CRYPTREC Report 2020

令和３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、総務省及び経済産業省が主催してい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によって共同で運営されている暗号技術活用委員会の 2020 年度活動報告である。

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（以下、運用ガイドライン）の作成に注力している。

2020 年度は、新型コロナウイルスによるパンデミックの影響により例年の活動とは大きく異なり、上期は延期されていた 2019 年度の活動の締めくくりがメインの活動となったため、本年度の活動期間は実質的に下期に限定されることとなった。このため、2021 年度から新たな運用ガイドラインとして「鍵長に関するガイドライン」及び「暗号鍵管理参照プロファイル作成に関するガイダンス」を作成することとし、それらの作成方針を検討、取りまとめを行うところまでを行った。なお、今回検討を行った「鍵長に関するガイドライン」は、CRYPTREC 暗号リストに掲載された安全な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ガイダンスすることを目的としたものであり、CRYPTREC 暗号リストの構成要素となる重要なガイドラインである。また、「暗号鍵管理参照プロファイル作成に関するガイダンス」は、2020 年 7 月に公開した「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とすることを意図して企画されたものである。

今年度の成果をもとに、来年度以降、両ガイドラインの拡充を早期に図り、広く活用を促していくことが、ひいて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ことを期待している。

末筆ではあるが、例年とは大きく異なる活動状況にも関わらず、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。

2021 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、2020 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。

2019 年度以前の CRYPTREC Report は、CRYPTREC 事務局（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、総務省と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。

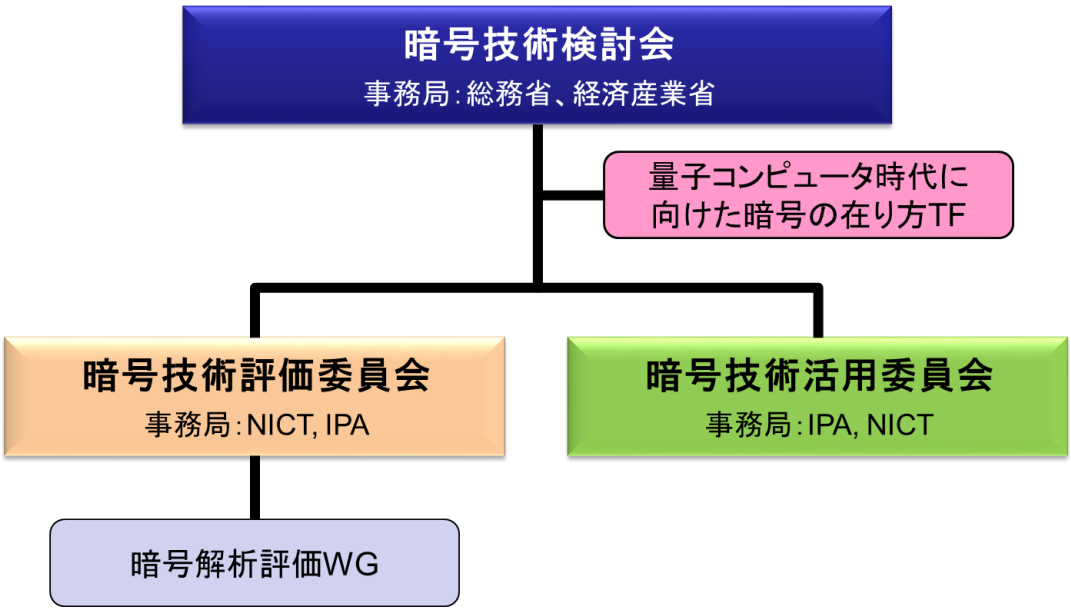

図 1　2020 年度の CRYPTREC の体制

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	宇根 正志	日本銀行 情報技術研究グループ長[2020 年 9 月まで]
委員	田村 裕子	日本銀行 企画役補佐[2020 年 9 月から]
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	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	杉尾 信行	株式会社 NTT ドコモ
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	内閣官房 政府 CIO 補佐官
委員	山岸 篤弘	日本情報経済社会推進協会 客員研究員
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：2021 年 3 月末時点）

