暗号技術検討会
２０２１年度　報告書

２０２２年３月

１．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。

2021年度の各委員会の活動として、暗号技術評価委員会では、暗号技術（署名）であるEdDSAのCRYPTREC暗号リスト（推奨候補暗号リスト）への追加を検討するため、2020年度の安全性評価に引き続き実装性能評価を行った。また、同委員会の下に暗号技術調査WG（耐量子計算機暗号）及び暗号技術調査WG（高機能暗号）を設置して、それぞれ耐量子計算機暗号及び高機能暗号に関するガイドラインを作成するための執筆方針を決定した。また、軽量暗号に関するガイドラインの作成については、2016年度版の軽量暗号ガイドラインを更新するための基となる調査報告を行い、今後の作成方針を決定した。また、暗号技術調査WG（耐量子計算機暗号）では、「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」の予測図を更新した。暗号技術活用委員会では、CRYPTREC暗号リストの改定に向けた利用実績に関する選定基準の検討、「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」の作成を行った。また、同委員会の下に設置された暗号鍵管理ガイダンスWGにおいて、「暗号鍵管理ガイダンス」の作成方針を決定した。なお、「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」は2021年度開催しなかった。これらの2021年度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 2021」を参照いただきたい。

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。

2022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、2021年9月に発足したデジタル庁、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、デジタル庁、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。

2021年度のCRYPTRECにおいては、暗号技術評価委員会では、暗号技術（署名）であるEdDSAのCRYPTREC暗号リスト（推奨候補暗号リスト）への追加を検討するため、2020年度の安全性評価に引き続き実装性能評価を行った。また、同委員会の下に暗号技術調査WG（耐量子計算機暗号）及び暗号技術調査WG（高機能暗号）を設置して、それぞれ耐量子計算機暗号及び高機能暗号に関するガイドラインを作成するための執筆方針を決定した。また、軽量暗号に関するガイドラインの作成については、2016年度版の軽量暗号ガイドラインを更新するための基となる調査報告を行い、今後の作成方針を決定した。また、暗号技術調査WG（耐量子計算機暗号）では、「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」の予測図を更新した。暗号技術活用委員会では、CRYPTREC暗号リストの改定に向けた利用実績に関する選定基準の検討、「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」の作成を行った。また、同委員会の下に設置された暗号鍵管理ガイダンスWGにおいて、「暗号鍵管理ガイダンス」の作成方針を決定した。

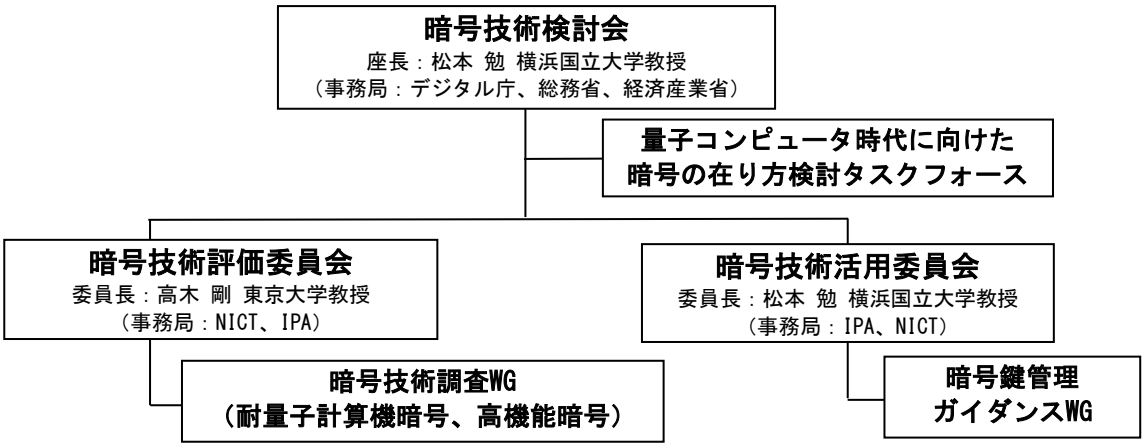

図2.2-1　2021年度CRYPTREC体制図

２．３．暗号技術検討会の開催実績

2021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、暗号技術検討会2021年度報告書に係る承認等を行うために開催した。

【第 1 回】2022年3月30日（火）14:00～16:00
（主な議題）
- 暗号技術検討会　開催要綱の改定について
- 2021年度暗号技術評価委員会 活動報告について
- 2021年度暗号技術活用委員会 活動報告について
- 利用実績による選定基準について
- 暗号強度要件に関する設定基準について
- 暗号鍵設定ガイダンスについて
- CRYPTREC暗号リストの改定について
- 暗号技術検討会 2021年度 報告書（案）について

（概要）
- 暗号技術検討会　開催要綱の改定について事務局より説明が行った。
- 2021年度暗号技術評価委員会について事務局より活動報告を行った。
- 2021年度暗号技術活用委員会について事務局より活動報告を行った。
- 暗号強度要件に関する設定基準について事務局より説明が行われ、原案のとおり承認された。
- 暗号強度要件に関する設定基準について事務局より説明が行われ、原案のとおり承認された。
- 暗号鍵設定ガイダンスについて事務局より説明が行われ、原案のとおり承認された。
- CRYPTREC暗号リストの改定について事務局より説明が行われ、原案のとおり承認された。
- 暗号技術検討会 2021年度 報告書（案）について事務局より説明が行われ、議論結果を追記することとした上で承認された。

