CRYPTREC GL-3002-1.0

暗号鍵管理システム設計指針（基本編）

令和２年７月

独立行政法人情報処理推進機構
国立研究開発法人情報通信研究機構

目次

【修正履歴】

修正日	修正内容
2020.07.07	第 1 版公開
2019.7.12 (draft ver.)	ドラフト版公開

1 はじめに

1.1. 位置づけ

「暗号鍵管理システム設計指針（基本編）」（以下、「本設計指針」という）は、6.1.1 節に示すようなセキュアな暗号アルゴリズムを利用する上で極めて重要な役割を果たす**暗号鍵**の管理に関する在り方を解説し、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る。

具体的には、本設計指針では、暗号鍵管理の必要性を認識してもらうために「暗号鍵管理の在り方」（暗号鍵管理の位置づけと検討すべき枠組み）について解説する。これは、あらゆる暗号鍵管理を検討する際の基礎となる考え方を示したものである。

さらに、「暗号鍵管理についての技術的内容」について解説する。この解説は、CKMS の包括的な設計指針である NIST SP800-130「A Framework for Designing Cryptographic Key Management Systems」の解説書・利用手引書として活用できるように構成してある。NIST SP800-130 は、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ものである。本設計指針では、それらの項目を『暗号鍵管理における目的に応じた』対象範囲に分類・再構成することによってそれぞれの項目の目的や必要性を明確化した。

なお、本設計指針は、SP800-130 同様、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**。また、セキュリティ要求事項は定義せず、具体的な特定のセキュリティ機能の採用を義務づけることもしない。よって、**どのようにそれらの要求事項に対応（例えば、ポリシー、暗号アルゴリズム、デバイス等の選択）するかは CKMS 設計者に委ねられ、それらの対応方針が設計仕様書や運用マニュアル等に記載される**。

暗号鍵管理における検討漏れがないかどうか、対応方針が適正かどうかの判断は、セキュリティシステム管理責任者・CKMS 調達責任者が行うことであり、必要に応じて、別のガイドラインやドキュメント等を参考にすべきである。

本設計指針は、SP800-130 同様、以下の利点を提供する。

a) CKMS の要求事項を提示することで CKMS 設計タスクを定義する助けになる
b) CKMS 設計者に、CKMS 全体に必要な要素を考慮するように促す
c) CKMS 設計者に、CKMS にセキュリティを提供できる要素と仕組みを考慮するように促す
d) 異なる複数の適合 CKMS 及びその機能について論理的に比較するために使用できる
e) 実装されている CKMS の機能仕様が明文化されることで、CKMS セキュリティアセスメントを実行する助けになる
f) セクタ（業界や企業、部署等）ごとの CKMS プロファイルの基礎を形成する

1.2. 想定読者

イントロダクションとして記載されている 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ており、CKMS 設計者だけでなく、セキュリティシステム管理責任者、システムインテグレータ、及び調達責任者を含んでいる。

「暗号鍵管理についての技術的内容」となる 4 章以降については、SP800-130 と同様、主として CKMS 設計者を想定読者としている。

1.3. 適用範囲

本設計指針は、あらゆる分野・あらゆる領域の全ての CKMS を対象とする。CKMS は、暗号処理及びその処理で利用する暗号鍵を管理するシステム全体を包含する。ただし、暗号処理及び暗号鍵を管理・運用するのに必要な機能以外の部分は本設計指針の対象外である。

また、本設計指針の適用範囲に CKMS のシステム規模は問わない。もっとも小さい単純なものは一つのデバイス（の一部分）からなる場合（図 1-1）もあるし、暗号鍵管理センタで複数のデバイスを集中管理するような大規模システムの場合（図 1-2）もある。例えば、前者は暗号モジュールを使うデバイス、後者は社内情報システムなどが挙げられる。

どの範囲を CKMS の対象とするのかは、「暗号鍵管理システムの設計原理と運用ポリシー」の中で CKMS 設計者によって具体的に定義される。

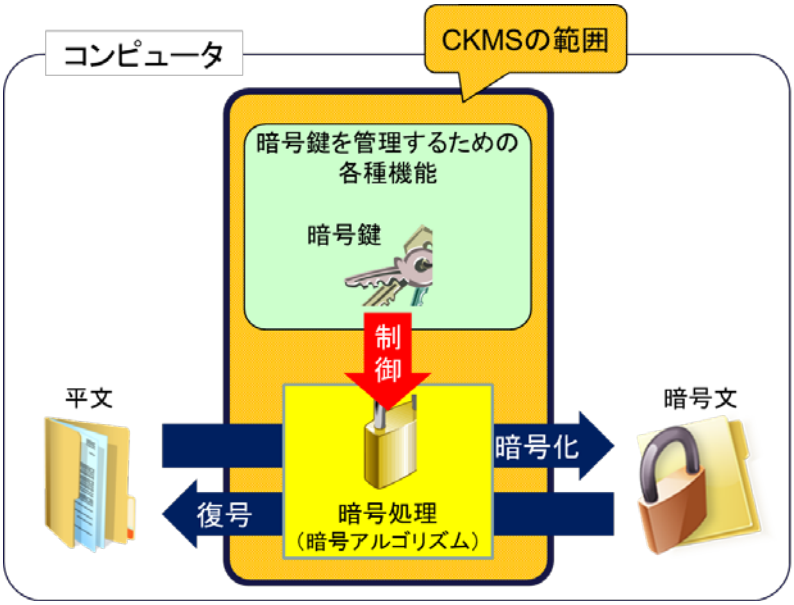

図 1-1 単純な CKMS の概要例

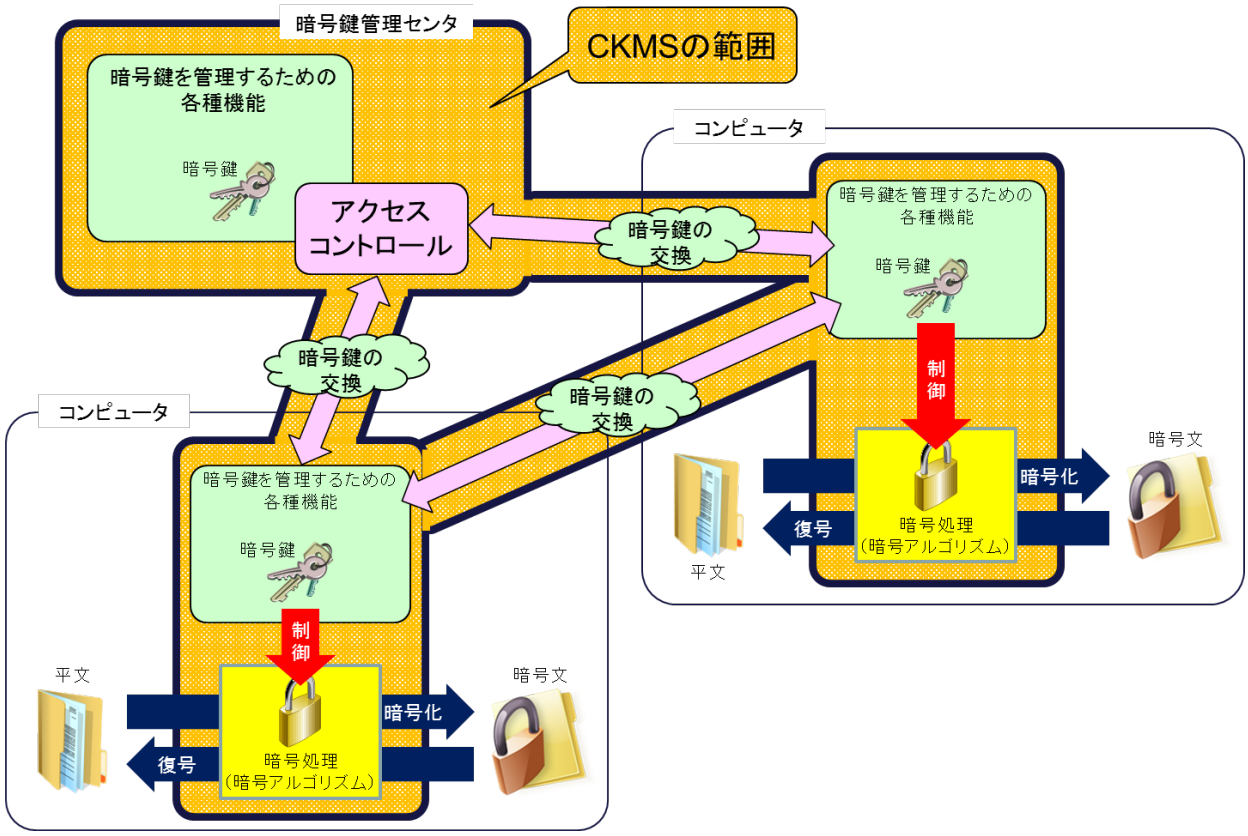

図 1-2　複雑な CKMS の概要例

1.4.　構成

本設計指針は、9 章で構成されており、章立ては以下のとおりである。

2 章では、イントロダクションとして暗号鍵管理の在り方や考え方について解説する。あらゆる暗号鍵管理における基礎をなすものである。

3 章では、本設計指針の活用方法について解説する。

4 章以降が CKMS の包括的な設計指針である SP800-130 の解説書・利用手引書として活用できるように、SP800-130 の内容を再構成したものである。暗号鍵管理における目的ごとに章分けをしている。なお、本設計指針だけでも項目や概要が分かるように記載しているが、正確な内容については SP800-130 を参照されたい。

1.5.　検討体制

本設計指針は、2018 年度及び 2019 年度 CRYPTREC 暗号技術活用委員会において作成された。

表 1-1　暗号技術活用委員会の構成（2020 年 3 月時点）

委員長	松本　勉	横浜国立大学　大学院環境情報研究院　教授
委員	上原　哲太郎	立命館大学　情報理工学部　教授
委員	垣内　由梨香	マイクロソフト株式会社　セキュリティレスポンスチーム セキュリティプログラムマネージャー
委員	菊池　浩明	明治大学　総合数理学部　先端メディアサイエンス学科　教授
委員	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	杉尾　信行	株式会社 NTT ドコモ　情報セキュリティ部
委員	清藤　武暢	日本銀行金融研究所　情報技術研究センター 主査　[2019 年 8 月まで]
委員	宇根　正志	日本銀行金融研究所　情報技術研究センター 情報技術研究グループ長　[2019 年 9 月から]
委員	手塚　悟	慶應義塾大学　環境情報学部　教授
委員	寺村　亮一	株式会社 NDIAS　自動車セキュリティ事業部　マネージャー
委員	松本　泰	セコム株式会社　IS 研究所 コミュニケーションプラットフォームディビジョン マネージャー
委員	三澤　学	三菱電機株式会社　情報技術総合研究所 情報ネットワーク基盤技術部 トラステッドシステム技術グループ　主席研究員
委員	満塩　尚史	内閣官房　情報通信技術(IT)総合戦略室　政府 CIO 補佐官
委員	山岸　篤弘	一般財団法人日本情報経済社会推進協会 電子署名・認証センター　客員研究員
委員	山口　利恵	東京大学　大学院情報理工学系研究科 ソーシャル ICT 研究センター　特任准教授
委員	渡邊　創	国立研究開発法人産業技術総合研究所 サイバーフィジカルセキュリティ研究センター 副研究センター長
事務局	神田 雅透	情報処理推進機構　セキュリティセンター
	橋本 徹	〃
	伊藤 忠彦	〃 [2019 年 8 月から]
	盛合 志帆	情報通信研究機構　サイバーセキュリティ研究所[2019 年 7 月まで]
	野島　良	〃 [2019 年 8 月から]
	吉田 真紀	〃
	大久保 美也子	〃

1.6. 参考資料

NIST SP800-130：
https://csrc.nist.gov/publications/detail/sp/800-130/final

NIST SP800-130 日本語訳：
https://www.ipa.go.jp/files/000083774.pdf

2 暗号鍵管理の在り方

2.1 暗号鍵管理の必要性

暗号アルゴリズムは、機密性、完全性、認証を目的として使われる。

- 機密性：
  データを認可されない開示（窃取）から保護することで、情報保護のために使われる。セキュアな暗号アルゴリズムであれば、対称鍵又はプライベート鍵（暗号鍵の一種、詳細は 7.1 節参照）を持つ認可された当事者のみが暗号文を元の平文に復号できる。
- 完全性：
  データを認可されない改変（改ざん）から保護することで、改ざん検知・メッセージ認証のために使われる。暗号アルゴリズムを使ったセキュアな認証コードやデジタル署名であれば、正当な暗号鍵を持たないエンティティによるデータ改ざんを当該データの使用前に検出できる。
- 認証：
  データが正しいエンティティから来たものであることを確認（ソース認証）したり、相手が正しいエンティティであることを確認（エンティティ認証）したりするために使われる。暗号アルゴリズムを使ったセキュアな認証方法やデジタル署名であれば、正当な暗号鍵を持たないエンティティを使用前に検出できる。なお、方式によっては、エンティティの個体認証や権限認可までも含めることがある。

総務省と経済産業省は、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、2013 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）」を策定した。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

- 電子政府推奨暗号リスト：
  CRYPTREC により安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨する暗号技術のリスト
- 推奨候補暗号リスト：
  CRYPTREC により安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト
- 運用監視暗号リスト：
  実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったと CRYPTREC に

より確認された暗号技術のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。

実際、「政府機関の情報セキュリティ対策のための統一基準（平成 30 年度版）」（平成 30 年 7 月 25 日、サイバーセキュリティ戦略本部）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、以下の通り、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。

6.1.5 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、以下の措置を講ずること。
（略）
(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」を参照**した上で、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並びにそれを利用した安全なプロトコル及びその運用方法について、以下の事項を含めて定めること。
(ア) 職員等が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、**「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用**させること。
(イ) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、**「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用**すること。
(ウ) 暗号化及び電子署名に使用するアルゴリズムが危殆化した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること。
(エ) **暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定める**こと。
（以下、略）

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。これは、図 2-1 に示すように、暗号アルゴリズムの脆弱性を攻撃される場合の攻撃対象範囲や想定リスクと、暗号鍵管理の脆弱性も含めて攻撃される場合の攻撃対象範囲や想定リスクが違うことに起因する。

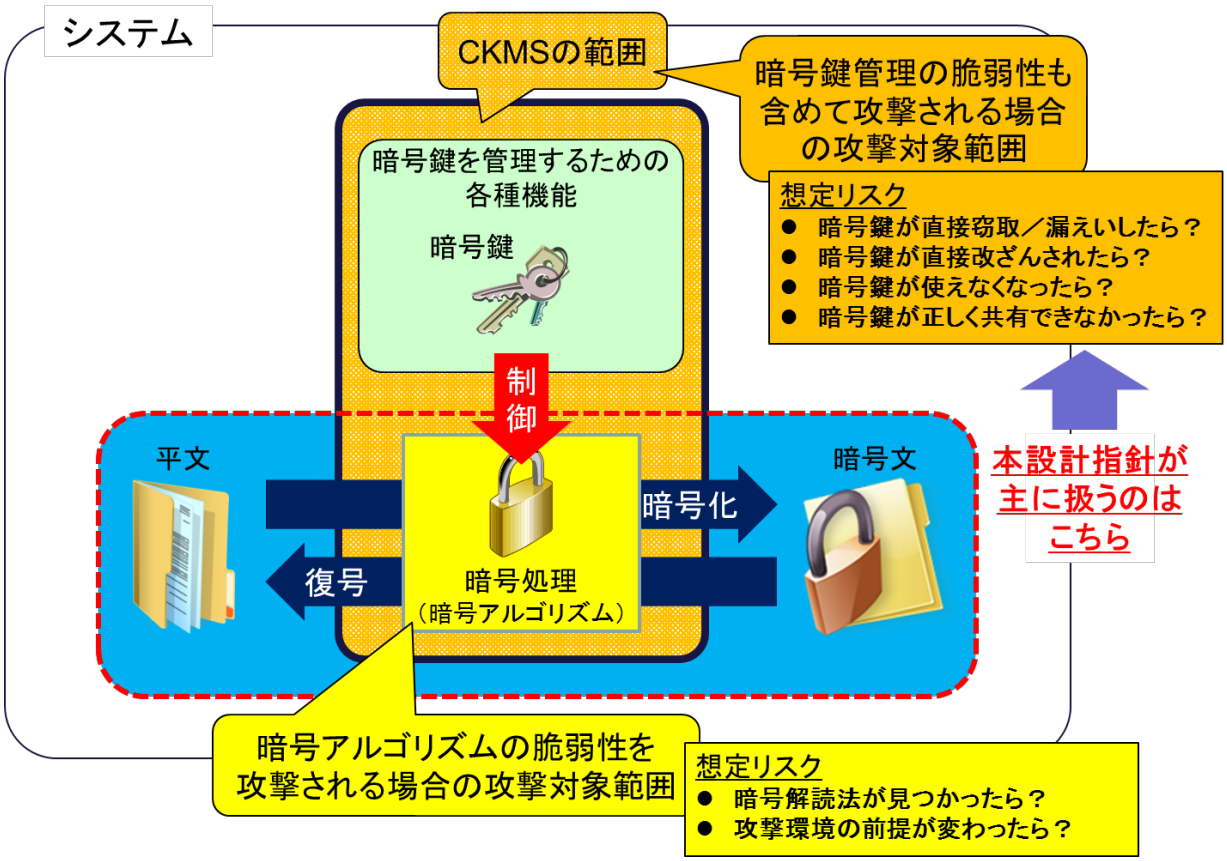

図 2-1　暗号アルゴリズムと CKMS の攻撃対象範囲／想定リスクの違い

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いる数多くのインシデントが発生している。

今まで日本では、暗号アルゴリズムや鍵長の選択など、特定の項目についてのガイドラインはあるものの、暗号鍵管理（システム）の設計指針の基準となる包括的・統一的なガイドラインが作られていなかった。その結果、暗号アルゴリズムや鍵長などの選択と比較すると、暗号鍵管理の重要性が十分に認識されず、暗号鍵のライフサイクルや安全な保管方法、危殆化時の対策など、暗号鍵管理上重要な項目について検討が不十分になっている恐れがある。このことは、システム全体の安全性確保に支障を来たす原因となり得る。

2.2　暗号鍵管理の考え方の枠組み

本設計指針では、国内外の暗号鍵管理に関するガイドラインを調査し、これらのガイドラインに記載された内容から、暗号鍵管理の考え方の枠組みを図 2-2 のように整理し、暗号鍵管理のための設計仕様書や運用マニュアルがどのように作られるべきかを明確にした。

暗号鍵管理の構成要素は、「Framework Requirements」「Profile Requirements」「System Requirements」「Guidance」の 4 つからなる。図 2-3 は、各構成要素の関連性を示す一例である。

