CRYPTREC Report 2022

令和 5 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、デジタル庁、総務省及び経済産業省が主催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及び国立研究開発法人情報通信研究機構が共同で運営する暗号技術活用委員会の 2022 年度活動を報告するものである。

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している。特に、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群の作成に注力している。

2022 年度は、CRYPTREC 暗号リストの改定が 10 年ぶりに実施された。この改定にあたって、暗号技術活用委員会では、IPA が実施した「暗号アルゴリズムの利用実績に関する調査」結果の妥当性を確認したうえで、2021 年度に承認された「利用実績に基づく選定基準（選定ルール）」に基づき、現在の推奨候補暗号リストに掲載されているアルゴリズムから電子政府推奨暗号リストへの推薦候補案について検討・選定し、暗号技術検討会に推薦した。

また、安全な暗号利用のためには暗号鍵管理が重要であることを踏まえ、2021 年度から設置した暗号鍵管理ガイダンスワーキンググループにて「暗号鍵管理システム設計指針（基本編）」をより活用しやすくするためのサポート文書の作成を行っており、この度、「暗号鍵管理ガイダンス」として取りまとめた。本ガイダンスは、「暗号鍵管理システム設計指針（基本編）」で記載が求められる項目を検討する際の有用な副読本として、暗号鍵管理が必要なシステムの設計者向けに、暗号鍵管理の設計で明記する事項や考慮点などを解説している。

改定された CRYPTREC 暗号リストの活用に加え、今年度の成果をもとに適切な暗号鍵管理を促していくことは、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と期待している。

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。

2023 年 3 月

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、2022 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。

2021 年度以前の CRYPTREC Report は、CRYPTREC 事務局（デジタル庁、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」という。）は、図 1 に示すように、デジタル庁、総務省及び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（以下「IPA」という。）と国立研究開発法人情報通信研究機構（以下「NICT」という。）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」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。