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
- 暗号技術の電子政府推奨暗号リストからの降格
- 暗号技術に関する注意喚起レポートのCRYPTRECホームページへの公表
- 推奨候補暗号リストへの新規暗号（事務局選出）の追加
- 新世代暗号に係る調査

また、次期CRYPTREC暗号リストとは別文書として、耐量子計算機暗号、高機能暗号、及び、軽量暗号に関するガイドラインを作成する。基本方針は以下のとおりである。

- 耐量子計算機暗号に関するガイドラインを作成するため、2021年度に、耐量子計算機暗号に関するワーキンググループを設置する。2022年度中に当該ガイドラインを作成する。
- 高機能暗号に関するガイドラインを作成するため、2021年度に、高機能暗号に関するワーキンググループを設置する。2022年度中に当該ガイドラインを作成する。
- 軽量暗号に関するガイドラインについては、2016年度に作成した「CRYPTREC暗号技術ガイドライン（軽量暗号)」の更新のため、2021年度は、掲載されている暗号方式に関わる安全性解析について、2017年度以降の技術動向調査を行う。2023年度中を目途に現ガイドラインを更新する。

これらの課題について2021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．暗号技術の安全性及び実装に係る監視及び評価

学会等での情報収集に基づくCRYPTREC暗号等の監視活動を行った。監視報告の詳細については、CRYPTREC Report 2021（暗号技術評価委員会報告）に掲載する。

３．１．３．推奨候補暗号リストへの新規暗号（事務局選出）の追加に向けた検討

ディジタル署名EdDSAは、RFC8032[1]で規定され、TLS1.3で採用された（RFC 8446[2]）署名アルゴリズムである。さらに、TLS1.2のようなTLS1.3 より前のバージョンでは、ECDSAと同じ暗号スイートを使ってEdDSAも利用可能となった（RFC8422[3]）。

[1] RFC8032, “Edwards-Curve Digital Signature Algorithm (EdDSA) ”, Jan. 2017
[2] RFC8446, “The Transport Layer Security (TLS) Protocol Version 1.3”, Aug. 2018
[3] RFC8422, “Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier”, Aug. 2018

ディジタル署名 EdDSA の安全性評価について、2020年度に評価を行い、EdDSAの曲線および方式の構成いずれについても安全性に問題は見つからなかったことから、「国際標準化等の実績がある」ことを根拠とした事務局で選出する暗号アルゴリズムの候補として、CRYPTREC暗号リストへの追加を視野に入れて評価を行うことが承認された。

2021年度は、EdDSA の実装性能評価を行い、十分な実装性能があることを確認し、2020年度に実施した安全性評価および今年度実施した実装性能評価の結果に基づき、EdDSA はディジタル署名として十分な安全性及び実装性能を有していると判断したので、CRYPTREC暗号リストの推奨候補暗号リストへ追加することを提案した。

３．１．４．暗号技術調査ワーキンググループ（耐量子計算機暗号）

大規模な量子コンピュータが実用化されても安全性を保てると期待される暗号（耐量子計算機暗号:PQC）の研究開発及び標準化などが各国で進められている。そこで、2021年度、暗号技術評価委員会では、耐量子計算機暗号に関するガイドライン（以下「耐量子計算機ガイドライン」という）を作成するためにワーキンググループを設置することが承認されていたことから、「新技術等に関する調査及び評価」の活動として暗号技術調査ワーキンググループ（耐量子計算機暗号）（以下「耐量子計算機暗号WG」という）を設置した。以下が主な検討項目である。

- 耐量子計算機暗号の研究動向調査をもとに、主要な耐量子計算機暗号についてのガイドラインを2021年度から2022年度にかけて作成する。
- 「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」の予測図の更新する。

それらの成果（３．１．４．１～３．１．４．２節）は2021年度第2回暗号技術評価委員会にて報告され、了承された。

３．１．４．１．耐量子計算機暗号に関するガイドラインの作成方針

ガイドライン及び調査報告書の作成

耐量子計算機暗号ガイドラインは、暗号理論に精通していない利用者を対象とし、耐量子計算機暗号に関する調査報告書は、暗号理論の研究者や技術者を対象とし、基本的には耐量子計算機暗号ガイドラインは調査報告書から技術的詳細を省き、その一部を抜粋したものする。ただし、暗号理論に精通していない利用者のために、耐量子計算機暗号の活用方法を耐量子計算機暗号ガイドラインでは記載し、調査報告書には記載しない。

ガイドライン及び調査報告書に記載する暗号方式の選定基準及び候補について

主要な公開鍵暗号方式（NIST PQC標準化への提案方式等）を記載するが、対象となる暗号方式は執筆担当委員が選定する。

記載すべき項目及び章立て

i. 導入
ii. PQC の活用方法（ガイドラインにのみ記載）
iii. 格子に基づく暗号技術
iv. 符号に基づく暗号技術
v. 多変数多項式に基づく暗号技術
vi. 同種写像に基づく暗号技術
vii. ハッシュ関数に基づく署名技術

- iii 章以降の構成（A 章の場合）

A.1. 安全性の根拠となる問題の説明（例：LWE問題、シンドローム復号問題）
A.2. 代表的な暗号方式の構成法（例：Regev暗号、McEliece暗号）
A.3. 主要な暗号方式
A.3.1. 暗号方式1（例：CRYSTALS-KYBER, Classic McEliece）
A.3.2. 暗号方式2
A.3.3. 暗号方式3
・・・
A.4. まとめ