それぞれの構成内容は以下の小節で説明する。

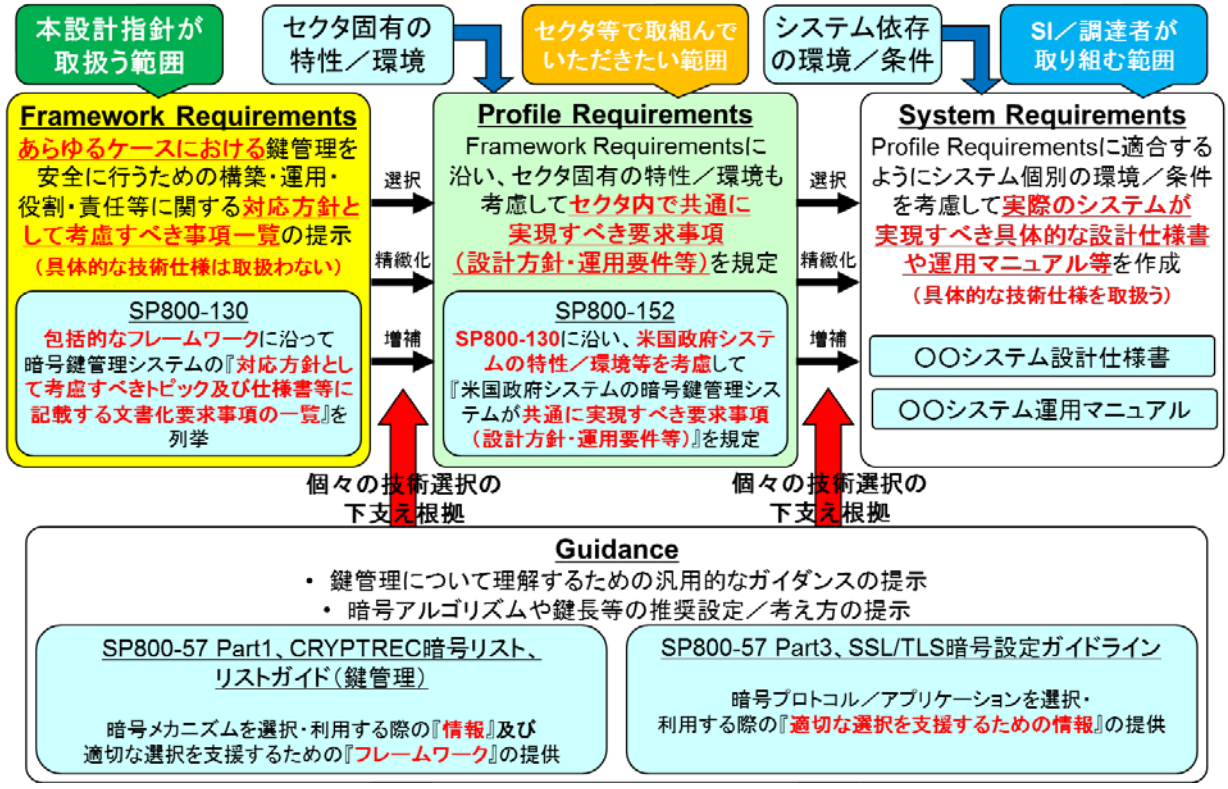

図 2-2　暗号鍵管理の考え方の枠組み

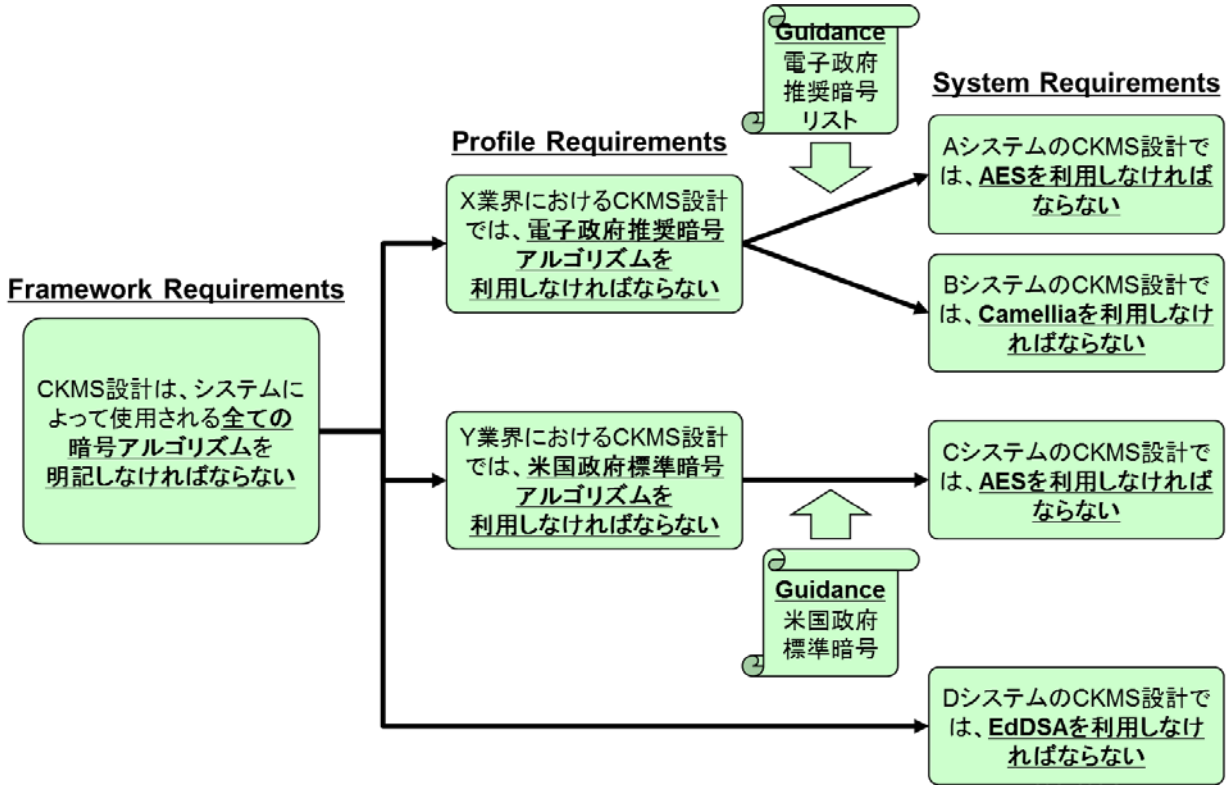

図 2-3　各構成要素の関係性の例

2.2.1　Framework Requirements

Framework Requirements は、暗号鍵を必要とするあらゆるユースケースにおける CKMS を対象に、暗号鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として考慮すべき一連の事項を包括的なフレームワークとして取りまとめたものある。SP800-130 が代表例であるとともに、本設計指針もここに位置する。

Framework Requirements の目的は、CKMS における設計・運用方針を明確化させ、後述する Profile Requirements や System Requirements にその設計・運用方針の内容を明記させることにある。つまり、Profile Requirements や System Requirements を具体的に検討・設計する際の考え方や検討項目を列挙した設計手引書的な位置づけのものであり、セクタ（業界や企業、部署等）固有の特性や利用環境等を考慮して当該セクタ内で共通に実現すべき要求事項（設計・運用要件等）にブレークダウンしたプロファイルを作成する際の指針となるように作られている。

このため、Framework Requirements の要求事項はすべて「○○を**明記しなければならない**」という形をとる一方、システムの個別事情には踏み込まず、採用すべき具体的な技術仕様を規定しない。例えば、図 2-3 のように、システムが利用する暗号アルゴリズムに関して、Framework Requirements では「暗号アルゴリズムを明記しなければならない」という検討項目はあるが、「どのような暗号アルゴリズムを使わなければならないか」といった技術仕様は規定しない。

具体的に「○○をどのように実行（対策）するか」といった詳細な技術仕様の規定は、セクタ別あるいはシステム個別の固有の特性や環境等に依存して決定すべき側面が強いと考えられる。このため、どのような要求仕様／設計方法を採用するかは、CKMS 設計者、又は SP800-130 や本

設計指針に基づいた Profile Requirements のような他のドキュメントに委ねられる。

本設計指針を参考に、各業界や各社が Profile Requirements や System Requirements の作成に自ら取り組んでいただくことを期待している理由はそこにある。

2.2.2 Profile Requirements

本設計指針において、「セクタ」とは、製品、システム又はサービスへの共通の要求事項を持つ組織のグループのことである。多くの企業等が集まる業界単位の場合も、一社あるいは一部署の場合もある。

Profile Requirements は、セクタ固有の特性や環境を踏まえたセクタ内で共通に実現すべき要求事項（設計方針・運用要件等）を規定したものである。セクタ内での相互運用システムにおいて満たさなければならないセキュリティと相互運用性に関わる要求事項一式を規定するようなものであり、Framework Requirements に記載されている項目一覧に沿って、後述する Guidance の技術的根拠を加味しながらセクタでの必要性を満たすように選択、増補、あるいは精緻化される。例えば、SP800-152 は、セクタ＝米国政府と位置付けた、米国政府向け CKMS Profile Requirements であり、米国政府システム共通の CKMS としての要求事項が規定されている。

Framework Requirements は各々の記載項目について検討することを要求するものの、具体的な設計方針や要求事項の是非を判断するものではない。Profile Requirements や System Requirements を作成する段階で、Framework Requirements の各々の記載項目に対応すべきかどうかを検討し、要求事項として対応すべきと判断した場合に具体的な設計方針や要求事項が決められる。つまり、「要求事項の対象」と判断した項目については、どのような対応を取ることが要求されるのかを Profile Requirements のひとつ又はそれ以上の要求事項として対応付けられる。例えば、図 2-3 のように、システムが利用する暗号アルゴリズムに関しての「暗号アルゴリズムを明記しなければならない」という Framework Requirements の検討項目に対して、「電子政府推奨暗号アルゴリズムを利用しなければならない」「米国政府標準暗号アルゴリズムを利用しなければならない」等といった要求事項を規定する。

なお、Framework Requirements の各々の検討項目において、その目的及び概要に照らして「要求事項の対象外」と判断した項目については Profile Requirements から除外することが可能である。例えば、自然災害での BCP 計画が別のドキュメントで規定されており、CKMS 設計の仕様書に含める必要がない場合、9.5 節の「CKMS の障害・災害発生時の BCP 対策」は対象外とすることができる。その場合、対象外と判断した理由を Profile Requirements に記述しておくことが強く望まれる。もしくは、考慮対象の範囲を先に明示しておくことによって、考慮対象外の範囲を明確化しておく。

2.2.3 System Requirements

System Requirements は、システム個別の利用環境や条件等を考慮して作成された、実際の CKMS が実現すべき具体的な設計仕様書や運用マニュアル等（以下、「CKMS 設計書」という）のことである。システムが依存する利用環境や条件等と Guidance の技術的根拠の両方を加味して、参照する Profile Requirements に適合するように選択、増補、あるいは精緻化され、具体的な技術仕様

として取りまとめられる。また、参照する Profile Requirements がない場合には、Framework Requirements を活用して要求事項を直接規定することもできる。

なお、参照する Profile Requirements の要求事項に適合するように System Requirements での要求事項が決められたとしても、別の Profile Requirements の要求事項には適合しない場合があることに注意されたい。

2.2.4 Guidance

暗号鍵管理についての技術的な理解を助け、推奨設定などを提供する文献のことである。Framework Requirements から Profile Requirements を、また Profile Requirements から System Requirements を策定する場合の選択や精緻化おける技術的根拠となるものである。例えば、セキュアな暗号アルゴリズムや鍵長の選択を支援するためのドキュメントがある。暗号アルゴリズムを対象としたものには SP800-57 part 1 や CRYPTREC 暗号リスト、リストガイド（鍵管理）が、暗号プロトコルを対象としたものには SP800-57 part 3 や TLS 暗号設定ガイドラインなどが該当する。

2.3 暗号鍵管理における検討項目の目的別分類

SP800-130 では、CKMS を構築するうえで考えるべき検討項目（Framework Requirements）が網羅的にカバーされており、この範囲をベースに検討を行えば CKMS 設計・運用上の仕様記載漏れはほとんどないと思われる。事実、「CKMS 設計者は、カバーされている全てのトピックを取り扱うチェックリストとして本フレームワークを使用することが期待される」と記載されている。しかしながら、検討項目が全部で 258 個もあるものの、実際の CKMS の利用環境によっては重点的に取り扱ったほうがよい項目もあれば取り扱う必要がない項目も含まれている。

そこで本設計指針では、SP800-130 に記載されているトピックスや Framework Requirements を大きく以下の 6 つの『暗号鍵管理における目的（取り扱い項目）に応じた対象範囲』に分類・グループ化することによって、検討すべき項目の目的や必要性を明確化し、分かりやすく整理し直した。これにより、対象とする CKMS の利用環境に応じて本当に必要な検討項目をあらかじめ抽出することができ、効率よく CKMS 設計・構築に反映できると期待している。併せて SP800-130 全体の日本語訳[1]も公開している。

【A】暗号鍵管理システムの設計原理と運用ポリシー

CKMS として実現すべき全体方針を取り決める検討項目（A.01～A.69）を集めており、本設計指針第 4 章にまとめている。ここには、主に以下のような検討項目を含んでいる。

[1] NIST SP800-130 日本語訳, https://www.ipa.go.jp/files/000083774.pdf

- 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、B 以降の検討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。

【B】暗号アルゴリズム運用のための暗号鍵管理オペレーション対策

A での方針を実現するために、生成から廃棄までのライフサイクル全期間にわたって暗号鍵を管理するのに必要となる機能や運用方法を取り決める検討項目（B.01～B.81）を集めており、本設計指針第 5 章にまとめている。ここには、主に以下のような検討項目を含んでいる。

- どのような目的を持つ暗号鍵を利用するのか
- その暗号鍵はどこでどのように保管されるのか
- 暗号鍵の生成から廃棄までのライフサイクル全期間中どのように暗号鍵を運用し、それを実現するために必要な機能群はどういったものか

ここでの検討項目は「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。

【C】暗号アルゴリズムの選択

利用する暗号アルゴリズムの選択条件を取り決める検討項目（C.01, C.02）を集めており、本設計指針第 6 章にまとめている。ここには、主に以下のような検討項目を含んでいる。

- どのようなセキュリティ強度の暗号アルゴリズムを利用するか

ここでの検討にあたっては、A 及び B の方針（検討結果）に合致するように取り決めなければならない。

【D】暗号アルゴリズム運用に必要な鍵情報の管理

B で規定した個々の暗号鍵及び当該暗号鍵に関連付けられているメタデータについて、具体的な設定方法や保管方法などを取り決める検討項目（D.01～D.10）を集めており、本設計指針第 7 章にまとめている。ここには、主に以下のような検討項目を含んでいる。

- 暗号鍵及びメタデータ（総称して「鍵情報」という。）の有効期間はどのぐらいか
- どのように鍵情報を生成するか
- どのように窃取や改ざんなどから鍵情報を保護するか

ここでの検討にあたっても、A 及び B の方針（検討結果）に合致するように取り決めなければならない。

【E】暗号鍵管理デバイスのセキュリティ対策

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）を集めており、本設計指針第 8 章にまとめている。ここには、主に以下のような検討項目を含んでいる。

- 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

ここでの検討項目は「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、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いる。特に、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・保管を行う主な実現手段であるため、特出しで取り上げられている。

【F】暗号鍵管理システムのオペレーション対策

CKMS 全体に対して、必要に応じて検討する項目（F.01～F.57）を集めており、本設計指針第 9 章にまとめている。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。

上記 6 つの目的の関係性を図 2-4 に示す。上記の【A】～【D】は CKMS の利用環境に関わらず検討する必要がある項目をまとめている。【E】は個々のデバイスにおける暗号鍵の実際の運用・管理が必要な場合に、また【F】はシステム全体での運用・管理までも包含する場合に追加

で必要となる検討項目である。【E】や【F】を含める必要があるか否かは、CKMS 設定者と、システム管理責任者や調達責任者等との合意により決めるべきものである。

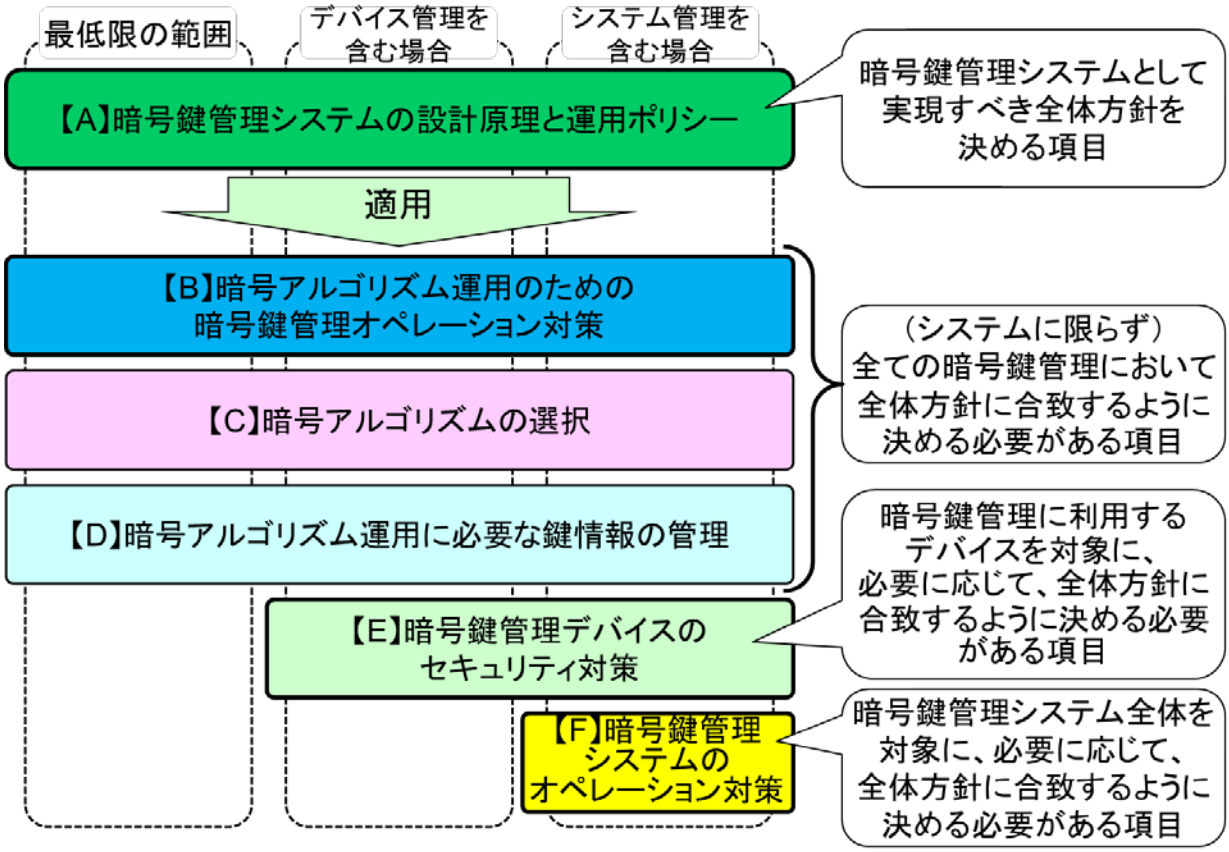

図 2-4　暗号鍵管理における目的別分類関係

また、表 2-1 に各目的とそれに対応する取り扱い項目を示す。本設計指針での 4 章以降が各目的それぞれに、また取り扱い項目がそれぞれの章の小節に該当する。参考まで、それぞれの取り扱い項目が、SP800-130 でのどの節に記載されている内容であるかを SP800-130 での該当節欄に記載している。

表 2-1　目的別分類と取り扱い項目一覧

	目的	取り扱い項目	SP800-130 での該当節
A	（4 章）暗号鍵管理システムの設計原理と運用ポリシー	（4.1 節）CKMS セキュリティポリシー	4.3, 4.4, 4.5
		（4.2 節）情報管理ポリシー等からの要求事項	4.6, 4.7
		（4.3 節）セキュリティドメインポリシー	4.9
		（4.4 節）CKMS における役割と責任	5
		（4.5 節）CKMS の構築環境／実現目標	2.10, 3.1, 3.2, 3.4, 3.5, 6.2, 7
		（4.6 節）標準／規制に対する適合性	3.3, 4.8
		（4.7 節）将来的な移行対策の必要性	7, 12
B	（5 章）暗号アルゴリズム運用のための暗号鍵管理オペレーション対策	（5.1 節）CKMS 設計	2.5
		（5.2 節）鍵情報のライフサイクル	6.3
		（5.3 節）鍵情報のライフサイクル管理機能	6.4, 6.8
		（5.4 節）鍵情報の保管方法	6.4, 6.5
		（5.5 節）鍵情報の鍵確立方法	6.4, 6.6
		（5.6 節）鍵情報の破損時の BCP 対策	10.7
		（5.7 節）鍵情報の危殆化時の BCP 対策	6.8
C	（6 章）暗号アルゴリズムの選択	（6.1 節）暗号アルゴリズムのセキュリティ	2.1
		（6.2 節）CRYPTREC 暗号リスト	―
D	（6 章／7 章）暗号アルゴリズム運用に必要な鍵情報の管理	（7.1 節）鍵情報の種類	2.2, 6.1, 6.2
		（7.2 節）鍵情報の選択	6.1, 6.2
		（7.3 節）鍵情報の保護方針	6.2
E	（8 章）暗号鍵管理デバイスのセキュリティ対策	（8.1 節）鍵情報へのアクセスコントロール	6.4, 6.7, 6.8, 8.4
		（8.2 節）セキュリティ評価・試験	9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7
		（8.3 節）暗号モジュールの障害時の BCP 対策	10.6
F	（9 章）暗号鍵管理システムのオペレーション対策	（9.1 節）CKMS へのアクセスコントロール	8.1, 8.2, 8.3
		（9.2 節）システム保証	9.8
		（9.3 節）セキュリティアセスメント	11.1, 11.2, 11.3, 11.4
		（9.4 節）CKMS のアクセスコントロールの危殆化時の BCP 対策	6.8
		（9.5 節）CKMS の障害・災害発生時の BCP 対策	10.1, 10.2, 10.3, 10.4, 10.5

2.4　セキュリティポリシーの階層構造

各種ポリシーは組織目標をサポートするように設計されるべきであり、情報管理レベルの課題を取り扱う上位のポリシーからデータ保護に関する特定のルールを取り扱う下位のポリシーで構成される階層構造のポリシー群を形成することが多い（図 2-5 参照）。ポリシーの各層は様々な形態で相互に関係し、中間層及び下位層に位置するポリシーはより高位層のポリシーよりもさらに詳細に規定される。

