暗号技術検討会
２０２３年度　報告書

２０２４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における、暗号アルゴリズムの安全性の評価及び監視を通じたセキュリティ確保、そして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取組が果たすべき役割も大きくなっている。

2023年度は、暗号技術検討会の活動として、CRYPTREC暗号リスト更新案の承認等を行った。そして、各委員会の活動として、暗号技術評価委員会では、軽量暗号技術に対する実装性能評価及び標準化動向調査を実施し、軽量暗号ガイドラインを更新した。また、同委員会の下に設置した暗号技術調査WG（耐量子計算機暗号）において、耐量子計算機暗号に関する調査報告書及びガイドライン(いずれも2024年度版)の作成に向けた研究技術動向調査を行うとともに、「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」の予測図を更新した。暗号技術活用委員会では、2020年に公開したTLS暗号設定ガイドラインの改訂を行った。また、同委員会の下に設置した暗号鍵管理ガイダンスWGにおいて、2022年度に発行した「暗号鍵管理ガイダンス」の拡充に向けた検討を行った。これらの2023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 2023」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。

末筆ではあるが、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。

2024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。

その後、2021年のデジタル庁発足に伴いデジタル庁が加わり、デジタル庁、総務省及び経済産業省は、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、継続的に暗号技術検討会を開催している。

暗号技術検討会での検討を経て、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CRYPTREC暗号リストとして改定され、2023年3月に再改定された。

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。

2023年度は、暗号技術検討会では、CRYPTREC暗号リスト更新案の承認等を行った。暗号技術評価委員会では、軽量暗号技術に対する実装性能評価及び標準化動向調査を実施し、軽量暗号ガイドラインを作成した。また、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）において、耐量子計算機暗号に関する調査報告書とガイドライン（それぞれ2024年度版）の作成に向けた研究技術動向調査を行うとともに、「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、2020年に公開したTLS暗号設定ガイドラインの改訂を行った。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、2022年度に発行した「暗号鍵管理ガイダンス」の拡充に向けた検討を行った。

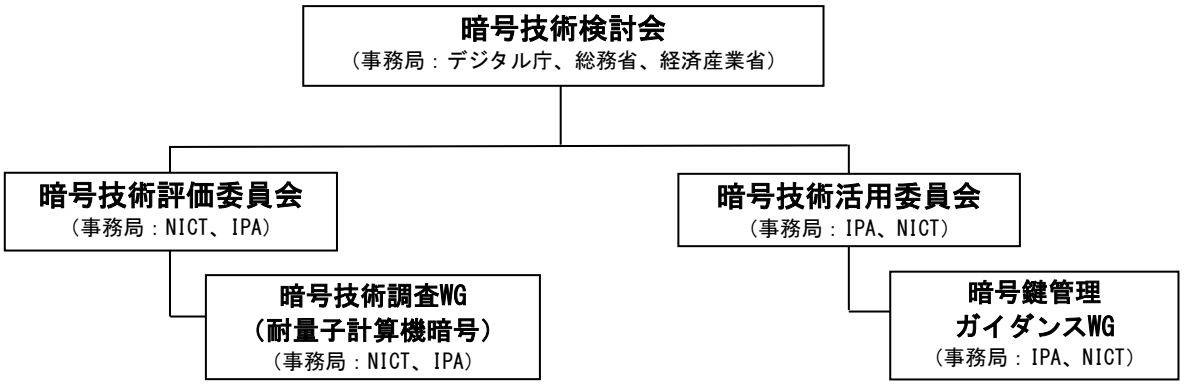

図2.2-1　CRYPTREC体制図（2023年度）

２．３．暗号技術検討会の開催実績

2023年度、暗号技術検討会は、下記内容について検討を行うため１回開催した。

【第 1 回】2024年3月26日（火）10:00～12:00

（主な議題）

・2023年度暗号技術評価委員会 活動報告について【報告】
・軽量暗号に関する外部評価報告書（案）CRYPTREC暗号技術ガイドライン（軽量暗号）（案）について【承認】
・2023年度暗号技術活用委員会 活動報告について【報告】
・TLS暗号設定ガイドライン（案）について【承認】
・Triple DES等の取り扱いに係る暗号技術活用委員会からの意見について【報告】
・CRYPTREC暗号リストの更新について【承認】
・電子署名法特定認証業務の暗号基準の改正スケジュールについて【報告】
・2024年度暗号技術評価委員会活動計画（案）について【承認】
・2024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 2023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NICTより2023年度の活動報告が行われた。
・CRYPTREC暗号技術ガイドライン案（軽量暗号）（案）についてNICT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IPAより2023年度の活動報告が行われた。
・TLS暗号設定ガイドライン（案）についてIPAより説明が行われ、原案のとおり承認された。
・Triple DES等の取り扱いに係る暗号技術活用委員会からの意見についてIPAより報告が行われた。
・CRYPTREC暗号リスト（更新事務局案）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。
・電子署名法特定認証業務の暗号基準の改正スケジュールについて、デジタル庁より報告が行われた。
・2024年度暗号技術評価委員会活動計画（案）についてNICTより説明が行われ、原案のとおり承認された。
・2024年度暗号技術活用委員会活動計画（案）についてIPA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 2023年度 報告書（案）について事務局より説明が行われ、議論結果を反映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、CRYPTREC暗号リストとは別の文書として、耐量子計算機暗号、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（2024年度版）を作成するため、2023-2024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。
- 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、2023年度は、NIST Lightweight Cryptography Projectで最終選考方式に選出されたAsconについて実装性能評価及び標準化動向調査を行った。そして、昨年度までに実施した調査と、今年度の調査を含め、2024年3月に現ガイドラインを更新した。

