CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術活用委員会活動報告

暗号鍵管理ガイダンスWG活動報告

2023年7月26日

暗号技術活用委員会 委員長
（横浜国立大学 教授） 松本　勉

暗号鍵管理ガイダンスWG　主査
（立命館大学 教授） 上原　哲太郎

目次

目次

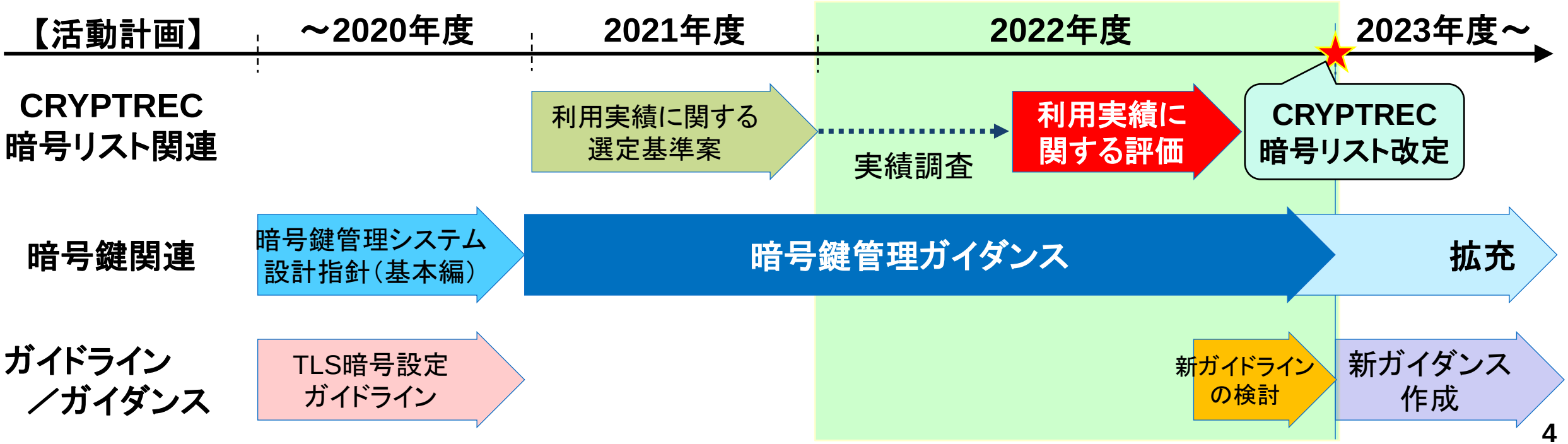
暗号技術活用委員会活動目的＆計画

【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活動体制（2021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

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 （耐量子計算機暗号）
- 暗号技術調査WG （高機能暗号）

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

暗号技術活用委員会委員

CRYPTREC
Cryptography Research and Evaluation Committees

（注）2023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	Microsoft Corporation　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	GMOサイバーセキュリティbyイエラエ株式会社　執行役員
委員	松本　泰	セコム株式会社　顧問
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

暗号鍵管理ガイダンスWG委員（2021-2022年度）（注）2023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	GMOサイバーセキュリティ byイエラエ株式会社　取締役CTO of Development
委員	菊池　浩明	明治大学　教授
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　係長
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

1. 暗号技術活用委員会　概要

2. 2022年度暗号技術活用委員会　活動概要
   - CRYPTREC暗号リスト改定　ー　利用実績に関する評価
   - 暗号鍵管理ガイドライン作成
   - 暗号利活用のために作成すべきガイダンス候補の検討

3. 暗号鍵管理ガイダンスWG　活動概要（上原主査より）
   - 暗号鍵管理ガイダンスの紹介

2022年度 暗号技術活用委員会審議状況

回	開催日	議案
メール	2022年7月7日 ～ 7月15日	• 2022年度暗号鍵管理ガイダンスWG活動計画について
第一回	2022年8月4日	• 2022年度暗号技術活用委員会活動計画について • 暗号アルゴリズム利用実績調査の中間報告について • 2022年度暗号鍵管理ガイダンスWG活動計画について • 暗号鍵管理ガイダンスWG進捗報告について • 運用ガイドライン／ガイダンス候補について
第二回	2022年12月20日	• 暗号アルゴリズム利用実績調査の最終報告について • 電子政府推奨暗号リスト掲載への推薦候補案について • 暗号鍵管理ガイダンスWG進捗報告について • 運用ガイドライン／ガイダンス候補について
第三回	2023年3月14日	• 暗号鍵管理ガイダンスWG活動報告 • 運用ガイドライン／ガイダンス候補について • 2022年度暗号技術活用委員会活動報告案について

CRYPTREC暗号リスト改定作業

【2019年度～2020年度　暗号技術検討会】

CRYPTREC暗号リストの構成

- ✓ CRYPTREC暗号リストについて、次の**3リスト構成は維持**し、リスト間の**遷移ルールを明確化**。
  - **①電子政府推奨暗号リスト**（安全性・実装性能が確認され、利用実績や普及見込みがあると判断されたもの）
  - **②推奨候補暗号リスト**（安全性・実装性能が確認され、今後①のリストに掲載される可能性のあるもの）
  - **③運用監視暗号リスト**（危殆化等により推奨すべき状態ではなく、互換性維持のために継続利用を容認するもの）
- ✓ 各暗号技術は十分成熟しているため、技術分類※は変更せず、新たな暗号技術の公募は実施しない。
  ※7分類：公開鍵暗号／共通鍵暗号／ハッシュ関数／暗号利用モード／メッセージ認証コード／認証暗号／エンティティ認証

CRYPTREC暗号リストの今後の改定

- ✓ 2003年に作成、2013年に改定を行い、**今般、2023年目途に改定作業中**であり、10年単位で改定。
- ✓ 常に危殆化等の監視を行い、必要に応じた暗号技術の加除等も行っており、10年単位とする必要はない。

