CRYPTREC Report 2018

平成 31 年 3 月

独立行政法人情報処理推進機構
国立研究開発法人情報通信研究機構

「暗号技術活用委員会報告」

目次

はじめに

本報告書は、総務省及び経済産業省が主催している暗号技術検討会の下に設置され、独立行政法人情報処理推進機構及び国立研究開発法人情報通信研究機構によって共同で運営されている暗号技術活用委員会の 2018 年度活動報告である。

暗号技術活用委員会は、電子政府の安全性及び信頼性を確保し国民が安心して電子政府を利用できる環境を整備するため、暗号利用に関するセキュリティ対策の推進、暗号技術の利用促進に向けた環境整備を主に担当する委員会である。2015 年度に、暗号技術活用委員会の活動目的の軸足を、「暗号技術を主軸とした検討」から「情報システムのセキュリティ確保に寄与する暗号技術等に係る成果物の提供」に移すことに定義し直し、2016 年度から新たな目的に基づいて活動を開始した。

暗号技術活用委員会では、実運用とセキュリティ確保の両面の観点から、運用面でのマネジメントに関するガイドライン（以下、運用ガイドライン）の作成に注力している。

今年度から、2017 年度に実施した「鍵管理に関する運用ガイドライン作成に向けた事前調査」の結果を踏まえ、鍵管理に関する運用ガイドラインの整備を開始した。これは、暗号技術の安全な利用にあたっては、安全な暗号アルゴリズムの選定だけでなく、安全な鍵管理が重要であるにも関わらず、日本では今までに鍵管理について公的にまとめられたガイドラインがなかったことの問題意識に基づいている。

今年度は、鍵管理を考えるうえでのあるべき構造を整理し、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検討した。さらに、その結果を踏まえて、「暗号鍵管理システム設計指針（基本編）」のドラフト案作成を進めているところである。ドラフト案は CRYPTREC シンポジウム 2019 での公開を予定している。

来年度以降も、「暗号鍵管理システム設計指針（基本編）」の正式発行をはじめ、運用ガイドラインの拡充を図っていくことが、ひいては情報システムのセキュリティ確保の底上げ、暗号の普及促進・セキュリティ産業の競争力強化に繋がり、より安心・安全な情報化社会の実現に結び付くことを期待している。

末筆ではあるが、本活動に様々な形でご協力下さった委員の皆様、関係者の皆様に対して深く謝意を表する次第である。

暗号技術活用委員会 委員長　松本 勉

本報告書の利用にあたって

本報告書の想定読者は、一般的な情報セキュリティの基礎知識を有している方である。例えば、電子署名や GPKI[1] システム等、暗号関連の電子政府関連システムに関係する業務に従事している方などを想定している。しかしながら、個別テーマの調査報告等については、ある程度の暗号技術の知識を備えていることが望まれる。

本報告書は、2018 年度の暗号技術活用委員会の活動内容と成果概要を記述した。

2017 年度以前の CRYPTREC Report は、CRYPTREC 事務局（総務省、経済産業省、国立研究開発法人情報通信研究機構、及び独立行政法人情報処理推進機構）が共同で運営する下記の Web サイトから参照できる。

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

CRYPTREC 報告書

本報告書ならびに上記 Web サイトから入手した CRYPTREC 活動に関する情報の利用に起因して生じた不利益や問題について、本委員会及び事務局は一切責任をもっていない。

本報告書に対するご意見、お問い合わせは、CRYPTREC 事務局までご連絡いただけると幸いである。

【問合せ先】 info@cryptrec.go.jp

[1] GPKI：Government Public Key Infrastructure（政府認証基盤）

委員会構成

暗号技術活用委員会（以下「活用委員会」）は、図 1 に示すように、総務省と経済産業省が共同で運営する暗号技術検討会の下に設置され、独立行政法人情報処理推進機構（IPA）と国立研究開発法人情報通信研究機構（NICT）が共同で運営している。

活用委員会は、電子政府の安全性及び信頼性を確保し国民が安心して電子政府を利用できる環境を整備するため、暗号利用に関するセキュリティ対策の推進、暗号技術の利用促進に向けた環境整備を主に担当する委員会である。

