暗号技術検討会
２０２２年度　報告書

２０２３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。

2022年度の各委員会の活動として、暗号技術評価委員会では、同委員会の下に設置された暗号技術調査WG（耐量子計算機暗号）及び暗号技術調査WG（高機能暗号）において、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案を作成した。また、軽量暗号ガイドラインについては、ガイドライン更新のための基となる調査のため、軽量暗号技術に対する安全性評価及び実装性能評価を実施し、標準化動向についても併せて調査した。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評価、暗号利活用のために作成すべきガイダンス候補の検討を行った。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」の構成を見直しつつ、2022年度版の作成を行った。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2022年度開催しなかった。これらの2022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 2022」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。

2023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月に改定が行われ、CRYPTREC暗号リストとして発表され、2023年4月に再改定を行っている。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。

2022年度のCRYPTRECにおいては、暗号技術評価委員会では、同委員会の下に設置された暗号技術調査WG（耐量子計算機暗号）及び暗号技術調査WG（高機能暗号）において、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案を作成した。また、軽量暗号ガイドラインについては、ガイドライン更新のための基となる調査のため、NIST Lightweight Cryptography Projectのファイナリストを対象とした安全性評価及び実装性能評価を実施した。なお、安全性評価に関しては、ISO/IEC標準規格として29192シリーズで規格化された軽量メッセージ認証コードの1つであるTsudik's keymodeも追加対象とした。また、標準化動向についても併せて調査した。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評価、暗号利活用のために作成すべきガイダンス候補の検討を行った。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」の構成を見直しつつ、2022年度版の作成を行った。

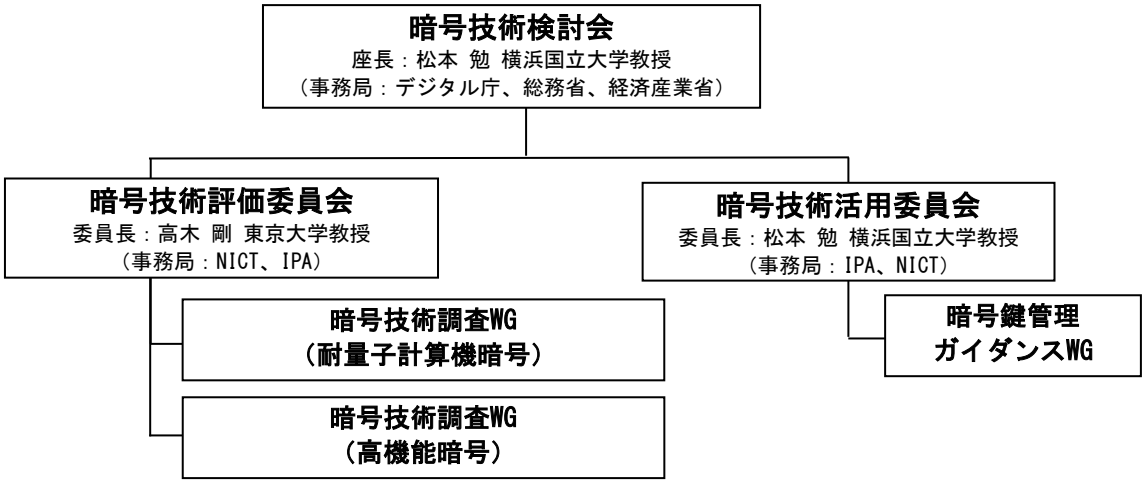

図2.2-1　2022年度CRYPTREC体制図

２．３．暗号技術検討会の開催実績

2022年度の暗号技術検討会は、CRYPTREC 暗号リストの改定案に係る承認等を行うために第1回を開催し、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並びに意見募集を経たCRYPTREC暗号リストの改定案及び暗号技術検討会2022年度報告書に係る承認等を行うために第2回を開催した。

