CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術活用委員会活動報告

2022年7月5日

暗号技術活用委員会 委員長
（横浜国立大学 教授）
松本　勉

目次

1. 暗号技術活用委員会　概要

2. 2019年度暗号技術活用委員会　活動概要
   - TLS暗号設定ガイドライン
   - 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）』

3. 2020 - 2021年度暗号技術活用委員会　活動概要
   - CRYPTREC暗号リスト改定に向けた利用実績による選定基準（案）
   - 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準
   - 暗号鍵設定ガイダンス
   - 暗号鍵管理ガイダンス作成に向けた検討

目次

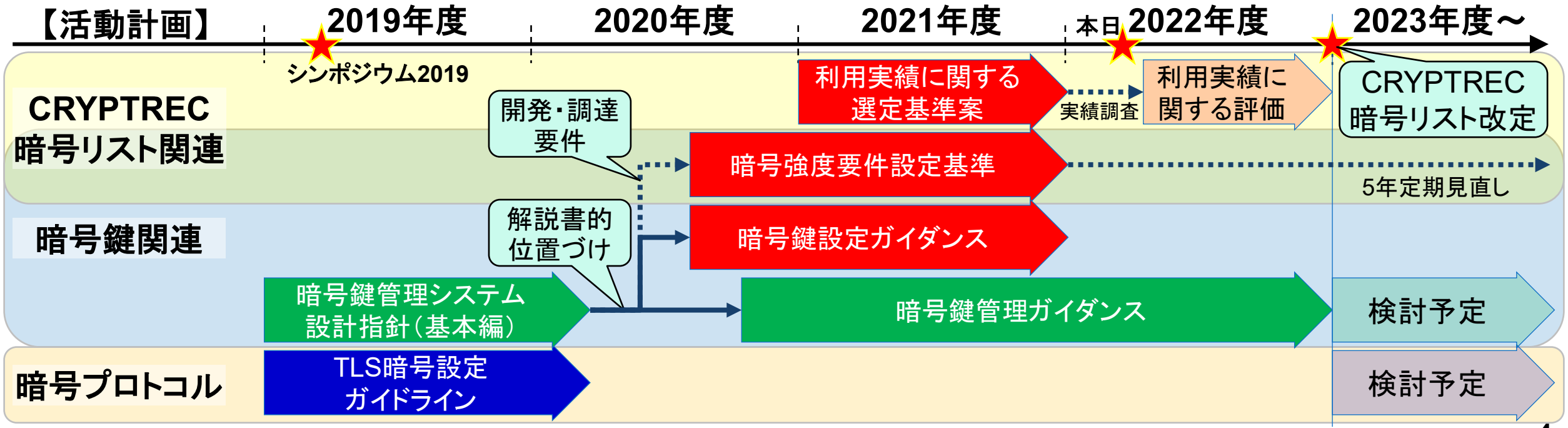
暗号技術活用委員会活動目的＆計画

【活動目的】

暗号技術活用委員会では、**情報システム全般のセキュリティ確保に寄与**することを目的として、**暗号の取り扱いに関する観点から必要な活動**を行うものとする。

具体的には、実運用とセキュリティ確保の両面の観点から、以下の対象を取り扱う。

- 暗号アルゴリズムの利用及び設定に関する運用マネジメント
- 暗号プロトコルの利用及び設定に関する運用マネジメント
- その他、情報システム全体のセキュリティ確保に有用な暗号に関わる運用マネジメント



CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC活動体制（2019年度～2020年度）

暗号技術検討会

① CRYPTREC暗号のセキュリティ及び信頼性確保のための調査・検討
② CRYPTREC暗号リストの改定に関する調査・検討
③ 関係機関と連携した暗号技術の普及による情報セキュリティ対策の推進検討・提言

量子コンピュータ時代に向けた暗号の在り方検討タスクフォース
（2019年6月～）

暗号技術評価委員会

① 暗号技術の安全性及び実装に係る監視及び評価
② 新世代暗号に係る調査
③ 暗号技術の安全な利用方法に関する調査

暗号技術調査WG（暗号解析評価）
（2019～2020年度）

暗号技術活用委員会

① 暗号の普及促進・セキュリティ産業の競争力強化に係る検討
② 暗号技術の利用状況に係る調査及び必要な対策の検討
③ 暗号政策の中長期的視点からの取組の検討

TLS暗号設定ガイドラインWG
（2019年度）

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC活動体制（2020年度～2022年度）

暗号技術検討会

① CRYPTREC暗号のセキュリティ及び信頼性確保のための調査・検討
② CRYPTREC暗号リストの改定に関する調査・検討
③ 関係機関と連携した暗号技術の普及による情報セキュリティ対策の推進検討・提言

- 量子コンピュータ時代に向けた暗号の在り方検討タスクフォース（2019年6月～）

暗号技術評価委員会

① 暗号技術の安全性及び実装に係る監視及び評価
② 新世代暗号に係る調査
③ 暗号技術の安全な利用方法に関する調査

- 暗号技術調査WG（暗号解析評価）（～2020年度）
- 暗号技術調査WG（耐量子計算機暗号）（2021年度～）
- 暗号技術調査WG（高機能暗号）（2021年度～）

暗号技術活用委員会

① 暗号の普及促進・セキュリティ産業の競争力強化に係る検討
② 暗号技術の利用状況に係る調査及び必要な対策の検討
③ 暗号政策の中長期的視点からの取組の検討

- 暗号鍵管理ガイダンスWG（2021年度～）

暗号技術活用委員会委員

CRYPTREC
Cryptography Research and Evaluation Committees

（注）2022年3月末時点

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	佐藤　直之	SCSK株式会社　シニアプロフェッショナルコンサルタント
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	田村　裕子	日本銀行　企画役補佐
委員	手塚　悟	慶應義塾大学　教授
委員	寺村　亮一	株式会社イエラエセキュリティ　執行役員
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	デジタル庁　セキュリティアーキテクト
委員	山岸　篤弘	日本情報経済社会推進協会　客員研究員（2022年2月まで）
委員	山口　利恵	東京大学　特任准教授
委員	渡邊　創	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

TLS暗号設定ガイドラインWG委員（2019年度）

CRYPTREC Cryptography Research and Evaluation Committees

（注）2020年6月末時点

主査	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	漆嶌　賢二	GMOグローバルサイン株式会社　部長
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	菅野　哲	株式会社レビダム　代表取締役
委員	菊池　浩明	明治大学　教授
委員	北村　英志	グーグル合同会社　デベロッパーアドポケイト
委員	島岡　政基	セコム株式会社　主任研究員
委員	杉尾　信行	株式会社NTTドコモ
委員	杉原　弘祐	セコムトラストシステムズ株式会社
委員	松本　照悟	アマゾンウェブサービスジャパン株式会社　シニアセキュリティコンサルタント

暗号鍵管理ガイダンスWG委員（2021-2022年度）

（注）2022年3月末時点

主査	上原　哲太郎	立命館大学　教授
委員	漆嶌　賢二	GMOグローバルサイン株式会社　部長
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	菅野　哲	株式会社イエラエセキュリティ　取締役CTO of Development
委員	菊池　浩明	明治大学　教授
委員	楠　正憲	デジタル庁　統括官
委員	小林　浩二	パナソニック株式会社　オートモーティブ社　主任技師
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	西原　敏夫	シスコシステムズ合同会社　シニアセキュリティアーキテクト
委員	舟木　康浩	タレスDIC CPLジャパン株式会社　セールスエンジニアマネージャー
委員	満塩　尚史	デジタル庁　セキュリティアーキテクト