なお、活用委員会と連携して活動する「暗号技術評価委員会（以下「評価委員会」）」も暗号技術検討会の下に設置され、NICT と IPA が共同で運営している。

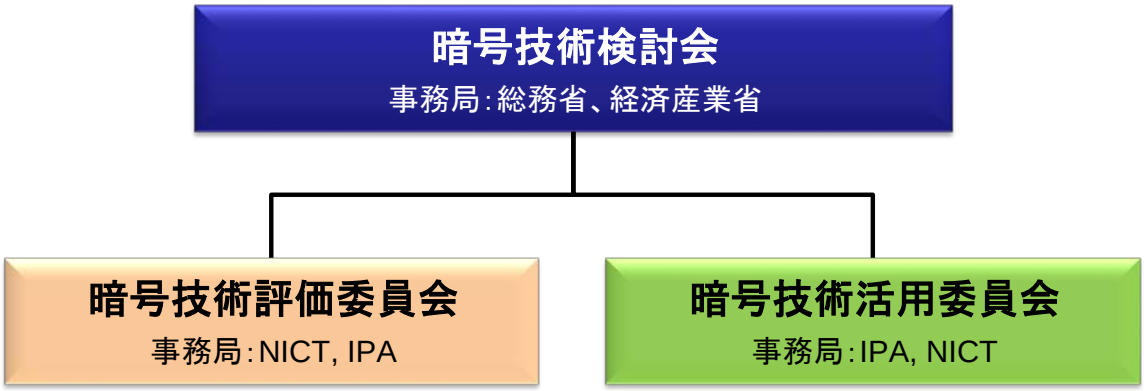

図 1　2018 年度の CRYPTREC の体制

委員名簿

暗号技術活用委員会

委員長	松本 勉	横浜国立大学 教授
委員	上原 哲太郎	立命館大学 教授
委員	垣内 由梨香	マイクロソフト株式会社 セキュリティプログラムマネージャー
委員	菊池 浩明	明治大学 教授
委員	須賀 祐治	株式会社インターネットイニシアティブ シニアエンジニア
委員	杉尾 信行	株式会社NTT ドコモ
委員	清藤 武暢	日本銀行 主査
委員	手塚 悟	慶応義塾大学 特任教授
委員	寺村 亮一	株式会社NDIAS マネージャー
委員	松本 泰	セコム株式会社 マネージャー
委員	三澤 学	三菱電機株式会社 主席研究員
委員	満塩 尚史	内閣官房 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 客員研究員
委員	山口 利恵	東京大学 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

オブザーバー

内田 稔	内閣官房内閣サイバーセキュリティセンター
久保山 拓	内閣官房内閣サイバーセキュリティセンター
高木 浩光	内閣官房内閣サイバーセキュリティセンター
徳永 竜一	内閣官房内閣サイバーセキュリティセンター
岡田 崇志	個人情報保護委員会事務局
小高 久義	総務省 行政管理局
上東 孝旭	総務省 情報流通行政局[2018年7月まで]
守屋 潤一	総務省 情報流通行政局[2018年7月まで]
豊重 巨之	総務省 サイバーセキュリティ統括官室[2018年8月から]
遠藤 琢	総務省 サイバーセキュリティ統括官室[2018年8月から]
三島 崇	経済産業省 産業技術環境局
稲垣 良一	経済産業省 商務情報政策局

飯山 貴啓	経済産業省 商務情報政策局
荒木 美敬	外務省 大臣官房 情報通信課[2018 年 7 月から]
中元 隼	外務省 大臣官房 情報通信課[2018 年 7 月から]
魚住 拓摩	外務省 大臣官房 情報通信課[2018 年 7 月から]
前田 哲宏	防衛省 整備計画局
岡野 孝子	警察大学校
相原 大輔	警察大学校
古谷 元紀	警察大学校

事務局

独立行政法人情報処理推進機構（江口純一[2018年7月まで]、瓜生和久[2018年7月から]、時田俊雄、小暮淳、神田雅透、橋本徹、兼城麻子[2018年10月まで]、菅野淳[2018年11月から]）

国立研究開発法人情報通信研究機構（宮崎哲弥、盛合志帆、吉田真紀、大久保美也子、篠原直行、黒川貴司、金森祥子）

第1章　2018 年度活動内容

1.1. 活動内容

2017 年度に実施した「鍵管理に関する運用ガイドライン作成に向けた事前調査」の結果を踏まえ、今後 2 年間かけて鍵管理に関する運用ガイドライン（鍵管理ガイドライン）の整備を開始した。