【第 1 回】2023年2月27日（月）～2023年3月8日（水）（書類審議）
（主な議題）
・公募提案暗号の自主取下げ要望に対する取り扱いルールの策定並びに「ECDSA、 ECDH 及び SC2000」の取扱いについて
・CRYPTREC 暗号リストの改定案について
・意見募集の実施方法及びその後の対応案について
（概要）
・CRYPTREC暗号リストの改定案について、原案のとおり承認された。
・意見募集の実施方法及びその後の対応案について、原案のとおり承認された。

【第 2 回】2023年3月30日（木）9:00～11:00
（主な議題）
・2022年度暗号技術評価委員会 活動報告について【報告】
・CRYPTREC暗号技術ガイドライン案（耐量子計算機暗号）及び CRYPTREC暗号技術ガイドライン案（高機能暗号）について【承認】
・2022年度暗号技術活用委員会 活動報告について【報告】
・暗号鍵管理ガイダンスについて【承認】
・CRYPTREC暗号リストの改定案に対する意見募集に寄せられたご意見に対するデジタル庁、総務省及び経済産業省の考え方案並びにCRYPTREC暗号リストの改定案について【承認】
・2023年度暗号技術評価委員会活動計画（案）について【承認】
・2023年度暗号技術活用委員会活動計画（案）について【承認】
・暗号技術検討会 2022年度 報告書（案）について【承認】
（概要）
・暗号技術評価委員会について事務局より2022年度の活動報告を行った。
・CRYPTREC暗号技術ガイドライン案（耐量子計算機暗号）及び CRYPTREC暗号技術ガイドライン案（高機能暗号）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。
・暗号技術活用委員会について事務局より2022年度の活動報告を行った。
・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暗号リストの改定案に対する意見募集に寄せられたご意見に対するデジタル庁、総務省及び経済産業省の考え方案並びにCRYPTREC暗号リストの改定案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。
・2023年度暗号技術評価委員会活動計画（案）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。

・2023年度暗号技術活用委員会活動計画（案）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 2022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に係る検討
- 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）の追加に係る検討
- 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案を作成する。基本方針は次のとおりである。

- 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、2021-2022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し、当該ガイドライン案を作成する。
- 高機能暗号に関するガイドラインを作成するため、2021-2022年度に、高機能暗号に関するワーキンググループを設置し、当該ガイドライン案を作成する。
- 軽量暗号に関するガイドラインについては、2016年度に作成された「CRYPTREC暗号技術ガイドライン（軽量暗号）」の更新のため、2022年度は、掲載されている暗号方式に関す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ための案を作成する。

これらの課題について2022年度に行った具体的な検討内容を、次のとおり報告する。

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 2022（暗号技術評価委員会報告）に掲載する。

３．１．３．自主取下げに係る電子メールによる審議と結果

ECDSA、ECDH及びSC2000の応募暗号について取下げの申請があったため、暗号技術評価委員会として次の対応を行った。

表2：取下げの申請に対する対応

	理由
ECDSA及びECDH	取扱いを応募暗号技術からCRYPTREC事務局が選出した暗号技術に変更し、現状通り電子政府推奨暗号リストに記載することは妥当であると判断す

	る。仕様書の参照先についても変更無しとする。
SC2000	応募社の判断を尊重し、取下げの申請を認める。推奨候補暗号リストから当該暗号技術を削除することは妥当であると判断する。

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、2020年度第2回暗号技術検討会において、耐量子計算機暗号ガイドラインの作成に向け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：PQC WG）を設置することが承認された。また、「素因数分解の困難性に関する計算量評価」及び「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」の予測図の更新を PQC WG で実施することが承認された。

そして、2021年度及び2022年度の2年間で耐量子計算機暗号ガイドライン案を作成した。

2021年度のPQC WGでは、ガイドライン案作成の準備として、耐量子計算機暗号に関する研究動向調査を行い、ガイドライン案執筆方針を次のように定めた。

- 耐量子計算機暗号のスコープ
  公開鍵暗号を中心にまとめる。
- 耐量子計算機暗号に関する現状調査
  ガイドライン案及び調査報告書に記載する耐量子計算機暗号を5分類とし、さらに耐量子計算機暗号の活用方法をガイドライン案のみに記載する。これらの項目に関する情報を調査した。
- ガイドライン案及び調査報告書の目次案
  - i. 導入
  - ii. PQC の活用方法（ガイドライン案のみに記載）
  - 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（例：LWE問題、シンドローム復号問題）
    A.2. 代表的な暗号方式（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