→ 次の改定以後は、改定後5年以内を目途に暗号技術検討会において改定是非を判断することとする。

【2021年度　暗号技術検討会】

利用実績による選定基準の策定

- ✓ 遷移ルールに基づき、「推奨候補暗号リスト」から「電子政府推奨暗号リスト」に昇格させるための**利用実績による選定基準（選定ルール）を明確化**。

利用実績による選定基準

考慮項目		選定目安
採用実績	以下のいずれかを満たす場合、昇格の検討対象に含める。なお、採用実績は、 • 5年ごとに実施予定の大規模アンケート調査による「**利用実績調査**」 • 必要に応じて、事務局が（大規模アンケート調査によらずに）情報収集する「**利用実態確認**」 により確認するものとする。	
	① **利用実績調査**の結果、電子政府推奨暗号リストに掲載されている（同一カテゴリの）暗号技術の採用実績と遜色がないことが確認された場合	電子政府推奨暗号リスト掲載の（同一カテゴリの）暗号技術の採用実績と同等以上の採用実績がある推奨候補暗号リスト掲載の暗号技術を昇格検討対象とする。
	② **利用実績調査**又は**利用実態確認**の結果、**電子政府システムや重要インフラ等日本の基幹システム**においてすでに利用されていることが確認された場合	必要に応じて、利用実績調査に代わって、各府省庁等への照会を実施し、照会結果（クローズドな利用を含め）を基に昇格検討対象を選定する。
	利用実績調査又は**利用実態確認**の結果、③～⑤のいずれかが確認された場合： ③ **利用者が多い主要な汎用製品群の複数**に搭載されるなど、明らかに採用が進展していると判断された場合 ④ **利用者が多い主要なオープンソースソフトウェアの複数**に搭載されるなど、明らかに採用が進展していると判断された場合 ⑤ **利用者が多い主要なサービスやプロトコルの複数**で利用されるなど、明らかに採用が進展していると判断された場合	「複数」「利用者が多い（主要な）」というキーワードの両方を十分に満たし、明らかな採用促進が確認された場合には、必要に応じて、昇格検討対象とする。 ※「複数」の意味は、必要条件として「2個以上が必要」ということであって、「2個以上あればよい」という十分条件としての意味ではないことに留意
標準化実績	以下を満たす場合、昇格の検討対象に含める。	
	⑥ **利用実績調査**の結果、電子政府推奨暗号リストに掲載されている（同一カテゴリの）暗号技術の採用実績と遜色がないことが確認された場合	電子政府推奨暗号リスト掲載の（同一カテゴリの）暗号技術の採用実績と同等以上の採用実績がある推奨候補暗号リスト掲載の暗号技術は昇格検討対象とする。

電子政府推奨暗号リストへの選定方法

暗号技術評価委員会で特定の暗号技術につき
安全性及び実装性の評価を実施し、
その結果により暗号技術検討会が**推奨候補暗号リストに含めると決定**

暗号技術活用委員会は、**利用実績による選定基準**に基づき、
電子政府推奨暗号リスト掲載への**昇格の検討対象となる暗号技術を検討・選定**し、暗号技術検討会に推薦

暗号技術検討会では、推薦された暗号技術に対し、**根拠となる利用実態につき再度の確認・審議**を行い、電子政府推奨暗号リスト掲載への昇格に問題がないと判断した場合**電子政府推奨暗号リスト掲載暗号技術に選定**

利用実績調査概要

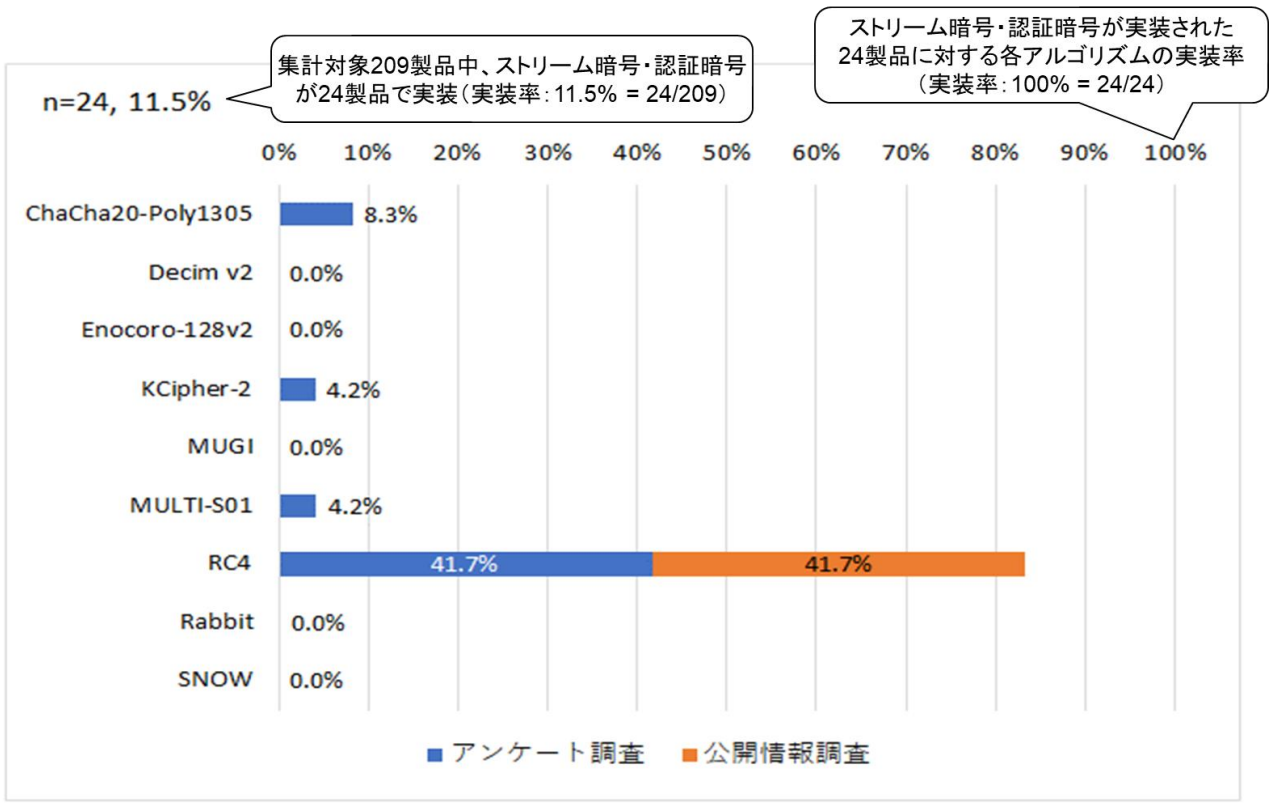
IPAが実施した「利用実績調査」結果を活用

調査対象	実績
(A) 応募暗号アルゴリズムの応募者に対するアンケート調査	• 全8社から回答受領
(B) 暗号アルゴリズムを搭載している市販製品の販売会社への調査	• アンケート回収数：211社301製品（※配布数：2,600社以上） ⇓ **• 集計対象数：101社209製品** • アンケート有効集計：60社109製品 • 公開情報調査（補充調査）：41社100製品
(C) 日本の政府機関等に対する調査	**• 集計対象数：98省庁システム** **• 集計対象規格数：17件**
(D) 国際標準規格・民間規格等に対する調査	**• 集計対象規格数：171件** • 規格調査数：IPAが指定した25件 • 別途追加規格調査結果：146件
(E) オープンソースソフトウェアでの利用実績調査	**• 集計対象規格数：30件**

