CRYPTREC GL-3002-0.0

暗号鍵管理システム設計指針（基本編）

ドラフト版

（2019.7.12 版）

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

注意

本設計指針はドラフト版です。正式版とは異なる場合がありますのでご注意ください。
本ドラフト版についてご意見がございましたら、2019 年 10 月 31 日までに
下記までメールにてご連絡ください。
なお、頂いたご意見は正式版作成及び委員会審議にて参考にさせていただきますが、
個別の回答は行いませんので、ご容赦ください。

e-mail: comment-ckms@cryptrec.go.jp

以下の事項については、本設計指針では精査しておりません。
正式版の公開までに見直す予定としております。

- **用語の（特に他ドキュメント類との）統一性**
- **4 章以降の記載内容（現状は、SP800-130 での該当部分の日本語訳抜粋になっているため、今後、若干の解説を追記する予定）**

【修正履歴】

修正日	修正内容
2019.7.12　(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、セキュアな暗号利用の前提として重要な暗号鍵の管理に関する在り方を解説し、実際の暗号鍵管理システム（以下、「CKMS」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。

まずイントロダクションとして暗号鍵管理の必要性を認識してもらうために、暗号鍵管理がどのような位置づけにあり、どのような枠組みに従って検討すべきものなのかといった「暗号鍵管理の在り方」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。

「暗号鍵管理についての技術的内容」については、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。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。

したがって、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として、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だけである。加えて、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。どのようにそれらの要求事項に対応（例えば、ポリシーや暗号アルゴリズム、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。

また、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 調達責任者が行うべきであり、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 の要求項目を提示することで 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メカニズム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。

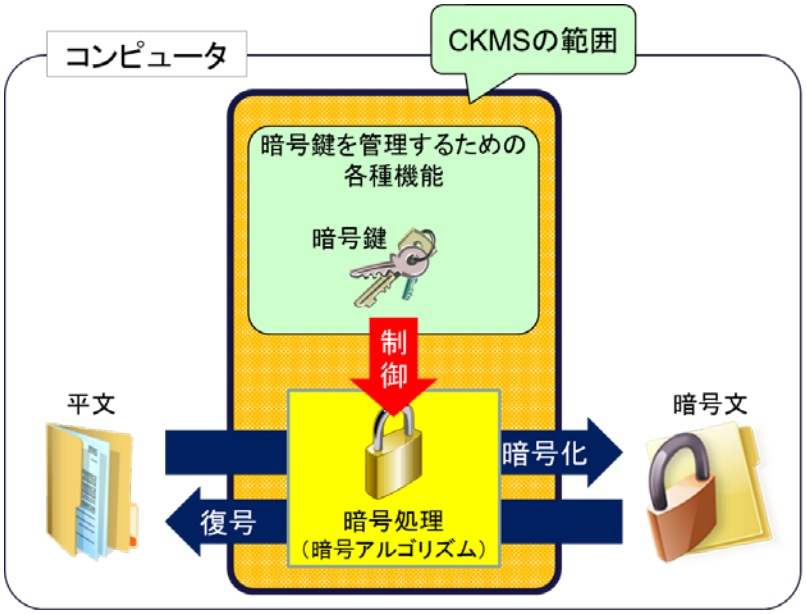


図 1-1 単純な CKMS の概要例

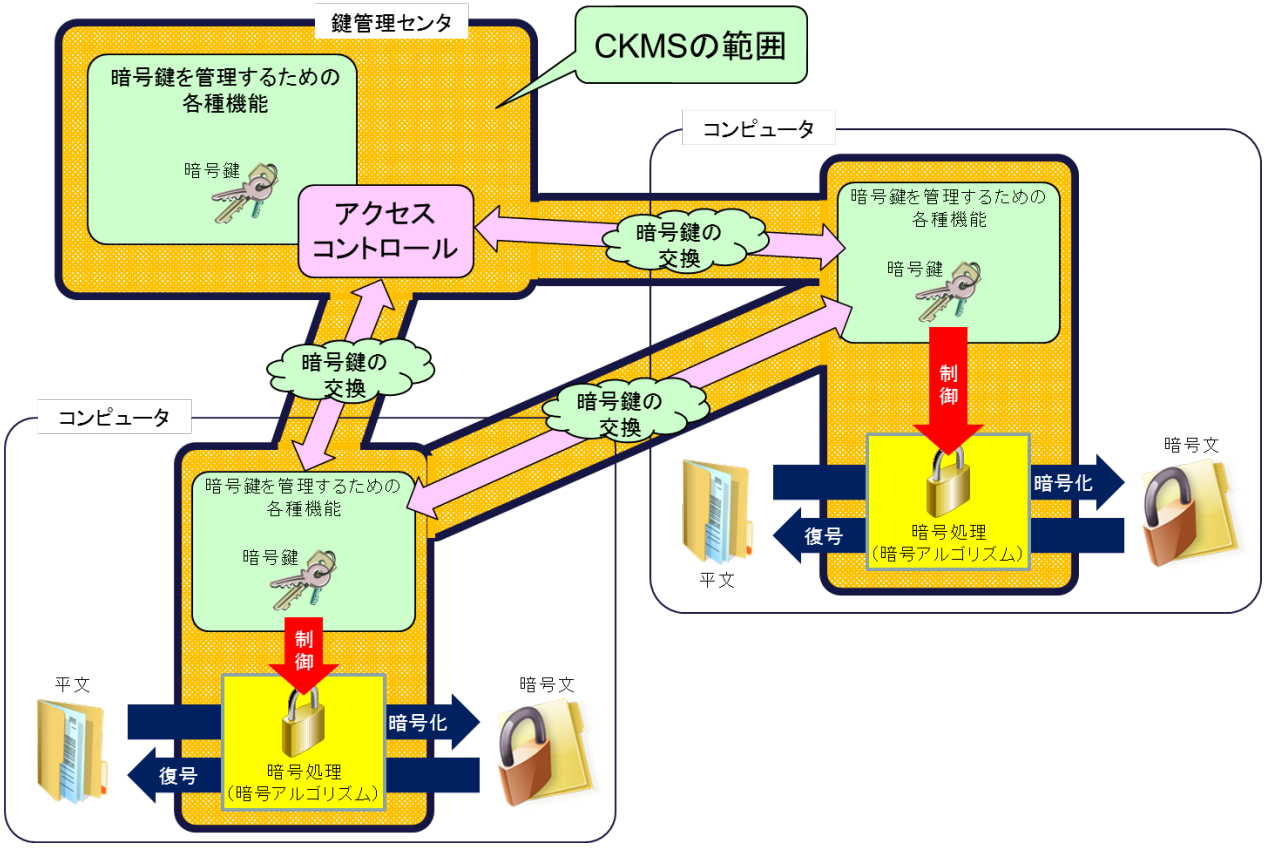


図 1-2　複雑な CKMS の概要例

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（2019 年 6 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　情報システム学科　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　サービスイノベーション部
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
委員	手塚　悟	慶應義塾大学　大学院政策・メディア研究科　特任教授
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	〃
	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
	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　ドラフト版：
https://www.ipa.go.jp/security/publications/nist/index.html