そして、2022年度暗号技術評価委員会において、2022年度のPQC WGの活動として次の2点を実施する活動計画が承認された。

- 耐量子計算機暗号ガイドライン案の執筆
- 「素因数分解の困難性に関する計算量評価」及び「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

これらの成果（３．１．４．１～３．１．４．２節）は2022年度第2回暗号技術評価委員会で報告され、了承された。

３．１．４．１．耐量子計算機暗号ガイドライン案の執筆方針

耐量子計算機暗号ガイドライン案及び調査報告書

耐量子計算機暗号ガイドライン案は、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案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案には記載し、調査報告書には記載しない。

耐量子計算機暗号ガイドライン案及び調査報告書に記載する暗号方式の選定基準

公開鍵暗号方式である主要な耐量子計算機暗号（NIST PQC標準化への提案方式等）を記載するが、対象とする暗号方式は PQC WG の承認を得たものとする。

ガイドライン案の章立て案

1　はじめに
　1.1　耐量子計算機暗号(PQC) の必要性について
　1.2　PQC の研究及び標準化等に関する動向
　1.3　本調査における代表的なPQC の5 種類の分類を調査対象として選択した理由
2　PQC の活用方法
　2.1　暗号の利用形態
　2.2　各利用形態における課題
　2.3　各利用形態における対策
3　格子に基づく暗号技術
　3.1　格子に基づく暗号技術の安全性の根拠となる問題
　3.2　代表的な格子に基づく暗号方式
　3.3　格子に基づく主要な暗号方式: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON
　3.4　格子に基づく暗号技術に関するまとめ
4　符号に基づく暗号技術

３．１．４．２．「素因数分解の困難性に関する計算量評価」及び「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」及び「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、「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ことができるように、2006年度に設置された暗号技術調査WG（公開鍵暗号）で作成された。2019年度の暗号技術評価委員会で、今後の予測図の取扱いについて審議し、対応方針（「今後の予測図の取扱い」及び「今後の公開鍵暗号のパラメータ選択」）を決定した。2022年度は、対応方針の説明文を一般の読者に一層読みやすくなるように、次のとおり修正した。

予測図の取扱いに係る対応方針

〈今後の予測図の取扱い〉

(1) いわゆるムーアの法則を仮定して外挿線を年度末からプラス20年後まで従来通り直線で引き、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予測図 ※を当面の間更新していく。

〈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、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。

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2022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）。