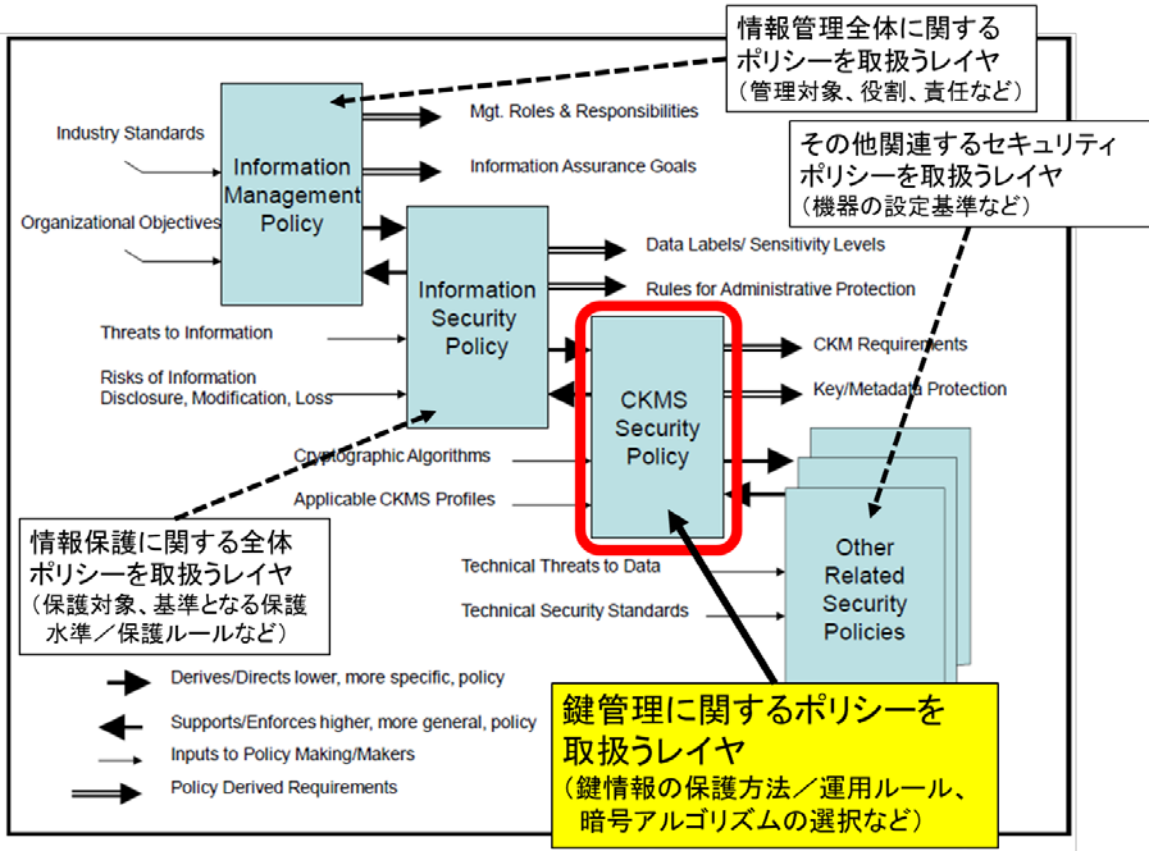

図 2-5　セキュリティポリシーの関連図（出典：SP800-130 より一部改変）

情報管理ポリシーは、情報管理全体に関するポリシーを取り扱う。具体的には、情報管理対象の特定、各種管理者の役割及び責任範囲、情報管理を実行するために必要な権限等を規定する。

情報セキュリティポリシーは、情報管理ポリシーで特定された情報管理対象に対する情報保護のための全体ポリシーを取り扱う。例えば、保護対象となる情報（カテゴリ）の特定、情報の機密レベルの区分や各機密レベルに応じたセキュリティ保護水準・ルール等を規定する。

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の規定を技術的に実現するように、CKMS によって使用される全ての暗号鍵とメタデータの機密性、完全性及び可用性を保護するためのルールを確立し、暗号鍵、暗号アルゴリズム及びセキュリティメカニズムの使用方法と保護方法を規定する。CKMS セキュリティポリシーに則って、CKMS の設計や運用が行われる。

このことは、CKMS セキュリティポリシーの作成及び CKMS 設計に先立ち、情報管理ポリシー及び情報セキュリティポリシーが作られていることを前提とすることを意味する。CKMS セキュリティポリシーから情報管理ポリシーや情報セキュリティポリシーが作られるわけではないことに留意されたい。

本設計指針の利用にあたっても、情報管理ポリシー及び情報セキュリティポリシーが別途作成済みであることを前提とする。もしそれらのポリシーが作成されていないのであれば、CKMS セキュリティポリシーの作成や CKMS 設計に入る前に、情報管理ポリシー及び情報セキュリティポリシーを策定することが先決である。

2.5 暗号鍵管理における時間管理

暗号鍵管理においては「時間」の概念が非常に重要である。時間管理の中で、いつまでに何を準備しなければならないのかを判断し、仕様書や運用マニュアルに組み入れておく必要があるためである。

本設計指針では、時間管理の概念を以下のように定義する。図 2-6 が暗号鍵管理における時間管理の概念図である。

- CKMS のセキュリティライフタイム：
  CKMS の運用開始から運用終了までの期間のことをいう。

- （暗号アルゴリズムの）セキュリティライフタイム：
  暗号アルゴリズムが利用できる運用開始から運用終了までの期間のことをいう。この期間が CKMS のセキュリティライフタイムよりも短ければ、将来的によりセキュリティ強度が高い暗号アルゴリズムへの移行が必要となる(図 2-6 の「暗号アルゴリズムの移行」)。
  なお、本指針では、単に「セキュリティライフタイム」ということがある。

- （情報の）ライフタイム：
  情報が生成されてから廃棄されるまでの期間のことをいう。通常、この期間全体にわたって情報が保護されるようにする必要がある。
  もしこの期間中に、情報を保護するために利用している暗号鍵が廃棄・失効することがあれば、暗号鍵を交換したうえで、再度保護しなおす必要がある（図 2-6 の「暗号鍵の交換」）。また、利用している暗号アルゴリズムのセキュリティライフタイムが終了する場合には、暗号鍵だけでなく暗号アルゴリズムも交換したうえで、再度保護しなおす必要がある（図 2-6 の「保護手段の移行」）。
  なお、本指針では、単に「ライフタイム」ということがある。

➢ 最大許容暗号鍵有効期間：
同一の鍵情報（暗号鍵やメタデータ）が利用可能な期間の最大許容値のことをいう。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（図 2-6 の「暗号鍵の延長不可」）。

➢ 暗号鍵有効期間：
鍵情報（暗号鍵やメタデータ）が生成されてから廃棄される（予定を含む）までの期間のことをいう。暗号鍵の更新処理（5.3 節⑨）を行って新たに設定される廃棄時期が最大許容暗号鍵有効期間内であれば、その廃棄時期まで同一の鍵情報（暗号鍵やメタデータ）を継続して使うこともできる（図 2-6 の「暗号鍵の延長可」）。

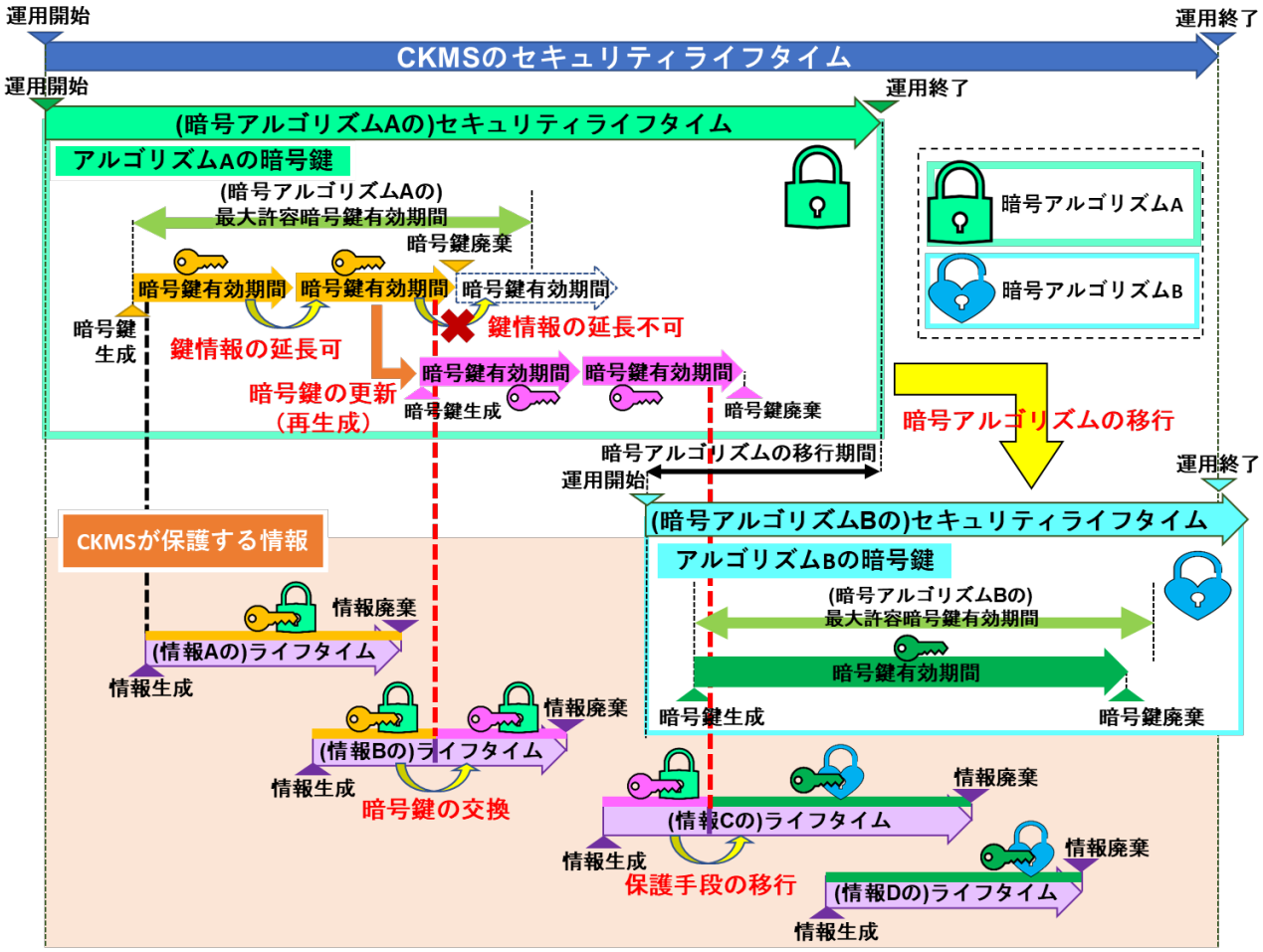

図 2-6　暗号鍵管理における時間管理の概念図

2.6　関連ガイドラインの俯瞰図

国内外において暗号鍵管理に関するガイドラインがいくつか発行されており、それらを網羅的

に調査した。図 2-7 に示すように、調査結果からは SP 800-57 Part1 と SP 800-130 は非常に強い関連性を持ち、また暗号鍵管理全体のフレームワークとして最も基本的な文献であると考えられることが分かった。

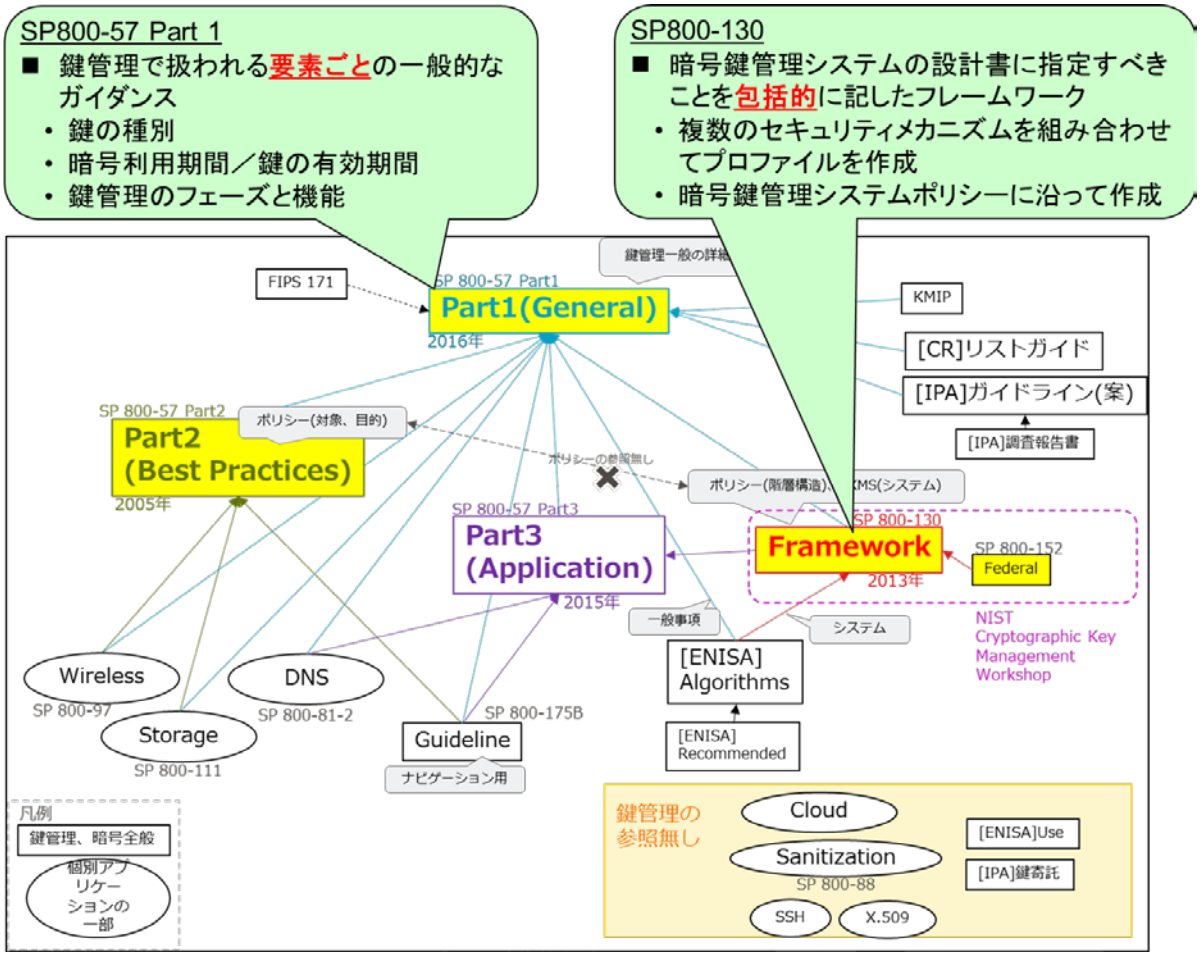

図 2-7　各文献における暗号鍵管理に関する他文献への参照関係

具体的には、SP800-57 Part 1 では「暗号鍵管理で扱われる要素ごとの一般的なガイダンス」について記載されており、特に、暗号アルゴリズムの利用期間（セキュリティライフタイム）、暗号鍵の種別、暗号鍵の有効期間、暗号鍵管理のフェーズと機能といったトピックスが取り上げられている。このため、多くのガイドラインが暗号鍵管理の一般的事項として SP 800-57 Part 1 を参照しており、暗号鍵管理の基礎的な位置付けにある。また、SP800-130 では「CKMS 設計書に指定すべきことを包括的に記したフレームワーク」を提示しており、CKMS ポリシーに沿って複数のセキュリティメカニズムを組み合わせてプロファイルを作成するための指針を示している。実際、米国政府の CKMS 設計ガイドライン SP800-152 からは、SP800-57 ではなく、SP800-130 が参照されている。

2.6.1 SP800-57

暗号アルゴリズムを不適切に選択した場合、セキュリティを確保することは困難である。仮にプロトコルやアプリケーションにおいて不適切な選択がなされた場合、実際のセキュリティにほとんど（あるいは、まったく）寄与しない。そこで、暗号アルゴリズムを選択・利用する際のバックグランド情報の提供及び適切な選択を支援するためのフレームワークを提供するために、SP800-57 Recommendation for Key Management が作成された。

SP800-57 は、Part 1 General、Part 2 Best Practices for Key Management Organization、Part 3 Application の 3 つが作られており、それぞれ想定読者や記載内容が異なる。

Part 1 は、暗号鍵管理の一般的なガイダンスを提供していて、想定読者はシステム管理者、暗号モジュール開発者、プロトコル開発者、システム管理者と幅が広い。内容も Hash や MAC、乱数生成等の暗号アルゴリズムの説明から暗号鍵管理まで幅広く書かれている。2005 年に初版が発行され、2006 年、2007 年、2012 年（revision 3）、2016 年（revision 4）に改訂されている。

基本的には、暗号鍵管理の理解のためのガイダンスとなっており、「一般的な暗号鍵管理ガイダンス」の章と「暗号鍵管理のフェーズと機能」の章で構成されている。

- 「一般的な暗号鍵管理ガイダンス」では、鍵の種別を説明し、鍵の種別や非対称鍵／対称鍵ごとに鍵の有効期間を詳しく説明している。鍵サイズや暗号スイートについても述べられている。
- 「暗号鍵管理のフェーズと機能」では、運用前、運用、運用後、破棄後の 4 つのフェーズでの暗号鍵管理の機能が説明されている。

Part 2 は、組織が暗号鍵管理のポリシーを作成する際に検討する内容とポリシーを実現するための文書に書くべき内容をガイドすることを目的にしている。公開鍵暗号基盤（PKI: Public Key Infrastracture）をモデルとした鍵管理基盤（KMI: Key Management Infrastracture）の概念を示しており、特に、暗号鍵の確立と管理の役割を担う米国連邦政府システムの所有者と管理者向けに書かれている。実際、ここでの暗号鍵管理ポリシーの内容は、電子認証局の暗号鍵管理ポリシーである CP/CPS（Certification Policies and Certification Practice Statements）に似たものである。

2005 年に Part 1 と同時に発行されて以降、改訂されていなかったが、2019 年 5 月に Revision 1 が公開された。

Part 3 は、以下のアプリケーションに対して、セキュリティおよび適合性の問題、調達ガイダンス、システムの設置者／管理者／ユーザごとの推奨事項が述べられている。

[アプリケーション]

PKI、IPsec、TLS、S/MIME、ケルベロス、OTAR 鍵管理メッセージ(KMM)、DNSSEC、暗号化ファイルシステム(EFS)

2.6.2 SP800-130

SP800-130 A Framework for Designing Cryptographic Key Management Systems は、CKMS 設計時に考慮すべきトピックスや対処すべき仕様要求を検討する際に、利用ケースに依存しない汎用的に利用可能なフレームワークとして提供するために作成された。望ましい CKMS を構築、調達及び評価するため、統一的な仕様を作成できるように設計時に文書化する必要がある事項を洗い出したものであり、主に CKMS 設計者が CKMS の要求仕様を決定する際のチェックリストとして活用できるように、包括的なフレームワークに沿って仕様書等に記載する文書化要求事項の一覧を列挙している。

なお、SP800-130 では、フレームワークに沿って CKMS の検討項目について文書化することを要求しているだけであって、CKMS におけるいかなる特定のポリシー、手続き、セキュリティ要求事項、システム設計制約を課しているものではない。また、特定のセキュリティ機能を義務づけるわけでもない。どのような要求仕様／設計方法を採用するかは、設計者、又は本フレームワークに基づいた Profile Requirements のような他のドキュメントに委ねられる。

SP800-130 の構成は以下の通り。

1 章（序説） 暗号鍵管理フレームワークの紹介とその背後のモティベーションを記載

2 章（フレームワークの基本） 本フレームワークの基本的な概念をカバーし、フレームワークの概要を記載

3 章（目標） 堅牢な CKMS の目標を定義する。

4 章（セキュリティポリシー） 構成、典型的な内容、並びに情報管理、情報セキュリティ、CKMS セキュリティ及び他の関連するセキュリティポリシーの必要性について説明

5 章（役割及び責任） CKMS をサポートする役割と責任を提示

6 章（暗号鍵及びメタデータ） CKMS の最も重要な要素をカバー：利用可能な鍵タイプを列挙し定義した鍵及びメタデータ、鍵メタデータ、及びアクセスコントロールの考慮、セキュリティ課題及び回復メカニズムを備えた鍵及びメタデータの管理機能。

7 章(相互運用性及び移行） 相互運用性の必要性､及び将来のニーズに適応するための CKMS の機能における容易に移行するための機能についての考察

8 章（セキュリティコントロール） 典型的な CKMS に適用可能なセキュリティコントロールを記載

9 章（テスト及びシステム保証） セキュリティテストと保証について記載

10 章（災害復旧） 一般的な災害復旧、及び CKMS 特有の災害復旧について説明

11 章（セキュリティアセスメント） CKMS のセキュリティアセスメントについて説明

12 章（技術的課題） 暗号アルゴリズム、鍵確立プロトコル、CKMS デバイス、及び量子コンピュータに関する新しい攻撃によってもたらされる技術的課題について簡潔に説明

2.6.3 SP800-152

SP800-152 A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)は、SP800-130 を基に作られた米国連邦政府向けの暗号鍵管理プロファイルである。連邦政府機関や請負業者が全ての暗号鍵や関連付けられたメタデータを管理するために利用する米国連邦 CKMS に対する

要求事項を明示したものであり、CKMS 設計者だけでなく、米国連邦 CKMS の調達者や管理者も想定読者の対象である。

表 2-2 に SP800-130 と SP800-152 の対応関係例を示す。SP800-152 では、米国政府システムとして使うことを前提として、SP800-130 の各要求事項に対してどのように対処するかの米国連邦政府の要件が 3 つのレベルで規定されている。

“Profile Requirements (PR)”：必須要件 (shall または shall not)
“Profile Augmentations (PA)”：推奨要件 (should または should not)
“Profile Features (PF)”：オプション要件 (could)

表 2-2　SP800-130 と SP800-152 の対応関係例

SP800-130	**SP800-152**
4. Security Policies	**4 Security Policies**
4.8 Laws, Rules, and Regulations **FR [Frame Requirements]:4.14** The CKMS design **shall specify** the countries and/or regions of countries where it is intended for use and **any legal restrictions** that the CKMS is intended to enforce. （必須：あらゆる法的制限を明記）	4.10 Laws, Rules, and Regulations **PR [Profile Requirements]:4.17** A Federal CKMS **shall comply with U.S. Federal laws, rules and regulations**. （必須：米国の連邦法、規則、及び規制に準拠） **PA [Profile Augmentations]:4.8** A Federal CKMS **should comply with the rules and regulations of the countries** in which it is operating and providing key-management services. （推奨：利用国での規則や規制に準拠） **PF [Profile Features]:4.2** A Federal CKMS **could be configurable to comply with the policies** of one or more national and international organizations. （オプション：複数のポリシーに準拠するように設定変更が可能）