2018 年度は、「鍵管理に関する運用ガイドライン作成に向けた事前調査」の結果を踏まえて、(1)鍵管理に関するフレームワークの検討、ならびに(2)(1)の検討結果に基づく鍵管理ガイドライン「暗号鍵管理システム設計指針（基本編）」のドラフト版の作成、を実施した。

1.2. 開催状況

2018 年度の活用委員会は 2 回開催された。各回会合の概要は表 1-1 のとおり。この他、鍵管理ガイドラインについての技術検討会合を別途開催した。

表 1-1　2018 年度暗号技術活用委員会　開催概要

回	開催日	議案
第 1 回	2018 年 9 月 6 日	■ 活用委員会活動計画の確認 ■ 鍵管理に関するフレームワークについての検討
技術検討会合	2018 年 12 月 26 日	■ 鍵管理ガイドラインのドラフト素案作成に向けた技術的検討
第 2 回	2019 年 3 月 14 日	■ 鍵管理ガイドラインのドラフト素案の審議 ■ 次期 CRYPTREC 暗号リスト策定に向けた方針についての検討

第2章　成果概要

2.1. 鍵管理に関するフレームワーク（暗号鍵管理システム設計指針）についての検討

鍵管理に関連する代表的なガイドラインの事前調査結果（図 1-1）を踏まえ、以下の調査対象のガイドラインについて、想定読者や目的、及び相互の関連性について、より詳細に調査を行った。

＜調査対象とするガイドライン＞

- SP800-57 Part1 revision4: Recommendation for Key Management, Part 1: General
- SP800-57 Part2 revision1(draft): Recommendation for Key Management, Part 2: Best Practices for Key Management Organization
- SP800-130: A Framework for Designing Cryptographic Key Management Systems
- SP800-152: A Profile for U.S. Federal Cryptographic Key Management Systems

