職掌分散（separation of duties）のような手続き的セキュリティ d) 開発環境及びメンテナンス環境の保護、及び認可されたユーザにアクセスを許可するアクセスコントロールの提供のためのコンピュータセキュリティコントロール	9.8.3 節

		e) ハッキングの試みから開発環境及びメンテナンス環境を保護するためのネットワークセキュリティコントロール f) 開発下のソフトウェア及びその制御データの完全性を保護するための暗号学的セキュリティコントロール g) ツール（例えば、エディタ、コンパイラ、ソフトウェアリンカ、ローダ等）が信頼でき、マルウェアのソースでないことを保証するために利用する手段	

解説・考慮点

CKMS 開発環境及びメンテナンス環境は、物理的、人的、及びハッキングの脅威から適切に保護されなければならない。また、コンパイラ、ソフトウェアリンカ、テキストエディタといった開発ツールを自動的に信頼すべきではない。
項目 F.23 は、CKMS の設計にあたって、セキュアな開発環境及びメンテナンス環境を実現するための要求事項を明確化することを求めたものである。これには、物理的セキュリティ、人的セキュリティ、及びシステムセキュリティの全てを含む。

CKMS の開発や構築の過程、あるいはメンテナンスの過程でマルウェアを混入させてしまったり、バックドアが作り込まれてしまったりすることを防止するための要求項目である。開発やテスト、メンテナンスなどの人員が悪意を持って不正行為を行う可能性もあれば、意図せずにマルウェアが混入する可能性もある。開発を実施するエリアを外部アクセスから厳格に管理する、外部とのネットワーク接続を遮断するなどの物理的対策、悪意を持った人員による不正操作を抑止する相互監視などの人的対策、開発に利用するコンパイラなどの開発ツールを経由したマルウェア感染防止に関わる対策など様々な緩和策が考えられる。

なお、調達したデバイスやコンポーネントにマルウェアが感染している可能性もある。これはサプライチェーンセキュリティと呼ばれる領域に関わる事項であるが、責任はベンダ側が負うものであり、利用側での緩和策は信頼できるベンダの製品を採用すること等に限定される。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.23	当該 CKMS の開発に当って、開発環境のセキュリティとして以下の内容を実施する。 a) CKMS の開発に利用するエリアは、CKMS 運用時と同じエリアを利用し、入退室管理を施している。 d) CKMS の開発を担当する人員は、CKMS の管理者ロールを有する人員の一部であり、開発環境やツールへのコンピュータアクセスコントロールを施している。 e) 開発環境は外部アクセスからネットワークセキュリティコントロールを施している。

	g) 開発ツールからのマルウェア混入のリスクを低減させるため、開発ツールのうち、コンパイラ、リンカなどの実行コードを生成するツール、及びインストーラは有償版（サポート契約付き）を利用する。また、自社開発のツールもセキュアコーディングや脆弱性検査などを実施して開発されたツールであることを確認する。

④ 欠陥修正能力に関する要求事項を決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.24	FR9.13	CKMS 設計は、以下を含む、システムの欠陥を検知する CKMS の能力を明記しなければならない： a) 既知解テスト b) エラー訂正コード c) 異常故障診断技術 d) 機能テスト	9.8.4 節
F.25	FR9.14	CKMS 設計は、以下を含む、欠陥を報告する CKMS の能力を明記しなければならない：ステータスレポートメッセージを機密性、完全性、及びソース認証保護付きで作成する能力、及び認可されない遅延を検知する能力	9.8.4 節
F.26	FR9.15	CKMS 設計は、欠陥を分析し、かつ起こりやすい又はよく知られている欠陥に対する修正を作成／取得する CKMS の能力を明記しなければならない。	9.8.4 節
F.27	FR9.16	CKMS 設計は、機密性、完全性、及びソース認証保護付きで修正を送信し、かつ認可されない遅延を検知する CKMS の能力を明記しなければならない。	9.8.4 節
F.28	FR9.17	CKMS 設計は、時宜を得て修正を実装する CKMS の能力を明記しなければならない。	9.8.4 節

解説・考慮点

CKMS は、迅速かつセキュアな方法でシステムの欠陥を検知、報告及び修正する能力を持つべきである。特に、自動化された技術であることが望ましい。
CKMS の設計にあたって、項目 F.24～F.28 は、欠陥修正能力に関する要求事項を明確化することを求めたものである。F.24 は検知、F.25 は報告[13]、F.26～F.28 は修正・対処に相当する。

上記のように欠陥の検知、報告、修正に関わる対応を明確にすることを要求している。

[13] 「暗号鍵管理システム設計指針（基本編）」では F.25 に対して「通知」と「報告」の表記が混在しているが、SP 800-130 では report となっており、本書では「報告」で統一した。

FIPS 140-2 には、暗号モジュールのセキュリティ要件として、自己テストに関わる要件がまとめられている。暗号アルゴリズムの実装に関わる既知解テストやソフトウェアのインテグリティテストがまとめられており、インテグリティテストではエラー訂正コードに基づく方法と、MAC やデジタル署名などの認証データに基づく方法が書かれている。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.24	当該 CKMS で利用する HSM は FIPS 140-2/-3 レベル 3 の認証取得を要件としている。その要件として、HSM 内に実装されている ECDSA 署名アルゴリズム及びその内部で用いるハッシュ関数 SHA-256 と SHA-384 では既知解テストを実施している。また、ECDSA の鍵生成や署名生成時のナンス生成に利用する乱数生成器においてエントロピー試験やポスト処理部の既知解テストを実施している。また、HSM 起動時にファームウェアの完全性テストを実施している。 CA サーバで動作するサーバ OS 及び CA ソフトウェアも起動時にセキュアブートを実施しており、ブート時に起動するコードに付与されたデジタル署名の検証を実施する。また、CA サーバを継続的に動作させる場合、サーバ監視プログラムを動作させ、状態監視及び異常検知を継続的に実施する。可能であれば、サーバ OS 及び CA ソフトウェアに関する定期的なテストを実施する。
F.25	当該 CKMS で利用する HSM において、自己テストでエラーを検出した場合の状況を表す診断コードなどのステータスレポートは、完全性保護や内容の秘匿などを実施した上でベンダに送付される。
F.26	当該 CKMS では、HSM 及び CA ソフトウェア、サーバ OS はそれぞれのベンダと保守契約を締結する。これらのデバイス及びソフトウェアコンポーネントにおける欠陥の分析、修正コードの作成やデバイス交換などの修正対応はベンダ側の体制に委ねる。
F.27	当該 CKMS では、HSM のファームウェア更新において、更新ファームウェアイメージの完全性と作成元の認証を行えるよう、セキュアなアップデート機能のサポートを要求する。 CA サーバのサーバ OS 及び CA ソフトウェアに対する修正パッチの配布においても同様の機能がサポートされる。
F.28	当該 CKMS では、F.26 に記載のように、ベンダと有償のサポート契約を締結する。サポート契約において、欠陥や脆弱性の対応条項があることを確認する。欠陥の検知時にはタイムリーに修正対応を実施できるようベンダと調整する。

4.3　セキュリティアセスメント

解説・考慮点

本節は、SP 800-130 の 11 章に記載されている事項について解説したものである。
CKMS のセキュリティを維持するため、CKMS のセキュリティライフタイムを通して様々なタイミングでいくつかのセキュリティアセスメントが実施される。また、必要に応じて、メンテナンスも実施しなければならない。本節では、セキュリティアセスメント及びメンテナンスについて取り扱う。

CKMS はシステムの初期立ち上げ時だけではなく、定期的または必要に応じてセキュリティアセスメントを実施するべきである。例えば、CKMS の構成要素であるデバイスやコンポーネントに対する新たな脆弱性の発見や、新たな攻撃手法の考案などにより、設計当初と比較してセキュリティが低下する恐れがある。また、運用の過程で、担当者の退職や異動による変更がシステムのアクセス権や通知先などに速やかに反映されていないことなどを起点に、不正操作やセキュリティインシデントのリスクが発生する可能性も生じる。これらのリスクを特定するためには、システム構成や運用状況の変化を監視し、必要に応じてセキュリティアセスメントを実施することが重要である。

