暗号技術検討会
２０１８年度　報告書

２０１９年３月

目　　次

１．はじめに

情報通信技術の急速な発展により、自動車、家電、医療、農業、工場など様々な分野で、あらゆるモノがネットワークに繋がる IoT 社会が到来し、サイバー空間と実空間の高度な融合により、多様なニーズにきめ細やかに対応したモノやサービスを提供できる社会への産業構造の変化が進みつつある。一方で、IoT 機器の普及に伴うサイバー攻撃の起点の増加や、サイバー攻撃自体の巧妙化・複雑化が続く中で、サイバー攻撃の影響が実空間にまで到達するリスクも増していくと考えられる。このような産業構造、社会の変化に伴うサイバー攻撃の脅威の増大に対応したセキュリティ確保が求められる中、暗号技術は既に様々な製品やサービスに組み込まれ、セキュリティを支える基盤技術として欠かせないものであるが、IoT 機器から得られる大量のデータの流通・連携を支える上でも、その重要性は一層増すと考えられる。

このような社会の変化に伴い、CRYPTREC においても、これまで取り組んできた暗号アルゴリズムのセキュリティ確保を引き続き推進することに加えて、暗号アルゴリズムを利用したプロトコルのセキュリティ確保のための活動拡大や、情報システム全体のセキュリティ確保に向けた暗号技術の利活用のための情報提供等の貢献が求められている。

本年度の活動として、暗号技術評価委員会では、学会等での情報収集に基づく CRYPTREC 暗号等の監視、普及が進んでいる暗号利用モード（XTS）に係る安全性評価等を行ったほか、同委員会の下に設置された暗号技術調査 WG において、耐量子計算機暗号に関する技術報告書を発行した。暗号技術活用委員会では、鍵管理に関する運用ガイドライン等の作成に向けた検討を行っているところである。これらの 2018 年度の両委員会の活動の詳細については、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取りまとめる「CRYPTREC Report 2018」を参照いただきたい。そして、暗号技術検討会では、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」（以下「CRYPTREC 暗号リスト」という。）の改定に向けて、各委員会での議論も踏まえた検討を行った。

今後も暗号技術を用いた情報システム及び情報社会全体のセキュリティ確保のために、成果物の検討や情報発信等を行っていく所存である。

末筆であるが、暗号技術検討会及び関係委員会等に御協力いただいた構成員、オブザーバの方々をはじめ、関係者の皆様に心から謝意を表する次第である。

2019 年 3 月

暗号技術検討会
座長　松本　勉

２．暗号技術検討会開催の背景及び開催状況

２．１．暗号技術検討会開催の背景

暗号技術は情報セキュリティの基盤技術であり、その安全性を暗号技術の専門家により技術的、専門的な見地から客観的に評価することが重要である。電子政府のセキュリティ確保のためには、安全性に優れた暗号技術を利用することが不可欠である。

このため、総務省及び経済産業省は、客観的な評価により安全性及び実装性に優れると判断される暗号技術をリスト化し、各府省に対してその利用を推奨することにより、高度な安全性と信頼性に支えられ、国民が安心して利用できる電子政府の構築に貢献することを目指し、2001 年 5 月に最初の暗号技術検討会を開催した。

暗号技術検討会において 2003 年 2 月に策定された電子政府推奨暗号リストは、2013 年 3 月に 10 年ぶりの改定が行われ、CRYPTREC 暗号リストとして発表されたが、その後においても、電子政府推奨暗号等の安全性を評価・監視し、暗号技術の更なる普及促進を行うため、総務省及び経済産業省は、継続的に暗号技術検討会を開催している。

２．２．CRYPTREC の体制

CRYPTREC とは、Cryptography Research and Evaluation Committees の略であり、総務省及び経済産業省が共同で開催する暗号技術検討会（座長：松本勉横浜国立大学教授）と、国立研究開発法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で開催する委員会から構成される暗号技術評価プロジェクトをいう。

2018 年度の CRYPTREC においては、暗号技術評価委員会では、学会等での情報収集に基づく CRYPTREC 暗号等の監視等を行い、暗号技術活用委員会では、鍵管理に関する運用ガイドライン（鍵管理ガイドライン）等の作成を行った。