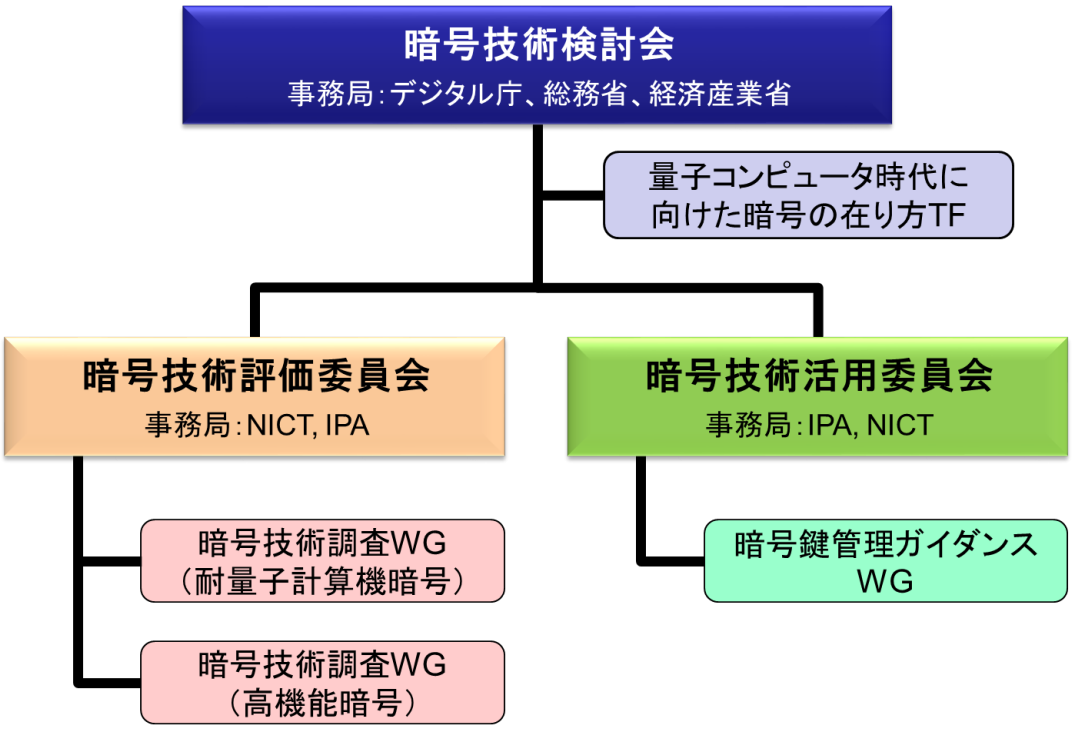

図 1 2022 年度の CRYPTREC の体制

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	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
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 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

（所属：2023 年 3 月末時点）

オブザーバー

高木 浩光	内閣官房内閣サイバーセキュリティセンター
東 隆夫	内閣官房内閣サイバーセキュリティセンター
宮崎 俊一	内閣官房内閣サイバーセキュリティセンター
高橋 元	内閣官房内閣サイバーセキュリティセンター
原田 貴志	個人情報保護委員会 事務局
千葉 亮輔	デジタル庁 デジタル社会共通機能グループ
角田 梨翔	デジタル庁 デジタル社会共通機能グループ[2022 年 12 月まで]
桜田 啓介	デジタル庁 デジタル社会共通機能グループ[2022 年 7 月から]
弓 智宏	デジタル庁 デジタル社会共通機能グループ[2022 年 7 月から]
稲見 唯睦	デジタル庁 デジタル社会共通機能グループ[2022 年 7 月から]
武井 亮	デジタル庁 デジタル社会共通機能グループ[2022 年 12 月から]
和田 憲拓	総務省 サイバーセキュリティ統括官室[2022 年 7 月まで]
河合 直樹	総務省 サイバーセキュリティ統括官室[2022 年 8 月から]

服部 裕史　　総務省 サイバーセキュリティ統括官室
増田 幸司　　総務省 サイバーセキュリティ統括官室[2022 年 7 月まで]
榎 聡美　　総務省 サイバーセキュリティ統括官室
村山 裕紀　　経済産業省 商務情報政策局[2022 年 7 月まで]
澤田 知子　　経済産業省 商務情報政策局[2022 年 7 月から]
塚本 大介　　経済産業省 商務情報政策局
和平 悠希　　経済産業省 商務情報政策局
石巻 克基　　経済産業省 商務情報政策局[2022 年 11 月まで]
木下 誠　　外務省 大臣官房 情報通信課
人見 悠太郎　外務省 大臣官房 情報通信課
小林 圭寿　　防衛省 整備計画局情報通信課
椛木 隆慎　　防衛省 整備計画局情報通信課
松川 陽介　　防衛省 整備計画局情報通信課[2022 年 12 月まで]
鈴木 直人　　防衛省 整備計画局情報通信課[2023 年 2 月から]
北尻 弦樹　　防衛省 整備計画局情報通信課[2023 年 2 月から]
井上 智樹　　警察大学校
黒澤 敦　　警察大学校[2023 年 2 月から]

事務局

独立行政法人情報処理推進機構（瓜生和久[2022年5月まで]、高柳大輔[2022年6月から]、神田雅透、石川誠、松﨑博子、白岩裕子）
国立研究開発法人情報通信研究機構（盛合志帆、野島良、吉田真紀、大久保美也子、篠原直行、黒川貴司、金森祥子、青野良範、小川一人、伊藤竜馬）

第1章　2022 年度活動内容

1.1. 活動内容

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っている。

2022 年度の活動概要は以下の通りである。

（1）利用実績に関する評価

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、運用監視暗号リストの 3 つのリストで構成されている。