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、情報保護や改ざん検知、認証・認可などで使われる。

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。

「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。

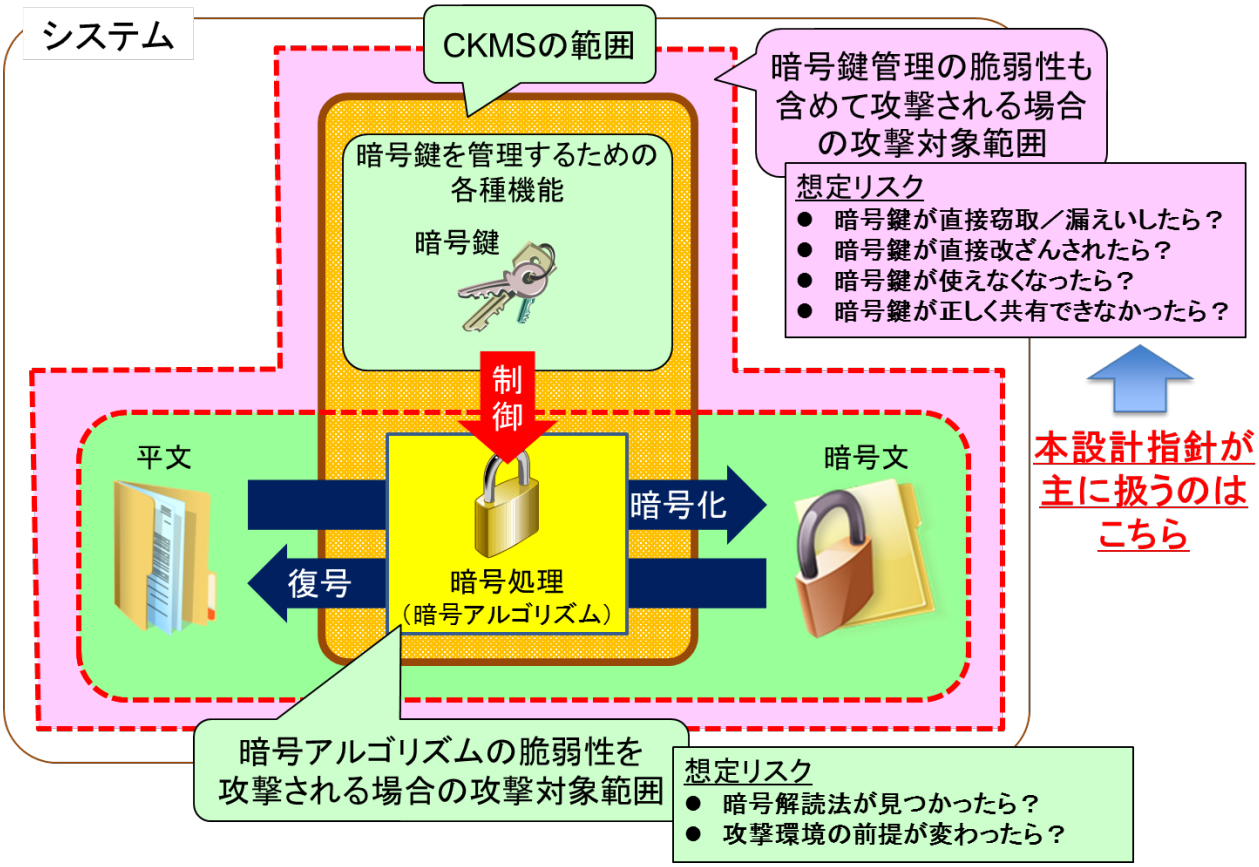


図 2-1　暗号アルゴリズムと CKMS の攻撃対象範囲／想定リスクの違い

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、鍵情報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。

構成要素としては、「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。

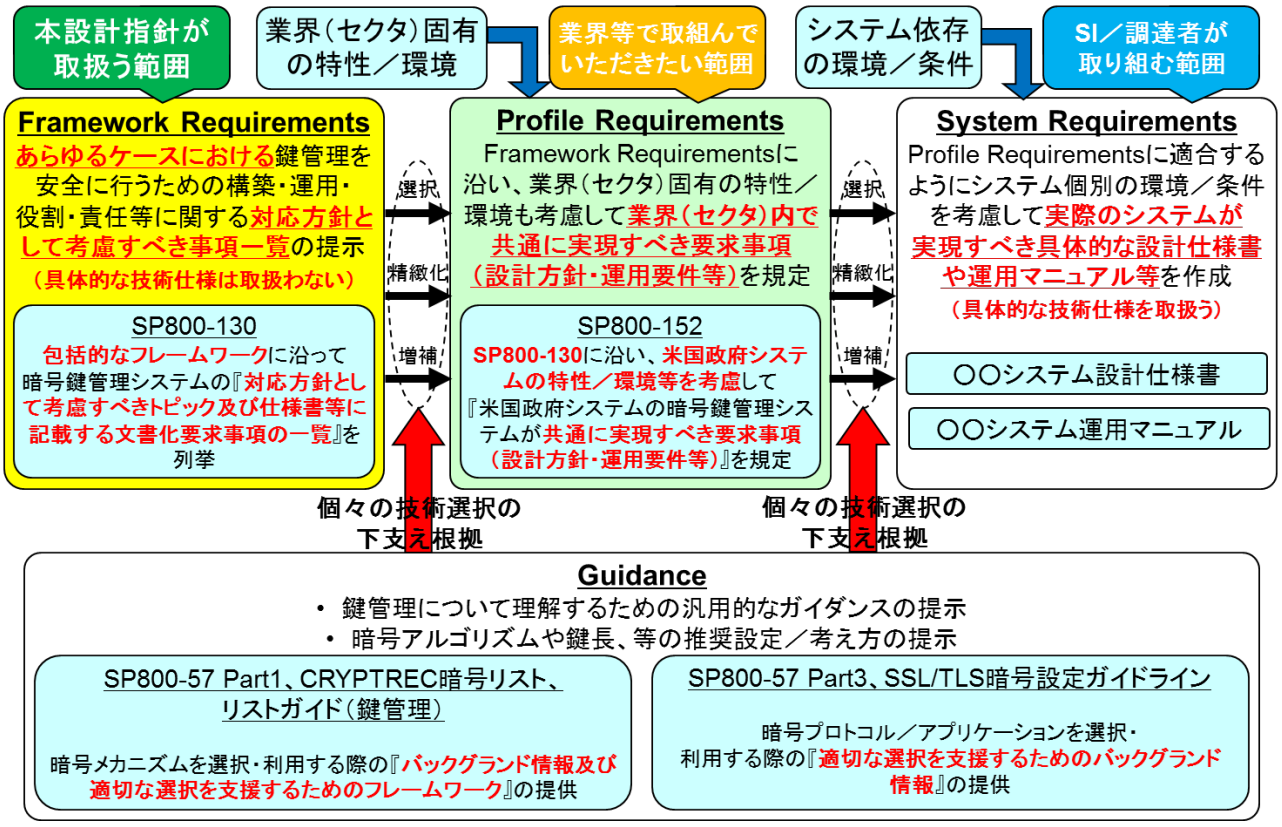


図 2-2　暗号鍵管理の考え方の枠組み

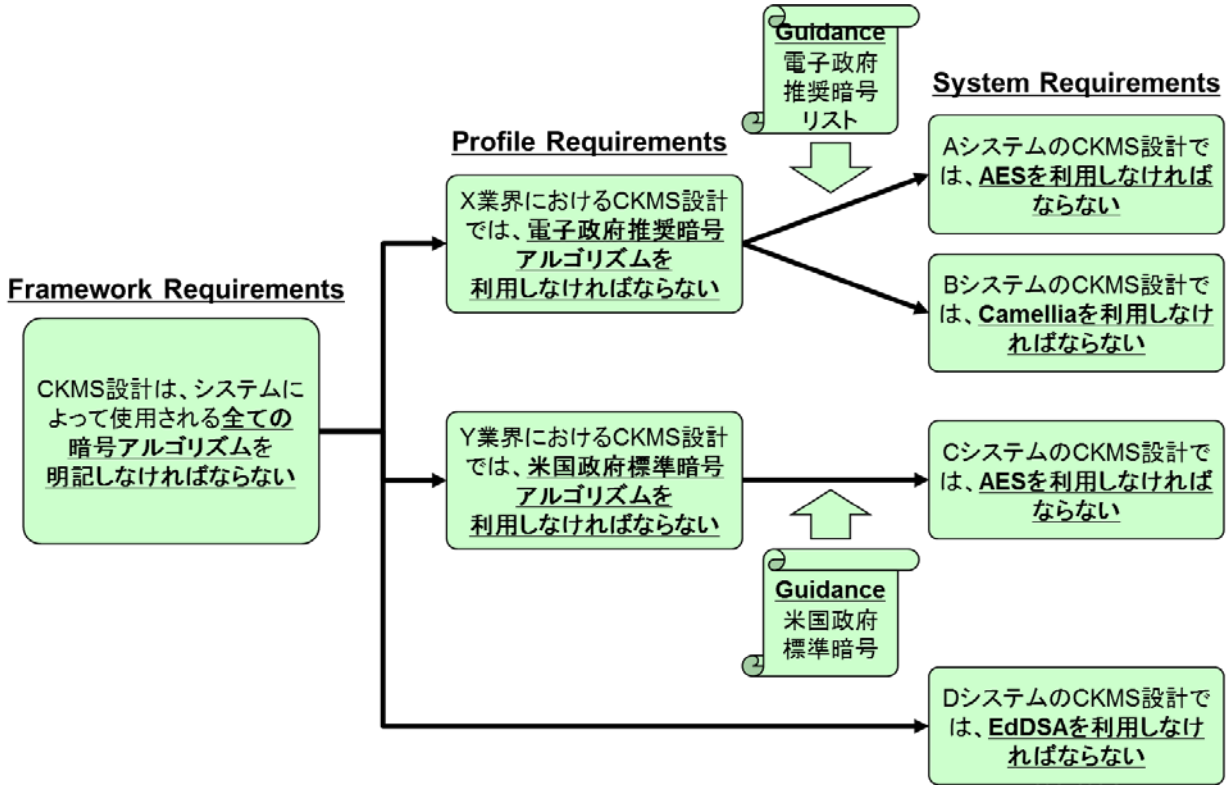


図 2-3　各構成要素の関係性の例

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、CKMS 設計書に明記させることにある。後述する 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、各業界等の固有の特性や利用環境等を考慮して業界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 の要求項目はすべて「○○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、業界（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

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である。

Profile Requirements は、業界（セクタ）固有の特性や環境を踏まえた業界（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。具体的には、業界（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業界（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 は米国政府向けの CKMS 用 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。しかし、検討すべき項目（Framework Requirements）が全部で 258 個もあり、かつ記載内容も教科書的な並びになっているため、本当に必要な個所を見つけ出すことが難しい。

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、分かりやすく表現することを目指している。併せて SP800-130 全体の日本語訳も作成している。

【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。

- 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 の利用者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について、具体的な鍵情報の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。

- 鍵情報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。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。