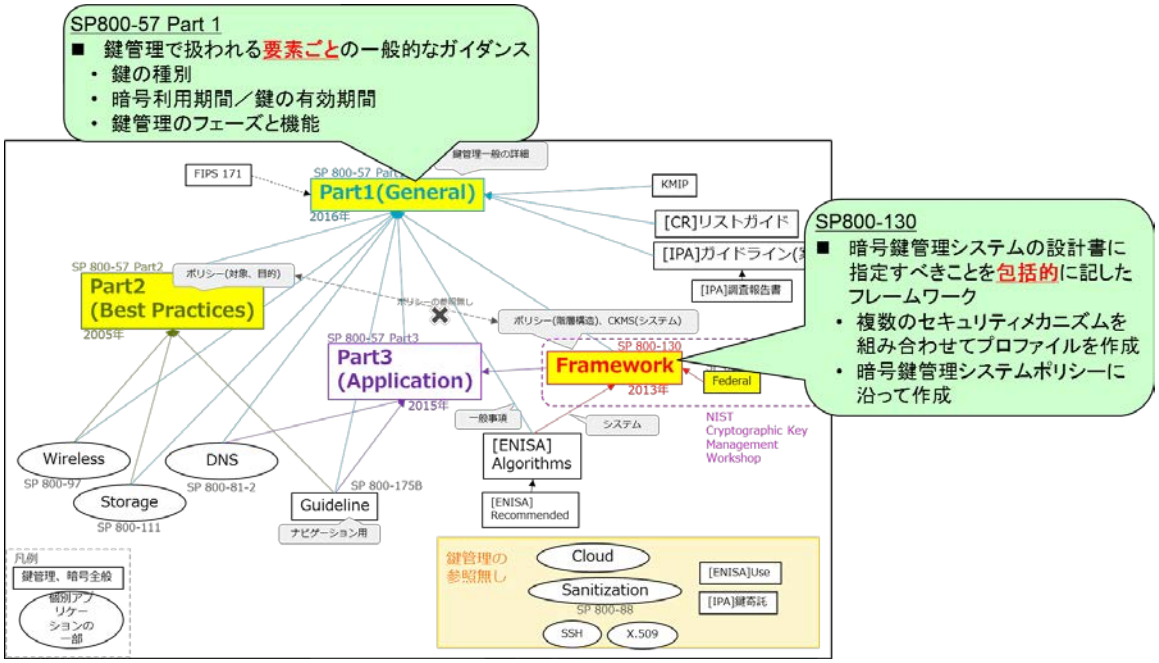

図 1-1　鍵管理に関連する代表的なガイドラインの事前調査結果

各ガイドラインの想定読者や目的は表 1-2 のとおりである。

簡単に言えば、SP800-57 Part 1 では「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、鍵管理のフェーズと機能といった、鍵管理に必要な個々の技術的なトピックスをまとめて取り上げている。

一方、SP800-130 では、あらゆるユースケースにおける暗号鍵管理システムを対象とした「暗号鍵管理システムの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、その思想は暗号鍵管理システムにおける設計・運用方針を明確化させることにある。具体的には、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・運用用件等）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、検討が必要な項目を列挙したものである。

実際、米国では、米国政府システムの暗号鍵管理システムが共通に実現すべき要求事項（設計方針・運用要件等）としてのプロファイルが SP800-152 として作成されている。図 1-2、図 1-3 に示すように、SP800-130 での要求事項である「○○を明記しなければならない」と

いう項目に対して、SP800-152 では具体的に「○○をどう実行する」かという視点で、各項目が対比できるようになっている。

表 1-2　各ガイドラインの想定読者や目的

SP800-57 Recommendation for Key Management	暗号メカニズムの不適切な選択による安全性確保は困難であり、プロトコルやアプリケーションの実際の安全性にほとんどまたはまったく寄与しない。暗号メカニズムを選択・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の提供が目的
Part 1: General	• システム開発者／管理者： 役に立つ汎用的な鍵管理ガイダンス • 暗号モジュール開発者： 具体的なアプリケーションでサポートが必要となる鍵管理特性の理解のための汎用的なガイダンス • プロトコル開発者： 具体的なアルゴリズムスイートによる鍵管理特性の確認や理解 • システム管理者： 構成設定の最適な決定のための推奨
Part 2: Best Practices for Key Management Organization	• システム／アプリケーション所有者： 組織の適切な鍵管理基盤の特定、鍵管理方針の確立、及び鍵管理の実践と計画を規定する際の使用に適合するガイダンス • 特に、暗号鍵の確立と管理の役割を担う連邦政府システムの所有者と管理者向け
SP800-130 A Framework for Designing Cryptographic Key Management Systems	暗号鍵管理システムの設計時に考慮すべきトピックスや対処すべき仕様要求について記載されたフレームワークを提供が目的 • 暗号鍵管理システム設計者： チェックリストとして活用 （カバーすべき全てのトピックに対する対処方法、暗号鍵管理システムに関する全ての観点での検討、暗号鍵管理システム内でのポリシー／コンポーネント／デバイスの選択、決定事項の明示、詳細仕様や理由を含めた全ての決定方針の文書化、等）
SP800-152 A Profile for U.S. Federal Cryptographic Key Management Systems	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連邦暗号鍵管理システムに対する要求事項を明示 • 暗号鍵管理システムの設計者／実装者： 適切なセキュリティサービスや鍵管理機能の選択／実装を支援 • 連邦暗号鍵管理システムの調達者／管理者／サービス利用機関：適切な暗号鍵管理システムの選択を支援