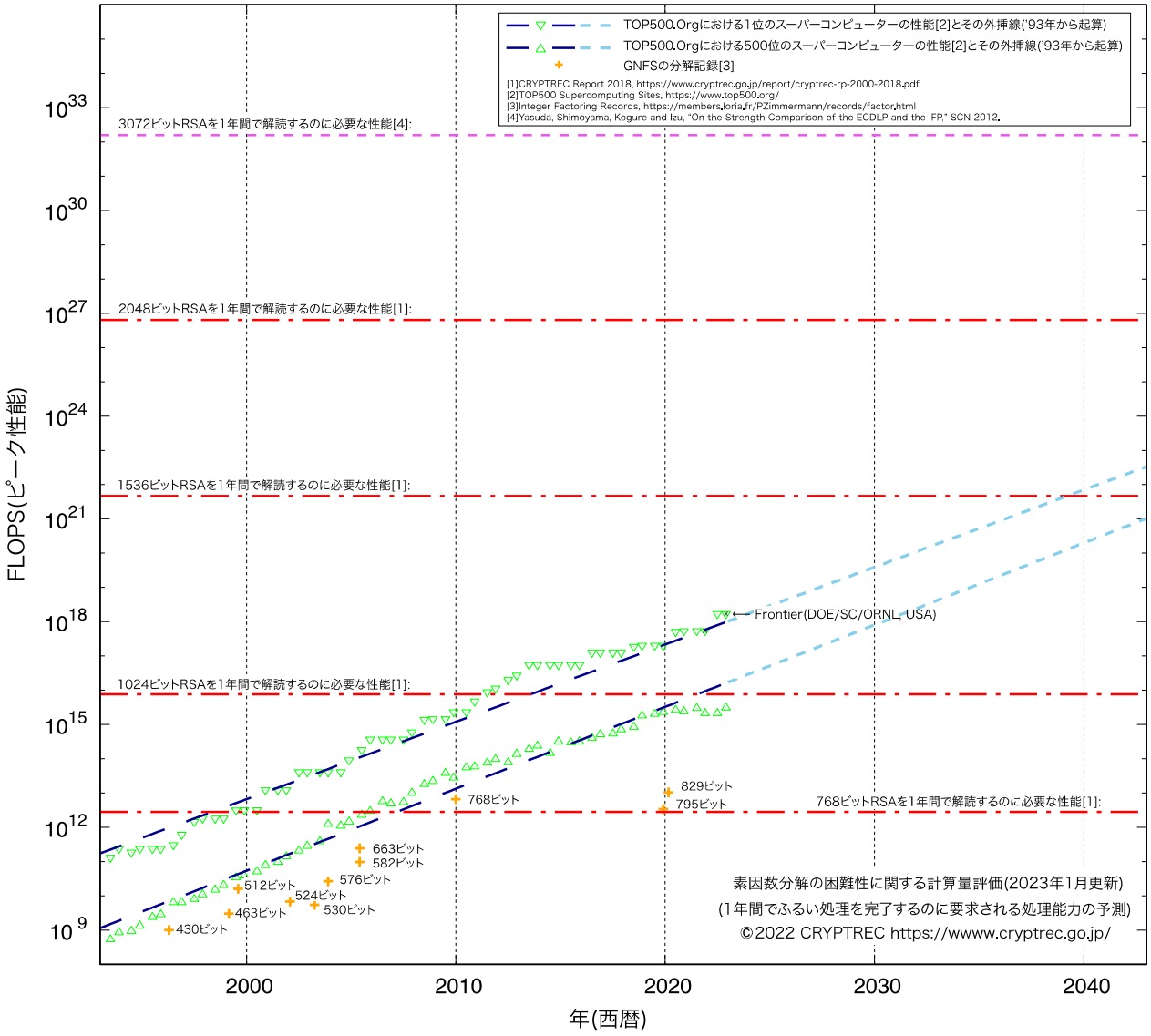

図3.2-1：素因数分解の困難性に関する計算量評価（2023年1月更新）[1]