2022 年度に CRYPTREC 暗号リストの改定が予定されており、その際、推奨候補暗号リストから電子政府推奨暗号リストへの昇格にあたって利用実績に基づいた選定が行われることが決まっている [2]。そこで、IPA が実施する「暗号アルゴリズムの利用実績に関する調査」による調査結果に基づき、2021 年度に承認された利用実績による選定基準の下で利用実績に関する評価を行った。また、その評価結果に基づき、電子政府推奨暗号リストへの推薦候補案を決定し、暗号技術検討会に報告した。

（2）暗号鍵管理ガイダンスの作成

情報を安全に取り扱うためには、通信情報や保管情報の暗号化に使う暗号アルゴリズムのみに注意を払うだけでは不十分であり、その暗号アルゴリズムに用いられる暗号鍵の管理が適切に行われる必要がある。

そこで、暗号鍵管理ガイドラインの拡充を目的として暗号鍵管理ガイダンス WG を設置し、2021 年度に取りまとめた作業の進め方に基づき、「暗号鍵管理システム設計指針（基本編）[3]」の解説書となる「暗号鍵管理ガイダンス」を作成した。

（3）暗号利活用のために作成すべきガイダンス候補の検討

2023 年度以降に暗号利活用のために作成すべきガイダンス候補を検討し、今後の執筆に向けた準備を行った。

---

[2] CRYPTREC、暗号技術検討会 2020 年度報告書、https://www.cryptrec.go.jp/report/cryptrec-rp-1000-2020.pdf

[3] CRYPTREC、暗号鍵管理システム設計指針（基本編）、https://www.cryptrec.go.jp/report/cryptrec-gl-3002-1.0.pdf

1.2. 開催状況

2022 年度に開催された暗号技術活用委員会での審議概要は表 1-1 のとおりである。

表 1-1　2022 年度暗号技術活用委員会　開催概要

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

第2章　成果概要

2.1. 利用実績に関する評価

2.2.1. 暗号アルゴリズム利用実績調査報告の検証

IPA が実施した「暗号アルゴリズムの利用実績に関する調査」では、電子政府推奨暗号リストに掲載する暗号アルゴリズムを選定するために、製品やシステム等で利用している暗号アルゴリズム名称を特定し、当該暗号アルゴリズムがどの程度利用されているか、またどの程度の標準化や規格化に採用されているかといった「暗号アルゴリズムの製品化、利用実績」を収集することを意図している。また、政府機関に対する調査、国際標準規格・民間規格に対する調査、オープンソースソフトウェアでの利用実績調査も併せて実施した。

本調査における調査対象及び調査実績は表 2-1 の通りである。集計対象数が本調査における母集団として最終的に扱うことになった有効回答数である。各暗号アルゴリズムの具体的な利用実績など、詳細については、IPA の暗号アルゴリズムの利用実績に関する調査報告書（2022 年度）を参照されたい[4]。

暗号技術活用委員会としては、IPA の調査が適正に実施されており、利用実績に関する評価として用いることができるかどうかの観点から、調査結果の検証を行った。その結果、利用実績に関する評価結果として用いることに問題はないと判断した。

なお、国際標準規格・民間規格に対する利用実績の評価にあたっては、今回の IPA の調査結果（25 件）のほかに、2012 年度、2019 年度及び 2021 年度に実施した利用実績調査結果のうち現在も有効な規格（146 件）を加えた合計 171 件を対象に評価を実施したことに注意されたい。

表 2-1　暗号アルゴリズムの利用実績に関する調査結果概要

調査対象	調査実績
(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	● 応募暗号アルゴリズムの応募会社全 8 社（16 アルゴリズム）から回答受領 ➢ アルゴリズム実績提供：11 アルゴリズム → 調査(C)(D)(E)の情報として活用 ➢ 製品実績提供：4 アルゴリズム → 調査(B)の情報として活用