本節では、セキュリティアセスメントを実施する状況とアセスメントにおけるスコープを整理することを求めている。また、各種のセキュリティコントロールによる堅牢化を維持するためのメンテナンス作業も定めることを求めている。

① 完全セキュリティアセスメントで実行される要求事項を決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.29	FR11.1	CKMS 設計は、完全な CKMS セキュリティアセスメントの前又は同時に行われる、必要な保証実行策を明記しなければならない。	11.1 節
F.30	FR11.2	CKMS 設計は、完全なセキュリティアセスメントが繰り返される状況を明記しなければならない。	11.1 節
F.31	FR11.3	CKMS 設計は、あらゆる CKMS デバイスについて、認証を受けた全ての認証プログラムを明記しなければならない。	11.1.1 節
F.32	FR11.4	CKMS 設計は、認証済みデバイスに対する全ての認証番号を明記しなければならない。	11.1.1 節
F.33	FR11.5	CKMS 設計は、完全なセキュリティアセスメントの一部として、アーキテクチャレビューを必要とするかどうかを明記しなければならない。	11.1.2 節
F.34	FR11.6	アーキテクチャレビューが必要である場合、CKMS 設計は、アーキテクチャレビューチームに必要なスキルセットを明記しなけれ	11.1.2 節

		ばならない。	
F.35	FR11.7	CKMS 設計は、必要な全ての CKMS の機能テスト及びセキュリティテストを明記しなければならない。	11.1.3 節
F.36	FR11.8	CKMS 設計は、今までに実行された全ての機能テスト及びセキュリティテストの結果を報告しなければならない。	11.1.3 節
F.37	FR11.9	CKMS 設計は、今までに実行されたあらゆる完了したペネトレーションテストの結果を明記しなければならない。	11.1.4 節

解説・考慮点

配備前又は配備時に実施すべきセキュリティアセスメントであり、セキュリティアセスメントに課すことができる実行策には以下のものが含まれる。

- 第三者検証のレビュー（CAVP、JCMVP/CMVP、CC などの検証プログラム、等）
- システム設計のアーキテクチャレビュー
- 機能テスト及びセキュリティテスト
- ペネトレーションテスト

CKMS の設計にあたって、項目 F.29～F.37 は、完全セキュリティアセスメントで実行される要求事項を明確化することを求めたものである。F.29 はアセスメントの内容、F.30 はアセスメントの実施条件、F.31 及び F.32 は検証プログラム、F.33 及び F.34 はアーキテクチャレビュー、F.35 及び F.36 は機能テスト及びセキュリティテスト、F.37 はペネトレーションテストに関する要求事項がそれぞれ対象である。なお、F.31～F.37 で該当しない項目は検討対象外である。

上記のように、SP 800-130 ではセキュリティアセスメントとして、第三者検証のレビュー、システム設計のアーキテクチャレビュー、機能テスト及びセキュリティテスト、ペネトレーションテストの 4 つを具体的な実行策として記載している。このうち、第三者検証のレビュー、機能テスト及びセキュリティテストは、本ガイダンスの「3.2 セキュリティ評価・試験」でも検討項目としている。これらのテストについて、評価の対象やスコープが同一ならば既に実施した試験結果や検証資料を確認するだけでよい。

本節では、完全なセキュリティアセスメントとして実施する実行策を定めることと、どのような場面で完全なアセスメントを実施するか（再度実施するか）を定めることを求めている。実行策は上記の 4 つ以外を実施してもよいが、上記 4 つの実行策のそれぞれについては実施するかどうか、実施する場合には実施内容を定めること、これまでの実施結果を確認することを求めている。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.29	当該 CKMS において、完全セキュリティアセスメントでは次の 4 つを実施する。利用する HSM に関わる第三者認証のレビュー、CKMS 全体のアーキテクチャレビュー、CKMS 提供機能に関わる機能テスト及びセキュリティテスト、CKMS を模擬した環境に対するペネトレーションテストである。
F.30	当該 CKMS において、完全セキュリティアセスメントはシステム構築完了後、運用開始前に実施する。十分な結果でなかったテストは合格するまで再度実施する。運用開始以降は、原則として完全セキュリティアセスメントは実施しない。
F.31	完全セキュリティアセスメントの一項目である第三者検証のレビューとして、利用する HSM が FIPS 140-2/-3 レベル 3 認証を取得済であり、現在も有効であることを確認する。
F.32	F.31 において、HSM ベンダから認証情報の提供を受け、CMVP の認証番号を確認する。
F.33	当該 CKMS において、完全セキュリティアセスメントの一項目であるアーキテクチャレビューは、プライベート CA システム全体を対象として実施する。社内でセキュリティシステムの構築経験を持つ専門家によるレビューを実施する。適当な専門家がアサインできない場合は外部のセキュリティコンサルタントにレビューを委託する。
F.34	F.33 のアーキテクチャレビューにおいて、レビューアーは以下の技術に関する十分な実務経験を持つことを条件とする：コンピュータセキュリティ、ネットワークセキュリティ、暗号と情報セキュリティ、コンピュータシステム構築、セキュリティアーキテクチャ設計、リスク管理、セキュリティテスト。 また、公的な資格として、CISSP (Certified Information Systems Security Professional)、情報処理安全確保支援士（Registered Information Security Specialist, RISS）、CISM (Certified Information Security Manager)、ISO/IEC 27001 Lead Auditor などアーキテクチャレビューに必要な知識を有していることが望ましい。
F.35	当該 CKMS において、完全セキュリティアセスメントの一項目である機能テスト及びセキュリティテストは、プライベート CA の機能である、IoT 製品向け証明書の発行、同証明書に関わる失効リスト（CRL）の発行の 2 つに対して実施する。具体的には、本ガイダンス 3.2 節の③機能テスト及びセキュリティテストと同一であり、E.29 に記載している。
F.36	F.35 の機能テスト及びセキュリティテストは、本ガイダンス 3.2 節の E.29 として先に実施済であれば、完全セキュリティアセスメント時にはテスト結果を確認し、それが現在の設計及び運用環境において有効であることを評価する。

F.37	当該 CKMS において、ペネトレーションテストはセキュリティアセスメントの一環として実施を検討する場合がある。これまでに実施した結果はないが、セキュリティアセスメントにおける他のテスト結果や運用状況を踏まえて、必要に応じて実施する。 なお、運用前または運用中のアセスメントにおいて、セキュリティコントロールに重大な脆弱性が見つかった場合には、ペネトレーションテストを実施することで、脆弱性の悪用が可能かどうかを評価する。この場合、検証用のテスト環境を構築して以下のゴールを設定したテストを実施する。 ● 脆弱性がセキュリティコントロールに与える影響の確認 ● セキュリティコントロール機能により、システム障害や脅威が発生した場合でも、設計されたセキュリティ要件を満たす状態に回復するかの確認 また、ペネトレーションテストの結果は文書化し、セキュリティアセスメントの一部として関係者に報告する。

② 定期的なセキュリティレビューで実行される要求事項を決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.38	FR11.10	CKMS 設計は、セキュリティレビューの周期を明記しなければならない。	11.2 節
F.39	FR11.11	CKMS 設計は、CKMS デバイスの観点から、セキュリティレビューのスコープを明記しなければならない。	11.2 節
F.40	FR11.12	CKMS 設計は、レビュー対象のそれぞれの CKMS デバイスに対して行われる実行策の観点で、定期的なセキュリティレビューのスコープを明記しなければならない。	11.2 節
F.41	FR11.13	CKMS 設計は、定期的なセキュリティレビューの一部として実行される機能テスト及びセキュリティテストを明記しなければならない。	11.2 節