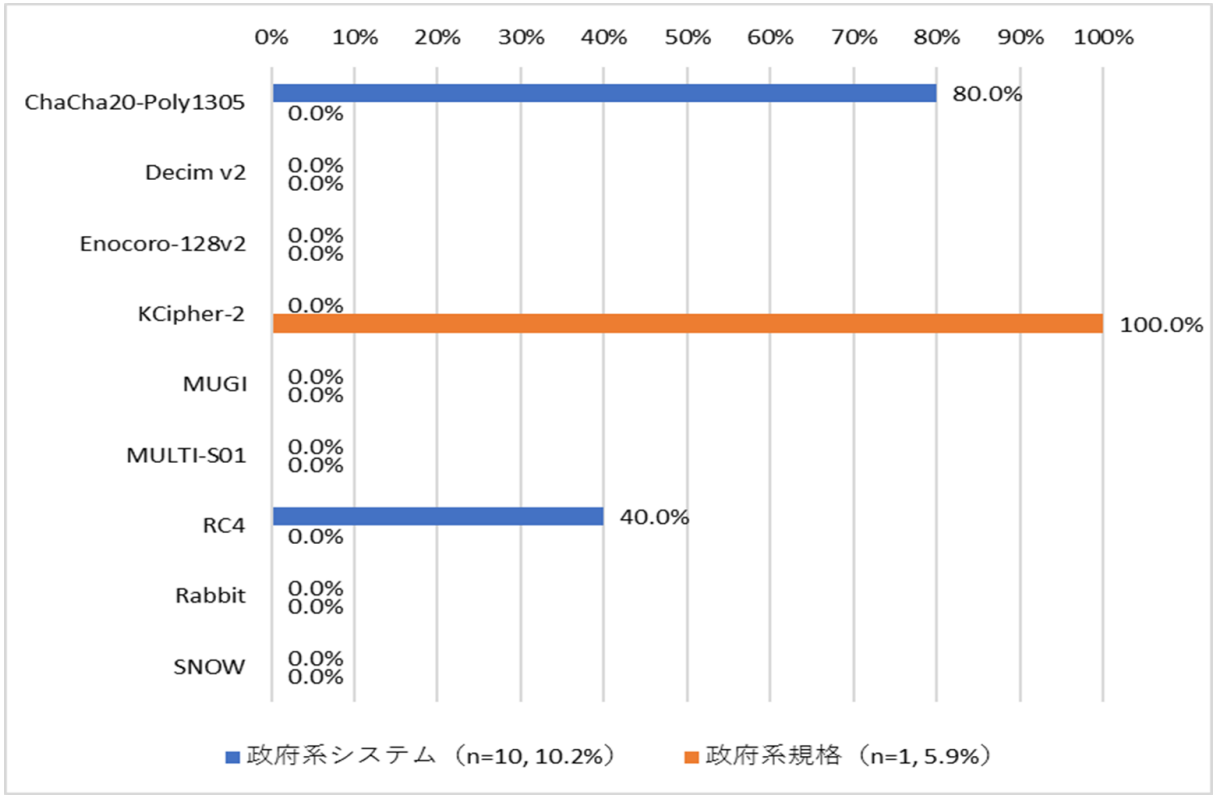
利用実績ー例：共通鍵暗号（ストリーム暗号・認証暗号）

技術分類ごと・調査対象ごとに集計。同一技術分類の暗号技術の利用実績を比較

市販製品（共通鍵暗号（ストリーム暗号・認証暗号））



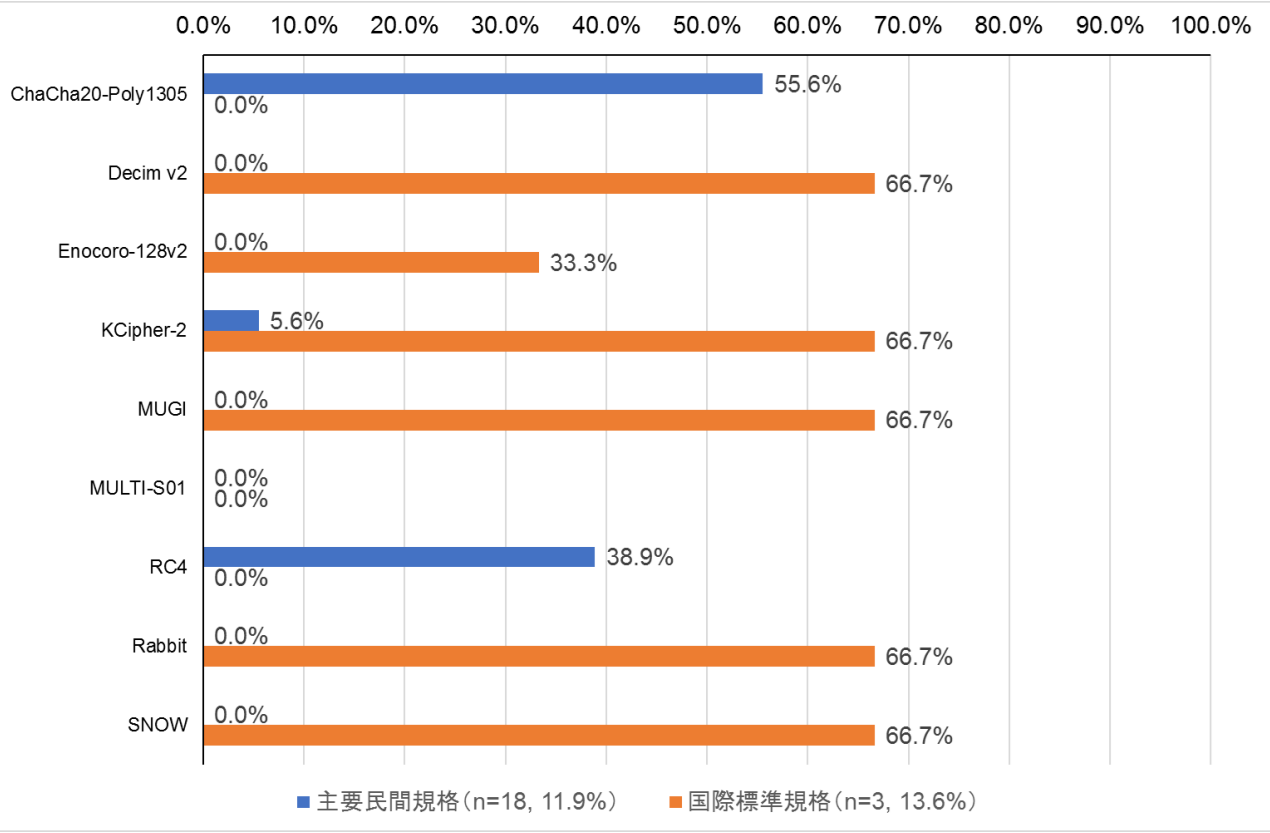
政府系情報システム・規格（共通鍵暗号（ストリーム暗号・認証暗号））



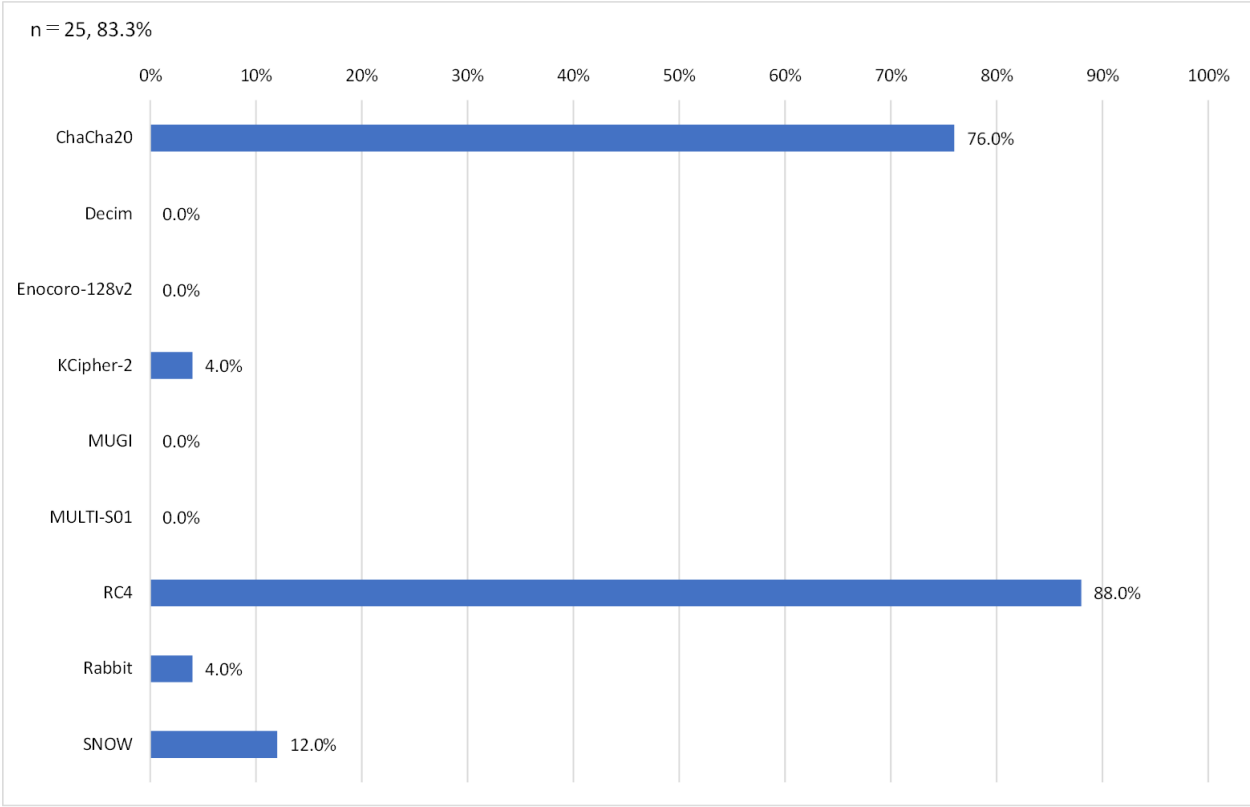
利用実績ー例：共通鍵暗号（ストリーム暗号・認証暗号）

技術分類ごと・調査対象ごとに集計。同一技術分類の暗号技術の利用実績を比較

標準規格・民間規格（共通鍵暗号（ストリーム暗号・認証暗号））



オープンソースソフトウェア（共通鍵暗号（ストリーム暗号・認証暗号））



電子政府推奨暗号リスト掲載への推薦候補案選定

技術分類		推薦候補	推薦しない候補	理由
公開鍵暗号	署名	**EdDSA**	該当なし	● **考慮項目④において、他の署名と比較して利用実績があると認められる**
	鍵共有	**該当なし**	PSEC-KEM	● 他の鍵共有と比較して優位な利用実績があるとは認められない
共通鍵暗号	64ビットブロック暗号	**該当なし**	CIPHERUNICORN-E Hierocrypt-L1 MISTY1	● 他の64ビットブロック暗号と比較して優位な利用実績があるとは認められない
	128ビットブロック暗号	**該当なし**	CIPHERUNICORN-A CLEFIA Hierocrypt-3 SC2000	● 他の128ビットブロック暗号と比較して優位な利用実績があるとは認められない
	ストリーム暗号	**該当なし**	Enocoro-128v2 MUGI MULTI-S01	● 他のストリーム暗号と比較して優位な利用実績があるとは認められない

技術分類		推薦候補	推薦しない候補	理由
ハッシュ関数		**SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE128 SHAKE256**	該当なし	● **考慮項目④において、他のハッシュ関数と比較して利用実績があると認められる**
認証暗号		**ChaCha20-Poly1305**	該当なし	● **考慮項目①②④について、利用実績があると認められる**
暗号利用モード	秘匿モード	**XTS**	該当なし	● **考慮項目①②④について、他の秘匿モードと比較して利用実績があると認められる**