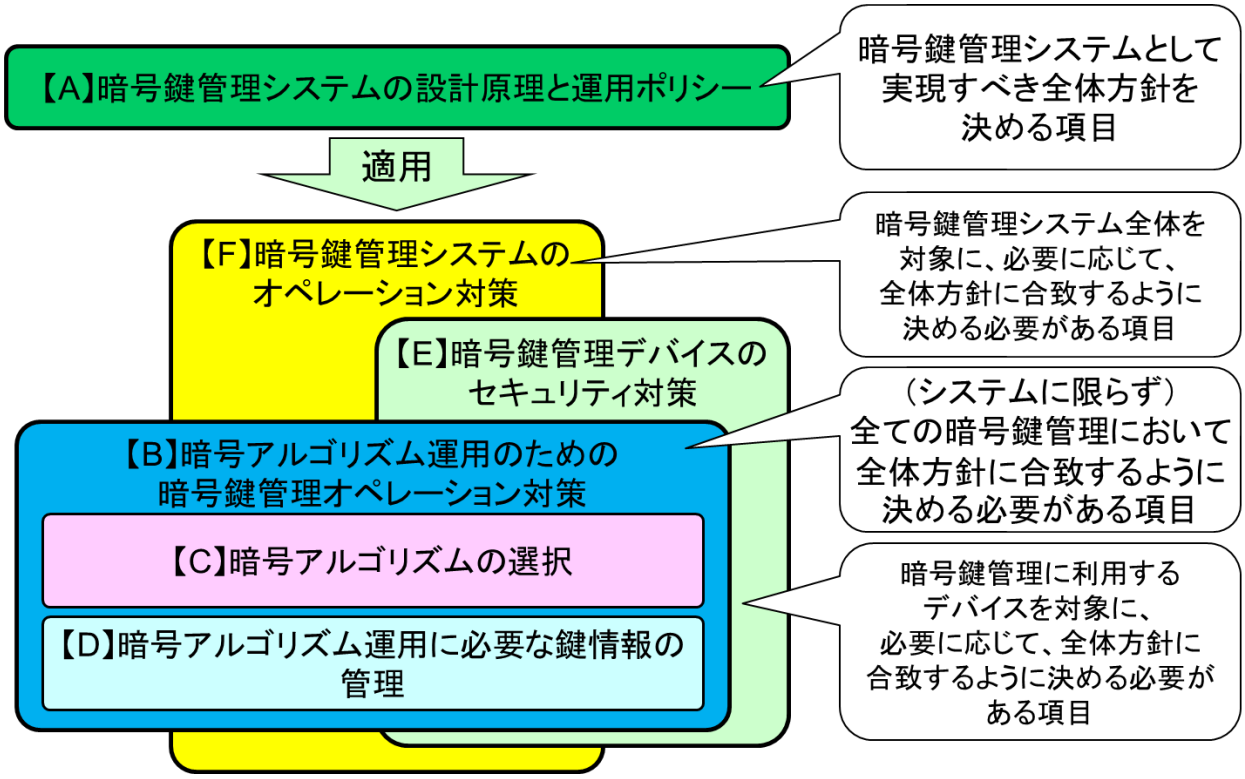


図 2-4　暗号鍵管理における目的別分類関係

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。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。

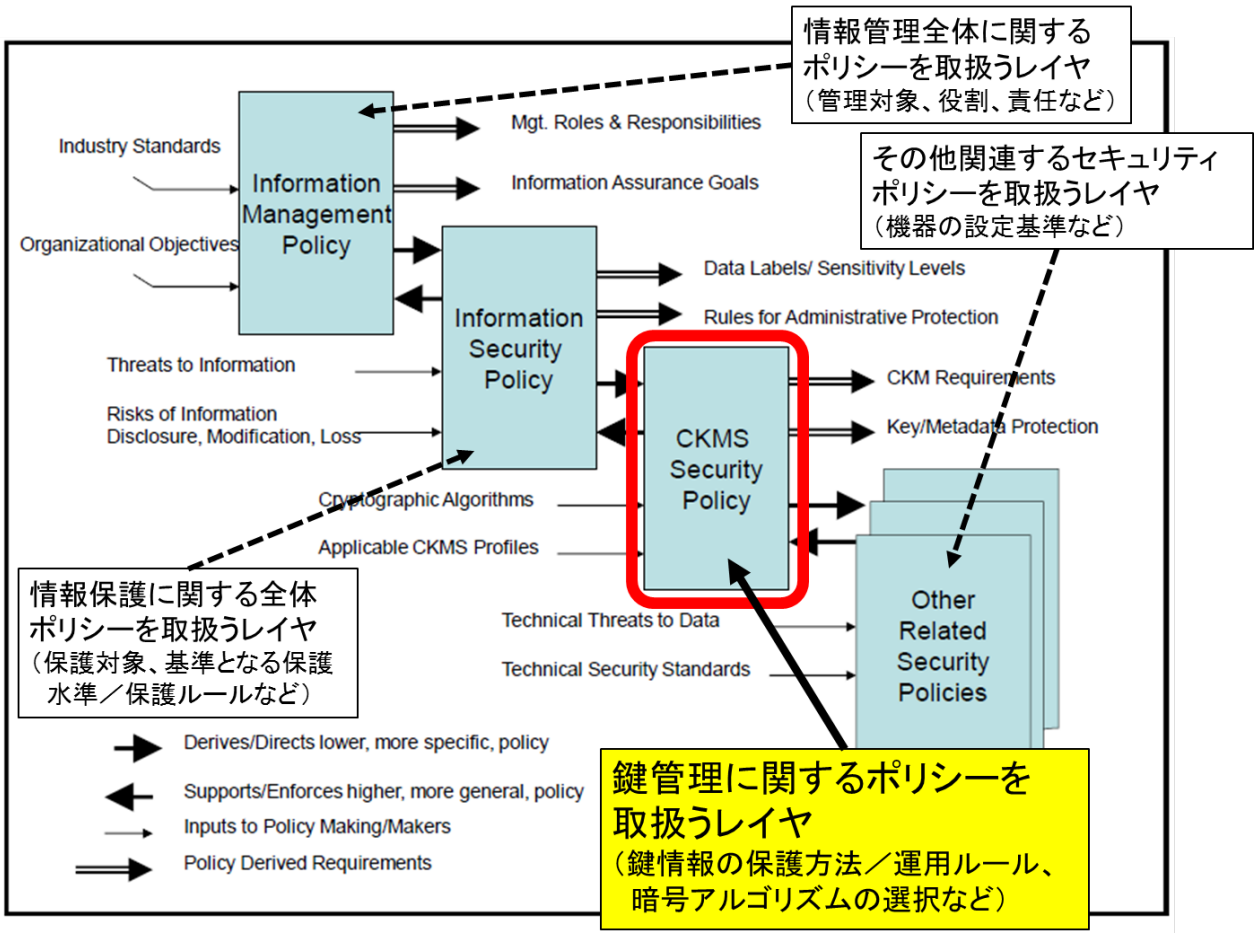


図 3　　セキュリティポリシーの関連図（SP800-130 より）

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 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 2-5 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。

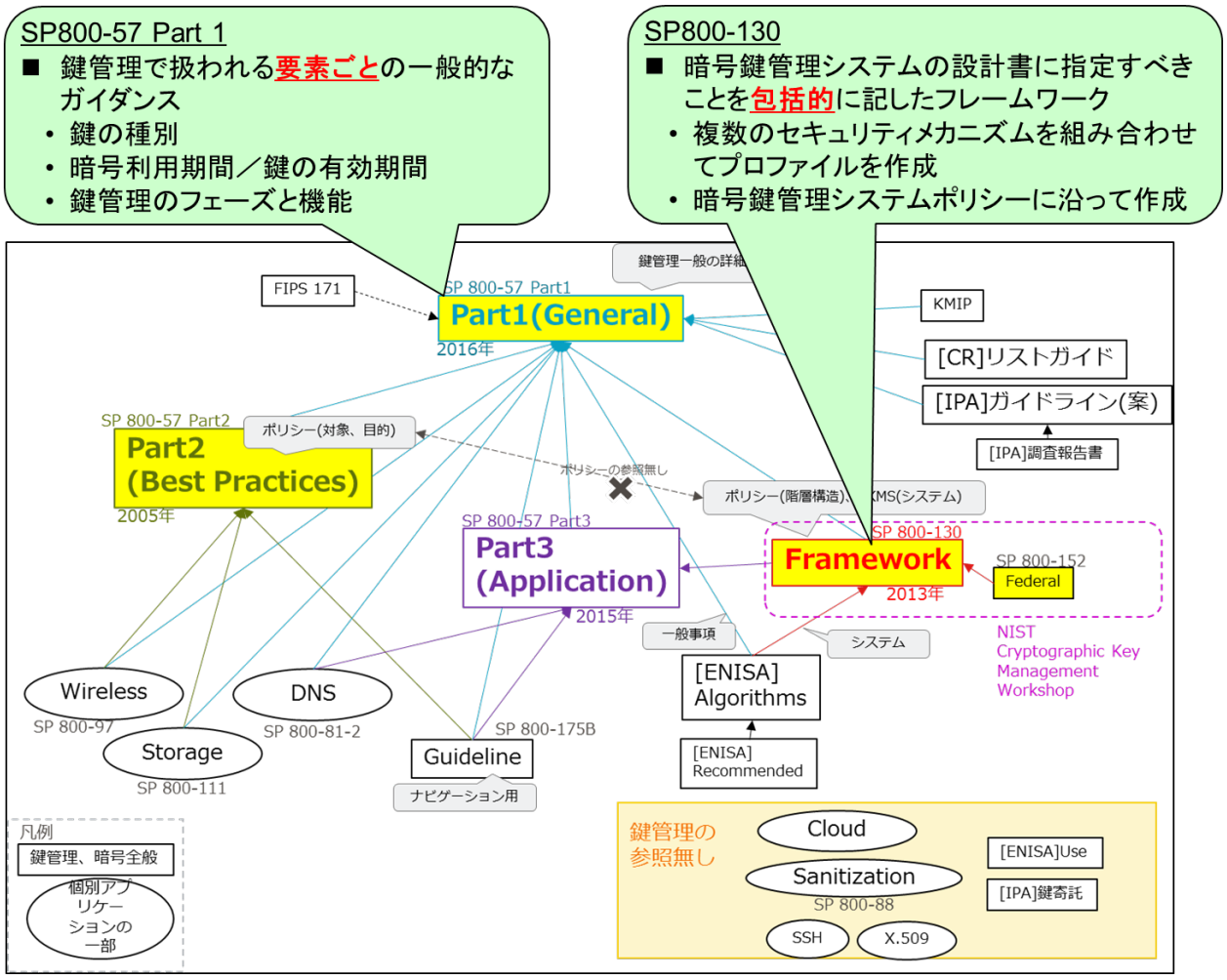


図 2-5 各文献における暗号鍵管理に関する他文献への参照関係

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、鍵の種別、暗号利用期間／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、CKMS の設計ガイドラインとしては、SP800-57 ではなく、SP800-130 が参照されている。

