暗号鍵管理システム設計指針（基本編）概要

情報処理推進機構　セキュリティセンター
セキュリティ技術評価部　暗号グループ
神田　雅透

安全性に違いを感じますか？　それはなぜですか？

鍵そのものの強度の違い

https://www.secom.co.jp/anshinnavi/column/backnumber257.html

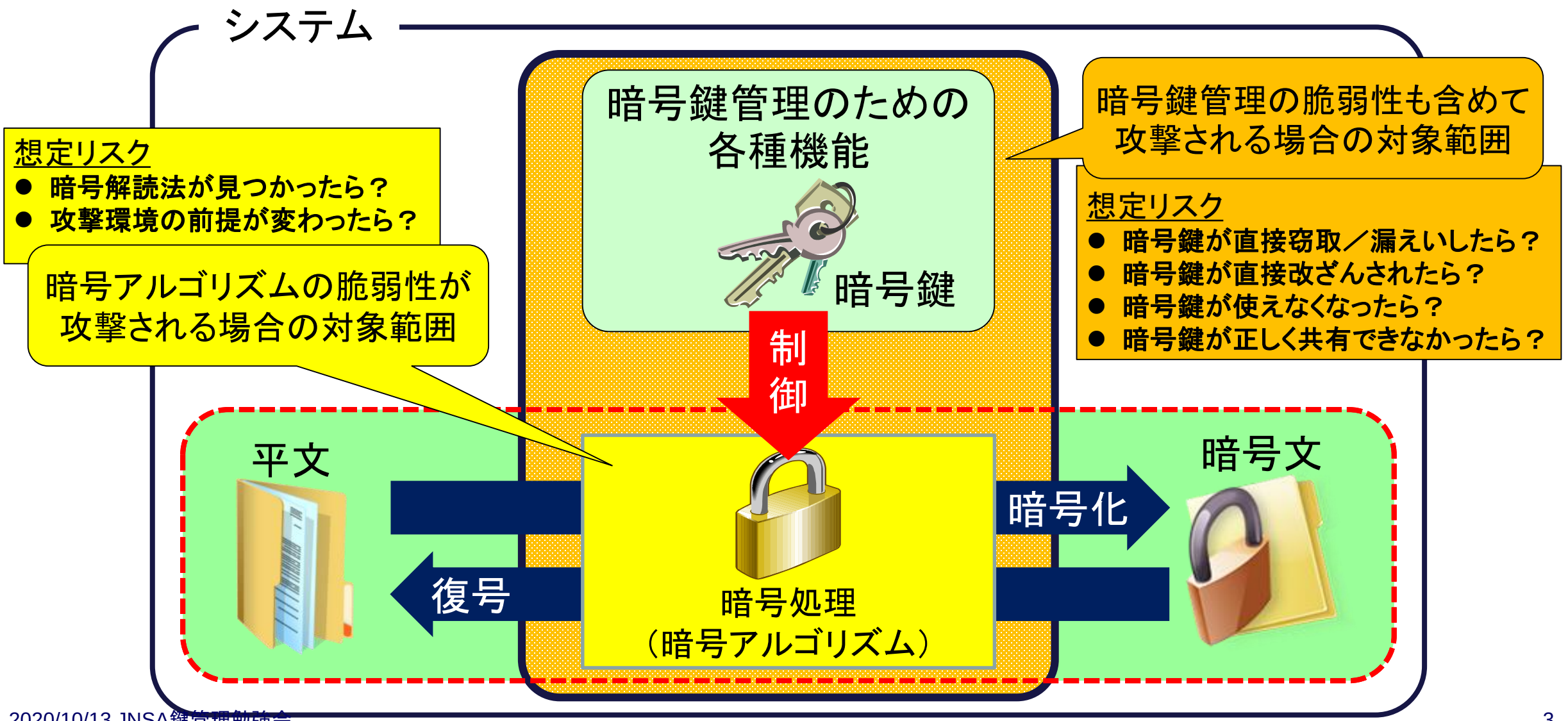
鍵の保管方法（管理）の違い

https://www.pref.yamanashi.jp/police/p_anzen/anzenansin/akisu-sinobikomi.html

「キー ボックス **ドアノブ**」で Google画像検索

「キー ボックス **守衛室**」で Google画像検索

なぜ暗号鍵管理が必要なのか



素朴な疑問

「**鍵管理って重要ですよね。**」のフレーズの

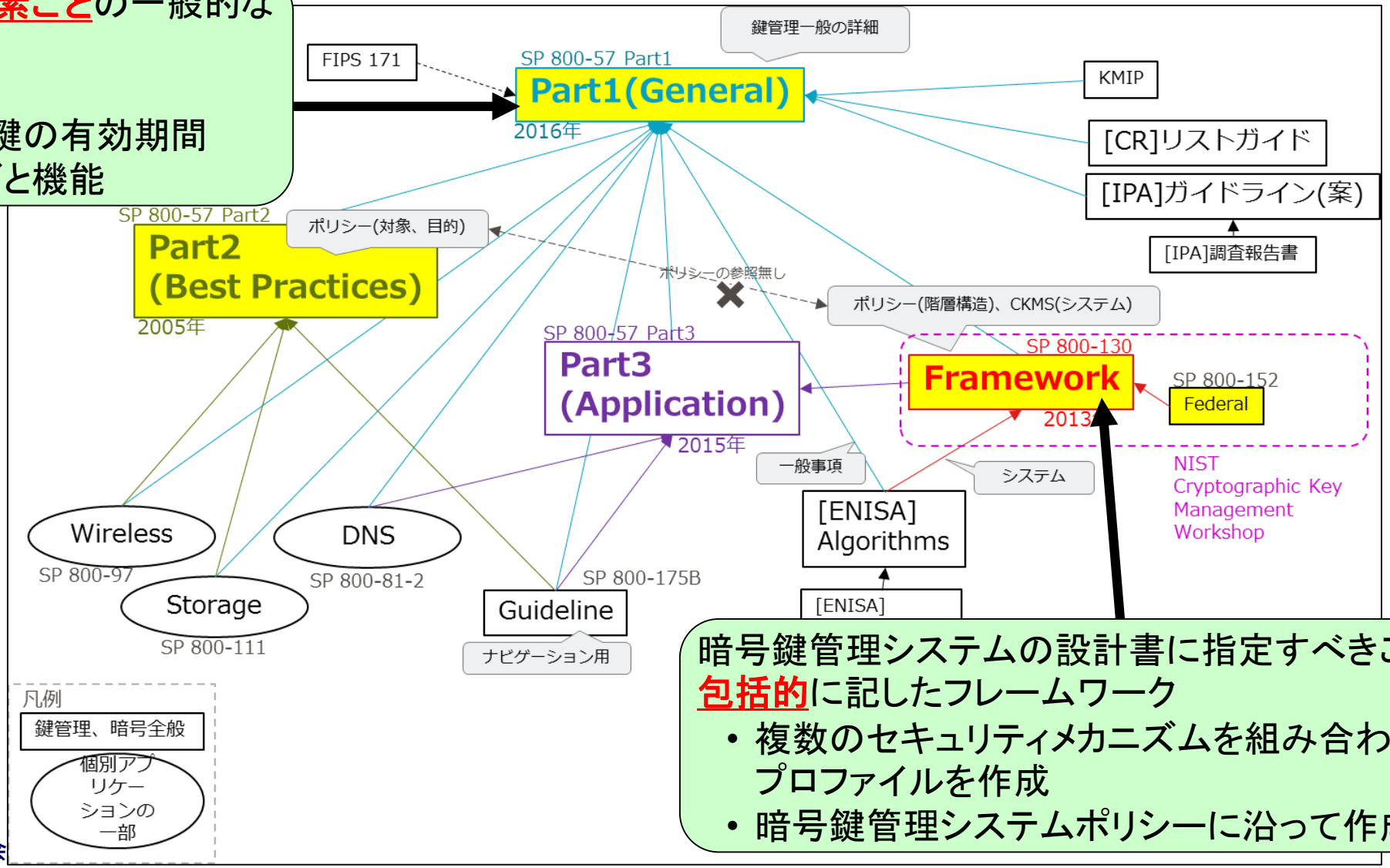
次によく出てくるのは

「**でも、何すればいいのかよく分からないんですよね。**」

鍵管理ガイドラインがないわけではないのに、
昔から言われていることなのに、
「鍵管理って何？」から抜け出せないのはなぜ？

はじめにやったこと
～暗号鍵管理に関連するガイドラインの俯瞰

鍵管理で扱われる**要素ごと**の一般的なガイダンス
- 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



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
- 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
- 暗号鍵管理システムポリシーに沿って作成

7月7日に公開しました

■ 新しい暗号鍵管理ガイドラインを作ってみました

https://www.ipa.go.jp/security/vuln/ckms.html

暗号鍵管理ガイドライン

実際の暗号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
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ります。そ
タのライフサイクルを踏まえた運用、安全な暗号鍵の保管、暗号鍵危殆化時の対策などを行う上で参考とな
まとめています。

「暗号鍵管理システム設計指針（基本編）」の内容

「暗号鍵管理システム設計指針（基本編）」は、あらゆる分野・あらゆる領域の全ての暗号鍵管理システム