オブザーバー

木村 誠一郎	内閣官房内閣サイバーセキュリティセンター
川崎 明彦	内閣官房内閣サイバーセキュリティセンター
高木 浩光	内閣官房内閣サイバーセキュリティセンター
小林　宏至	内閣官房内閣サイバーセキュリティセンター[2020 年 12 月まで]
東 隆夫	内閣官房内閣サイバーセキュリティセンター[2021 年 1 月から]
衛門 愛子	個人情報保護委員会 事務局[2020 年 7 月まで]
柏原 陽	個人情報保護委員会 事務局[2020 年 7 月から]
千葉 英之	総務省 行政管理局
梅城 崇師	総務省 サイバーセキュリティ統括官室
黒田 淳	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

三島 崇　　経済産業省 産業技術環境局
上田 翔太　　経済産業省 商務情報政策局
飯山 貴啓　　経済産業省 商務情報政策局[2020 年 8 月まで]
村山 裕紀　　経済産業省 商務情報政策局[2020 年 9 月から]
松原 祐衣子　外務省 大臣官房 情報通信課
伊藤 江美子　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
山口 義隆　　警察大学校[2020 年 12 月まで]
山添 正裕　　警察大学校[2021 年 1 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、小暮淳、橋本徹、天内日紗子[2020年9月まで]、木島慶子[2020年10月から]、伊藤 忠彦[2021年1月から]、石川 誠[2021年1月から]）
国立研究開発法人情報通信研究機構（久保田実、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、高橋しおり、青野良範、高安 敦、小川 一人、伊藤 竜馬）

第1章　2020 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。

2020 年度は、新型コロナウイルスの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を 2020 年 6 月 1 日に開催し、その後「TLS 暗号設定ガイドライン」及び「暗号鍵管理システム設計指針（基本編）」の公開（2020 年 7 月 7 日公開）に向けた作業を行ったなどの影響により、実質的に下期のみの活動となった。

このため、今年度の活動内容としては、2021 年度からの運用ガイドラインの整備に向けて、「鍵長ガイドライン（仮）」の作成方針の取りまとめ、及び「暗号鍵管理の参照プロファイル」の作成に向けた検討を開始することとした。

（1）鍵長ガイドライン（仮）の作成方針の取りまとめ

CRYPTREC では、CRYPTREC 暗号リストとして安全な暗号アルゴリズムを選定してきたが、安全に利用する推奨鍵長について明示したものはなかった。しかしながら、安全性を実際に維持するためには推奨鍵長を適宜見直す必要がある。一方、実際の中長期的な情報システムの運用管理上、事前対策なしに利用すべき鍵長が途中で変わることは暗号アルゴリズムを交換するのとほぼ同様のコストがかかるなどの影響が発生することが想定される。

そこで、中長期的な推奨鍵長をガイダンスすることにより、情報システム設計時に必要な対策を検討することを促すためのガイドラインを 2021 年度に作成することとし、2020 年度は作成方針案の取りまとめまでを行った。

（2）暗号鍵管理の参照プロファイルの作成に向けた検討

2020 年 7 月に、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。

引き続き、暗号鍵管理ガイドラインの拡充を目的として、具体的な参照プロファイルの作成を 2021 年度から開始することとし、2020 年度は今後の進め方を取りまとめるところまでを行った。

1.2. 開催状況

2020 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　2020 年度暗号技術活用委員会　開催概要

回	開催日	議案
第一回 (注)	2020 年 6 月 1 日	■ TLS 暗号設定ガイドライン WG 活動及びガイドライン案について ■ 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 ■ 暗号鍵管理システム設計指針（基本編）について ■ 2020 年度暗号技術活用委員会活動案について
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

（注）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

第2章　成果概要

2.1. 鍵長ガイドライン（仮）の作成方針の取りまとめについて

CRYPTREC 暗号リストとして安全な暗号アルゴリズムを選定してきたが、安全に利用する推奨鍵長について明示したものはなかったため、中長期的な推奨鍵長をガイダンスすることにより、情報システム設計時に必要な対策を検討することを促すためのガイドラインを 2021 年度に作成することとした。