目次

2019年度 暗号技術活用委員会審議状況

回	開催日	議案
2019年度 第一回	2019年 6月12日	■活用委員会活動計画について ■TLS暗号設定ガイドラインWG活動計画について ■暗号鍵管理システム設計指針（基本編）ドラフト版について
2020年度 第一回	2020年 6月1日	■TLS暗号設定ガイドラインについて ■暗号鍵管理システム設計指針（基本編）について ■EdDSAに関する安全性評価の必要性について ■運用監視暗号リストからの削除について

これらを紹介

（注）2020年度第一回は新型コロナウイルス感染拡大防止の観点から
延期とした2019年度第二回会合の代替会合として開催したもの

『TLS暗号設定ガイドライン』とは

CRYPTREC Cryptography Research and Evaluation Committees

2020年7月7日公開

■ 有識者の知見を集約したTLSを安全に使うためのBest Practice

- TLSの**安全性と可用性（相互接続性）のバランス**を踏まえた推奨暗号設定方法をガイダンス
- ユースケースに応じた3段階の設定基準を用意
  「高セキュリティ型」「推奨セキュリティ型」「セキュリティ例外型」
- 設定確認するための「チェックリスト」
- OpenSSLやWindows等の「サーバ設定方法例」

利用環境の実態を考慮して設定方法をアップデート

■ 主な想定読者

暗号のエキスパートではない想定読者層が対象

- 具体的な構築・設定を行うサーバ構築者
- サービス提供に責任を持つサーバ管理者
- サーバ構築を発注するシステム担当者

2015年
SSL/TLS暗号設定ガイドライン（第1.0/1.1版）

2018年
SSL/TLS暗号設定ガイドライン（第2.0版）

今回

2020年
TLS暗号設定ガイドライン（第3.0版）

TLS利用環境の変化

TLS1.0／1.1排除の動きが本格化。TLS1.3のサポート開始

- 「Deprecating TLSv1.0 and TLSv1.1」のドラフト審議中（18.9.14～）
- 主要ブラウザベンダが2020年前半にTLS1.0/1.1を無効化するアナウンス
- サポート率（2014年 → 2020年 → **2022年**）：
  TLS1.0（99.3% → 62.9% → **36.5%**）、TLS1.2（25.7% → 96.5% → **99.8%**）、
  TLS1.3（ー → 22.0% → **55.5%**）

民間CA発行のSHA-1利用サーバ証明書は全て有効期限切れ

- しかも、SHA-1の「Prefix-collision attack」が見つかる → 致命的攻撃

Perfect Forward Secrecyのサポート進展

- 主要ブラウザデフォルト有効率：2014年 5.0% → 2020年 82.7% → **2022年 90.7%**

SSL/TLS暗号設定ガイドラインに掲載されていないアルゴリズムの利用拡大

- ChaCha20-Poly1305, EdDSA

TLS暗号設定ガイドラインWGでの検討テーマ

議論テーマ	2019年度			2020年度
	第一回 (19/9/2)	第二回 (19/11/19)	第三回 (20/1/7)	第一回 (20/5/26)
①ガイドライン名の名称変更	★			
②3段構成の概要の見直し	◎	★		
③推奨プロトコルバージョンの見直し	◎	★		
④サーバ証明書推奨設定の見直し	◎	★		
⑤推奨暗号スイートの見直し	○	◎	★	
⑥具体的な設定方法の見直し	★			
⑦情報提供として記載している内容の見直し			◎	★
⑧ブラウザでの標記に関する留意点の見直し			◎	★
⑨(専用)サーバ—ブラウザ以外も含めた利用形態			○	★
⑩常時HTTPS化に伴う留意点			○	★
⑪コラムの題材			○	★

凡例: ★:結論を確認　◎:重点的に議論し、方向性を決定　○:自由議論

TLS暗号設定ガイドラインで扱っている設定項目

■ 安全性への寄与度を考慮し、より現実的かつ実効性が高い要求設定に区分
- ●最低限の安全性を確保するために必ず満たさなければならない「遵守項目」
- ●よりよい安全性を実現するために満たすことが望ましい「推奨項目」

要求設定	遵守	プロトコルバージョン	利用禁止プロトコルバージョンを利用不可にする設定
		サーバ証明書	利用する暗号アルゴリズムと鍵長の設定
			発行・更新時の鍵情報の生成方法の明確化
			警告表示の回避方法の明確化
		暗号スイート	利用禁止暗号アルゴリズムを利用不可にする設定
			公開鍵暗号の鍵長の設定
	推奨	プロトコルバージョン	利用プロトコルバージョンの優先順位付け
		暗号スイート	利用推奨暗号アルゴリズムのみでの設定
			推奨暗号スイートの優先順位付け

例えば、【推奨】利用推奨暗号＆【遵守】利用禁止暗号

		高セキュリティ型	推奨セキュリティ型	セキュリティ例外型	共通の利用禁止暗号
バージョン		TLS1.3（必須）、TLS1.2（オプション）	TLS1.2（必須）、TLS1.3（オプション）	TLS1.3 ～ TLS1.0のいずれか	
鍵交換		DHE ECDHE	DHE ECDHE	DH DHE ECDH ECDHE RSAES-PKCS1-V1_5	なし
署名		ECDSA RSASSA-PKCS1-v1_5 RSASSA-PSS*2*3	ECDSA RSASSA-PKCS1-v1_5	ECDSA RSASSA-PKCS1-v1_5	GOST R 34.10-2012*1
暗号化	64ビットブロック暗号	–	–	–	RC2, EXPORT-RC2, IDEA, DES, EXPORT-DES, GOST 28147-89*1, Magma*1, 3-key Triple DES
	128ビットブロック暗号	AES Camellia*4	AES Camellia*4	AES Camellia*4	Kuznyechik*1, ARIA, SEED
	利用モード	CCM, CCM_8 GCM	CBC CCM, CCM_8 GCM	CBC CCM, CCM_8 GCM	CTR_OMAC*1
	ストリーム	ChaCha20-Poly1305	ChaCha20-Poly1305	ChaCha20-Poly1305	RC4, EXPORT-RC4
ハッシュ関数(HMAC)		SHA-256 SHA-384	SHA-1 SHA-256 SHA-384	SHA-1 SHA-256 SHA-384	MD5, GOST R 34.11-2012*1
推奨しないが利用を妨げない		DSA EdDSA*2	RSAES-PKCS1-V1_5 DSA EdDSA*2	DSA EdDSA*2	凡例： *1 現在ID（RFCではない） *2 暗号スイートのIANA登録番号として管理されていない *3 TLS1.3でのみ利用可 *4 TLS1.2以前で利用可
追加の利用禁止暗号		DH ECDH RSAES-PKCS1-V1_5 CBC SHA-1	DH ECDH	なし	