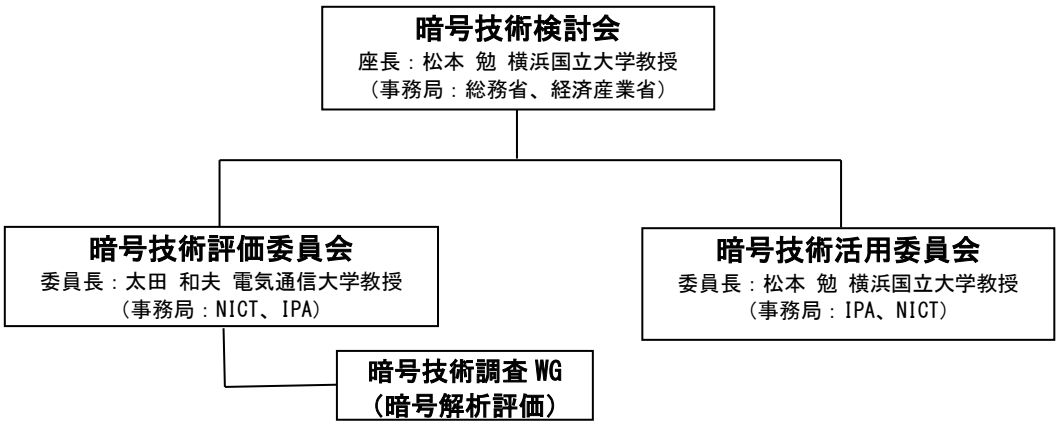

図 2.2.1　2018 年度 CRYPTREC 体制図

２．３．暗号技術検討会の開催実績

2018 年度の暗号技術検討会は、暗号技術評価委員会、暗号技術活用委員会の活動報告、次期 CRYPTREC 暗号リストの改定に向けた検討に係る審議、「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」の設置に係る承認等を行うために１回開催した。

【第 1 回】2019 年 3 月 29 日（金）10:00～11:30
（主な議題）
・ 2018 年度 暗号技術評価委員会 活動報告について
・ 2018 年度 暗号技術活用委員会 活動報告について
・ 次期 CRYPTREC 暗号リストの改定に向けた検討について
・ 「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」の設置について
・ 暗号技術検討会 2018 年度 報告書（案）について
（概要）
・ 2018 年度の暗号技術評価委員会及び暗号技術活用委員会の活動報告が行われた。
・ 次期 CRYPTREC 暗号リストの改定に向けた検討及び「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」の設置について、事務局から説明し、タスクフォースの設置は原案のとおり承認された。構成員からは、時間が経過するほど量子コンピュータによるリスクは高まり、耐量子計算機暗号に対応したシステムへの移行に要するコストは増加すると考えられるため、早期にタスクフォースでの検討を開始してほしいとのコメントや、Society5.0 時代において、多用に使用される暗号技術を整理することが重要とのコメントがあった。
・ 暗号技術検討会 2018 年度 報告書（案）について事務局より説明を行った。構成員からは、「４．今後の CRYPTREC の活動について」に「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」の検討事項の一つである、その他新たな暗号技術の動向等（軽量暗号や秘密計算に利用される準同型暗号等）を踏まえた検討等を行うことを明記した方が良いとのコメントを受け、事務局において原案に修正を行った上で、構成員から一任された座長の承認を受けることとなった。

３．各委員会の活動報告

３．１．暗号技術評価委員会

３．１．１．活動の概要

暗号技術評価委員会は、CRYPTREC 暗号リストに掲載されている暗号技術や電子政府システム等で利用される暗号技術の安全性維持及び信頼性確保のために安全性及び実装に係る監視及び評価を行う。主要な検討課題は以下のとおりである。

・暗号技術の安全性及び実装に係る監視及び評価
・推奨候補暗号リストへの新規暗号（事務局選出）の追加
・新技術等に関する調査及び評価

これらの課題について 2018 年度に行った具体的な検討内容を、以下のとおり報告する。

３．１．２．2018 年度の活動内容

暗号技術の安全性及び実装に係る監視及び評価

2018 年度は、①学会等での情報収集に基づく CRYPTREC 暗号等の監視、②「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の更新の検討を実施した。

①について、研究集会、国際会議、研究論文誌の情報等を収集し、リスト掲載暗号の安全性について監視活動を行った。

②について、「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の更新を検討し、T.Kleinjung 氏および A.K.Lenstra 氏に計算量見積もりの主要部分の評価を依頼し、素因数分解の困難性に関する計算量の再評価を実施し、計算量見積もりの再評価レポートなどを得た。評価レポートは、CRYPTREC ホームページに公開予定。一方、近年の計算機の性能向上が鈍化傾向にあることを踏まえ、この傾向を予測図にどのように反映するかについては慎重に検討する必要があるという意見を踏まえ、今年度は前年度までと同じ方法により更新を行うとともに、以降の予測図の在り方については、次年度継続検討を行うこととした。