2.5.1 SP800-57

暗号アルゴリズムの不適切な選択によるセキュリティ確保は困難であり、プロトコルやアプリケーションの実際のセキュリティにほとんど（あるいは、まったく）寄与しないことから、SP800-57 Recommendation for Key Management は、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作成された。

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）をモデルとした鍵管理基盤（KMI）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、認証局の暗号鍵管理ポリシーである CP/CPS 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／システム利用者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、無線回線経由の鍵更新(OTAR)鍵管理メッセージ(KMM)、DNSSEC、暗号化ファイルシステム(EFS)

2.5.2 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 の必要な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

2.5.3 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、

> **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

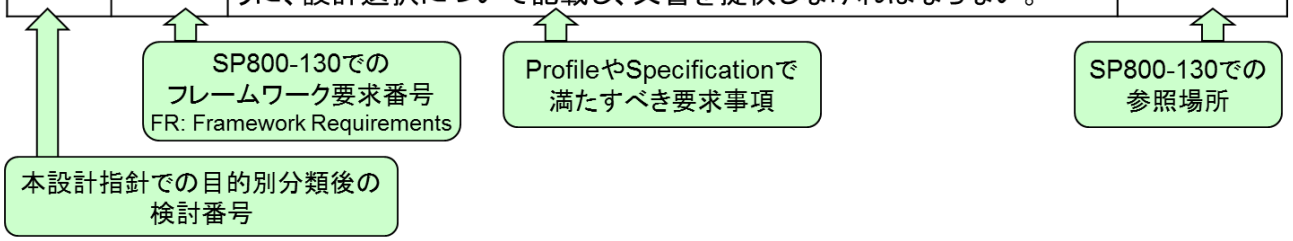


図 3-1 Framework Requirements の表示例

- 「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項目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

- **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、今回設計する CKMS が取り扱う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。

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、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、対象外の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判断の対象外としてよい。

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暗号鍵及びメタデータ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 では暗号鍵及びメタデータ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。

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。

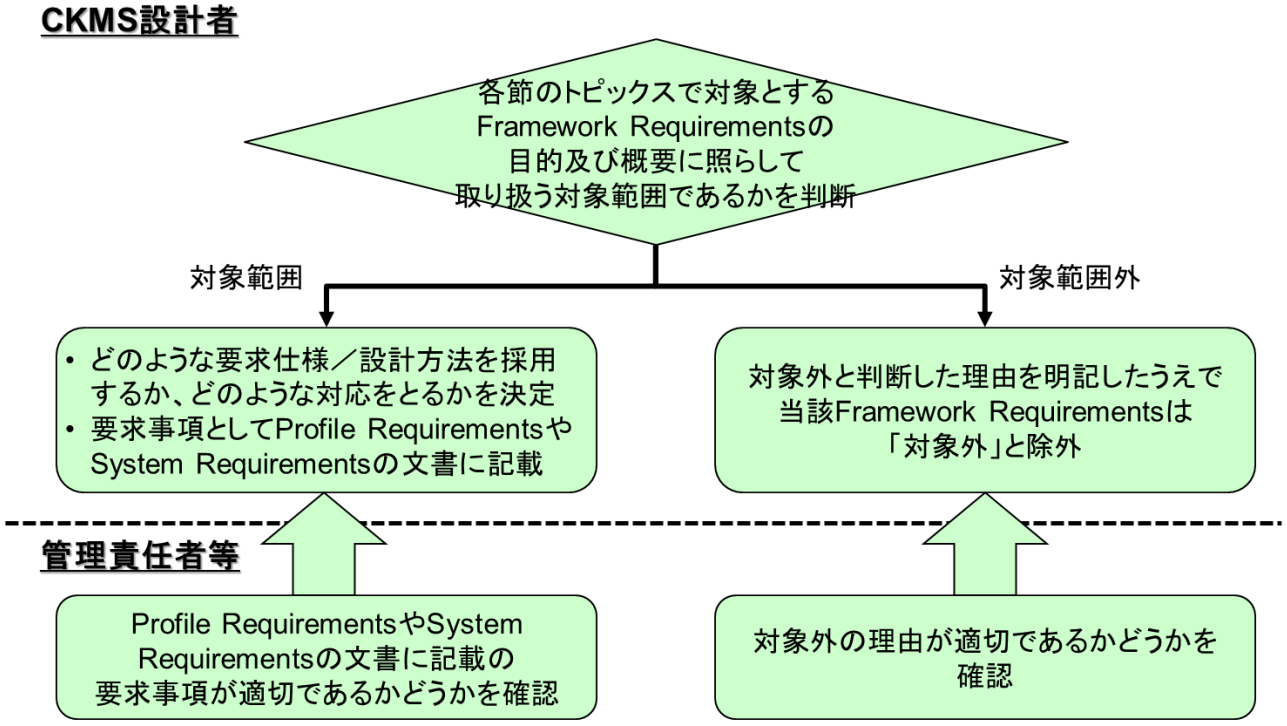


図 3-2　本設計指針の活用方法

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である。概要は以下の通り。

① CKMS 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暗号鍵及びメタデータの保護のためのルールを規定する。

- CKMS によって使用される全ての暗号鍵及びメタデータの機密性、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
  - ✧ 鍵ライフサイクル全体にわたってカバーされる。
  - ✧ 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（情報管理ポリシーや情報セキュリティポリシー）と整合している必要がある。
- CKMS 設計文書には、セキュリティ機能が CKMS セキュリティポリシーをサポートするためにいつどのように使用されるのかを記述すべき。
  - ✧ CKMS 設計が 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するのは CKMS を使用する組織の責任
- ポリシーを守ることに責任を持つ役員・従業員がポリシーを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。

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

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、それらを意識すべきである。

- CKMS 設計は、他のどのセキュリティポリシーが、CKMS の適切でセキュアな運用を実行するために要求されているのかを記載すべき。

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フォームの形で規定されている場合には注意を要する。

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である。概要は以下の通り。

① 機微な情報を管理するために、CKMS の特定機能として、個人の説明責任（Personal accountability）が情報管理ポリシー等の要求事項に記載される場合がある。

- 個人の説明責任についてのポリシーは、機微な情報（＝暗号鍵とメタデータ）にアクセスする各個人に自らの行動に対する説明責任を負わせる。
- CKMS 設計者は、CKMS が個人の説明責任をサポートすることを意図するかどうかを決定すべき。

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、CKMS の特定機能として、以下の保証（のいずれか）が情報管理ポリシー等に記載される場合がある**

- 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	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