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網羅的に提供し、
ピックス及び設計書等に明示的に記載する要求事項を取りまとめたガイドラインとして作成されたものです

具体的には、暗号鍵管理の必要性を認識してもらうために「暗号鍵管理の在り方（暗号鍵管理の位置づけと
と、NIST SP800-130「A Framework for Designing Cryptographic Key Management Systems」の
して活用できるように構成した「暗号鍵管理についての技術的内容」とで構成されています。

なお、本ガイドラインは、暗号技術評価プロジェクトCRYPTRECで作成されました。

本設計指針の章立ては以下のとおりです。

- 1章と2章は、イントロダクションとして、本ガイドラインの目的、暗号鍵管理の在り方や考え方につ
- 3章は、本設計指針の活用方法について解説しています。
- 4章から9章は、NIST SP800-130の解説書・利用手引書として活用できるように、NIST SP800-130
号鍵管理における目的ごとに章分けをしています。なお、本設計指針だけでも項目や概要が分かるよう
が、正確な内容についてはNIST SP800-130を参照してください。
- Appendixには、本ガイドラインとNIST SP800-130で使用されている用語の対応関係も示した用語集
- チェックリストは、システム等の運用環境に照らして4章から9章に記載されている考慮事項（Framew
から必要な事項を適切に選択し、その記載事項に従って具体的な要件として暗号鍵管理のための設計仕
ル等が作成されているかを確認できるように作られています。

資料のダウンロード

暗号鍵管理システム設計指針（基本編）

暗号鍵管理システム設計指針 (2020年7月7日第1版公開)

- 暗号鍵管理システム設計指針（基本編）第1版（全128ページ、3.86MB）
- 暗号鍵管理システム設計指針（基本編）チェックリスト 第1版（PDF形式 309KB）
- 暗号鍵管理システム設計指針（基本編）チェックリスト 第1版（Excel形式 45kB）

参考情報

- 日本語訳
  - NIST SP800-130 A Framework for Designing Cryptographic Key Management Systems
    ※免責事項
    原文にできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありません。
    本翻訳物に記載されている情報より生じる損失または損害に対して、いかなる人物あるいは団体にも責任を負うものではありません。

