CRYPTREC Report 2021

令和 4 年 6 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 2021 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。

2021 年度の成果の第一は、暗号アルゴリズムの鍵長に関して 2 つの文書を作成したことである。このうち「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」は、CRYPTREC 暗号リストに掲載された暗号アルゴリズムを安全に利用するための鍵長を初めて公式に規定したものであり、CRYPTREC 暗号リストの構成要素の一つと位置付けられる。

また、2022 年度予定の CRYPTREC 暗号リストの改定に向けた準備として検討した結果を「利用実績に関する選定基準（案）」としてまとめている。これは、暗号利用実績調査の結果に照らして新しい電子政府推奨暗号リストを選定する際に、今後活用される予定である。

さらに、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、「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、新たに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進めている。

今年度の成果をもとに、CRYPTREC 暗号リストによる暗号アルゴリズムの選択だけでなく、鍵長の選択や暗号鍵の管理にも留意して正しい暗号利用を促していくことで、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。

2022 年 6 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、2021 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。

2020 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。

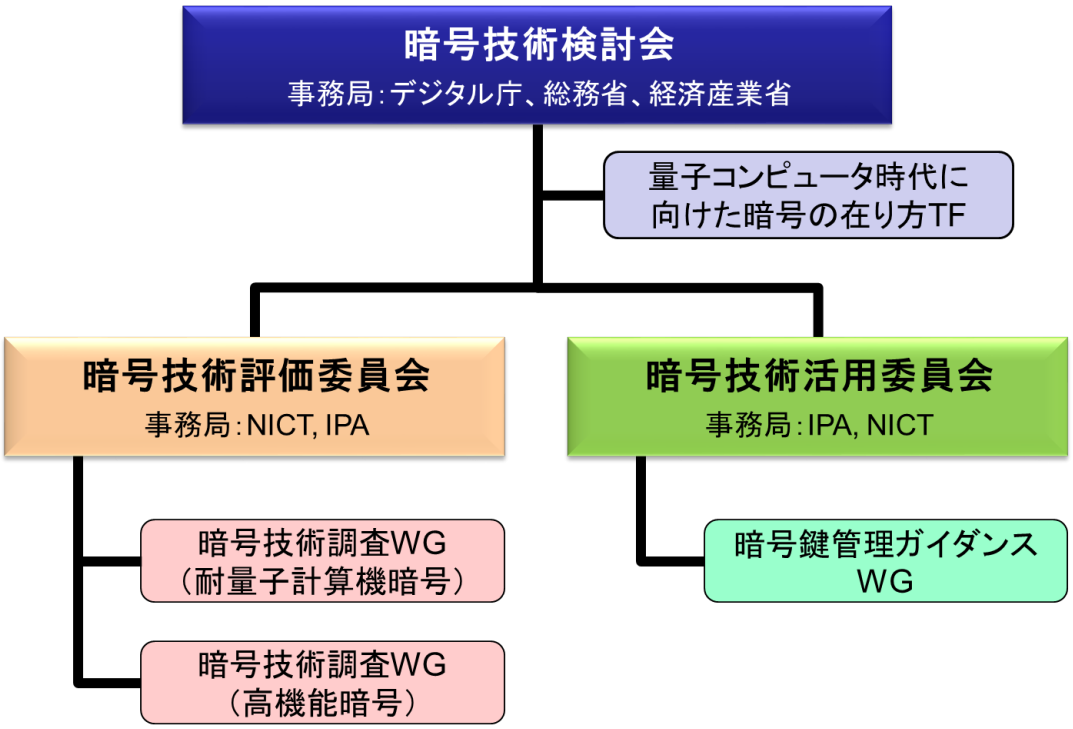

図 1 2021 年度の CRYPTREC の体制

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[2]
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：2022 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
武藤 健一郎	内閣官房内閣サイバーセキュリティセンター[2021 年 10 月まで]
高橋 元	内閣官房内閣サイバーセキュリティセンター[2021 年 11 月から]
柏原 陽	個人情報保護委員会 事務局[2021 年 6 月まで]
原田 貴志	個人情報保護委員会 事務局[2021 年 7 月から]
千葉 亮輔	デジタル庁 デジタル社会共通機能グループ[2022 年 1 月から]
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 1 月から]
梅城 崇師	総務省 サイバーセキュリティ統括官室[2021 年 6 月まで]

[2] 2022 年 2 月まで在籍

和田 憲拓　　総務省 サイバーセキュリティ統括官室[2021 年 7 月から]
服部 裕史　　総務省 サイバーセキュリティ統括官室
山下 恵一　　総務省 サイバーセキュリティ統括官室[2021 年 6 月まで]
増田 幸司　　総務省 サイバーセキュリティ統括官室[2021 年 7 月から]
村山 裕紀　　経済産業省 商務情報政策局
上田 翔太　　経済産業省 商務情報政策局[2021 年 6 月まで]
和平 悠希　　経済産業省 商務情報政策局[2021 年 7 月から]
伊藤 江美子　外務省 大臣官房 情報通信課[2021 年 11 月まで]
木下 誠　　外務省 大臣官房 情報通信課
村上 匠　　外務省 大臣官房 情報通信課[2022 年 1 月まで]
人見 悠太郎　外務省 大臣官房 情報通信課[2022 年 2 月から]
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
伊藤 愼崇　　警察大学校
岡原 亮　　警察大学校[2021 年 11 月から]

事務局

独立行政法人情報処理推進機構（瓜生和久、神田雅透、石川誠、伊藤忠彦、大久保智史、木島慶子）

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、高安敦（2021年9月まで）、小川一人、伊藤竜馬）

第1章　2021 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。

2021 年度の活動概要は以下の通りである。

（1） 利用実績に関する選定基準（案）の検討

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 [3]。

そこで、昇格のための具体的な利用実績に関する選定基準案を検討・策定した。なお、策定した選定基準案は暗号技術検討会に報告され、改めて審議される。また、利用実績調査は 2022 年度上期に IPA にて実施する計画である。

（2） 「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」及び「暗号鍵設定ガイダンス」の作成

安全な暗号利用に係る運用ガイドラインとして、2020 年度の検討結果を踏まえて取りまとめた作成方針に基づき、2 つの鍵長に関連するドキュメントを作成した。

一つは、「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」である。

これは、CRYPTREC 暗号リストに掲載されている暗号技術を利用する際に、適切なセキュリティ強度を実現するためのアルゴリズム及び鍵長の選択方法を規定したガイドラインであり、CRYPTREC 暗号リストの一要素を成すものである。したがって、利用する鍵長について、本書の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意されたい。例えば、政府機関等のサイバーセキュリティ対策のための統一基準 [4]において適用対象となる情報システム（暗号化機能・電子署名機能の導入を行うものに限る。）の調達・開発にあたって、調達要件や開発要件として採用すべき暗号アルゴリズム及び鍵長を決定する際の活用を想定している。

もう一つは、「暗号鍵設定ガイダンス」である。

これは、利用用途を特定せず、鍵長の選択方法や暗号鍵の設定に関する一般的なガイ

---

3 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

4 内閣サイバーセキュリティセンター（NISC）、政府機関等のサイバーセキュリティ対策のための統一基準（令和 3 年度版）、https://www.nisc.go.jp/pdf/policy/general/kijyunr3.pdf

ダンスを提供する。調達要件や開発要件などを具体的に定めるものではなく、鍵長の選択方法や暗号鍵の設定などについて考え方や留意点を示すものである。

（3） 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、2020 年度に公開した「暗号鍵管理システム設計指針（基本編）」の解説書となる「暗号鍵管理ガイダンス」の検討を開始した。

2020 年度に取りまとめた作業の進め方に基づき、暗号鍵管理ガイダンス WG を設置して検討を行っている。なお、本ガイダンスの完成は 2022 年度の予定である。

1.2. 開催状況

2021 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　2021 年度暗号技術活用委員会　開催概要

回	開催日	議案
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 ● 暗号鍵設定ガイダンス（仮称）について ● 利用実績による選定基準（案）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

第2章　成果概要

2.1. 利用実績による選定基準（案）について

利用実績に基づく選定基準（選定ルール）は、2012 年度に現在の CRYPTREC 暗号リストの形に改定された際に初めて導入されたものである。当時定めた選定基準は表 2-1 のとおりである。