[1] 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。

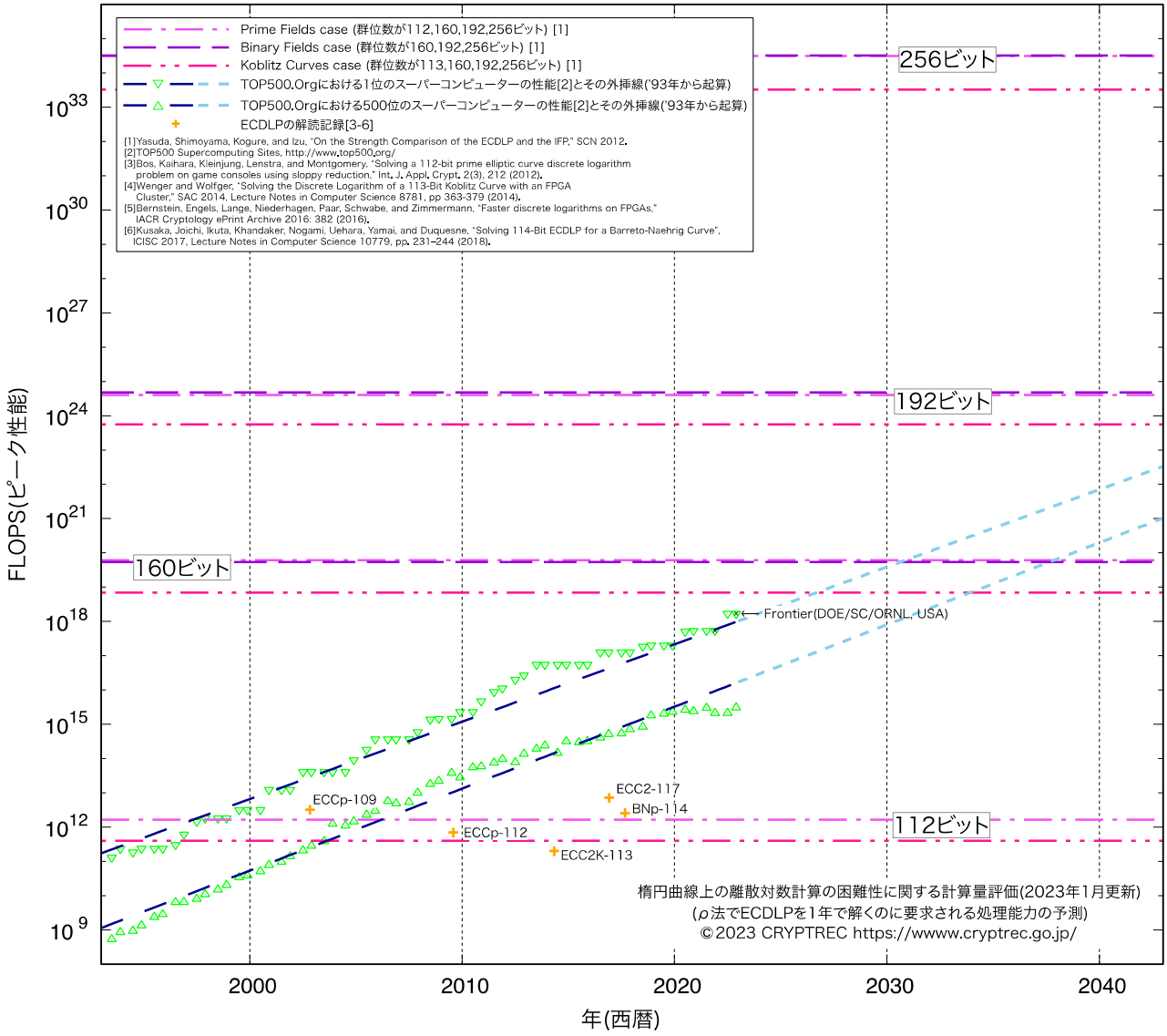

図3.2-2：楕円曲線上の離散対数計算の困難性に関する計算量評価（2023年1月更新）[2]

[2] 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回暗号技術検討会で、高機能暗号ガイドラインの作成に向けて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年度及び2022年度の2年間で高機能暗号ガイドライン案を作成した。

2021年度の高機能暗号WGでは、ガイドライン案作成の準備として、高機能暗号のスコープの明確化、技術に関する調査及びアプリケーションに関する調査を行い、ガイドライン案執筆方針を次のように定めた。

- 高機能暗号のスコープ
  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。
- 高機能暗号技術に関する現状調査
  ガイドライン案に記載する高機能暗号を 3 分類、17 項目とし、それぞれの項目について“技術”、“活用事例”及び“標準化”を調査した。
- 高機能暗号のアプリケーションに関する調査
  日本電気株式会社及び三菱電機株式会社に対して 2022 年度にヒアリングを実施することとし、日本電気株式会社にはプライバシ保護、三菱電機株式会社にはＤＢ関連のデータ保護のアプリケーション事例を紹介いただくこととした。

そして、2022年度暗号技術評価委員会において、2022年度の高機能暗号WGの活動として次の2点を実施する活動計画が承認された。

- 2021 年度に定めた目次案に沿ったガイドライン案の執筆
- 高機能暗号のアプリケーションに関するヒアリング調査及び調査内容のガイドライン案への反映

これらの成果（３．１．５．１～３．１．５．２節）は2022年度第2回暗号技術評価委員会で報告され、了承された。

３．１．５．１．2021年度に定めた目次案に沿ったガイドライン案の執筆

ガイドライン案の執筆

高機能暗号ガイドライン案は、高機能暗号の導入を考え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した。