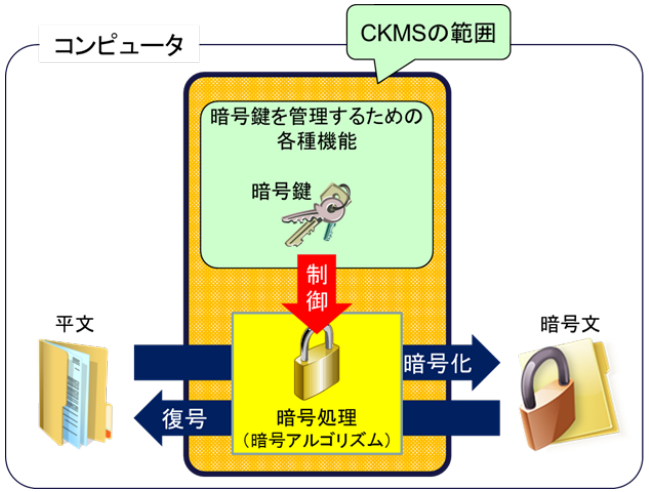
『暗号鍵管理システム設計指針（基本編）』とは

CRYPTREC Cryptography Research and Evaluation Committees

2020年7月7日公開

あらゆる分野／領域の暗号鍵管理システム（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検討事項（Framework Requirements）を網羅的にカバーする指針

- イントロダクション＞「鍵管理」の在り方／考え方の解説
- 技術的な中身＞SP800-130の理解を深める利用手引き
  - SP800-130の Framework Requirements を『暗号鍵管理における目的に応じた』対象範囲に分類・整理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



- セキュリティ要求事項は定義せず、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

本設計指針が取扱う範囲

業界（セクタ）固有の特性／環境

業界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、業界（セクタ）固有の特性／環境も考慮して**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

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に適合するように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『**バックグランド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、**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バックグランド情報**』の提供

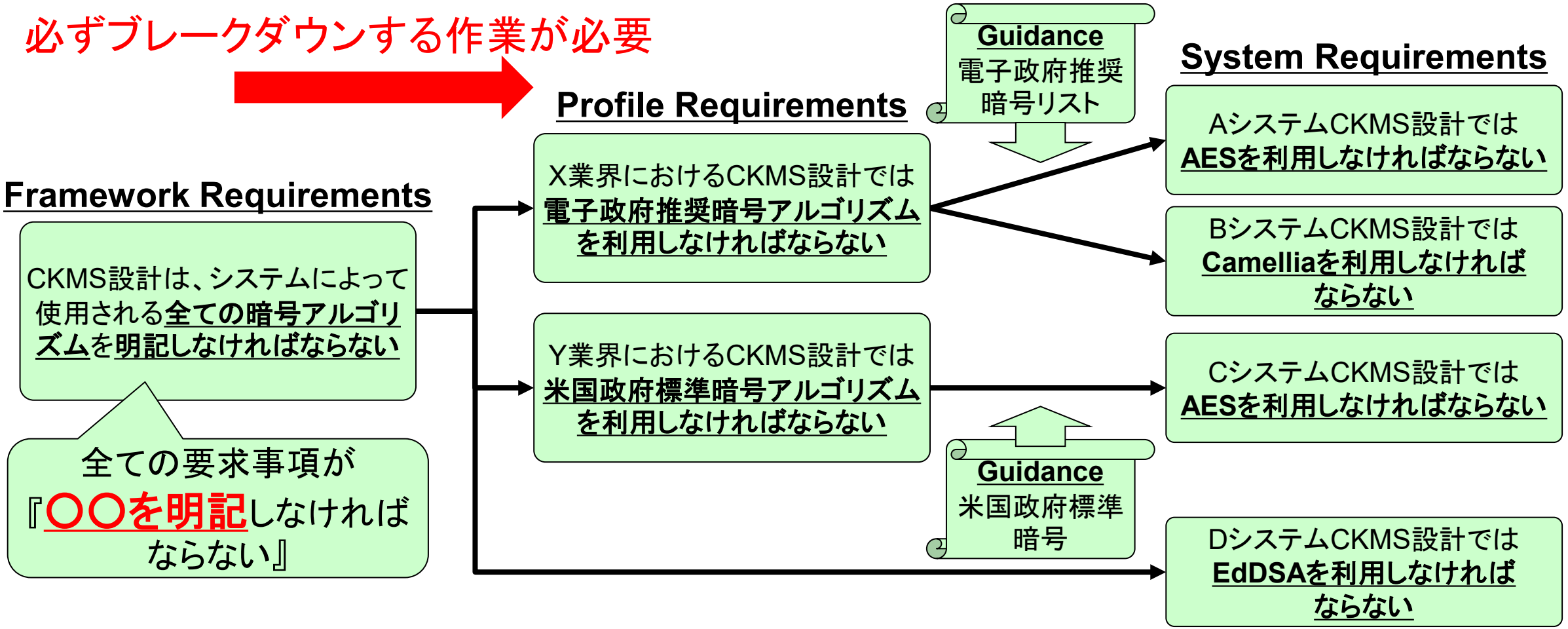
「Framework Requirements」と「Profile/System Requirements」の違い