4　IPA、暗号アルゴリズムの利用実績に関する調査報告書（2022 年度）、https://www.ipa.go.jp/security/reports/crypto/crypto-algorithm-2022.html

(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	● アンケート配布数： ➢ 14 業界団体 2,535 社 ➢ 個別コンタクト 102 社 ➢ 調査パネル 23,747 名 ⇓ ● <u>アンケート回収数：合計 211 社 301 製品</u> ➢ 業界団体：2,535 社 → 65 社 114 製品 ➢ 個別：108 社 → 28 社 37 製品 ➢ (A)調査：4 社 4 製品 ➢ 調査パネル：23,747 名 → 146 製品 ⇓ ● アンケート有効回答数： ➢ 合計 82 社 128 製品（利用アルゴリズム不明 19 製品を含む） ⇓ ● <u>集計対象：合計 101 社 209 製品</u> ➢ アンケート有効回答：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	● <u>規格調査数：全 30 件</u> ⇓ ● <u>集計対象：合計 17 件</u> ➢ 暗号アルゴリズム記載ありは 17 件 ● <u>集計対象： 政府機関で利用されている 98 システム</u>
(D) 国際標準規格・民間規格等に対する調査	● <u>規格調査数：IPA が指定した 25 件</u> ⇓ ● <u>集計対象：合計 25 件</u>
(E) オープンソースソフトウェアでの利用実績調査	● <u>OSS 調査数：IPA が指定した 30 件</u> ⇓ ● <u>集計対象：合計 30 件</u>

2.2.2. 電子政府推奨暗号リスト掲載への推薦候補案の選定

IPA が実施した暗号アルゴリズム利用実績調査の結果、及び 2021 年度に承認された利用実績に基づく選定基準（選定ルール）に基づき、現在の推奨候補暗号リストに掲載のア

ルゴリズムのうち、電子政府推奨暗号リスト掲載への推薦候補案について検討・選定し、暗号技術検討会に推薦した。

【検討方針】

IPA が実施した暗号アルゴリズム利用実績調査では、現在の推奨候補暗号リストに掲載のアルゴリズムのうち、EdDSA のみアンケートによる利用実績調査の対象外であった。

このため、「EdDSA」以外の「推奨候補暗号リスト」に掲載の暗号アルゴリズムについては「利用実績調査（考慮項目①～⑥）」結果に基づいて判定し、「EdDSA」については「利用実態確認（考慮項目②～⑤）」結果に基づいて判定することとした。

表 2-2　選定ルール

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を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**	**「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**

	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	**「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を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掲載への推薦候補案】

- **エンティティ認証、ハッシュ関数、署名を除いた技術分類について：**

技術分類		推薦候補	推薦しない候補	理由
公開鍵暗号	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
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

- **エンティティ認証について：**

技術分類	推薦候補	推薦しない候補	理由
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

- **ハッシュ関数について：**

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

- **EdDSA について：**

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

2.2.3. SC2000 の CRYPTREC 暗号リストからの取下げ申請への対応

富士通株式会社から取下げ申請があった SC2000 について、審議の結果、暗号技術検討

会で CRYPTREC 暗号リストからの取下げルールを整備することを条件に、申請を了承することとした。

2.2. 暗号鍵管理ガイダンスの作成

情報を安全に取り扱うためには、通信情報や保管情報の暗号化に使う暗号アルゴリズムのみに注意を払うだけでは不十分であり、その暗号アルゴリズムに用いられる暗号鍵の管理が適切に行われる必要がある。そこで、2020 年度に鍵管理のフレームワークとなる「暗号鍵管理システム設計指針（基本編）[5]」を公開したことに引き続き、2021 年度から暗号鍵管理ガイドラインの拡充を目的として暗号鍵管理ガイダンスを作成するため、暗号鍵管理ガイダンス WG を設置した。

本ガイダンスは「暗号鍵管理システム設計指針（基本編）」で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しており、暗号鍵管理が必要なシステムの設計者向けに、暗号鍵管理の設計で明記する事項や考慮点などを解説している。