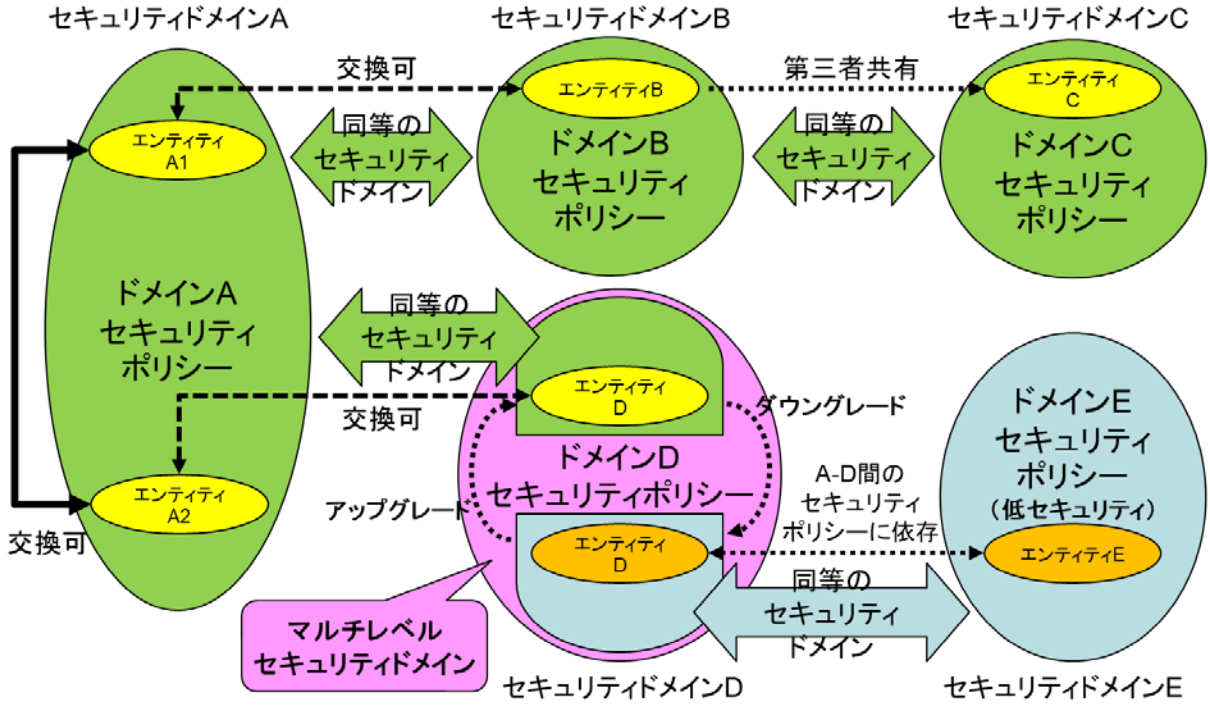
4.3　セキュリティドメインポリシー

本節は、SP800-130 の 4.9 節に記載されている事項である。概要は以下の通り。

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。
  - ➢ 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、それらのエンティティはドメインセキュリティポリシーが要求する保護を提供しながら暗号鍵及びメタデータを交換できる。
  - ➢ セキュリティドメインの例は、公開鍵証明書を発行する公開鍵基盤（PKI）。
- ドメインセキュリティポリシーは、時々、改訂又はアップデートされることが望ましい。

- 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、交換した鍵及びメタデータ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。



① **特定のドメイン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それが実行される前にドメイン管理者が必ず承認するべき。**

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
A.14	FR4.26	CKMS 設計は、異なるドメインセキュリティポリシーと異なるアプリケーションをサポートするように、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.15	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

4.3.2 異なるセキュリティドメイン間での鍵情報の交換

① エンティティが同じセキュリティドメインに属していない場合、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する。

- ドメイン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

② 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に、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になる。

- オーソリティは、あらゆる潜在的な危殆化の影響を軽減するために、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に対して、鍵情報の交換を制限又は拒否することもある。
- 共有した鍵やメタデータが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）と認識するべき。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
A.16	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.17	FR4.16	CKMS 設計は、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.18	FR4.17	CKMS 設計は、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.19	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.20	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.21	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

4.3.3 マルチレベル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。
  - 異なったセキュリティレベルで運用しているエンティティからの鍵やメタデータを処理できるようになる。

① エンティティは、2 つの保護レベルを区別し、異なる保護レベルの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。

② 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、リスクなしには実行できない。

- アップグレードは、低レベルドメインからの鍵やメタデータのソース及び信頼性（authenticity）に信頼と確信を持っている場合にのみ行うべき
- ダウングレードは、送付する鍵やメタデータが低レベルのセキュリティしか要求しないとの確信を持つべき

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である。概要は以下の通り。

- CKMS における役割には以下のようなものがある（ただし、以下は例であり、これだけに限らない）。

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）

① **責任者／管理者／運用者／利用者（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必要な、鍵とメタデータを管理する一連の機能へのアクセスが提供されるべきである。**

- 複数の個人にそれぞれの役割が割り当てられることも、1 人の個人に複数の役割が割り当てられることもある。
- ある役割に関しては、同時に両方の役割（例：監査と運用）が割り当てられる人がいないように分離されるべき。
- 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。

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／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である。概要は以下の通り。

4.5.1 構築環境

- 構築環境

① **CKMS は、暗号鍵及びメタデータを保護、管理及び確立するために設計されたポリシー、手続き、デバイス及びコンポーネントの一式として記述できる。**

✧ “コンポーネント（component）”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

✧ “デバイス（device）”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可能性がある。

✧ いくつかのトランザクションは信頼される第三者機関によるタイムスタンプを必要とするかもしれない。

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。

- セキュリティプロトコルでの CKMS 視点での実現目標
  - 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、静的鍵（static key）及び一時鍵（ephemeral key）の安全な生成、配付、保管及び保護

① CKMS を運用するネットワーク視点での実現目標

- 以下の点を踏まえ、通信バックボーンを形成するネットワークへの負の影響を最小化するような設計する。
  - 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

- 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。

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

- 以下の潜在的なユーザニーズについて検討したうえで設計する。
  - 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 セキュアな処理、データ保管、及び通信へのニーズ増大の負荷に耐えるためのパフォーマンス及びスケーラビリティを設計に組み入れる。

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 相互運用の必要性

① 相互運用しようとするシステムへの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きる。

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 CKMS の使用にあたって最も重大な制約は、習熟していないユーザに対してシステムがもたらす難しさにある。

- ほとんどのユーザは暗号セキュリティエキスパートではなく、使用しているセキュリティ機能の目的を理解していないかもしれないことに留意すべき
- セキュリティは一般に製品の最優先の目的ではないので、透過的なセキュリティが望ましい
- 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は以下の通り：
  - ✧ 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
- ユーザの技量に適応したユーザインタフェースは、新規で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

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	FR3.11	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
A.49	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.50	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

4.5.5 市販製品の活用

① 市販製品は、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。

- 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た市販製品は、どの顧客の要求も完全には満たさないかもしれない
- CKMS の市販製品の設計に拡張性と拡充性を許容しサポートするべき

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 で使用される市販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、市販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市販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である。概要は以下の通り。

① 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

- 標準への適合は、製品の製造期間（time-to-production）又は実装の作業時間（time-to-operation）も削減させ得る。
- 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
  - ✧ 市場に製品が出回る前に実装の誤りを発見し除去するのに有用

② CKMS が使用される地域、州、及び国家の法律、ルール及び規制に従うべき

- 国際的に使用できるように設計される場合、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

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、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である。概要は以下の通り。

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されるべき。

- 将来的により強力なアルゴリズム及び鍵長に移行するための移行戦略を用意するべき
- 円滑な移行には、少なくとも 2 つのアルゴリズム（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
- 異なった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アルゴリズムを上回らないことにも留意すべき
  - ✧ 可能な限り素早く移行することが最善

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 **CKMS は長期にわたるセキュリティライフタイムを持つように設計され実装されるべきであるため、技術の進歩に起因する潜在的な脅威を考慮すべき。**

- **暗号アルゴリズムに対する新しい攻撃**
  - ✧ 最終的には、暗号アルゴリズムを完全に更新又は置き換える必要があるかもしれない
  - ✧ 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更新ができるような方法で暗号モジュール内に実装すべき

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 の副のハッシュ関数）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**
  - ✧ 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
  - ✧ 一旦広く使用されるようになると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が多い

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 デバイスに対する新しい攻撃**
  - ✧ 認可されない当事者が外部から 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すべき

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

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である。概要は以下の通り。

① 機微なデータを保護するための鍵を使用するエンティティに暗号鍵を提供するために、システムをどのように構築できるかを記述する

- CKMS が取り扱う各鍵タイプの利用用途、暗号鍵の生成場所及び生成方法、保管中及び配送中の暗号鍵の保護方法、及び暗号鍵が配送されるエンティティのタイプの概略を示すべき

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) それぞれの鍵タイプの用途 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 d) 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、鍵やメタデータの保護方法 e) 配送時の鍵やメタデータの保護方法 f) 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タイプ（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 鍵情報のライフサイクル