新世代暗号に係る調査

本項目に係る活動に関しては、暗号利用モード XTS の安全性評価を行った。XTS モードは、以下の条件下では、暗号利用モード（秘匿モード）として CRYPTREC 暗号リストへ追加するための安全性要件を満たしていると判断した。

（条件 1）利用用途は IEEE および NIST SP-800-38E の規格に沿ったストレージやディスクの暗号化に限る。

（条件 2）XTS 内のブロック暗号には、 CRYPTREC 暗号リスト掲載の 128 ビットブロック暗号を使う。

（条件 3）鍵を変えずに処理するデータ量は、2^{20} ブロックまでとする。

新技術等に関する調査及び評価

本項目に係る活動に関しては、①耐量子計算機暗号の技術動向調査等、②今後の CRYPTREC 暗号リストにかかわる検討を実施した。

①について、暗号技術評価委員会の下に暗号技術調査 WG（暗号解析評価）を設置し、主に、耐量子計算機暗号（Post-Quantum Cryptography）の技術動向調査・執筆を実施し、技術報告書を完成させた。技術報告書は、CRYPTREC ホームページに公開する。

②について、第一回委員会では、CRYPTREC における耐量子計算機暗号への対応について議論し、第二回委員会では、次期 CRYPTREC 暗号リストに向けた方針の議論を行った。委員会で出た意見をまとめ、暗号技術検討会に報告した。

３．１．３．暗号技術評価委員会の開催状況

2018 年度、暗号技術評価委員会は計２回開催した。各回会合の概要は表 3.1.1 のとおりである。

表 3.1.1　暗号技術評価委員会の開催状況

回	開催日	議題
第１回	2018 年７月 19 日	・ 暗号技術評価委員会活動計画の具体的な進め方の検討 ・ 暗号技術調査ワーキンググループ（暗号解析評価）の活動計画案の検討 ・ XTS モードの安全性評価について外部評価実施の検討 ・ CRYPTREC における耐量子計算機暗号への対応について検討 ・ 監視活動状況報告
第２回	2019 年３月 11 日	・ 暗号技術調査ワーキンググループ（暗号解析評価）の活動報告 ・ XTS モードの安全性評価に関する外部評価レポート報告及び安全性評価検討 ・ 次期 CRYPTREC 暗号リストに向けた方針の検討 ・ 監視活動状況報告 ・ CRYPTREC Report 2018（暗号技術評価委員会報告）の目次案提示 ・ CRYPTREC シンポジウム概要案提示

2018 年度、暗号技術調査 WG（暗号解析評価）は計３回開催した。各回会合の概要は表

3.1.2 のとおりである。

表 3.1.2　暗号技術調査 WG（暗号解析評価）の開催状況

回	開催日	議題
第 1 回	2018 年 6 月 27 日	事前調整会議での議論を基に技術報告書の執筆方針を決定
第 2 回	2018 年 10 月 12 日	技術報告書の各章について、中間報告を実施。加筆・修正について議論。
第 3 回	2019 年 2 月 15 日	技術報告書の執筆完了。最終調整を実施。

３．２．暗号技術活用委員会

３．２．１．活動の概要

2017 年度に実施した「鍵管理に関する運用ガイドライン作成に向けた事前調査」の結果を踏まえ、2018 年度は鍵管理ガイドラインの作成を開始し、主に以下の活動を行った。

- 鍵管理に関するフレームワークの検討
- 上記の検討結果に基づく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）」のドラフト版の作成

３．２．２．2018 年度の活動内容

鍵管理に関連する代表的なガイドラインの事前調査結果（図 3.2.1）を踏まえ、以下の調査対象のガイドラインについて、想定読者や目的、及び相互の関連性について、より詳細に調査を行った。

鍵管理に関するフレームワーク（暗号鍵管理システム設計指針）についての検討

＜調査対象とするガイドライン＞

- SP800-57 Part1 revision4: Recommendation for Key Management, Part 1: General
- SP800-57 Part2 revision1(draft): Recommendation for Key Management, Part 2: Best Practices for Key Management Organization
- SP800-130: A Framework for Designing Cryptographic Key Management Systems
- SP800-152: A Profile for U.S. Federal Cryptographic Key Management Systems