【2012 年当時の選定基準の概要抜粋】

表 2-1　2012 年当時の選定基準

<table>
<tr><td></td><td colspan="2">評価 A</td><td colspan="2">評価 B</td></tr>
<tr><td>市販製品での採用実績（販売会社数・種類・種別）</td><td>提案会社・グループ会社以外での採用、且つ採用割合 50%以上</td><td rowspan="4">うち、3 項目以上</td><td>提案会社・グループ会社以外での採用、且つ採用割合 50%以上</td><td rowspan="8">うち、3 項目以上</td></tr>
<tr><td>オープンソースプロジェクトでの採用実績</td><td>採用割合 50%以上</td><td>採用割合 50%以上</td></tr>
<tr><td>政府系システム規格での採用実績</td><td>採用割合 50%以上</td><td>採用割合 50%以上</td></tr>
<tr><td>国際的な民間メジャー規格での採用実績</td><td>採用割合 50%以上</td><td>採用割合 50%以上</td></tr>
<tr><td>利用促進を図る際の障壁の除去</td><td colspan="2"></td><td>特許無償ライセンスの付与</td></tr>
<tr><td>標準化・規格化の促進を図るハードルの低さ</td><td colspan="2"></td><td>技術的、標準化、採用実績のいずれかでアピールポイントがある</td></tr>
<tr><td>実装コスト低減を図るハードルの低さ</td><td colspan="2"></td><td>採用実績、オープンソースプロジェクトのいずれかでアピールポイント（採用割合 10%以上）がある</td></tr>
<tr><td>調達コスト低減を図るハードルの低さ</td><td colspan="2"></td><td>市販製品又は政府系システムでの採用実績(採用割合 10%以上）がある</td></tr>
</table>

【2012 年当時の選定基準の検討状況】

- 利用実績に基づく選定に関する知見があったわけではないので、暗号運用委員会（当時、現在の活用委員会の前身）にてゼロベースで検討した。
- 2009 年度に経済産業省が実施した「暗号モジュールの市場動向等に関する調査研究」における「暗号アルゴリズムの市場性」の調査結果をベースに、利用実績を評価するための閾値を検討した。
- 電子政府における調達競争性の確保を考慮し、電子政府推奨暗号リストに掲載するのは「利用実績が十分であり、今後も安定的に利用可能である（評価 A)」か、「利用実績は十分ではないが、今後の利用促進の可能性が高い（評価 B)」と判断できるような暗号アルゴリズムを選定することを目指した。特に、提案会社とは資本関係がない複数の企業から調達可能であることを重視した。

2021 年度の活用委員会では、以下の観点を踏まえ、2012 年当時の選定基準をどのように見直すべきかの検討を行った。

- 電子政府推奨暗号リストに掲載されている暗号アルゴリズムは、すでに利用中のシステムが存在するという前提に立ち、利用実績調査の結果如何を問わず、電子政府推奨暗号リストから外すことはしない。つまり、求められる選定基準は、推奨候補暗号リストから電子政府推奨暗号リストに**昇格するための選定基準**である。
- CRYPTREC 暗号リストにあるカテゴリの暗号アルゴリズムについて公募する予定は当面なく、2022 年度改定にあたっても**公募は実施しない**。そのため、推奨候補暗号リストに新たに追加される可能性があるのは、事実上、**事務局推薦によるものだけ**と考えてよく、追加される時点で「ある程度の標準化や製品化が進んでおり、近いうちに普及が見込める（普及する可能性が高い)」と判断されていることを前提においてもよい。
- 掲載から 20 年を超えた後に実施する最初の利用実績調査で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できなかったものは推奨候補暗号リストから削除されることが明確化されたことを考慮する必要があるかもしれない。
- 今では、ISO や ITU-T、IETF、IEEE などの標準規格において、CRYPTREC 暗号リストにあるカテゴリでの暗号技術そのものの標準化作業が進んでいるものはそれほど多くない。
- クローズド（＝セキュリティ上の理由等により、関係者以外にどの暗号アルゴリズムが利用されているかを公開しない）な利用実績をどのように扱うのがよいか。

これらの検討の結果、以下の理由により、選定基準（案）に電子政府推奨暗号リストへの昇格のための明確な選定基準・閾値は設けないとの結論に至った。また、今回作成した選定

基準（案）は昇格の目安としてのものであり、実際の昇格判断は個々の状況を鑑みて個別に行うものとした。

なお、活用委員会にて決定した選定基準（案）は、暗号技術検討会に報告された。

- 暗号アルゴリズムの普及の仕方が、利用の前提・環境整備としての「標準化」を踏まえて**徐々に利用が広がっていく**以前の流れから、「有力ベンダが大規模採用」した影響を受けて**急速にその周辺に利用範囲が広がり**後から標準化につながっていく流れに変わってきていることに留意すべきである。
  - 5 年ごとの「利用実績」調査では急激な利用実績の変動に対応できず、判断の遅れにつながる
  - 有力ベンダの採用状況などから近い将来主流になっていく可能性が高いと判断できるような暗号アルゴリズムであれば、早いうちから採用できる環境を整えるべき
  - 結果として、今後の電子政府推奨暗号リストへの昇格は、**「1）5 年ごとの利用実績調査」に基づくケースよりも、「2）その他、普及していることが明らか又は急速な普及が大いに見込まれる」場合に随時昇格させるケースが主軸**になっていく可能性が高い
- 「2）その他、普及していることが明らか又は急速な普及が大いに見込まれる」場合に随時昇格させるケースを想定するならば、その際の普及状況として様々な場面が想定されるため、厳格な基準・閾値と定めたとしても適切な運用ができない可能性がある。
  - 昇格が適切と認められる状況であったとしても、定めた基準・閾値を満たさないという理由で昇格できないのでは本末転倒
  - 有力ベンダの今後の採用状況などの未来予測も加味して利用実績を判断すべき
- クローズドな利用での実績については、従来と同様、原則カウントしない。
  - ただし、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での利用が確認された場合に限り、例外的に扱う
  - 利用実績がないことによる推奨候補暗号リストからの削除にあたっては、CRYPTREC 暗号リストの主たる利用者である各府省庁に事前照会を行い、コメントを踏まえたうえで最終判断を行うものとする

【今回の選定基準（案）】

本選定基準は、暗号技術評価委員会で安全性及び実装性の評価を実施し、その評価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した暗号技術に対して、電子政府推奨暗号リストへの昇格を決めるための基準である。昇格検討対象の暗号技術は、以下の考慮項目での目安に基づき、暗号技術活用委員会にて検討、選定し、暗号技術検討会に推薦する。

推薦された暗号技術について、暗号技術検討会では、その根拠となった利用実態を再度確

認・審議を行い、電子政府推奨暗号リストへの昇格に問題がないと判断した場合に電子政府推奨暗号リストに選定する。

表 2-2　利用実績調査による選定基準（案）

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。**

＜目安の理由＞

- ①は「利用実績調査」の結果に基づく基準として整備する。
  電子政府推奨暗号リストと推奨候補暗号リストの採用実績に著しい不整合が起きないようにするための指標とする。
- ②～⑤は「その他、普及していることが明らか又は急速な普及が大いに見込まれる」ケースに対応する基準として整備する。①の場合と異なり、必ずしも利用実績調査を実施するわけではなく、利用実態確認だけで採用実績を確認する場合もあるので、採用割合での判断は行わない。象徴的な利用形態での採用実績がどれだけ進んだかを主な指標とする。
  - ②については、CRYPTREC の設置目的からして明らかに管理する必要があることへの対応。また、クローズドな利用での実績であったとしても、CRYPTREC 暗号リストの主たる利用者である各府省庁に事前照会を踏まえた判断根拠になり得る
  - ③～⑤については、「複数」「利用者が多い（主要）」というキーワードの両方を満たすことを例示しておくことで、「明らかな採用促進、又は急速な普及の可能性」の判断目安とすることを意図している。なお、実際に判断にあたっては、利用実態確認で収集した関連情報を基にした活用委員会での審議結果に基づく
- 標準化実績については、標準化が進んだだけでは採用実績に直ちに結びつくわけではなく、また標準化されるまでに時間がかかる。このため、利用実績に急激な変化が起こりにくいことを考慮し、「利用実績調査」の結果に基づく基準のみを整備する。
  - さらに、標準化が進んで急速に利用が進展した場合であっても、採用実績の③や④などで対処することが可能

2.2. 「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」の作成

2020 年度活用委員会での議論を踏まえ、2021 年度活用委員会では表 2-3 のとおりに作成方針を定め、「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」を作成した。作成にあたっては、以下の論点について主に検討を行い、検討結果を設定基準に反映させた。