CRYPTREC Cryptography Research and Evaluation Committees

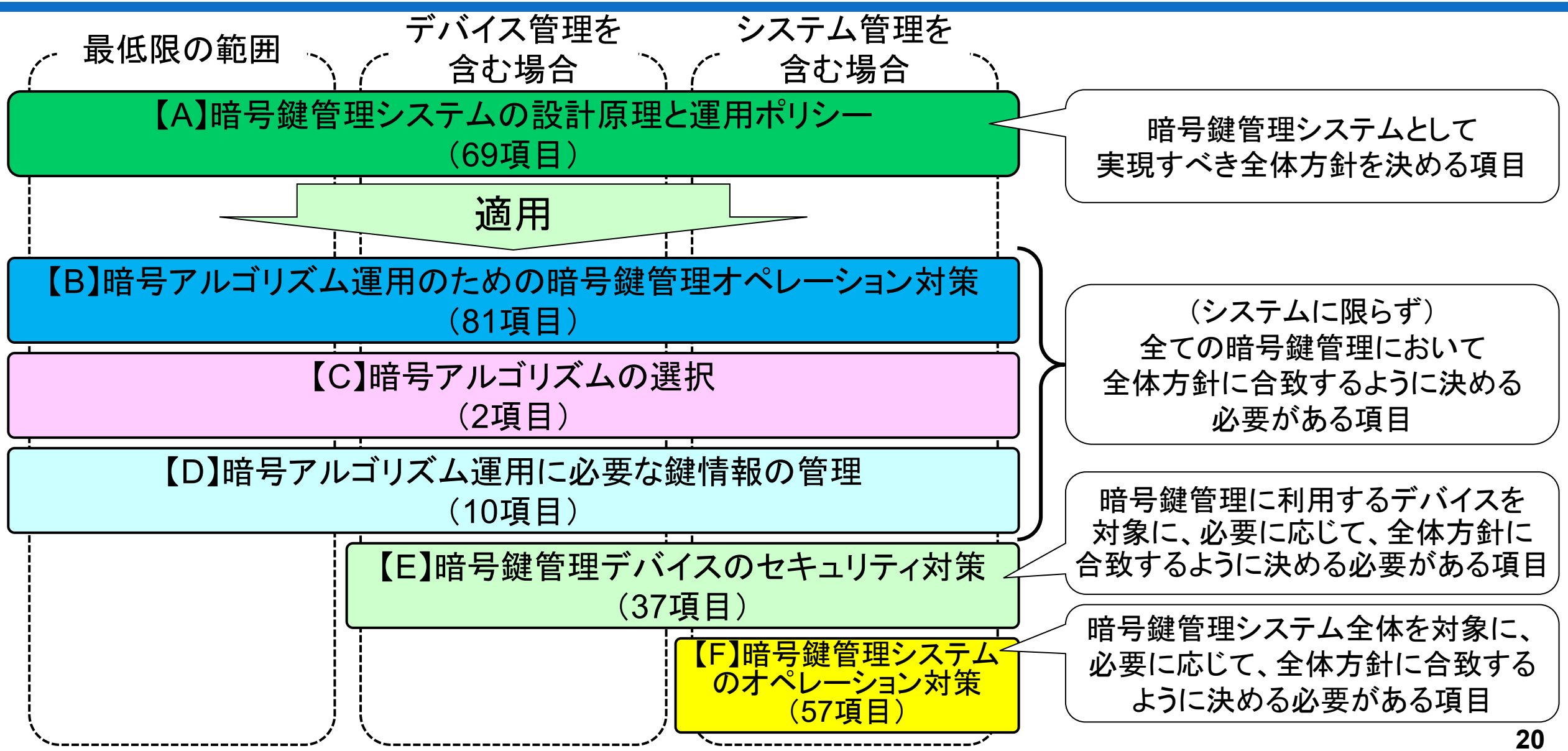
暗号鍵管理システムで検討すべき事項は同じでも実現方法は違う

Framework requirements　　Profile/System requirements

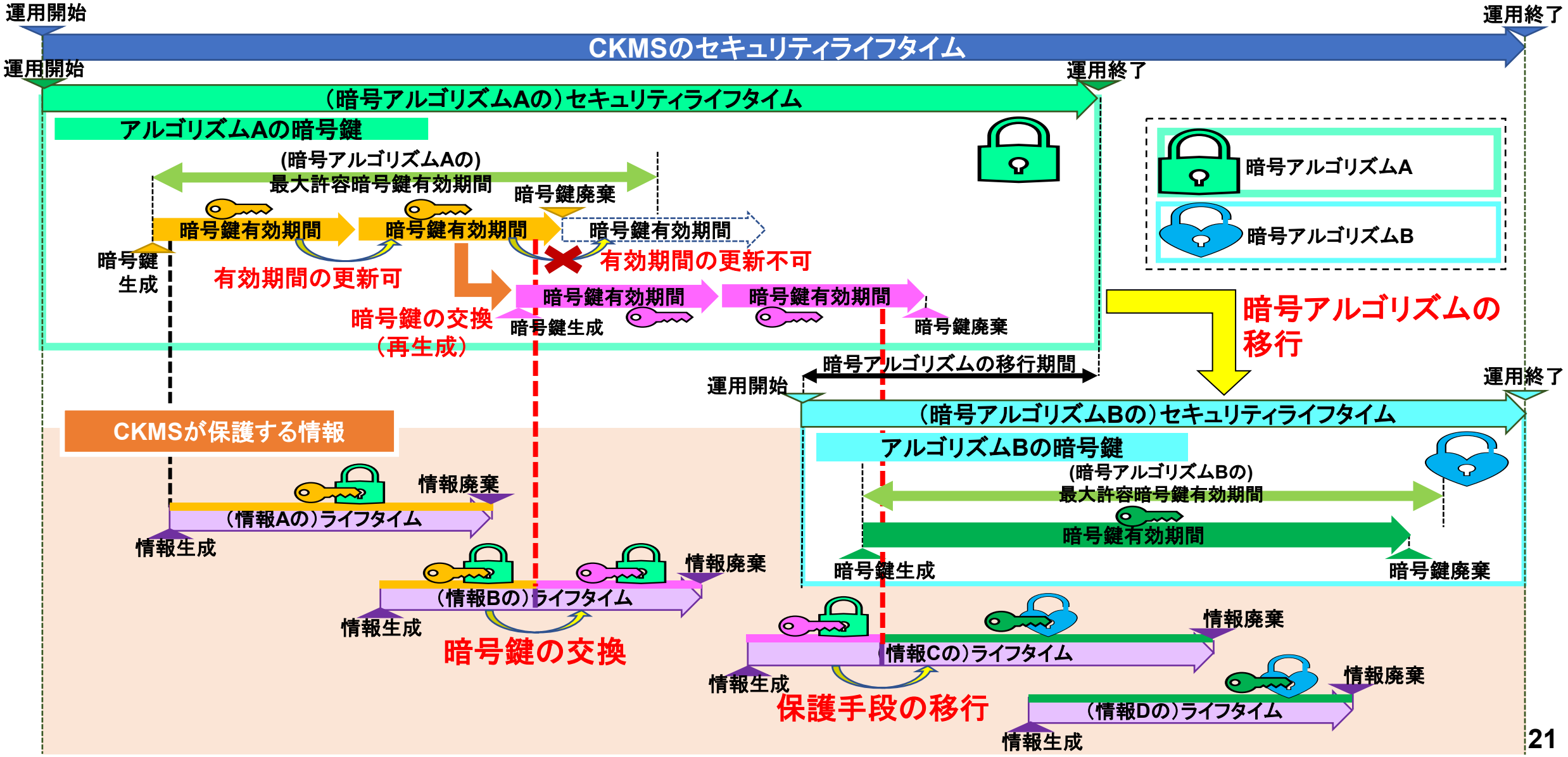
必ずブレークダウンする作業が必要



暗号鍵管理における目的別分類関係



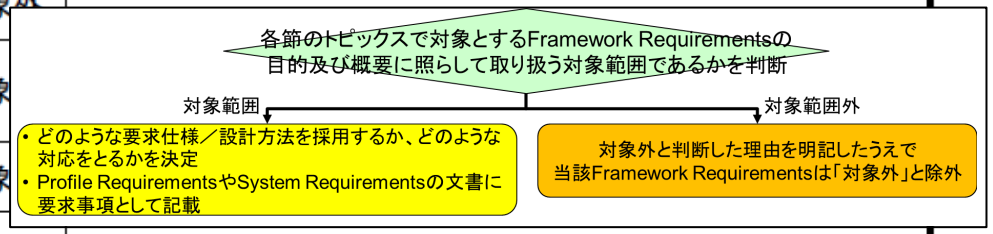
暗号鍵管理における時間管理の概念図



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

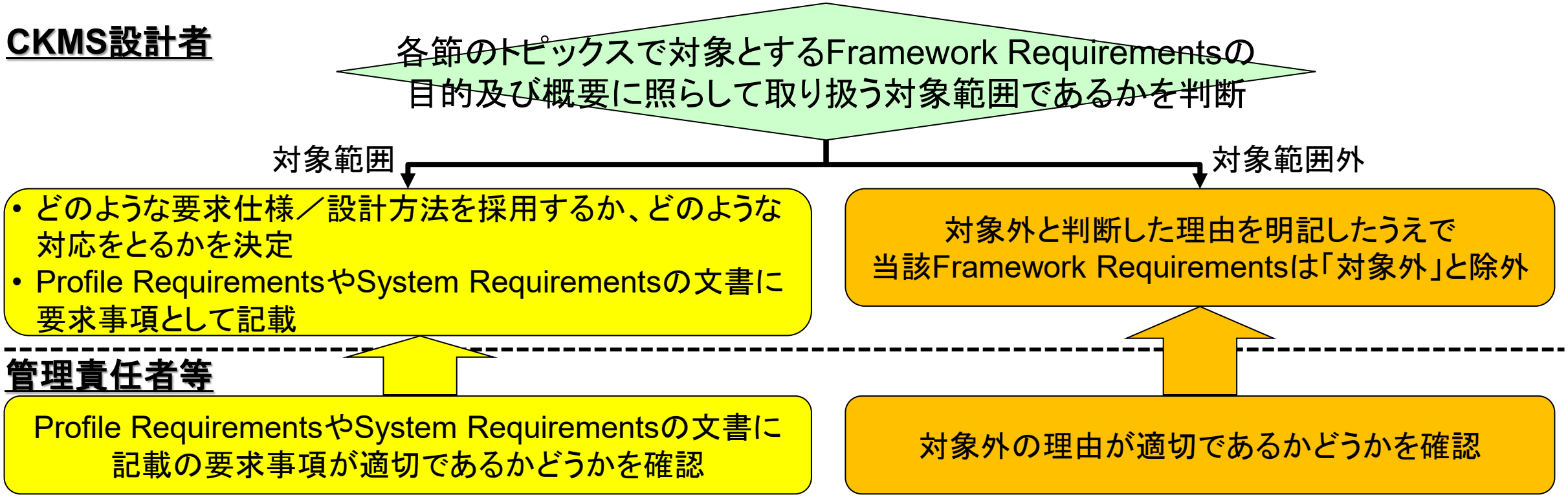
検討番号(4章)	FR番号	Framework Requirementsの内容	SP800-130	チェック	その判断理由
A.01	FR4.1	CKMS設計は、実行するために設計した設定可能なオプションとサブポリシーを含むCKMSセキュリティポリシーを明記しなければならない。	4.3節	済・対象外	
A.02	FR4.2	CKMS設計は、CKMSセキュリティポリシーがCKMSによってどのように実行されるのか(例えば、ポリシーが要求する保護を提供するために使用されるメカニズム)を明記しなければならない。	4.3節	済・対象	
A.03	FR4.4	CKMS設計は、CKMSセキュリティポリシーを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	
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	



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



目次

1. 暗号技術活用委員会　概要

2. 2019年度暗号技術活用委員会　活動概要
   - TLS暗号設定ガイドライン
   - 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）』