解説・考慮点

システムコントロール、物理コントロール、手続き的コントロール及び人間によるコントロールが規定等に整備され、その通りに運用していることを保証するために、定期的にレビュー[14]を実施すべきである。このレビューでは、少なくとも、前回のセキュリティレビューからのシステム変更箇所の検査、及び定期的な機能テスト及びセキュリティテストの実行が行われる。CKMS の設計にあたって、項目 F.38～F.41 は、定期的なセキュリティレビューで実行される要求事項を明確化することを求めたものである。F.38 はレビューの実施条件、F.39 及び F.40

[14] 「暗号鍵管理システム設計指針（基本編）」では「定期的なセキュリティアセスメント」と表記されている。SP 800-130 では periodic security review となっており、「定期的なセキュリティレビュー」と表記するのが適当と考え、本書では節のタイトルを含め、そのような表記で統一した。

はレビューの範囲及び内容、F.41 は機能テスト及びセキュリティテストに関する要求事項がそれぞれ対象である。

上記のように、定期的なセキュリティレビューとして実施する内容と頻度（実施時期）を定めることを要求している。定期的なセキュリティレビューは完全なセキュリティアセスメントを補完するものであり、CKMS の設計時に定めたセキュリティ要件が運用中に適切に維持されているかを確認するものである。例えば、デバイスに最新のアップデートを適用した結果、提供されていた機能やメカニズムの一部に仕様変更があり、対応が必要であったり、それによって CMVP 等の第三者セキュリティ認証が失効したりする可能性がある。前回レビュー時点からの変更箇所の検査や、機能テスト及びセキュリティテストの実施によって、そのようなリスクを早期に検出できる。

なお、定期的レビューに関わる CKMS 運用中の活動として以下が挙げられる。

a) CKMS 内のデバイスやコンポーネント向けにベンダから提供されたアップデートパッチを適用すべきかどうかを検証環境で確認・検討し、必要なパッチを本番環境に適用する活動
b) CKMS 内で取得した実行要求や操作のログを分析して、不正操作や異常な要求がないかを確認する活動
c) CKMS エンティティとして権限を有する担当者の変更管理を行い、不要な権限を削除し、新しい担当者への適切な権限を付与する活動

これらの活動は、日常的に実施されるセキュリティメンテナンスとして位置づけられる。定期的なセキュリティレビューの一項目として、これらのメンテナンスが適切に実施されていることを確認し、必要に応じて改善提案を行う。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.38	当該 CKMS の管理担当は、定期的なセキュリティレビューとして以下の内容を実施する。 ● セキュリティパッチの適用状況のチェック HSM、CA ソフトウェア、及び CA サーバの OS のそれぞれに対してセキュリティパッチが適用されているか確認する ● 操作ログのレビュー CA サーバ及び HSM における操作ログを定期的に確認し、異常な操作やアクセスがないかどうかをチェックする ● エンティティ及び ACL の最新化チェック CA サーバ及び HSM に登録されたエンティティ及び ACL が運用ポリシーに基づき正確かつ最新であることを確認する。レビュー時には変更履歴を照合し、未承認の変更がないことを確認する

	これらのレビューは、F.44 で定義されたセキュリティメンテナンスの一環として実施される日常的な活動を定期的に振り返る目的で行う。具体的な頻度は、各組織のセキュリティポリシーやリスク評価に基づき、システムの重要度や使用状況に応じて柔軟に設定する。
F.39	F.38 に記載したように、当該 CKMS を構成するデバイスとして HSM 及び CA サーバを対象に、ソフトウェア部品の更新と脆弱性情報への対応を主とした定期的なセキュリティレビューを実施する。
F.40	定期的なセキュリティレビューの実施内容は F.38 に記載したものである。
F.41	当該 CKMS における HSM 及び CA サーバにパッチプログラムを適用する場合、CKMS が提供する機能への影響を確認するため、検証環境を用いた機能テストを実施する。この機能テストでは F.35 に準拠した手順に基づき、以下を検証する。 ● システム全体が正常に動作していること ● 暗号鍵管理や署名生成などの CKMS の主要機能が影響を受けていないこと ● パッチ適用後もセキュリティ要件が満たされていること この機能テストの結果は記録として保管し、問題が発生した場合には適切な修正を速やかに実施する。

③ 追加のセキュリティアセスメントで実行される要求事項を決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.42	FR11.14	CKMS 設計は、追加のセキュリティアセスメントが実施されるべき状況を明記しなければならない。	11.3 節
F.43	FR11.15	CKMS 設計は、追加のセキュリティアセスメントのスコープを明記しなければならない。	11.3 節

解説・考慮点

システムに著しい変更が加えられたとき、以下の範囲での変更箇所への追加のセキュリティアセスメントを実行すべきである。なお、累積的なシステム変更が著しい場合には、完全セキュリティアセスメントを実施すべきである。

- 前回のセキュリティアセスメント以降の第三者認証されたデバイスへの変更
- システム設計変更後のアーキテクチャレビュー
- CKMS の機能テスト及びセキュリティテスト

CKMS の設計にあたって、項目 F.42 及び F.43 は、追加のセキュリティアセスメントで実行される要求事項を明確化することを求めたものである。F.42 はアセスメントの実施条件、F.43 はアセスメントの範囲及び内容に関する要求事項がそれぞれ対象である。

上記のように、CKMS に大きなシステム変更があった場合には、追加のセキュリティアセスメントを実施すべきである。追加アセスメントの項目は、完全なセキュリティアセスメントの項目に基づいてシステム変更の影響に応じて選択する。「大きなシステム変更」とは、以下のようなケースを指す。

- CKMS 全体、または CKMS を構成する中核デバイスに関わる機能変更（例：暗号鍵生成、署名、認証機能などの改修や追加）
- 中核デバイスのハードウェアやソフトウェアの置き換え
- CKMS の性能や機能に関わる増強（例：新しいデバイスの統合やシステム拡張）

これらの変更が、CKMS のセキュリティ要件や運用ポリシーに及ぼす影響を評価するために、適切なスコープでのセキュリティアセスメントを実施することが求められる。

なお、上記のような「大きなシステム変更」が重要な機能等に及んだ場合、完全なセキュリティアセスメントを実施すべきである。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.42	当該 CKMS において、追加のセキュリティアセスメントは次の状況で実施する。 ● HSM、CA ソフトウェア、及び CA サーバの OS におけるメジャーなソフトウェアバージョンの更新時（機能変更を伴う大規模な更新を含む） ● OS セキュリティを支援するソフトウェアの新規導入、ベンダ変更、及びメジャーなバージョンの更新時 ● HSM のリプレイス時 ● CA サーバのリプレイス時
F.43	F.42 に記載した追加セキュリティアセスメントでは次の 3 つを実施する。 ● HSM に関わる第三者認証のレビュー ● CKMS 全体のアーキテクチャレビュー ● CKMS 提供機能に関わる機能テスト及びセキュリティテスト HSM のリプレイス時には、FIPS 140-2/-3 レベル 3 の認証が有効であることを確認する。

④ セキュリティメンテナンスで実行される要求事項を決めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.44	FR11.16	CKMS 設計は、セキュリティを維持するために、実行することが必要な堅牢化アクティビティをリスト化しなければならない。	11.4 節

解説・考慮点

当初は特定のセキュリティレベルを実現していた CKMS であっても、設定が変更されたり新しい脅威が発見されたりすることで、セキュリティレベルが低下することがある。そのため、セキュリティアセスメントとは別に、CKMS のセキュリティを維持・強化するために、堅牢化ガイドラインに従って適切に CKMS のメンテナンスを実施し、必要に応じてアップグレードすることが必要である。セキュリティメンテナンスには、以下の対策例が含まれる。

- CKMS を最新のセキュリティパッチで更新する
- 堅牢化ガイドラインに従ってシステム設定を定期的にレビューする
- 堅牢化ガイドラインに従って CKMS を定期的にテストする
- 更新された堅牢化ガイドラインを適用する
- 定期的なペネトレーションテストを行う