詳細は、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[5]を参照されたい。

表 2-3　「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」の作成方針

文書体系	CRYPTREC 暗号リストの一要素を成すものとし、LS を附番
利用目的	政府機関等のサイバーセキュリティ対策のための統一基準において適用対象となる情報システム（暗号化機能・電子署名機能の導入を行うものに限る。）の調達又は開発にあたって、調達要件又は開発要件として採用すべき暗号アルゴリズム及び鍵長を決定する
想定読者	上記システムの調達又は開発に係る情報システムセキュリティ責任者・システム担当者・調達担当者、など。（その他の利用者は、ボランタリベースと位置付ける）
備考	「CRYPTREC 暗号リスト」と一体的に直接参照するものとし、「政府機関の情報セキュリティ対策のための統一基準」での利用を第一義とする
主な論点	● 「鍵長設定の要件」と「移行」に絞って記載してよいか ● 電子政府システムの運用期間として取り扱う範囲をどこまで想定するか ● ビットセキュリティの基準をどこまで区切るか ● 電子政府システムの運用寿命とセキュリティ強度要件の関係をどのように整理するか ● セキュリティ強度要件をどのように設定するか ● セキュリティ強度要件に付与するラベリング名を何にするか ● 情報の機微度、あるいはインパクトレベルによって要件に差をつけるか

<u>設定基準の位置づけ</u>

CRYPTREC 暗号リストに掲載されている暗号技術を利用する際に、適切なセキュリティ強度を実現するためのアルゴリズム及び鍵長の選択方法を規定したものであり、CRYPTREC 暗号リストとの関係を図 2-1 に示す。

なお、利用する鍵長について、本書の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストをはじめ、CRYPTREC 暗号リストの暗号技術を利用しているとは見なされないことを明確化している。

[5] CRYPTREC、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、https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022.pdf

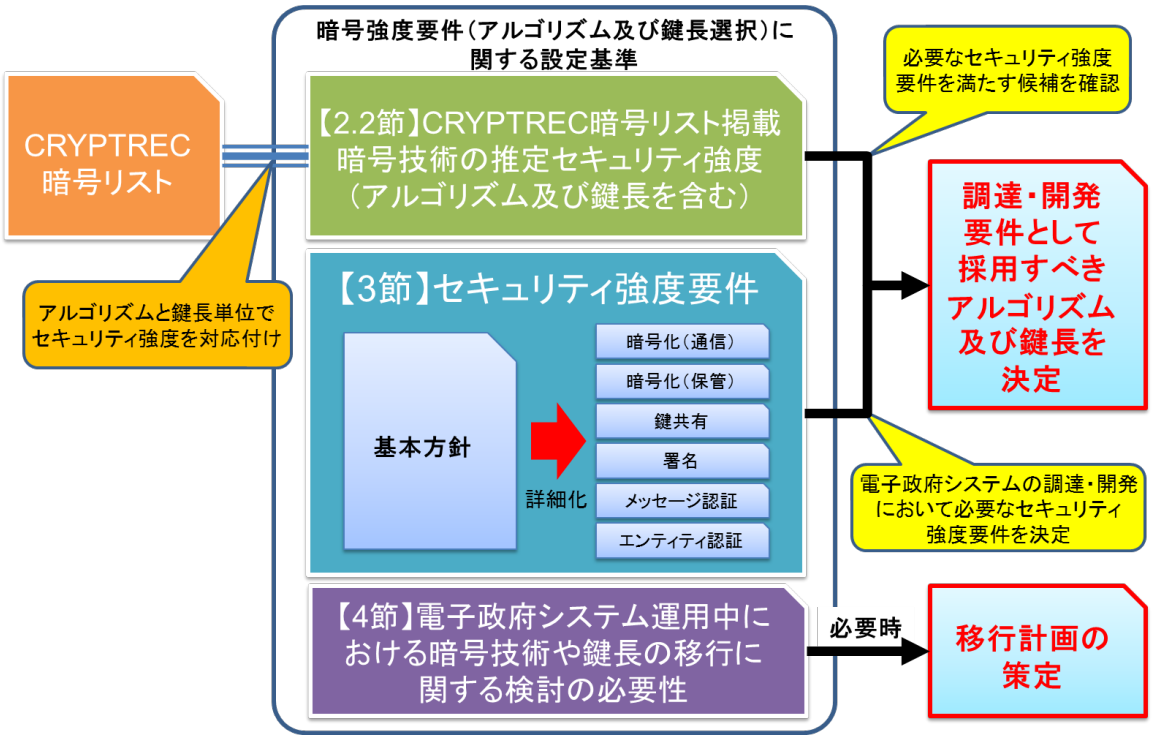

図 2-1　「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の位置づけ

<u>セキュリティ強度要件の基本設定方針概要</u>

電子政府システムを調達又は開発する際は、そのシステムの運用寿命全体と、その期間に実現するセキュリティ強度の関係を考慮してセキュリティ強度要件を設定し、その強度要件を満たすアルゴリズムと鍵長の組合せを調達・開発要件としなければならない。セキュリティ強度要件の設定にあたっては、電子政府システムの検討状況を踏まえ、以下の要件設定方法のいずれかを選択して行う（図 2-2 参照）。

必要なセキュリティ強度要件は表 2-4 をベースとして、電子政府システムの想定運用終了・廃棄年又は利用期間の終了年を基準に設定する。例えば、電子政府システムの運用終了・廃棄年が 2057 年予定であれば「2051～2060」の列を参照し、192 ビット以上のセキュリティ強度要件を設定する。なお、本要件は 2021 年末時点での暗号技術の安全性評価の現状等を踏まえたうえで、2070 年までの予測可能なセキュリティマージンを持った基準として定めたものである。