３．１．４．２．「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」の予測図の更新

「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」の予測図（以下単に「予測図」という。）は公開鍵暗号方式のセキュリティパラメータの選択について検討を行うため、2006年度に設置された暗号技術調査WG（公開鍵暗号）において作成された。当時、米国NISTは「NIST SP 800-57 Part 1 (Revised)(May,2006)」において暗号技術の鍵サイズに関して「80ビットセキュリティの利用期限を2010年まで」と推奨していた。現在では「NIST SP 800-57 Part 1 (Revision 5)(May,2020)」において「112ビットセキュリティの利用期限を2030年まで」と推奨している。

これらの状況を踏まえて、2019年度暗号技術評価委員会において、今後の予測図の取扱いについて審議し、下記のとおりの対応方針を決定していた。

今後の予測図の取扱いについて

これまでの暗号の鍵長の推奨値は、いわゆるムーアの法則（集積回路上のトランジスタ数が18ヶ月毎に2倍になる）を主な根拠として設定されてきた。ところが、近年、計算機の性能向上は以前と比べて鈍化してきている。今後の予測図のあり方に対して、下記のとおり、対応方針を決定した。

対応方針
〈今後の予測図の取扱い〉
(1) 予測図を従来通り、いわゆるムーアの法則を仮定して外挿線を年度末から20年後まで直線で引

き[4]、評価に大きな変動がないと考えられる限りにおいては、安全サイドに倒した評価として当面の間更新していく。なお、予測図は各国・国際標準化機関等により示されている主要な暗号技術の安全性基準と比較すると、より現状に則した評価であり、危殆化時期がそれらよりも先に延びるものとなっている。

〈今後の公開鍵暗号のパラメータ選択〉

(2) 公開鍵暗号のパラメータ選択に関する対応方針については、安全性以外にも相互接続性など、運用上の観点もあるため、今後は、暗号技術評価委員会だけではなく、暗号技術検討会、暗号技術活用委員会や関係各所などを含めて検討する。

予測図の更新について

素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関する計算量評価に大幅な進展はなかったため、TOP500.orgにおける2021年6月・11月のベンチマーク結果を追加して予測図の更新を行った（図3.2-1及び図3.2-2）。

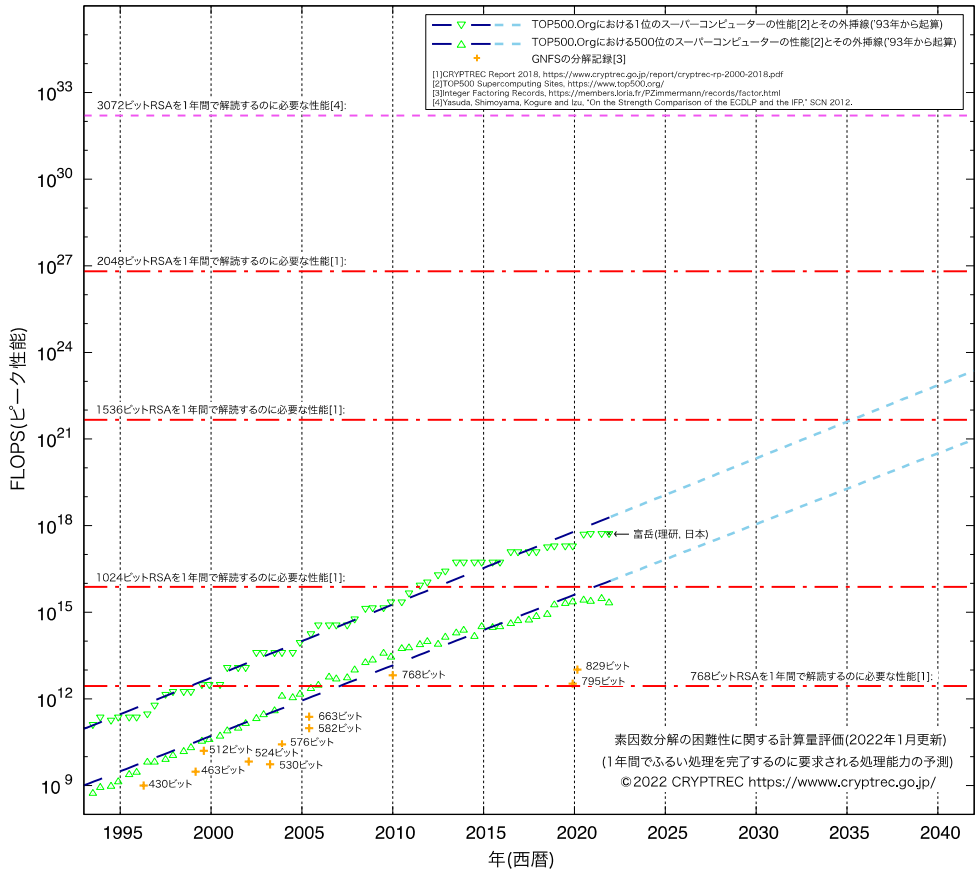

図3.2-1：素因数分解の困難性に関する計算量評価（2022年1月更新）[5]