3. 2020 - 2021年度暗号技術活用委員会　活動概要
   - CRYPTREC暗号リスト改定に向けた利用実績による選定基準（案）
   - 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準
   - 暗号鍵設定ガイダンス
   - 暗号鍵管理ガイダンス作成に向けた検討

2020-2021年度 暗号技術活用委員会審議状況

回	開催日	議案
2020年度 第一回	2020年 6月1日	新型コロナウイルス感染拡大防止の観点から延期とした2019年度第二回会合の代替会合として開催したもの
2020年度 第二回	2021年 1月15日	■ 2020年度活用委員会活動計画の確認 ■ 推奨鍵長ガイドライン（仮）についての検討 ■ 暗号鍵管理の参照プロファイルについての検討
第三回	2021年 3月2日	■ 鍵長ガイドライン（仮）（方向案）についての検討 ■ 暗号鍵管理の参照プロファイルについての検討（二回目） ■ 2020年度暗号技術活用委員会活動報告案について
2021年度 第一回	2021年 6月30日	■ 2021年度暗号技術活用委員会活動計画の確認 ■ 暗号鍵管理ガイダンスWG活動計画について ■ 利用実績による選定基準について ■ 鍵長設定要件（仮称）について ■ 鍵長設定ガイダンス（一般用）（仮称）について
第二回	2021年 12月13日	■ 利用実績調査による選定基準案について ■ 鍵長設定要件（仮称）について ■ 鍵長設定ガイダンス（一般用）（仮称）について
第三回	2022年 3月1日	■ メール審議結果及び暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準について ■ 利用実績による選定基準（案）について ■ 暗号鍵設定ガイダンス（仮称）について ■ 暗号鍵管理ガイダンスWG活動報告 ■ 2021年度暗号技術活用委員会活動報告案について

講演「CRYPTREC暗号リスト改定に向けた動向及び暗号強度要件設定基準の紹介」で紹介

こちらを紹介

暗号鍵の鍵長設定に関する2つのドキュメント

CRYPTREC LS-0003-2022

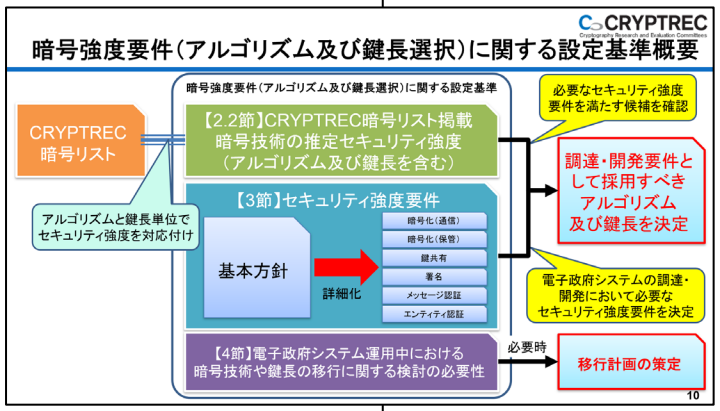
CRYPTREC暗号リストと
セットで使うことを想定した
鍵長の**設定基準**