そこで、以下の論点について、第二回と第三回の委員会で検討を行い、ガイドライン作成に向けた方針案を取りまとめた。

【論点】

- ガイドラインの位置づけ
  - 文書体系
  - 利用目的
  - 想定読者
- 安全性の基準の考え方
- ガイドラインで示すべき内容（項目）
  - 前提条件
  - 具体的な技術的検討項目（考え方）

<u>ガイドラインの位置づけ</u>

鍵長の選択にあたっては、「鍵そのものの有効期間」「対象システムの寿命や利用環境」「対象データの機微度や保護期間」などの要因を総合的に勘案する必要がある。例えば、1 年間だけ保護できれば良いシステムと、30 年間保護する必要があるシステムとでは、必要な安全性を達成するために選択すべき鍵長が異なる。また、デバイスなどで利用可能なリソース量の違いによっても選択できる鍵長の範囲が変わってくる。このことは、システムの開発や運用、調達の責任者が、利用用途や利用環境等を踏まえて実際に採用する鍵長を決める必要があることを意味する。

一方、CRYPTREC 暗号リストは、電子政府システム用途で利用することを一義的な目的としている。実際、政府機関の情報セキュリティ対策のための統一基準では、『情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、以下の事項を含めて定めること。』とされている。したがって、

CRYPTREC 暗号リストの一要素としての鍵長の選択ということであれば、電子政府システム用途での安全な利用を前提としたものとなる。

以上の違いを踏まえ、「用途を限定して満たすべき鍵長の要件を規定する」という考え方に基づく文書と「用途を限定せずに鍵長の設定方法に関するガイダンスを提供する」という考え方に基づく文書とに明確に分離し、両方の文書の検討を進めることとなった。具体的には、前者の位置づけのものを「鍵長設定要件（仮)」とし、CRYPTREC 暗号リストの一要素を成すものとする。一方、後者の位置づけのものを「鍵長設定ガイダンス（仮）(一般用)」とし、運用ガイドラインの一つとする。

両者の利用目的などの違いは、以下の表のとおりである。

表 2-1 ガイドラインの位置づけ

	「鍵長設定要件（仮）」	「鍵長設定ガイダンス(仮)(一般用)」
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。	運用ガイドラインの一つと位置付け。CRYPTREC で作成するなら GL を附番
利用目的	電子政府システム用途で利用する場合の鍵長選択に関する要件を規定	用途を特定せず、鍵長やアルゴリズムの選択方法に関するガイダンスを提供
想定読者	電子政府システム用途での情報システム調達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、等 （その他の利用者は、ボランタリベースと位置付ける）	システム又はアプリケーションの所有者や管理者、設計者、開発者、運用担当者、利用者、等
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。	SP800-57 Part 1 に記載がある「鍵長やアルゴリズムの選択以外の鍵管理に関する事項（鍵状態遷移や保護手段等）」は「鍵管理ガイダンス（仮）」に分ける。