メッセージ認証コード		**該当なし**	PC-MAC-AES	● 他のメッセージ認証コードと比較して優位な利用実績があるとは認められない
エンティティ認証		**ISO/IEC 9798-4**	該当なし	● **考慮項目①②において、他のエンティティ認証と比較して利用実績があると認められる**

暗号利活用のためのガイダンス

■ 暗号鍵管理ガイダンス

この後に 上原主査 から報告

■ 2023年度以降の運用ガイドライン／ガイダンス作成に向けた検討

1	認証についてのガイダンス（特に二要素認証）
2	身元（本人）確認のためのガイダンス（例えばeKYC）
3	電子メールに関するガイドライン／ガイダンス
4	クラウドにおける鍵管理ガイダンス
5	組込機器の開発における、暗号プロトコル（例：認証プロトコル）のパラメータ選定基準
6	経営層も含めた人達を対象にした、暗号技術の啓発ドキュメント
7	暗号の使い方に関するガイドライン（ガイダンス）
8	PKIガイドライン（ガイダンス）
9	暗号化消去
10	DNSの暗号に関わるガイドライン（ガイダンス）
11	暗号資産

12	eシール
13	APIに関するガイドライン／ガイダンス
14	高機能暗号の標準化
15	耐量子計算機暗号のガイダンス
16	耐量子計算機暗号への移行に関するガイダンス
17	FIDOなどの普及促進を促すガイダンス
18	リモート署名などの普及促進を促すガイダンス
19	暗号化消去などの普及促進を促すガイダンス
20	**TLS暗号設定ガイドラインのアップデート**
21	運用ガイドラインやガイダンスに求められるニーズ／課題の整理

2023年度
実施決定

目次

1. 暗号技術活用委員会　概要

2. 2022年度暗号技術活用委員会　活動概要
   - CRYPTREC暗号リスト改定　ー　利用実績に関する評価
   - 暗号鍵管理ガイドライン作成
   - 暗号利活用のために作成すべきガイダンス候補の検討

3. 暗号鍵管理ガイダンスWG　活動概要（上原主査より）
   - 暗号鍵管理ガイダンスの紹介

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	Microsoft Corporation　セキュリティプログラムマネージャー
委員	菅野　哲	GMOサイバーセキュリティ byイエラエ株式会社　取締役CTO of Development
委員	菊池　浩明	明治大学　教授
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　係長
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