ガイドライン本体

チェックリスト

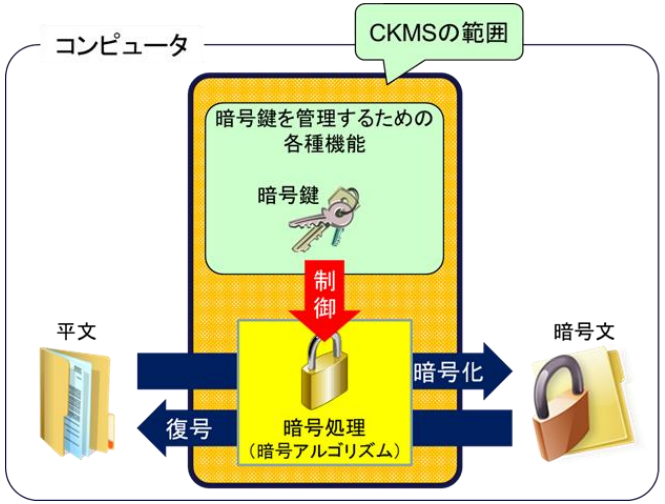
SP800-130 日本語訳

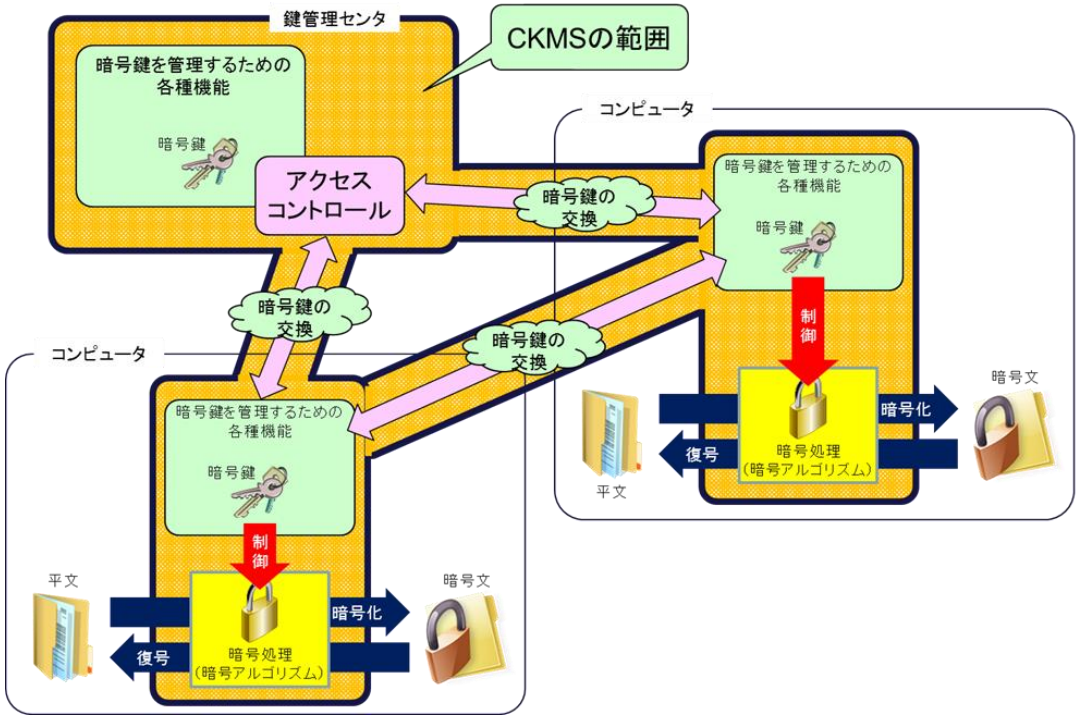
『暗号鍵管理システム設計指針（基本編）』とは

- **あらゆる分野・あらゆる領域**の全ての暗号鍵管理システムを対象
- 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（Framework Requirements）を網羅的に提供
- 設計書等に明示的に記載する要求事項を取りまとめた

CKMSのシステム規模は問わない

- 「暗号鍵管理システムの設計原理と運用ポリシー」の中で設計者が具体的に定義





『暗号鍵管理システム設計指針（基本編）』とは

- あらゆる分野・あらゆる領域の全ての暗号鍵管理システムを対象
- 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（Framework Requirements）を網羅的に提供**
- 設計書等に**明示的に記載する要求事項を取りまとめた**

暗号鍵管理の考え方の枠組みを整理し、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化

- 「暗号鍵管理の在り方」:
  暗号鍵管理の必要性を認識してもらうための解説
- 「暗号鍵管理についての技術的内容」:
  NIST SP800-130「A Framework for Designing Cryptographic Key Management Systems」の解説書として活用

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を義務づけない

- どのように要求事項に対応するか
  → 設計者に委ねられる
- 対応方針が適正かどうかの判断
  → 運用管理者や調達責任者が行う

暗号鍵管理の考え方の枠組みを整理
暗号鍵管理の設計仕様書や運用マニュアルの位置づけを明確化

本設計指針が取扱う範囲

セクタ固有の特性／環境

セクタ等で取組んでいただきたい範囲

システム依存の環境／条件

SI／調達者が取り組む範囲

Framework Requirements
あらゆるケースにおける鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として考慮すべき事項一覧の提示
（具体的な技術仕様は取扱わない）

SP800-130
包括的なフレームワークに沿って暗号鍵管理システムの『対応方針として考慮すべきトピック及び仕様書等に記載する文書化要求事項の一覧』を列挙

選択
精緻化
増補

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

SP800-152
SP800-130に沿い、米国政府システムの特性／環境等を考慮して『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）』を規定

選択
精緻化
増補

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

〇〇システム設計仕様書

〇〇システム運用マニュアル

個々の技術選択の下支え根拠

個々の技術選択の下支え根拠

Guidance
- 鍵管理について理解するための汎用的なガイダンスの提示
- 暗号アルゴリズムや鍵長等の推奨設定／考え方の提示

SP800-57 Part1、CRYPTREC暗号リスト、リストガイド（鍵管理）
暗号メカニズムを選択・利用する際の『情報』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