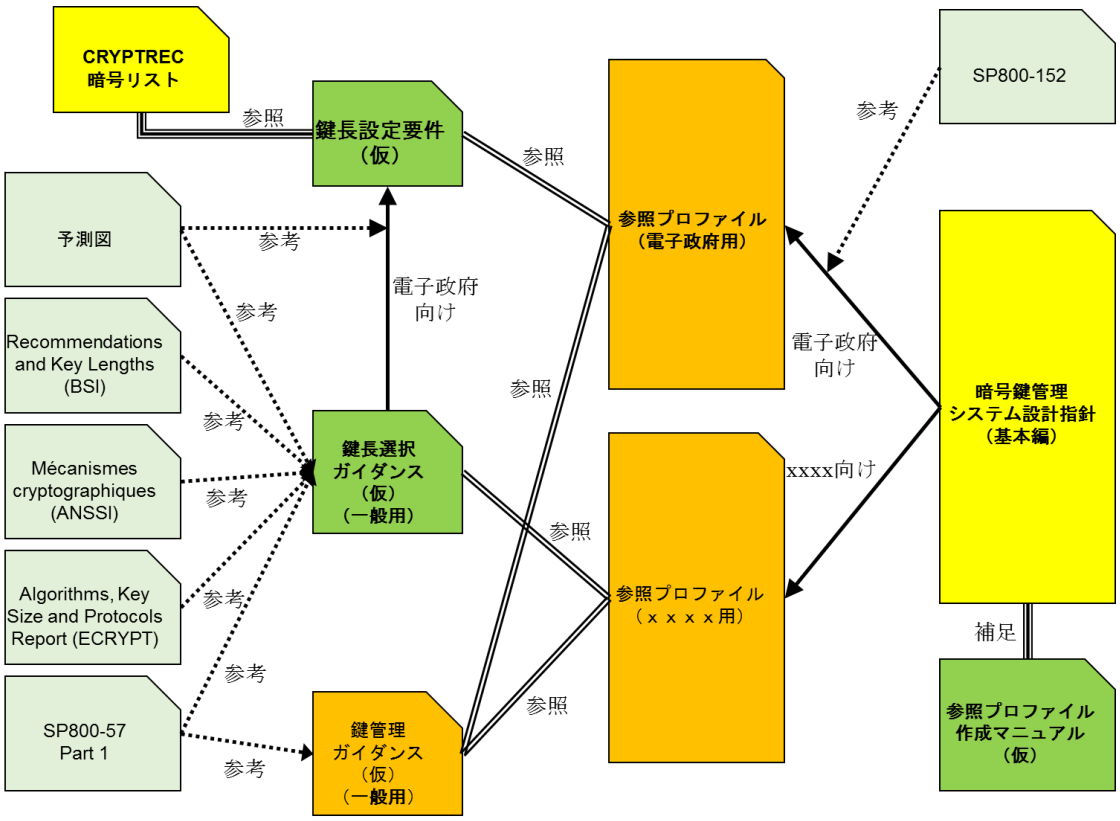

図 2　将来的に目指す鍵管理ガイドライン等の相関

<u>安全性基準の考え方</u>

- **様々なドキュメントで使われている「ビットセキュリティ（セキュリティレベル、セキュリティ強度）」を基本単位として鍵長を定める**

  具体的には、コンセンサスが得やすく、かつ合理的な判断を行うことを目的とするため、基準とするビットセキュリティをある程度の間隔をもって設定することとする。例えば、ビットセキュリティの基準として、比較的コンセンサスが得られていると思われる 112 ビット、128 ビット、192 ビット、256 ビットを採用するとともに、その他に、80 ビット、100 ビット（又は 96 ビット）、160 ビット、224 ビットを設定するかどうかを検討していく。

表 2-2　【参考】ビットセキュリティ（セキュリティレベル、セキュリティ強度）の説明

BSI（独）	● A cryptographic mechanism achieves a security level of n bits if costs which are equivalent to 2^n calculations of the encryption function of an efficient block cipher (e.g. AES) are tied to each attack against the mechanism which breaks the security objective of the mechanism with a high probability of success.

	● Approximate computing power R required (in multiples of the computing power needed for a simple cryptographic operation, e.g. one-time evaluation of a block cipher on a single block) for the calculation of discrete logarithms in elliptic curves (ECDLP) and/or the factorisation of general composite numbers of the specified bit lengths.
NIST（米）	● A number associated with the amount of work (i.e., the number of operations) that is required to break a cryptographic algorithm or system. In this Recommendation, the security strength is specified in bits and is a specific value from the set {80, 112, 128, 192, 256}. ● Given a few plaintext blocks and the corresponding ciphertext, an algorithm that can provide X bits of security would, on average, take 2^{X-1} T units of time to attack, where T is the amount of time that is required to perform one encryption of a plaintext value and compare the result against the corresponding ciphertext value.
ECRYPT（EU）	● For example the best attack against a block cipher of key length kb should be equivalent to 2^{kb} block cipher invocations, whereas the best known attack against an elliptic curve system with group order of ke bits should be $2^{ke}/2$ elliptic curve group operations.