ガイドライン案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を記載するが、対象とする暗号方式は暗号技術調査ワーキンググループ（高機能暗号）の承認を得たものとする。

ガイドライン案の章立て案

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

２．４．４　活用事例から見た高機能暗号の利用方法

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MAC、マルチMAC、集約署名、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　しきい値署名

参考文献

３．３　その他の高機能暗号技術

３．３．１　秘密分散

３．３．２　マルチパーティ計算－秘密分散ベース

３．３．３　マルチパーティ計算－Garbled Circuitベース－

３．３．４　ゼロ知識証明

３．３．５　Oblivious Random Access Machine (ORAM)

３．３．６　Private Information Retrieval (PIR)

３．３．７　検索可能暗号

参考文献

４．　おわりに

３．１．５．２．高機能暗号のアプリケーションに関するヒアリング調査及び調査内容のガイドライン案への反映

2021年度の高機能暗号WGにおいて、高機能暗号により既存技術よりも効率的になる分野、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した。この活動の一環で、より深くアプリケーションや応用例を把握するためにエンドユーザのヒアリングを検討し、2022年度第1回及び第2回の高機能暗号WGにおいて、次のヒアリングを実施した。

① 日本電気株式会社：秘密分散を利用した医療データ活用

② 三菱電機株式会社：検索可能暗号＆属性ベース暗号

ヒアリングは、発表及び質疑形式で実施した。

ヒアリング内容は、ガイドライン案の“２．４．４章活用事例から見た高機能暗号の利用方法”に掲載したが、ヒアリング先の企業、団体及び個人等の宣伝とならないように、可能な限り企業名、団体名及び個人名などを削除することとし、その旨ヒアリング先からも了解を得た。

３．１．６．「CRYPTREC暗号技術ガイドライン（軽量暗号）」更新に関する活動

３．１．６．１．背景

2019年度に設置された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において、「CRYPTRECにおいて、軽量暗号はCRYPTREC暗号リストには組み込まず、別途ガイドラインという形で取り扱う」方針が決定され、2020年度第2回暗号技術検討会において、2016年度に策定された「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」という。）を2023年度中目処で更新する方針が承認された。2021年度第2回暗号技術評価委員会において、その具体的な更新方針が承認された。

当該更新方針に従い、2022年度は、NIST軽量暗号プロジェクト（NIST Lightweight Cryptography Project ． 以下、「NIST LWC」という）のファイナリスト10方式（ASCON, Elephant, GIFT-COFB, Grain-128AEAD, ISAP, PHOTON-Beetle, Romulus, SPARKLE, TinyJAMBU, Xoodyak）を対象とした安全性評価及び実装性能評価を外部評価により実施した。なお、安全性評価に関しては、これら10方式に加え、ISO/IEC標準規格として 29192シリーズで規格化されている軽量メッセージ認証コードの1つであるTsudik's keymodeも対象とした。また、軽量暗号に係る NIST公開文書やISO/IECなどの標準化動向に関する調査を外部評価により実施した。

なお、2023年2月7日に、NIST LWC 最終選考結果が発表され、 ASCON が選定された。

３．１．６．２．実施概要

安全性評価、実装性能評価及び標準化動向調査について、外部評価により次のとおり実施した。

- 安全性評価：NIST LWCファイナリストに選定された10方式及びISO/IEC標準として規格化され

たTsudik's keymode の安全性に関する調査及び評価を実施した。

- 実装性能評価：NIST LWCファイナリストに選定された10方式の実装性能（ハードウェア及びソフトウェア）に関する調査及び評価を実施した。
- 標準化動向調査：軽量暗号を取り巻く標準化動向(CAESARプロジェクト、ISO/IECの軽量暗号関連カテゴリ及びNIST LWCなど)の調査を実施した。