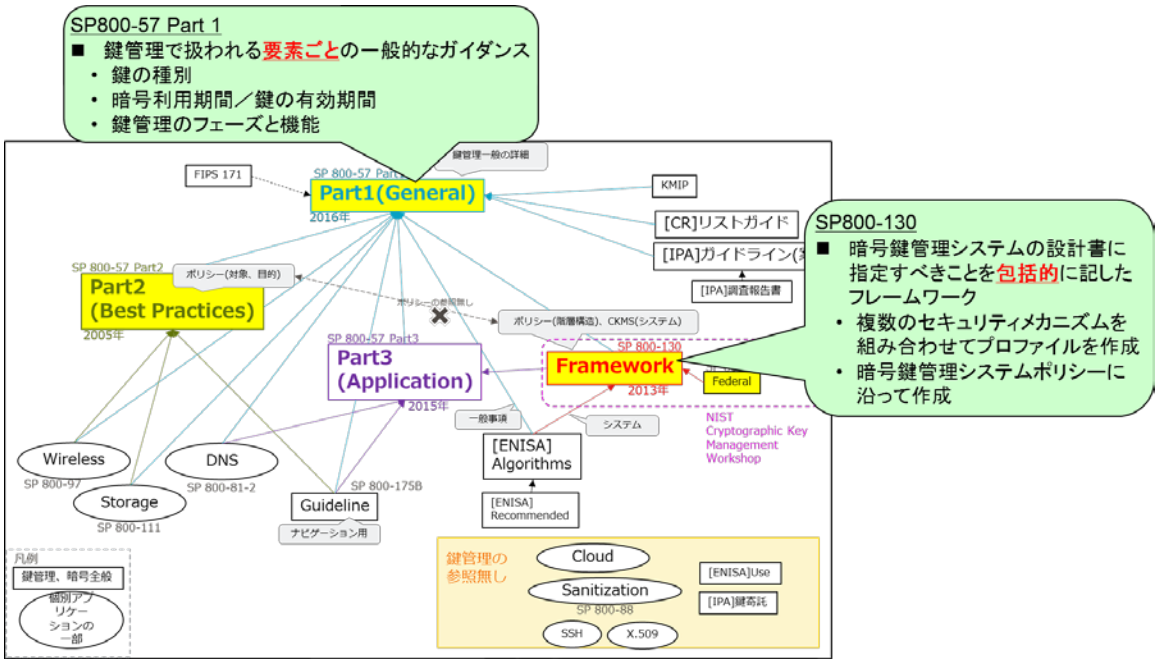

図 3.2.1　鍵管理に関連する代表的なガイドラインの事前調査結果

表 3.2.1　各ガイドラインの想定読者や目的

SP800-57 Recommendation for Key Management	暗号メカニズムの不適切な選択による安全性確保は困難であり、プロトコルやアプリケーションの実際の安全性にほとんどまたはまったく寄与しない。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の提供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が目的
Part 1: General	・システム開発者／管理者 役に立つ汎用的な鍵管理ガイダンス ・暗号モジュール開発者 具体的なアプリケーションでサポートが必要となる鍵管理特性の理解のための汎用的なガイダンス ・プロトコル開発者 具体的なアルゴリズムスイートによる鍵管理特性の確認や理解 ・システム管理者： 構成設定の最適な決定のための推奨
Part 2: Best Practices for Key Management Organization	・システム／アプリケーション所有者 組織の適切な鍵管理基盤の特定、鍵管理方針の確立、及び鍵管理の実践と計画を規定する際の使用に適合するガイダンス ・特に、暗号鍵の確立と管理の役割を担う連邦政府システムの所有者と管理者向け
SP800-130 A Framework for Designing Cryptographic Key Management Systems	暗号鍵管理システムの設計時に考慮すべきトピックや対処すべき仕様要求について記載されたフレームワークを提供が目的 ・暗号鍵管理システム設計者： チェックリストとして活用（カバーすべき全てのトピックに対する対処方法、暗号鍵管理システムに関する全ての観点での検討、暗号鍵管理システム内でのポリシー／コンポーネント／デバイスの選択、決定事項の明示、詳細仕様や理由を含めた全ての決定方針の文書化、等）
SP800-152 A Profile for U.S. Federal Cryptographic Key Management Systems	連邦政府機関や請負業者が全ての暗号鍵や関連メタデータを管理するために利用する連邦暗号鍵管理システムに対する要求事項を明示 ・暗号鍵管理システムの設計者／実装者： 適切なセキュリティサービスや鍵管理機能の選択／実装を支援 ・連邦暗号鍵管理システムの調達者／管理者／サービス利用機関：適切な暗号鍵管理システムの選択を支援