- **対象システムの「想定運用終了年」を基準とした、採用すべき「ビットセキュリティ」を表現したものとする**

  システムの設計・構築・運用の開始時期ではなく、システムの運用終了・廃棄までの「システム寿命（システムライフタイム）」に着目する。つまり、システムの運用終了・廃棄まで安全に運用できる鍵長を選択できるようにすることを基本とする。

  システムの設計・構築・運用の開始時期時では安全とされる鍵長であっても、運用終了～廃棄までの維持期間も安全に運用できる鍵長でなければ、システム運用期間中に「暗号アルゴリズムや鍵長の移行」が必須となることを意味する。

図 3　システム寿命

- **「移行（Transition）」の考え方や必要性について言及する**

  運用中のシステムから新しいシステムに瞬時に切り替えるということは大変困難である。そのため、新旧システムの併用期間が設定され、その期間中に徐々に切り替えていくのが一般的である。一方、セキュリティシステムの場合、その切り替えが終わる前にセキュリティ上の問題が生じないようにしなければならないため、移行完了の時期を先に決定し、そこからさかのぼる形で移行開始時期を決める必要がある。

  さらには、危殆化などのセキュリティ上の理由により、緊急に移行を行わなければならなくなることもある。

  とりわけ、長期運用のシステムでは、上述したような対応に迫られるリスクが高いため、予め「暗号アルゴリズムや鍵長の移行」についての対応策を検討しておくことが望ましい。

- **原則として 5 年周期で「要求するビットセキュリティ」の内容を再確認することとする**

  前提として長期は「現時点」での判断結果に基づくものであって、最後まで保証するものではない。そのため、5 年ごとにその時々の最新の知見を考慮して内容を再確認し、必要に応じて変更するルールを導入する。

- **今回は、量子コンピュータによる危殆化は原則的に想定しない**

  暗号技術評価委員会傘下の暗号調査 WG（暗号解析評価）での報告において「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の合成数を素因数分解することは困難であり、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ない限りは現代暗号の脅威にはならないと考えることができる。」との見解が出されている。このことは、現時点において、暗号解読で用いるほど大きなパラメータを扱える量子コンピュータの実現時期を含め、量子コンピュータによる危殆化の時期を予測することは事実上極めて困難であることを意味している。

  このため、今回は量子コンピュータによる危殆化は想定しないこととし、注意喚起として「Quantum Safe Security」について何らかの形で記載するものとする。今後、暗号解読が実際に扱える量子コンピュータの実現時期について十分に信頼できる予測がされるなど、状況の変化が明確になった時点で、内容を再考する。

- **以下のラベリングをつける方向で検討する**

  暗号化や署名などでは、新規に暗号化や署名などを行う「新規データの生成」のタイミングと、生成済のデータに対して復号や署名検証などを行う「生成済データの処理」のタイミングが大きく異なる場合がある。一方、鍵交換やエンティティ認証では、通

常、送信者が行う「新規データの生成」のタイミングと受信者が行う「生成済データの処理」のタイミングはほぼ同じである。
このような特性の違いを考慮して、利用可否を整理するのがこのラベリングの役目である。

表 2-3　ラベリング例

	新規データの生成	生成済データの処理
暗号化（通信時）	利用可（＝acceptable）	利用可（＝acceptable）
	利用不可（＝disable/disallowed）	利用不可（＝disable/disallowed）
		＜復号を認めるかは要検討＞
暗号化（保管時）	利用可（＝acceptable）	利用可（＝acceptable）
	利用不可（＝disable/disallowed）	復号のみ可（＝deprecated/legacy use）
		利用不可(注)（＝disable/disallowed）
鍵交換	利用可（＝acceptable）	利用可（＝acceptable）
	利用不可（＝disable/disallowed）	利用不可（＝disable/disallowed）
		＜再構成を認めるかは要検討＞
署名	利用可（＝acceptable）	利用可（＝acceptable）
	利用不可（＝disable/disallowed）	検証のみ可（＝deprecated/legacy use）
		利用不可(注)（＝disable/disallowed）
MAC	利用可（＝acceptable）	利用可（＝acceptable）
	利用不可（＝disable/disallowed）	検証のみ可（＝deprecated/legacy use）
		利用不可(注)（＝disable/disallowed）
エンティティ認証	利用可（＝acceptable）	利用可（＝acceptable）
	利用不可（＝disable/disallowed）	利用不可（＝disable/disallowed）