3 本設計指針の活用方法

本設計指針の目的は、SP800-130 に記載されている以下の要件、

> **FR:2.3 適合 CKMS 設計は、本フレームワークの要求事項で要求されているように、設計選択について記載し、文書を提供しなければならない。**

を実現することにある。

そのため、本章以降は、主に CKMS の Profile Requirements や System Requirements を作成する設計者を対象に、具体的なプロファイルや仕様書等を作成する際に本設計指針を活用することを想定している。加えて、作成されたプロファイルや仕様書等が漏れなく適切な検討を踏まえて作成されたものであるかどうかをシステム管理責任者や調達責任者が確認・比較できるようにすること期待している。

2.3 節に記載した通り、SP800-130 に記載されている Framework Requirements を『暗号鍵管理における目的（取り扱い項目）に応じた対象範囲』に分類・グループ化したものを 4 章以降の各節にまとめている。各節の標題が検討すべきトピックスとしての取り扱い項目を表している。各項目について、SP800-130 の該当する部分の概要を記載しており、図 3-1 の形式で Framework Requirements を取りまとめている。

検討番号	FR番号	Framework Requirementsの内容	SP800-130 参照章
#x.01	FR1.1	適合CKMS設計は、本フレームワークの全ての必須（“shall”）要求事項を満たさなければならない。	4.3節
#x.02	FR2.3	適合CKMS設計は、本フレームワークの要求事項で要求されているように、設計選択について記載し、文書を提供しなければならない。	4.3節

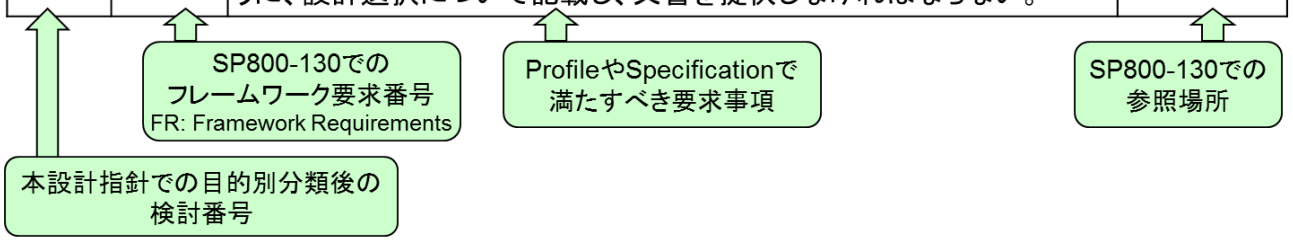

図 3-1 Framework Requirements の表示例

- 「検討番号」は、本設計指針での 6 つの目的別分類を行った後の検討項目にナンバリングした検討番号である。本設計指針の中では本番号をキーインデックスとする。例えば、「#A.01」は「暗号鍵管理システムの設計原理と運用ポリシー」の「1 番目」の検討番号を意味する。
- 「FR 番号」は、SP800-130 のなかで利用されているフレームワーク要求番号であり、SP800-130 との対応を確認する際に利用する番号である。

- 「Framework Requiremtns の内容」は、当該 Framework Requirements における SP800-130 の日本語訳を記載している。詳細な内容の確認が必要な場合には、SP800-130 の該当箇所（「SP800-130 参照章」の該当節）を参照されたい。
- 「SP800-130 参照章」は、SP800-130 で当該 Framework Requirements が記載されている節番号を示している。

IPA から SP800-130 の日本語訳が公開されているので、本設計指針と併せて活用されたい。なお、この日本語訳はできるだけ忠実に翻訳するよう努めているが完全性や正確性を保証するものではないので、必要があれば、適宜 SP800-130 原本を確認するように留意されたい。

● 前提

本設計指針の利用にあたって、情報管理ポリシー及び情報セキュリティポリシーが別途作成済みであることを前提とする。もしそれらのポリシーが作成されていないのであれば、CKMS セキュリティポリシーの作成や CKMS 設計に入る前に、情報管理ポリシー及び情報セキュリティポリシーを策定することが先決である。

● 検討範囲の目安

CKMS 設計にあたって、2.3 節の目的別分類を参考に要求事項の検討範囲を決める必要がある。以下に検討範囲の目安を示す。

【A】暗号鍵管理システムの設計原理と運用ポリシー
【B】暗号アルゴリズム運用のための暗号鍵管理オペレーション対策
【C】暗号アルゴリズムの選択
【D】暗号アルゴリズム運用に必要な鍵情報の管理
【E】暗号鍵管理デバイスのセキュリティ対策
【F】暗号鍵管理システムのオペレーション対策

表 3-1　検討範囲の目安

	CKMS の範囲	A	B	C	D	E	F
I	一般的な暗号鍵管理システムの利用形態であるが、個々のデバイスやシステム全体の運用・管理までは視野に入れない CKMS 設計（狭義の意味での暗号鍵管理を実現するケース）	○	○	○	○	－	－
II	個々のデバイスにおける暗号鍵の実際の運用・管理までを含めた CKMS 設計	○	○	○	○	○	－
III	システム全体での運用・管理を含めた CKMS 設計	○	○	○	○	○	○

凡例：　○：原則対象となる検討項目の範囲（対象外になるかどうかは項目ごとに個別に判断）
　　－：対象外となる可能性が高い検討項目の範囲

- **明記レベル**

Profile Requirements や System Requirements の作成にあたっては、CKMS の要求事項としてどの程度の強制力を持たせるのかを混同しないように明記しなければならない。

強制力が強いものが「必須」及び「禁止」で、この要求条件を満たしていない CKMS は仕様不適合となる。次いで「要望」で、できる限りこの事項を満たすように求めているものの、満たしていないからと言って CKMS が仕様不適合とは言えないものである。ただし、この事項を満たしている CKMS と満たしていない CKMS とでは、前者を有利に取り扱うべきである。

「オプション」は、満たしても満たさなくてもよい事項であり、その事項を満たすかどうかは CKMS の実装者・開発者に委ねられる。

- 【必須】：必ず満たさなければならない要求事項を記述する際に利用する。「○○しなければならない。」
- 【要望】：できるだけ満たすように求める事項を記述する際に利用する。「○○すべきである。」
- 【オプション】：満たすようにしてもよい事項を記述する際に利用する。「○○してもよい。」「○○することがあり得る。」
- 【禁止】：絶対にしてはならない要求事項を記述する際に利用する。「○○してはならない。」

- **CKMS 設計者にとっての具体的な活用方法：**

a) 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。この目的及びそれに続く概要に照らし合わせて、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対象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 b）に進み、対象範囲外と判断すれば c）に進む。

例）4.1 節 CKMS セキュリティポリシーでは、「①CKMS セキュリティポリシーは、CKMS がサポートしなければならない鍵情報の保護のためのルールを規定する」ことを目的とした Framework Requirements が 2 つ（A.01、A.02）ある。CKMS では鍵情報の保護は必須であることから、これらの Framework Requirements は「対象範囲」と判断する。

全てのトピックスについて判断を実施することを原則とする。
ただし、CKMS 設計者とシステム管理責任者や調達責任者等との合意に基づいて今回設計する CKMS の対象範囲を先に明確化しておくことなどにより、検討不要な要求事項の範囲であることが明らかなトピックスについては、CKMS 仕様書等にその合意内容を「前提条件」として記載しておくことを条件に、判断対象から除外してよい。その際、判断対象から除外したことが後でわかるように、CKMS 仕様書やチェックリスト等に「前提条件に基づき、検討不要なトピックス」等の備考を記しておくべきである。

b) 対象範囲の Framework Requirements ごとに、どのような要求仕様／設計方法を採用するか、あるいはどのような対応をとるかを決定し、その内容を要求事項として Profile Requirements や System Requirements の文書に記載する。なお、一つの Framework Requirements に対して要求事項は一つとは限らず、複数となる場合もある。

例）Framework Requirements で「○○のための手段を明記しなければならない」とあれば、どのような対策手段を使うのか、その対抗手段をどこにどのように実装するのか、誰がその対抗手段を運用するのか、などを記載する。

c) 対象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 Requirements は「対象外」と除外する。

例）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を行わないシステムであるのであれば、「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を行わないため」との理由を明記したうえで、4.3.3 節の Framework Requirements（A.22～A.26）を対象外とする。

- **システム管理責任者や調達責任者等にとっての具体的な活用方法：**

d) Framework Requirements ごとに、Profile Requirements や System Requirements の文書に記載された要求事項の内容が適切であるかどうかを確認する。また、対象外と判断された項目については、対象外と判断した理由が適切であるかどうかを確認する。

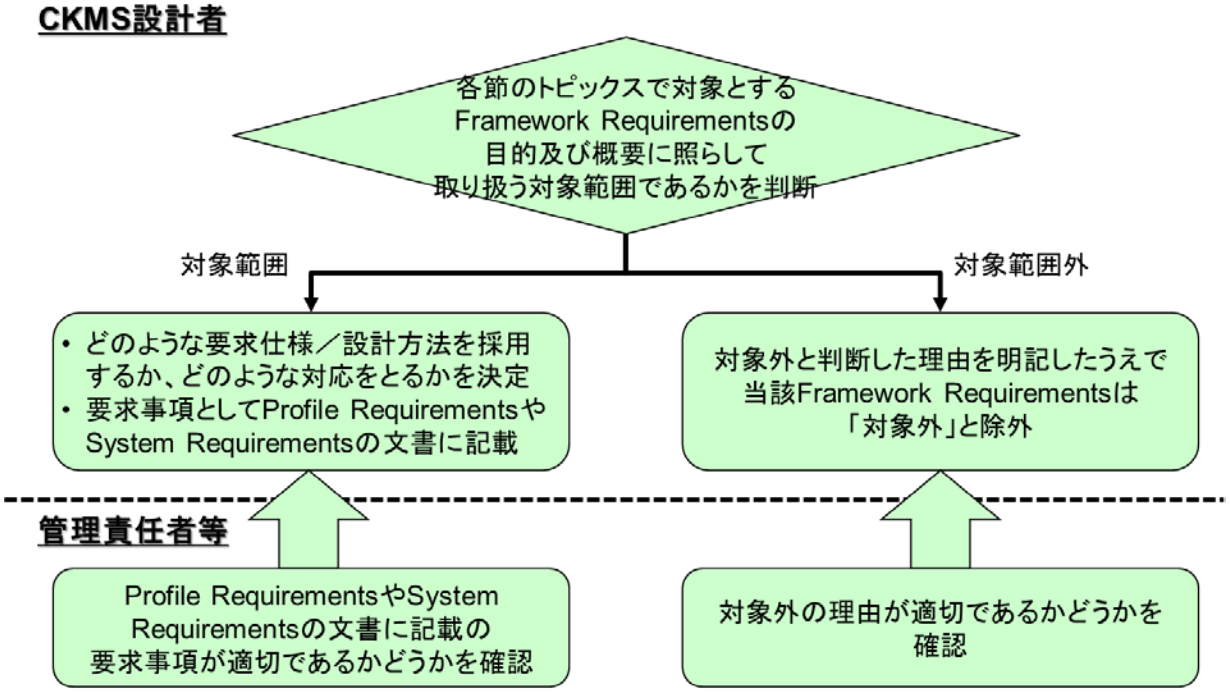

図 3-2　本設計指針の活用方法

4 暗号鍵管理システム（CKMS）の設計原理と運用ポリシー

4.1 CKMS セキュリティポリシー

本節は、SP800-130 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。

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、検討番号 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。
- 2.4 節に示すように、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。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
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

【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

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。

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、検討番号 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

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。

検討番号 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検討項目である。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

4.2 情報管理ポリシー等からの要求事項

本節は、SP800-130 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事項があり得る。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。

「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。

検討番号 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

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が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が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

検討番号 A.07～A.13 は、CKMS の設計にあたって、そのような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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

4.3 ドメインのセキュリティポリシー

本節は、SP800-130 の 4.9 節に記載されている事項について解説したものであり、セキュリティドメインにおける取り扱いについて取り扱う。

4.3.1 セキュリティドメイン

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。

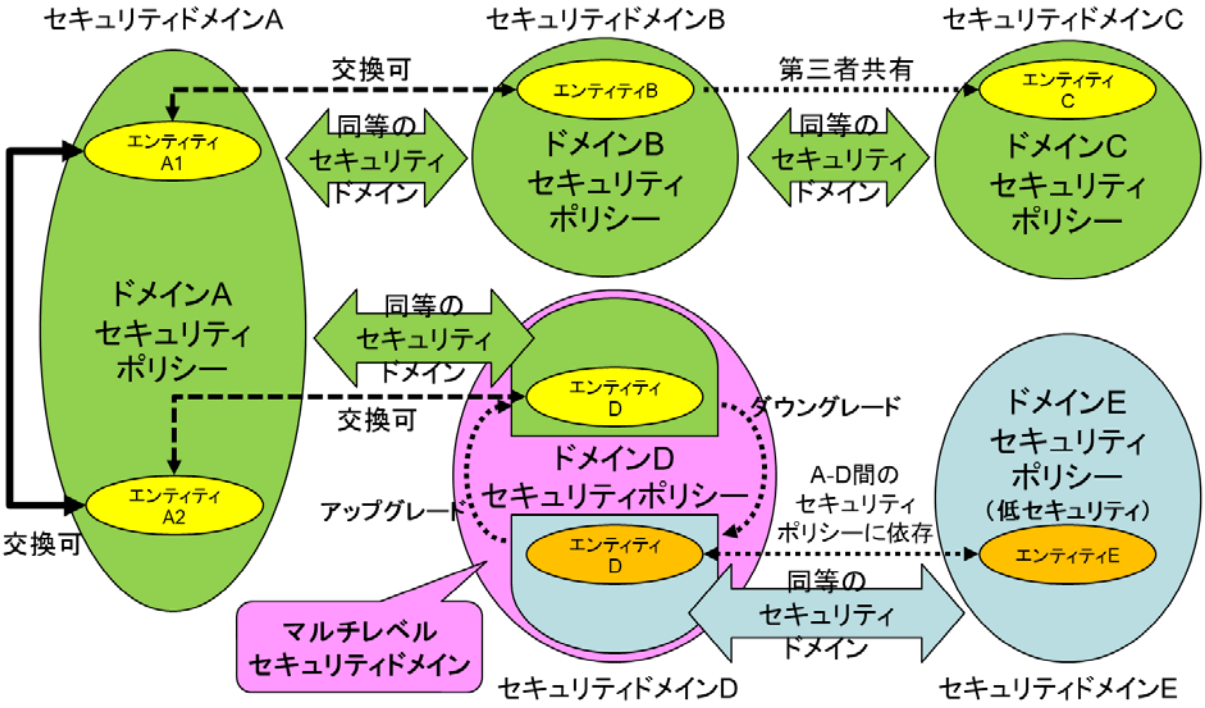

図 4-1　セキュリティドメインとセキュリティポリシーの関係

4.3.2　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。

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。

検討番号 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検討項目である。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
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）とディスティネ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。	4.9.2 節
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

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。

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、検討番号 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に従った設定が可能であるか、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検討項目である。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

4.3.3 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

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。

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。

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、検討番号 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検討項目である。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

4.4 CKMS における役割と責任

本節は、SP800-130 の 5 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 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 を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。

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。

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（System Authority）
b) システム管理者
c) 暗号責任者（Cryptographic Officer）
d) ドメインオーソリティ（Domain Authority）
e) 鍵管理者（Key Custodian）
f) 鍵所有者
g) CKMS ユーザ
h) 監査責任者（Audit Administrator）
i) 登録エージェント
j) 鍵復元エージェント（Key-Recovery Agent）
k) CKMS オペレータ（CKMS Operator）

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、検討番号 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が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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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（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

4.5 CKMS の構築環境及び実現目標

本節は、SP800-130 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。

4.5.1 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。

検討項目 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）。

	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

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、検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

4.5.2 実現目標

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、以下の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。

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。

検討項目 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

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

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。

検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

検討項目 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）

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

CKMS の設計にあたって、検討項目 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検討項目である。

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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

4.5.3　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。

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、検討項目 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。したがって、システム間の相互運用がなければ検討対象外である。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

4.5.4 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。

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、検討項目 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。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
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

4.5.5 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。

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、検討項目 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。したがって、CKMS のセキュリティ機能部分に商用既製品を採用しない場合には検討対象外である。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
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

4.6　標準／規制に対する適合性

本節は、SP800-130 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。

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、検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

4.7　将来的な移行対策の必要性

本節は、SP800-130 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。

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。

検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

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。検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

- 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

- 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

- 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。
  例えば、大きなキュービットの量子コンピュータが構築されれば、既存の公開鍵暗号アルゴリズムのセキュリティが脅かされるかもしれず、これらのアルゴリズムに暗号鍵の確立を依存する CKMS に対して重大な影響を与える可能性がある。
  一方、量子コンピュータに耐性がある公開鍵暗号アルゴリズム（耐量子計算機暗号）についての研究や標準化が現在進行中であるが、現時点で広く受け入れられている解はまだ見出されていない。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

5 暗号アルゴリズム運用のための暗号鍵管理オペレーション対策

5.1 CKMS 設計

本節は、SP800-130 の 2.5 節に記載されている事項について解説したものである。

① 暗号鍵を提供するために CKMS をどのように構築するかの概要を明確化しなければならない。

検討項目 B.01 は、CKMS の設計にあたって、暗号鍵を提供するために CKMS をどのように構築するかの概要を明確化することを要求したものである。ここでは、機微なデータを保護するための暗号鍵に対する設計方針や実現目標（要求事項）、詳細を決める文書へのインデックス等を簡潔な概要で明記することが求められる。例えば、利用する鍵タイプ（7.1 節表 7-1 参照）、暗号鍵の生成場所及び生成方法、保管中及び配送中の保護方法、暗号鍵が配送されるエンティティのタイプなどが対象となる。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.01	FR2.4	CKMS 設計は、以下を含む CKMS システムの高レベルの概要を明記しなければならない： a) 利用するそれぞれの鍵タイプ b) 鍵が生成される場所と手段 c) それぞれの鍵タイプとの信頼関係で使用されるメタデータ要素（7.1 節表 7-2 参照） d) 鍵情報（暗号鍵やメタデータ）が存在しているそれぞれのエンティティのストレージにおける、鍵情報（暗号鍵やメタデータ）の保護方法 e) 配送時の鍵情報（暗号鍵やメタデータ）の保護方法 f) 鍵情報（暗号鍵やメタデータ）が配送され得る先となるエンティティの種類（例えば、ユーザ、ユーザデバイス、ネットワークデバイス）	2.5 節

5.2　暗号鍵のライフサイクル

本節は、SP800-130 の 6.3 節に記載されている事項について解説したものである。

① 暗号鍵のライフサイクル全体にわたって取り得る鍵状態及び遷移条件を定義しなければならない。

暗号鍵のライフサイクルの一般形は、SP 800-57 part1 の 7 節「鍵状態と遷移（Key States and Transitions）」に基づく（図 5-1 参照）。これをベースに、CKMS とそのアプリケーションに適切な鍵状態と遷移条件を選択し定義する。なお、SP800-57 と SP800-130 とでは鍵状態の種類について記載内容に一部違いがあるが、SP800-57 のほうが分かりやすいので、本設計指針では SP800-57 に記載の鍵状態を基本とすることを推奨する。

検討項目 B.02 及び B.03 は、CKMS の設計にあたって、暗号鍵のライフサイクル全体を対象に定義した全ての鍵状態及び遷移条件を明確化することを要求したものである。ここで定義した鍵状態及び遷移条件を管理・実行するために必要な全ての管理機能を次節以降で規定することが求められる。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.02	FR6.15	CKMS 設計は、CKMS の鍵が取り得る全ての状態を明記しなければならない。	6.3 節
B.03	FR6.16	CKMS 設計は、全ての CKMS 鍵状態間の遷移、及び遷移を起こすことに関係するデータ（入力と出力）を明記しなければならない。	6.3 節