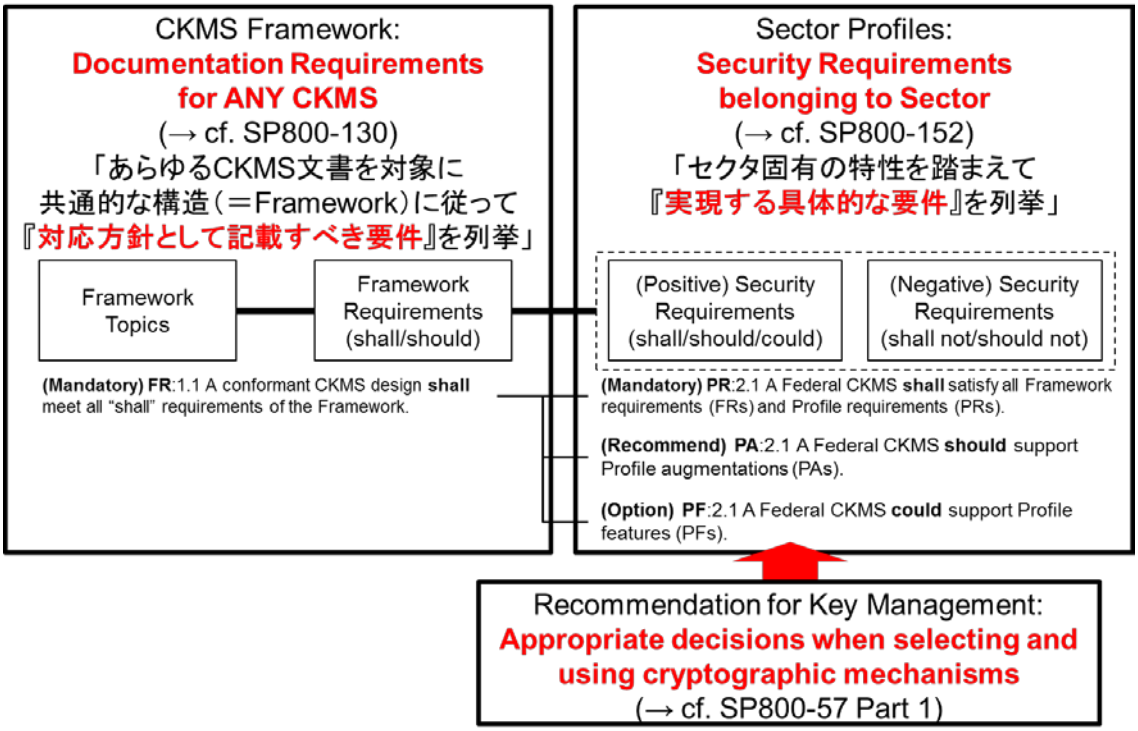

図 1-2 Framework と Profile の関係

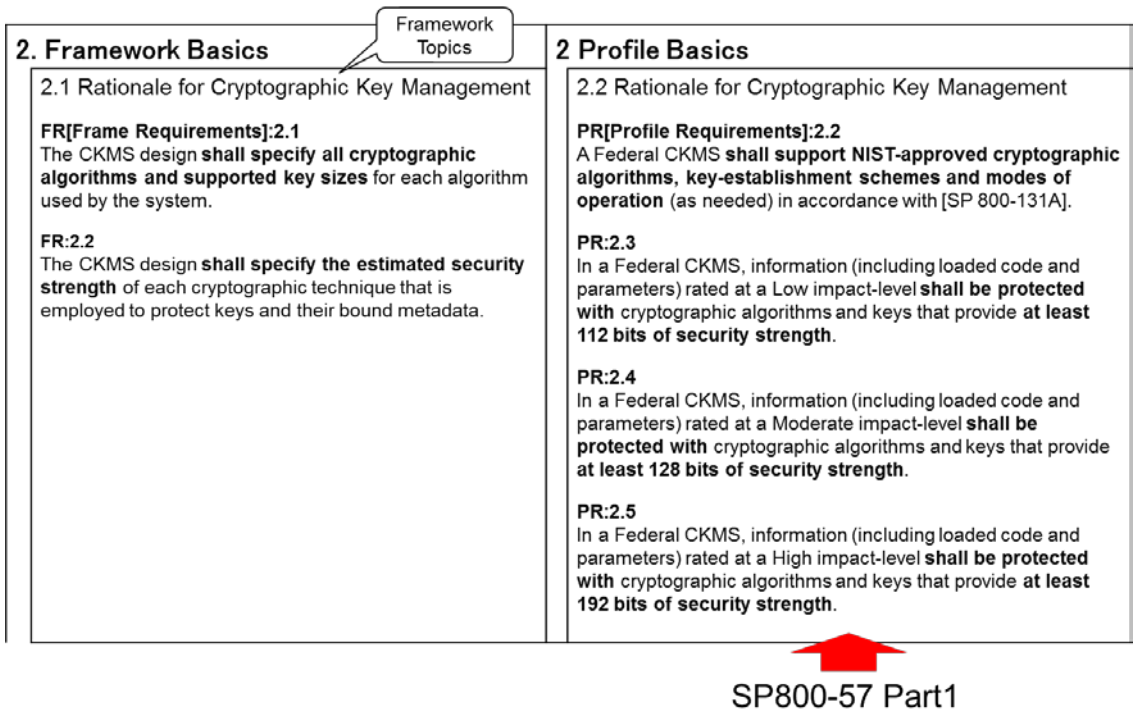

図 1-3 SP800-130:Framework（左）と SP800-152:Profile（右）の関係

これらのガイドラインに記載された内容から、鍵管理を考えるうえでのあるべき構造を図1-4 のように整理し、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。構成要素としては以下の 4 つからなる。