項目 F.44 は、CKMS の設計にあたって、セキュリティメンテナンスで実行される要求事項を明確化することを求めたものである。

本節②の定期的セキュリティアセスメントに記載したように、CKMS 運用中にセキュリティを維持するための日常的な活動に以下のものがある。

a) CKMS 内のデバイスやコンポーネント向けにベンダから提供されたアップデートパッチの適用可否を検討し、必要なパッチの適用や対策技術の導入を検討する
   - パッチ適用時には、CKMS の機能やセキュリティ要件に与える影響を評価し、運用後の動作確認を実施する
   - パッチ適用されない場合、該当する脆弱性に対する対策技術の導入を検討する

b) CKMS 内で取得した実行要求や操作ログを分析して、不正操作や異常な要求がないかを検出・対応する
   - 異常が検出された場合、速やかに原因分析を行い、必要な対策を実施する

c) CKMS エンティティとして権限を有する担当者の変更管理を行い、ACL の設定を正確かつ最新の状態に維持する
   - 担当者の異動やアクセス権変更要求が発生した際に更新を行い、定期的なレビューを実施することで適切なアクセス制御を維持する

これらの活動は、CKMS のセキュリティメンテナンスとして位置づけられ、システムの安全性と運用の堅牢性を確保するために継続的に実施する。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.44	当該 CKMS ではセキュリティメンテナンスとして以下の内容を実施する。 a) HSM、CA ソフトウェア、及び CA サーバの OS に対するセキュリティパッチの適用判断及び適用状況のチェック

	● ベンダからパッチがリリースされた時点でパッチの適用可否を判断し、適用後の動作確認を行う b) CA サーバ及び HSM における操作ログの確認と分析 ● 不正操作や異常な要求がないかを毎日または定期的に確認し、必要に応じて対応を実施する c) CA サーバ及び HSM に登録されたエンティティ及び ACL の最新化チェック ● アクセス権の変更要求が発生した時点や定期的なレビュー時に設定の正確性及び最新性を確認する 上記項目については、帳票を用いるなど棚卸し管理を実現できる仕組みを合わせて検討する。

4.4 CKMS へのアクセスコントロールの危殆化時の BCP 対策

解説・考慮点

本節は、SP 800-130 の 6.8 節に記載されている事項について解説したものである。なお、SP 800-130 の 6.8 節には 8 つの小節があるが、「設計指針」では内容に依存してそれらを 5.3 節、5.7 節、8.1 節、9.4 節に分離して記載してある[15]。

アクセスコントロールには、セキュリティ境界において、認可されたエンティティのみがセキュリティ境界内部に入れるようにするための門番としての役割がある。逆に言えば、アクセスコントロールが危殆化することは、直ちにセキュリティ危殆化につながるリスクがある。本節では、アクセスコントロールが危殆化した場合の対策を取り扱う。

アクセスコントロールの危殆化が検知された場合、鍵情報の危殆化と同様、次のステップを参考に、適切な当事者に危殆化を警告し、望ましくない影響を軽減し、最後にセキュアな状態に復帰することが必要である。

a) その原因及び範囲を決定するために危殆化を評価
b) 鍵情報（暗号鍵やメタデータ）の露出を最小化するために危殆化軽減手段を実行
c) 危殆化の再発を防止するために適切な是正手段を実施
d) CKMS をセキュアな運用状態に復帰させる

本節は一般的な情報システムにおけるアクセスコントロールが危殆化した場合の BCP 対策と共通する部分が多い。一方、CKMS 固有の要素としては管理する鍵情報の危殆化にまで影響が及んだかどうかをアセスメントし、その可能性がある場合には暗号モジュールや鍵情報の危殆化時の対応が必要となることが挙げられる。また、CKMS が管理する鍵を利用する情報システムの重

[15] 暗号鍵管理ガイダンスではそれぞれ以下の節に対応する。設計指針の 5.3 節と 5.7 節はガイダンス Part 1 の 2.3 節と 2.7 節、設計指針の 8.1 節と 9.4 節はガイダンス Part 2 の 3.1 節と 4.4 節である。

要性によってアクセスコントロールの強靭性に関わる要求レベルも様々である。このようなCKMS固有の観点も考慮して、情報システム全般におけるアクセスコントロールに責任を持つチーム（例えば、社内情報システムに関わるインシデントレスポンスチーム：CSIRT）とCKMS管理チームが連携して本節のBCP対策を実施することが望ましい。

① 物理セキュリティの危殆化に対するBCP対策を定めなければならない。

項目	FR番号	Framework Requirementsの内容	SP 800-130
F.45	FR6.123	CKMS設計は、あらゆるCKMSのコンポーネント又はデバイスへの物理セキュリティ侵害がCKMSによって検知されたときに、自動的に通知されるエンティティを明記しなければならない。	6.8.8節
F.46	FR6.122	CKMS設計は、CKMSがどのように暗号モジュール以外のコンポーネント及びデバイスへの認可されない（不正な）物理アクセスから回復するかを明記しなければならない。	6.8.8節
F.47	FR6.124	CKMS設計は、侵害された領域がどのようにセキュアな状態に再確立できるかを明記しなければならない。	6.8.8節

解説・考慮点

CKMSの物理セキュリティ侵害は、暗号鍵又は暗号モジュールの危殆化とは別の危殆化をもたらす可能性がある。一旦セキュリティが侵害されると、侵害された領域全体の完全性が疑わしくなるうえ、新しい暗号鍵及び機微な情報をまた将来危殆化させられるように、領域内のロジックを改ざんしている可能性がある。つまり、暗号鍵又は暗号モジュールの危殆化に対するBCP対策だけでは不十分であるかもしれない。

CKMSの設計にあたって、項目F.45は、物理セキュリティの侵害を検知した時の対応や手続きを明確化することを、F.46及びF.47はBCP対策として物理セキュリティの危殆化からの復旧を行うための手続きや要求事項を明確化することを求めたものである。
なお、物理セキュリティの危殆化に伴う暗号鍵又は暗号モジュールの危殆化の場合には、最初に物理セキュリティの危殆化に対するBCP対策を実施しなければならない。

本ガイダンスの4.1節で定めた物理セキュリティコントロールが危殆化して、設定したエンティティ以外の主体による物理アクセスが検知された場合（あるいは疑われる場合）、通報先や回復の手続きを定めることを要求している。

上記のように、別に定める暗号モジュールや鍵情報への危殆化対策（本ガイダンスの3.1.2節及びガイダンスPart 1の2.7節）と整合をとりながら、これらを補完する対策が求められる。不正な物理アクセスの波及範囲によっては、暗号モジュールや鍵情報の危殆化対策の実行も求められる。

CKMS の物理セキュリティコントロールの回復時には、同様の侵害を発生させないようなコントロール手段の構築と共に、侵害によって保護エリア内にバックドアが仕込まれていないかの検査が求められる。バックドアとしては物理的な仕掛け（例えば、盗聴器やリモートコントロール可能な装置）以外に、CKMS を構成するデバイスにおけるセキュリティコントロールの迂回となる設定変更やマルウェア設置なども考えられる。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。CKMS の物理アクセスコントロールとして、CKMS の設置エリア以外にその外側の建物や敷地へのコントロールもとられる。ここでは、CKMS の設置エリア内への不審者侵入を対象とする。建物や敷地への侵入に関わる検知や物理的アクセスコントロールの回復手順については組織の運用マニュアルに従った対応がされるものとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.45	当該 CKMS において、不審な物理アクセスの検知メカニズムは 4.1 節、F.04 に記載したとおりである。検知後の通報は CKMS 責任者及び CKMS 管理担当に行われる。
F.46	当該 CKMS において、CKMS 設置エリア内への不正な物理アクセスが検知あるいは疑われる場合、侵入経路と侵入範囲の特定、CA サーバや HSM への不正アクセスの痕跡調査、エリア内への不審な装置の有無などを調査する。調査結果に基づいて、侵入経路や侵入範囲に対する物理アクセスコントロールの強化対策を実施して機能回復を進める。その過程で暫定的な措置として、従来の物理アクセスコントロールの代替手段を講じる場合もある。回復時は侵入対策の刷新後に CKMS の再立ち上げを実施する。その際、CA サーバ及び HSM に対して初期化と再インストール、もしくはバックアップからの復元を実施する。
F.47	F.46 に記載したように、物理アクセスコントロールの機能回復及び機能強化に加えて、侵入対策の刷新後に CKMS の再立ち上げを実施する。また、CA サーバや HSM などの暗号モジュール、及びそれらデバイス内部の鍵情報の危殆化対策も影響範囲の調査結果に基づいて実施する。