これらの課題について2023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 2023（暗号技術評価委員会報告）に掲載する。

３．１．３．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、その量子コンピュータを用いた攻撃に対し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を作成するために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」、「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。

2022年度に耐量子計算機暗号に関する調査報告書とガイドライン（それぞれ2022年度版）を作成・公開したが、その後もNISTをはじめとする世界各国の機関において耐量子計算機暗号の選定・標準化活動が継続されており、情勢が流動的であることを鑑み、2023-2024年度の2年間で再度、耐量子計算機暗号に関する調査報告書とガイドライン（それぞれ2024年度版）を作成することが承認された。

2023年度のPQC WGの活動では調査報告書・ガイドライン作成の準備として、2022年度版が出版された以降の研究技術動向に関して調査を行った。ガイドライン執筆方針の基本的な部分は2022年度版調査報告書・ガイドラインを踏襲している。

- 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分類とする。2022年度版とは異なり、耐量子計算機暗号の活用方法を調査報告書・ガイドラインの両方に記載。導入の章の内容について2022年度版では同じものであったが、ガイドラインでは技術的な詳細を省き簡略化する。これらの項目に関する情報を調査した。

- ガイドライン及び調査報告書の目次案

  i. 導入

  ii. PQC の活用方法

  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 は iii, iv, v, vi, vii を表す）

  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、2023年度第一回暗号技術評価委員会において、2023年度のPQC WGの活動として下記2点について実施する活動計画が承認された。

- 耐量子計算機暗号に関し、NISTのPQC標準化において第4ラウンドが進行中であることをはじめ技術開発、標準化活動が引き続き世界的に活発であることから、動向を今後2年間かけて調査・把握し、調査報告書・ガイドラインの改定を行う。
- 「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」の予測図を更新する。

それらの成果（３．１．３．１～３．１．３．２節）は2023年度第二回暗号技術評価委員会にて報告され、了承された。

３．１．３．１．耐量子計算機暗号に関する調査報告書・ガイドラインの作成方針

2024年度版の内容は、2022年度版の調査報告書・ガイドラインをベースとし、技術の進展に伴う部分を追記・修正する。なお、著者の著作権の関係から調査報告書・ガイドラインともに改定ではなく新規の扱いとし、過去の版と区別する必要がある際には（2024年度版）のように年度を明示する。

耐量子計算機暗号調査報告書・ガイドライン

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する。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とする。2022年度版とは異なり、耐量子計算機暗号の活用方法を調査報告書・ガイドラインの両方に記載する。導入の章の内容について2022年度版では同じものであったが、ガイドラインでは技術的な詳細を省き簡略化する。

耐量子計算機暗号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

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、対象となる暗号方式は PQC WG によって承認されたものである。

ガイドラインの章立て

1　はじめに

2　PQC の活用方法

3　格子に基づく暗号技術

4　符号に基づく暗号技術

5　多変数多項式に基づく暗号技術

6　同種写像に基づく暗号技術

7　ハッシュ関数に基づく署名技術

３．１．３．２．「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。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対応方針（「今後の予測図の取扱い」「今後の公開鍵暗号のパラメータ選択」）を決定した。2023年度において、対応方針の説明文をより一般の読者に読みやすくなるよう、以下のとおり修正した。

予測図の取扱い対応方針

〈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2023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3.1-1及び図3.1-2）。