暗号強度要件（アルゴリズム及び鍵長選択）に
関する設定基準

2022年7月
（Ver. 1.0）

CRYPTREC暗号リストと同様に省庁が発行主体

デジタル庁
総務省
経済産業省



CRYPTREC GL-3003-1.0

適切に鍵長を設定し、適切に
鍵管理を行って安全に運用して
いくための**技術的ガイダンス**

暗号鍵設定ガイダンス

2022年7月
（Ver. 1.0）

暗号運用ガイドラインの一つとして
IPA・NICTが発行主体

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

『暗号鍵設定ガイダンス』とは

暗号技術に用いられる暗号鍵に対して**適切に鍵長を設定**し、
さらに適切に鍵管理を行って**安全に運用**していくための技術的ガイダンス

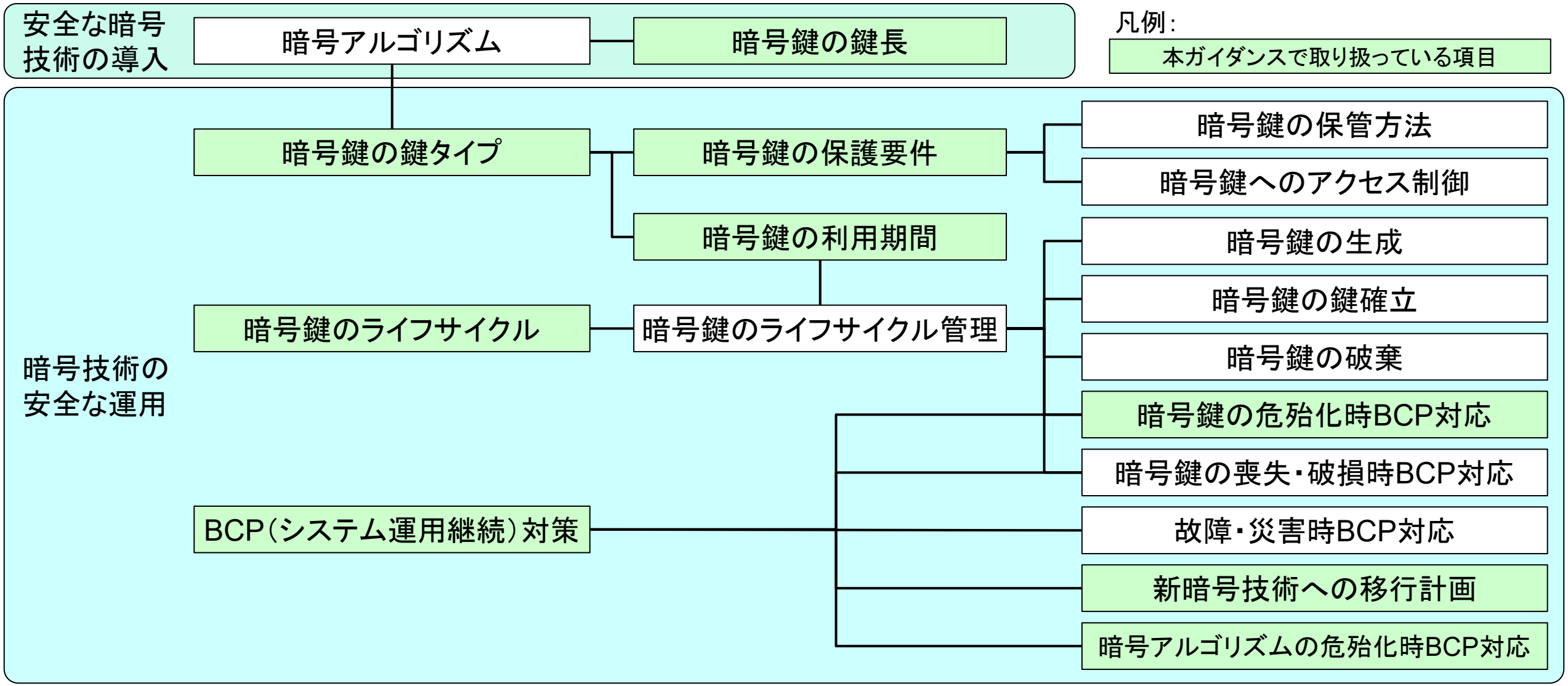
■ 想定読者

暗号技術を組込んだシステム又はアプリケーションの設計・開発・運用・提供にあたって、安全な暗号技術の選定、及び暗号技術の安全な運用方針・対策の作成や決定などに携わる管理者、設計者、開発者など

■ **「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」との位置づけの違いを明確化**

- **本ガイダンスは、暗号鍵についての鍵長設定や運用の考え方を解説するもので、強制的な要求（～しなければならない／～してはならない）は原則として使わない**
- **CRYPTREC暗号リストを利用していると見なされるためには、本ガイダンスではなく、「設定基準」のほうを利用して鍵長を設定しなければならない**

暗号鍵設定ガイダンスの取り扱い項目



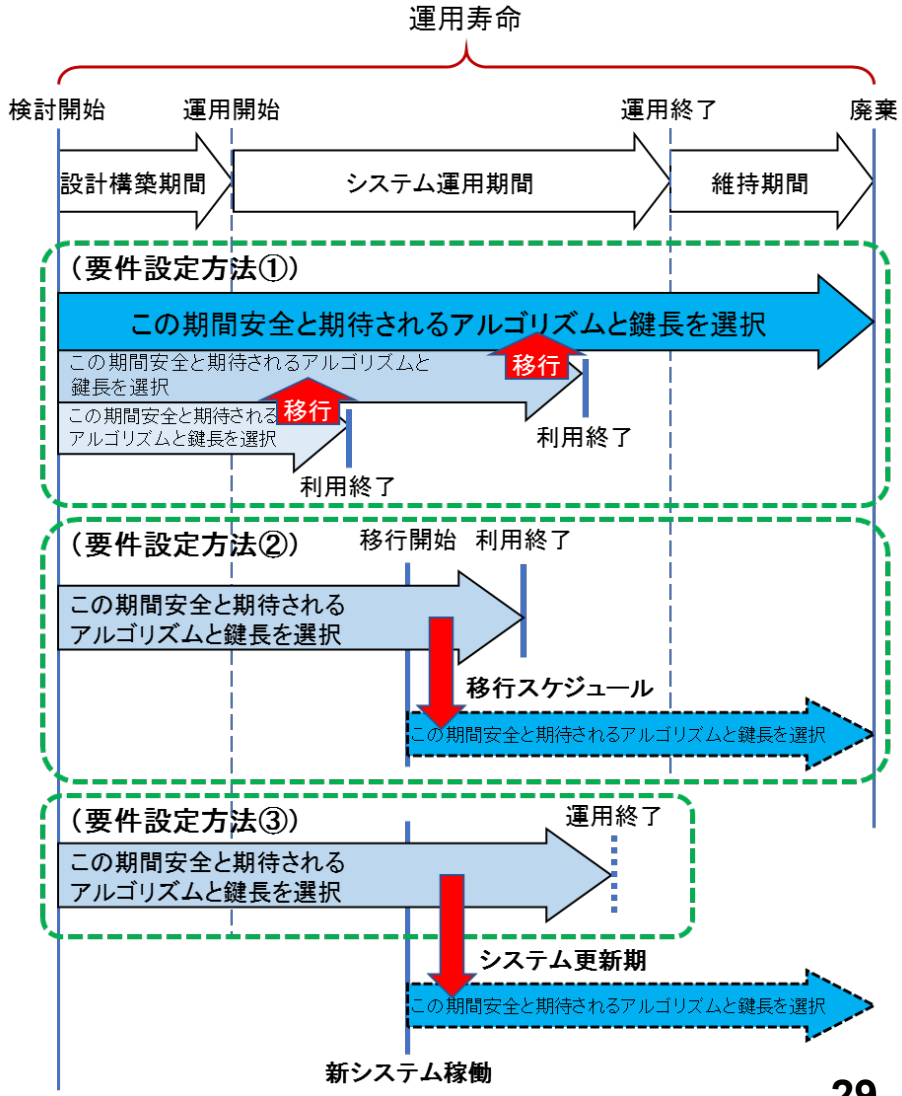
暗号鍵のセキュリティ強度要件（鍵長設定）の考え方

■ 今後10～15年程度なら安全と期待される強度（＝下限のビットセキュリティ強度）を提示
- ●一定のセキュリティマージンを追加したそれ以上のセキュリティ強度で設定
- ●Appendixに各国の推奨状況を記載

年	1982	2030	2040	2050	2060	2070
ANSSI	56	81 ～ 96	86 ～ 104	91 ～ 112	96 ～ 120	101 ～ 128
Lenstra	56	93	101	109	—	—
	56	88	95	102	—	—