② コンピュータシステムの危殆化に対する BCP 対策を定めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.48	FR6.114	CKMS 設計は、CKMS システムハードウェア、ソフトウェア、及びデータに対する認可されない改変を検出するために利用されるメカニズムを明記しなければならない。	6.8.5 節
F.49	FR6.115	CKMS 設計は、CKMS システムハードウェア、ソフトウェア、及びデータに対する認可されない改変からどのように CKMS が回復するのかを明記しなければならない。	6.8.5 節

解説・考慮点

重要なファイルへの改ざんが監視ユーティリティによって検出又はイベントログに表示された場合、当該ファイルは、正当でセキュアであると分かっているセキュアなストレージに保管されたバックアップファイルを使って置き換えるべきである。また、広範囲にわたってソフトウェアが改ざんされた場合、当該ソフトウェアは後述する障害・災害発生時の BCP 対策に記載された手順を準用すべきである。 CKMS の設計にあたって、項目 F.48 は、ハードウェア、ソフトウェア、及びデータに対する改ざんを検知するための要求事項を明確化することを、F.49 は BCP 対策としてハードウェア、ソフトウェア、及びデータに対する改ざんからの復旧を行うための手続きや要求事項を明確化することを求めたものである。

CKMS におけるコンピュータシステムのセキュリティコントロールは 4.1.2 節で定めている。4.1.2 節で定めた各種のセキュリティコントロールが迂回されたり不正な変更がされたりしないように権限の管理や設定変更に関わる監視を行う。主に 4.1.2 ④の監査機能によって、操作ログを元に監視が行われるのが一般的であるが、ログ自体が改ざんされないようにすることが前提となる。

コンピュータシステムにおける危殆化の検出と回復の手順を定めることが要求されている。多層防御のどこまでが無効化されたか危殆化事象の評価を行い、影響範囲に応じた回復手順を定めることが重要である。また、回復手順において再発防止策を検討し、多層防御の強化を図ることも重要である。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.48	当該 CKMS において、コンピュータシステムの危殆化の検知は、CA サーバにおいてセキュアブートにおけるソフトウェアのインテグリティチェックや操作ログの確認による。操作ログは CKMS 管理担当者によって異常な操作ログの有無が定期的に確認される。
F.49	当該 CKMS において、コンピュータシステムの危殆化や障害発生時、災害発生時の復旧対策として、重要な鍵情報や設定情報などは定期的にバックアップを取得しておく。機能回復時にはバックアップデータを利用して再設定を行う。また、危殆化事象の評価を行い、適切な再発防止策をとり、コンピュータシステムのセキュリティコントロールを強化する。なお、CA サーバや HSM などの暗号モジュールの危殆化や内部の鍵情報の危殆化が疑われる場合は、それぞれの危殆化時の対応策を実施する。

③ ネットワークセキュリティコントロールの危殆化に対する BCP 対策を定めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.50	FR6.116	CKMS 設計は、システムによって使用されるネットワークセキュリティコントロールの危殆化からどのように回復するかを明記しなければならない。特に、 a) CKMS 設計は、それぞれのネットワークセキュリティコントロールデバイスに対して考えられる危殆化シナリオを明記しなければならない。 b) CKMS 設計は、それぞれの想定される危殆化シナリオに対して、この節に記載されたどの軽減技術が採用されるかを明記しなければならない。 c) CKMS 設計は、採用されるあらゆる追加又は代替の軽減技術を明記しなければならない。	6.8.6 節

解説・考慮点

ネットワークセキュリティコントロールの危殆化は CKMS 自体の危殆化につながり得る。以下が危殆化の例である。

- ネットワークセキュリティコントロールデバイスの物理的危殆化
- ネットワークセキュリティコントロールデバイスで使用されるひとつ以上の暗号鍵の危殆化
- ネットワークセキュリティコントロールデバイスを管理するために使用されるひとつ以上の暗号鍵の危殆化
- 危殆化につながるネットワークアーキテクチャの変更（例えば、誰かが VPN 接続されたワークステーションをセキュアでないネットワークに接続し、VPN ワークステーションがイントラネットを攻撃するために使用される）
- 特権ユーザのパスワード（例えば、システム管理者のパスワード）の危殆化
- プラットフォーム OS の危殆化
- ネットワークセキュリティアプリケーション（例えば、ファイアウォール、IDS 等）の危殆化
- プロトコルへの新しい攻撃による危殆化

ネットワークセキュリティコントロールの危殆化の状況によって、取るべき是正措置（軽減措置や回復手段）が異なる。このため、全ての状況において、インシデントを完全に調査し、ネットワークセキュリティコントロールの危殆化に起因して他のシステム及び暗号鍵のどれが危殆化した可能性があるのかを特定する必要がある。

BCP 対策としての復旧策も、個々の危殆化のシナリオごとに用意する必要がある。具体的な対策については SP 800-130、6.8.6 節に記載されている。

項目 F.50 は、CKMS の設計にあたって、BCP 対策としてネットワークセキュリティコントロールの危殆化からの復旧を行うための手続きや要求事項を個々の危殆化のシナリオごとに明確化することを求めたものである。

CKMS におけるネットワークセキュリティコントロールは 4.1.3 節で定めている。これらはネットワーク境界の防御やネットワーク経由での侵入の検知や防御を行うメカニズムであり、上記のように、様々な危殆化シナリオが考えられる。SP 800-130、6.8.6 節に上記の危殆化シナリオに応じた危殆化対応の概要が記載されているので、これを参考に危殆化時の回復手順を定めることが推奨される。

多層防御のどこまでが無効化されたか危殆化事象の評価を行い、影響範囲に応じた回復手順を定めることが重要である。また、回復手順において再発防止策を検討し、多層防御の強化を図ることも重要である。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.50	当該 CKMS におけるネットワークセキュリティコントロールについて、4.1.3 節、F.17 に記載したように、フィルタリング機能を搭載したルータ、ホスト搭載型の IDS、外部からのシステム管理の目的で設置した VPN がある。 a) 危殆化シナリオとして、以下の 3 つを想定する。 ● ルータの物理的危殆化 ● ルータや VPN アクセスポイントを管理する特権ユーザのパスワードの危殆化 ● IDS の危殆化 b) 上記の危殆化シナリオに対する是正措置として、以下を定める。 ● ルータの物理的危殆化の是正措置としては、ルータ製品の置き換えを実施する。フィルタリング機能や処理性能、特権ユーザの認証機能については従来機と同等以上の製品を採用する。 ● ルータや VPN アクセスポイントにおける特権ユーザのパスワード危殆化の是正措置としては、パスワードの置き換えとパスワードエントロピーのチェックを実施する。また、より強固な新たな認証方式があれば是正措置の候補とする（例えば 2 要素認証など）。 ● IDS 危殆化の是正措置としては、セキュリティパッチの適用、及び、同等以上の攻撃検出性能を有するアプリケーション製品への置き換えを検討する。 また、上記是正措置に加えて、CKMS のマルウェアスキャン、インテグリティチェック、ログの確認を含む危殆化事象の評価を行い、CA サーバや HSM などの暗号モジュールの危殆化や内部の鍵情報の危殆化が疑われる場合は、それぞれの危殆化時の対応策を実施する。 c) 上記 a)b)に記載した事項以外に実施する緩和策として、以下を定める。

	● フィルタリングルールや侵入検知シグネチャの設定や更新状況の確認 ● ルータや IDS における通信ログの監視と分析 ● パスワード管理など情報セキュリティの教育及びインシデント対応訓練の実施