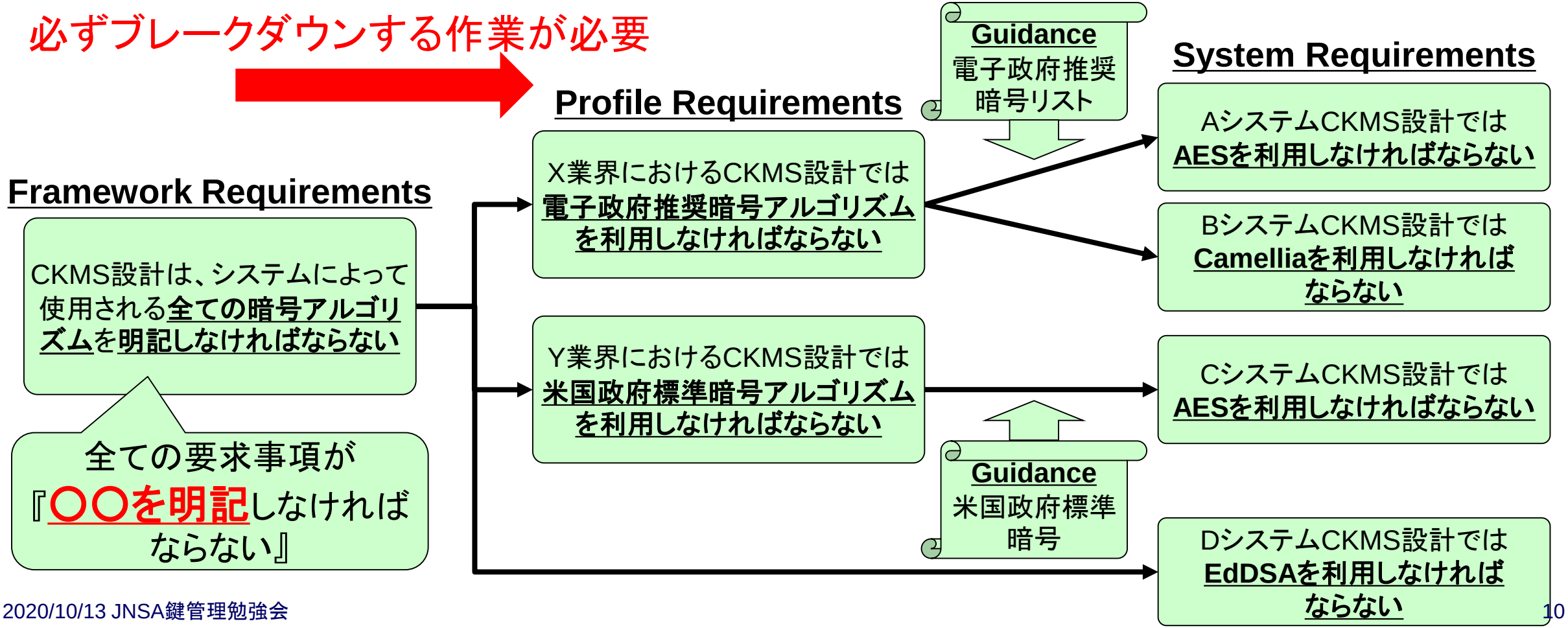
SP800-57 Part3、SSL/TLS暗号設定ガイドライン
暗号プロトコル／アプリケーションを選択・利用する際の『適切な選択を支援するための情報』の提供

暗号鍵管理の考え方の枠組みを整理
～「What about」と「How to」の違い

暗号鍵管理システムで検討すべき事項は同じでも実現方法は違う

Framework requirements　　Profile/System requirements

必ずブレークダウンする作業が必要



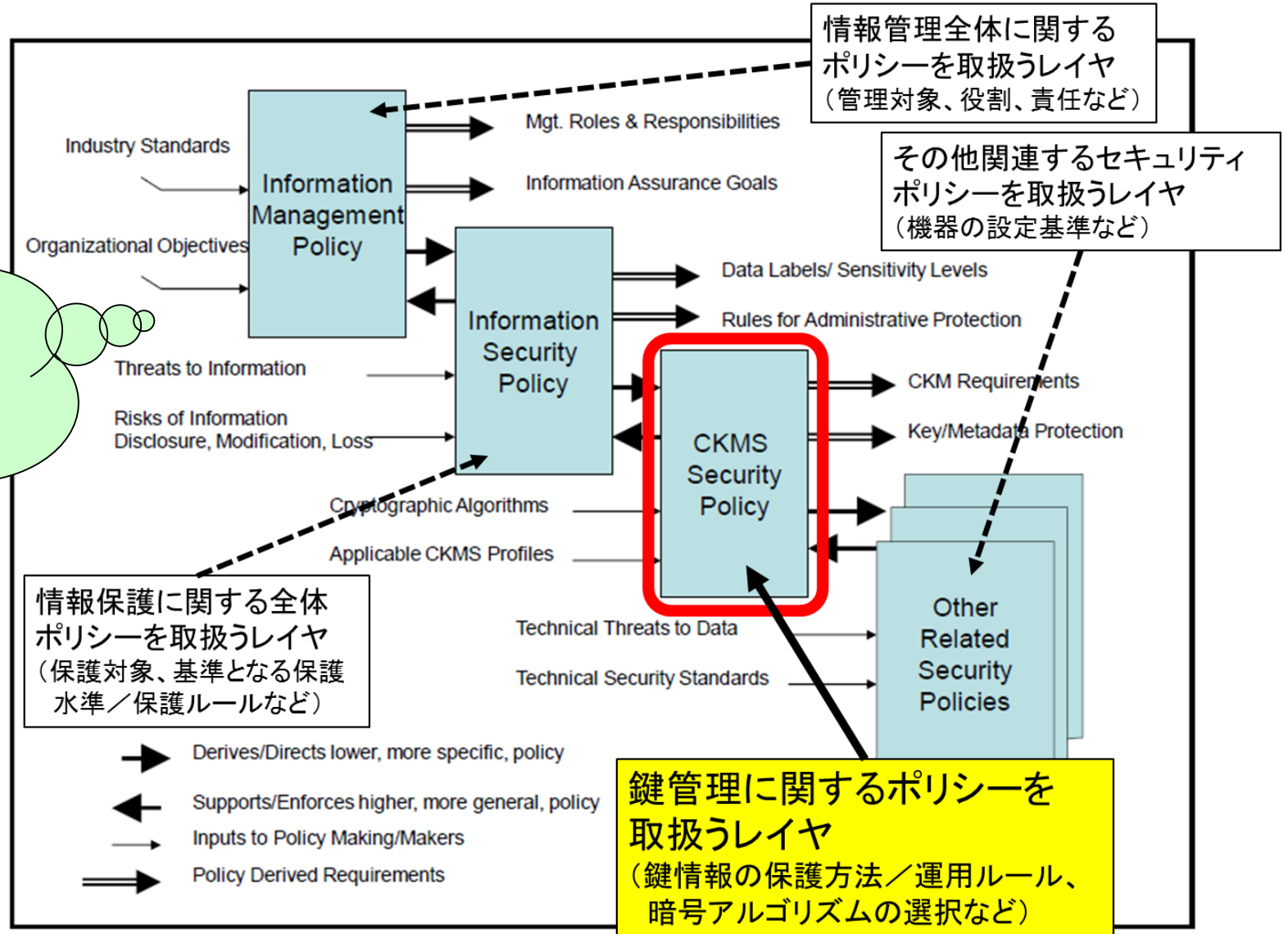
（参考）SP800-130とSP800-152の関係例

■ SP800-152
『米国連邦政府』におけるCKMS Profile Requirementsを規定したもの

SP800-130 (Frame Requirements)	SP800-152 (Profile Requirements)
4. Security Policies	4. Security Policies
4.8 Laws, Rules, and Regulations FR: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. （利用地域と**あらゆる法的制限を明記しなければならない**）	4.10 Laws, Rules, and Regulations PR [Profile Requirements]:4.17 A Federal CKMS **shall comply with U.S. Federal** laws, rules and regulations. （**米国**の連邦法、規則、及び規制に**準拠しなければならない**） 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. （**利用国**での規則や規制に**準拠することを推奨**） PF [Profile Features]:4.2 A Federal CKMS **could be configurable to comply with** the policies of **one or more** national and international organizations. （**複数**のポリシーに**準拠するように設定変更可能なオプション**）