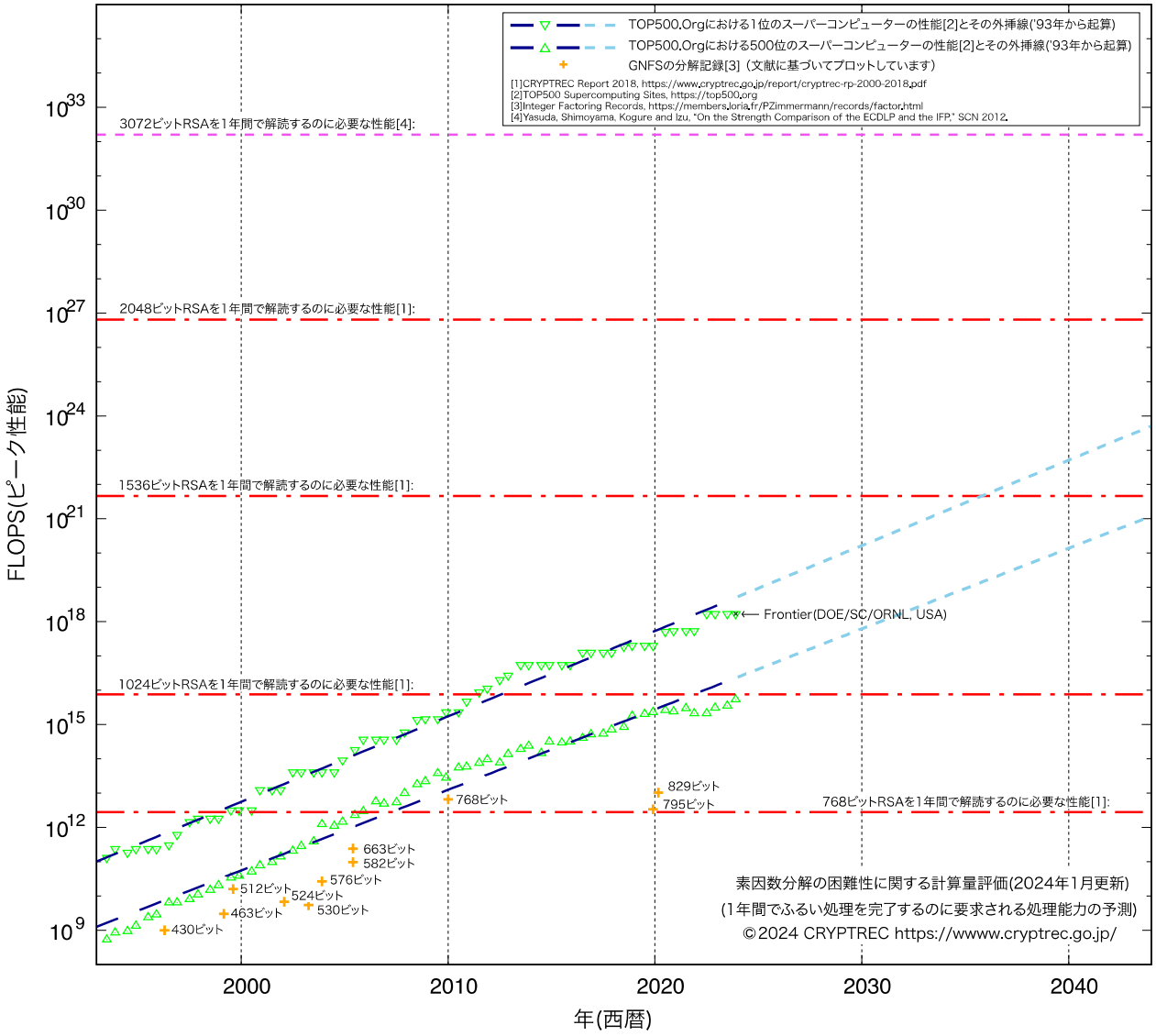

図3.1-1：素因数分解の困難性に関する計算量評価（2024年1月更新）[1]

[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。

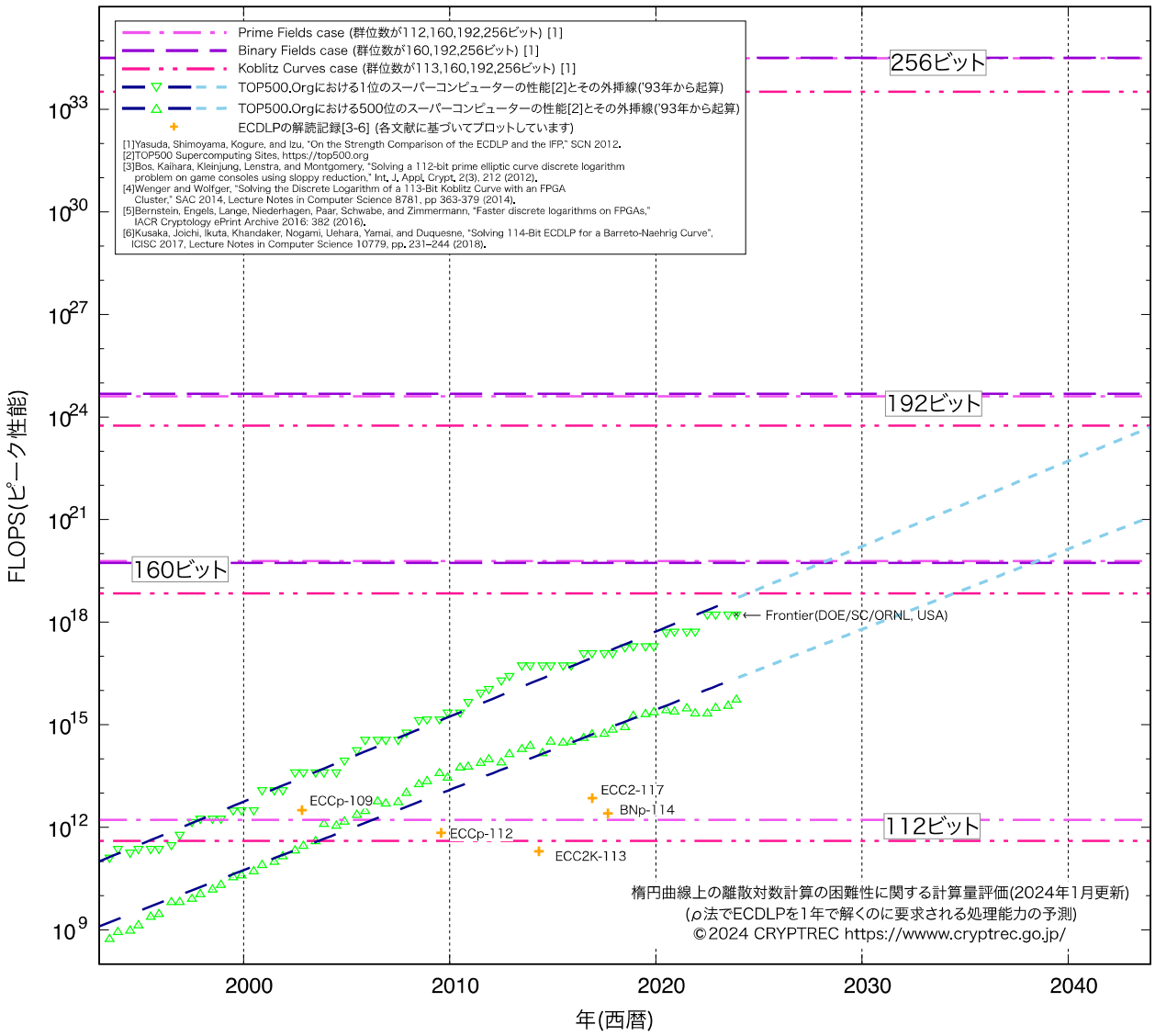

図3.1-2：楕円曲線上の離散対数計算の困難性に関する計算量評価（2024年1月更新）[2]