本ガイダンスの位置づけと想定読者は以下の通りである。

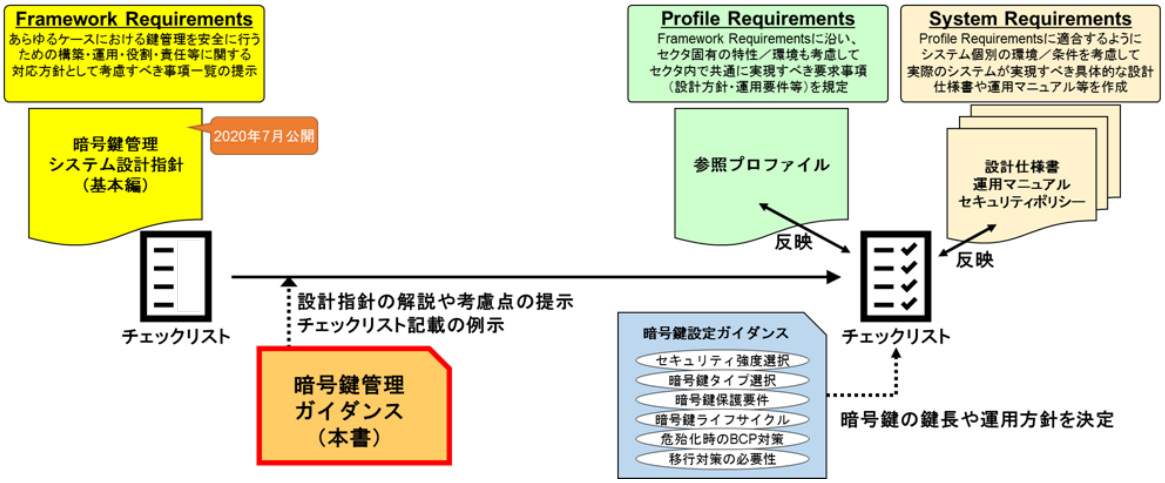

図 2-1　「暗号鍵管理ガイダンス」作成の位置づけ

位置づけ

- 暗号鍵管理機能を持つシステム設計者のガイダンスを作成する。このガイダンスは 2020 年に発行した「暗号鍵管理システム設計指針（基本編）」を詳しく解説することを中心に作成する

[5] CRYPTREC、暗号鍵管理システム設計指針（基本編）、https://www.cryptrec.go.jp/report/cryptrec-gl-3002-1.0.pdf

- 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
- 暗号鍵管理における特に注意すべきリスクを説明する

<u>想定読者</u>

- 暗号鍵管理機能を持つシステム設計者

注意：

2021 年度 WG にて決定した執筆方針では、「暗号鍵管理プロファイルを作成するためのガイダンス」として作成することを目的とし、想定読者も「暗号鍵管理機能を持つシステム設計者」「暗号鍵管理の参照プロファイル作成担当者」及び「暗号鍵管理プロファイルの利用者／暗号鍵管理機能を持つシステム調達者」と幅広く対象としていた。
しかしながら、これらの想定読者の皆に対して理解してもらおうと多くの恩恵や効用を記載した結果、各節ごとの記載内容に大きなブレが生じ、逆に本来伝えるべき人に伝えるべき内容が伝わらない状態になったと判断した。このため、想定読者の対象を見直して、「暗号鍵管理システム設計指針（基本編）」と同様、「暗号鍵管理機能を持つシステム設計者」に絞り込んだうえで、システム設計者に伝えるべき内容に整理することにしたことに留意されたい。

【本ガイダンス概要】

具体的には、「暗号鍵管理システム設計指針（基本編）」で記載されている検討項目のうち、暗号鍵管理システム（CKMS）の利用環境に関わらず検討する必要がある【B】、【C】、【D】に該当する項目に関して、各検討項目についての解説・考慮点を具体的に説明している。また、これらの理解を助けるため、簡単なシステム（トイモデル）を具体的に取り上げ、そのシステムで設定された構成や運用条件などを踏まえた場合の各々の検討項目における記載例を提供している。