（注）:「暗号化（保管時）」「署名」「MAC」の生成済データの処理については、暗号技術以外の手段で何らかのリスク低減措置が取られていれば、（期限を決めずに）リスク受容を条件に利用不可とまではしなくてもよいかもしれない。

ガイドラインで示すべき内容（項目）

- **「鍵長設定要件（仮）」の作成方針**

  CRYPTREC 暗号リスト記載の暗号アルゴリズムを電子政府システム用途で利用する場合を前提とした鍵長やアルゴリズムの選択に関する要件、及び「移行（Transition）」の考え方や必要性に絞って記載するものとする。すなわち、CRYPTREC 暗号リストに記載がない暗号アルゴリズム（例：軽量暗号、高機能暗号）や電子政府システム用途以外（例：自動車、IoT デバイス、制御システム）は考慮しない。

  - 112 ビットセキュリティ以上を対象とする。

  また、「取り扱う期間」は、30 年程度以上、又は電子政府システム用途や法令上で最も長い運用期間を目安として検討していく。その際、強めの要件を意図し、「最小」＞「レガシーシステム・ユース」の区分けを採用する。

  - 「最小」：新規調達・更新調達で使う際の基準
  - 「レガシーシステム・ユース」：既存システムや暗号化済・署名済データを使う際の基準

- **「鍵長設定ガイダンス（仮）（一般用）」の作成方針**

  用途を特定せず、鍵長やアルゴリズムの選択方法に関するガイダンスとして、「鍵長設定の考え方」、「移行の考え方や必要性」、「鍵タイプ」及び「（鍵タイプごとの）推奨暗号利用期間」について記載するものとする。「鍵長設定の考え方」では、CRYPTREC 暗号リスト記載の暗号アルゴリズムに限定せず、目的に応じた鍵長設定の考え方を示す。また、CRYPTREC 暗号リストに記載がない暗号アルゴリズム（例：軽量暗号、高機能暗号）についても含める。

  - 80 ビットセキュリティ、又は 100 ビットセキュリティ（96 ビットセキュリティ）以上を対象とする。

  「取り扱う期間」は、暗号技術評価委員会が作成している素因数分解の予測図が発行年＋20 年であることを考慮し、20 年から 30 年程度を目途に適切な期間を検討していく。また、用途を限定しない以上、どの程度のセキュリティを求めるかの判断は読者が行うことを原則とし、要件としての意図は求めないこととする。その代わりの対策として、鍵長以外でのセキュリティ確保の考え方も示す。例えば、「移行に向けた事前準備」「鍵利用期間の制限」「危殆化発生時対応計画」の組合せ、など。

2.2. 暗号鍵管理参照プロファイルの作成に向けた検討結果について

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、具体的な参照プロファイルの作成を 2021 年度から開始することとしている。

そこで、以下の論点について、数回の委員会で検討を行い、今後の進め方を取りまとめた。

【論点】

- 位置づけの整理
  - 目的
  - 想定システム・サービス
  - 期待点・メリット
  - 懸念点・デメリット
- 今後の進め方

<u>位置づけの整理</u>

参照プロファイルは、詳細なシステムやサービスを想定するほど、厳密なプロファイルを作成することが可能になると考えられるが、その他のシステムやサービスへの転用が難しくなると思われる。一方、具体的なシステムやサービスを想定しないと、プロファイルの作成そのものが難しい。

そこで、具体的な参照プロファイルの作成方法を検討するにあたり、まず出来上がりの文書の位置づけの整理を以下のようにまとめた。

表 2-4　位置づけの整理

	考え方 1	考え方 2	考え方 3
目標	CKMS チェックリスト（の一部項目）に、そのまま流用、もしくは少々の改変で利用可能な形になっている<u>参照プロファイルを作成</u> ● CA 局の CP/CPS と同程度のレベルでのプロファイルをイメージ	CKMS チェックリストの中で「必要最小限の統一的条件（ベースライン）」を取りまとめた<u>参照プロファイルを作成</u> ● SP800-152（米国政府システム共通プロファイル）と同程度のレベルでのプロファイルをイメージ	参照プロファイルそのものではなく、参照プロファイルの<u>作成マニュアルを作成</u> ● 暗号鍵管理システム設計指針（基本編）の解説を兼ねる