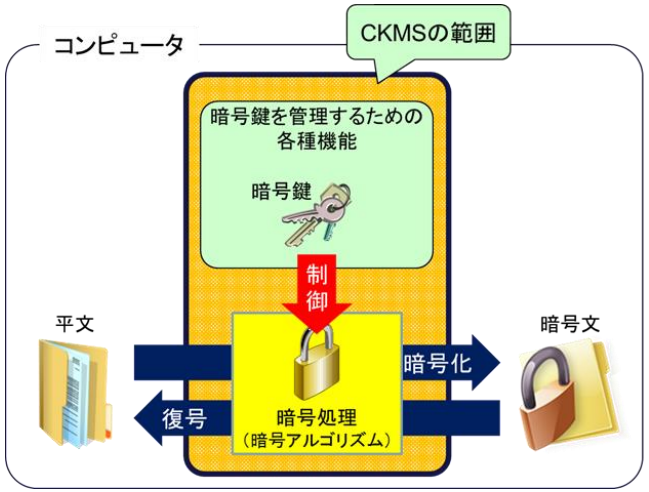
『暗号鍵管理システム設計指針（基本編）』とは

CRYPTREC Cryptography Research and Evaluation Committees

2020年7月7日公開

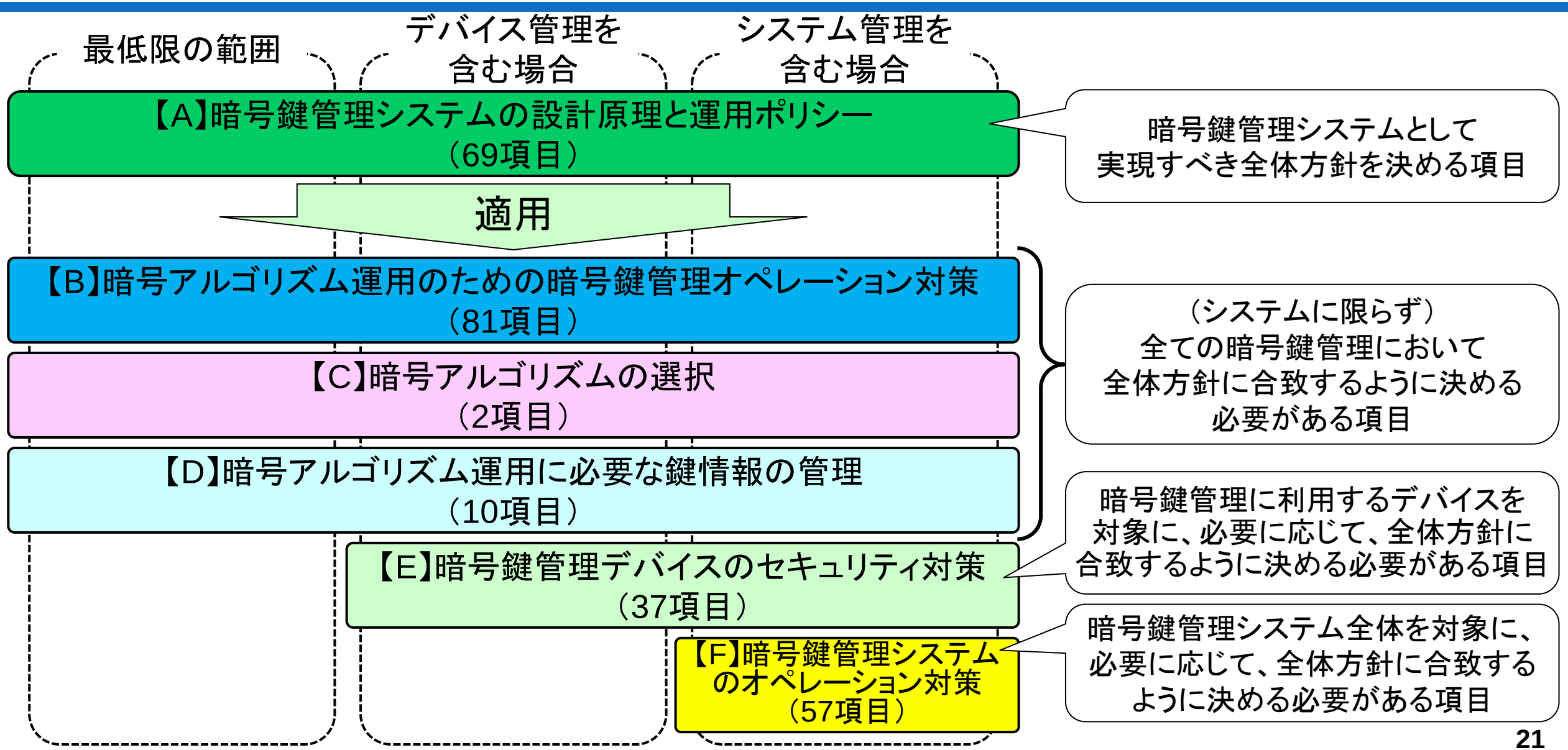
あらゆる分野／領域の暗号鍵管理システム（CKMS）を対象に
暗号鍵管理を安全に行うための構築・運用・役割・責任等に関する
対応方針として考慮すべき検討事項（Framework Requirements）を網羅的にカバーする指針

- 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

暗号鍵管理における目的別分類関係



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

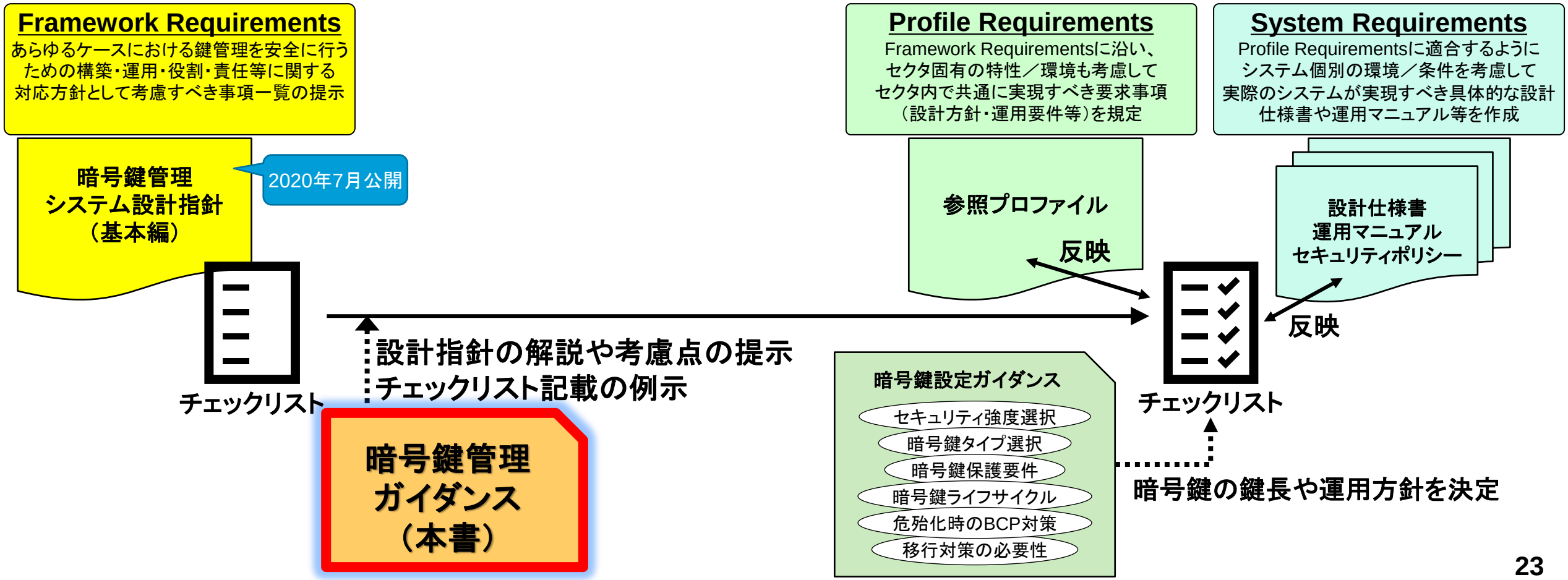
SP800-57 Part3、**TLS暗号設定ガイドライン**

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

『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

■ 位置づけ

- 「暗号鍵管理システム設計指針（基本編）」を詳しく解説し、記載が求められる項目について検討する際の**有用な副読本**となることを目的とする
  具体的には、「暗号鍵管理システム設計指針（基本編）」で記載されている以下の項目に関して、各検討項目についての**解説・考慮点を具体的に説明**する
  - 【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
  - 【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
- 理解を助けるため、**シンプルなモデル（トイモデル）を例示**し説明する
- シンプルなモデルを用いた説明においては、鍵管理における**要求や思想が理解できるような記載**を行う（**※“推奨しているわけではない”ことに注意**）
- 暗号鍵管理における特に注意すべきリスクを説明する