ブレークダウンする時の根拠は？
～『適切』な暗号鍵管理のために

暗号鍵管理の前に
情報管理ポリシーや
情報セキュリティポリシー
を定めるほうが先決



出展：SP800-130

暗号鍵管理における時間管理を考慮することの重要性 ～鍵情報のライフサイクル

- 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
  - 鍵情報のライフサイクルは、鍵状態と遷移（Key States and Transitions）に基づく

【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

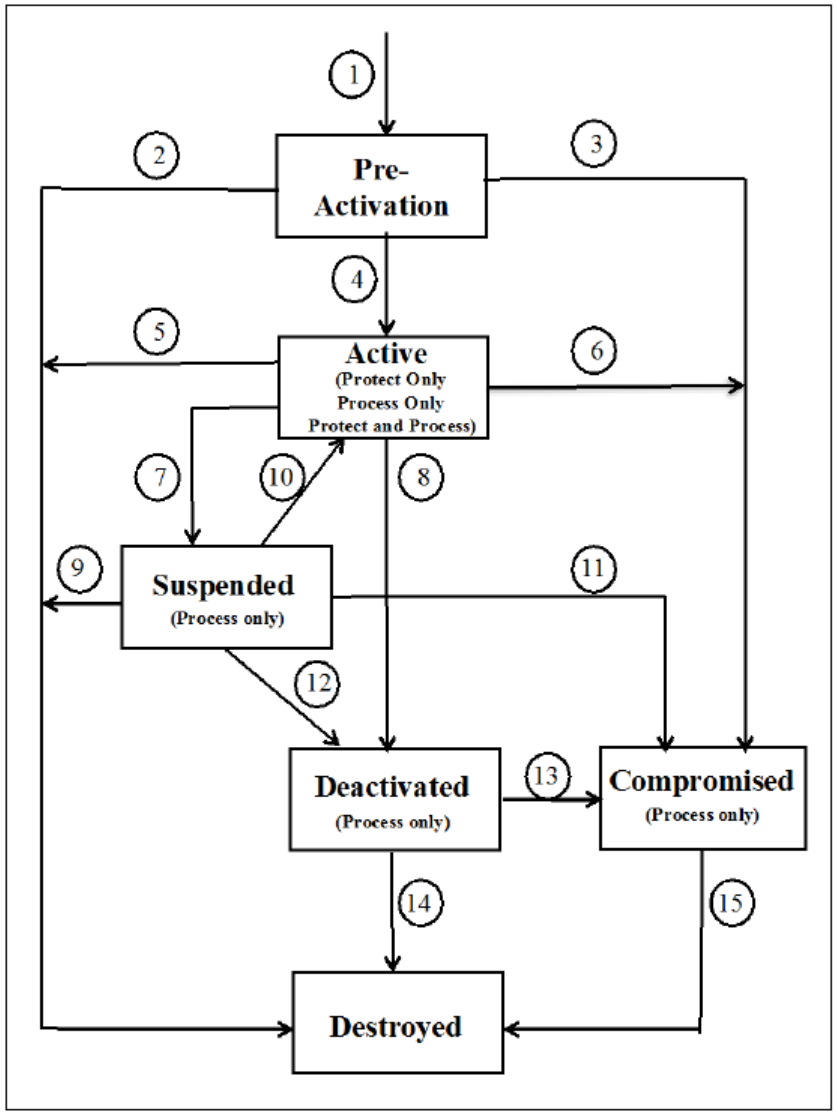
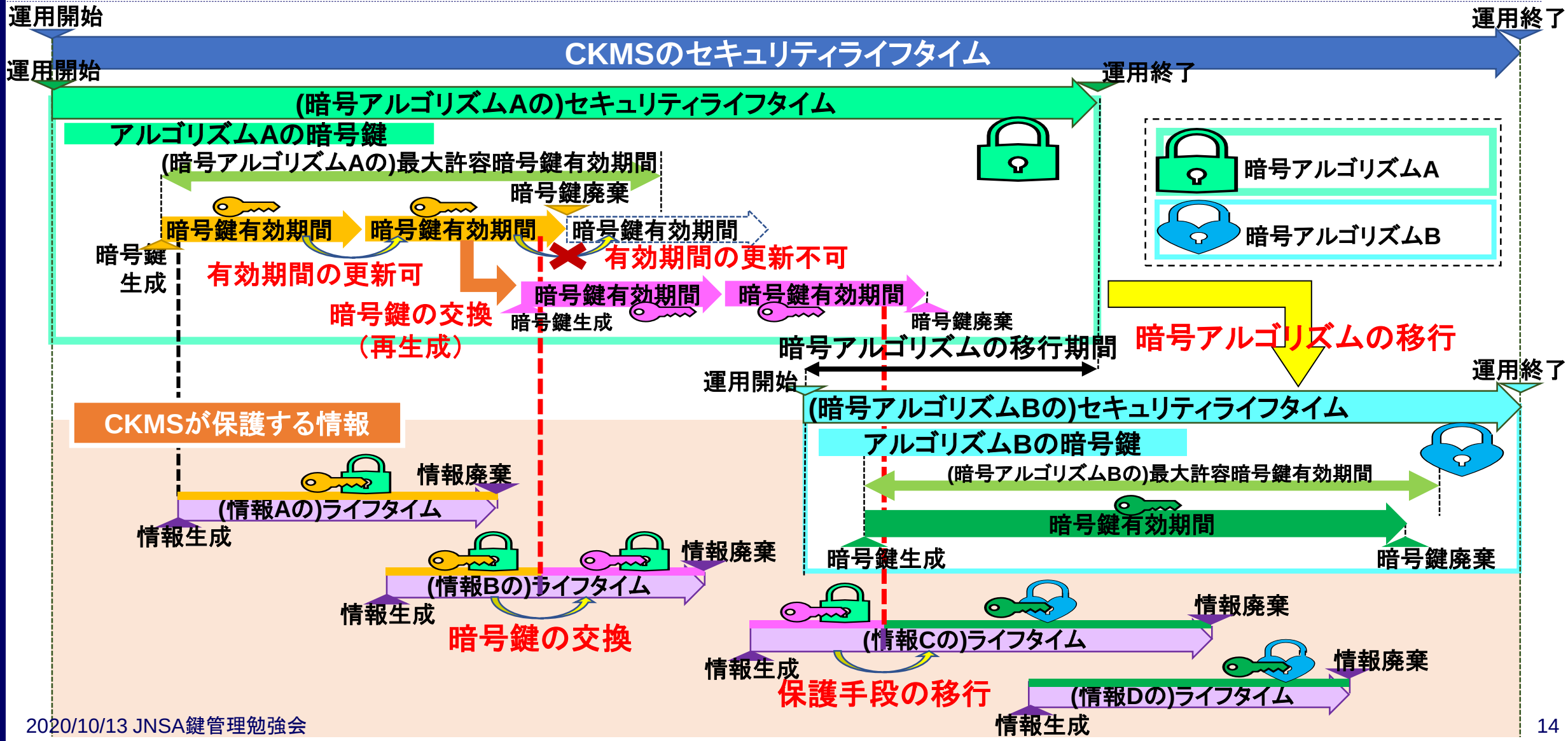