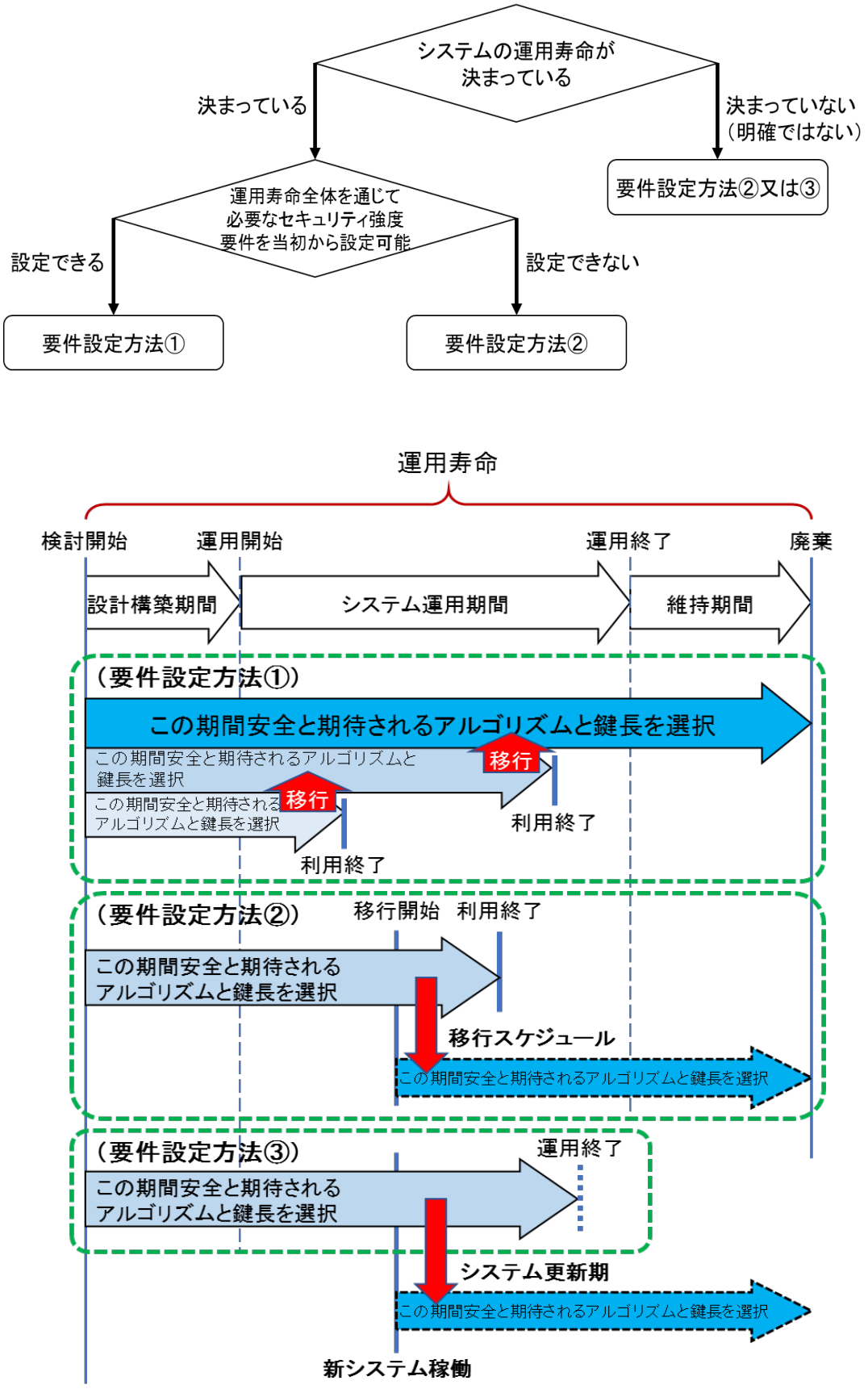

図 2-2　セキュリティ強度要件の基本設定方針の概要

【要件設定方法①】

電子政府システムの運用寿命全体を通して必要なセキュリティ強度要件を設定し、その強度要件を満たすアルゴリズムと鍵長の組合せをサポート（実装）しなければならない。

- 利用終了時期を明確化し、それまでにより安全なアルゴリズム及び鍵長に移行することを条件に、その期間中は安全と期待されるアルゴリズムと鍵長の組合せを一緒にサポート（実装）してもよい

【要件設定方法②】

何らかの制約により、運用寿命全体を通して必要なセキュリティ強度要件を当初から設定することが困難である場合、セキュリティ強度要件を切り替える移行時期を明確化したスケジュールを立案することを条件としたうえで、その移行時期終了まで安全に運用するために必要なセキュリティ強度要件を設定し、その強度要件を満たすアルゴリズムと鍵長の組合せをサポート（実装）しなければならない。

- 移行スケジュールには移行開始予定時期及び移行完了予定時期を明示すべき

【要件設定方法③】

運用寿命が決まっていない（明確ではない）場合、システム更新期を明確化したスケジュールを立案することを条件としたうえで、その更新期まで安全に運用するために必要なセキュリティ強度要件を設定し、その強度要件を満たすアルゴリズムと鍵長の組合せをサポート（実装）しなければならない。

- 新システムの稼働開始予定時期及び新旧システムの併用運用想定期間も示しておくことが望ましい

表 2-4 の設定基準において、特に留意すべき点は、量子コンピュータによる暗号解読に対する考え方である。

大規模な量子コンピュータが利用可能になった場合、Shor のアルゴリズムにより多項式時間で素因数分解問題や（楕円）離散対数問題が解けることが知られており、とりわけ CRYPTREC 暗号リストの公開鍵暗号（守秘、署名、鍵共有）に掲載されている全てのアルゴリズムにとって理論的には大きな脅威になっている [6]。しかしながら、2021 年 3 月時点の CRYPTREC 調査 [7]では、「現状の量子コンピュータでは暗号で用いるほど大きなパラメータ

---

6 共通鍵暗号、暗号利用モード、メッセージ認証コードに対しては、おおむね鍵長の半分程度のセキュリティ強度に低下するが、公開鍵暗号ほど大きな影響は受けないと評価されている。つまり、鍵長を 256 ビットにするなどの対策で対処可能である。詳細については、CRYPTREC Report 2019「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」を参照されたい。
https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2019r1.pdf

7 CRYPTREC Report 2020「Shor の量子アルゴリズムによる現代暗号への脅威に関する調査」を参照されたい。https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2020.pdf

の合成数を素因数分解することは困難であり、暗号で用いるパラメータの問題を解くためには量子ビット数やゲート計算のエラー率など量子コンピュータの性能の大幅な向上が必要であると考える。」と結論付けている。このことは、現時点で実現されている量子コンピュータと実際の暗号解読を行うのに必要とされる量子コンピュータの性能に関しては依然として大きな乖離があることを意味している。

したがって、本設定基準では量子コンピュータによる暗号技術の危殆化は将来的なリスク要因として位置づけ、推定セキュリティ強度の評価に量子コンピュータの影響は考慮していない。また、将来的なアルゴリズム及び鍵長の選択要件においてもその影響を考慮しないものとしている。

今後、暗号解読手法の進展や大規模量子コンピュータの実現等により、暗号アルゴリズム及び鍵長によっては推定セキュリティ強度が見直される可能性があるため、本設定基準及び推定セキュリティ強度は少なくとも 5 年ごとに再確認することとしている。

表 2-4　セキュリティ強度要件の基本設定基準

<table>
<tr><th colspan="2">想定運用終了・廃棄年
／利用期間</th><th>2022～2030</th><th>2031～2040</th><th>2041～2050</th><th>2051～2060</th><th>2061～2070</th></tr>
<tr><td rowspan="2">112 ビット
セキュリティ</td><td>新規生成*1)</td><td rowspan="2">移行完遂期間
*4)</td><td>利用不可</td><td rowspan="2">利用不可</td><td rowspan="2">利用不可</td><td rowspan="2">利用不可</td></tr>
<tr><td>処理*2)</td><td>許容*3)</td></tr>
<tr><td rowspan="2">128 ビット
セキュリティ</td><td>新規生成*1)</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">移行完遂期間
*4)</td><td>利用不可</td><td rowspan="2">利用不可</td></tr>
<tr><td>処理*2)</td><td>許容*3)</td></tr>
<tr><td rowspan="2">192 ビット
セキュリティ</td><td>新規生成*1)</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td></tr>
<tr><td>処理*2)</td></tr>
<tr><td rowspan="2">256 ビット
セキュリティ</td><td>新規生成*1)</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td></tr>
<tr><td>処理*2)</td></tr>
</table>

*1) 新規に暗号処理を実行する場合（例：暗号化、署名生成）

*2) 処理済みのデータに対して処理を実行する場合（例：復号、署名検証）

*3) 処理済みのデータに対する正当性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合

*4) よりセキュリティ強度の高い暗号技術又は鍵長への移行を完遂させなければならない期間。利用する暗号処理が短期間で完結する場合（例：エンティティ認証）、又は既存の電子政府システムの継続利用やそれらとの互換性・相互接続性維持のための利用に限定

アルゴリズム及び鍵長の選択・実装要件及び利用要件の基本方針

- 設定されたセキュリティ強度要件と同じかそれ以上のセキュリティ強度を満たすアルゴリズム及び鍵長の組合せを推定セキュリティ強度の表から選択してサポート（実装）しなければならない。
- 設定したセキュリティ強度要件以下の安全性のアルゴリズム及び鍵長をサポート（実装）すること自体は妨げない。ただし、サポート（実装）されたアルゴリズム及び鍵長のすべてが常に利用されてよいわけではなく、その利用期間については、そのセキュリティ強度に応じて、セキュリティ強度要件に従って定めなければならない。