4.5 CKMS 設備への障害・災害発生時の BCP 対策

解説・考慮点

本節は、SP 800-130 の 10.1 節から 10.5 節に記載されている事項について解説したものである。
CKMS の障害は情報へのアクセスの停止につながる可能性がある。障害が発生する原因としては、システム故障のほか、災害等による物理的損害や公共サービスの供給停止などがある。本節では、災害等を含めたあらゆる事象発生時にどのように運用継続性を達成するのかについて取り扱う。

なお、本節では鍵情報の喪失・破損からの復旧を想定しており、各検討項目の内容が検討項目 B.71 及び B.72 の内容（「設計指針」の 5.6 節[16]）に矛盾しないようにすべきである。また、流出や暴露などの鍵情報の危殆化からの復旧は想定していないことに注意されたい。鍵情報の危殆化からの復旧に関しては、「設計指針」における 5.7 節及び 9.4 節[17]を参照して定める必要がある。

① CKMS 設備への物理的損害発生時における BCP 対策を定めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.51	FR10.1	CKMS 設計は、必要な環境的、火災、及び物理的なアクセスコントロール保護メカニズム、及び損害からの基幹及び全てのバックアップ設備への回復手続きを明記しなければならない。	10.1 節

解説・考慮点

設備への物理的損害発生を想定したバックアップ及び回復設備は、保護されるデータ及び CKMS 運用の価値と機微度にふさわしいレベルで設計、実装及び運用されるべきである。例えば、風水害や地震は環境リスクであり、火災は環境リスク及び設備設計に依存したリスクの両方に該当する。

[16] 暗号鍵管理ガイダンスでは Part 1 の 2.6 節に対応する。
[17] 暗号鍵管理ガイダンスではそれぞれ Part 1 の 2.7 節と Part 2 の 4.4 節に対応する。

項目 F.51 は、CKMS の設計にあたって、CKMS 設備への物理的損害発生を想定した BCP 対策として準備すべき要求事項、及び、復旧を行うための手続きや要求事項を明確化することを求めたものである。なお、物理的損害には、システム故障だけでなく、風水害や地震、火災などのあらゆるリスクに起因するものも含む。

上記のように、地震及び水害などの自然災害、並びに火災及び事故などの人為災害が発生して CKMS を収容した施設やエリアに対して損害が生じ、CKMS の運用が困難となる、物理的アクセスコントロールに影響が及ぶなどの事態が考えられる。予めそうした状況を想定して予防措置や回復の手順を定めておくなどの BCP 対策を検討することを求めている。

CKMS が管理する鍵情報を利用する情報システムや対象製品におけるサービス継続の重要性や必要性を踏まえて、BCP 対策を検討することが重要である。BCP に関わる一般的な予防措置としては、冗長系を用意すること、内部の重要な情報をバックアップすること、及び保険に加入することなどがある。冗長系への切り替え及びバックアップ情報からの復旧などの訓練を定期的に行うことも重要である。また、本節の災害対応については、事前に施設レベルで準拠する耐震基準、火災・風水害の防災基準の準備状況、及び非常用電源の有無などを確認しておくことも具体的な対応項目として挙げられる。

施設への災害に関わる BCP 対策について、以下のような文献が参考になる。

- 「データセンター　セキュリティ　ガイドブック」、日本データセンター協会
- 「金融機関等コンピュータシステムの安全対策基準・解説書」、金融情報システムセンター

また、保護されるデータ及び CKMS 運用の価値と機微度にふさわしいレベルの決定にあたっては、FIPS 199 及び FIPS 200 が参考になる。

CKMS の施設レベルの災害発生に伴って、物理アクセスコントロールが無効となった結果、正規エンティティ以外が管理エリアにアクセス可能となるなど、各種のセキュリティコントロールが危殆化した状態と同様の状況も生じ得る。CKMS の復旧においては、このような点も踏まえた手順を検討することが望ましい。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.51	CKMS が提供する機能のうち、IoT 製品向け証明書の発行については、IoT 製品の製造設備の構成要素の一つと捉えることができる。また、証明書の失効機能については、CKMS が機能を停止している間は新たな失効処理を実行できないが、機能停止が短期間であれば IoT 製品の運用に与える影響は限定的である。以上の理由から、当該 CKMS の災害対策は IoT 製品の製造設備と同程度の基準とする。なお、IoT 製品の生産においては同一の機能を持つ製造ラインが、複数拠点に存在する。ある拠点が稼働できない場合は、他の拠点にて生産を補うことは可能であり、それぞれの製造拠点が代替の製造拠点を構成しているため、以下の方針とする。 1. 基本方針 災害復旧対策を目的としたプライベート CA システム単位の冗長化は行わない。ただし、製造工場において障害対策として以下を実施する。CA サーバにおけるディスクの冗長化、CA サーバ及びルータについて予備デバイスの準備、HSM に対して障害発生時に代替機が提供される保守契約の締結。 2. バックアップの取得と保管 CA サーバの設定、ルータの設定、並びに HSM 内部の鍵情報及び設定のバックアップを、各デバイスの設定及び鍵情報の変更前後に取得する。バックアップは、製造工場のバックアップ設備と同じ基準を満たす場所（例えば、幾つかの製造拠点）にも保管する。 3. 物理セキュリティ危殆化時の対策 地震・火災等により物理セキュリティが危殆化した際は、鍵情報及び CKMS へのアクセスコントロールが危殆化したものとして対応する。具体的な対策は暗号鍵管理ガイダンス Part1「2.7 鍵情報の危殆化時の BCP 対策」及び本ガイダンス「4.4 CKMS へのアクセスコントロールの危殆化時の BCP 対策」を参照する。 4. 復旧手順の準備 災害が発生した製造拠点における復旧手順を準備する。 ● 予備デバイス及び代替機への必要なパッチ及びアップデートの適用 ● 予備デバイス及び代替機への初期状態からのソフトウェアのセットアップ ● 予備デバイス及び代替機へのバックアップからの設定及び鍵情報のリカバリー ● 鍵情報及び CKMS へのアクセスコントロール危殆化からの回復 ● CKMS の運用再開 5. 復旧訓練の実施 災害シナリオを想定した復旧訓練を年 1 回実施する。

② 公共サービス（電気、水道、下水道、空調等）の停止時における BCP 対策を定めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.52	FR10.2	CKMS 設計は、基幹及び全てのバックアップ設備に対する、電気、水道、衛生、暖房、冷房、及び空気清浄に関する推奨要求値だけでなく最小要求値についても明記しなければならない。	10.2 節

解説・考慮点

CKMS の継続的な可用性を保証するためには、通常運用時及び非常時において、全ての CKMS デバイスの要求を満たすのに十分な電力が基幹及び全てのバックアップ CKMS 設備で利用可能であるように準備されておく必要がある。例えば、同じ影響を受けないようにするため、基幹設備とバックアップ設備とは別系統の独立した電力線から電力供給を受けることが必要である。

項目 F.52 は、CKMS の設計にあたって、公共サービス（電気、水道、下水道、空調等）の停止を想定した BCP 対策として準備すべき代替手段への要求事項を明確化することを求めたものである。最小要求値とは、公共サービスの停止に伴って代替手段が切り替わった時に、CKMS の継続的な可用性を保証するために最低限確保することが必要な電力や水道、空調などの容量のことである。

上記のように、CKMS の運用に必要な電気及び水道などの公共サービスの停止を想定した BCP 対策に関わる項目である。公共サービスの停止によって空調の稼働にも影響が及ぶ。本節①で述べたように、災害が原因となり公共サービスが停止する場合もある。電力については、自家発電設備や UPS など蓄電設備を設置する対策が考えられる。また、CKMS への電力供給の推奨要求値や最小要求値を明確にすることで、準備すべきバックアップ電源の選定基準を定める。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。以下に記載した最小要求値は仮想的な数値であることに注意されたい。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.52	F.51 と同様に、当該 CKMS は IoT 製品の製造設備と同程度の対策を必要とする。公共サービス停止時の対策は、製造工場の対策を前提とし、製造工場がその最小保証値を維持できない場合には安全にシステムを停止し、公共サービス復旧後に CKMS を再稼働する。ただし、CKMS 単体の対策として、製造設備全体での対策である自家発電設備に加え、短時間の電力供給停止及び電源異常（過電圧・過負荷・雷など）への対応として UPS を設置する。UPS は CA サーバ、HSM、ルータへの短時間の電力供給が可能であればよいため、以下の方針とする。 ● 1500VA、30 分の電力供給が可能な UPS を選定する