各ガイドラインの想定読者や目的は表 3.2.1 のとおりである。簡単に言えば、SP800-57 Part 1 では「鍵管理で扱われる要素ごとの一般的なガイダンス」について記載されており、特に、鍵の種別、暗号利用期間／鍵の有効期間、鍵管理のフェーズと機能といったトピックが取り上げられている。また、SP800-130 では「暗号鍵管理システムの設計書に指定すべきことを包括的に記したフレームワーク」を提示しており、暗号鍵管理システムポリシーに沿って複数のセキュリティメカニズムを組み合わせてプロファイルを作成するための指針を示している。

これらのガイドラインに記載された内容から、鍵管理を考えるうえでのあるべき構造を図 3.2.2 のように整理し、鍵管理のための設計仕様書や運用マニュアルがどのように作られるべきかを明確にした。構成要素としては以下の四つからなる。

①「Guidance」：鍵管理についての技術的な理解を助け、推奨設定などを提供する文献。例えば、SP800-57 part 1、同 part 3、CRYPTREC 暗号リスト、リストガイド（鍵管理）、SSL/TLS 暗号設定ガイドライン、などが該当する。

②「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を包括的に一覧として取りまとめたもの。SP800-130 が代表例である。あらゆるケースに適用できるように、採用すべき具体的な技術仕様は規定しておらず、あくまで③Profile Requirements や④System Requirements を具体的に検討・設計する際の考え方や検討項目を示す、設計手引書的な位置づけのものである。

③「Profile Requirements」：業界（セクタ）固有の特性や環境を踏まえた共通的な条件や設計ポリシーに基づき、①Guidance の技術的根拠を加味して、②Framework Requirements に沿って、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）を規定したもの。例えば、SP800-152 は、米国政府システム共通の暗号鍵管理システムとしての要求事項が規定されたものである。

④「System Requirements」：③Profile Requirements に適合するように、システム個別の環境／条件を考慮して作成された、実際の暗号鍵管理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のこと。システムが依存する環境や条件と①Guidance の技術的根拠の両方を加味して、具体的な技術仕様として取りまとめられる。