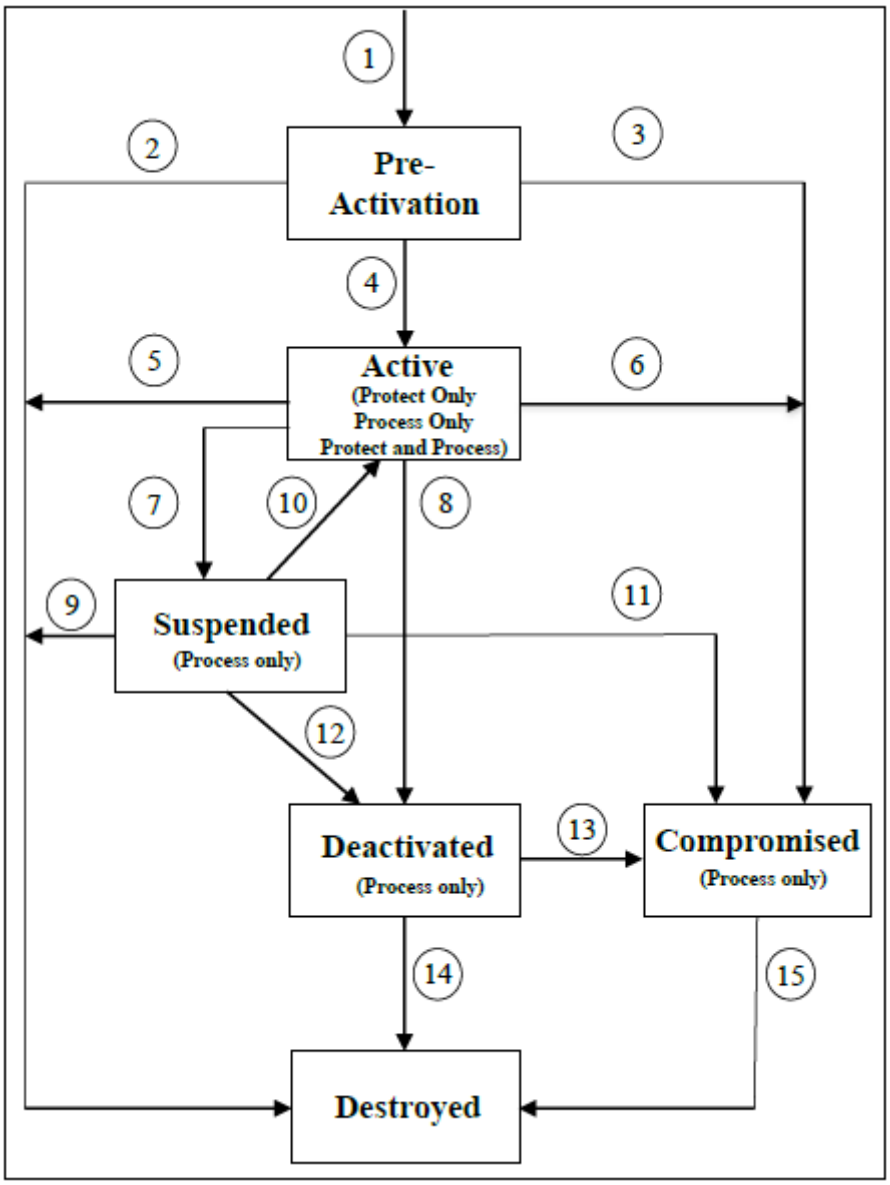

図 5-1　鍵状態及び遷移の例（SP800-57 Part 1 revision 5 より引用）

【鍵状態】

- ✧ 活性化前（Pre-Activation）
- ✧ 活性化（Active）
- ✧ 非活性化（Deactivated）
- ✧ 一時停止（Suspended）
- ✧ 危殆化（Compromised）
- ✧ 破壊（Destroyed）

【遷移】

- ✧ 正常な遷移：①→④→⑧→⑭
- ✧ それ以外はすべて何らかの異常による遷移

5.3　暗号鍵のライフサイクル管理機能

本節は、SP800-130 の 6.4 節、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、SP800-130 の 6.4 節には 28 の小節があるが、本指針では内容に依存してそれらを 5.2 節、5.3 節、5.4 節、8.1 節に分離して記載してある。また、SP800-130 の 6.8 節にも 8 つの小節があるが、本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。

① 鍵情報に対する管理のために実行される機能の全体像を定めなければならない。

検討項目 B.04 は、CKMS の設計にあたって、5.2 節で定義した暗号鍵のライフサイクルにおける鍵状態及び遷移条件を管理・実行するために必要な全ての管理機能を明確化し、実装することを要求したものである。対象となる管理機能は本節の②以降である。

検討項目 B.05 は、管理機能に共通して入出力されるデータについて、完全性や機密性、ソース認証が必要となるものがあれば、それらを明確化することを要求したものである。これには、エンティティの認証及び認可が含まれることもある。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.04	FR6.17	CKMS 設計は、実装されサポートされる鍵情報（暗号鍵及びメタデータ）の管理機能を明記しなければならない。	6.4 節
B.05	FR6.18	CKMS 設計は、CKMS に実装されるそれぞれの鍵情報（暗号鍵及びメタデータ）の管理機能のパラメタに適用される完全性、機密性、及びソース認証（source-authentication）の処理（service）を特定しなければならない。	6.4 節

② 鍵活性化機能への要求事項を決めなければならない。

暗号鍵の活性化前状態から活性化状態への遷移（④）を提供する機能である。

検討項目 B.06 及び B.07 は、CKMS の設計にあたって、鍵活性化の手順や遷移条件、通知方法等、鍵活性化機能への要求事項を明確化することを求めたものである。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.06	FR6.22	CKMS 設計は、それぞれの鍵タイプがどのように活性化されるか、及び鍵が活性化される状況を明記しなければならない。	6.4.3 節

B.07	FR6.23	それぞれの鍵タイプに対して、CKMS 設計は、鍵活性化の通知の要求事項を明記しなければならない。それには、どの当事者に通知されるか、どのように通知されるか、どのセキュリティ処理（services）が通知に適用されるか、及び通知の期間が含まれる。	6.4.3 節

③ 暗号機能の実行場所を決めなければならない。

データへの暗号学的保護を実際に提供する機能であり、署名生成、署名検証、暗号化、復号、鍵ラッピング、鍵アンラッピング、MAC 生成、及び MAC 検証を含む。

検討項目 B.08 は、CKMS の設計にあたって、暗号機能がどこで実行されるのか明確化することを要求したものである。一般には、暗号モジュールの内部で実行されることが望ましい。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.08	FR6.69	CKMS 設計は、サポートされている全ての暗号機能、及びそれらの暗号機能が CKMS のどこで実行されるか（例えば、CA、ホスト、又はエンドユーザシステム）を明記しなければならない。	6.4.27 節

④ 鍵非活性化機能への要求事項を決めなければならない。

暗号鍵の非活性化状態への遷移（⑧、⑫）を提供する機能である。活性化と非活性化の間の時間は暗号鍵有効期間と見なされ、通常、この時間は保護するデータの機微度と CKMS への脅威に基づいて決められる。CKMS セキュリティポリシーには当該ポリシーがカバーするあらゆる鍵タイプについて最大許容暗号鍵有効期間を記載すべきであり、その期間を超えた暗号鍵有効期間を設定してはならない。

検討項目 B.09～B.12 は、CKMS の設計にあたって、鍵非活性化の手順や遷移条件、変更方法、通知方法等、鍵非活性化機能への要求事項を明確化することを求めたものである。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.09	FR6.24	CKMS 設計は、各鍵タイプに対して、鍵の非活性化がどのように決定されるのか（例えば、暗号鍵有効期間（cryptoperiod）による、使用回数による、又はデータ量による）を明記しなければならない。	6.4.4 節

B.10	FR6.25	CKMS 設計は、それぞれの鍵タイプがどのように非活性化されるか（例えば、非活性化日時、使用回数、又は保護されたデータの量に基づいて、手動で行われるのか自動で行われるのか）を明記しなければならない。	6.4.4 節
B.11	FR6.26	CKMS 設計は、それぞれの鍵タイプの非活性化日時がどのように変更できるかを明記しなければならない。	6.4.4 節
B.12	FR6.27	それぞれの鍵タイプに対して、CKMS 設計は、鍵タイプの非活性化の事前通知の要求事項を明記しなければならない。それには、CKMS がサポートするどの役割に通知されるか、どのように通知されるか、どのセキュリティ処理（services）が通知に適用されるか、及び通知の期間が含まれる。	6.4.4 節

⑤ 鍵失効機能への要求事項を決めなければならない。

暗号鍵有効期間より前に当該暗号鍵の使用を終了させる必要が生じた場合に行われ、暗号鍵の危殆化状態への遷移（③、⑥、⑪、⑬）を提供する機能である。鍵非活性化機能との違いは、「危殆化による安全性低下」起因か、「（安全性低下とは関係なしに）暗号鍵有効期間満了」起因かによる。

この機能が実行されると、過去に保護された情報の処理のための使用に対しても完全なセキュリティは保証されないので、当該暗号鍵を速やかに置き換える能力とその鍵を使用する当事者に危殆化／失効を通知する能力を備えているべきである。危殆化／失効の通知方法としては、危殆化鍵リスト、証明書失効リスト（CRLs）、ホワイトリスト、クエリホワイトリスト、OCSP（Online Certificate Status Protocol）がある。

なお、暗号鍵は多くの理由によって失効させられるので、どのような理由によるものかも保持すべきである。

CKMS の設計にあたって、検討項目 B.13 は、鍵失効の遷移条件及び通知方法といった鍵失効機能への要求事項を明確化することを求めたものである。B.14 は、実際に利用する具体的な鍵失効メカニズム及び通知メカニズムを明確化することを要求したものである。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.13	FR6.28	CKMS 設計は、いつ、どのように、どのような状況で失効が実行され、失効情報を依拠する当事者が利用可能になるかを明記しなければならない。	6.4.5 節

B.14	FR6.108	CKMS 設計は、使用される又は使用できる鍵失効メカニズム及び関連付けられた依拠するエンティティへの通知メカニズムを明記しなければならない。	6.8.3 節

⑥ 暗号鍵の一時停止機能及び再活性化機能への要求事項を決めなければならない。

暗号鍵の一時停止状態への遷移（⑦）を提供する一時停止機能、及び活性化状態への遷移（⑩）を再度提供する再活性化機能のことである。鍵失効機能との違いは「可逆」であり「再活性化」が可能であることであり、これらの機能は必ずセットで用いられる。

一般に、「誤使用」や「誤配置」、「危殆化の疑い」のレベルでの利用が想定されているが、必ずしも一時停止状態を定義する必要はなく、直接失効状態に移行しても構わない。

検討項目 B.15 及び B.16 は、CKMS の設計にあたって、暗号鍵の一時停止の遷移条件及び通知方法といった一時停止機能への要求事項を明確化することを求めたものである。B.17 は、一時停止された暗号鍵が利用されないように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。B.18 及び B.19 は、暗号鍵を再活性化するための遷移条件及び通知方法といった再活性化機能への要求事項を明確化することを求めたものである。

なお、鍵状態において一時停止状態を定義しない場合には、これらの検討項目は対象外である。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.15	FR6.29	CKMS 設計は、どのように、どのような状況で鍵が一時停止されるかを明記しなければならない。	6.4.6 節
B.16	FR6.30	CKMS 設計は、どのように一時停止情報を依拠又は通信する当事者が利用可能になるかを明記しなければならない。	6.4.6 節
B.17	FR6.32	CKMS 設計は、どのように一時停止された鍵によるセキュリティ処理（services）の実行を防止するのかを明記しなければならない。	6.4.6 節
B.18	FR6.31	CKMS 設計は、どのように、どのような状況で一時停止された鍵が再活性化されるかを明記しなければならない。	6.4.6 節
B.19	FR6.33	CKMS 設計は、どのように再活性化情報を依拠又は通信する当事者が利用可能になるのかを明記しなければならない。	6.4.6 節

⑦ 鍵情報の破壊機能への要求事項を決めなければならない。

暗号鍵の破壊状態への遷移（②、⑤、⑨、⑭、⑮）を提供する機能である。暗号鍵及びそのメタデータの一部は使用されることがなくなったときに復元できないように破壊されるべきであり、バックアップストレージメディアに保管されている場合にはメディア内の暗号鍵を、コピーが存在する場合には当該コピーも含めて破壊する手段を用意すべきである。

検討項目 B.20 は、CKMS の設計にあたって、鍵情報を破壊するための条件及び具体的な破壊方法、並びに当該鍵情報がどこに存在するかを含めて明確化することを要求したものである。B.21 は、鍵情報が破壊されたことの通知方法といった破壊機能への要求事項を明確化することを求めたものである。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.20	FR6.38	CKMS 設計は、どのように、どのような条件で鍵が意図して破壊されるか、及び破壊がコンポーネントへの局所的（local）なものであるか CKMS 全体への共通的（universal）なものであるかを明記しなければならない。	6.4.9 節
B.21	FR6.39	それぞれの鍵タイプに対して、CKMS 設計は、鍵破壊の事前通知の要求事項を明記しなければならない。それには、どの当事者に通知されるか、どのように通知されるか、どのセキュリティ処理（services）が通知に適用されるか、及び通知の時期が含まれる。	6.4.9 節

⑧ 鍵生成機能への要求事項を決めなければならない。

CKMS の設計にあたって、検討項目 B.22 は暗号鍵を生成する手段について、B.23 は暗号鍵を生成する際に利用する乱数生成器について明確化することを要求したものである。一般に、鍵生成手段は暗号鍵と対になる暗号アルゴリズムの仕様に依存し、暗号目的として設計された乱数生成器の使用を要求する。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.22	FR6.19	CKMS 設計は、それぞれの鍵タイプに対して、CKMS で使用される鍵生成手段を明記しなければならない。	6.4.1 節
B.23	FR6.20	CKMS 設計は、対称鍵及びプライベート鍵を生成するのに使用される元となる乱数生成器を明記しなければならない。	6.4.1 節

⑨ 鍵導出機能／鍵更新機能への要求事項を決めなければならない。

暗号鍵の生成では、鍵生成機能を利用する代わりに、鍵導出機能や鍵更新機能を利用することがある。

鍵導出機能では、一部が秘密であるような独立した他の情報（他の暗号鍵、共有秘密やパスワードなど）から不可逆な形で暗号鍵が導出されるプロセスを実行する。例えば、鍵確立プロトコルでは互いの共有秘密から共有鍵を導出する。

鍵更新機能では、「元鍵」から「別鍵」を計算で導出し、導出した「別鍵」で「元鍵」を置き換えるプロセスを実行する。なお、別鍵を導出する際に他の秘密データを使用しない場合には、元鍵と更新方法を知っている攻撃者が将来にわたるあらゆる時期の更新した別鍵を知りうるというセキュリティリスクにさらされる。

検討項目 B.24 及び B.25 は、CKMS の設計にあたって、鍵導出機能／鍵更新機能が利用される条件や鍵導出方法、通知方法等といった鍵導出機能／鍵更新機能への要求事項を明確化することを求めたものである。

なお、これらの機能は採用必須の機能ではなく、CKMS の設計で採用しなければ検討対象外である。逆に、採用してはならないという要求事項の場合もあり得る。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
B.24	FR6.36	CKMS 設計は、鍵を導出又は更新するために使用される全てのプロセス、及び鍵が導出又は更新される状況を明記しなければならない。	6.4.8 節
B.25	FR6.37	それぞれの鍵タイプに対して、CKMS 設計は、鍵の導出又は更新の事前通知の要求事項を明記しなければならない。それには、どの当事者に通知されるか、どのように通知されるか、どのセキュリティ処理（services）が通知に適用されるか、及び通知の期間が含まれる。	6.4.8 節

⑩ 対称鍵の検証機能への要求事項を決めなければならない。

対称鍵及びそのメタデータに対するテストを実行する機能である。

検討項目 B.26 は、CKMS の設計にあたって、対称鍵の検証機能が利用される条件や検証方法等といった対称鍵の検証機能への要求事項を明確化することを求めたものである。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
B.26	FR6.66	CKMS 設計は、どのように、どこで、どのような状況で、対称鍵やそのメタデータが検証されるかを明記しなければならない。	6.4.24 節

⑪ 公開鍵の検証機能への要求事項を決めなければならない。

公開鍵についてある種の正当性チェックを実行して公開鍵が数学的に正しいことを保証し、公開ドメインパラメタについてもドメインパラメタが数学的に正しいことの保証を提供する機能である。また、トラストアンカーから始まる公開鍵証明書のチェーン（証明書パス）の中にある全ての署名を検証することによって当該公開鍵の信頼を確立する。

CKMS の設計にあたって、検討項目 B.27～B.29 は、公開鍵の検証機能が利用される条件や検証方法等といった公開鍵の検証機能への要求事項を明確化することを求めたものである。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.27	FR6.63	CKMS 設計は、どのように、どこで、どのような状況で、公開鍵ドメインパラメタが検証されるかを明記しなければならない。	6.4.21 節
B.28	FR6.64	CKMS 設計は、どのように、どこで、どのような状況で、公開鍵が検証されるかを明記しなければならない。	6.4.22 節
B.29	FR6.65	CKMS 設計は、どのように、どこで、どのような状況で公開鍵証明書パスが検証されるかを明記しなければならない。	6.4.23 節

⑫ トラストアンカー管理機能への要求事項を決めなければならない。

トラストアンカーなしでは信頼されない公開鍵に対して信頼を確立するために使用されるトラストアンカーを保管・管理する機能である。トラストアンカーは公開鍵の信頼性の起点となるため、その完全性は CKMS のセキュリティにとって極めて重要である。

CKMS の設計にあたって、検討項目 B.30 はトラストアンカー管理機能についてどのようなものを受け入れるのかといった要求事項を、B.31 及び B.32 はトラストアンカーを完全かつセキュアに配送・保管・追加・削除等といったメンテナンスを行うためのトラストアンカー管理機能への要求事項を明確化することを求めたものである。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
B.30	FR6.70	CKMS 設計は、サポートされている全てのトラストアンカー管理機能を明記しなければならない（[RFC6024[2]] を参照）。	6.4.28 節
B.31	FR6.71	CKMS 設計は、依拠するエンティティがトラストアンカーについてのソース認証（source authentication）及び完全性検証を実行できるように、どのようにそれらのトラストアンカーがセキュアに配付されるかを明記しなければならない。	6.4.28 節
B.32	FR6.72	CKMS 設計は、依拠するエンティティのシステムのトラストアンカーストアに対して、認可された追加、変更、削除のみが行えることを保証するために、どのように依拠するエンティティのシステムでトラストアンカーが管理されるかを明記しなければならない。	6.4.28 節

⑬ 公開鍵の有効期間延長機能への要求事項を決めなければならない。

新しい有効期限を設定した「同じ公開鍵」を含む新しい公開鍵証明書を発行することで、以前の有効期間を超えて既存の公開鍵に対する新しい有効期間を確立するための機能である。なお、延長後の有効期間の合計が CKMS セキュリティポリシー等で定める公開鍵の最大許容暗号鍵有効期間を超える場合には、当該公開鍵の延長を行ってはならない。

CKMS の設計にあたって、検討項目 B.33 及び B.34 は、公開鍵の有効期間延長機能が利用される条件や事前通知方法等といった公開鍵の有効期間延長機能への要求事項を明確化することを求めたものである。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
B.33	FR6.34	CKMS 設計は、どのように、どのような条件で公開鍵の有効期間が延長できるかを明記しなければならない。	6.4.7 節

[2] トラストアンカー管理要件、https://www.ietf.org/rfc/rfc6024.txt
RFC 6024 では、標準的なトラストアンカー管理メカニズムの欠如が招くいくつかの問題について記述し、これらの問題に対処するために設計されたデータフォーマットとプッシュベースのプロトコルの要件を定義する。

B.34	FR6.35	それぞれの鍵タイプに対して、CKMS 設計は、鍵タイプの有効期間延長の事前通知の要求事項を明記しなければならない。それには、どの当事者に通知されるか、どのように通知されるか、どのセキュリティ処理（services）が通知に適用されるか、及び通知の期間が含まれる。	6.4.7 節

⑭ 所有者登録機能への要求事項を決めなければならない。

セキュリティエンティティ（個人、組織、デバイス、又はプロセス）及びメタデータを伴う暗号鍵の最初の登録を行うための機能である。典型的には、エンティティの対称鍵、公開鍵又はプライベート鍵の初期セットと、エンティティ識別子及びメタデータとも結び付ける登録プロセスが存在する。

検討項目 B.35 は、CKMS の設計にあたって、所有者登録機能への要求事項を明確化することを求めたものである。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.35	FR6.21	CKMS 設計は、鍵と所有者の識別子を結び付けるプロセスを含めて、所有者登録に関わる全てのプロセスを明記しなければならない。	6.4.2 節

⑮ プライベート鍵所持の検証機能への要求事項を決めなければならない。

公開鍵の所有者であると主張する者が対応するプライベート鍵を所持していることの保証を得るために、公開鍵を受領したエンティティによって使用される機能である。

検討項目 B.36 は、CKMS の設計にあたって、プライベート鍵所持の検証機能が利用される条件や検証方法等といったプライベート鍵所持の検証機能への要求事項を明確化することを求めたものである。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.36	FR6.68	CKMS 設計は、どのように、どこで、どのような状況で、プライベート鍵とそのメタデータの所持が検証されるかを明記しなければならない。	6.4.26 節

⑯ プライベート鍵の検証機能への要求事項を決めなければならない。

プライベート鍵に対してある種のテストを実行し、鍵ペアの仕様を満たすことの保証を提供するための機能である。この機能は、プライベート鍵の所有者又はプライベート鍵の所有者の代理として振舞う信頼される第三者のみが実行できる。

検討項目 B.37 は、CKMS の設計にあたって、プライベート鍵の検証機能が利用される条件や検証方法等といったプライベート鍵の検証機能への要求事項を明確化することを求めたものである。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.37	FR6.67	CKMS 設計は、どのように、どこで、どのような状況で、プライベート鍵又は鍵ペア、あるいはそのメタデータが検証されるかを明記しなければならない。	6.4.25 節

⑰ 暗号鍵とメタデータの関連付け機能への要求事項を決めなければならない。

暗号鍵に関連付けられているメタデータ要素がある場合、それらを関連付けるための機能である。関連付けを提供する保護メカニズムには、暗号学的プロセスを使用する場合と信頼プロセスを使用する場合とがある。直感的には、前者は、暗号鍵とメタデータの組で計算されたデジタル署名など、暗号アルゴリズムによって関連付けが保証される。後者は、信頼されるエンティティからのメタデータの対面手渡しやセキュアなストレージでの保管など、物理的な手段で関連付けが保証される。