なお、本ガイダンスで対象とする範囲は、「狭義」の意味での暗号鍵管理に相当するものである。暗号鍵管理システム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を取り扱っていることに留意されたい（ちなみに、【E】や【F】までを含む場合、「広義」の意味での暗号鍵管理と称す）。

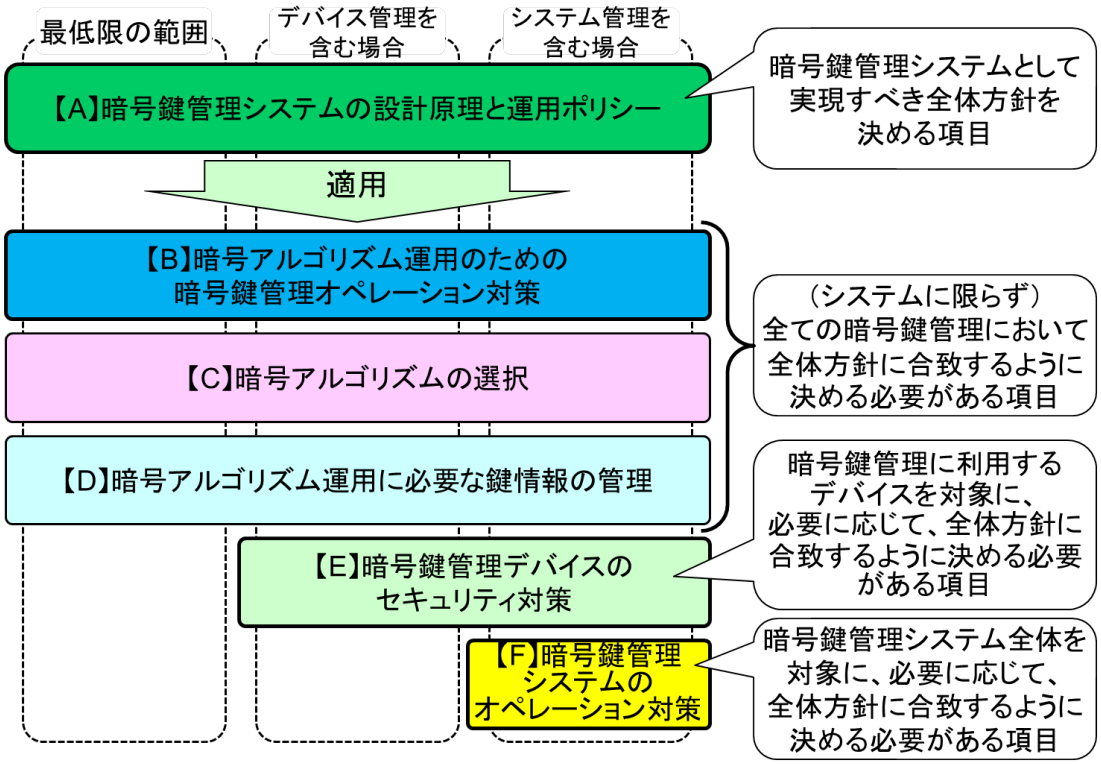

図 2-2　暗号鍵管理における目的別分類関係（「暗号鍵管理システム設計指針」より）

今回の暗号鍵ガイダンスの章構成は以下のとおりである。

1. はじめに
2. 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
   - 2.1. CKMS 設計
   - 2.2. 暗号鍵のライフサイクル
   - 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
   - 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
3. 暗号アルゴリズムの選択
   - 3.1. 暗号アルゴリズムのセキュリティ
4. 暗号アルゴリズム運用に必要な鍵情報の管理
   - 4.1. 鍵情報の種類
   - 4.2. 鍵情報の選択
   - 4.3. 鍵情報の保護方針