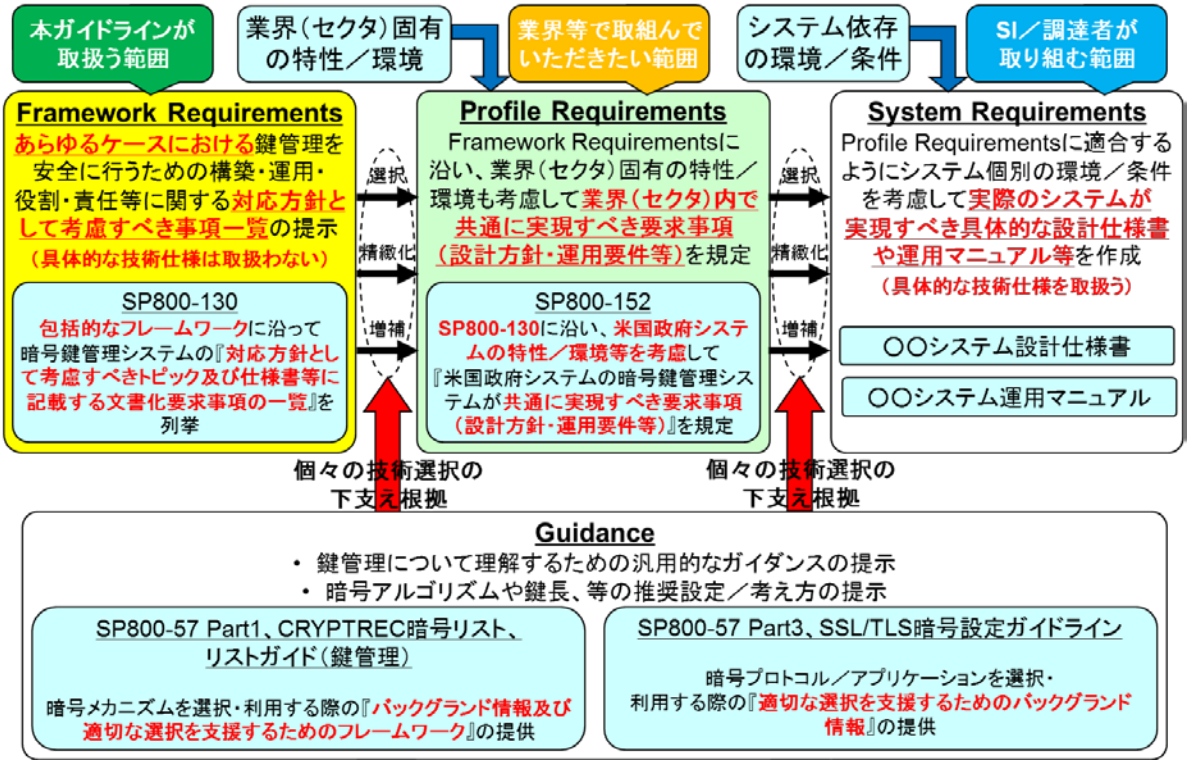

図 3.2.2　鍵管理を考えるうえでのあるべき構造

暗号技術活用委員会としては、①Guidance に含まれるガイドラインだけでは鍵管理ガイドラインとして不十分であり、②Framework Requirements を扱うガイドラインを作成すべきと判断し、SP800-130 をベースに作業を行うこととした。なお、③Profile Requirements や④

System Requirements については、個別の要件や環境等に依存する側面が強くなると考えられるため、各業界等で取り組んでいただくことを期待している。

暗号鍵管理システム設計指針（基本編）のドラフト素案の取りまとめ

SP800-130 では、暗号鍵管理システムを構築するうえで考えるべき検討項目が網羅的にカバーされており、この範囲をベースに考えれば漏れはほとんどないと思われる。しかし、検討すべき項目（Framework Requirements）が全部で 258 個もあり、かつ記載内容も教科書的な並びになっているため、必要な個所を見つけ出すことが難しい。

一方、日本では、今まで SP800-130 のような暗号鍵管理システムの設計指針の基準となる包括的・統一的な鍵管理ガイドラインが作られていないため、「鍵管理」のあり方や考え方が十分に解説されていなかった。その結果、Guidance に含まれるガイドラインを「鍵管理ガイドライン」としてきた経緯もあり、Guidance に記載がある特定の項目（例えば、暗号アルゴリズムや鍵長など）については細かく規定しているのにも関わらず、鍵管理上は重要なのに Guidance が扱っていない項目（例えば、鍵のライフサイクルや安全な鍵の保管方法、危殆化時の対策など）については規定がなかったり抽象的な記述の規定にとどまったりといったことが懸念される。このことは、鍵管理（システム）という視点で見てみると、規定した内容の粒度にムラを生じさせるということであり、システム全体の安全性確保を困難にする原因になると推察される。

そこで、暗号技術活用委員会では、イントロダクションとして鍵管理のあり方や考え方を解説し、技術的には SP800-130 の理解を深める解説書・利用手引きとして活用するための「暗号鍵管理システム設計指針（基本編）」を「鍵管理ガイドライン」として位置付けることとした。