本節は、SP800-130 の 6.3 節に記載されている事項である。概要は以下の通り。

① CKMS 設計者は、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。

- 鍵情報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。

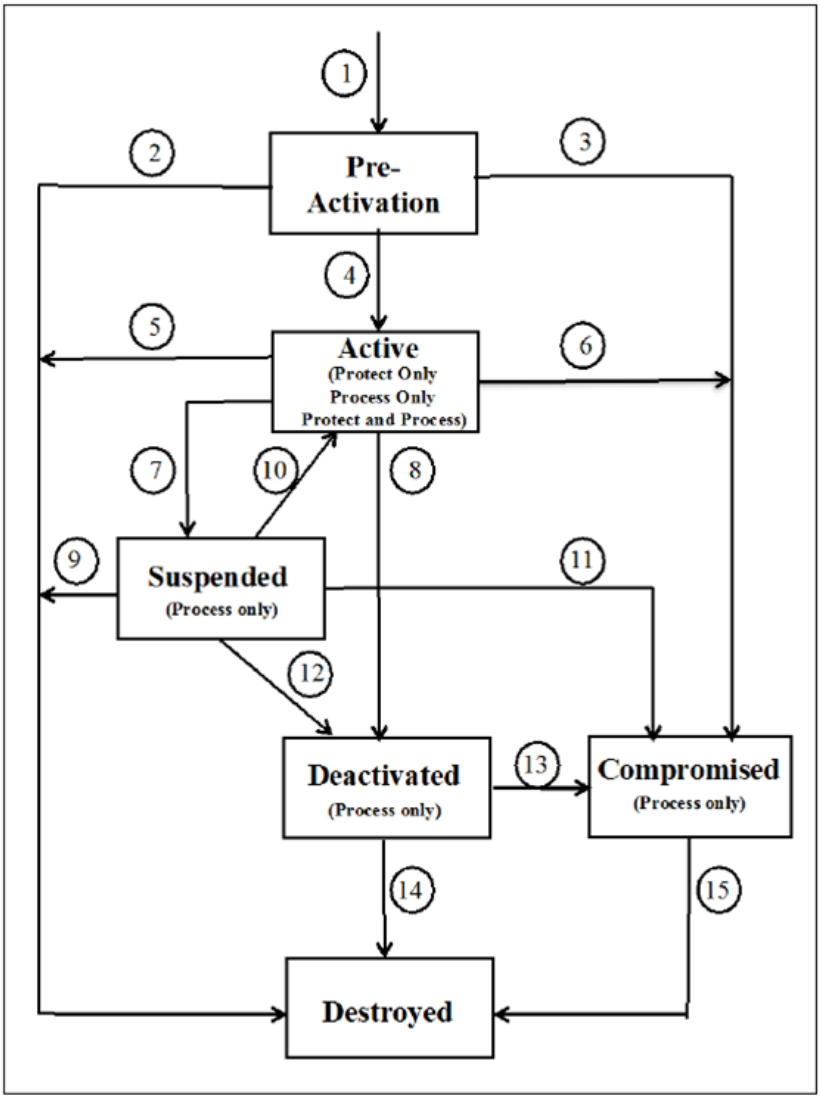


Figure 3: Key state and transition example.

【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

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

5.3 鍵情報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である。概要は以下の通り。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 節に分離して記載してある。

① 暗号鍵及びメタデータに対する管理のために実行される機能の全体像

- 本節に挙げるような、暗号鍵及びメタデータの生成、変更、置き換え、及び破壊の機能を持っているべき
- 呼び出しエンティティの認証（authentication）と認可（authorization）はアクセスコントロールシステムによって実行される。
- 暗号鍵及びメタデータの入力／出力に当たって、完全性、ソース認証（source authentication）、機密性について適用される処理がある場合がある。

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

- 暗号鍵の活性化前（Pre-activation）状態から活性化（Active）状態への遷移（④）を提供

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

- データへの暗号学的保護を実際に提供
  - 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 検証を含み得る
  - 暗号モジュールの内部で実行されるべき

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

- 暗号鍵の非活性化（Deactivate）状態への遷移（⑧、⑫）を提供。非活性化の契機は、日時、使用回数、保護したデータ量などがある。
- 活性化と非活性化の間の時間は暗号有効期間（cryptoperiod）と見なされる。
  - 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では、そのポリシーでカバーされるデータを保護するために使用されるあらゆる鍵タイプについて最大許容の暗号有効期間を記載すべきである。

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 暗号鍵の一時停止機能及び再活性化機能

- 暗号鍵の一時停止（Suspended）状態への遷移（⑦）、及び活性化（Active）状態への遷移（⑩）を提供
  - ✧ 以下の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
- 「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

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
B.13	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.14	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.15	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.16	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.17	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

⑥ 鍵失効機能

- 確立された暗号鍵の暗号有効期間（cryptoperiod）より前にその鍵の認可された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（Compromised）状態への遷移（③、⑥、⑪、⑬）を提供

- ✧ 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）暗号利用期間満了」起因かによる。
- ✧ 過去に保護された情報の処理のための使用に対しても認可されず、セキュリティは保証されない。

- ➢ 暗号鍵は多くの理由によって失効させられるので、暗号鍵（非対称鍵と対称鍵の両方）を速やかに置き換える能力と、依拠する当事者（その鍵を使用する者）に危殆化／失効を通知する能力を備えているべき
- ➢ 鍵失効メカニズムは以下を考慮すべきである：
  - 失効情報の適時性に対する依拠する当事者の要求事項
  - 依拠する当事者の計算及び通信能力の限界
  - インフラコストの考慮

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
B.18	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.19	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

⑦ 暗号鍵及びメタデータの破壊機能

- ➢ 暗号鍵の破壊（Destroyed）状態への遷移（②、⑤、⑨、⑭、⑮）を提供
- ➢ 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
  - ✧ バックアップストレージメディアが使用されている場合、メディア内の暗号鍵を破壊する手段を用意すべき

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

- 典型的には、暗号鍵と対になる暗号アルゴリズムの仕様に依存する。
- 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／鍵アップデート機能

- 鍵導出機能：
  一部が秘密であるような他の情報（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。
  - ✧ 鍵確立プロトコルでは互いの共有秘密（shared secret）から共有鍵を導出
- 鍵アップデート機能：
  鍵導出によって「元鍵（original key）」から「別鍵（another key）」を導出し、導出した「別鍵」で「元鍵」を置き換えるプロセスを実行する。
  - ✧ 元鍵とアップデート方法を知っている敵対者は、将来にわたるあらゆる時期のアップデート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可能性がある。

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、鍵を導出又はアップデートするために使用される全てのプロセス、及び鍵が導出又はアップデート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、鍵の導出又はアップデート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

- 対称鍵及びそのメタデータに対するテストを実行する。

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

- 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のある程度の保証を提供する。
- ある種の公開鍵暗号アルゴリズムの公開ドメインパラメタについて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。
- トラストアンカーなしでは信頼されない公開鍵についての信頼は、依拠するエンティティが信頼する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確立する。

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 トラストアンカーストアの管理機能

- トラストアンカーなしでは信頼されない他の公開鍵についての信頼を確立するために使用する。
  - ✧ トラストアンカーの完全性は CKMS のセキュリティにとって極めて重要

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] 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 公開鍵の更新機能

- 新しい有効期間を持った「同じ公開鍵」を含む新しい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サブジェクト公開鍵に対する新しい有効期間を確立する。
  - ✧ 与えられた公開鍵の更新期間の合計は、その鍵の暗号有効期間（cryptoperiod）を超えてはならない。

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が更新できるかを明記しなければならない。	6.4.7 節
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。	6.4.7 節

⑭ 所有者登録機能

- セキュリティエンティティ（すなわち、個人（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。
  - ✧ 典型的には、エンティティの秘密鍵、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。
  - ✧ セキュリティを保ちながら（なりすましの脅威から保護しながら）完全に自動化することは困難である。

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

- 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する鍵ペアの所有者であることの保証を得ることを望む、公開鍵を受領したエンティティによって使用される

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（又は鍵ペア）の検証機能

- プライベート鍵に対してある種のテストを実行し、その仕様を満たすことの保証を提供する。
  - 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 鍵とメタデータの関連付け機能

- 暗号鍵に関連付けられているいくつかのメタデータ要素がある場合、それらを関連付けるとともに、その関連付けを提供する保護メカニズムも決定しなければならない。
  - 関連付けには、暗号学的プロセス又は信頼プロセス（trusted process）を使用する

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

- 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。
  - ✧ 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

- 暗号鍵に関連付けられたメタデータを削除する。
  - ✧ 削除権限が付与されているものに限定される

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 鍵メタデータのリスト化機能

- エンティティに認可されている鍵メタデータをリスト化することを当該エンティティが実行できる

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である。概要は以下の通り。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 節に分離して記載してある。

① 保管中の暗号鍵及びメタデータのセキュリティ

- CKMS ストレージシステムは、あらゆるデータが格納されるより前に、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検証すべき
- 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及びアクセスコントロールも必要とする。
  - ✧ 鍵暗号化鍵の階層のトップレベルでは、典型的には物理的に保護されなければならない鍵が存在する。
  - ✧ 暗号鍵に訂正不能なエラーの混入が検出された場合、その鍵は使用すべきでない。
- CKMS は、認可されたユーザのみが保管された鍵にアクセスできるようにすべき
  - ✧ CKMS はある種のアクセスコントロールシステム（ACS）を備えているべき
- CKMS は、価値のあるデータの復元を提供するのに必要な鍵のバックアップ、アーカイブ、及び復元のための手段を搭載すべき

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回復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 運用中の暗号鍵及びメタデータの保管機能

- 運用中の暗号鍵及びメタデータの保管には、暗号鍵やメタデータをメディアへ移すことを含む。
- 暗号鍵及びメタデータが暗号モジュールの外部に保管されるときに、それらは物理的又は暗号学的に保護されるべき。

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 暗号鍵及びメタデータのバックアップ機能

- 鍵及びメタデータのバックアップには、鍵やメタデータを安全な設備へコピーすることを含む。
  - オリジナルの（運用中の）コピーが喪失、改変、又はその他の理由で利用不能状態になったときにそのコピーを復元できるようにする

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 **暗号鍵及びメタデータのアーカイブ機能**

- 鍵やメタデータのアーカイブには、鍵やメタデータを必要なときに復元できるように、それらを長期保管用のストレージ設備に安全に配置することを含む。
  - ✧ アーカイブされた鍵やメタデータは物理的又は暗号学的に保護されなければならない。
  - ✧ 鍵及びメタデータをアーカイブすることは、通常、アーカイブされた鍵やメタデータを新しい保管メディアに移動するための手段を要求する。
- アーカイブされた鍵やメタデータに提供される保護の継続性はアーカイブ鍵の暗号有効期間が期限切れになるときに考慮される必要がある。
- 鍵やメタデータのアーカイブ又は破壊を実行するとき、鍵やメタデータが法律や規則で要求される期間利用可能であるように、適用される法律や規則を考慮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.55	FR6.50	CKMS 設計は、どのように、どこで、どのような状況で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有効期間（cryptoperiod）の期限切れ後に、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 **暗号鍵及びメタデータの復元機能**