３．１．４．「CRYPTREC暗号技術ガイドライン（軽量暗号）」更新に関わる活動

３．１．４．１．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」ことが決定され、2020年度第二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」という）を2023年度中を目処に更新することが承認された。2021年度第二回暗号技術評価委員会においてその更新方針が承認された。

[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。

当該更新方針に従い、今年度は、NIST軽量暗号プロジェクト（NIST Lightweight Cryptography Project． 以下、「NIST LWC」という）の選定方式Asconを対象とした実装性能評価を外部評価により実施した。また、軽量暗号に関わる NIST公開文書やISO/IECなどの標準化動向に関わる調査を外部評価により実施した。その外部評価実施内容を報告する。

そして、2021年度から2023年度にかけて実施した外部評価報告書を基に「CRYPTREC暗号技術ガイドライン（軽量暗号）」2023年度版を作成した。

３．１．４．２．評価・調査実施概要

Asconの実装性能評価と標準化動向調査について、以下のとおり外部評価を実施した。

- 実装性能評価：NIST LWCで選定されたAscon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：NIST LWCでAsconを選出するに至った選考過程や選考理由に関する調査、並びにAsconの標準化動向(IETF、W3C、ISO/IEC、ITU-T、Global Platformの5団体)に関する調査を実施した。

３．１．４．２．１．調査結果概要

[軽量暗号Asconの実装性能に関する調査及び評価結果概要]

Asconの実装性能について、物理攻撃耐性を持つ実装性能評価も含めた調査結果は以下の通りである。

- 実装面における特徴：Asconは認証暗号モードとハッシュモードに対応する軽量な暗号アルゴリズムであり、以下の特徴を有する。
  - 5ビットのコンパクトなS-boxを繰り返し使用
  - ラウンド処理を並列実装可能
  - 概ね全ての処理を同じラウンド処理の繰り返しで実現可能

  これらの特徴を鑑み、実装コストと処理性能のトレードオフの観点から高い柔軟性がある。
- 物理攻撃対策：代表的な物理攻撃対策技術として、Threshold Implementation (TI)とその発展的技術であるDomain Oriented Masking (DOM)がある。これらの物理攻撃対策を施したAsconの実装評価に関する調査結果をまとめた。
- 物理攻撃耐性評価：代表的な物理攻撃耐性評価技術として、相関電力解析（CPA)、Test Vector Leakage Assessment (TVLA)、テンプレート攻撃（TA)、などがある。 これらの評価技術を使用したAsconの物理攻撃耐性評価に関する調査結果をまとめた。

[標準化動向調査結果概要]

- 最終ラウンドにおける評価基準と選定プロセス：NISTはステータスレポートNISTIR 8454を発行し、最終ラウンドにおける評価基準や選定プロセスについて明らかにした。評価基準と選定プロセスの対応関係は次の表のとおり。

評価基準	選定プロセス
暗号学的安全性	第三者による安全性評価、耐量子安全性
制約のある環境下におけるソフトウェア及びハードウェアでの実装性能	ベンチマーク
サイドチャネル攻撃	ベンチマーク
知的財産	知的財産に関する声明
その他	バリエーション、設計の微調整

- Asconが選出されるに至った選定指標や評価の観点：次の表に示す選定指標においてAsconが評価された。

選定指標	評価
機能	● 認証暗号モードとハッシュモードに加え、XOF[3]機能を含む。 ● 暗号学的置換ベースの設計により、追加機能の実装コストが少ない。
成熟度	● CAESAR コンペティションのユースケース１（軽量アプリケーション） ● 最終ラウンドにおける設計の微調整なし
安全性	● 第三者による安全性評価が最も多いファイナリスト ● 他ファイナリストよりも先行的に安全性評価が行われているにも関わらず依然として高い安全性を維持
実装性能	● ソフトウェアとハードウェアの両面で非常に優れた性能を発揮 ● 実装コストと処理性能の様々なトレードオフをサポートする柔軟性 ● 物理攻撃対策にかかる追加コストが低い。

- 標準化動向：Asconに関するNIST以外の組織での標準化動向についてまとめる。調査対象の標準化団体は、IETF、W3C、ISO/IEC、ITU-T、Global Platformの5団体である。2024年3月現在、IETFを除く4団体においてAsconに関する標準化動向は確認できなかった。IETFでは以下でAsconが取り上げられている。

  - インターネットドラフト“Secure UAS Network RID and C2 Transport”
  - インターネットドラフト“Properties of AEAD algorithms”
  - IETF 117におけるTLS WGでの発表“New Post-Quantum Signatures on the Horizon”

  その他、産業界でもAsconを利用可能な環境を提供するような動向がある。

[3] eXtendable Output Function：可変長出力関数

３．１．４．２．２．外部評価報告書に対する暗号技術評価委員会の見解

2件の外部評価報告書は、今年度の調査対象であるAsconの実装性能及び標準化動向に関する技術動向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、本報告書をCRYPTRECの技術調査報告書とすることが了承された。