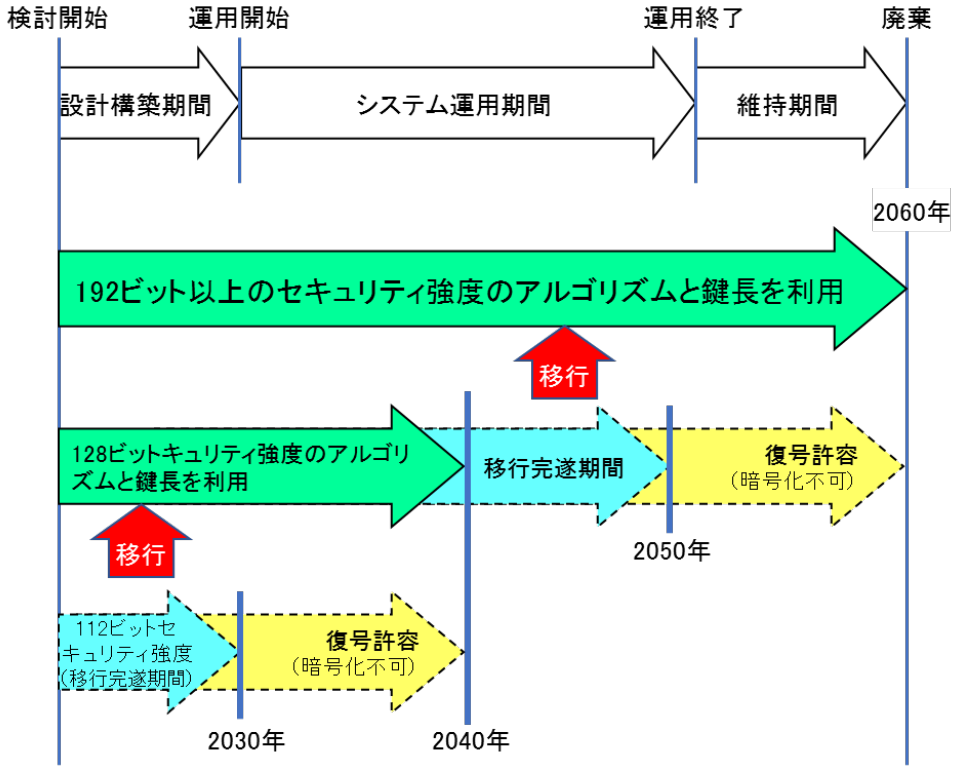

図 2-3　アルゴリズム及び鍵長の実装（サポート）要件

- データのセキュリティ寿命は利用するアルゴリズムのセキュリティ寿命に包含されなければならない。

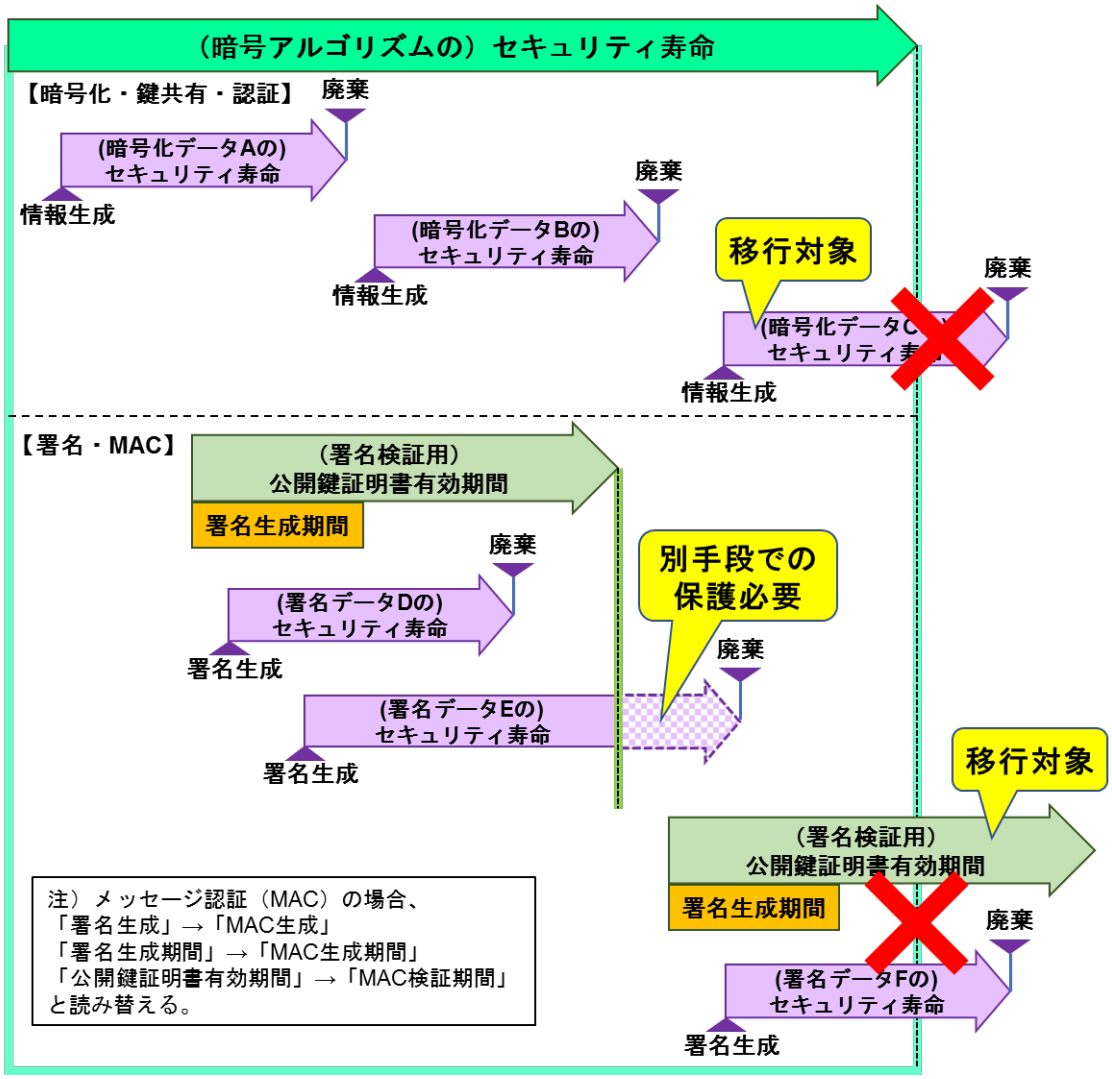

図 2-4　アルゴリズム及び鍵長の利用要件

CRYPTREC 暗号リスト上の暗号技術とセキュリティ強度との対応

本設定基準の中では、2021 年末時点での CRYPTREC 暗号リストに記載の暗号アルゴリズムごとの安全性評価の現状等を踏まえた推定セキュリティ強度を示している。これらは、今後、暗号解読手法の進展や大規模量子コンピュータの実現等により、推定セキュリティ強度が見直される可能性がある（少なくとも 5 年ごとに再確認される）。

運用中における暗号技術及び鍵長移行に関する検討の必要性

新しいアルゴリズム及び鍵長に移行するのは、多くの場合、非常に時間とコストがかかる作業であることを念頭に置いておく必要がある。実際、過去にあったアルゴリズムや鍵長における大規模な移行（例：DES から AES への移行、RSA での鍵長 1024 ビットから 2048 ビットへの移行、SHA-1 から SHA-256 への移行など）では、移行準備から移行完了までに

5 年から 10 年単位の時間がかかっている。

そのため、利用しているアルゴリズムや鍵長がセキュリティ寿命を迎える少なくとも 5 年前までには、より強力なアルゴリズム及び鍵長への移行計画を策定すべきである。また、その移行計画を立てる際には、いつからどのくらいの期間をかけてどのアルゴリズムや鍵長に移行するのかを明確にすべきである。

外部要因により、利用しているアルゴリズムや鍵長の移行に関する検討を行う必要が出てくるケースとして、以下のようなものがある。これらに該当する事象が発生した場合には、直ちに内容の確認を行い、必要に応じて移行計画を策定しなければならない。本設定基準では、これらに応じて移行計画を策定する際に考慮しなければならないポイントを示している。

- 電子政府システムの運用寿命の延長に伴う対応
- セキュリティ強度要件の設定変更に伴う対応
- 暗号技術の推定セキュリティ強度の変更に伴う対応
- 運用監視暗号リストに掲載されたアルゴリズムの継続利用にあたっての対応
- 突発的な理由に伴う緊急移行にあたっての対応
- 量子コンピュータの実現リスクへの対応

2.3. 「暗号鍵設定ガイダンス」の作成

本書では、まず安全な暗号技術の導入の観点から、暗号技術を利用する際の鍵長の選択方法に関する一般的な考え方を解説する。また、暗号技術の安全な運用の観点から、適切に暗号鍵の管理を行うために必要となる項目についての技術的概要を示すことを目的としている。

2020 年度活用委員会での議論を踏まえ、2021 年度の活用委員会では表 2-5 のとおりに作成方針を定め、「暗号鍵設定ガイダンス」を作成した。作成にあたっては、以下の論点について主に検討を行い、検討結果を設定基準に反映させた。

具体的には、暗号鍵を安全に設定し、運用していくために考慮すべき項目として以下の項目を解説している。詳細については、暗号鍵設定ガイダンス [8]を参照されたい。

8 CRYPTREC、暗号鍵設定ガイダンス、https://www.cryptrec.go.jp/report/cryptrec-gl-3003-1.0.pdf

表 2-5　「暗号鍵設定ガイダンス」の作成方針

文書体系	運用ガイドラインの一つと位置付け。GL を附番
利用目的	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を提供する
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
備考	SP800-57 Part 1 に記載がある「アルゴリズムや鍵長の設定以外の鍵管理に関する事項（保護手段など）」は「暗号鍵管理ガイダンス」に分ける
主な論点	● 「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の明確化 ● ビットセキュリティの基準をどこまで区切るか ● システムやアプリケーションの運用寿命とセキュリティ強度要件の関係をどのように整理するか ● 求められるセキュリティ強度要件の考え方 ● 「暗号鍵のライフサイクル」「暗号鍵の（タイプごとの）利用期間」「鍵の保護」についての記載内容 ● 移行に関する検討の必要性についての記載内容