③ 通信及び計算機能の機能停止時における BCP 対策を定めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.53	FR10.3	CKMS 設計は、ユーザ、エンタープライズ、及び CKMS アプリケーションによる予測されるニーズに見合うサービスの運用継続を保証するために、設計内に存在し、かつ運用中に利用可能であることを要求される通信及び計算機能の冗長性を明記しなければならない。	10.3 節

解説・考慮点

CKMS の高可用性を保証するためには、必要な機能を実行しユーザが要求するサービスを提供するために十分な通信及び計算能力を必要とする。このため、もともと CKMS には冗長な通信設備等がバックアップとして設置されることも多い。一方、非常時にはこのバックアップ手段が代替手段として活用できる。

項目 F.53 は、CKMS の設計にあたって、ユーザニーズの増大への対応の他、通信及び計算機能の機能停止を想定した BCP 対策としても利用可能な代替手段への要求事項を明確化することを求めたものである。

上記のように、CKMS の運用に必要な通信及び計算機能の可用性に関わる項目である。通信に関しては、障害に備えて冗長性を備えたネットワーク構成や回線の二重化といった対策が採用される。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.53	当該 CKMS の通信は製造工場内の LAN 及びインターネット接続回線を使用する。また、当該 CKMS の計算機能の冗長性については CA サーバと HSM、ルータが対象となる。以下の方針とする。 1. 通信の冗長化 LAN へは平時には有線ケーブルを使用して接続し、バックアップとして無線アクセスポイントを用意する。有事に備え、無線アクセスポイントへの切り替え手順を定める。 インターネット接続回線は、施設全体で通信事業者と回線二重化の障害対策がとられている。そのため、CKMS 独自の対策は実施しない。 2. 計算機能の冗長化

	CA サーバ及びルータの予備デバイスを用意し、製造工場内に保管する。HSM は障害発生時に代替機が提供される保守契約を結ぶ。 3. バックアップの取得と保管 CA サーバ、ルータの設定、並びに HSM 内部の鍵情報及び設定のバックアップを、設定及び鍵情報の変更前後に取得する。バックアップは、製造工場内に保管する。 4. 復旧手順の準備 製造工場において以下の内容を実施するための復旧手順を準備する。 ● 予備デバイス及び代替機への必要なパッチ及びアップデートの適用 ● 予備デバイス及び代替機への初期状態からのソフトウェアのセットアップ ● 予備デバイス及び代替機へのバックアップからの設定及び鍵情報のリカバリー ● CKMS の運用再開 5. 復旧訓練の実施 障害シナリオを想定した復旧訓練を年 1 回実施する

④ ハードウェア障害発生時における BCP 対策を定めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.54	FR10.4	CKMS 設計は、バックアップの方策、及びハードウェアコンポーネント及びデバイスの障害からの回復のための方策を明記しなければならない。	10.4 節

解説・考慮点

CKMS は情報管理システムのセキュアな運用にとって極めて重要であるため、CKMS コンポーネント及びデバイスのハードウェア障害の影響は最小限に抑えることが望ましい。そのためには、例えば、同じ故障を引き起こすことがないようにするため、基幹システムからの独立性を持っているバックアップシステムを常時スタンバイしておくといった対策がある。
ただし、ハードウェア障害からの回復が容易でありスピードもある対策は一般にコストがかかるものであり、CKMS の設計において冗長性と対策コストとの間の最適なトレードオフを見出すことが必要である。

項目 F.54 は、CKMS の設計にあたって、システムハードウェア障害発生を想定した BCP 対策としても準備すべき要求事項、及び、復旧を行うための手続きや要求事項を明確化することを求めたものである。

CKMS を構成するデバイスにハードウェア障害が発生した場合、その影響を最小限に抑えるための項目である。冗長性を持たせることを基本方針とする。メインのハードウェアとバックアップとなるハードウェアを常時稼働させ、障害発生時に速やかにバックアップ系に移行する方法と、バックアップ系を常時稼働させず、メイン系の状態を定期的に同期させる方法がある。バックアップ系はメイン系から独立性を持つことが不可欠であり、同一の障害がメイン系とバックア

ップ系の両方に影響しないように設計することが重要である。なお、障害発生時の影響を最小限に抑えようとすれば、その分コストが高くなるというトレードオフがある。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.54	F.53 に記載のとおり、当該 CKMS では CA サーバとルータは製造工場内に予備デバイスを準備するが、HSM は障害発生時に代替機が提供される保守契約を結ぶものとする。バックアップ取得と復旧の手順は次のようになる。 ● CA サーバ及びルータ ソフトウェア及び設定情報を変更する都度、バックアップを取得し、予備機へ同期する。復旧の際は予備機を起動して予備機に切り替える。 ● HSM 鍵情報、設定情報及びソフトウェアを変更する都度、バックアップを取得する。復旧の際は代替機を取り寄せ、バックアップからリカバリーする。

⑤ ソフトウェア障害発生時における BCP 対策を定めなければならない。

項目	FR 番号	Framework Requirements の内容	SP 800-130
F.55	FR10.5	CKMS 設計は、システムソフトウェアの正しさを検証するために、CKMS によって提供されている全ての技術を明記しなければならない。	10.5 節
F.56	FR10.6	CKMS 設計は、ソフトウェアがメモリにロードされたときにソフトウェアの改変又は破損を検知するために、CKMS によって提供される全ての技術を明記しなければならない。	10.5 節
F.57	FR10.7	CKMS 設計は、バックアップ及び重大なソフトウェア障害からの回復のための方策を明記しなければならない。	10.5 節

解説・考慮点

ソフトウェア障害の原因としては、「（製造時の）ソフトウェアバグ」と「（実行時の）予期せぬソフトウェアの破損」がある。前者のような多くのソフトウェア障害は、良好な確立されたプログラミング実践を使用してコードを書くことで防ぐことができる。一方、後者のような、コードが破損する障害は可能な限り速やかに検知されるべきである。これには、マルウェア感染も含まれる。

ソフトウェア障害はいずれ起きるとの仮定の下で運用すべきであり、その対策として、完全なセキュア状態のシステムバックアップが定期的に作成され、最新の CKMS のセキュア状態がリロードされて修復され、CKMS が運用可能な状態に復旧できるようにすることが推奨される。

CKMS の設計にあたって、項目 F.55 はソフトウェア障害を発生させないための対策としての要求事項を明確化することを、F.56 はソフトウェア障害の原因となるリスクを検知するための要求事項を明確化することを、F.57 はソフトウェア障害発生を想定した BCP 対策としても準備すべき要求事項、及び、復旧を行うための手続きや要求事項を明確化することを求めたものである。

上記のように、本節は、ソフトウェア障害に関わる緩和策、及びソフトウェア障害を起因とする障害対策に関わる要件である。ソフトウェアの開発工程におけるバグや脆弱性の作り込みを低減する手法については、製品セキュリティと呼ばれる領域でベストプラクティスがある。セキュリティに配慮したコーディング規約（セキュアコーディング）の適用やソースコードの静的解析などが該当する。また、既知脆弱性の検査やファジングテストを実施することも推奨される。例えば、「脆弱性対処に向けた製品開発者向けガイド（IPA）」に解説がある。

ソフトウェアの破損を検知する具体的な手法としては、ソフトウェアのインテグリティチェックや既知解テストなどが挙げられる。

ソフトウェアのバグや脆弱性を完全に除去することや、ソフトウェア破損を実行前に完全に検出することは困難である。そのため、ソフトウェア障害を起因とした障害への対策を検討しておくことが重要である。障害発生時に発生前の正常な状態にリカバリーできるように備える必要がある。そのためには、ソフトウェアや設定情報が正常かつ安全な状態にあるときに取得したバックアップを保存しておくことが有効な緩和策となる。