① 「Guidance」: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。例えば、SP800-57 part 1、同 part 3、CRYPTREC 暗号リスト、リストガイド（鍵管理）、SSL/TLS 暗号設定ガイドライン、などが該当する。

② 「Framework Requirements」：あらゆるケースにおける鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として考慮すべき事項を包括的に一覧として取りまとめたもの。SP800-130 が代表例である。あらゆるケースに適用できるように、採用すべき具体的な技術仕様は規定しておらず、あくまで③Profile Requirements や④System Requirements を具体的に検討・設計する際の考え方や検討項目を示す、設計手引書的な位置づけのものである。

③ 「Profile Requirements」：業界（セクタ）固有の特性や環境を踏まえた共通的な条件や設計ポリシーに基づき、①Guidance の技術的根拠を加味して、②Framework Requirements に沿って、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。例えば、SP800-152 は、米国政府システム共通の暗号鍵管理システムとしての要求事項が規定されたものである。

④ 「System Requirements」：③Profile Requirements に適合するように、システム個別の環境／条件を考慮して作成された、実際の暗号鍵管理システムが実現すべき具体的な設計仕様書や運用マニュアル等のこと。システムが依存する環境や条件と①Guidance の技術的根拠の両方を加味して、具体的な技術仕様として取りまとめられる。

暗号技術活用委員会としては、①Guidance に含まれるガイドラインだけでは鍵管理ガイドラインとして不十分であり、②Framework Requirements を扱うガイドラインを作成すべきと判断し、SP800-130 をベースに作業を行うこととした。なお、③Profile Requirements や④System Requirements については、個別の要件や環境等に依存する側面が強くなると考えられるため、各業界等で取り組んでいただくことを期待している。