■ 想定読者

- 暗号鍵管理機能を持つシステム設計者

2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

CRYPTREC Cryptography Research and Evaluation Committees

CKMS設計における、暗号鍵の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

- 2.1CKMS設計
- 2.2暗号鍵のライフサイクル

→ CKMS設計の全体的な考え方の整理

2.1/2.2で決めた内容と矛盾しないように決める

- 2.3 暗号鍵のライフサイクル管理機能
- 2.4 鍵情報の保管方法
- 2.5 鍵情報の鍵確立方法

→ 上記の考え方を実現するために必要となる機能要件や運用方法の明確化

- 2.6 鍵情報の喪失・破損時のBCP対策
- 2.7 鍵情報の危殆化時のBCP対策

→ BCP対策（例外運用方法）の明確化

2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

CRYPTREC Cryptography Research and Evaluation Committees

2.1 CKMS設計

① 暗号鍵を提供するためにCKMSをどのように構築するかの概要

- CKMSを**どのような設計方針の下でどのように構築されるのかの高レベルの概要**整理
- 次節以降に決める必要がある事項を検討する際に**本概要で定めたことと矛盾していないことが確認できる程度に具体化した情報**のことであり、**次節以降では、本概要に記載したことに矛盾するような内容を定めてはならないことに注意**
- CKMS設計としてどこまでの範囲を対象とするのかを決め、それに応じて境界を定める

2.2 暗号鍵のライフサイクル

① 暗号鍵のライフサイクル全体にわたって取り得る鍵状態及び遷移条件の決定

- CKMS設計の観点からは、**どのような状態が存在し、どのような条件によって状態遷移が起きるのか**を明らかにする
- **本節で記載したことと次節での内容とが整合的であるようにしなければならないことに注意**

2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

CRYPTREC Cryptography Research and Evaluation Committees

2.3 暗号鍵のライフサイクル管理機能

① 鍵情報に対する管理のために実行される機能の全体像

- 暗号鍵のライフサイクル管理機能として②以降で対象となる機能を全て明記することによって、**詳細を定めなければいけない項目に抜けが生じないようにする**
- ライフサイクル管理機能が暗号鍵のライフサイクルを実現するための手段であるので、**2.2節で記載したことと整合的であるようにしなければならない**
- 鍵情報が誤った使い方をされていないことを確認

② 鍵活性化機能への要求事項

- 活性化前状態から活性化状態への遷移を実現するための手順や遷移条件を具体化
- 2.2節で記載した活性化状態への遷移条件と整合的であるようにしなければならない

③ 暗号機能の実行場所の特定

- 暗号機能が実行されるところでは必ず暗号鍵が平文の形で使われることになるため、暗号鍵が保管される場所と並んで、もっとも暗号鍵の危殆化が発生しやすい場所
- したがって、暗号機能がある場所や実行場所を把握しておくことで、暗号鍵が狙われるリスクを低減させるために重点的に対策・保護すべき場所の絞り込みに活用できる

2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

CRYPTREC Cryptography Research and Evaluation Committees

2.6 鍵情報の喪失・破損時のBCP対策

① 鍵情報の喪失・破損に対するBCP対策の決定

- 鍵情報（暗号鍵やメタデータ）が喪失又は破損した場合で、バックアップもアーカイブもされていなかった場合、当該暗号鍵で保護されているデータの喪失につながる可能性がある
- 重大な災害は、多数の運用中の鍵情報の喪失又は破損を一気に引き起こす可能性が高い
- 鍵情報の喪失や破損時のBCPを実現するためにどのような対策が必要かを検討し、その結果、**鍵情報のバックアップやアーカイブを行うこととした場合には、バックアップやアーカイブの方針をまず定める必要**がある
- ここで定めたことは**B.52～B.61（バックアップ方法／アーカイブ方法／復元方法）の上位規定として機能することから、B.52～B.61の内容はここでの内容に沿って設定されなければならず、また矛盾していないことを確認することが重要**

3章 暗号アルゴリズムの選択

CKMS設計では、要求される保護レベル（セキュリティ強度）を満たすように暗号アルゴリズムと鍵長を決定しなければならない

セキュリティ強度 → 暗号アルゴリズムと鍵長

3.1 暗号アルゴリズムのセキュリティ

① 要求される保護レベル（セキュリティ強度）に対応した暗号アルゴリズムの決定

- セキュリティ強度の決定では、扱う情報の資産価値、情報の機密性や完全性などのほか、該当システムの利用期間の終了年も重要な要因の一つ
- 具体的に必要なセキュリティ強度の決定にあたっては、**「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」又は「暗号鍵設定ガイダンス」を参考**
- 資産価値が高い情報と評価されると、その情報を扱うシステムではより強いセキュリティが求められることがある

4章 暗号アルゴリズム運用に必要な鍵情報の管理

管理すべき暗号鍵を漏れなく洗い出し、2章で用意される機能や運用方法等を適切に組み合わせてそれらの暗号鍵を安全に管理していることを明確にする

- 4.1 鍵情報の種類 ・・・ 暗号鍵とメタデータの説明
- 4.2 鍵情報の選択 ・・・ 暗号鍵の洗い出しと個々の暗号鍵に対する管理方法を明確化
- 4.3 鍵情報の保護方針 ・・・ 主にメタデータを対象とした保護方針が対象