● 暗号鍵の鍵長

システムやアプリケーションなどのセキュリティ（暗号学的安全性）に直接影響する項目である。どのような暗号処理に使う鍵なのか（鍵タイプ）、どのぐらいの期間利用するものなのかに依存して必要なセキュリティ強度要件を検討し、その要件を満たす適切な鍵長を選択する必要がある。

なお、「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」との最大の違いは、求められるセキュリティ強度要件の考え方が違うことである。「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」では電子政府システムにおいて十分なセキュリティ強度を持たせるために必要な要件として予め規定しているのに対して、本ガイダンスでは実際の利用用途や利用期間、環境、コスト、その他様々な制約条件を踏まえて、読者が必要なセキュリティ強度を決めるように勧めている。

目安として、表 2-6 でのビットセキュリティを**下限のセキュリティ強度**として、**一定のセキュリティマージン（数十ビット）を追加**したそれ以上のセキュリティ強度で設定することが望ましいとしている。

ただし、「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」に合致しない鍵長を用いた場合には、CRYPTREC 暗号リストの暗号技術を利用しているとは見なされないことに留意されたい。

表 2-6　1982 年の DES と同等のセキュリティを提供すると推定される（＝その後 10～15 年程度安全と期待される）ビットセキュリティ

	1982	2030	2040	2050	2060	2070
ANSSI（2014）[9]	56	81 ～ 96	86 ～ 104	91 ～ 112	96 ～ 120	101 ～ 128
Lenstra（2001）[10]	56	93	101	109	－	－
Lenstra（2004）[11]	56	88	95	102	－	－

- 暗号鍵の鍵タイプ

  どのような暗号処理に使う暗号鍵なのかによって決まる項目である。鍵タイプの種類によって、暗号鍵に求められるセキュリティ要件（保護要件）は異なる。

  そのような要件として、以下の項目を挙げている。

  - セキュリティ特性
  - 関連性保護
  - 保証の必要性
  - 保護期間

- 暗号鍵のライフサイクル

  個々の暗号鍵の生成から破棄までの鍵状態とその間の遷移を示す項目である。暗号鍵の取扱いで重要なのは、利用する様々な鍵に対して、当該鍵のライフサイクルを正しく運用管理することである。とりわけ、利用期間が経過した暗号鍵を利用停止・破棄することや、暗号鍵の危殆化が起きた又は疑われる場合の当該鍵の利用を制限・破棄することなどを適切に行うことによって、暗号鍵そのものの安全性を確保することが必要である。また、鍵の危殆化対策を予め講じておくことも鍵の危殆化の可能性や影響を最小限に抑えることに役立つ。

---

9 Mécanismes cryptographiques - Règles et recommandations, Rev. 2.03, ANSSI , 02/2014 https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf

10 Selecting Cryptographic Key Sizes, Arjen K. Lenstra and Eric R. Verheul, Journal of Cryptology, vol. 14, p. 255-293, 2001. https://link.springer.com/content/pdf/10.1007/s00145-001-0009-4.pdf

11 Key Lengths, Arjen K. Lenstra, The Handbook of Information Security, 06/2004. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.694.8206

このほか、運用中における暗号技術及び鍵長移行に関する検討の必要性についても言及している。

2.4. 暗号鍵管理ガイダンス作成に向けた検討結果について

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）[12]」を公開したことに引き続き、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。

暗号鍵管理ガイダンス WG では、情報システム設計者とシステム調達者が、暗号鍵管理を適切に扱うための支援を目的に活動をおこなっている。そのため、本 WG では暗号鍵管理の検討の第一歩として、各々の業界が自己の業界の事情を盛り込んだ参照プロファイルを作成することを支援するための暗号鍵管理ガイダンスを作成している。なお、暗号鍵管理ガイダンスの位置づけと想定読者は以下のとおりとしている。

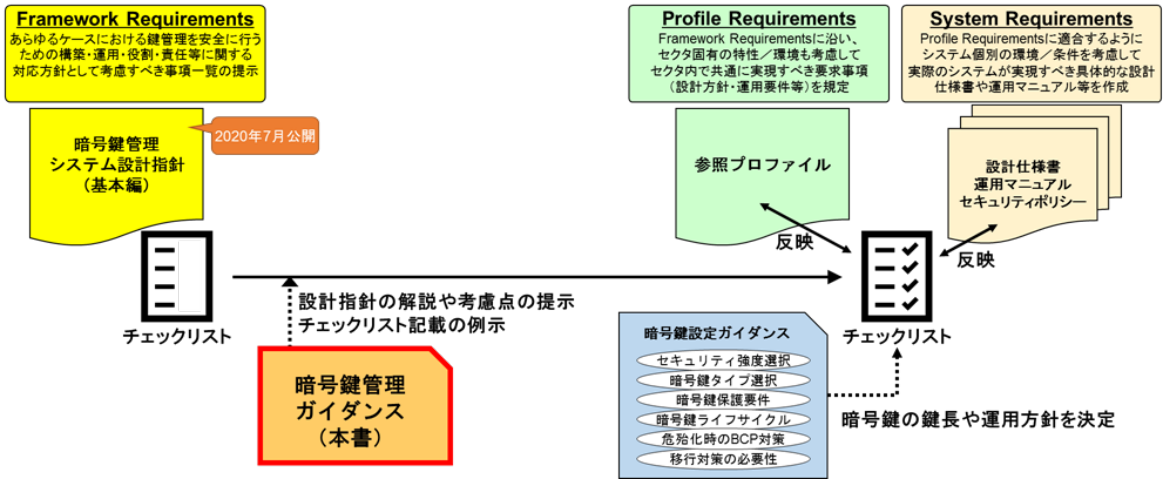

図 2-5　「暗号鍵管理ガイダンス」作成の位置づけ

位置づけ

- 暗号鍵管理プロファイルを作成するためのガイダンスを作成する。ただし、特定の業界において使用する参照可能なプロファイルは含まれない点については注意されたい。
- 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。

12 https://www.cryptrec.go.jp/report/cryptrec-gl-3002-1.0.pdf

- 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や、発生しうる失敗例を説明する。

<u>想定読者</u>

- 暗号鍵管理機能を持つシステム設計者
- 各業界において、暗号鍵管理の参照プロファイルを作成する担当者
- 一部の内容については、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等

2021 年度は、実際のガイダンス作成の進め方についての検討を行い、ガイダンス作成に向けた執筆方針の方向性を取りまとめることに注力した。WG での具体的な活動報告については、別紙「2021 年度暗号鍵管理ガイダンス WG 活動報告」を参照されたい。

【ガイダンス内容のイメージ】

本ガイダンスでは、要求内容については基本的に暗号鍵管理システム設計指針（基本編）の Frame Requirements の内容をそのまま転記し、「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」を中心に説明を加筆する。

表 2-7　「暗号鍵管理ガイダンス」の執筆内容

各節のフォーマット		
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**

【ガイダンス作成の進め方】

暗号鍵管理システム設計指針（基本編）の要件（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。

- 暗号鍵管理システム設計指針（基本編）での 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
- トイモデルを使ったガイダンスの中で CBP に該当する部分を参考
- 「ユースケースを例題・想定した記載」は本文中に想定しない

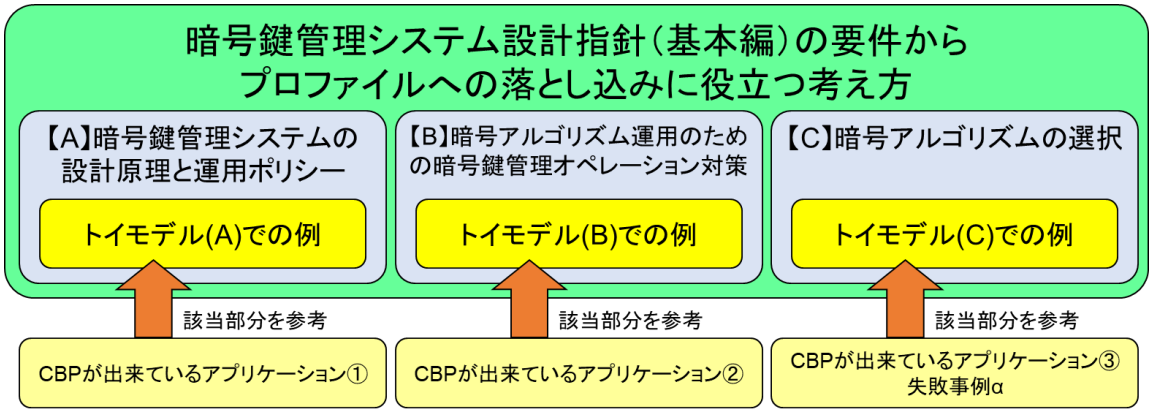

図 2-6　「暗号鍵管理ガイダンス」作成の進め方

今後、要求内容に対して、「どのように判断すればよいのか」「何をすれば対応済みと言えるのか」についての考え方を示すことを目的に、以下の意義を考慮して記載する内容を決めていくものとする。