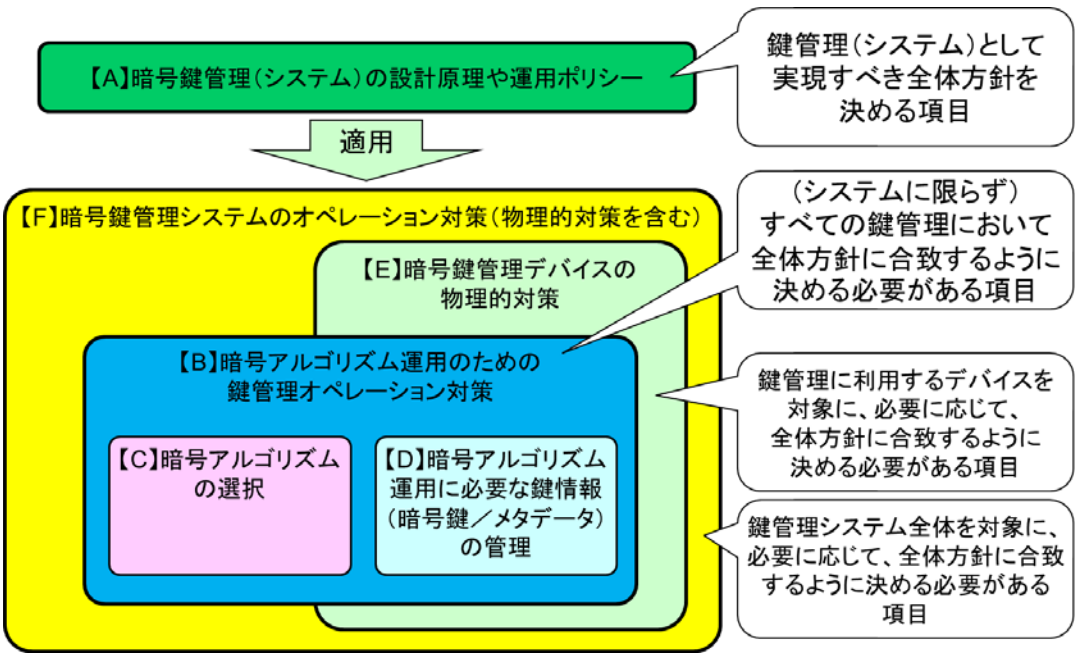

図 3.2.3　鍵管理における目的

その方針に基づき、(i) SP800-130 全体の日本語訳を作成するとともに、(ii) SP800-130 に記載されているトピックやFramework Requirements を『鍵管理における目的』に応じた対象範囲に分類・グループ化することによって、検討すべき項目の目的や必要性を明確化し、分かりやすく表現することを目指している。具体的には、どのような目的のためにどのような項目を取り扱わなければならないのかを関係性が分かるように、六つの目的に分類・再構築する方向で、ドラフト素案の取りまとめを行っている（図 3.2.3、図 3.2.4 参照)。

2章（フレームワークの基本）:フレームワークの基本的な概念をカバーし、フレームワークの概要を記載
3章（目的）:堅牢な暗号鍵管理システム(CKMS)の目的を定義
4章（セキュリティポリシー）:システム構成、及び情報管理、情報セキュリティ、CKMSセキュリティ並びに他の関連するセキュリティポリシーの必要性について記載
5章（役割と責任）:CKMSをサポートする役割と責任を提示
6章（暗号鍵とメタデータ）:CKMSの最も重要な要素(利用可能な鍵とメタデータの定義、及び鍵とメタデータの管理機能、等)を包括的に記載
7章（相互運用性と移行）:相互運用性と将来ニーズに対応するための容易な移行能力の必要性について記載
8章（セキュリティコントロール）:典型的なCKMSに適用されるセキュリティコントロールを記載
9章（テストとシステム保証）:セキュリティテストと保証について記載
10章（災害復旧）:一般及びCKMS特有の災害復旧について記載
11章（セキュリティアセスメント）:CKMSのセキュリティアセスメントについて記載
12章（技術的課題）:暗号アルゴリズム、鍵確立プロトコル、デバイス、量子コンピュータに関する新しい攻撃によってもたらされる技術的課題について記載

	目的	取扱い項目
A	暗号鍵管理（システム）の設計原理や運用ポリシー	セキュリティポリシー
		暗号鍵管理システムの構築環境／利用条件
		将来的な移行対策
B	暗号アルゴリズム運用のための鍵管理オペレーション対策	鍵情報のライフサイクル
		鍵情報のライフサイクル管理機能
		鍵情報の保管方法
		鍵情報の鍵確立方法
		鍵情報の危殆化時の BCP 対策
C	暗号アルゴリズムの選択	暗号アルゴリズムの安全性
D	暗号アルゴリズム運用に必要な鍵情報（暗号鍵／メタデータ）の管理	鍵情報（暗号鍵／メタデータ）の選択
		鍵情報の保護方針
E	暗号鍵管理デバイスの物理的対策	鍵情報へのアクセスコントロール
		セキュリティ評価・試験／システム保証
F	暗号鍵管理システムのオペレーション対策（物理的対策を含む）	暗号鍵管理システム（物理／OS とデバイス／ネットワーク）へのアクセスコントロール
		災害発生時の BCP／復旧対策（バックアップ）

図 3.2.4　SP800-130 目次と暗号鍵管理システム設計指針（基本編）（ドラフト素案）との対比

３．２．３．暗号技術活用委員会の開催状況

2018 年度に２回開催された暗号技術活用委員会での審議概要は表 3.2.1 のとおりである。この他、暗号技術活用委員会とは別に、鍵管理ガイドラインについての技術検討会合を開催した。