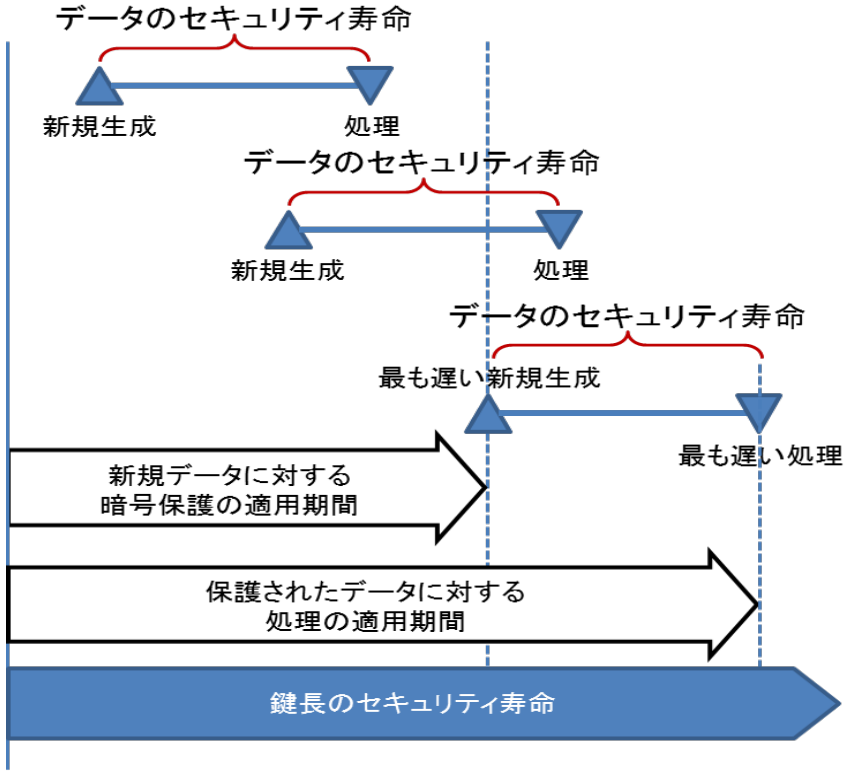
■ 暗号鍵の鍵長設定に影響を与える『寿命』
- ●システムの運用寿命
- ●鍵長のセキュリティ寿命
- ●データのセキュリティ寿命

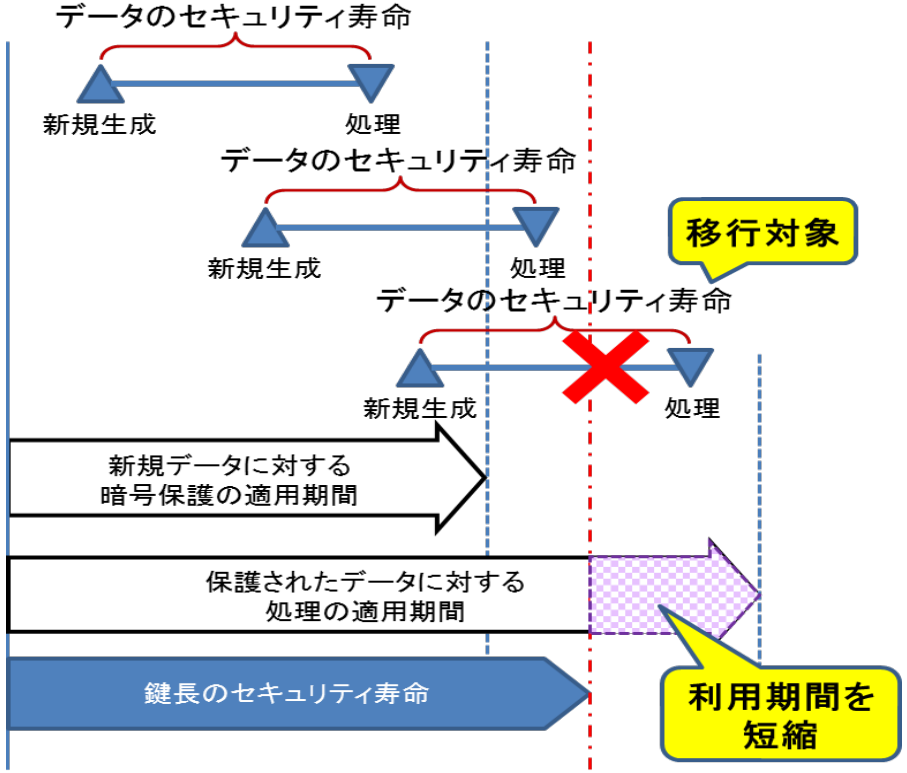
システムの運用寿命と求められるセキュリティ強度



鍵長の利用期間の考え方

データのセキュリティ寿命		
暗号化	通信時	（鍵共有後から）通信が終了するまでの期間
	保管時	データが暗号化されてから、復号する必要がなくなるまでの期間
	鍵共有	鍵共有を行っている期間
署名		署名生成してから、当該署名の署名検証を行う必要がなくなるまでの期間
メッセージ認証		MACを生成してから、当該データの完全性検証を行う必要がなくなるまでの期間
エンティティ認証		エンティティ認証を行っている期間