Figure 3: Key state and transition example.

暗号鍵管理における時間管理を考慮することの重要性 ～CKMSのセキュリティライフサイクル



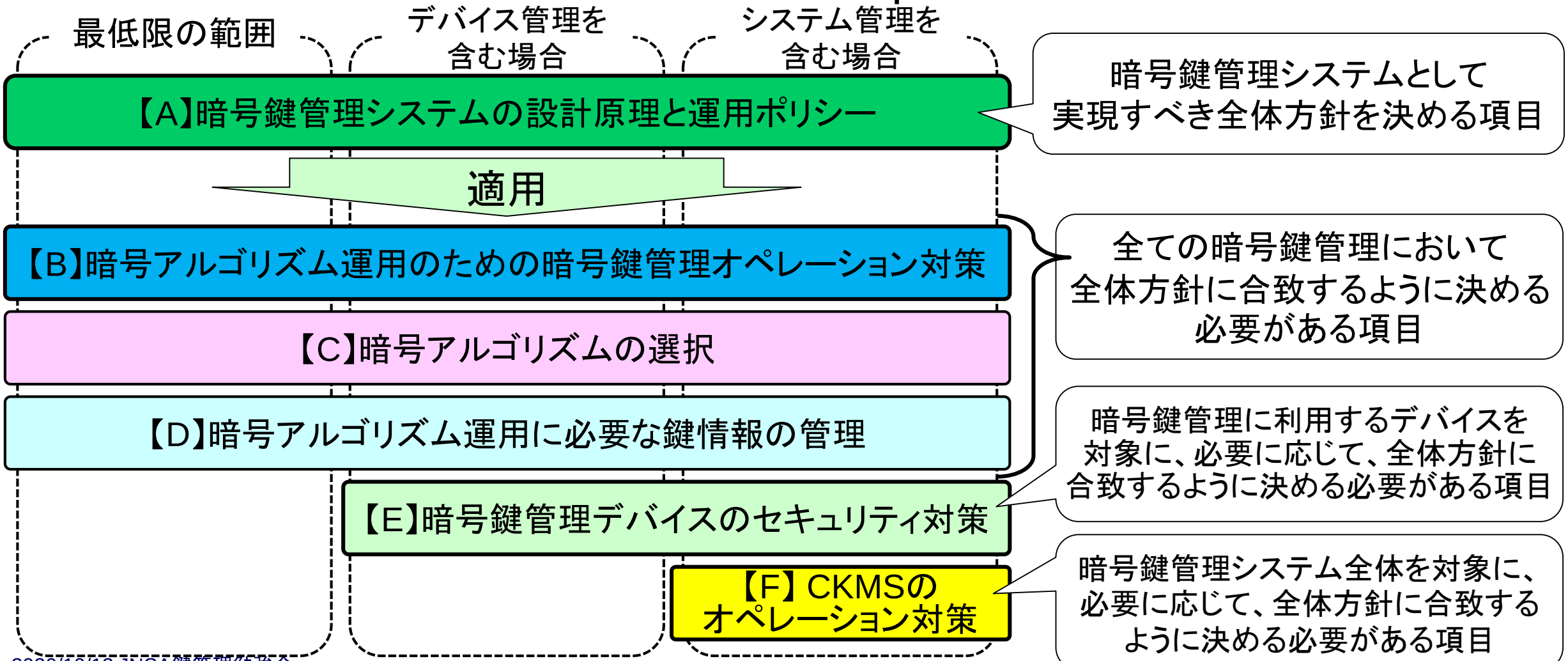
SP800-130

■ 256個のCKMS Framework Requirementsを提示

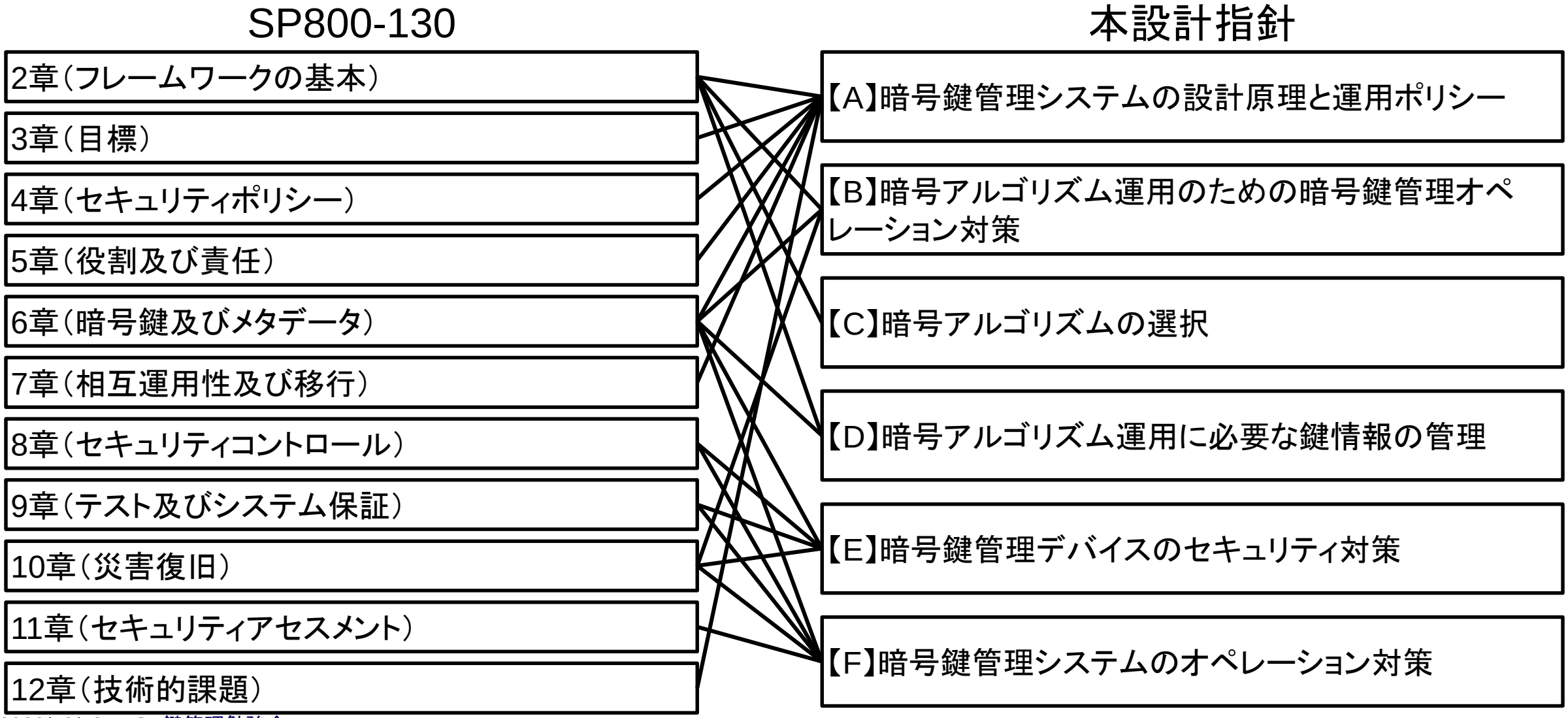
2章（フレームワークの基本）	本フレームワークの基本的な概念をカバー
3章（目標）	堅牢なCMSの目標を定義
4章（セキュリティポリシー）	CKMSセキュリティ及び関連するセキュリティポリシーの必要性を説明
5章（役割及び責任）	CKMSをサポートする担当者の役割と責任を提示
6章（暗号鍵及びメタデータ）	鍵及びメタデータ、及びアクセスコントロールの考慮、セキュリティ課題及び回復メカニズムを備えた鍵及びメタデータの管理機能をカバー
7章（相互運用性及び移行）	相互運用性の必要性、及び将来のニーズに適応するためのCKMSの機能における容易に移行するための機能についての考察
8章（セキュリティコントロール）	典型的なCKMSに適用可能なセキュリティコントロールについての考察
9章（テスト及びシステム保証）	CKMSデバイスについてのセキュリティテストと保証についての考察
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の考察
11章（セキュリティアセスメント）	CKMS全体のセキュリティアセスメントについての考察
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の考察

暗号鍵管理における検討項目

■ SP800-130での256個のFramework Requirementsを目的別に再構成



本設計指針とSP800-130の対応関係



暗号鍵管理における検討項目

【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（69項目）

- 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
- 将来的な移行対策を準備しておく必要があるか

	SP800-130該当節
（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