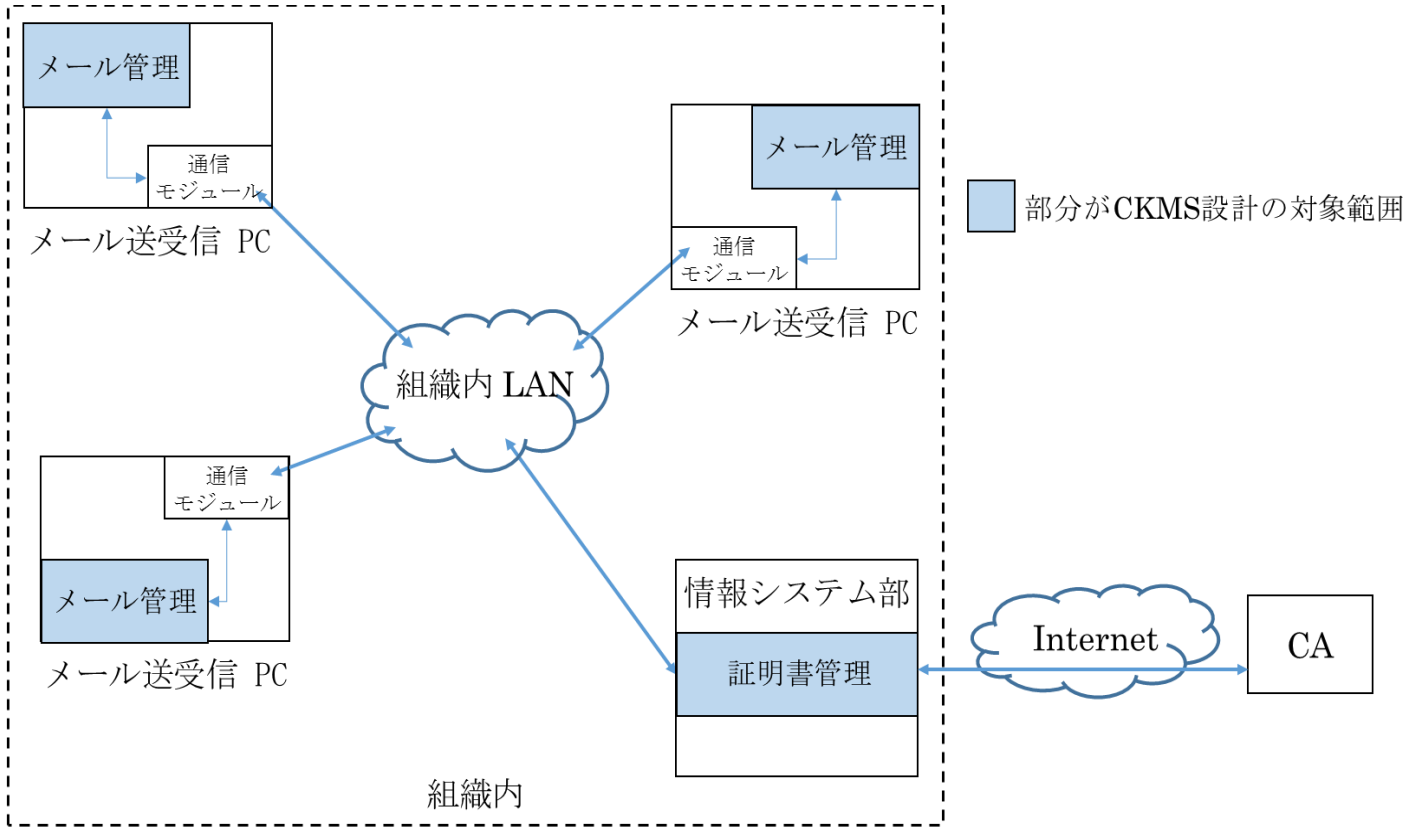
4.2 鍵情報の選択

① 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、保護方針などの決定

- CKMS設計で**明示的に選択や管理する必要がある全ての鍵（タイプ）が対象**
- CKMS設計で明示的に選択や管理しておらず、プロトコルや製品仕様により**内部処理として自動的に生成・使用される暗号鍵は基本的には含まない**
- 製品やアプリケーション、システムが自動的に生成・使用される暗号鍵を**「ブラックボックスとして使っている」という認識を持つ**ことが重要。信頼性に確信が持てない暗号モジュールを使用している場合などは、可能であれば、内部の処理を調査し、暗号鍵の信頼性を確認することが望ましい
- 暗号鍵とメタデータが正しく関連付けられていることを保証するための方法を明確化し、利用用途や想定される脅威等を踏まえて必要なセキュリティ強度を提供する機能や方法を選択することが重要

2章で取り扱うトイモデル

■ メールの送信元認証をS/MIMEの署名付きメールで実現するシステム

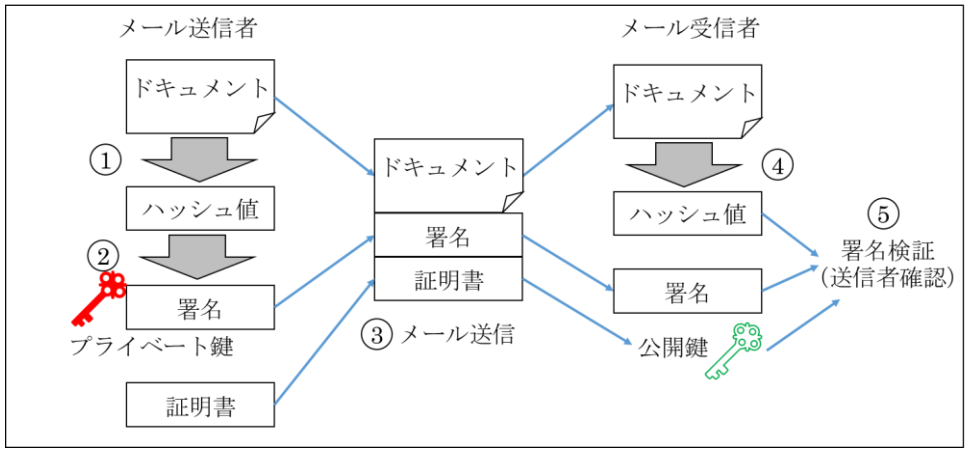


※ メール送受信などを処理する通信モジュールは含まない

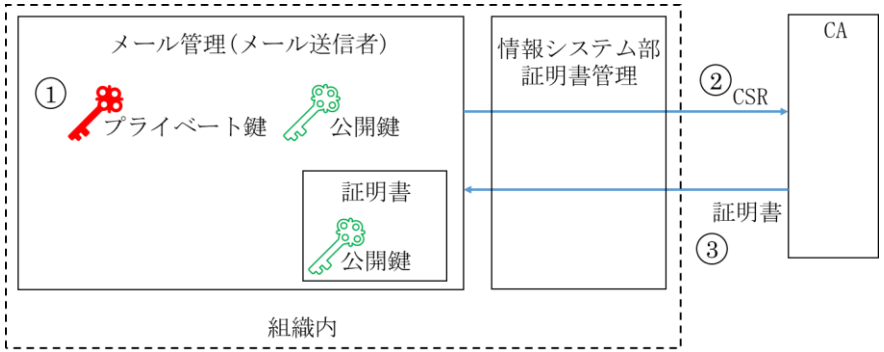
※ CAは、外部のパブリックCAであり、CKMSには含まない

【CKMS設計範囲】

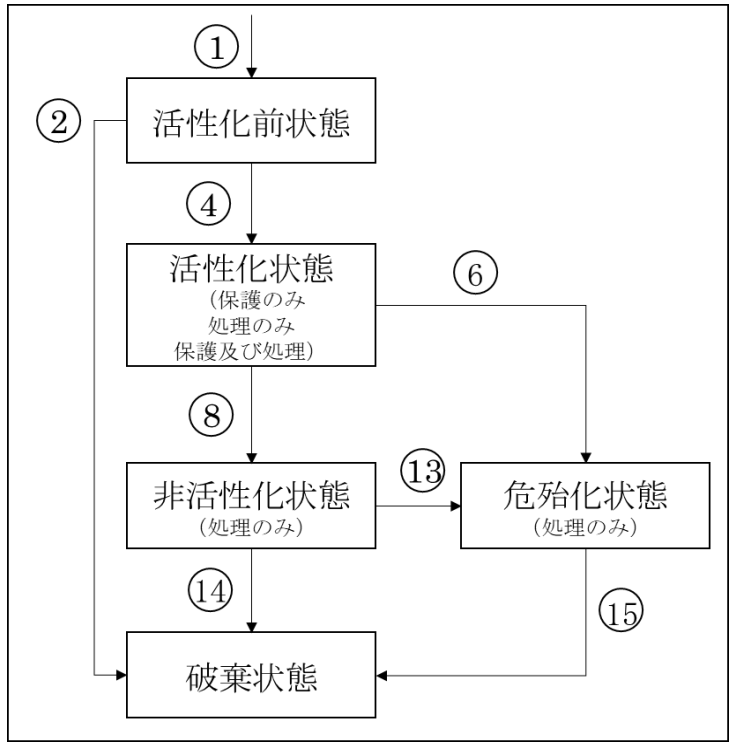
- メールの署名生成と署名検証の処理



- 署名生成や署名検証に使う暗号鍵の管理
- 公開鍵証明書の発行処理



2章のトイモデルでの運用条件



【トイモデルで設定するライフサイクル】

- 有効期間前の活性化前状態、有効期間内の活性化状態、有効期間後の非活性化状態に遷移（証明書の有効期限ベースに自動遷移）
- 実際に鍵が破棄されると破棄状態に遷移（手動）
- 署名プライベート鍵の危殆化が疑われる場合は危殆化状態に遷移
- 署名プライベート鍵が危殆化状態に遷移した場合、署名公開鍵も同時に危殆化状態に遷移
- 一時停止状態は設定しない
- これら以外の遷移条件は設定しない