- 前もってバックアップ、アーカイブ又は保管された鍵やそのメタデータのコピーを取得することを含む
- 鍵やメタデータは、復元のための全てのルールが満たされ検証された後に、認可されたエンティティ（例えば、その所有者又は信頼されるエンティティ（trusted entity））によって復元する。

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である。概要は以下の通り。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 節に分離して記載してある。

① 鍵確立機能

- 2 つ又はそれ以上のエンティティ間で鍵をセキュアに共有するプロセスで、方法として以下の 2 つがある。
  - 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、その鍵及び（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、その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 鍵配送における暗号鍵及びメタデータのセキュリティ

- 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とアクセスコントロールを必要とする
  - 暗号鍵に訂正不能なエラーの混入が検出された場合、使用前に新しい又は訂正された暗号鍵を確立すべき
  - 機密性保護のためには、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
- 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も保護されるべき
- 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その鍵が来たことの保証が必要である。

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。	6.6.1 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、配送される鍵マテリアル（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 鍵合意における暗号鍵及びメタデータのセキュリティ

- 鍵合意プロセスに参加する各エンティティは、典型的には他方のエンティティ識別子（ID）の保証を必要とする。

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

- 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鍵を確立したことの確認をするために使用する。

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
B.68	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

B.69	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

⑤ 暗号鍵の提供のために開発されている有名な鍵確立プロトコル

- 以下に有名な鍵確立プロトコルをいくつか挙げる
  - ✧ 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）
- 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

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である。概要は以下の通り。

① 鍵情報の破損に対する BCP 対策

- 破損した暗号鍵及びメタデータは、破損が検知されたときには可能な限り速やかに置き換え又は訂正すべき
- 破損した暗号鍵、又は破損したメタデータが付随した暗号鍵がデータを保護するために使用されていた場合、機微なデータの喪失又は危殆化が結果として起こる可能性があるため、セキュリティ上の結果を評価すべき
- 暗号鍵がバックアップもアーカイブもされていなかった場合、新しい暗号鍵で置き換えなければならず、元の暗号鍵で保護された情報は失われる可能性がある
  - ✧ 重大な災害は、多数の運用中の暗号鍵及びメタデータの喪失又は破損を引き起こす可能性がある

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である。概要は以下の通り。

- 全ての潜在的なセキュリティ問題を防止する完璧な CKMS を設計することは困難あるいは不可能ですらある。
  - CKMS は危殆化及び改ざんを検知するように設計すべき
  - 望ましくない影響を軽減し、適切な当事者に危殆化を警告し、かつ危殆化又は改ざんが検知された際にセキュアな状態に回復する（又は回復を手助けする）ようにする
- 危殆化が検出されたときの回復手順：
  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

- 鍵タイプ及び鍵の用途に依存し、以下のセキュリティ処理（service）に対する結果をもたらし得る：
  a) 機密性の喪失
  b) 完全性の喪失
  c) 認証の喪失
  d) 否認防止の喪失
  e) これらの喪失の組み合わせ
- 危殆化した暗号鍵によって保護されたデータに対しても、同じセキュリティ処理（service）及び場合によっては他のセキュリティ処理（service）の喪失をもたらす可能性が高い
- 使用するそれぞれの暗号鍵に対して暗号有効期間（cryptoperiod）又は利用制限（usage limit）を設定することで、検出されない暗号鍵の危殆化の露出を制限すべき
  - ✧ 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有効期間を実用的な最短期間にしておくことがよい
  - ✧ 鍵導出鍵とマスタ鍵も定期的に変更すべき

- 暗号鍵の危殆化は、その鍵が保護する他の多くの暗号鍵の危殆化をもたらす可能性があるため、暗号鍵の危殆化の影響を最小化するように CKMS を設計することが重要
  - ✧ 危殆化した暗号鍵だけでなく、その危殆化した鍵のセキュリティに依存する他の暗号鍵も、可能な限り速やかに置き換えるべき

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

- メタデータ要素及びその使われ方に依存して、メタデータ要素の危殆化は、鍵の危殆化又は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
- メタデータの完全性を容易に検証できるように、それらの関連付けられた鍵と暗号学的に結びつけられるべき

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

- 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
  - a) セキュリティ障害を起こす人間の能力を最小化する
  - b) セキュリティ障害を起こした行動を隠蔽する人間の能力を最小化する
  - c) 誰が、又は何がセキュリティ障害を起こしたのかを決定することを補助する
  - d) 障害のネガティブな結果を軽減する
- 情報セキュリティポリシー及び CKMS 機能に基づいた回復手続きで、以下のような対応をすべきである。
  - e) システムの完全なシャットダウン
  - f) 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
  - g) 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
  - h) 危殆化した暗号鍵へのフラグ付け
- 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の対応策がある

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である。概要は以下の通り。

① **CKMS によって管理される暗号鍵を使用する暗号アルゴリズムは、攻撃者（になりそうな人）が回避したり解読したりすることが実行不可能であるような保護レベル（セキュリティ強度）を提供するようにすべき**

- 暗号アルゴリズムは、データに対して 3 つの主要なタイプの保護を提供するために使用される：機密性、完全性、ソース認証（source authentication）。
  - ✧ CKMS によって、ライフサイクル全体にわたって管理及び保護されている暗号鍵を使用する
- 暗号アルゴリズムの中身（例えば、アルゴリズム、暗号鍵、及びメタデータ）を改ざんと窃取から物理的及び論理的に保護している暗号モジュール（ハードウェア、ソフトウェア、ファームウェア、又はその組み合わせ）内に存在しているべき
  - ✧ 暗号モジュールは CKMS の一部で、暗号鍵、メタデータ、及びユーザデータに対して暗号学的保護を提供できる

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[1]）で表現され、鍵長[2]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

[1] 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

[2] 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 4 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[3]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 曲線パラメータ P-xxx を利用）の ECDH のこと
- ECDSA-xxx：鍵長が xxx ビット（例えば NIST 曲線パラメータ 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

6.2 CRYPTREC 暗号リスト

CRYPTREC では、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、「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。

[3] 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である。概要は以下の通り。

- 暗号鍵は、特性と用途（＋オプション）に応じて分類される

特性	公開（Public）
	プライベート（Private）
	対称（Symmetric）

オプション	静的（Static）
	一時的（Ephemeral）

用途	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）

- SP800-130 で分類する鍵タイプは以下の通り。

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
  - 暗号鍵は、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と関連付けられなければならない
    - ただし、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
- メタデータの各ユニットはメタデータ要素と呼ばれる
- 暗号鍵と選択されたメタデータ要素の間の信頼関係は、暗号鍵管理機能を実行するために CKMS によって必要とされることが多い
  - 暗号鍵とメタデータとの信頼関係は、暗号学的結び付き（cryptographic binding）あるいは信頼プロセス（trusted process）によって確立する
    - 暗号学的結び付き（cryptographic binding）は、暗号鍵及び関連付けられたメタデータ要素に適切な暗号検証機能を適用することで検証
    - システムに保管されたメタデータは、ストレージの場所と特性に依存して、暗号鍵との信頼関係を物理的セキュリティ手段又は暗号学的手段を利用して保持され得る
- SP800-130 で取り上げる典型的なメタデータ要素は以下の通り。

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である。概要は以下の通り。

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、保護方針などを記載する

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、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） 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	6.2.2 節

		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である。概要は以下の通り。

① 暗号鍵、メタデータ及びそれらの信頼関係の保護方法についてのメタデータ要素内に含まれている情報を保護するために、暗号メカニズムが利用される場合に以下を実施する

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）（上記の項目 s）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: 上記の項目 g）を参照 ii. 鍵パラメタ: 上記の項目 i）を参照 iii. 鍵識別子: 上記の項目 b）を参照 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）（上記の項目 t）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（上記の項目 u）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

② 暗号鍵、メタデータ及びそれらの信頼関係の保護方法についてのメタデータ要素内に含まれている情報を保護するために、7.3.1　信頼プロセス（非暗号メカニズム）が利用される場合に以下を実施する

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）（上記の項目 s）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）（上記の項目 t）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（上記の項目 u）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である。概要は以下の通り。

- CKMS のセキュリティは、暗号鍵及びメタデータの管理機能の適切なシーケンスと実行に依存する。
  - 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、機微な暗号鍵及びメタデータへのアクセスをコントロールするために動作する。

8.1.1 アクセスコントロールシステム

① 暗号鍵及びメタデータ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、及び全ての適用可能な制限が満たされていることを保証することが必要

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 暗号モジュールの目的は、セキュリティ機能の完全性と暗号鍵及びメタデータの保護

- 暗号モジュールは、暗号ベースのセキュリティ機能を実装するハードウェアやソフトウェア、ファームウェアの集合で表し、暗号境界内の全てを包含する。
- 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及び実装されていない
  - ✧ 暗号化が実行される多くのコンピュータには、通常、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、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
- CKMS は、暗号モジュールを使用して暗号鍵を生成、保管、使用、及び保護すべき
  - ✧ 暗号モジュールセキュリティポリシーに従い、実行するように作られるべき。

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 暗号鍵及びメタデータの暗号モジュールへの入出力のための機能及び制限