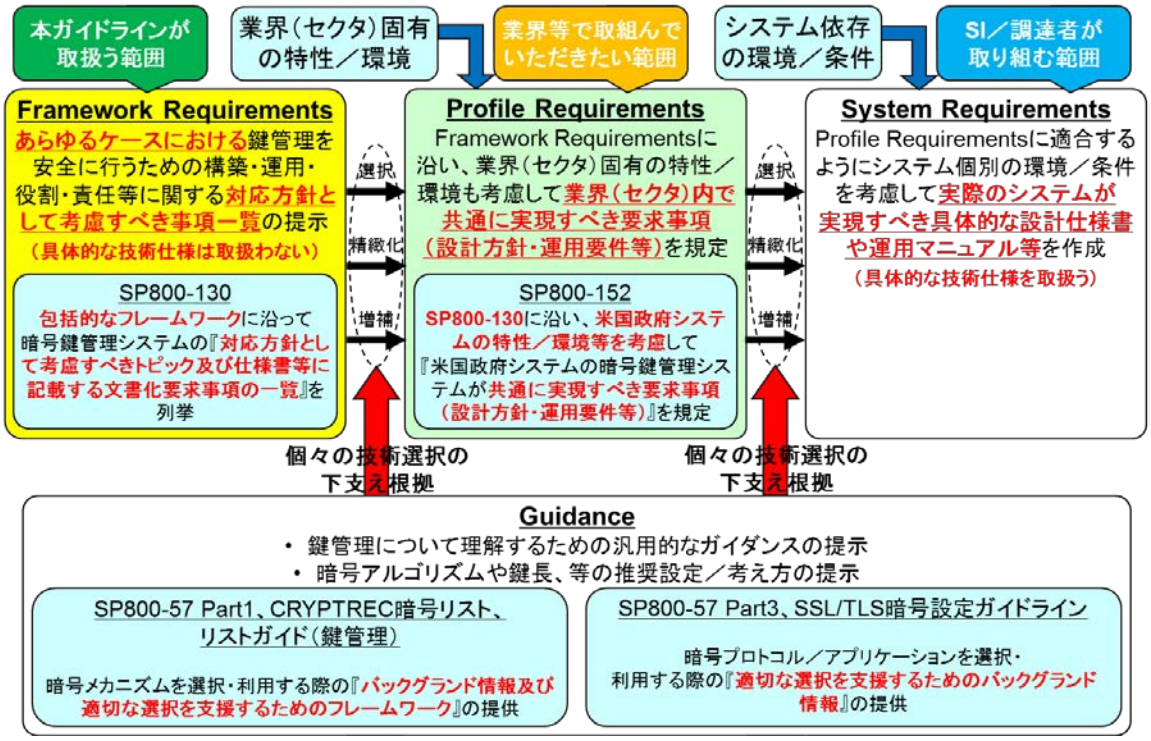

図 1-4　鍵管理を考えるうえでのあるべき構造

2.2. 暗号鍵管理システム設計指針（基本編）のドラフト素案の取りまとめ

SP800-130 では、暗号鍵管理システム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考えれば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、必要な個所を見つけ出すことが難しい。

一方、日本では、今まで SP800-130 のような暗号鍵管理システムの設計指針の基準となる包括的・統一的な鍵管理ガイドラインが作られていないため、「鍵管理」のあり方や考え方が十分に解説されていなかった。その結果、Guidance に含まれるガイドラインを「鍵管理ガイドライン」としてきた経緯もあり、Guidance に記載がある特定の項目（例えば、暗号アルゴリズムや鍵長など）については細かく規定しているのにも関わらず、鍵管理上は重要なのに Guidance が扱っていない項目（例えば、鍵のライフサイクルや安全な鍵の保管方法、危殆化時の対策など）については規定がなかったり抽象的な記述の規定にとどまったりといったことが懸念される。このことは、鍵管理（システム）という視点で見てみると、規定した内容の粒度にバラつきが生じる可能性が大いにあり、システム全体の安全性確保を困難にする原因になると推察される。

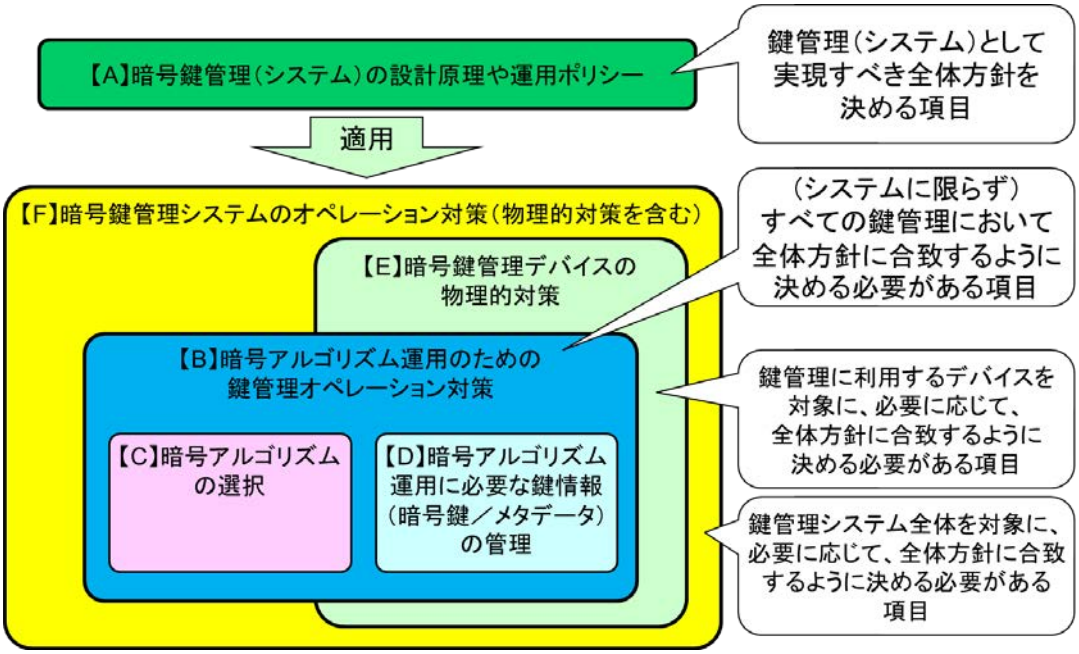

図 1-5　鍵管理における目的

そこで、暗号技術活用委員会では、イントロダクションとして鍵管理のあり方や考え方を解説し、技術的には SP800-130 の理解を深める解説書・利用手引きとして活用するための「暗号鍵管理システム設計指針（基本編）」を「鍵管理ガイドライン」として位置付けることとした。