３．１．４．３．2023年度版ガイドラインの作成

以下の手順により2023年度版ガイドラインを作成した。

- 2021年度から2023年度にかけて実施した外部評価に基づき、事務局にて2016年度版ガイドラインの更新を行い、完成したものを2023年度版ガイドライン（ドラフト版）とする。
- 事務局が作成した2023年度版ガイドライン（ドラフト版）について、掲載内容の適切性や情報の過不足などを2名の外部有識者によりレビューいただくとともに、第二回暗号技術評価委員会にてレビュー結果を報告いただく。
- レビュー結果に基づき、事務局にて2023年度版ガイドライン（ドラフト版）の更新を行う。更新内容について外部有識者に了解頂いたものを最終的な2023 年度版ガイドライン（案）とする。

３．１．４．３．１．2023年度版ガイドライン（ドラフト版）の作成

2023年度版ガイドライン（ドラフト版）の作成にあたり、以下の表に示す目次の赤字部分を新たに更新した。黒字部分は、2016年版ガイドラインと同一である。

章		章タイトル	概要
第1章		はじめに	導入、謝辞
第2章		軽量暗号とその活用法	
	2.1	軽量暗号とは	定義、代表的な軽量暗号
	2.2	軽量暗号の標準化動向	● CAESAR コンペティション ● NIST LWC ● 他標準化団体における Ascon の検討状況
	2.3	軽量暗号はどこに使えるのか	家電、スマートテレビ、スマート農業、医療、自動車、等での活用例
	2.4	どんな軽量暗号、パラメータを選べばいいか	一般的方針、鍵長・ブロック長の選択、利用シナリオ、等
	2.5	軽量暗号活用例と効果	家電、スマートテレビ、スマート農業、医療、自動車、等での効果
第3章		軽量暗号の実装性能	
	3.1	ブロック暗号の実装性能	12種類の軽量ブロック暗号に対するハードウェア・ソフトウェア実装評価
	3.2	認証暗号の実装性能	10種類の軽量認証暗号に対するソフトウェア実装評価
	3.3	ASCONの実装性能	● ハードウェア実装性能

			● ソフトウェア実装性能 ● 物理攻撃耐性評価
第4章		代表的な軽量暗号	
	4.1	ブロック暗号	各技術分野の各方式に関する仕様等の調査結果
	4.2	ストリーム暗号	
	4.3	ハッシュ関数	
	4.4	メッセージ認証コード	
	4.5	認証暗号	
付録A		Asconの物理攻撃耐性	
	A.1	サイドチャネル攻撃対策	● Threshold Implementation ● Domain Oriented Masking
	A.2	サイドチャネル解析・漏洩評価	● 相関電力解析 ● 故障利用攻撃 ● Test Vector Leakage Assessment ● テンプレート攻撃
付録B		CAESAR final portfolio: AEGIS, COLM	AEGIS、COLMに関する仕様等の調査結果
付録C		NIST LWC ファイナリスト（Asconを除く）	Asconを除くNIST LWCファイナリスト9方式に関する仕様等の調査結果

３．１．４．３．２．外部有識者によるレビュー概要

2023年度版ガイドライン（ドラフト版）に対し、本間尚文氏(東北大学)と峯松一彦氏（日本電気株式会社）にその掲載内容の適切性や情報の過不足などをレビューいただいた。レビュー内容の概要は以下のとおりである。

- 本間氏によるレビュー：主に第1章から第3章の更新内容に関するレビューを実施し、1箇所の構成変更（付録Aを新たに追加）といくつかの確認が必要と思われる箇所を除き、改定内容・構成が妥当である。

- 峯松氏によるレビュー：主に第4章と付録B・Cの更新内容に関するレビューを実施し、全般的に記載内容に関して大きな疑義を呈する箇所はなく、改定内容が妥当である。

３．１．４．３．３．ガイドラインの作成外部評価報告書に対する暗号技術評価委員会の見解

2023年度版ガイドラインは、軽量暗号に関する最新動向を踏まえて2016年度版ガイドラインを更新したものであり、暗号技術ガイドラインとして十分な内容を含んでいると考えられる。また、外部有識者によるレビューより更新内容の妥当性が評価されたことから、2023年度版ガイドライン（案）を暗号技術ガイドラインとすることが了承された。

３．１．５．暗号技術評価委員会の開催実績

2023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	議案
第1回	2023年7月3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 ■　軽量暗号ガイドラインの更新について、公開スケジュールに関する報告 ■　ガイドライン作成にあたり、外部評価を行うこと、外部有識者によるレビューを行うことに関する審議 ■　監視状況報告
第2回	2024月2月27日	■　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 ■　軽量暗号ガイドラインに係る技術動向調査結果の報告 ■　軽量暗号ガイドラインに関するレビューの報告 ■　軽量暗号ガイドラインに関する審議 ■　監視状況報告 ■　CRYPTREC Report 2023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

2023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 2023暗号技術活用委員会報告[4]を参照されたい。

(1) TLS暗号設定ガイドラインの改訂

現在の「TLS暗号設定ガイドライン(Ver3.0.1)」の公開(2020年7月)以降、CRYPTRECではCRYPTREC暗号リストの改定、「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（以降「強度要件設定基準」と表記)」の策定を行っている。このため、これらCRYPTREC成果の取り込み及び３年間のTLSに関するRFC規格化や技術環境の変化なども踏まえ、本ガイドラインを改訂する。