《トイモデルと記載例》

本節のトイモデルも 1 章に示した、IoT 製品（家電想定）向けプライベート CA システムとする。

IoT 製品（家電想定）向けプライベート CA システムにおける記載例

F.55	自社で開発するソフトウェアについては、バグや脆弱性の作り込みを低減するセキュアコーディング手法を適用し開発する。CKMS の本格的な運用開始前にテストを実施し、機能が正しく動作するか、不正な変更や故障が発生していないか確かめる。また、使用するソフトウェア（CA サーバ、ルータ、HSM にて動作する OS やアプリケーションなど）について、バグや脆弱性に起因したパッチ及びソフトウェアアップデートが提供された場合には、リリースノートを確認する等して修復が保証されていることを確認し、パッチ及びソフトウェアアップデートを適用する。適用後には、運用開始前に CKMS の運用に悪影響がないことをテストし確認する。
F.56	CA サーバはセキュアブートによりソフトウェアの改変及び破損を検知する。また、HSM は適宜自己テストを実行することによりソフトウェアの改変及び破損を検知する。

F.57	ソフトウェアや設定情報が正常かつ安全な状態にあるときにバックアップを取得する。 バックアップから CKMS を回復した後、CKMS の運用を再開する前に、CKMS の運用に悪影響がないことをテストし確認する。 なお、重大なソフトウェア障害から回復する場合、そのソフトウェア障害は分析され修復が保証されたものである必要がある。

Appendix 参考資料一覧

本文に記載した参考資料、規格、制度、資格、技術論文等を一覧としてまとめる。概ね本文での記載順に、章を単位に記載した。章の間で重複するものもある。

■ 1 章　はじめに

- 「政府機関のサイバーセキュリティ対策のための統一基準（令和 5 年度版）」、NISC
  https://www.nisc.go.jp/pdf/policy/general/kijyunr5.pdf
- 「CRYPTREC 暗号リスト（電子政府推奨暗号リスト）」、CRYPTREC
  https://www.cryptrec.go.jp/list.html
- 「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」、CRYPTREC
  https://www.cryptrec.go.jp/list.html
- 「暗号鍵設定ガイダンス」、CRYPTREC
  https://www.cryptrec.go.jp/op_guidelines.html
- 「暗号鍵管理システム設計指針（基本編）」、CRYPTREC
  https://www.cryptrec.go.jp/op_guidelines.html
- 「暗号鍵管理ガイダンス Part 1（2023 年 5 月発行）」、CRYPTREC
  https://www.cryptrec.go.jp/op_guidelines.html
- NIST SP 800-130（A Framework for Designing Cryptographic Key Management Systems）
  https://csrc.nist.gov/pubs/sp/800/130/final

■ 2 章　暗号鍵管理システム（CKMS）の設計原理と運用ポリシー

- RFC 3647（Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework）
  https://www.rfc-editor.org/rfc/rfc3647
- NIST SP 800-57 Part 2（Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations）
  https://csrc.nist.gov/pubs/sp/800/57/pt2/r1/final
- 政府認証基盤 GPKI（Government Public Key Infrastructure）
  https://www.gpki.go.jp/
- PKCS #11（Cryptographic Token Interface Base Specification）
  https://www.oasis-open.org/2023/08/10/two-pkcs-11-oasis-standards-published/
- PKCS #10（Certification Request Syntax Specification）
  https://www.rfc-editor.org/rfc/rfc2986
- RFC 5280（Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile）
  https://www.rfc-editor.org/rfc/rfc5280
- FIPS 140-2/-3
  https://csrc.nist.gov/pubs/fips/140-2/upd2/final

https://csrc.nist.gov/pubs/fips/140-3/final

- ISO/IEC 15408
  https://www.iso.org/standard/72891.html
  https://www.ipa.go.jp/security/jisec/about/kijun.html
- CMVP 認証
  https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program
- 政府情報システムのためのセキュリティ評価制度（クラウドサービスの評価認証制度）ISMAP
  https://www.ismap.go.jp/csm?id=csm_ismap_index
- セキュリティ要件適合評価及びラベリング制度（JC-STAR）
  https://www.ipa.go.jp/security/jc-star/index.html
- サイバーレジリエンス法、欧州
  https://www.cyberresilienceact.eu/
- サイバーセキュリティ法、中国
  http://www.npc.gov.cn/zgrdw/npc/xinwen/2016-11/07/content_2001605.htm
- GDPR（General Data Protection Regulation）、欧州
  https://eur-lex.europa.eu/eli/reg/2016/679/oj
- 電子署名法
  https://www.digital.go.jp/policies/digitalsign
- 「暗号強度要件（アルゴリズム及び鍵長）設定基準」、CRYPTREC
  https://www.cryptrec.go.jp/list.html
- 「注意喚起情報」、CRYPTREC
  https://www.cryptrec.go.jp/er.html

■ 3 章　暗号鍵管理デバイスへのセキュリティ対策

- FIPS 140-2/-3
  https://csrc.nist.gov/pubs/fips/140-2/upd2/final
  https://csrc.nist.gov/pubs/fips/140-3/final
- ISO/IEC 15408
  https://www.iso.org/standard/72891.html
  https://www.ipa.go.jp/security/jisec/about/kijun.html
- PKCS #11（Cryptographic Token Interface Base Specification）
  https://www.oasis-open.org/2023/08/10/two-pkcs-11-oasis-standards-published/
- Shamir の秘密分散法
  https://dl.acm.org/doi/10.1145/359168.359176
- CMVP 認証
  https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program
- CAVP 認証
  https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program

■ 4 章　暗号鍵管理システム（CKMS）のオペレーション対策

- 「データセンター セキュリティ ガイドブック」、日本データセンター協会
  https://www.jdcc.or.jp/topics/127/
- 「金融機関等コンピュータシステムの安全対策基準・解説書」、金融情報システムセンター
  https://www.fisc.or.jp/publication/guideline_pdf.php
- FIPS 140-2/-3
  https://csrc.nist.gov/pubs/fips/140-2/upd2/final
  https://csrc.nist.gov/pubs/fips/140-3/final
- CMVP 認証
  https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program
- 「セキュリティ設定共通化手順 SCAP（Security Content Automation Protocol）概説」、IPA
  https://www.ipa.go.jp/security/vuln/scap/scap.html
- NIST SP 800-207（Zero Trust Architecture)
  https://csrc.nist.gov/pubs/sp/800/207/final
- 「脆弱性対処に向けた製品開発者向けガイド」、IPA
  https://www.ipa.go.jp/security/guide/vuln/forvendor.html
- 「ソフトウェア管理に向けた SBOM の導入に関する手引」、経済産業省
  https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html
  https://www.meti.go.jp/policy/netsecurity/vendor.html#id05
- CISSP (Certified Information Systems Security Professional)
  https://japan.isc2.org/cissp_about.html
- 情報処理安全確保支援士（Registered Information Security Specialist, RISS）
  https://www.ipa.go.jp/jinzai/riss/index.html
- CISM (Certified Information Security Manager)
  https://www.isaca.org/credentialing/cism
- FIPS 199（Standards for Security Categorization of Federal Information and Information Systems）
  https://csrc.nist.gov/pubs/fips/199/final
- FIPS 200（Minimum Security Requirements for Federal Information and Information Systems）
  https://csrc.nist.gov/pubs/fips/200/final

発行日　2025 年 4 月 25 日　　第 1 版発行

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

暗号鍵管理ガイダンス Part 2

～ 暗号鍵管理システム設計指針の理解を助ける副読本 ～

【作成】

CRYPTREC
Cryptography Research and Evaluation Commitees

CRYPTREC とは、デジタル庁・総務省・経済産業省・NICT・IPA が実施している暗号技術評価プロジェクトのこと。暗号技術の専門家により安全性と実装性に優れると判断された CRYPTREC 暗号リストを作成・公表している。

【発行】

独立行政法人情報処理推進機構 セキュリティセンター

2025 年 4 月 25 日　第 1 版