暗号鍵管理における検討項目

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	①CKMSの設計にあたって、CKMSセキュリティポリシーを作成しなければならない。	A.01～A.02
	②CKMSセキュリティポリシーは、他のセキュリティポリシーや組織の様々なポリシーに依存することがあるので、それらを意識しなければならない。	A.03～A.04
	③CKMSセキュリティポリシーがCKMS内に電子的に保管され自動的に処理される場合には正しい処理が行われるように注意をしなければならない。	A.05
4.2 情報管理ポリシー等からの要求事項	①機微な情報を管理するために、「個人の説明責任（Personal accountability）」について情報管理ポリシー等の要求事項に記載される場合には、どのように対応するかを決めなければならない。	A.06
	②エンティティに対するプライバシーの提供、関連法令の遵守、又はセキュリティ強化のために、「匿名性」「連結不可能性」「観測不可能性」（のいずれか）の保証について情報管理ポリシー等に記載される場合には、どのように対応するかを決めなければならない。	A.07～A.13

検討番号A.01はCKMSセキュリティポリシーを作成することを、A.02はそのCKMSセキュリティポリシーに明記すべき内容及びその実現・利用方法について明確化することを要求したもの

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。
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。

暗号鍵管理における検討項目の目的別分類

【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

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な機能や運用方法を決める検討項目（81項目）

- 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

（5.1節）CKMS設計
（5.2節）鍵情報のライフサイクル
（5.3節）鍵情報のライフサイクル管理機能
（5.4節）鍵情報の保管方法
（5.5節）鍵情報の鍵確立方法
（5.6節）鍵情報の破損時のBCP対策
（5.7節）鍵情報の危殆化時のBCP対策