３．１．６．３．調査結果概要

[安全性評価結果概要]

NIST LWCファイナリストに選定された10方式及びISO/IEC標準として規格化されたTsudik's keymodeの安全性評価について、2022年9月現在の調査結果概要は次のとおり。

安全性を脅かす攻撃が存在しない方式	特定の場合を除き、 安全性を脅かす方式が存在しない方式
ASCON, Elephant, GIFT-COFB, Grain-128AEAD, ISAP, PHOTON-Beetle, Romulus, SPARKLE, Xoodyak	TinyJAMBU, Tsudik's keymode

TinyJAMBUでは、関連鍵設定の場合に現実的な計算量での偽造攻撃が実行可能である。本攻撃が成立するような関連鍵の使用を避けることで、TinyJAMBUの安全性確保が可能であることを確認した。

Tsudik's keymodeでは、使用するハッシュ関数が伸長攻撃と呼ばれる攻撃を許す場合に偽造攻撃が実行可能になるという既知の脆弱性が存在する。伸長攻撃が実行不可能なハッシュ関数を使用することで、Tsudik's keymodeの安全性確保が可能であることを確認した。

[実装性能評価結果概要]

各方式の現時点での実装性能を確認した。

- ハードウェア実装：回路面積及びスループット性能に着目して評価した。例えば、Xilinx 社の Artix-7 上では、TinyJAMBU の回路面積が小さいこと、SPARKLE は比較的面積コストが大きくなることなどを確認した。
- ソフトウェア実装：レイテンシ、コードサイズ、RAMサイズなどに着目して評価した。例えば、低リソースプラットフォーム (Arm Cortex-M0)上では、Elephant が最もレイテンシが高く、TinyJAMBU、Xoodyak、ASCON、SPARKLE が低レイテンシであることが判明した。コートサイズは、ASCON が最も大きく、他の候補暗号方式には大きな差が見られなかった。RAM の使用量は、コンパイル時の静的なメモリサイズのレポートから、どのアルゴリズムも約1KByte程度であった。

[標準化動向調査結果概要]

CAESARプロジェクト、ISO/IECの軽量暗号関連カテゴリ及びNIST LWC などの状況を調査した。調査結果から、軽量暗号をとりまく現状を確認した。例えば、2016年度版ガイドラインに掲載されている SIMON と SPECKは、ISO/IECの軽量暗号カテゴリで議論されていたが、ISO/IEC標準の軽量暗号カテゴリでは規格化されず、自動認識・データキャプチャ技術の規格に対応する暗号方式カテゴリで規格化されていることを確認した。

また、評価指標に関して、安全性評価については、提案方式の設計根拠が十分に提示されない場合に、第3者による評価を十分に行えないと判断され、評価対象から外される事例などを確認した。実装性能評価については、従来は論文ごとに異なる環境や測定シナリオでの評価が示されることが多くあったが、近年は AES-GCM や SHA-256 など広く世界で利用されているアルゴリズムとの比較などにより、統一的な測定フレームワークを用いて評価することが一般化してきていることが明らかになった。

３．１．６．４．外部評価報告書に対する暗号技術評価委員会の見解

これらの外部評価報告書は、調査対象の暗号方式に対する安全性、実装性能及び標準化動向に係る調査として十分な内容を含んでいると考えられることから、これらの報告書をCRYPTREC の技術調査報告書とすることが了承された。

３．１．６．５．2023年度の計画

2021 年度第 2 回暗号技術評価委員会において承認された更新方針に従い、暗号技術評価委員会事務局でガイドライン更新案のドラフト版を執筆し、外部有識者にガイドラインとしての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いた後、2023 年度暗号技術評価委員会で更新案を審議する予定である。

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	2022年7月26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 ■ 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 ■ 外部評価（軽量暗号に関する技術動向調査）実施についての

		審議 ■ 監視状況報告
第2回	2023月2月27日	■ 自主取下げに係る電子メールによる審議の内容と結果の報告 ■ 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 ■ 軽量暗号に関する技術動向調査結果の報告 ■ 監視状況報告 ■ CRYPTREC Report 2022作成について ■ CRYPTRECシンポジウム開催について