- 暗号モジュールは、通常平文鍵への物理的保護を提供し、平文鍵が露出しないようにする。
  - ✧ 人間が平文の対称鍵又はプライベート鍵を見る必要が全くないような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。
  - ✧ 暗号モジュールから出力される前に、鍵に必要な暗号学的保護を適用すべき
- 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。

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、平文での秘密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、平文での秘密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、平文での秘密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への対策

- 暗号モジュールの危殆化はその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い、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
- 暗号モジュールは、物理的に（暗号モジュール内の暗号鍵へ直接アクセスする）、又は非侵襲的手段（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）によって危殆化され得る

- ✧ 物理的保護を提供するために、認可されないアクセスが許可されない場所、又は深刻な危殆化が起こる前に認可されないアクセスが速やかに検出されるような場所で、暗号モジュールは運用されるべき
- ✧ 非侵襲攻撃に対する保護を提供するため、そのモジュールの使用を信頼されるユーザに制限するか、又はこのような特定の種類の攻撃を防止するようにそのモジュールを設計すべき

➢ 実際の危殆化又は危殆化の疑いがあった後には、通常運用に戻る前に、そのモジュールをセキュア状態に再確立すべき

- ✧ 修理又は交換の後に、セキュリティ状態の確認とともに運用機能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.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 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、入力の正確さと（場合によっては）セキュリティが人間に依存する

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 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の一手法

- 機能を実行する前に、*n* 個中 *k* 個のエンティティが ACS の認証・認可されることを要求する
- 高度に機微な機能のために利用されるべき

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 鍵分割を必要とする場合の一手法

- *n* 個の分割鍵のそれぞれが n 個の信頼されるエンティティの一つに割り当てられ、そのうち *k* 個のエンティティが参加することに同意しない限り鍵が構成できない
- 多くの他の鍵を保護し、その危殆化が深刻な災害をもたらすようなルート鍵又はマスタ鍵を確立するために使用
  - バックアップのために、平文形式で分割鍵を CKMS に入力又は CKMS から出力される場合に使うことが多い

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である。概要は以下の通り。

- 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。
  - 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

① ベンダテスト：

- ベンダが自ら実施するテスト
  - 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：

- 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をテスト
  - 個々のデバイスの内部機能自体をテストするわけではなく、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（device-under-test）と保証ベースラインデバイス（assured-baseline device）が異なる組織によって独立に設計され実装されているか、テスト対象デバイス（device-under-test）の設計及び実装の関係者と独立して働く個人によって独立に設計され実装されていれば、このテストはより信用できる

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：**

- 暗号アルゴリズム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が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
  - ✧ 機能テスト：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
  - ✧ セキュリティテスト：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
- 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
  - ✧ ペネトレーションテストのスコープには、人的、設備及び手続きを含むべき
  - ✧ ペネトレーションテストチームによるあらゆる発見に対して、最初の配備の前に対処すべき

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：**

- デバイス又はシステムに対する特定の利用環境（例えば、温度範囲及び電圧範囲）を仮定することが多い。
  - ✧ その環境用に構築され、その環境の範囲内でテストされる。
  - ✧ 範囲外の環境で使用されると、セキュアな運用が失われる可能性がある。

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 **自己テスト：**

- 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テストする。

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：**

- 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参加者数が劇的に増加したときにデバイス又はシステムがどのように反応するかを見極めるためのテスト

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：**

- 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の第三者によるテスト
  - ✧ 暗号標準及び推奨事項への製品適合の検証プログラムが代表例

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である。概要は以下の通り。

① **暗号モジュール障害発生時におけるバックアップ及び回復**

- 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な、組み込まれたテスト機能を備えるべき
- 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

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である。概要は以下の通り。

9.1.1 物理セキュリティコントロール

① 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が窃取及び改ざんから保護されるように物理的に保護されるべき

- コンポーネントとデバイスのセキュリティの重要性に応じて、物理的に保護するためのメカニズムが選択されるべき

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

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

- OS セキュリティ

① コンピュータシステム上でセキュリティ機能が正しく実行されることを保証するためのセキュリティコントロールが存在すべき

- 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

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
F.03	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.04	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	8.2.1 節

		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 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.05	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

- デバイスセキュリティ

  ② 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。

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
F.06	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.07	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

- マルウェアからの保護

  ③ 通信、データ、ファイル等を保護されていないネットワークを通して受信する CKMS デバイスは、受信した情報へのマルウェアに対する対策をすべき

✧ 保護されていないネットワークを通して情報を何も受け取らない、又は全ての情報が強力に（例えば暗号学的に）認証されている場合には、マルウェア対策の重要性は下がるかもしれない

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
F.08	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.09	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

- 監査

④ 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

✧ 監査システムの完全性が保証できるように、改ざんから保護されるべき

✧ 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機能も備えるべき

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
F.10	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.11	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.12	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.13	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

⑤ 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ますます有用

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
F.14	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 ネットワーク化された CKMS デバイスは、ファイアウォールと侵入検知及び防御システムの組み合わせを使用して保護されるべき

- 境界コントロールデバイス（ファイアウォール、フィルタリングルータ、VPN、IDS、及び IPS など）は、物理的にセキュアな場所に配置されるべきであり、セキュアな操作に必要なユーザアカウントとネットワークサービスのみを設定するべき

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
F.15	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.16	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.17	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.18	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である。概要は以下の通り。

① 構成管理：

- 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

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
F.19	FR9.10	CKMS 設計は、以下を明記しなければならない： a) 構成制御の下に置かれているデバイス（ソースコード、スクリプト実装、実行コード、ファームウェア、ハードウェア、文書、及びテストコードを含む） b) 構成制御の下でコンポーネント及びデバイスへの認可された変更だけが行われたことを保証するための保護要求事項（例えば、形式的認可及び適切な記録保持）	9.8.1 節

② セキュアな配付：

- CKMS で使用される製品の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る）が必要である

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
F.20	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：

- CKMS 開発環境及びメンテナンス環境は、物理的、人的、及び IT 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。
  - ✧ 開発ツールを自動的に信頼すべきではない

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
F.21	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：**

- CKMS は、迅速かつセキュアな方法で欠陥を検知、報告及び修正する能力を持つべき

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
F.22	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.23	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.24	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.25	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.26	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である。概要は以下の通り。

① **完全セキュリティアセスメント：**

- 配備前又は配備時に完全セキュリティアセスメントを実施すべき。
- 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, 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

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
F.27	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.28	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.29	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.30	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.31	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.32	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.33	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.34	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.35	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 定期的セキュリティレビュー：

- 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主張どおりに整備され運用していることを保証するために、定期的に検査を実施
  - 前回のセキュリティレビューからのシステム変更箇所の検査
  - 定期的な機能テスト及びセキュリティテストを実行

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
F.36	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.37	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.38	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.39	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 セキュリティアセスメントの追加：

- 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
  - 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
- 累積的なシステム変更が著しい場合、完全セキュリティアセスメントを実施すべき

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
F.40	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.41	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：

- セキュリティを維持し強化するために、CKMS は適切に更新され、堅牢化ガイドラインに従ってレビューされテストされるべき。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

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
F.42	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である。概要は以下の通り。

① 物理セキュリティの危殆化からの回復

- 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
- セキュリティ関連ロジックが暗号モジュールの外部に存在する場合、そのロジックの完全性もまた保護されるべき
- 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
  - CKMS セキュリティポリシーに規定された通りに、適切なエンティティに侵害について通知すべき
  - 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又は追加している可能性がある

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
F.43	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.44	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
F.45	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.46	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.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からの回復

- 監視ユーティリティによる検出又はイベントログに表示され、重要なファイルに改ざんがあったとき、これらのファイルは、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ファイルを使って置き換えるべきである。
- 広範囲に改ざんがソフトウェアになされた場合、そのソフトウェアは後述する災害発生時の BCP／復旧対策に記載され手順を準用すべきである。

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からの回復

- CKMS の保護を提供するネットワークセキュリティコントロールの危殆化は CKMS そのものの危殆化につながり得る
- 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。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
- 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べき

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 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である。概要は以下の通り。

- CKMS の障害が情報へのアクセスの妨害又は停止につながるかもしれないという追加のリスクを伴う

① 設備への物理的損害発生時におけるバックアップ及び回復

- バックアップ及び回復設備は、保護されるデータ及び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
- 風水害はどちらも環境リスクであり、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

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）の停止時におけるバックアップ及び回復

- 通常運用時及び非常時において、全ての電子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べき

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バックアップ及び回復

- 高可用性を保証するために、冗長な通信設備が設置されることも多い。

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 システムハードウェア障害発生時におけるバックアップ及び回復

- 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を最小限に抑えることが望ましい
- ハードウェア障害からの回復の容易さ及びスピードとコストとの間でトレードオフの傾向がある
- 同じ故障を引き起こすことがないようにするため、可能な限り、バックアップシステムが基幹システムからの独立性を持っていることが不可欠

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 システムソフトウェア障害発生時におけるバックアップ及び回復

- 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へのエラー混入」がある

- ✧ 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
- ✧ コードにエラーが混入する障害は可能な限り速やかに検知されるべき

➢ 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できるようにすることが推奨される

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エラーの混入を検知するために、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

発行日　2019 年 7 月 12 日　ドラフト版

発行者

・〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
独立行政法人 情報処理推進機構
（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