(2) 暗号鍵管理ガイダンスの拡充

暗号鍵管理ガイドラインの拡充を目的として進めていた暗号鍵管理ガイダンスについて、2021年度・2022年度に引き続いて暗号鍵管理ガイダンスWGを設置し、2022年度発行版では記載を見送った部分の拡充を行う。2022年度版の内容見直しも含め、2024年度完成を目標とする。

３．２．２．TLS暗号設定ガイドラインの改訂

現行のTLS暗号設定ガイドライン（v3.0.1）からの一番大きな変更点は、強度要件設定基準の策定に伴い、安全性の基準として「鍵長」で表現されていた部分を「ビットセキュリティ」で表現するようにしたところである。これにより、「鍵長256ビットの楕円曲線」との要件に「X25519の楕円曲線」が許容されるか否かについて、明確に許容されることとなった。

また、３年間のTLS規格化や技術環境の変化なども踏まえ、主に以下の観点での議論を行い、必要な改訂を行うこととした。

① CRYPTREC暗号リスト改定等を踏まえたTLSでの利用を推奨／禁止する暗号アルゴリズムの改訂
② 「セキュリティ例外型」の取り扱い
③ DHEの強度設定について推奨要件の改訂要否
④ その他、改訂することが望ましい項目

作成したガイドラインv3.1ドラフト案に対する主な改訂内容を表3.2-1にまとめる。なお、今回の改訂では、推奨の設定内容に大きな影響を与える項目がないことから、バージョン名はv3.1とすることとした。

[4] CRYPTREC Report 2023 暗号技術活用委員会報告, https://www.cryptrec.go.jp/promo_cmte.html

表3.2-1　TLS暗号設定ガイドラインの主な改訂内容

項目	改訂内容概要
「鍵長」基準から「ビットセキュリティ」基準への変更	強度要件設定基準に従い、現行版（v3.0.1）の鍵長をそのままビットセキュリティ基準に置き換えた。なお、利用する楕円曲線は「強度要件設定基準」に記載のものから選択することを明記した。 また、セキュリティ例外型のDH／DHEの1024ビット鍵長は、対応するビットセキュリティ基準が存在しないため、鍵長表現のままとした。
CRYPTREC暗号リスト改定等を踏まえたTLSでの利用を推奨／禁止する暗号アルゴリズムの更新	改定されたCRYPTREC暗号リストによりリストの位置づけが変更されたアルゴリズム、及び3年間のTLSに関するRFC規格化や技術環境の変化などにより変更が必要と考えるアルゴリズムについて、以下のように改訂する。 ● サーバ証明書における DSA の利用推奨を削除する ● サーバ証明書における RSA-PSS の利用推奨を追加する ● EdDSA はサーバ証明書、暗号スイートとも利用推奨をしない ● 暗号スイートでの利用禁止暗号アルゴリズムに SM2（署名）、SM3、SM4 を追加する
「セキュリティ例外型」の取り扱い	移行を明確に促す観点から移行期限を明記した以下の表現に強化する。 「本ガイドラインで記載されているセキュリティ例外型の設定内容は、2029年度を目途とした改訂時に終了させる予定である。速やかに推奨セキュリティ型への移行を完了させるべきである。」
DHE の強度設定について推奨要件の改訂要否	以下のように改訂する。 ● 高セキュリティ型は 112 ビットセキュリティから 128 ビットセキュリティ以上に変更する。推奨セキュリティ型とセキュリティ例外型は変更しない。
その他	その他の主な改訂内容として以下のものがある。 ● 「Certificate Transparency」に関する節の追加 ● 「ブラウザを利用する際に注意すべきポイント」について、Microsoft、Google、Mozilla、Apple の各ブラウザの最新情報を反映 なお、IoT の普及という観点から組み込み系に向けた補足ドキュメントを検討してはどうかとの意見があったが、本ガイドラインの主たる読者層とは対象が異なると想定されることから、今後の新規ガイドラインの作成や拡充の候補として検討することになった。

３．２．３．暗号鍵管理ガイダンスの拡充

2022年度に発行した「暗号鍵管理ガイダンスVer.1.0」と今回作成中の「暗号鍵管理ガイダンス拡充分」は、「暗号鍵管理システム設計指針（基本編）」の章構成に対応して表3.2-2のとおりである。

なお、表3.2-2はガイダンス拡充分を別冊とした場合の章構成であり、暗号鍵管理ガイダンスVer.1.0にマージするか別冊とするかは2024年度の執筆状況を踏まえて決定する。

表3.2-2　暗号鍵管理ガイダンスの章構成

暗号鍵管理システム設計指針（基本編）	暗号鍵管理ガイダンスVer.1.0（2022年度発行）	暗号鍵管理ガイダンス拡充分（別冊時）
1. はじめに	1. はじめに	1. はじめに
2. 暗号鍵管理の在り方	（1章に集約）	（1章に集約）
3. 本設計指針の活用方法	（1章に集約）	（1章に集約）
4. 暗号鍵管理システム(CKMS)の設計原理と運用ポリシー		2. 暗号鍵管理システム(CKMS)の設計原理と運用ポリシー
5. 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	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	
6. 暗号アルゴリズムの選択	3. 暗号アルゴリズムの選択	
7. 暗号アルゴリズム運用に必要な鍵情報の管理	4. 暗号アルゴリズム運用に必要な鍵情報の管理	
8. 暗号鍵管理デバイスへのセキュリティ対策		3. 暗号鍵管理デバイスへのセキュリティ対策
9. 暗号鍵管理システム(CKMS)のオペレーション対策		4. 暗号鍵管理システム(CKMS)のオペレーション対策