想定システム・サービス	具体的なシステムモデル／サービスモデル	一般的・汎用的なシステムモデル／サービスモデル	システム・サービスは例示（シンプルなモデル、トイモデル）
期待点	うまく当てはまるケースであれば、個々の設計仕様書やプロファイルの作成の効率化がかなり図れる	想定範囲内に含まれる様々なシステム／サービスでの個々の設計仕様書やプロファイルの作成において、一定程度の安全性の底上げが期待できる（項目がある）	● 暗号鍵管理システム設計指針（基本編）の理解や、仕様書やプロファイルへの落とし込み方の理解が進むと期待できる ● 各業界の業界団体等が、該当の業態の実態に即したプロファイルを作る事が期待できる
懸念点	● 想定したシステムモデル／サービスモデルがそもそも現実的であるか不明 ● 想定から外れたシステムモデル／サービスモデルではほとんど使えない可能性が高い ● 他の（上位）ポリシーなどと整合しない可能性もある（現状の整合性、将来の相互運用性、両方で課題が発生する可能性がある） ● 一般企業が調査対象に含まれる場合、企業機密に近い情報が必要となる可能性もある	● 参照プロファイルに記載できるのは、CKMS チェックリストのごく一部にとどまると予想される ● 想定範囲内に含まれる様々なシステムモデル／サービスモデルでの条件の公約数的なものしかプロファイルに記載できない可能性が高い ● 多くの機関の情報を得る必要があることが予想される ● 「ベースライン」のスコープ定義においては、各機関の利害調整が必要となる可能性が高い	● 参照プロファイルではないので、個々の設計仕様書やプロファイルの作成のための流用はほぼ不可能 ● 体系的な理想形や推奨を提示しているわけではない

作成方針

懸念点を踏まえると、「考え方 1」では多くのシステムが使用できるプロファイル作成が難しく、さらに対象とする具体的なシステムの選定に時間がかかる可能性が高い。また、「考え方 2」では必要最小限の統一的条件の決め方が難しいことが予想される。そのため、まずは「考え方 3」で参照プロファイルの作成方法を整理するところから始めることとする。

その際、第一の想定読者は、プロファイル作成者や鍵管理システム設計者とする。但し、鍵管理システム調達者や利用者も想定読者とする。

作業スケジュールとしては 2 年計画とし、分野／領域を踏まえ、WG を発足させて検討を進める。

2021 年度は、重点的に説明が必要な項目の精査、及び各分野から情報を収集し記載するモデルの検討を行う。その後、本文のドキュメント化を進め、2022 年度に作成マニュアルを完成させる予定で作業を進める。なお、時間があれば、マニュアルの本文完成後に、マニュアルに沿って作成したプロファイル例を付録用に作成する。

例示としてのシンプルなモデルの候補は以下のものを含め、WG で検討を行う。

- オンプレミス HSM を利用した鍵へのアクセスコントロール（デバイス向け鍵管理、Web 用証明書）
- リモート管理された鍵へのアクセスコントロール（リモート署名、暗号化鍵のクラウド管理、等）
- クラウドデータに対するアクセスコントロール
- 失敗事例

第3章　今後に向けて

今年度の検討結果を踏まえ、2021 年度から「鍵長設定要件（仮)」、「鍵長設定ガイダンス（仮）(一般用)」、及び「暗号鍵管理参照プロファイル作成マニュアル」の作成を行う。なお、参照プロファイル作成マニュアルについては、CKMS 参照プロファイル検討 WG（仮）を設置して検討していく計画である。

また、2022 年度に計画されている CRYPTREC 暗号リストの改定に伴い、利用実績などに関する選定基準の検討も行う予定である。

CRYPTREC Report 2020
(暗号技術活用委員会報告 CRYPTREC RP-3000-2020)

不許複製 禁無断転載

発行日　2021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
(技術本部 セキュリティセンター 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