表 3.2.1　暗号技術活用委員会の開催状況

回	開催日	議題
第１回	2018 年９月６日	・活用委員会活動計画の確認 ・鍵管理に関するフレームワークについての検討
技術検討会合	2018 年 12 月 26 日	・鍵管理ガイドラインのドラフト素案作成に向けた技術的検討
第２回	2019 年３月 14 日	・鍵管理ガイドラインのドラフト素案の審議 ・次期 CRYPTREC 暗号リスト策定に向けた方針についての検討

４．今後のCRYPTRECの活動について

CRYPTREC では、暗号アルゴリズムの安全性確保やその利活用に係る議論のみならず、鍵管理の安全な運用に向けた取組など、暗号をとりまく環境変化に応じた新たなニーズへの対応などに取り組むこととしている。

我が国において、耐量子計算機暗号について議論を行う必要性が高まっていることのほか、既存の産業分野のみならず、今後成長する産業分野で使われる技術にも暗号技術が組み込まれることが考えられる。

こうした状況を踏まえ、暗号技術検討会の下に、「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」を新たに設置し、大規模な量子コンピュータの動向や新たな暗号技術の動向等を考慮して次期 CRYPTREC 暗号リストに求められる要件等を検討する。暗号技術評価委員会においては、引き続き、暗号技術の安全性に係る監視・評価及び実装に係る技術の監視・評価を行うとともに、同委員会の下に設置された暗号技術調査 WG において、量子計算機の共通鍵暗号への影響の調査を行う。また、素因数分解問題や離散対数問題の困難性に関する計算量の予測図の今後の方針について検討を行う。暗号技術活用委員会においては、2019 年度末の完成を目途に「暗号鍵管理システム設計指針（基本編）」の作成作業等を行うとともに、同委員会の下に TLS 暗号設定ガイドライン WG を設置し、2017 年度に一部改訂した SSL/TLS 暗号設定ガイドラインの大幅見直しを検討する。なお、両委員会の範囲を超えるものについては、必要に応じて、暗号技術検討会で審議・判断する。

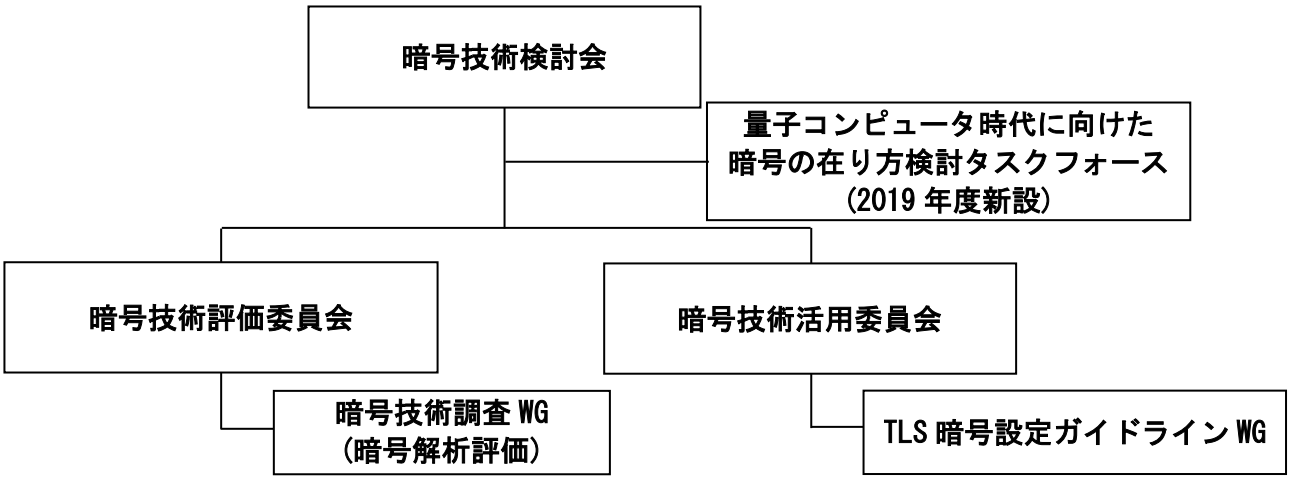

図 4.1.1　2019 年度 CRYPTREC の体制図（予定）