[4] 2020年度暗号技術評価委員会にて、直線の外挿範囲を「年度末から20年後」と変更した。

[5] スーパーコンピューターの性能の伸びに関する外挿線は僅かであるが鈍化してきている。

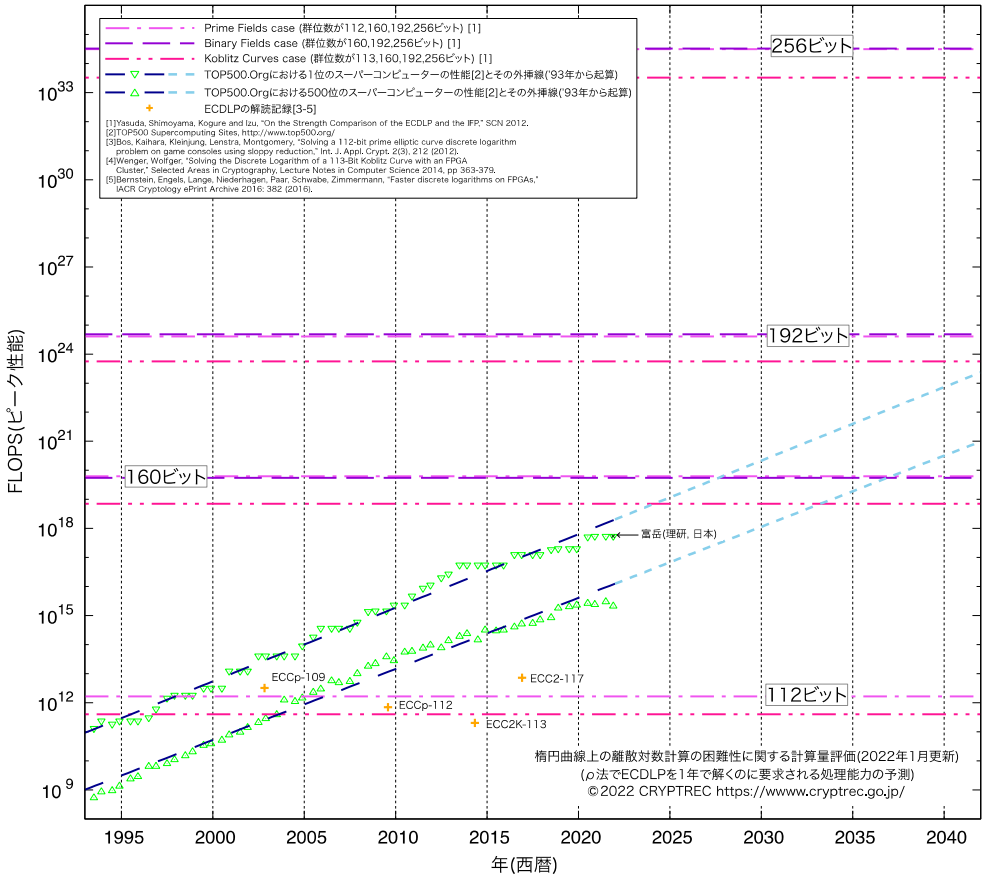

図3.2-2：楕円曲線上の離散対数計算の困難性に関する計算量評価（2022年1月更新）[6]

[6] スーパーコンピューターの性能の伸びに関する外挿線は僅かであるが鈍化してきている。

３．１．５．暗号技術調査ワーキンググループ（高機能暗号）

公開鍵暗号は、アプリケーションが多様となりその活用が広まっている。その中で、従来の公開鍵暗号よりも機能が向上した高機能暗号を利用してアプリケーションに適用することが有効と考えられている。そこで、2020年度第2回暗号技術検討会において高機能暗号ガイドラインを作成するために暗号技術調査ワーキンググループ（高機能暗号）（以下「高機能暗号WG」という）を設置することが承認された。

そして、2021年度暗号技術評価委員会において、2021年度の高機能暗号WGの活動として下記3点について実施する活動計画が承認された。

- 高機能暗号のスコープの明確化
- 高機能暗号技術に関する現状調査
- 高機能暗号のアプリケーションに関する調査

高機能暗号WGでは、上記3点について実施した。それらの成果（３．１．５．１～３．１．５．３節）は2021年度第2回暗号技術評価委員会にて報告され、了承された。

３．１．５．１．高機能暗号のスコープの明確化

「高機能暗号」に対して一般的に合意されている定義がない。そこで、高機能暗号に関するガイドライン（以下「本ガイドライン」という）で記載する高機能暗号が何を指すものか定義する必要がある。このため、本ガイドラインで扱う高機能暗号のスコープを議論した。

そして、本ガイドラインでは、高機能暗号を「従来の暗号技術に対して、機能が追加・向上されるなどの優位性を主張する暗号、および、従来の暗号技術では困難であった事象を解決できるなどの新規機能を有することを主張する暗号技術」とした。ただし、今後の議論により修正が必要な場合は、高機能暗号WGにおいて議論し、修正することとした。

３．１．５．２．高機能暗号技術に関する調査

高機能暗号に関する現在の活用事例、標準化動向、アルゴリズムを調査し、現状を情報共有するとともに、将来的に利用される可能性がある高機能暗号を精査する。

この調査のため、第1回高機能暗号WGにおいて、本ガイドラインに掲載する可能性がある高機能暗号を列挙するとともに、高機能暗号を

- 守秘
- 認証・署名
- その他

に分類した。そして、調査すべき高機能暗号の対象を

- 守秘
  - IDベース暗号、属性ベース暗号、放送型暗号、しきい値暗号、準同型暗号、プロキシ再暗号化
- 認証・署名
  - IDベース署名、属性ベース署名、集約署名・MAC・マルチ署名、グループ署名、リング