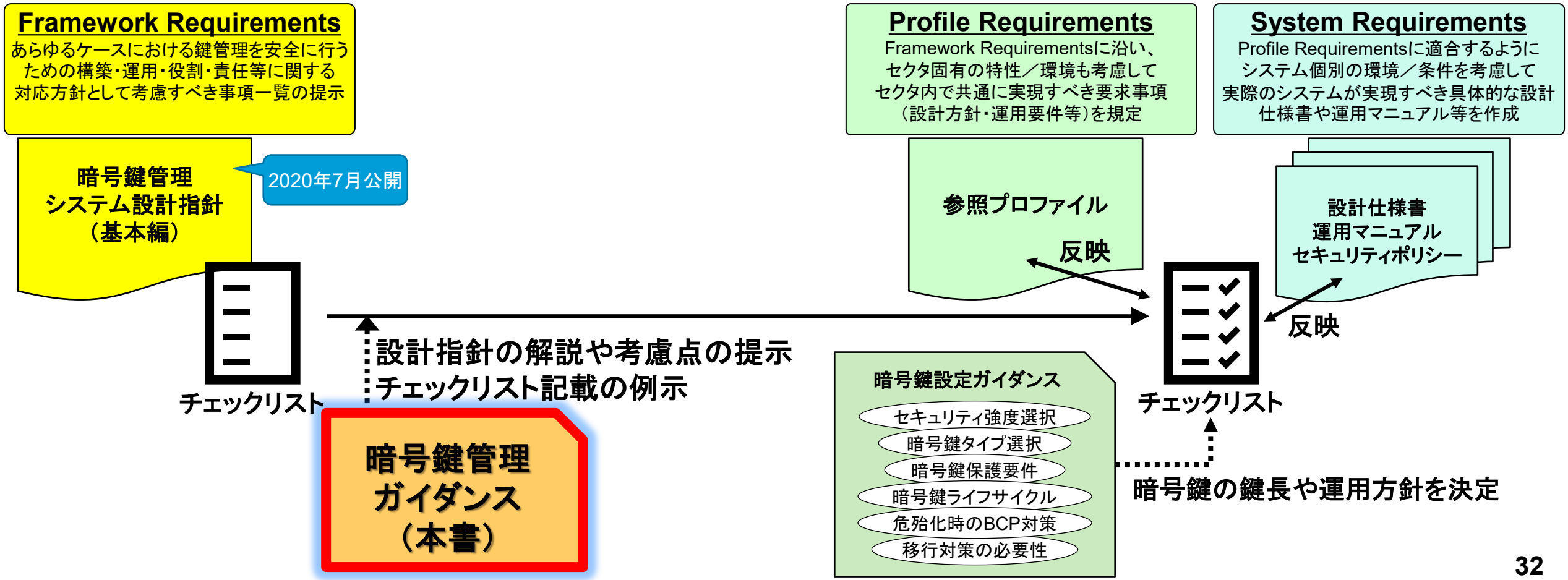
暗号鍵の種類（鍵タイプ）と保護要件

鍵タイプ	セキュリティ特性	関連性保護	保証の必要性	保護期間
データ暗号化対称鍵	機密性 完全性 可用性	● 当該鍵を共有しているエンティティ ● 暗号化データ	―	当該鍵の生成から、データのセキュリティ寿命が尽きる又は利用期間が終わるまでのいずれか遅い方の期間
鍵共有対称鍵	機密性 完全性 可用性	● 当該鍵を共有しているエンティティ ● 暗号化された鍵	―	当該鍵の生成から、利用期間が終わる又は暗号化された鍵が保護を必要としなくなるまでのいずれか遅い方の期間
鍵共有プライベート鍵	機密性 完全性 可用性	● 鍵共有公開鍵 ● 暗号化された鍵	保有	当該鍵の生成から交換した全ての鍵の保護期間が終了するまで
鍵共有公開鍵	完全性	● 鍵共有プライベート鍵	有効性	当該鍵の生成から利用期間終了まで
署名プライベート鍵	機密性 完全性	● 署名検証公開鍵	保有	当該鍵の生成から利用期間終了まで
署名検証公開鍵	完全性 可用性	● 署名プライベート鍵 ● 署名データ	有効性	当該鍵の生成から署名データの検証が不要になるまで
認証対称鍵	機密性 完全性 可用性	● 当該鍵を共有しているエンティティ ● 認証データ	―	当該鍵の生成から認証データの検証が不要になるまで
認証プライベート鍵	機密性 完全性	● 認証公開鍵	保有	当該鍵の生成から利用期間終了まで
認証公開鍵	完全性 可用性	● 認証プライベート鍵 ● 認証データ	有効性	当該鍵の生成から認証データの検証が不要になるまで

『暗号鍵管理ガイダンス』とは

「暗号鍵管理システム設計指針（基本編）」の**解説書**を目指す

- 暗号鍵管理プロファイルを作成するためのガイダンス
- 暗号鍵管理で必要となる項目について、シンプルなモデルを例示し説明



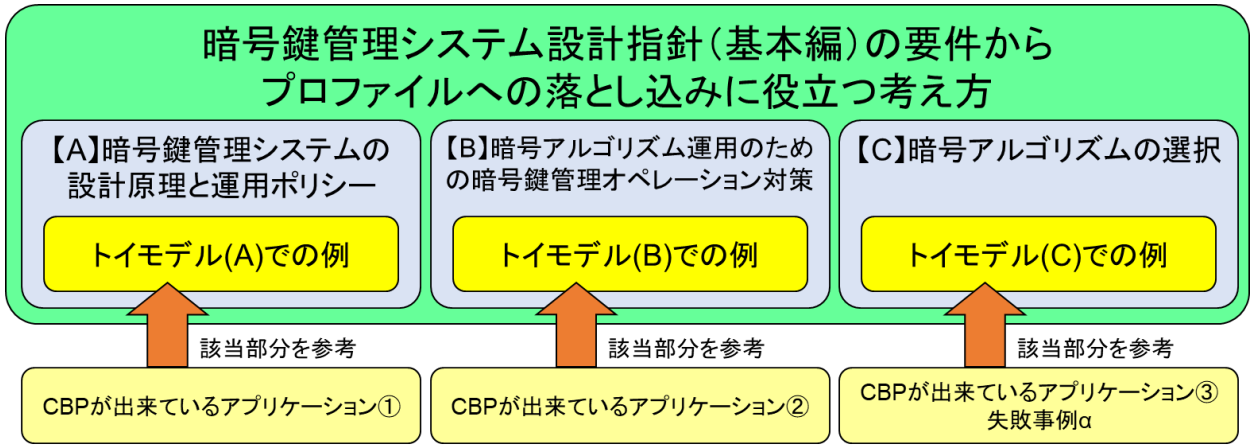
ガイダンス内容のイメージ

■ 暗号鍵管理システム設計指針（基本編）のFrame Requirementsについて「ガイダンスで記載する説明事項」と「チェックリストの記載例」を中心に説明

検討番号	*.**	―
要求内容	暗号鍵管理システム設計指針（基本編）の説明やFrame Requirementsの内容を基本的に引用	● 目的・趣旨 ● 要求事項 ● 記載内容
ガイダンスで記載する説明事項	**1. 要求に対する判断理由に関する考え方を記載 2. 必要に応じて、要求に関する補足説明を記載**	**● 解説・考慮点**
チェックリストの記載例	**トイモデルを利用した判断理由の記載内容を例示**	**● トイモデルとチェックリストの記載例**

■ チェックリストの解説にあたって、参考例として「トイモデル」を使う

●6つの目的別分類ごとに、理解しやすいトイモデルを用意



ガイダンス作成の進め方

■ 暗号鍵管理ガイダンスWGを設置して検討
主査：上原　哲太郎（立命館大学　情報理工学部　教授）

この後、「暗号化消去と暗号鍵管理」の講演をしていただきます

■ 要求内容に対する考え方について、以下の意義を考慮して記載内容を決定

- 鍵管理に必要な情報を集中的に管理できる
- 暗号鍵管理システム新規設計時に必要な要素を漏れなく検討できる
- Crypto Agility等、どの暗号アルゴリズムがどのように利用されているかを把握できる
- 情報アセットの洗い出しに利用できる（保護すべき企業の重要資産の洗い出しに利用可能）
- インシデント発生時のレスポンスが早くなる & 説明責任に有用
- 監査対象から各リスト項目が漏れる可能性を減らす
- 将来的な対策に有用。例えば、量子コンピュータの実現に伴う移行計画、災害時事業継続計画など

2022年度末の完成を目指して作成を進めていきます

本日紹介したドキュメントなど

- TLS暗号設定ガイドライン及び関連参考資料
  - CRYPTREC HP: https://www.cryptrec.go.jp/op_guidelines.html
  - IPA HP：https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html
- 暗号鍵管理システム設計指針（基本編）
  - CRYPTREC HP: https://www.cryptrec.go.jp/op_guidelines.html
  - IPA HP： https://www.ipa.go.jp/security/vuln/ckms.html
- 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準
  - CRYPTREC HP: https://www.cryptrec.go.jp/list.html
- 暗号鍵設定ガイダンス
  - CRYPTREC HP: https://www.cryptrec.go.jp/op_guidelines.html
  - IPA HP： https://www.ipa.go.jp/security/vuln/ckms_setting.html
- NIST SP日本語訳
  - IPA HP: https://www.ipa.go.jp/security/ipg/crypt.html

SP800-57 Part1 rev.5, SP800-88 rev.1, SP800-130, SP800-175A/B

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