2023年度は、「暗号鍵管理システムの設計原理と運用ポリシー」及び「暗号鍵管理デバイスへのセキュリティ対策」について、記載すべき内容をダイジェスト形式で整理した。整理した主な概要は以下のとおりである。

【トイモデル】

暗号鍵管理システムのシンプルなモデル（トイモデル）を例示し、それに対する各検討項目への対応例を説明するためのモデルとして、「暗号鍵管理システムの設計原理と運用ポリシー」及び「暗号鍵管理デバイスへのセキュリティ対策」の節に記載するトイモデルを、IoT製品向けのプライベートCAシステムとすることに決定した。

【暗号鍵管理システムの設計原理と運用ポリシーでの解説・考慮点の主な概要】

節番号	FR番号	「解説・考慮点」の説明概要
4.1節 CKMSセキュリティポリシー	A.01-A.05	セキュリティポリシーとはCKMSが実現するセキュリティ機能や運用方針の概要を定めたもの。CKMSを利用するシステムやCKMSが構築されるIT環境のポリシーなどと矛盾がないことが前提

4.2節 情報管理ポリシー等からの要求事項	A.06	個人の説明責任が求められるケース（監査、リスクマネジメントの観点）を想定してCKMSでのサポートメカニズムを記載
	A.07-A.13	匿名性、連結不可能性、観測不可能性のサポート有無とサポートする場合のメカニズムを記載。一般に、匿名性、連結不可能性、観測不可能性を要求するのは特殊なケース
4.3節 ドメインのセキュリティポリシー	A.14-A.19	異なるセキュリティドメイン間での鍵情報の交換がなければ対象外。GPKIは異なるセキュリティドメイン間での鍵交換の事例
	A.22-A.26	マルチレベルのセキュリティドメインでの鍵情報の交換がなければ対象外。一般に、マルチレベルのセキュリティドメインでの鍵情報の交換は特殊なケース
4.4節 CKMSにおける役割と責任	A.27-A.28	CKMSの運用に関わるエンティティを定め、エンティティに割り当てる役割と実行できる鍵情報の管理機能へのアクセス権（権限）を定義する。
	A.29-A.31	不必要な権限の割り当てや権限の分離が不十分な場合、内部犯行を誘発するリスクがある
4.5節 CKMSの構築環境及び実現目標	A.32	CKMSを構成する主要なデバイスおよびコンポーネントの一式を定める
	A.33-A.36	CKMSが要求する時刻の精度や利用する権威時刻ソース、第三者タイムスタンプの要求有無を定める
	A.39-A.42	初期及び将来を想定してユーザ数やCKMS性能面の目標、負荷増大時の対応策を定める
	A.43-A.46	CKMS内デバイスやCKMS間の相互運用を可能とするため、インタフェース、プロトコル、コマンド仕様を定める
	A.47-A.50	使いやすいユーザインタフェースを検討し、ヒューマンエラーを防止する
	A.51-A.53	どのような商用既製品を利用してどのようなセキュリティ機能を実行するかを定める
4.6節 標準／規制に対する適合性	A.54-A.55	暗号アルゴリズム、暗号モジュール、セキュリティ認証などの標準への準拠性を明確にする
	A.57	CKMSが使用される国家・地域の法的規制を明確にする。欧州のサイバーセキュリティ法、中国のデータセキュリティ法、各国のデータ規制など
4.7節 将来的な移行対策の必要性	A.58-A.61	CKMSは暗号アルゴリズムのセキュリティライフタイムを超えたサービス提供や、危殆化により、暗号アルゴリズムの置き換えが必要になる。そのため、複数の暗号アルゴリズムや異なる鍵長をサポートするケースも多い
	A.62-A.69	技術の進歩をウォッチすると共に、予め潜在的な脅威に対する影響評価の実施を推奨する

【暗号鍵管理デバイスへのセキュリティ対策での解説・考慮点の主な概要】

節番号	FR番号	「解説・考慮点」の説明概要
8.1節 鍵情報へのアクセスコントロール	E.01-E.04	暗号モジュールの各機能の実行を認可されたエンティティに限定する。実行権を管理するアクセスコントロールシステム(ACS)は暗号モジュールと連動して動作する
	E.05	ACSによるエンティティ識別、認証、認可の粒度や機能を明確にする
	E.07-E.20	暗号モジュールとは､暗号境界内で暗号処理を実行するハードウェアもしくはソフトウェアの集合｡暗号境界内で利用される暗号鍵の保護機能を有する
	E.08-E.14	暗号モジュールへの鍵情報の入出力を平文形式で行うことは望ましくない｡出力は暗号化して行うことが望ましく､主に外部での保管(バックアップなど) 目的である
	E.21	鍵情報の入力を人間が行う場合､その正確さとセキュリティ面の問題がある。こうした入力がない場合は対象外
	E.22-E.25	マルチパーティコントロールを利用する機能を明確にする｡暗号鍵分割(K out of N秘密分散)やマルチパーティ機能をベンダに確認する
8.2節 セキュリティ評価・試験	E.26-E.34	いずれもシステムレベルの試験項目であるが、特に暗号モジュール(HSMなど)にも関連するものはベンダテスト、機能テスト、セキュリティテスト、環境テスト、セルフチェックテスト、第三者テストである
	E.26-E.34	FIPS140などの認証試験で上記テストをカバーするものが多い
8.3節 暗号モジュールの障害時の BCP 対策	E.35	暗号モジュールはセルフテスト機能を備えることが望ましい。FIPS140-2/-3の要件に動作前や条件付きのセルフテスト機能がある
	E.37	回復可能なエラー発生時のセルフテストを含む回復の手順､回復困難なエラー発生時の暗号モジュールの交換手順(鍵情報のバックアップや破壊を含む)を明確にする