署名、しきい値署名

- その他
  - マルチパーティ計算－秘密分散ベース、マルチパーティ計算－Garbled Circuitベース、ゼロ知識証明、検索可能暗号、Private Information Retrieval、Oblivious RA

の１８項目とし、それぞれに対し、“技術”、“活用事例”、“標準化”についてＷＧ委員が分担し調査した。

３．１．５．３．高機能暗号のアプリケーションに関する調査

既存技術より効率的になる分野、既存技術でカバーできていない分野などで、高機能暗号の活用が期待される分野を整理する。この活動の一環として、より深くアプリケーション、応用例を知るためにエンドユーザのヒアリングを検討する。そして、審議により、以下の4件の候補を決定した。

① 秘密分散を利用した医療データ活用
② 検索可能暗号＆属性ベース暗号
③ 属性ベース暗号を利用した放送サービスの拡張
④ マルチパーティ計算を利用した秘密情報秘匿したデータ分析

このうち、2件を選び、2022年度にヒアリングを行うこととした。ヒアリングは、2022年度の第1回、第2回高機能暗号WGにおいて、発表、質疑形式で行う予定である。

このヒアリング内容は、本ガイドラインの応用事例に掲載することとするが、ヒアリング先である企業、団体、個人の宣伝とはならないように、できるだけ、企業、団体、個人名などを削除できるようにし、ヒアリング先に了解を得ることとした。

３．１．５．４．高機能暗号に関するガイドラインの作成方針

ガイドラインの作成

高機能暗号ガイドラインは、高機能暗号を導入することを考えられている技術開発者や、コンソーシアム・標準化団体に関与する技術者などを読者として想定し、暗号理論に精通していない方々を対象として執筆する。

ガイドラインに記載する暗号方式の選定基準及び候補について

主要な高機能暗号方式として、対象となる暗号方式は執筆担当委員が選定する。

ガイドラインの章立て

2021年度の調査項目を本ガイドラインの目次とし、2022年度に執筆を行う。

１．　はじめに
２．　高機能暗号技術とその活用法
　２．１　高機能暗号とは
　２．２　高機能暗号の種類と分類
　２．３　高機能暗号はどこに使えるか、その有用性
　２．４　高機能暗号の活用事例と標準化動向

２．４．１　守秘関連の暗号技術の活用事例と標準化動向
２．４．２　認証・署名関連の技術の活用事例と標準化動向
２．４．３　その他の技術の活用事例と標準化動向
参考文献
３．　主な高機能暗号技術のアルゴリズム・プロトコルとその性能
３．１　守秘関連の高機能暗号技術
３．１．１　IDベース暗号
３．１．２　属性ベース暗号
３．１．３　放送型暗号
３．１．４　準同型暗号
３．１．５　プロキシ再暗号化
参考文献
３．２　認証・署名を目的とした高機能暗号技術
３．２．１　属性ベース署名
３．２．２　集約署名、集約MAC、マルチ署名
３．２．３　グループ署名
３．２．４　リング署名
３．２．５　閾値署名
参考文献
３．３　その他の高機能暗号技術
３．３．１　マルチパーティ計算－秘密分散ベース
３．３．２　マルチパーティ計算－Garbled Circuitベース－
３．３．３　ゼロ知識証明
３．３．４　検索可能暗号
３．３．５　Private Information Retrieval (PIR)
３．３．６　Oblivious RAM (ORAM)
参考文献
４．おわりに

３．１．６．軽量暗号に関するガイドラインの作成に関する活動

2020年度第2回暗号技術検討会にて、2016年度に作成した「CRYPTREC暗号技術ガイドライン（軽量暗号）」（以下、2016年度版ガイドラインと呼ぶ）の更新のため、2021年度は、掲載されている暗号方式に関わる安全性解析について、2017年度以降の技術動向調査を行い、2023年度中を目途に現ガイドラインを更新することが承認された。

2016年度版ガイドラインに掲載されている暗号方式に関わる安全性解析について、2017年度以降の技術動向調査を行った。また、現ガイドラインの更新方針を決定した。

３．１．６．１．軽量暗号に関する技術動向調査

2021年9月の時点で脅威に繋がる脆弱性が指摘されているか否かについて調査を実施した。調査報告書は、技術調査報告書として CRYPTREC ホームページに公開する。

調査概要は下記の通り。

- 調査対象
  - 2017 年 3 月に公開した「CRYPTREC 暗号技術ガイドライン（軽量暗号)」に掲載されている方式について、2017 年 3 月以降に大幅な安全性の劣化につながる脆弱性が見つかっているか否かについて調査。
  - 軽量暗号に関わる ISO/IEC 29192 シリーズに近年採録されたもしくは採録される予定の方式について、「CRYPTREC 暗号技術ガイドライン（軽量暗号)」における掲載の有無およびそれらの安全性について調査。
  - 「CRYPTREC 暗号技術ガイドライン（軽量暗号)」公開時に CAESAR プロジェクトが終了していなかったことから、CAESAR プロジェクトで最終的に選ばれたポートフォーリオ 6 方式について、「CRYPTREC 暗号技術ガイドライン（軽量暗号)」における掲載の有無およびそれらの安全性について調査。
- 実施方法
  - 事務局により調査を行い、調査報告書を執筆し、外部有識者による調査報告書のレビューを実施した。
- 調査結果概要