３．２．暗号技術活用委員会

３．２．１．活動の概要

2022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 2022暗号技術活用委員会報告[3]を参照されたい。

(1) 利用実績に関する評価

2022年度は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。

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う。

(2) 暗号鍵管理ガイダンスの作成

暗号鍵管理ガイドラインの拡充を目的として、2021年度に取りまとめた作業の進め方に基づき、暗号鍵管理ガイダンスWGにて暗号鍵管理ガイダンスを作成する。

(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

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う。

３．２．２．2022年度の活動内容

３．２．２．１．利用実績に関する評価

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）（下表）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[4]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。

---

[3] CRYPTREC Report 2022 暗号技術活用委員会報告, https://www.cryptrec.go.jp/promo_cmte.html

[4] IPA、「暗号アルゴリズムの利用実績に関する調査報告書」の公開、https://www.ipa.go.jp/security/fy24/reports/cryptrec/crypto-algorithm/crypt_usageper_report.html

表　利用実績に基づく選定基準（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	該当なし	●考慮項目④において、他のハ

	SHA3-256 SHA3-384 SHA3-512 SHAKE128 SHAKE256		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

３．２．２．２．自主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。

３．２．２．３．暗号鍵管理ガイダンスの作成

暗号鍵管理検討の初めとして、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する点などを解説することを目的としたガイダンスである。本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
- 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

想定読者

- 暗号鍵管理機能を持つシステム設計者

2022年度版暗号鍵ガイダンスの章構成は以下のとおりである。具体的には、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書かれている。

1. はじめに
   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. 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
   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。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. 暗号アルゴリズムの選択
   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. 暗号アルゴリズム運用に必要な鍵情報の管理
   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サーバの鍵設定・管理をモデルにして記載例を示した。

３．２．２．４．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。

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）

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

３．２．３．暗号技術活用委員会の開催状況

2022年度の暗号技術活用委員会での審議概要は表の通りである。

表　暗号技術活用委員会の開催状況

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

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。

2023年度も、CRYPTREC暗号リストの改定を必要に応じて行うべく、その改定に向けた検討を進める。

暗号技術評価委員会においては、耐量子計算機暗号ガイドライン案が承認されたところであるが、NISTのPQC標準化における第4ラウンドなどが進行中であることから、引き続き耐量子計算機暗号に関する最新動向を把握する必要がある。また、現在、軽量暗号に関するガイドラインの更新に向けた検討を進めており、2023年度に更新案を審議する予定である。

暗号技術活用委員会においては、2022年度版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の拡充を行う。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ダンス作成に着手する予定である。

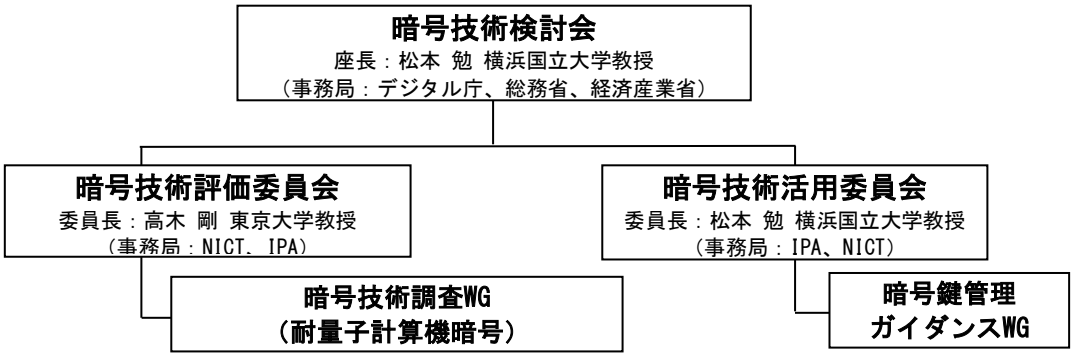

図4-1 2023年度CRYPTRECの体制図（予定）