- 鍵管理に必要な情報を集中的に管理できる（検索も可能）
- 「該当する情報がない」ことが確認できる
- インシデント発生時のレスポンスが早くなる
- インシデント発生時の説明責任に有用
- 監査対象から各リスト項目が漏れる可能性を減らす
- 情報アセットの洗い出しに利用できる（企業の重要資産の洗い出しに利用可能）
- 引き継ぎ等が容易になる
- 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
- 将来的な対策の文脈で有用。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

第3章　今後に向けて

2022 年度に予定されている CRYPTREC 暗号リストの改定に向け、IPA と協力して暗号利用実績調査を実施し、策定された選定基準に照らし合わせた実績評価を行う。また、暗号鍵管理ガイダンス WG にて検討中の暗号鍵管理ガイダンスを完成させる予定である。

【別紙】

2021 年度　暗号鍵管理ガイダンス WG 活動報告

1.　2021 年度の活動内容

1.1　活動内容

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）」を公開したことに引き続き、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。

暗号鍵管理ガイダンス WG では、情報システム設計者とシステム調達者が、暗号鍵管理を適切に扱うための支援を目的に活動をおこなっている。そのため、本 WG では暗号鍵管理検討の始めとして、各業界が自業界の事情を盛り込んだ参照プロファイルを作成することを支援するための暗号鍵管理ガイダンスを作成している。なお、暗号鍵管理ガイダンスの位置づけと想定読者は以下の通りとする。

<u>位置づけ</u>

- 暗号鍵管理プロファイルを作成するためのガイダンスを作成する。ただし、特定の業界において使用する参照可能なプロファイルは含まれない点については注意されたい
- 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や、発生しうる失敗例を説明する

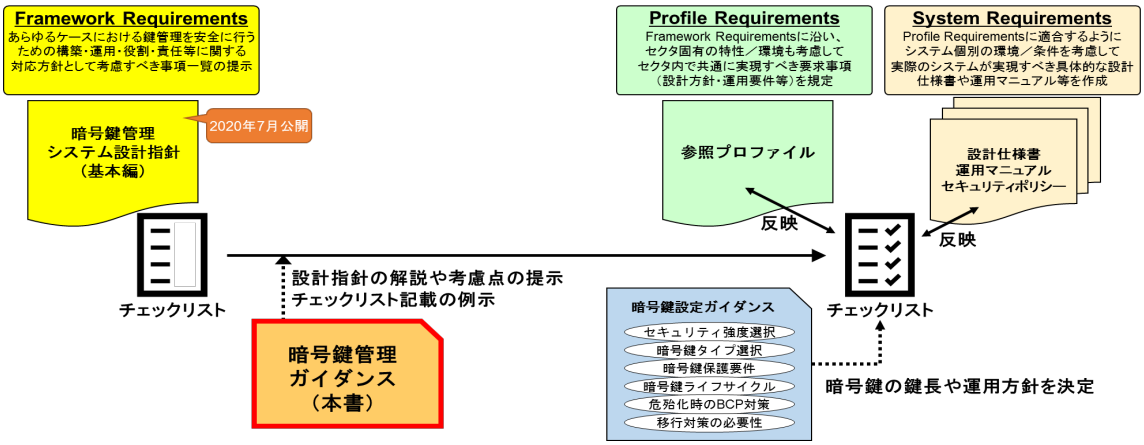

図 1-1　「暗号鍵管理ガイダンス」の位置づけ

想定読者

- 暗号鍵管理機能を持つシステム設計者
- 各業界において、暗号鍵管理の参照プロファイルを作成する担当者
- 一部の内容については、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等

1.2 暗号鍵管理ガイダンス WG の開催状況

暗号鍵管理ガイダンス WG での審議概要は表 1-1 のとおりである。

表 1-1 暗号鍵管理ガイダンス WG 開催状況

回	開催日	議案
第一回	2021 年 7 月 26 日	■ CRYPTREC 活動について ➢ CRYPTREC 全体の活動概要 ➢ 2021 年度暗号技術活用委員会活動計画 ➢ 2021 年度暗号鍵管理ガイダンス WG 活動計画 ■ 暗号鍵管理ガイダンスについて ➢ 執筆方針について
第二回	2021 年 11 月 17 日	■ 執筆方針の変更点について ■ ガイダンス記載方法の検討 ■ 参考資料についての検討
第三回	2022 年 2 月 16 日	■ 3 章の節ごとの記載方針の説明と審議 ■ 実際の記載例に関する審議 ■ 記載の詳細に関する情報収集

1.3 暗号鍵管理ガイダンス WG の委員構成

暗号鍵管理ガイダンス WG の委員構成は表 1-1 のとおりである。

表 1-1　暗号鍵管理ガイダンス WG　委員構成

主査	上原　哲太郎	立命館大学　情報理工学部　情報理工学科　教授
委員	漆嶌　賢二	GMO グローバルサイン株式会社　プロダクトマネジメント部 部長
委員	垣内　由梨香	マイクロソフト株式会社　セキュリティレスポンスチーム 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　総合数理学部　先端メディアサイエンス学科　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　開発本部 プラットフォーム開発センター　セキュリティプラットフォーム開発課　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 セキュリティ本部セキュリティ情報統括室　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　カスタマーエクスペリエンス シニアセキュリティアーキテクト
委員	舟木　康浩	タレス DIS CPL ジャパン株式会社　クラウドプロテクション& ライセンシング　データプロテクション事業本部 セールスエンジニアマネージャ
委員	満塩　尚史	デジタル庁 戦略・組織グループ　セキュリティ危機管理チーム セキュリティアーキテクト

（2022 年 3 月 31 日現在）

2.　成果概要

2.1　活動概要

2021 年度の当初計画では以下の項目の検討を行う予定としていたが、実際のガイダンス作成の進め方についての検討に多くの時間を費やしたため、ガイダンス作成に向けた執筆方針の方向性を取りまとめることに注力した。

【当初計画での検討項目】

- 鍵管理プロファイルを理解するために必要な知識の整理
- 所定の用途の鍵管理プロファイルを作成するために必要な情報の整理
- 上記のうち特に重点的に説明が必要な項目の精査
- 記載するモデルの検討
- 失敗例についても各業界から情報を収集、整理し、公開方法についての検討

2.2　ガイダンス作成の進め方

当初のガイダンス作成の進め方としては、暗号鍵管理システムの理解を進めてもらうことを期待して、①（シンプルなモデルを利用した）具体例を提示して、鍵管理における要求や思想が理解できるように説明、②（ありがちな）失敗例を提示して、暗号鍵管理における特に注意すべきリスクや発生しうる失敗を分かりやすく説明することを想定していた。

この想定のもと、以下の進め方案をベースに検討を行った。

【当初のガイダンス作成の進め方案】

- Current Best Practices（CBP）がすでに出来ているアプリケーションを抽象化・類型化し、類型ごとにトイモデルを作成
- 抽象化や匿名化を駆使して、失敗事例を人工的に作り直し、公表できる形式に整理
- トイモデルや失敗事例を参考に、暗号鍵管理システム設計指針（基本編）の要件からプロファイルへの落とし込みに役立つ考え方を抽出し、ガイダンスとして記載