【システム運用条件（一部）】

- 暗号鍵生成はメール送信PCにおいて信頼できる方法で生成し、プライベート鍵はライフサイクル全般を通じてPC外部に複製されることはない。
- CAから公開鍵証明書を受信したときに、当該証明書の正当性を確認する。
- 公開鍵証明書の有効期間が始まった鍵ペアは自動的に活性化状態となる。
- 署名の生成や検証は、メール送受信PCのメール管理部でのみ行う。
- 署名付きメールを受信したとき、受信した公開鍵証明書の正当性を検証する。公開鍵証明書の有効期限切れした鍵ペアは、自動的に非活性化状態になる。
- 鍵の所有者が当該鍵を必要ないと判断したとき、手動で削除する。
- 情報システム部を介してパブリックなCA局に署名を依頼することで、信頼できる証明書チェーンを構築し、基本的なトラストアンカー管理は更新機能などOSの機能より実現する。
- 公開鍵証明書の運用管理は、情報システム部の担当者が行う。
- 暗号鍵の危殆化が疑われるときは失効処理を行う。
- 暗号鍵のバックアップ、アーカイブは行わない。
- 暗号鍵とメタデータの関連付けは公開鍵証明書により行う（暗号学的プロセス）。
- メタデータの変更・削除・リスト化は認めない。
- 暗号鍵の一時停止状態は設定しない。
- 鍵導出機能や鍵更新機能は使用しない。
- 対象鍵は使用しない。
- 鍵情報の機密性や完全性は、OSのアクセスコントロールシステムにより保護する。
- 個々のメール利用者が使用するPCにおいて、使用しているOSのログ保存機能により、署名プライベート鍵のアクセスログを管理する。アクセスログはシステム管理者しか確認できない。

2章のトイモデルでのチェックリスト記載例

B.01	a) 利用するそれぞれの鍵タイプ 署名プライベート鍵、署名公開鍵 b) 鍵が生成される場所と手段 鍵の生成はメール送信者のPCで行われる 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 鍵の有効期間、親鍵（CAの署名公開鍵）、CAとの信頼関係 d) 鍵情報（暗号鍵やメタデータ）が存在しているそれぞれのエンティティのストレージにおける、鍵情報（暗号鍵やメタデータ）の保護方法 署名プライベート鍵はアクセスコントロールで保護される e) 配送時の鍵情報（暗号鍵やメタデータ）の保護方法 メール受信者に送信する公開鍵証明書はCAが署名している f) 鍵情報（暗号鍵やメタデータ）が配送され得る先となるエンティティの種類（例えば、ユーザ、ユーザデバイス、ネットワークデバイス） 公開鍵証明書はメールを送受信するユーザに配布
B.02	活性化前状態、活性化状態、危殆化状態、非活性化状態、破壊状態
B.03	● 署名プライベート鍵と署名公開鍵の鍵ペア生成後に活性化前状態に遷移 ● 証明書に記載された有効期間の開始時に活性化前状態から活性化状態に遷移 ● 活性化状態に遷移前に署名プライベート鍵に問題が生じた場合は、活性化前状態から破壊状態へ遷移 ● 有効期限の終了時に活性化状態から非活性化状態に遷移 ● 鍵の破壊条件を満たした場合に非活性化状態から破壊状態に遷移 ● 活性化状態に遷移後に署名プライベート鍵の危殆化が疑われる事象が発生した場合は、活性化状態又は非活性化状態から危殆化状態に遷移。署名公開鍵も同時に危殆化状態に遷移させる ● 証明書失効リスト（CRLリスト）に記載された署名公開鍵は危殆化状態に遷移 ● 危殆化処理完了時に破壊状態に遷移 ● 上記以外の遷移は設定しない

B.04	● メール送信者PCの鍵生成機能により、署名プライベート鍵と署名公開鍵を生成する。 ● 公開鍵証明書の有効期間が開始したら、鍵活性化機能により、署名プライベート鍵と署名公開鍵を活性化状態にする。 ● メール送信者PCの暗号機能により、メールのドキュメントに署名する。 ● メールを受信したら、メール送信者から送られてきたことを確認するために、メール受信者PCの暗号機能により署名の完全性を確認する。 ● 公開鍵の検証機能により、署名公開鍵に対する公開鍵証明書に対する完全性を確認し、公開鍵及びパラメタの検証を行う。 ● OSでのトラストアンカー管理機能により、ルートCAの公開鍵証明書を保管・管理する。情報の更新は、OS又はブラウザの自動アップデートにより実施する。 ● 公開鍵証明書の有効期間が終了したら、鍵非活性化機能により、署名プライベート鍵と署名公開鍵を非活性化状態にする。 ● 署名プライベート鍵と署名公開鍵は、破壊条件を満たした場合、破壊機能により、鍵を破壊する。 ● 署名プライベート鍵の危殆化が疑われるときは、鍵失効機能により、署名プライベート鍵の失効処理を行う。署名公開鍵についても同様の処理を行う。 ● 利用者の管理は情報システム部が行うものとし、そのために必要な管理機能は情報システム部管理の機器により実現する。 ● 暗号鍵とメタデータの検証及び関連付けについては、公開鍵証明書の申請段階で情報システム部がその正当性を検証するものとし、そのために必要な管理機能は情報システム部管理の機器により実現する。
B.05	● 署名公開鍵と関連メタデータの完全性は、公開鍵証明書のCA署名検証により確認する。 ● 署名プライベート鍵の機密性は、OSのファイルアクセス機能により当該鍵を作成したユーザ以外が鍵ファイルにアクセスできないように管理することで実現する。 ● CAの署名公開鍵はOSの信頼できる公開鍵証明書（トラストアンカー）からなるチェーンの有効性により完全性を確認する。 ● OSの信頼できる公開鍵証明書（トラストアンカー）の更新は、OS又はブラウザの自動アップデートにより実行される。

暗号鍵管理ガイダンスの拡充を目指します

■ 2023年度以降も暗号鍵管理ガイダンスWGを継続します

ガイダンス章構成 （凡例：✔ 記載対象）	2022年度版 暗号鍵管理ガイダンス	今後拡充する部分
1. 初めに	✔	✔
2. 暗号鍵管理システム（CKMS）の設計原理と運用ポリシー		✔
3. 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	✔	
4. 暗号アルゴリズムの選択	✔	
5. 暗号アルゴリズム運用に必要な鍵情報の管理	✔	
6. 暗号鍵管理デバイスへのセキュリティ対策		✔
7. 暗号鍵管理システム（CKMS）のオペレーション対策		✔

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