1 章では、イントロダクションとして、暗号鍵管理の重要性、及び本ガイダンスの位置づけについて説明している。

2 章は、暗号鍵管理システム設計指針（基本編）での「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」における検討項目についての解説・考慮点を記載している。具体的には、CKMS においてどのように暗号鍵が管理されるかを対象にしており、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検討項目を取り扱っている。例えば、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を整理し、それ以降に決めなければならない各項目ではここで決めた内容に矛盾するような内容で定めてはならないことの重要性を指摘している。このほか、使用している暗号鍵の状態や遷移条件、実施する処理に関する管理機能や、鍵情報の保管、鍵確立、鍵情報の喪失、破損、危殆化などが発生したときの BCP 対策に求められる項目での解説・考慮点を説明している。また、簡単なモデル（トイモデル）として S/MIME をモデルに取り上げ、記載例を示した。

3 章は、暗号鍵管理システム設計指針（基本編）での「暗号アルゴリズムの選択」における検討項目についての解説・考慮点を記載している。具体的には、暗号アルゴリズムや鍵長を選択に関する重要なポイントの解説、特に CRYPTREC 暗号リスト（電子政府推奨暗号リスト）、暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準や暗号鍵設定ガイダンスを参考に選択することを推奨している。また、Web ブラウザをクライアントとするクライアントーサーバシステムをモデルにした記載例を示した。

4 章は、暗号鍵管理システム設計指針（基本編）での「暗号アルゴリズム運用に必要な鍵情報の管理」における検討項目についての解説・考慮点を記載している。ここでは、3 章で決定した暗号アルゴリズムを運用するときに必要な鍵情報の管理の説明、具体的には管理すべき全ての鍵を明確にし、その鍵とメタデータの保護方法についての解説・考慮点を記載している。また、関係者がアクセス可能な Web サーバシステムをモデルにして記載例を示した。

2.3. 運用ガイドライン／ガイダンス作成に向けた検討結果について

2023 年度以降に作成すべきガイドライン／ガイダンスの候補について、以下の視点を踏まえ、検討を行った。今回の議論を踏まえ、どのガイドライン／ガイダンスを作成するかを 2023 年度活動計画に反映することを決定した。

- **ガイドライン／ガイダンスの整理学**

A. 以前から求められていた利用方法のガイドライン・ガイダンス：1)、2)、3)、8)、9)、19)

B. 設定・設計に関するガイドライン・ガイダンス：4)、12)、20)
C. 啓発ガイダンス：5)、6)、7)、15)
D. 新しい利用方法のガイドライン・ガイダンス：10)、11)
E. 少し早い（2023 年度着手ではなくてもいい）かもしれないガイドライン・ガイダンス：13)、14)
F. 他団体との連携で作るといいかもしれないガイドライン・ガイダンス：16)、17)、18)
G. その他：21)

- **検討にあたっての視点**
  - どのようなガイドライン／ガイダンスが求められているか
  - CRYPTREC がメインで作るのがよいか、それとも他の組織（IPA、業界団体など）がメインで／共同で作るのがよいか
  - 暗号技術の切り口メインで有用なガイドライン／ガイダンスになるか（暗号以外の部分がメインになったりしないか）

表 2-3　候補に挙がったガイドライン／ガイダンスのテーマ

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

第3章　今後に向けて

今年度、暗号鍵管理ガイダンスを完成させたところであるが、「暗号鍵管理システム設計指針（基本編）」に記載がありながら今回解説・考慮点の記載を見送った部分（暗号鍵管理システムの設計原理と運用ポリシー、暗号鍵管理デバイスのセキュリティ対策、暗号鍵管理システムのオペレーション対策）がある。このため、引き続き、暗号鍵管理ガイダンス WG にて解説・考慮点を検討し、その拡充を行っていく予定である。

また、TLS 暗号設定ガイドラインのアップデートを実施するとともに、2022 年度活用委員会での議論を踏まえ、暗号利活用に向けた新たな有用なガイドライン／ガイダンス作成に着手する予定である。

CRYPTREC Report 2022
(暗号技術活用委員会報告　CRYPTREC RP-3000-2022)

発行日　2023年6月30日 第1版（印刷版）
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
(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)
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