３．２．４．Triple DES等の取り扱いについて

NISTがTriple DESを規定していたSP 800-67 Revision 2を2023 年12 月31 日に（予定通り）廃止したことに伴い、暗号技術検討会事務局からのTriple DESの取り扱いについての意見聴取の依頼に対し、暗号技術活用委員会としては検討の結果、以下のように回答した。

【Triple DESの扱いに対する意見】

- 現時点では､「運用監視暗号リスト」からの削除を検討する必要性はない

- 現時点では、「運用監視暗号リスト」の条件である「互換性維持以外の目的での利用は推奨しない。」が実質的かつ十分な制約になっており、特段の利用制限を付加する必要性もない
- 「SP 800-67 Revision 2が2023年12月に廃止されたが、それ以外は、運用監視暗号リストに移行した時点での状況とほとんど変わっていないため、Triple DESの位置づけに変更はない。」との注釈を付記する

【上記意見に至った理由】

① 廃止理由が、安全性が著しく低下したわけではなく、NISTのスケジュールに基づく動きであること
② 利用実績調査結果からは依然として極めて高い実装率であること
③ すでに運用監視暗号リストに掲載されており、互換性維持以外の目的での利用が推奨されていないこと
④ NISTも、Triple DESですでに暗号化されたデータに対する処理は引き続き許容していること
⑤ 「電子政府推奨暗号リスト」に掲載されているDSAは、現在のFIPS PUB 186-5では廃止されているが、FIPS PUB 186-5になるときに削除すべきとの議論はなかったこと

【運用監視暗号リスト掲載のアルゴリズムの取り扱いに対する意見】

運用監視暗号リスト掲載の暗号アルゴリズムは、新規に極力使用しないように促していく活動を積極的に進めるべきである。

【DSAの扱いに対する意見】

今回、Triple DESの取り扱いについて検討することになった理由が「SP 800-67 Revision 2が廃止された」ことが契機になっていると承知している。その場合、上記⑤に記載の通り、DSAも「現在のFIPS PUB 186-5では廃止されている」ことから、Triple DESとの注釈と同様の注釈を追記すべきではないか。

３．２．５．暗号技術活用委員会の開催状況

2023年度の暗号技術活用委員会での審議概要は表3.2-3の通りである。

表3.2-3　暗号技術活用委員会の開催状況

回	開催日	議案
第一回	2023年7月11日	● 2023 年度暗号技術活用委員会活動計画について ● 2023 年度暗号鍵管理ガイダンス WG 活動計画について ● TLS 暗号設定ガイドライン改訂について
メール	2024年1月12日～2月15日	● TLS 暗号設定ガイドライン改訂案 v3.1 のメール審議

第二回	2024年3月5日	● TLS 暗号設定ガイドライン改訂内容について ● 2023 年度暗号鍵管理ガイダンス WG 活動報告 ● Triple DES に関する扱いについて ● 2023 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、2024年度も、電子政府推奨暗号等の安全性を評価・監視するとともに、暗号技術の更なる普及促進を行うべく検討を進める。

暗号技術検討会においては、CRYPTREC暗号リストの更新等について必要に応じて検討を行う予定である。

暗号技術評価委員会においては、NISTをはじめとする世界各国の機関において耐量子計算機暗号の選定・標準化活動が継続されており、情勢が流動的であることを鑑み、引き続き耐量子計算機暗号に関する最新動向を把握し、耐量子計算機暗号ガイドラインの改定に向けた検討を進め、2024年度に改定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年度に公開した暗号鍵管理ガイダンスについて、引き続き、「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解説・考慮点の記載を見送った部分の拡充を行い、2024年度に拡充案を審議する予定である。また、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。

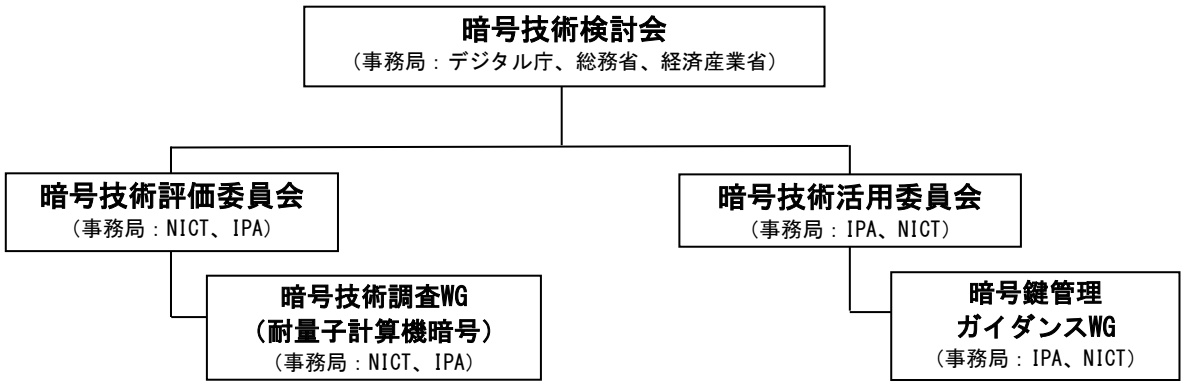

図4-1 CRYPTREC体制図（2024年度）（予定）