なお、暗号鍵とメタデータの関連付けは、当該鍵情報の生成時のほか、配送時、登録時、保管時など、暗号鍵有効期間を通じて完全性を維持する必要がある。

CKMS の設計にあたって、検討項目 B.38 及び B.39 は、関連付け機能が利用される対象や条件、関連付けの方法等といった関連付け機能への要求事項を明確化することを求めたものである。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.38	FR6.40	使用されているそれぞれの鍵タイプに対して、CKMS 設計は、何のメタデータが鍵と関連付けられているか、どのようにメタデータが鍵と関連付けられているか、及びメタデータが鍵と関連付けえられる状況を明記しなければならない。	6.4.10 節

B.39	FR6.41	使用されているそれぞれの鍵タイプに対して、CKMS 設計は、どのように次のセキュリティ処理（services）（保護）が関連付けられたメタデータに適用されるかを明記しなければならない：ソース認証（source authentication）、完全性、及び機密性。	6.4.10 節

⑱ メタデータの変更機能への要求事項を決めなければならない。

認可されたエンティティが、暗号鍵と関連付けられている既存の書き込み可能なメタデータを変更するために使用する機能である。認可されていないエンティティは本機能を利用できない。

検討項目 B.40 は、CKMS の設計にあたって、メタデータの変更機能が利用できる対象や条件、認可されていないエンティティの利用防止策等といったメタデータの変更機能への要求事項を明確化することを求めたものである。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.40	FR6.42	CKMS 設計は、関連付けられたメタデータが変更される状況を明記しなければならない。	6.4.11 節

⑲ メタデータの削除機能への要求事項を決めなければならない。

認可されたエンティティが、暗号鍵に関連付けられたメタデータを削除するために使用する機能である。削除権限が付与されているエンティティ以外は本機能を利用できない。

CKMS の設計にあたって、検討項目 B.41 は、メタデータの削除機能が利用できる対象や条件、認可されていないエンティティの利用防止策等といったメタデータの削除機能への要求事項を明確化することを求めたものである。B.42 は、具体的な削除方法の明確化することを要求したものである。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.41	FR6.43	CKMS 設計は、鍵と関連付けられたメタデータが削除される状況を明記しなければならない。	6.4.12 節
B.42	FR6.44	CKMS 設計は、関連付けられたメタデータを削除するために使われる手法を明記しなければならない。	6.4.12 節

⑳ 暗号鍵のメタデータリスト化機能への要求事項を決めなければならない。

エンティティに認可されている暗号鍵のメタデータのリスト化を当該エンティティが実行するための機能である。本機能は、自分の管理下にあるメタデータに対してのみ実行できる。

検討項目 B.43 は、CKMS の設計にあたって、メタデータリスト化機能が利用できる対象や条件といったメタデータリスト化機能への要求事項を明確化することを求めたものである。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.43	FR6.45	それぞれの鍵タイプに対して、CKMS 設計は、どのメタデータが認可されたエンティティによってリスト化が可能かどうかを明記しなければならない。	6.4.13 節

5.4 鍵情報の保管方法

本節は、SP800-130 の 6.4 節、6.5 節に記載されている事項について解説したものである。なお、SP800-130 の 6.4 節には 28 の小節があるが、本指針では内容に依存してそれらを 5.2 節、5.3 節、5.4 節、8.1 節に分離して記載してある。

① 保管中の鍵情報のセキュリティを確保するための手段を決めなければならない。

鍵情報の保管にあたっては、全ての暗号鍵は完全性保護を、加えて対称鍵及びプライベート鍵は機密性保護も必要とする。

完全性保護の観点からは、鍵情報がストレージに保管されるより前には入力エンティティの認可と入力されるデータの完全性を、利用する前には読み出したデータの完全性を検証すべきである。それらに訂正可能な破損が検出された場合には適切な訂正を行い、訂正不能な破損が検出された場合には当該暗号鍵は使用してはならない。

機密性保護の観点からは、鍵情報は、暗号化を伴わない物理セキュリティによる保護、対称鍵ラッピング鍵による暗号化、又は鍵分割による保護によって保管されるべきである。なお、対称鍵ラッピング鍵による再暗号化の場合、鍵ラッピング鍵の階層のトップレベルでは、確実な保護を行うために物理的に保護されなければならない鍵が存在することも多い。

また、認可されたユーザのみが保管された鍵情報にアクセスできるようにすべきであり、そのためのアクセスコントロールが必要である。

加えて、保管中の鍵情報が何らかの理由により使えなくなり、当該暗号鍵で保護されたデータを喪失する事態を防止するため、必要に応じて、データ復元を提供するのに必要な鍵情報のバックアップ、アーカイブ、及び復元のための手段を定めておいてもよい。

CKMS の設計にあたって、検討項目 B.44 及び B.45 は鍵情報を保管する時点での完全性保護を実現するための要求事項を、B.46～B.49 は保管中の鍵情報の完全性及び機密性の保護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。B.50 は、保管中の鍵情報が破損した際の対策を明確化することを要求したものである。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.44	FR6.73	CKMS 設計は、鍵情報（暗号鍵やメタデータ）をストレージに入れるエンティティの ID 認証及び認可検証に使用される手段を明記しなければならない。	6.5 節
B.45	FR6.74	CKMS 設計は、ストレージに入力する鍵情報（暗号鍵やメタデータ）の完全性検証に使用される手段を明記しなければならない。	6.5 節
B.46	FR6.75	CKMS 設計は、保管された対称鍵、プライベート鍵及びメタデータの機密性保護に使用される手段を明記しなければならない。	6.5 節
B.47	FR6.76	鍵ラッピング鍵（又は鍵ペア）が保管された鍵を保護するために使用される場合、CKMS 設計は、鍵ラッピング鍵（又は鍵ペア）を保護し、その使用を制御するために使用される手段を明記しなければならない。	6.5 節
B.48	FR6.77	CKMS 設計は、保管された鍵情報（暗号鍵及びメタデータ）の完全性保護に使用される手段を明記しなければならない。	6.5 節
B.49	FR6.78	CKMS 設計は、保管された鍵へのアクセスがどのように制御されるかを明記しなければならない。	6.5 節
B.50	FR6.79	CKMS 設計は、全ての保管された鍵を訂正又は復元するために使用される手法を明記しなければならない。	6.5 節

② 運用中の鍵情報の保管場所及び保護方法を決めなければならない。

運用中の鍵情報がどこに存在し、どのような保護状態に置かれているのかを全て明らかにしておく必要がある。特に、鍵情報が暗号モジュールの外部に保管されるときには物理的又は暗号学的に保護されるべきである。これには、外部メディアへの出し入れなども含む。

検討項目 B.51 は、CKMS の設計にあたって、鍵情報の保管場所や保護方法などの要求事項を明確化することを求めたものである。運用中の鍵情報は、B.51 で定めた保管場所以外に置かれないようにしなければならない。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.51	FR6.46	それぞれの鍵タイプに対して、CKMS 設計は、以下のことを明記しなければならない：それぞれの鍵タイプとそのメタデータが保管される状況、鍵とメタデータの保管場所、及び鍵とメタデータの保護方法。	6.4.14 節

③ 鍵情報のバックアップ方法を決めなければならない。

運用中の鍵情報が喪失、改変、又はその他の理由で利用不能状態になったときに当該データを復元できるようにするため、鍵情報を安全な設備・メディアにバックアップをする場合がある。

CKMS の設計にあたって、検討項目 B.52 は、鍵情報のバックアップを行うための条件を明確化することを、B.53 及び B.54 はバックアップされる鍵情報のセキュリティ、特に機密性保護を確保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。

なお、鍵情報のバックアップを実施しない場合には、検討対象外である。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.52	FR6.47	CKMS 設計は、どのように、どこで、どのような状況において鍵及びそのメタデータがバックアップされるかを明記しなければならない。	6.4.15 節
B.53	FR6.48	CKMS 設計は、バックアップされた鍵情報（暗号鍵及びメタデータ）の保護のためのセキュリティポリシーを明記しなければならない。	6.4.15 節
B.54	FR6.49	CKMS 設計は、鍵情報（暗号鍵及びメタデータ）のバックアップ中のセキュリティポリシーがどのように実装されるかを明記しなければならない。例えば、バックアップされた鍵情報（暗号鍵及びメタデータ）の配送及び保管中における、機密性とマルチパーティコントロールの要求事項の実装方法。	6.4.15 節

④ 鍵情報のアーカイブ方法を決めなければならない。

法律や規則等で要求される期間、鍵情報（暗号鍵やメタデータ）が利用可能であるようにするため、適用される法律や規則等を考慮して当該鍵情報（暗号鍵やメタデータ）のアーカイブ又は破棄を実行しなければならない。このため、鍵情報のアーカイブには、当該鍵情報（暗号鍵やメタデータ）を必要なときに復元できるように、長期保管用ストレージ設備に保管されることを含む。

一方、アーカイブされた鍵情報（暗号鍵やメタデータ）は、アーカイブされている期間、物理的又は暗号学的に保護されなければならない。例えば、アーカイブ鍵の暗号鍵有効期間が期限切れになる前の再暗号化や新しいメディアの出現によるメディア間の移動など、アーカイブされた鍵情報（暗号鍵やメタデータ）に提供される機密性保護の継続性についても考慮する必要がある。

CKMS の設計にあたって、検討項目 B.55 は、鍵情報のアーカイブを行うための条件を明確化することを、B.56 はアーカイブされた鍵情報を破棄するための要求事項を明確化することを、B.57 は機密性保護の継続性を確保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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.55	FR6.50	CKMS 設計は、どのように、どこで、どのような状況で鍵情報（暗号鍵やメタデータ）がアーカイブされるかを明記しなければならない。	6.4.16 節
B.56	FR6.51	CKMS 設計は、鍵情報（暗号鍵やメタデータ）のセキュアな破壊、又は新しい保管メディアに書き込まれた後の古い保管メディアのセキュアな破壊のための手法を明記しなければならない。	6.4.16 節
B.57	FR6.52	CKMS 設計は、アーカイブ鍵の暗号鍵有効期間（cryptoperiod）の期限切れ後に、鍵情報（暗号鍵やメタデータ）がどのように保護されるかを明記しなければならない。	6.4.16 節

⑤ 鍵情報の復元方法を決めなければならない。

バックアップやアーカイブされている鍵情報は、復元のための全てのルールが満たされていることを検証された後に、認可されたエンティティによって復元できるようにすべきである。

CKMS の設計にあたって、検討項目 B.58～B.61 は、バックアップやアーカイブされた鍵情報を復元するための条件や復元方法、要求事項を明確化することを求めたものである。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.58	FR6.53	CKMS 設計は、鍵情報（暗号鍵やメタデータ）の CKMS 復元ポリシーを明記しなければならない。	6.4.17 節
B.59	FR6.54	CKMS 設計は、鍵情報（暗号鍵やメタデータ）の復元ポリシーを実装及び実行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。	6.4.17 節
B.60	FR6.55	CKMS 設計は、どのように、どのような状況で鍵情報（暗号鍵やメタデータ）がそれぞれの鍵データベース又はメタデータ保管設備から復元されるかを明記しなければならない。	6.4.17 節
B.61	FR6.56	CKMS 設計は、鍵情報（暗号鍵やメタデータ）が復元中にどのように保護されるかを明記しなければならない。	6.4.17 節

5.5　鍵情報の鍵確立方法

本節は、SP800-130 の 6.4 節、6.6 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、SP800-130 の 6.4 節には 28 の小節があるが、本指針では内容に依存してそれらを 5.2 節、5.3 節、5.4 節、8.1 節に分離して記載してある。

① 鍵確立機能の利用局面を特定しなければならない。

鍵確立機能とは、2 つ又はそれ以上のエンティティ間で暗号鍵をセキュアに共有するプロセスのことであり、方法として以下の 2 つがある。

検討項目 B.62 は、CKMS の設計にあたって、鍵確立機能を利用する状況を特定することを要求したものである。

- 鍵配送（key transport）：
  一方のエンティティが共有する暗号鍵を生成し、当該暗号鍵及び（あれば）メタデータを他方のエンティティに配付する
- 鍵合意（key agreement）：
  両方のエンティティが共有鍵を導出するために使用される情報を共有し、当該情報から暗号鍵を導出する

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
B.62	FR6.57	CKMS 設計は、どのように、どのような状況で鍵及びそのメタデータが確立されるかを明記しなければならない。	6.4.18 節

② 鍵配送における鍵情報のセキュリティを確保するための要求事項を決めなければならない。

鍵情報の鍵配送には、郵便・宅配便などの物理的手段を使う場合とネットワークをする電子的手段を使う場合がある。いずれの手段であっても、全ての暗号鍵は完全性保護を、加えて対称鍵及びプライベート鍵は機密性保護も必要とする。

完全性保護の観点からは、配送された暗号鍵の受信者は、期待する認可された鍵送信者から当該暗号鍵が来たことの保証が必要である。また、暗号鍵の完全性検証を実行し、訂正可能な破損が検出された場合には適切な訂正を行い、訂正不能な破損が検出された場合には使用前に新しい又は訂正された暗号鍵を再確立すべきである。

機密性保護の観点からは、物理的保護か、対称鍵ラッピング鍵又はひとつ以上の非対称配送鍵ペアが関わる鍵確立技術が使用される。このラッピング鍵及び配送鍵は、配送に関わるエンドエンティティによって保護されるべきである。

CKMS の設計にあたって、検討項目 B.63 は鍵配送における機密性保護のための要求事項を、B.64 は完全性保護のための要求事項を、B.65 は鍵送信者を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。

なお、鍵情報の鍵配送を使う状況がなければ検討対象外である。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
B.63	FR6.80	CKMS 設計は、配送中の対称鍵及びプライベート鍵の機密性保護に使用される手段を明記しなければならない。	6.6.1 節
B.64	FR6.81	CKMS 設計は、配送された鍵の完全性保護に使用される手段、及びエラー検出後にどのように鍵が再構築又は置き換えられるのかを明記しなければならない。	6.6.1 節
B.65	FR6.82	CKMS 設計は、配送される鍵素材（keying material）の受信者に、どのように鍵送信者の識別子（ID）が認証されるかを明記しなければならない。	6.6.1 節

③ 鍵合意における鍵情報のセキュリティを確保するための要求事項を決めなければならない。

セキュアな鍵合意プロセスを利用する場合、そのプロセスに関与するそれぞれのエンティティは合意鍵を導出するために使われるある種の情報を提供しあうが、当該プロセスに関与していないエンティティは提供しあっている情報全て得たとしても合意鍵を得ることができない。逆に言えば、認可されていないエンティティが鍵合意プロセスに不正に入り込むことを防止することが重要であり、典型的には、鍵合意プロセスに参加する各エンティティは他方のエンティティ識別子の保証を必要とする。

CKMS の設計にあたって、検討項目 B.66 は鍵合意プロセスの手法について明確化することを、B.67 はエンティティの認証方法について明確化することを要求したものである。

なお、鍵情報の鍵合意を使う状況がなければ検討対象外である。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.66	FR6.83	CKMS 設計は、CKMS にサポートされるそれぞれの鍵合意スキームを明記しなければならない。	6.6.2 節
B.67	FR6.84	CKMS 設計は、鍵合意に参加するそれぞれのエンティティがどのように認証されるかを明記しなければならない。	6.6.2 節

④ 鍵確認機能を利用するための要求事項を決めなければならない。

鍵確立機能で共有された暗号鍵について、それぞれのエンティティが、実際に他方のエンティティが正しい暗号鍵を確立したことの確認をするために使用する機能である。

CKMS の設計にあたって、検討項目 B.68 は鍵確認を行うための条件を明確化することを、B.69 は鍵確認の手法について明確化することを求めたものである。

なお、鍵確立した鍵情報の鍵確認を行う状況がなければ検討対象外である。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.68	FR6.86	CKMS 設計は、それぞれの鍵確認が実行される状況を明記しなければならない。	6.6.3 節
B.69	FR6.85	CKMS 設計は、他方のエンティティと正しい鍵を確立したことを確認するために使用されるそれぞれの鍵確認手段を明記しなければならない。	6.6.3 節

⑤ 利用する鍵確立プロトコルを決めなければならない。

検討項目 B.70 は、CKMS の設計にあたって、利用する鍵確立プロトコルを全て明確化することを要求したものである。ここで、定められた以外の鍵確立プロトコルを利用してはならない。

以下に有名な鍵確立プロトコルをいくつか挙げている。SSH 以外は、米国政府での使用に当たってどの暗号オプションが推奨されるかのガイダンスを［SP 800-57-part3］に記載し、SSH は「RFC4251」に記載している。

- Internet Key Exchange（IKE）
- Transport Layer Security（TLS）
- Secure/Multipart Internet Mail Extensions（S/MIME）
- Kerberos
- Over-The-Air-Rekeying（OTAR）Key Management Messages
- Domain Name System Security Extensions（DNSSEC）
- Secure Shell（SSH）

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.70	FR6.87	CKMS 設計は、鍵確立と保管の目的のために CKMS によって採用されている全てのプロトコルを明記しなければならない。	6.6.4 節

5.6 鍵情報の喪失・破損時の BCP 対策

本節は、SP800-130 の 10.7 節に記載されている事項について解説したものである。

① 鍵情報の喪失・破損に対する BCP 対策を定めなければならない。

鍵情報（暗号鍵やメタデータ）が喪失又は破損した場合で、バックアップもアーカイブもされていなかった場合、当該暗号鍵で保護されているデータの喪失につながる可能性がある。

特に、重大な災害は、多数の運用中の鍵情報の喪失又は破損を引き起こす可能性が高い。この場合の BCP 対策として、鍵情報のバックアップは有効な手段であり、鍵情報の正当な復元を行うことで保護されているデータの喪失を防止することができる。

一方、鍵情報（暗号鍵やメタデータ）の喪失・破損の原因が紛失あるいは攻撃など人為的な要因に起因する場合、鍵情報（暗号鍵やメタデータ）の外部への流出などが否定できず、結果として当該暗号鍵で暗号化されていたデータの危殆化につながる可能性がある。この場

合には、バックアップから単に当該鍵情報（暗号鍵やメタデータ）の正当な復元を行うだけでは不十分であり、当該暗号鍵の利用停止や失効処理、潜在的なリスク評価、新しい暗号鍵への置き換え及びデータの再暗号化といった、5.7 節の対応を含む一連の BCP 対策が必要となる。

CKMS の設計にあたって、検討項目 B.71 は、BCP 対策として必要な鍵情報のバックアップを行うための手続きや要求事項を明確化することを、B.72 は BCP 対策として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、これらの検討項目で定めたことは B.52～B.61 の上位規定として機能し、B.52～B.61 の内容が B.71 及び B.72 の内容に矛盾してはならない。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.71	FR10.11	CKMS 設計は、暗号鍵及びそのメタデータをバックアップ及びアーカイブするための手続きを明記しなければならない。	10.7 節
B.72	FR10.12	CKMS 設計は、保管又は伝送された破損した鍵情報（暗号鍵及びメタデータ）を復元又は置き換えるための手続きを明記しなければならない。	10.7 節

5.7 鍵情報の危殆化時の BCP 対策

本節は、SP800-130 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、SP800-130 の 6.8 節には 8 つの小節があるが、本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。

そもそも全ての潜在的なセキュリティ問題を CKMS が防止し鍵情報の危殆化が発生しないようにすることは現実的でないことを前提として、CKMS の設計においては鍵情報の危殆化を速やかに検知できるようにすべきである。

鍵情報の危殆化が検知された場合、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

① 暗号鍵の危殆化に対する BCP 対策を定めなければならない。

暗号鍵の危殆化の影響は鍵タイプ及び鍵の用途に依存し、以下の結果をもたらし得る。

- 機密性の喪失
- 完全性の喪失
- 認証の喪失
- 否認防止の喪失
- これらの喪失の組み合わせ

しかも、危殆化した暗号鍵の使われ方によっては、当該暗号鍵で保護されたデータに対してだけでなく、当該暗号鍵が保護する他の多くの暗号鍵についても危殆化を連鎖的に引き起こす可能性がある。したがって、危殆化した暗号鍵の失効・置き換えはもとより、当該暗号鍵に依存する他の暗号鍵も可能な限り速やかに失効・置き換えを行うべきである。なお、暗号鍵の置き換えに伴い、データの再暗号化が必要となる。

また、暗号鍵の危殆化が検出されない、あるいは疑いの状態にとどまる場合がある。このような場合の暗号鍵の危殆化の影響を小さくするために、使用するそれぞれの暗号鍵に対して適切な暗号鍵有効期間の設定や利用範囲の制限をすることで検出されない暗号鍵の危殆化の時間を制限するのが望ましい。一般的には、対称鍵ラッピング鍵、鍵配送鍵、及び鍵合意鍵の暗号鍵有効期間を実用的な最短期間にしておくことがよい。この他、鍵導出鍵とマスタ鍵も定期的に変更したほうがよい。