  各方式の安全性解析状況について、次のとおり表にまとめた。

	分類１	分類２	分類３
ブロック暗号	CLEFIA、LED、Simon、Speck、LEA	Piccolo、Midori、PRESENT、PRINCE、TWINE	
ストリーム暗号	ChaCha、Enocoro、Trivium		Grain v1、MICKEY 2.0
ハッシュ関数	Keccak 、 PHOTON 、 QUARK 、SPONGENT、Lesamnta-LW		
MAC	SipHash、Tsudik’s keymode	Chaskey、LightMAC	
認証暗号	ACORN、ASCON、AES-OTR、CLOC and SILC、Deoxys、Joltik、Ketje、Minalpher、OCB1、OCB3、PRIMATEs、AEGIS、$COLM_{127}$	$COLM_0$	OCB2 、 AES-JAMBU 、Grain-128A

分類１：仕様段数において安全性を脅かす攻撃が存在しない方式

- ✧ 秘密鍵の全数探索よりも効率的に実行可能な攻撃が存在しない方式
- ✧ 安全性基準を脅かす攻撃が存在しない方式

分類２：特定の場合を除き、仕様段数において安全性を脅かす攻撃が存在しない方式

- ✧ 秘密鍵の全数探索よりも効率的に実行可能な攻撃が存在しない方式

分類３：仕様段数において安全性基準を満たさない方式

- ✧ 秘密鍵の全数探索よりも効率的に実行可能な攻撃が存在する方式
- ✧ 安全性基準を脅かす攻撃が存在する方式

３．１．６．２．軽量暗号ガイドライン更新方針

下記の通り更新を行うことを決定した。

- ➢ 更新形態

  2016 年度版ガイドラインに新規情報を追加・更新した文書を 2023 年度版ガイドラインとして公開する。

  - ・ 主たる追加は、2016 年度版ガイドラインの 4 章「代表的な軽量暗号」に相当する軽量暗号方式の紹介とする。
  - ・ 既に 4 章に掲載されている方式については、今年度実施した軽量暗号に関する技術動向調査(３．１．６．１参照)を基に更新する。
  - ・ 1 章～3 章は、2016 年度版ガイドラインをそのまま用いる。ただし、4 章に新規追加・更新する方式に関わる情報は、適切な章に節を追加し、掲載する。
  - ・ 付録を追加し、関連情報を掲載する。
- ➢ タイトル
  - ・ 「CRYPTREC 暗号技術ガイドライン（軽量暗号)」2023 年度版
- ➢ 追加情報の対象
  - ・ NIST Lightweight コンペティション最終選考で採択された方式
  - ・ 軽量な方式として ISO に近年採録されたもしくは採録される予定の方式
- ➢ 主な追加内容
  - ・ 1 章　はじめに
    - ✓ 追記箇所を説明する文章を追加する。
  - ・ 2 章 軽量暗号とその活用法
    - ✓ 節を追加し、2017 年以降の標準化動向を掲載する。
  - ・ 3 章 軽量暗号の性能比較
    - ✓ 節を追加し、 ″追加情報の対象″ の方式に関する安全性や実装性能に関わる評価・調査結果（2022 年度外部評価により実施予定）を掲載する。
  - ・ 4 章 代表的な軽量暗号
    - ✓ 2016 年度版ガイドライン掲載暗号について、今年度実施した軽量暗号に関わる調査報告書（３．１．６．１参照)を基に追記・更新する。
    - ✓ ″追加情報の対象″の方式について、掲載方式と同等の情報を掲載する。(2022 年度外部評価の実施結果を反映する)
  - ・ 付録(新規)
    - ✓ NIST Lightweight コンペティションファイナリスト(最終選考で採択されなかった方式)
    - ✓ CAESAR のスケジュールが後ろ倒しにずれ込み、最終選考が完結する前に 2016 年度版ガイドラインを公開することとなった。後に、CAESAR プロジェクトの最

終選考により、3 ケース各 2 方式(計 6 方式) が選ばれた。Use case 1: Lightweight applications について選ばれた 2 方式はすでに掲載していたが、Use case 2: High-performance applications および Use case 3: Defense in depth については、2 方式中 1 方式は掲載しているが、各 1 方式は掲載していない。ここで、未掲載の 2 方式を紹介する。

- 編集方法
  - 事務局で取りまとめ・編集を行い、更新版を作成し、暗号技術評価委員会にて審議いただく。
- 今後のスケジュール
  - 2022年：
    NIST Lightweight コンペティションファイナリストを対象とした安全性および実装性能に関わる調査・評価
  - 2023年：

事務局によりガイドラインの更新案を編集し、ドラフト版について外部有識者にガイドラインとして、掲載内容の適切性や情報の過不足などについてレビュー頂き、完成版を暗号技術評価委員会にて審議する

３．１．７．暗号技術評価委員会の開催実績

2021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3.2-5のとおりである。

表3.2-5　暗号技術評価委員会の開催状況

回	開催日	議案
第1回	2021年7月6日	■ 暗号技術評価委員会活動計画の具体的な進め方についての審議 ■ 外部評価（ディジタル署名EdDSAの実装性能に関する調査）実施についての審議 ■ 暗号技術調査ワーキンググループ（耐量子計算機暗号）の活動計画案の審議 ■ 暗号技術調査ワーキンググループ（高機能暗号）の活動計画案の審議 ■ 軽量暗号に関するガイドライン係る技術動向調査及び更新方針案の審議
第2回	2022月2月22日	■ 暗号技術評価委員会活動報告（案）についての審議 ■ ディジタル署名EdDSAの実装性能に関する調査結果の報告と暗号技術評価委員会としての見解について審議 ■ 暗号技術調査ワーキンググループ（耐量子計算機暗号）の活動内容の報告