その方針に基づき、(i) SP800-130 全体の日本語訳を作成するとともに、(ii) SP800-130 に記載されているトピックスや Framework Requirements を『鍵管理における目的』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。具体的には、どのような目的のためにどのような項目を取り扱わなければならないのかを関係性が分かるように、6 つの目的に分類・再構築する方向で、ドラフト素案の取りまとめを行っている（図 1-5、図 1-6 参照）。

2章（フレームワークの基本）：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（目的）：堅牢な暗号鍵管理システム（CKMS）の目的を定義
4章（セキュリティポリシー）：システム構成、及び情報管理、情報セキュリティ、CKMSセキュリティ並びに他の関連するセキュリティポリシーの必要性について記載
5章（役割と責任）：CKMSをサポートする役割と責任を提示
6章（暗号鍵とメタデータ）：CKMSの最も重要な要素（利用可能な鍵とメタデータの定義、及び鍵とメタデータの管理機能、等）を包括的に記載
7章（相互運用性と移行）：相互運用性と将来ニーズに対応するための容易な移行能力の必要性について記載
8章（セキュリティコントロール）：典型的なCKMSに適用されるセキュリティコントロールを記載
9章（テストとシステム保証）：セキュリティテストと保証について記載
10章（災害復旧）：一般及びCKMS特有の災害復旧について記載
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記載
12章（技術的課題）：暗号アルゴリズム、鍵確立プロトコル、デバイス、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記載

	目的	取扱い項目
A	暗号鍵管理（システム）の設計原理や運用ポリシー	セキュリティポリシー
		暗号鍵管理システムの構築環境／利用条件
		将来的な移行対策
B	暗号アルゴリズム運用のための鍵管理オペレーション対策	鍵情報のライフサイクル
		鍵情報のライフサイクル管理機能
		鍵情報の保管方法
		鍵情報の鍵確立方法
		鍵情報の危殆化時の BCP 対策
C	暗号アルゴリズムの選択	暗号アルゴリズムの安全性
D	暗号アルゴリズム運用に必要な鍵情報（暗号鍵／メタデータ）の管理	鍵情報（暗号鍵／メタデータ）の選択
		鍵情報の保護方針
E	暗号鍵管理デバイスの物理的対策	鍵情報へのアクセスコントロール
		セキュリティ評価・試験／システム保証
F	暗号鍵管理システムのオペレーション対策（物理的対策を含む）	暗号鍵管理システム（物理／OS とデバイス／ネットワーク）へのアクセスコントロール
		災害発生時の BCP／復旧対策（バックアップ）

図 1-6　SP800-130 目次と暗号鍵管理システム設計指針（基本編）（ドラフト素案）の対比

2.3. 次期 CRYPTREC 暗号リスト策定に向けた方針についての検討

2022 年度に予定されている次期 CRYPTREC 暗号リスト策定に向けた方針について、暗号技術活用委員会として議論を行ったところ、「策定方針を前提とするのではなく、リストの位置づけから根本的に見直したほうがよいとの意見が多数あった」とのまとめ意見を暗号技術検討会に報告することとなった。

第3章　今後に向けて

鍵管理ガイドラインについては、引き続き作業を行い、CRYPTREC シンポジウム 2019 でドラフト版を公開、2019 年度末に同ガイドラインを完成させる予定である。また、SP800-130 の日本語訳も公開する予定である。

2017 年度に一部改訂した SSL/TLS 暗号設定ガイドラインについては、その後の SSL3.0 利用禁止及び TLS1.3 リリース等を踏まえ、2019 年度に内容を大幅に見直す方針とする。

CRYPTREC Report 2018
(暗号技術活用委員会報告 CRYPTREC RP-3000-2018)

発行日　2019年6月28日 第1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