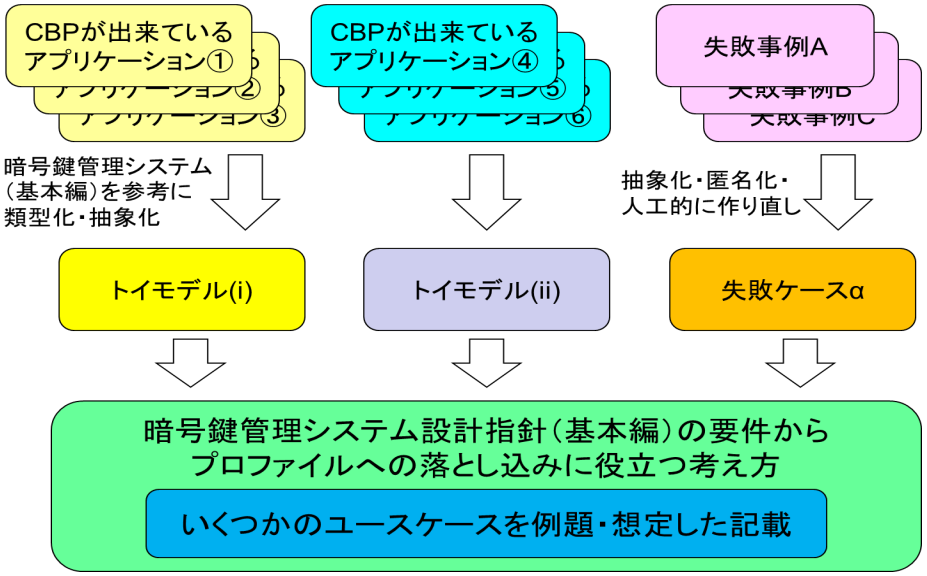

図 1-2　当初の「暗号鍵管理ガイダンス」作成の進め方

《考え方》

- CBP がすでに出来ているアプリケーション
  - お手本となる鍵管理の仕組みが機能している
  - 他でも参考にできる、暗号鍵管理システム設計指針（基本編）が求めるエッセンスのいくつかは実現されていると期待
- トイモデル（シンプルなモデル、簡略化したモデル）
  - 分かりやすくないと使う人が限られてしまうので、厳密性より分かりやすさを優先した方が各業界に貢献できると期待
  - 多くのトイモデルを記載できれば鍵管理要件を統括的に理解できると期待
- 失敗事例
  - 失敗例があると現実感もあり、ガイダンス読者の理解も進むと期待
  - 自社システムとの共通点がある場合に失敗を自覚することが可能
  - 失敗の影響をより適切に評価できる
  - しかし、企業は失敗事例を公開したくないはずなので、実例調整は必須（実例をそのまま出すことはしない）

しかしながら、検討を進めた結果、CBP が出来ているアプリケーションは厳密に固められているので、数種類の CBP を一つのトイモデルに類型化するのが難しいこと、また複雑で重いシステムが多いので、想定読者が理解し易いトイモデルへの抽象化がそもそも難しいことが分かった。さらに、業界ごと適切に類型化されたトイモデルでなければ想定読者にとってガイダンスとして使えないことから、トイモデルごとの読者数など、作業量に見合う効果があるかが課題として出てきた。

そのため、当初の「CBP を類型化・抽象化してトイモデルを作る」ことを止め、「ガイダンスとして説明しやすいトイモデルを先に作る」方針に変更することにした。

【変更後のガイダンス作成の進め方案】

暗号鍵管理システム設計指針（基本編）の要件（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。

- 暗号鍵管理システム設計指針（基本編）での 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
- トイモデルを使ったガイダンスの中で CBP に該当する部分を参考
- 「ユースケースを例題・想定した記載」は本文中に想定しない

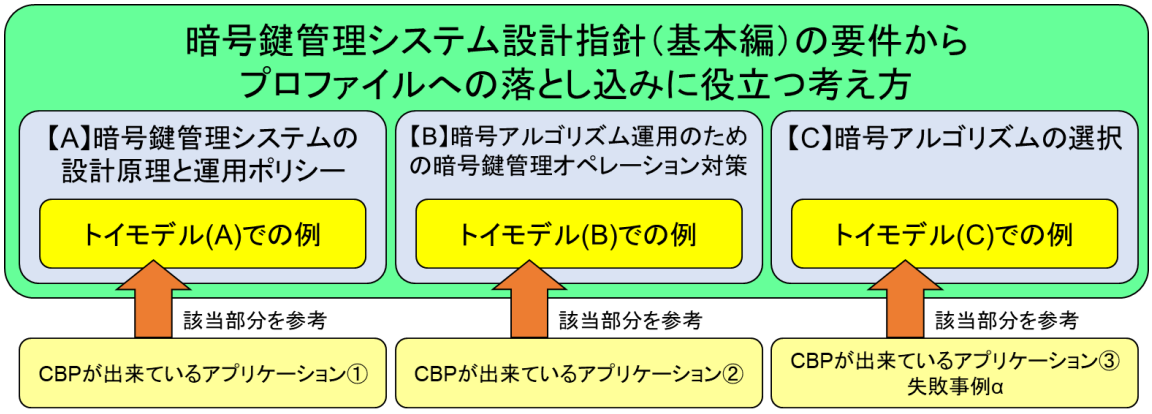

図 1-3　変更後の「暗号鍵管理ガイダンス」作成の進め方

《想定中のトイモデル》

【A】 暗号鍵管理システムの設計原理と運用ポリシー

- CA システム：
  ポリシーやメカニズムについて参考にできるドキュメントが多い

【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

- RFC2845, 8945（TSIG: Transaction SIGnature）：
  運用が非常にシンプルで説明しやすい

【C】 暗号アルゴリズムの選択

- TLS 通信等における暗号スイートの確立フェーズ：
  利用する暗号アルゴリズムの選択が行われるフェーズであり、説明しやすい

【D】 暗号アルゴリズム運用に必要な鍵情報の管理

- TLS サーバ等の鍵設定・管理：
  複数の鍵やメタデータが相互に関係するシンプルな鍵情報管理が行われており、説明しやすい

【E】 暗号鍵管理デバイスのセキュリティ対策

- クラウドを想定したアクセス制御等：
  CSA Japan のガイドラインが参照できる
- オンプレミスのアクセス制御等：
  JDCC のガイドラインが参照できる

【F】 暗号鍵管理システムのオペレーション対策

- 認定を受けた製品が TTP により運用されるモデルや eIDAS 関連の技術標準を利用している製品を参考に検討中：
  対象は、監査、アカウンタビリティ、アテステーション等が含まれているモデルを検討中

2.3　ガイダンス内容のイメージ

本ガイダンスでは、要求内容については基本的に暗号鍵管理システム設計指針（基本編）の Frame Requirements の内容をそのまま転記し、「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」を中心に説明を加筆する。

表 1-3　「暗号鍵管理ガイダンス」の執筆内容

各節のフォーマット		
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**

なお、同じような要求内容はまとめて説明を記載するほうが分かりやすいので、節構成として一緒に取りまとめることとした。例えば、「暗号鍵管理システムの設計原理と運用ポリシー」では以下のような構成を想定している。

- セキュリティポリシー（A.01～A.05）
- ポリシーなどからの要求事項（A.06～A.13）
- 異なるセキュリティドメイン間に関する事項（A.14～A.21）
- マルチレベルのセキュリティドメインの鍵情報（A.22～A.24）
- アップグレード・ダウングレード（A.25～A.26）
- 役割と責任（A.27～A.31）
- 構築環境（A.32）
- 日時の正確性（A.33～A.36）
- 実現目標（A.37～A.42）
- システム間の相互運用（A.43～A.46）
- ユーザーインターフェース（A.47～A.50）
- 商用既製品の活用（A.51～A.53）
- 標準／規制に対する適合性（A.54～A.57）
- 移行、脆弱性対応（A.58～A.69）

今後は、このようにグルーピングした要求内容ごとに、記載すべき解説・考慮点及び利用するトイモデルについての概要を議論していく。その際、要求内容に対して、「どのように判断すればよいのか」「何をすれば対応済みと言えるのか」についての考え方を示すことを目的に、以下の意義を考慮して記載する内容を決めていくものとする。

- 鍵管理に必要な情報を集中的に管理できる（検索も可能）
- 「該当する情報がない」ことが確認できる
- インシデント発生時のレスポンスが早くなる
- インシデント発生時の説明責任に有用
- 監査対象から各リスト項目が漏れる可能性を減らす
- 情報アセットの洗い出しに利用できる（企業の重要資産の洗い出しに利用可能）
- 引き継ぎ等が容易になる
- 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
- 将来的な対策の文脈で有用。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

2.4　ガイダンスの目次

ガイダンスの目次については、暗号鍵管理ステム設計指針（基本編）を踏襲して以下のように決定した。今後の議論により目次に修正が必要な場合は、WG において議論し、修正することとした。

---

8 章　暗号鍵管理システム（CKMS）のオペレーション対策
付録

3.　今後に向けて

今年度の検討結果を踏まえ、引き続き記載すべき解説・考慮点及び利用するトイモデルについての検討を進め、2022 年度末までに暗号鍵管理ガイダンスを完成させる予定である。

CRYPTREC Report 2021
(暗号技術活用委員会報告　CRYPTREC RP-3000-2021)

発行日　2022年6月30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
(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