		■ 暗号技術調査ワーキンググループ（高機能暗号）の活動内容の報告 ■ 軽量暗号ガイドラインに係る技術動向調査結果の報告及び更新方針の決定

３．２．暗号技術活用委員会

３．２．１．活動の概要

2021年度の活動概要は以下の通りである。詳細については、CRYPTREC Report 2021暗号技術活用委員会報告[7]を参照されたい。

(1) 利用実績に関する選定基準の検討

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[8]。
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・策定する。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《(従来仮称）鍵長設定要件》」及び「暗号鍵設定ガイダンス《(従来仮称）鍵長設定ガイダンス（一般用)》」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つの鍵長に関するドキュメントを作成する。
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《(従来仮称）鍵長設定要件》」である。これは、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・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ための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。
もう一つは、「暗号鍵設定ガイダンス《(従来仮称）鍵長設定ガイダンス（一般用)》」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) 暗号鍵管理プロファイルの作成ガイダンスの作成

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「暗号鍵管理プロファイルの作成ガイダンス（仮称)」を作成する。
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う。なお、ガイダンス文書の完成時期は2022年度を予定する。

---

[7] CRYPTREC Report 2021 暗号技術活用委員会報告, https://www.cryptrec.go.jp/promo_cmte.html
[8] CRYPTREC, 暗号技術検討会２０２０年度報告書, https://www.cryptrec.go.jp/adv_board.html

３．２．２．2021年度の活動内容

３．２．２．１．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。

2021年度の活用委員会では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。

- 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（＝関係者外秘）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3.2-1 利用実績による選定基準（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

３．２．２．２．「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年度の活用委員会では表3.2-2の通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[9]を参照されたい。

表3.2-2 「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）

[9] 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.html

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

設定基準の位置づけ

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3.2-1に示す。

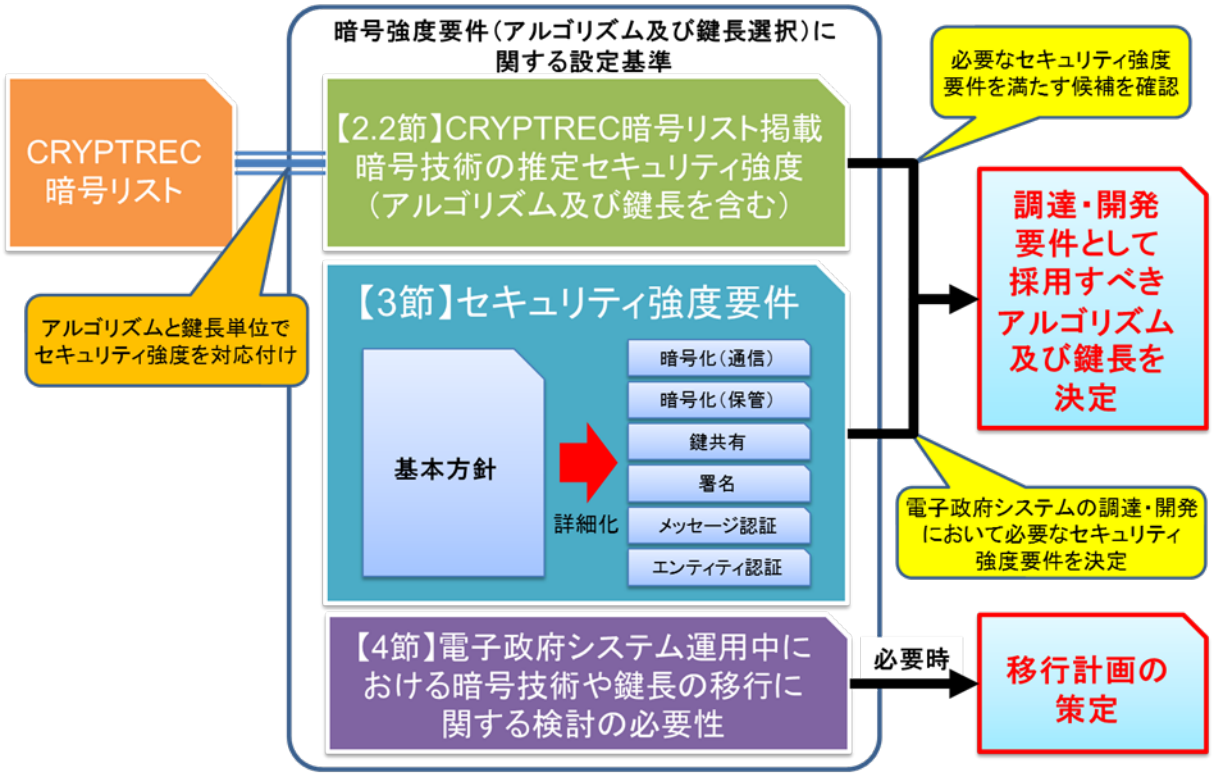

図3.2-1 「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の位置づけ

セキュリティ強度要件の基本設定方針概要

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。

必要なセキュリティ強度要件は表3.2-3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。

表3.2-3 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

なお、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。

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。
- 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。