CKMS の設計にあたって、検討項目 B.73 は暗号鍵に対する暗号鍵有効期間の設定や利用範囲の制限について明確化することを、B.74 は危殆化した暗号鍵（の鍵タイプ）だけでなく連鎖的に影響を受ける可能性がある別の暗号鍵（の鍵タイプ）を含めてどのような 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。B.75 は、危殆化した暗号鍵から連鎖的に影響を受ける別の暗号鍵の特定方法の明確化を要求したものである。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.73	FR6.102	CKMS 設計は、システムによって使用されているそれぞれの鍵タイプの受け入れ可能な暗号鍵有効期間（cryptoperiod）又は利用制限（usage limit）の範囲を明記しなければならない。	6.8.1 節
B.74	FR6.103	それぞれの鍵に対し、CKMS 設計は、セキュリティがその鍵に依存する他の鍵タイプを明記しなければならず、また初期鍵の危殆化が発生した時にそれに依存する鍵がどのように置き換えられるかを明記しなければならない。	6.8.1 節

B.75	FR6.104	CKMS 設計は、鍵が危殆化したときに他の危殆化した鍵を特定できるための手段を明記しなければならない。例えば、鍵導出鍵が危殆化したとき、導出された鍵をどのように特定するのか？	6.8.1 節

② メタデータの危殆化に対する BCP 対策を定めなければならない。

メタデータの危殆化は、メタデータ要素及びその使われ方に依存して、暗号鍵の危殆化や当該暗号鍵によって保護されるデータの危殆化につながる可能性がある。

CKMS の設計にあたって、検討項目 B.76 はメタデータの中でも危殆化が起こりやすい又は関連する暗号鍵の危殆化につながりやすいものがどれであるかを明確化することを、B.77 はメタデータに危殆化が起きた時にどのような影響が出るかを明確化することを要求したものである。B.78 はどのような 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.76	FR6.105	導入されたそれぞれの鍵タイプに対して、CKMS 設計は、どのメタデータ要素が危殆化（機密性、完全性、又はソース）しやすいのかを明記しなければならない。	6.8.2 節
B.77	FR6.106	CKMS 設計は、鍵のそれぞれの危殆化しやすいメタデータ要素に危殆化（機密性、完全性、又はソース）が起こったときに、起こり得るセキュリティ結果を明記しなければならない。	6.8.2 節
B.78	FR6.107	CKMS 設計は、それぞれの危殆化しやすいメタデータ要素での危殆化からどのように回復できるかを明記しなければならない。	6.8.2 節

③ 役員・従業員によるセキュリティ危殆化に対する BCP 対策を定めなければならない。

CKMS のセキュアな運用に責任のある人間が、自らそのセキュリティを危殆化させる場合がある。基本的には、悪影響を軽減するためには権限必要最小限ルールの徹底が重要であり、必要な人に必要な権限しか与えない、権限を悪用していないかを監査する、操作ログを隠蔽できないようにする、といった事前対策が考慮すべきである。

また、役員・従業員によるセキュリティ危殆化が発生した場合には、情報セキュリティポリシー及び CKMS 機能に基づいた以下のような回復手続きで対応・復旧すべきである。さらに、再発防止策としてのセキュリティポリシーや運用規程等の改訂もあり得る。

- システムの完全なシャットダウン
- 新しい暗号鍵によるバックアップ設備及びシステムの活性化
- 起こり得るセキュリティ障害についての現在及び潜在的ユーザへの通知
- 危殆化した暗号鍵へのフラグ付け・失効処理

加えて、管理上の懲戒から、役割又は地位からの解任、及び民事又は刑事裁判に関わる法的措置までを含む。

CKMS の設計にあたって、検討項目 B.79 及び B.80 は役員・従業員によるセキュリティ危殆化への事前対策としての要求事項を明確化することを求めたものである。B.81 は危殆化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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.79	FR6.117	CKMS 設計は、それぞれのサポートされる役割に提供される、あらゆる役員・従業員による危殆化の検知機能を明記しなければならない。	6.8.7 節
B.80	FR6.118	CKMS 設計は、それぞれのサポートされる役割に提供される、あらゆる役員・従業員による危殆化を最小化する機能を明記しなければならない。	6.8.7 節
B.81	FR6.119	CKMS 設計は、それぞれのサポートされる役割に提供される、CKMS 危殆化からの回復能力を明記しなければならない。	6.8.7 節

6 暗号アルゴリズムの選択

6.1 暗号アルゴリズムのセキュリティ

本節は、SP800-130 の 2.1 節に記載されている事項について解説したものであり、暗号アルゴリズムの選定方法について取り扱う。

① 要求される保護レベル（セキュリティ強度）に対応した暗号アルゴリズムを選定しなければならない。

CKMS がライフサイクル全体にわたって管理及び保護している暗号鍵を使用することで要求される保護レベル（セキュリティ強度）を満たすことができる暗号アルゴリズムを選定することが求められる。

検討項目 C.01 及び C.02 は、CKMS の設計にあたって、要求される保護レベル以上を実現していることを確認するために、採用している暗号アルゴリズム（鍵長を含む）及びセキュリティ強度の明確化を求めたものである。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
C.01	FR2.1	CKMS 設計は、システムによって使用される全ての暗号アルゴリズムとそれぞれのアルゴリズムでサポートされる全ての鍵長を明記しなければならない。	2.1 節
C.02	FR2.2	CKMS 設計は、鍵と鍵に結び付けられたメタデータを保護するために導入されているそれぞれの暗号技術について推定されるセキュリティ強度を明記しなければならない。	2.1 節

6.1.1 暗号アルゴリズムのセキュリティ強度

暗号アルゴリズムのセキュリティ強度を表す目安として“ビットセキュリティ（等価安全性ということもある)”という指標がある。具体的には、評価対象とする暗号アルゴリズムに対してもっとも効率的な解読手法を用いたときに、どの程度の計算量があれば解読できるか（解読計算量[3]）で表現され、鍵長[4]とは別に求められる。表記上、解読計算量が 2^x である場合に“x ビットセキュリティ”という。例えば、共通鍵暗号においては全数探索する際の鍵空間の大きさで 2^x（x

[3] 直感的には、基本となる暗号化処理の繰り返し回数のことである。例えば、解読計算量 2^{20} といえば、暗号化処理 2^{20} 回相当の演算を繰り返し行えば解読できることを意味する
[4] ハッシュ関数の場合はダイジェスト長に相当する

は共通鍵のビット長)、ハッシュ関数の例としては一方向性で 2^x、衝突困難性で $2^{(x/2)}$（x は出力ビット長）が解読計算量の（最大）理論値である。

“ビットセキュリティ”による評価では、どの暗号アルゴリズムであっても、解読計算量が大きければセキュリティが高く、逆に小さければセキュリティが低い。また、解読計算量が実現可能と考えられる計算量を大幅に上回っていれば、少なくとも現在知られているような解読手法ではその暗号アルゴリズムを破ることは現実的に不可能であると予測される。

表 6-1　ビットセキュリティ

<table>
<tr><th rowspan="2">ビットセキュリティ</th><th rowspan="2">暗号アルゴリズム</th><th colspan="3">（参考）長期的な利用期間※</th></tr>
<tr><th>利用上の条件</th><th>2030 年まで</th><th>2031 年以降</th></tr>
<tr><td rowspan="2">80 ビット</td><td rowspan="2">RSA-1024
DH-1024
ECDH-160
ECDSA-160
SHA-1</td><td>新規に処理をする場合</td><td>利用不可</td><td>利用不可</td></tr>
<tr><td>過去に処理したものを利用する場合</td><td colspan="2">過去のシステムとの互換性維持の利用だけを容認</td></tr>
<tr><td rowspan="2">112 ビット</td><td rowspan="2">RSA-2048
DH-2048
ECDH-224
ECDSA-224</td><td>新規に処理をする場合</td><td>利用可</td><td>利用不可</td></tr>
<tr><td>過去に処理したものを利用する場合</td><td>利用可</td><td>過去のシステムとの互換性維持の利用だけを容認</td></tr>
<tr><td>128 ビット</td><td>AES-128
Camellia-128
ECDH-256
ECDSA-256
SHA-256</td><td>特になし</td><td>利用可</td><td>利用可</td></tr>
<tr><td>128 ビットから 192 ビットの間</td><td>RSA-4096
DH-4096
HMAC-SHA-1</td><td>特になし</td><td>利用可</td><td>利用可</td></tr>
<tr><td>192 ビット</td><td>ECDH-384
ECDSA-384
SHA-384</td><td>特になし</td><td>利用可</td><td>利用可</td></tr>
<tr><td>256 ビット</td><td>AES-256
Camellia-256
ECDH-521
ECDSA-521
HMAC-SHA256</td><td>特になし</td><td>利用可</td><td>利用可</td></tr>
<tr><td>256 ビット以上</td><td>HMAC-SHA384</td><td>特になし</td><td>利用可</td><td>利用可</td></tr>
</table>

※　SP800-57 Part 1 revision 5 で記載している長期的な利用期間

そこで、暗号アルゴリズムの選択においては、“x ビットセキュリティ”の“x ビット”に着目して、長期的な利用期間の目安とする使い方ができる。例えば、NIST SP800-57 Part 1 revision 4[5]を参考にすると、電子政府推奨暗号リストに記載の暗号アルゴリズムのビットセキュリティは表 6-1 のように表現できる。なお、表記の便宜上、本設計指針では以下の表記を用いる。

- AES-xxx：鍵長が xxx ビットの AES のこと
- Camellia-xxx：鍵長が xxx ビットの Camellia のこと
- RSA-xxx：鍵長が xxx ビットの RSA のこと
- DH-xxx：鍵長が xxx ビットの DH のこと
- ECDH-xxx：鍵長が xxx ビット（例えば NIST 曲線パラメタ P-xxx を利用）の ECDH のこと
- ECDSA-xxx：鍵長が xxx ビット（例えば NIST 曲線パラメタ P-xxx を利用）の ECDSA のこと
- SHA-xxx：ハッシュ関数 SHA-xxx のこと
- HMAC-SHA-xxx：ハッシュ関数 SHA-xxx を HMAC に利用すること

[5] NIST SP800-57, Recommendation for Key Management – Part 1: General (Revision 4)

7 暗号アルゴリズム運用に必要な鍵情報の管理

7.1 鍵情報の種類

本節は、SP800-130 の 2.2 節、6.1 節、6.2 節に記載されている事項について解説したものである。

暗号鍵は、以下の通り、特性と用途（＋オプション）に応じて分類され、これらの組み合わせで「鍵タイプ」が定義される。SP800-130 で分類する鍵タイプは表 7-1 の通りである。

特性	公開（Public）	一般に公開できる情報
	プライベート（Private）	一人のユーザのみが秘密に保持する情報
	対称（Symmetric）	送信者と受信者が共通して秘密に保持する情報

オプション	静的（Static）	長期的に固定した情報
	一時的（Ephemeral）	1 つのセッションやトランザクションでのみ使われる情報

用途	データの暗号化／復号（Encryption/Decryption）
	鍵ラッピング（Key Wrapping）
	鍵配送（Key Transport）
	鍵合意（Key Agreement）
	署名（Signature）
	認証（Authentication）
	認可（Authorization）
	乱数生成（Random Number Generator（RNG））
	マスタ鍵（Master Key）

表 7-1　鍵タイプ一覧

1) 署名プライベート鍵（Private Signature Key）
2) 署名公開鍵（Public Signature Key）
3) 認証対称鍵（Symmetric Authentication Key）
4) 認証プライベート鍵（Private Authentication Key）
5) 認証公開鍵（Public Authentication Key）
6) データ暗号化／復号対称鍵（Symmetric Data Encryption/Decryption Key）
7) 鍵ラッピング対称鍵（Symmetric Key Wrapping Key）
8) 乱数生成対称鍵（Symmetric RNG Key）
9) 乱数生成プライベート鍵（Private RNG Key）
10) 乱数生成公開鍵（Public RNG Key）
11) マスタ対称鍵（Symmetric Master Key）
12) 鍵配送プライベート鍵（Private Key Transport Key）
13) 鍵配送公開鍵（Public Key Transport Key）
14) 鍵合意対称鍵（Symmetric Key Agreement Key）
15) 鍵合意静的プライベート鍵（Private Static Key Agreement Key）
16) 鍵合意静的公開鍵（Public Static Key Agreement Key）
17) 鍵合意一時的プライベート鍵（Private Ephemeral Key Agreement Key）
18) 鍵合意一時的公開鍵（Public Ephemeral Key Agreement Key）
19) 認可対称鍵（Symmetric Authorization Key）
20) 認可プライベート鍵（Private Authorization Key）
21) 認可公開鍵（Public Authorization Key）

メタデータは、CKMS によって明示的に記録され管理されている特定の暗号鍵に関連付けられている情報として定義されるものであり、特性、制約、受け入れられるユーザ及び適用可能なパラメタを指定する。メタデータの各ユニットはメタデータ要素と呼ばれる。SP800-130 で取り上げる典型的なメタデータ要素は表 7-2 の通りである。

暗号鍵の各種管理機能を実行するためには暗号鍵とメタデータが正しく関連付けられている必要がある。そのため、SP800-130 では、両者の関連付けは、両者に適切な暗号検証機能を適用し関連性が正しいことを検証する暗号学的プロセス、又は物理的なセキュリティ手段により両者の関連性が正しいことを確認する信頼プロセスのいずれかによって行うものとしている。関連付けられた暗号鍵とメタデータは信頼関係を持つという。

なお、ある暗号鍵に適用可能なメタデータ全てを関連付ける必要はなく、また一部又は全ての暗号鍵にいかなるメタデータの関連付けがない場合もある。

表 7-2　典型的なメタデータ要素一覧

a) 鍵ラベル（Key Label）
b) 鍵識別子（Key Identifier）
c) 所有者識別子（Owner Identifier）
d) 鍵ライフサイクル状態（Key Lifecycle State）
e) 鍵フォーマット指定子（Key Format Specifier）
f) 鍵生成に使用した製品（Product used to create the Key）
g) 鍵を使用する暗号アルゴリズム（Cryptographic Algorithm using the Key）
h) スキーム又は暗号利用モード（Scheme or Modes of Operation）
i) 鍵パラメタ（Parameters for the Key）
j) 鍵長（Length of the Key）
k) 鍵／アルゴリズム組のセキュリティ強度（Security Strength of the Key/Algorithm Pair）
l) 鍵タイプ（Key Type）
m) 鍵に対する適切なアプリケーション（Appropriate Applications for the Key）
n) 鍵セキュリティポリシー識別子（Key Security Policy Identifier）
o) 鍵アクセスコントロールリスト（Key Access Control List（ACL））
p) 鍵使用カウント（Key Usage Count）
q) 親鍵（Parent Key）
r) 鍵機微性（Key Sensitivity）
s) 鍵保護（Key Protections）
t) メタデータ保護（Metadata Protections）
u) 信頼関係保護（Trusted Association Protections）
v) 日時（Date Times）
w) 失効理由（Revocation Reason）

7.2　鍵情報の選択

本節は、SP800-130 の 6.1 節、6.2 節に記載されている事項について解説したものである。

① 鍵情報の選択にあたって、CKMS が取り扱う全ての鍵タイプの利用用途及び生成手段、メタデータ、信頼関係、保護方針などを決めなければならない。

CKMS の設計にあたって、検討項目 D.01～D.04 は、鍵情報の選択にあたっての要求事項を明確化することを求めたものである。D.01 は利用する鍵タイプの一覧、D.02 はメタデータに関しての要求事項、D.03 は鍵情報の利用条件や取り扱い方法、D.04 は書式方法を対象にしている。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
D.01	FR6.1	CKMS 設計は、使用されているそれぞれの鍵タイプを明記及び定義しなければならない。	6.1 節
D.02	FR6.2	システムで使用されているそれぞれの鍵タイプに対して、CKMS 設計は、信頼関係のために選択される全てのメタデータ要素、メタデータ要素が作成され鍵との関連付けが満たされている状況、及び関連付けの手段（すなわち、暗号メカニズム又は信頼プロセス）を明記しなければならない。	6.2.1 節
D.03	FR6.13	それぞれの鍵タイプに対して、CKMS 設計は、暗号鍵及びメタデータ要素に関する以下の情報を明記しなければならない： a) 鍵タイプ b) 暗号鍵有効期間（cryptoperiod）（静的鍵（static key）に対して） c) 生成手段 i. 使用した乱数生成器（RNG） ii. 鍵生成の仕様（例えば、署名鍵については［FIPS 186］、Diffie-Hellman 鍵確立鍵（key establishment key）については［SP800-56A］） d) それぞれのメタデータ要素に対して、以下を含める i. メタデータのソース ii. メタデータの検証方法 e) 鍵確立（key establishment）の手段 i. 鍵配送スキーム（使用されている場合） ii. 鍵合意スキーム（使用されている場合） iii. プロトコル名（名称があるプロトコルが使用されている場合） f) 暴露に対する保護（例えば、鍵の機密性、物理セキュリティ） g) 改ざんに対する保護（例えば、MAC 又はデジタル署名） h) 鍵を使用し得るアプリケーション（例えば、TLS、EFS、S/MIME、IPSec、PKINIT、SSH、等）	6.2.2 節

		i) 鍵の使用が許可されないアプリケーション j) 鍵保証（key assurances） i. 対称鍵保証（Symmetric key assurances）（例えば、フォーマットチェック） • 誰が保証を得るか • 保証が得られる状況 • どのように保証を得るか ii. 非対称鍵保証（Asymmetric key assurances）（例えば、所有と有効性の保証） • 誰が保証を得るか • 保証が得られる状況 • どのように保証を得るか iii. ドメインパラメタ有効性チェック • 誰が有効性チェックを実行するか • チェックが実行される状況 • どのようにドメインパラメタの有効性の保証を得るか	
D.04	FR6.14	CKMS 設計は、CKMS によって生成、保管、伝送、処理、及びその他管理される全ての鍵タイプ及びメタデータについて、全てのシンタックス、セマンティクス、及びフォーマットを明記しなければならない。	6.2.2 節

7.3 鍵情報の保護方針

本節は、SP800-130 の 6.2 節に記載されている事項について解説したものである。

① メタデータ要素内に含まれている情報を保護する方法を決めなければならない。

メタデータ要素内の暗号鍵、メタデータ及びそれらの信頼関係に関して、暗号学的プロセス又は信頼プロセスのいずれかにより保護しなければならない。

CKMS の設計にあたって、検討項目 D.05～D.07 は、暗号学的プロセスを利用する場合の保護方法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。D.05 は暗号鍵の保護、D.06 はメタデータの保護、D.07 は信頼関係の保護を対象にしている。

検討項目 D.08～D.10 は、信頼プロセスを利用する場合の保護方法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。D.05～D.07 と同様、D.08 は暗号鍵の保護、D.09 はメタデータの保護、D.10 は信頼関係の保護を対象にしている。

なお、D.05～D.07、D.08～D.10 のいずれかが対象である。

- 暗号学的プロセスを利用する場合

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
D.05	FR6.3	メタデータ要素の鍵保護（Key Protections）で使用されるそれぞれの暗号メカニズムに対して、CKMS 設計は、以下を明記しなければならない： i. 暗号アルゴリズム ii. 鍵パラメタ iii. 鍵識別子 iv. 保護値（protection value）：この要素は、完全性保護、機密性保護、又はソース認証（source authentication）の保護値（protection value）を含む。例えば、適切に実装された MAC 又はデジタル署名技術は、完全性保護やソース認証（source authentication）を提供し得る。 v. 保護が適用された時期 vi. 保護が検証された時期	6.2.1 節
D.06	FR6.5	メタデータ要素のメタデータ保護（Metadata Protections）で使用されるそれぞれの暗号メカニズムに対して、CKMS 設計は、以下を明記しなければならない： i. 暗号アルゴリズム ii. 鍵パラメタ iii. 鍵識別子 iv. 保護値（protection value）（例：MAC、デジタル署名） v. 保護が適用された時期 vi. 保護が検証された時期 一般に、特に鍵とメタデータがひとまとめにされる場合、鍵とメタデータに対して同じメカニズムが使用される。	6.2.1 節
D.07	FR6.7	メタデータ要素の信頼関係保護で使用されるそれぞれの暗号メカニズムに対して、CKMS 設計は、以下を明記しなければならない： i. 暗号アルゴリズム ii. 鍵パラメタ iii. 鍵識別子 iv. 保護値（protection value）（例：MAC、デジタル署名） v. 保護が適用された時期 vi. 保護が検証された時期	6.2.1 節

- 信頼プロセスを利用する場合

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
D.08	FR6.4	メタデータ要素の鍵保護（Key Protections）で使用される暗号学的ではないそれぞれの信頼プロセスに対して、CKMS 設計は、以下を明記しなければならない： i. 他のプロセスと区別するために使用されるプロセス識別子 ii. プロセスの説明又はプロセスの説明へのポインタ	6.2.1 節
D.09	FR6.6	メタデータ要素のメタデータ保護（Metadata Protections）で使用される暗号学的ではないそれぞれの信頼プロセスに対して、CKMS 設計は、以下を明記しなければならない： i. このプロセスを他のプロセスから区別するために使用される識別子 ii. プロセスの説明又はプロセスの説明へのポインタ	6.2.1 節
D.10	FR6.8	メタデータ要素の信頼関係保護で使用される暗号学的ではないそれぞれの信頼プロセスに対して、CKMS 設計は、以下を明記しなければならない： i. このプロセスを他のプロセスから区別するために使用される識別子 ii. プロセスの説明又はプロセスの説明へのポインタ	6.2.1 節

8 暗号鍵管理デバイスへのセキュリティ対策

8.1 鍵情報へのアクセスコントロール

本節は、SP800-130 の 6.4 節、6.7 節、6.8 節、8.4 節に記載されている事項について解説したものであり、鍵情報を実際に保管・運用するために利用する CKMS デバイスについて取り扱う。