暗号鍵管理における検討項目の目的別分類

【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決める検討項目（2項目）

- 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

（6.1節）暗号アルゴリズムのセキュリティ
（6.2節）CRYPTREC暗号リスト

【D】暗号アルゴリズム運用に必要な鍵情報の管理

具体的な鍵情報の設定方法や保管方法等を取り決める検討項目（10項目）

- 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

（7.1節）鍵情報の種類
（7.2節）鍵情報の選択
（7.3節）鍵情報の保護方針

暗号鍵管理における検討項目の目的別分類

【E】暗号鍵管理デバイスのセキュリティ対策

暗号鍵を管理するデバイスに対して、必要に応じて検討する項目（37項目）

- 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

（8.1節）鍵情報へのアクセスコントロール
（8.2節）セキュリティ評価・試験
（8.3節）暗号モジュールの障害時のBCP対策

暗号鍵管理における検討項目の目的別分類

【F】暗号鍵管理システムのオペレーション対策

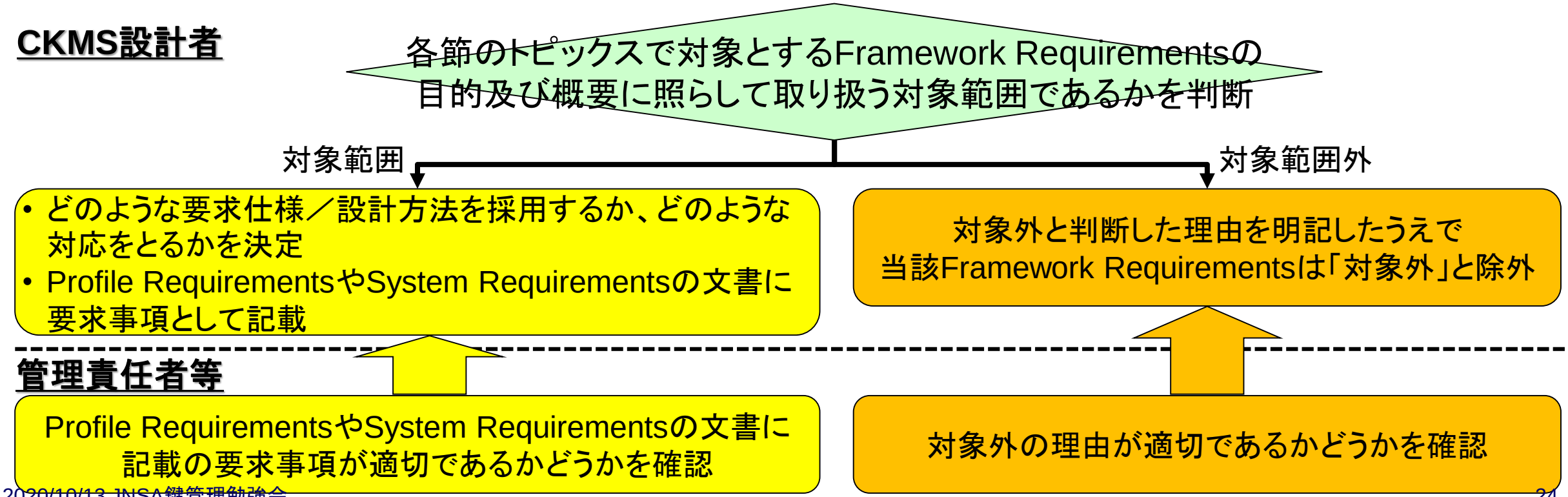
CKMS全体に対して、必要に応じて検討する項目（57項目）

- 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

（9.1節）CKMSへのアクセスコントロール
（9.2節）システム保証
（9.3節）セキュリティアセスメント
（9.4節）CKMSのアクセスコントロールの危殆化時のBCP対策
（9.5節）CKMSの障害・災害発生時のBCP対策

本設計指針の活用方法

- どのような要求仕様／設計方法を採用するかは、設計者、又はセキュリティプロファイル等の他ドキュメントに委ねられる
  - 設計者：選択し得るオプションリストとして使用して要求仕様を決定
  - 責任者：不適切な要求仕様や検討漏れがないかの確認リストとして活用



本設計指針の活用方法

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

【満たさなければ不適合となる要件】

- **【必須】:必ず満たさなければならない要求事項を記述する際に利用する。「○○しなければならない」**
- **【禁止】:絶対にしてはならない要求事項を記述する際に利用する。「○○してはならない」**

【満たすものを優先的に取り扱うべき要件】

- **【要望】:できるだけ満たすように求める事項を記述する際に利用する。「○○すべきである」**

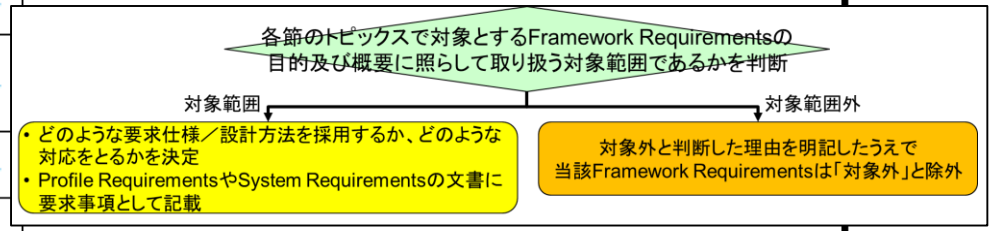
【上記以外の要件】

- **【オプション】:満たすようにしてもよい事項を記述する際に利用する。「○○してもよい」「○○することがあり得る」**

チェックリスト

CKMS設計指針（基本編）チェックシート　2020.07.07版

検討番号（4章）	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
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	済・対象外	
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	済・対象外	
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	済・対象外	
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	済・対象外	
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	済・対象外	
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	済・対象外	
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	済・対象外	
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	済・対象外	
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	済・対象外	
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	済・対象外	
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	済・対象外	



チェックリストの活用例

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

System Requirements

商用既製品：
- CMVP認証済HSMを利用**しなければならない**

HSMが実行**しなければならない**

セキュリティ機能：
- FIPSモードによる暗号鍵生成、配送、失効、破棄

鍵情報を保管**しなければならない**

場所：
- HSM：HSM内部
- クライアント：セキュアゾーン

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	済 対象外	採用するHSMに依存するため
B.04	FR6.17	CKMS設計は、実装されサポートされる鍵情報（暗号鍵及びメタデータ）の管理機能を明記しなければならない。	6.4節	済 対象外	
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	済 対象外	採用するHSMに依存するため
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	済 対象外	採用するHSMに依存するため

とは言ってみたものの
～　さて、これからどうしましょうか

- 「Framework」はできたけど（これだけで）使いこなすのはやっぱり難しい
  - 「How to」については何も言及していない
  - SP800-152があったからSP800-130が読み込めた面もある
  - 参照プロファイルがいりそう（というのは分かる）
- 参照プロファイルを（誰が）どうやって作る？
  - リモート署名
  - 暗号資産
  - リモート型鍵管理（クラウドとか・・・？）
  - ・・・・　色々ありそうではあるけど
- 認証製品とか使うと楽になる？？
  - 対策済とかいえるようになると便利・・・かな？

独立行政法人**情報処理推進機構**
Information-technology Promotion Agency, Japan