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

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

３．２．２．３．「暗号鍵設定ガイダンス」の作成

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3.2-4の通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。

詳細は、暗号鍵設定ガイダンス[10]を参照されたい。

[10] CRYPTREC, 暗号鍵設定ガイダンス, https://www.cryptrec.go.jp/op_guidelines.html

表3.2-4 「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

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。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。

- 暗号鍵の鍵長
- 暗号鍵の鍵タイプ
- 暗号鍵のライフサイクル
- 運用中における鍵長移行に関する検討の必要性

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。

３．２．２．４．暗号鍵管理の参照プロファイルの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）」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。

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。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。

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。
- 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。

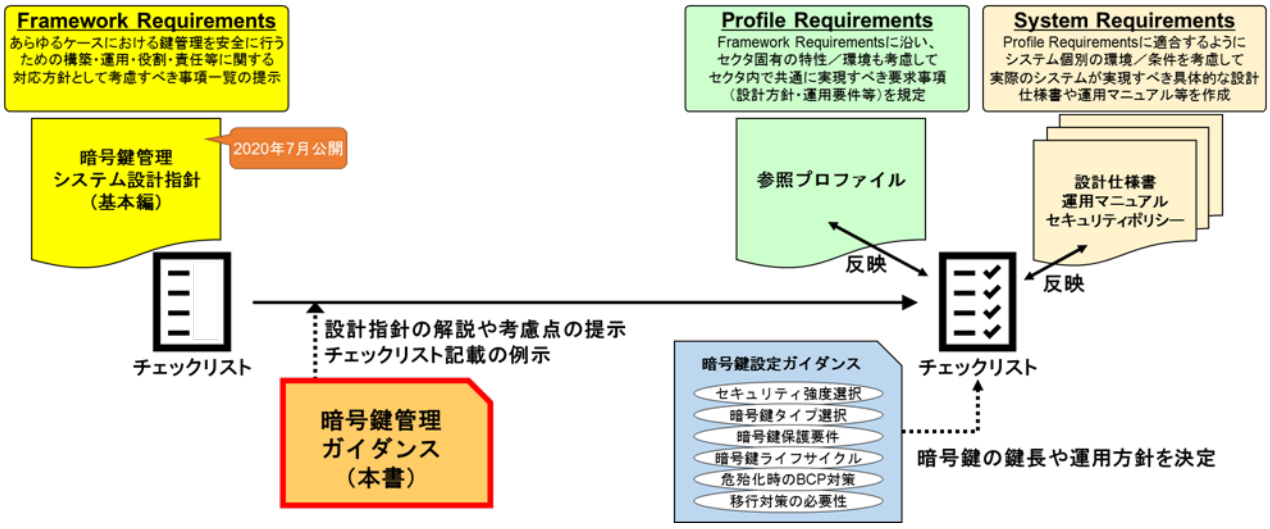

図3.2-2 「暗号鍵管理ガイダンス」作成の位置づけ

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

【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3.2-4 「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

３．２．３．暗号技術活用委員会の開催状況

2021年度の暗号技術活用委員会での審議概要は表3.2-5の通りである。

表3.2-5　暗号技術活用委員会の開催状況

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

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。2022年度にはCRYPTREC暗号リストの10年に一度の全面改定を予定しており、その改定に向けた検討を進めていく。

暗号技術評価委員会においては、CRYPTREC暗号リストの全面改定に向け、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、引き続き、耐量子計算機暗号、軽量暗号及び高機能暗号に関するガイドラインの作成に向けた検討を行う。暗号技術活用委員会においては、CRYPTREC暗号リストの全面改定に向け、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。

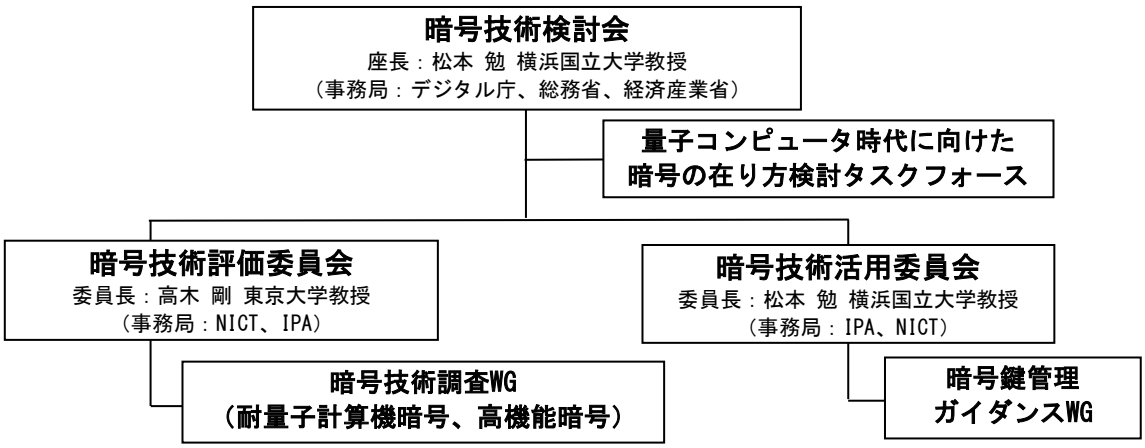

図4-1 2022年度CRYPTRECの体制図（予定）