なお、SP800-130 の 6.4 節には 28 の小節があるが、本指針では内容に依存してそれらを 5.2 節、5.3 節、5.4 節、8.1 節に分離して記載してある。また、6.8 節にも 8 つの小節があるが、本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。

8.1.1 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。

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、検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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 e) それぞれの鍵管理機能のアクセスコントロール	6.7.1 節
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

8.1.2 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。

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。

検討項目 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。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
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

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。

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。

暗号モジュールでの入出力機能は、ひとつ又はそれ以上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、並びに、外部での使用又は保管のために暗号モジュールから出力するために使用する。

CKMS の設計にあたって、検討項目 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。

なお、対称鍵やプライベート鍵などが平文形式で入出力しない場合には、E.12～E.15 は検討対象外である。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

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、検討項目 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 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

8.1.3　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。

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。

検討項目 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。なお、鍵情報の入力を人間に行わせない場合には検討対象外である。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

8.1.4　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。

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 の認証・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、検討項目 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。

なお、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検討対象外である。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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* 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。	6.7.4 節

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。

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* 個の分割鍵それぞれが *n* 人の信頼されるエンティティの誰か一人に割り当てられ、そのうち *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。

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ルート鍵やマスタ鍵を確立するために使用したり、バックアップのために平文形式で分割鍵を CKMS や暗号モジュールに入出力したりする場合に使うことが多い。

CKMS の設計にあたって、検討項目 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。

なお、鍵分割で管理される暗号鍵がない場合には検討対象外である。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

8.2 セキュリティ評価・試験

本節は、SP800-130 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。

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。

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。

検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

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、検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

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。

検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

④ 環境テストの実施概要を明確化しなければならない。

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、検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

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。

検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

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。

検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

⑦ 第三者テストの概要を明確化しなければならない。

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。暗号標準や推奨事項への製品適合の検証プログラム（CC 認証、JCMVP 認証、CMVP 認証、CAVP 認証、等）が代表例である。

検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

8.3 暗号モジュールの障害時の BCP 対策

本節は、SP800-130 の 10.6 節に記載されている事項について解説したものである。

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出来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。

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。

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、検討項目E.34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に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。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
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

9 暗号鍵管理システム（CKMS）のオペレーション対策

9.1 CKMS へのアクセスコントロール

本節は、SP800-130 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。

9.1.1 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。

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、検討項目 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 FCKMS 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、SP800-130 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

9.1.2　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。

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、検討項目 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。SP800-130 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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 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	8.2.1 節

		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

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。

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、検討項目 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。SP800-130 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

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、検討項目 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。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
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

④ 監査機能に対する要求事項を決めなければならない。

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、検討項目 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。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
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

9.1.3　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。

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、検討項目 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。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
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 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	8.3 節
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

9.2　システム保証

本節は、SP800-130 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。

① 構成管理に関する要求事項を決めなければならない。

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。

検討項目 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。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
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）	9.8.1 節

		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)	

② セキュアな配付に関する要求事項を決めなければならない。

CKMS で使用される製品には、セキュアな配付の保証（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。

検討項目 F.22 は、CKMS の設計にあたって、セキュアな配付を保証・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。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
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付の要求事項を明記しなければならない： a) 配付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) 配付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付が検知されることを保証するための保護要求事項 d) 製品の配付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

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。

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。

検討項目 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。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
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 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	9.8.3 節

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。

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、検討項目 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 は通知、F.26～F.28 は修正・対処に相当する。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
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

9.3 セキュリティアセスメント

本節は、SP800-130 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。

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。

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、検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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ばならない。	11.1.2 節
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。	11.1.3 節

② 定期的な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。

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、定期的にアセスメントを実施すべきである。このアセスメントでは、少なくとも、前回のセキュリティアセスメント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、検討項目 F.38～F.41 は、定期的な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.38 はアセスメントの実施条件、F.39 及び F.40 はアセスメントの範囲及び内容、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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

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、検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

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

検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

9.4 CKMS へのアクセスコントロールの危殆化時の BCP 対策

本節は、SP800-130 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、SP800-130 の 6.8 節には 8 つの小節があるが、本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。

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

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。

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、検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

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、検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

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 SP800-130 6.8.6 に記載されている。

検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

9.5 CKMS 設備への障害・災害発生時の BCP 対策

本節は、SP800-130 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を高いリスクを伴う。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（5.6節）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、5.7節及び9.4節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。

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。

検討項目 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。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
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

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。

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。

検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

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。

検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

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。

検討項目 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
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

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。

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、検討項目 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。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
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

Appendix 用語集

以下の用語集は本設計指針で使用されている用語と定義を含んでいる。併せて、SP800-130 との対応関係も示す。

本設計指針で使用されている用語	SP800-130で使用されている用語	定義
（暗号鍵やメタデータの）アーカイブ	Archive (key and/or metadata)	電子的な暗号鍵やメタデータを、記憶技術が変化しても維持される長期記憶媒体に格納すること。あるいは、アーカイブされた鍵やメタデータが格納される場所
アプリケーション	Application	一連の目標を達成したり、一連のサービスを提供したりするように設計され運用されているコンピュータプログラム
暗号、暗号技術	Cryptography	機密性、データの完全性、エンティティ認証、データ発信元認証などのセキュリティサービスを提供する数学的手法の使い方
暗号アルゴリズムの移行	Algorithm Transition	ある暗号アルゴリズムを別の暗号アルゴリズムに置き換えるために使用されるプロセスと手順
暗号鍵（鍵）	Cryptographic Key (Key)	暗号アルゴリズムへのパラメタを構成するビット列、整数、または文字列
暗号鍵管理システム（CKMS）	Cryptographic Key Management System (CKMS)	暗号鍵とそのメタデータの管理システム（世代管理、流通管理、ストレージ、バックアップ、アーカイブ、リカバリ、使用、失効、破壊など）。暗号鍵とメタデータを保護、管理、および、配付するために準備された方針、手順、デバイス、コンポーネント。 CKMSは、1つまたは複数のエンティティに代わって暗号鍵管理機能を実行する
暗号鍵有効期間	Cryptoperiod	特定の鍵の使用が認可されている期間、又は与えられたシステムやアプリケーションにおいて鍵の有効性が残存する期間
暗号境界	Cryptographic Boundary	明示的に定義された境界であり、その境界は暗号モジュールの全てのコンポーネントの外周に存在する
暗号責任者	Cryptographic Officer	CKMSの暗号コンポーネントおよびデバイスに対し、暗号部分に対する初期化および管理機能を実行する権限を与えられた個人

（関連付けを保護する）暗号学的プロセス	Cryptographic Binding (Binding)	CKMSが1つまたは複数の暗号技術を利用し、鍵と選択されたメタデータ要素との間の信頼関係を確立すること
暗号モジュール（モジュール）	Cryptographic Module (Module)	セキュリティ機能（例えば、暗号アルゴリズムと鍵生成）を実装した、暗号境界内に含まれるハードウェア、ソフトウェア、及びファームウェアのうち1つ以上を含む集合
暗号利用モード	Mode of Operation	暗号アルゴリズムと鍵を使ってデータを操作するための一連のルール。処理される追加データの有無にかかわらず、アルゴリズムの出力の全部または一部をアルゴリズムの次の反復の入力に戻すことを含むことが多い。例としては、暗号文フィードバック（CFB）、出力フィードバック（OFB）、暗号ブロック連鎖（CBC）などがある
一時停止状態	Suspended State	鍵のライフサイクル状態の1状態であり、以前に活性化状態だった鍵を、一時的にその状態から退避させるための状態。必要に応じて鍵を活性化状態に戻すことができる
エンティティ	Entity	個人、グループ、デバイス又はプロセスのこと。エンティティは、関連づけのために識別子を持つ。（パーティとも呼ばれることがある）
解読	Cryptanalyze	暗号の仕組みを破ること。より一般的には、数学的手法を応用した情報セキュリティサービスを破ること
鍵確認	Key Confirmation	あるエンティティ（鍵確認受容者）に対して、別のエンティティ（鍵確認プロバイダ）が実際に正しい対称鍵素材や共通の秘密を所有していることを保証する為の手順
鍵確立	Key Establishment	2つ以上の エンティティ 間で鍵を安全に共有されるプロセス 。あるエンティティから別のエンティティへ鍵を移送（鍵配送）する場合と、各エンティティの持つ情報を利用して導出（鍵共有）する場合がある
鍵合意	Key Agreement	鍵確立手順の1種であり、結果として生成される鍵素材は、二者以上の関係者の寄与情報から生成される。そのため、各エンティティは、結果として生成される鍵素材を、他のエンティティの寄与情報なしに事前に知ることはできない
鍵更新	Key Update	交換される（古い）暗号鍵から所定の関数を用いて新しい暗号鍵を計算し、その新しい暗号鍵と関連する鍵情報を置き換える手続き

鍵再生成	Rekey	交換される（古い）暗号鍵に依存しない方法で新しい暗号鍵を生成し、その新しい暗号鍵と関連する鍵情報を置き換える手続き
鍵状態の遷移	Key State Transition	1つの鍵ライフサイクル状態から別の鍵ライフサイクル状態に移行するプロセス
鍵所有者	Key Owner	暗号鍵または鍵ペアを使用することが許可されたエンティティ（例えば、人、グループ、組織、デバイス、またはモジュール）
鍵生成	Key Generation	暗号鍵を生成する手続き
鍵素材	Keying Material	鍵やメタデータ
鍵配送	Key Transport	鍵確立手順の1種であり、ある当事者（送信者）が鍵素材を選択および暗号化し、別の当事者（受信者）に素材を配付する鍵確立手順。典型的な方式では暗号を使用して鍵素材を保護するが、一部のアプリケーションでは（暗号の）代わりに、信頼できる輸送人を使用することもある（鍵配付と呼ぶこともある）
鍵ライフサイクル状態	Key Lifecycle State	暗号鍵の有効期間において、暗号鍵の使用状態を表す。暗号鍵の有効期間において、暗号鍵は何れか１つの状態を持つ。また状態の種類は有限となる。状態には、活性化前、活性化、一時停止、非活性化、危殆化、破壊が含まれる
鍵ラッピング	Key Wrapping	（関連する完全性を満たす為の情報と共に）暗号を用いて鍵を保護する方法。鍵の機密性及び完全性は、対称鍵を利用して提供される
鍵ラベル	Key Label	鍵ラベルは、鍵についての情報が記載されている、人間が読み取り可能で、場合によっては機械で読み取り可能な文字列を指す。鍵ラベルの例：「ルートCAプライベート鍵2009-29」、「メンテナンス共有鍵2005」
拡張性	Extensibility	システムの能力向上の容易さの尺度
活性化状態	Active State	鍵ライフサイクルの一状態。その状態においては、一連のアプリケーション、アルゴリズム、及びセキュリティエンティティにおいて、暗号鍵が使用可能となる
活性化前状態	Pre-Activation State	鍵のライフサイクル状態の１つであり、鍵の使用がまだ許可されていない状態
監査	Audit	データを、収集、分析、及び要約するための手順。そのデータは監査責任者がシステム管理者に対して、システムのセキュリティに関する報告を行うために必要となる

観測不可能性	Unobservability	観測者がCKMSでサポートされている通信データから、関与する当事者を特定または推論することができないことの保証
関連付け機能	Association Function	SP800-130では、鍵とメタデータを不正な変更や開示から保護し、メタデータの起源を認証する機能
関連付けられたメタデータ（メタデータ）	Associated Metadata (also Metadata)	本フレームワーク（SP800-130）では、CKMSによって明示的に記録され、管理され、保護される暗号鍵に関連付けられたプロパティを記述するために使用されるパラメタ
危殆化	Compromise	（例えば、鍵、メタデータ、又はセキュリティに関係する情報に対する）権限を伴わない開示、改変、置き換え、及び利用
危殆化状態	Compromised State	鍵ライフサイクルの状態。その状態において、鍵は侵害されたと指定されており、データ暗号化に鍵を使用しない。 特定の状況下では、鍵はすでに保護されたデータを処理するために使用されることがある
形式言語	Formal Language	曖昧性の無い規則により定義された構文（適切な構造の正しい文章を作成するための規則）を持つ言語。その言語において、構文的に正しく記載された全ての文章は、その文章の正しさをオートマトン（例えば、構文解析アプリケーションプログラムを実行するコンピュータ）によって確認できる
権威時刻ソース	Authoritative Time Source	正確な時間を提供する、信頼されるネットワークエンティティ。日本国内では、NICT公開NTPサービスが該当する
検証	Validate	実装が使用に適しているかの保証を得るために、暗号パラメタまたはモジュールをテストし、そのテスト結果を確認すること
堅牢化	Hardening	脆弱性にパッチを当て、不必要なサービスを無効にすることで、攻撃手段を排除するプロセス。コンピュータの堅牢化は、多層防御を行うために、複数の段階を踏んで行われる
最小権限の原則	Least Privilege	各エンティティは正当な使用に必要な情報とリソースにのみアクセスできるという（設計）原則
識別子	Identifier	エンティティ（例えば、鍵管理機能を実行するエンティティ）を示すために使用されるテキスト文字列。CKMSアクセス制御システムによって、鍵の集合から特定の鍵を選択するためにも使用される

失効状態	Revoked State	鍵ライフサイクルの1状態であり、以前にアクティブであった暗号鍵であるものの、データ保護の暗号化に使用することができない状態
商用既製品	Commercial Off-The-Shelf (COTS)	出来合いの技術やプロダクトであり、一般に販売、リース、またはライセンス供与が可能な製品
シンタックス	Syntax	ある言語で受理できる文章を構成するための規則
信頼	Trust	特定の機能またはサービスを正しく、公平かつ公正に実行する能力と、エンティティ及びその識別子が本物であることを保証する、エンティティの特性
信頼関係	Trusted Association	鍵とそのメタデータが適切に関連付けられ、特定の情報源から発信され、変更されておらず、不正な開示から保護されているという保証 を提供する、選択されたメタデータ要素と鍵の関係
スキーム	Scheme	適切に実装され、維持されている場合に（暗号化）サービスを提供できる変換セットの明確な仕様。スキームは、プリミティブより上位の構造体であり、プロトコルよりも下位の構造体となる
スケーラビリティ	Scalability	仕事量の増加に適応させるために、能力を上手に拡張する能力。または、その増加に対応するために拡張された能力
セキュリティドメイン	Security Domain	CKMSを有するエンティティの集合。各々のCKMSは、同じセキュリティポリシー（ドメインのセキュリティポリシー）で運用される
セキュリティドメイン（ドメイン）	Security Domain (Domain)	論理的なエンティティであり、そのエンティティは、共通の目標と制約を持つ「人、組織、情報システム」の集合
セキュリティポリシー	Security Policy	団体により作成された規則と要求からなり、情報とサービスの許容される使用や、情報の機密性・完全性・可用性の保護レベルと実現手段が含まれる
セキュリティ強度	Security Strength	暗号アルゴリズムまたは暗号システムを暗号解読するために必要な作業量（2を底とする対数で表現された作業回数）に関連付けられた数値
セクタ	Sector	製品、システム、またはサービスに対する、共通の目標、標準、及び要件を持つ組織の集合（連邦政府機関、民間組織、国際的なコンソーシアムなど）
設計者	Designer	新しいシステムに含まれるデバイスに対して、そのデバイスがどのように構造され、調整され、運用されるかを指定する能力、責任、権限を持つ人物または組織

セマンティクス	Semantics	ある言語において受理可能な文が意図する内容
相互運用性	Interoperability	エンティティの集合が、別のエンティティの集合に物理的に接続した場合における、論理的に通信する能力の尺度
適合CKMS	Compliant CKMS	本フレームワーク内で規定された各要件に対応した設計仕様を満たすCKMS
登録	Registration	登録エージェントによって実行される一連の手順。これらの手順によって、エンティティの識別、エンティティの認可、エンティティの鍵とエンティティの識別子（及び場合によっては他のメタデータ）の信頼できる関連付けが成される
匿名性	Anonymity	CKMSを利用した通信において、公開データと所有者とを関連付けることができないことを保証する性質
ドメインのセキュリティポリシーの同等性	Equivalent Security Domain Policies	2つのドメインのセキュリティポリシーにおいて、一方のセキュリティドメインと他方のセキュリティドメインの間で暗号鍵を交換することが許されており、また、もう一方のドメインが提供する同程度の保護方法で鍵を保護することが許されている場合、その2つのドメインのセキュリティポリシーは同等性を持つ
トラストアンカー	Trust Anchor	信頼木の基底に存在する、または信頼チェーン内の最も強いリンクとして存在する、1つ以上の信頼された公開鍵。当該公開鍵を基点にCKMSでの公開鍵基盤（PKI）が構成される
トラストアンカーストア	Trust Anchor Store	トラストアンカーの情報が格納される場所
パーティ	Party	エンティティを参照
破壊状態	Destroyed State	鍵ライフサイクルの一状態。その状態においては、その鍵の復元及び使用ができない
破損	Garbled	データ（例えば、暗号鍵）内の1つまたは複数の要素（例えば、ビット、数字、文字）が、改変または破壊されること
バックアップ（暗号鍵やメタデータ）	Backup (key and/or metadata)	運用過程において、鍵やメタデータを別の設備にコピーすること。このコピーは、鍵やメタデータの元の値が失われたり変更されたりした場合に、鍵やメタデータを復元するために利用される
ハッシュ値	Hash Value	ハッシュ関数によって生成された固定長のビット列
パラメタ	Parameters	特定のセキュリティ目標を達成する為の暗号アルゴリズムの出力を計算する時に、暗号アルゴリズムと共に使用される特定の変数とその値

非活性化状態	Deactivated State	鍵ライフサイクルにおける一状態。その状態においては、その鍵をデータ保護目的の暗号処理に使用しない状態。 特定の状況下では、鍵は過去に保護されたデータを処理するために使用されることがある
標準	Standard	権威（例えば、国や標準化機関）、慣行、または共通的な認識によって確立されたモデルや 例示
ファイアウォール	Firewall	セキュリティで保護されたコンピュータ内のOSと統合されたプロセスであり、望ましくないアプリケーションや望ましくないリモートユーザーによる、アクセスや操作を検知及び防止するプロセス
（鍵やメタデータの）復元	Recover (key and/or metadata)	バックアップまたはアーカイブ（ストレージ）から鍵やメタデータを取得または再構築すること
プライバシー	Privacy	エンティティに関する特定の情報の機密性とアクセス権が保護されていることの保証
プロファイル	Profile	顧客セクタ（例えば、連邦、私企業、または国際）の基準に適合するCKMSを作成するために使用される方針、手順、コンポーネントおよびデバイスの仕様
分割鍵	Key Split	1つ以上の鍵分割片を適切に組み合わせることで、暗号鍵を形成する（再生する）ことができるパラメタ
（鍵やメタデータの）保管	Store (key and/or metadata)	鍵やメタデータを、それらを復元することができる媒体に移動すること
マルウェア	Malware	（スパイウェア、ウイルスプログラム、ルートキット、トロイの木馬を含む）攻撃者によって設計・操作される、コンピュータのセキュリティを侵害するようなソフトウェア
メタデータ（関連付けられたメタデータ）	Metadata (also Associated Metadata)	本フレームワーク(SP800-130)では、CKMSによって明示的に記録・管理・保護された、暗号鍵のプロパティを記述するために使用されるパラメタ。
メタデータ要素	Metadata Element	CKMSによって明示的に記録および管理されるメタデータの中の一要素
役割	Role	個人または組織が環境またはコンテキスト範囲内で実行することが認可された、受け入れ可能な機能、サービス、およびタスクの集合
（公開鍵）有効期間	Validity Period	公開鍵証明書の有効期間
（鍵情報の）有効期間延長	Renewal	鍵情報の有効期限を延長して、延長した期間内は同じ暗号鍵をそのまま使用できるようにするための手続き

ユーザ	User	情報システム、情報システムの1つ以上のアプリケーション、それらのセキュリティ手順とサービス、およびそれらをサポートするCKMSを使用することを、組織およびポリシーによって認可された個人
ルータ	Router	データパケットを送受信したり、多様な通信エンティティの間で論理接続を確立したりする物理エンティティまたは論理的なエンティティ（通常、有線および無線の両方の通信デバイスを同時にサポートする）
ルートキット	Rootkit	標準のOS機能や他のアプリケーションを損傷させて、管理者からその存在を積極的に隠しながら、コンピュータへの不正な特権アクセスを可能にするマルウェア
連結不可能性	Unlinkability	情報処理システム内の2つ以上の関連イベントを、CKMSでサポートされた通信を用いて関連付けることができないことの保証
CKMSコンポーネント（コンポーネント）	CKMS Component (Component)	CKMSを実現（実装）するために使用されるハードウェア、ソフトウェア、またはファームウェア
CMKSデバイス（デバイス）	CKMS Device (Device)	特定の目的（ファイアウォール、ルータ、伝送デバイス、暗号モジュール、データストレージデバイスなど）の機能を提供するCKMSコンポーネントの任意の組み合わせ
CKMSプロファイル（「プロファイル」も参照）	CKMS Profile	利害を同一とするコミュニティ（例えば、米国政府、銀行、健康医療分野、航空宇宙など）がCKMSセキュリティ要件の仕様を規定するために使用する文章であり、その文章は実装に依存していない
CKMSモジュール	CKMS Module	特定の場所で必要な全てのCKMS機能を実行する論理エンティティ

発行日　2020 年 7 月 7 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
（技術本部　セキュリティセンター　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