

暗号技術検討会
2024年度 報告書

2025年3月

目次

1. はじめに	3
2. 暗号技術検討会開催の背景及び開催状況	4
2.1. 暗号技術検討会開催の背景	4
2.2. CRYPTRECの体制	4
2.3. 暗号技術検討会の開催実績	6
3. 各委員会の活動報告	7
3.1. 暗号技術評価委員会	7
3.1.1. 活動の概要	7
3.1.2. 暗号技術の安全性及び実装に係る監視及び評価	7
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）	7
3.1.4. 外部評価「量子コンピュータが共通鍵暗号の安全性に及ぼす影響」	12
3.1.5. 暗号技術評価委員会の開催実績	18
3.2. 暗号技術活用委員会	20
3.2.1. 活動の概要	20
3.2.2. 暗号鍵管理ガイダンスの拡充	20
3.2.3. 暗号利活用のための新たなガイダンスの作成	22
3.2.4. 暗号技術活用委員会の開催状況	23
4. 今後のCRYPTRECの活動について	24

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。

2024年度は、暗号技術検討会の活動として、耐量子計算機暗号（PQC）への対応についての承認等を行った。そして、各委員会の活動として、暗号技術評価委員会では、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）並びに量子コンピュータによる共通鍵暗号の安全性への影響に関する調査報告書（2024年度版）を作成したとともに、「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、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」の追補版として「暗号鍵管理ガイダンスPart 2」を作成したとともに、クラウドにおける鍵管理ガイダンスの検討を行った。これらの2024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 2024」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。

2025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（2024年5月に更新）。

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：松本勉国立研究開発法人産業技術総合研究所フェロー、横浜国立大学上席特別教授）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。

2024年度は、暗号技術検討会では、耐量子計算機暗号（PQC）への対応についての承認等を行った。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）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）並びに量子コンピュータによる共通鍵暗号の安全性への影響に関する調査報告書（2024年度版）を作成したとともに、「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、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」の追補版として「暗号鍵管理ガイダンスPart 2」を作成したとともに、クラウドにおける鍵管理ガイダンスの検討を行った。

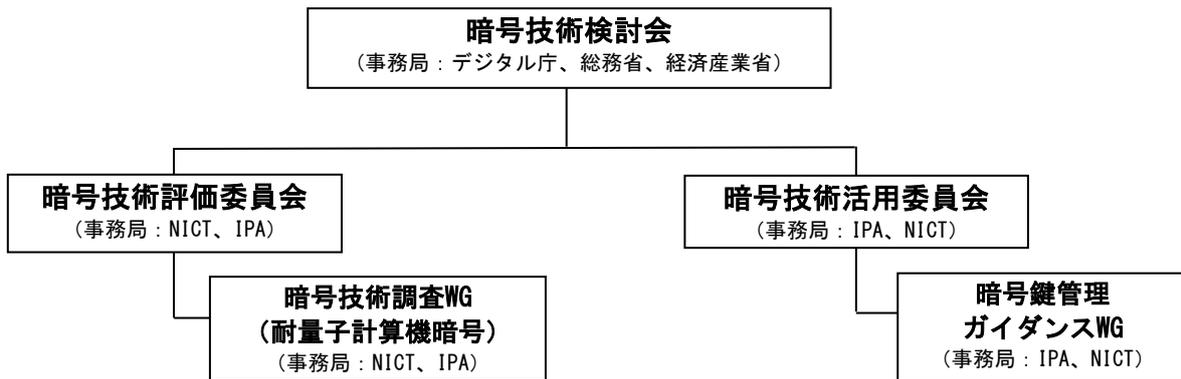


図2.2-1 CRYPTREC体制図 (2024年度)

2.3. 暗号技術検討会の開催実績

2024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】2025年3月25日（火）9:00～11:00

（主な議題）

- ・2024年度暗号技術評価委員会 活動報告について【報告】
- ・CRYPTREC暗号リスト仕様書の参照先変更について【報告】
- ・耐量子計算機暗号ガイドライン／調査報告書の更新について【承認】
- ・「量子コンピュータが共通鍵暗号の安全性に及ぼす影響」に関する外部評価報告書（案）について【承認】
- ・2024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（Part 2）について【承認】
- ・耐量子計算機暗号（PQC）への対応について【承認】
- ・2025年度暗号技術評価委員会活動計画（案）について【承認】
- ・2025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 2024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2024年度の活動報告が行われた。
- ・CRYPTREC暗号リスト仕様書の参照先変更についてNICTより報告が行われた。
- ・耐量子計算機暗号ガイドライン／調査報告書の更新についてNICTより説明が行われ、原案のとおり承認された。
- ・「量子コンピュータが共通鍵暗号の安全性に及ぼす影響」に関する外部評価報告書（案）についてNICTより説明が行われ、指摘事項への対応を前提とした上で承認された。
- ・暗号技術活用委員会についてIPAより2024年度の活動報告が行われた。
- ・暗号鍵管理ガイダンス（Part 2）についてIPAより説明が行われ、原案のとおり承認された。
- ・耐量子計算機暗号（PQC）への対応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。
- ・2025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。
- ・2025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 2024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ホームページでの公表
- ・ 推奨候補暗号リストへの新規暗号（事務局選出）の追加
- ・ 新技術暗号等に係る調査

また、CRYPTREC暗号リストとは別の文書として、「暗号技術ガイドライン（耐量子計算機暗号）2024年度版」「耐量子計算機暗号の研究動向調査報告書2024年度版」を作成した。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）、研究動向調査報告書（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した。
- ・ 2023年度までに実施した調査と、2024年度の調査を含め、2024年3月にガイドライン2022年度版および研究動向調査報告書2022年度版を更新し、2024年度版とした。

さらに、調査報告書「量子コンピュータによる共通鍵暗号の安全性への影響に関する調査及び評価2024年度版」を作成した。基本方針は以下のとおりである。

- ・ 量子コンピュータによる共通鍵暗号の安全性への影響に関する調査及び評価2024年度版については、2019年度に作成した「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」の更新のため、動向調査を行った。そして、実施した調査に基づき、2024年3月に調査報告書2019年度版を更新し、2024年度版とした。

これらの課題について2024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 2024（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

性を担保することが期待される暗号（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。2024年度についても、2024年度第一回暗号技術評価委員会において、PQC WGが設置されること、および、2024年度のPQC WGの活動として以下の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2024年度末までに調査・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。

これらの成果（3. 1. 3. 1～3. 1. 3. 2節）は2024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. 暗号技術調査ワーキンググループ（耐量子計算機暗号）

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。そして、2023-2024年度のPQC WGの活動により、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い、ガイドライン・調査報告書2024年度版を作成した。調査報告書・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 Scope

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。

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。

表3.1-1 ガイドラインの章立て

章	タイトル
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章以降の構成（A章の場合：Aは3，4，5，6，7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

- 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。

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。2024年度において、対応方針は以下のとおりとなっている。

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2024年6月と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）。

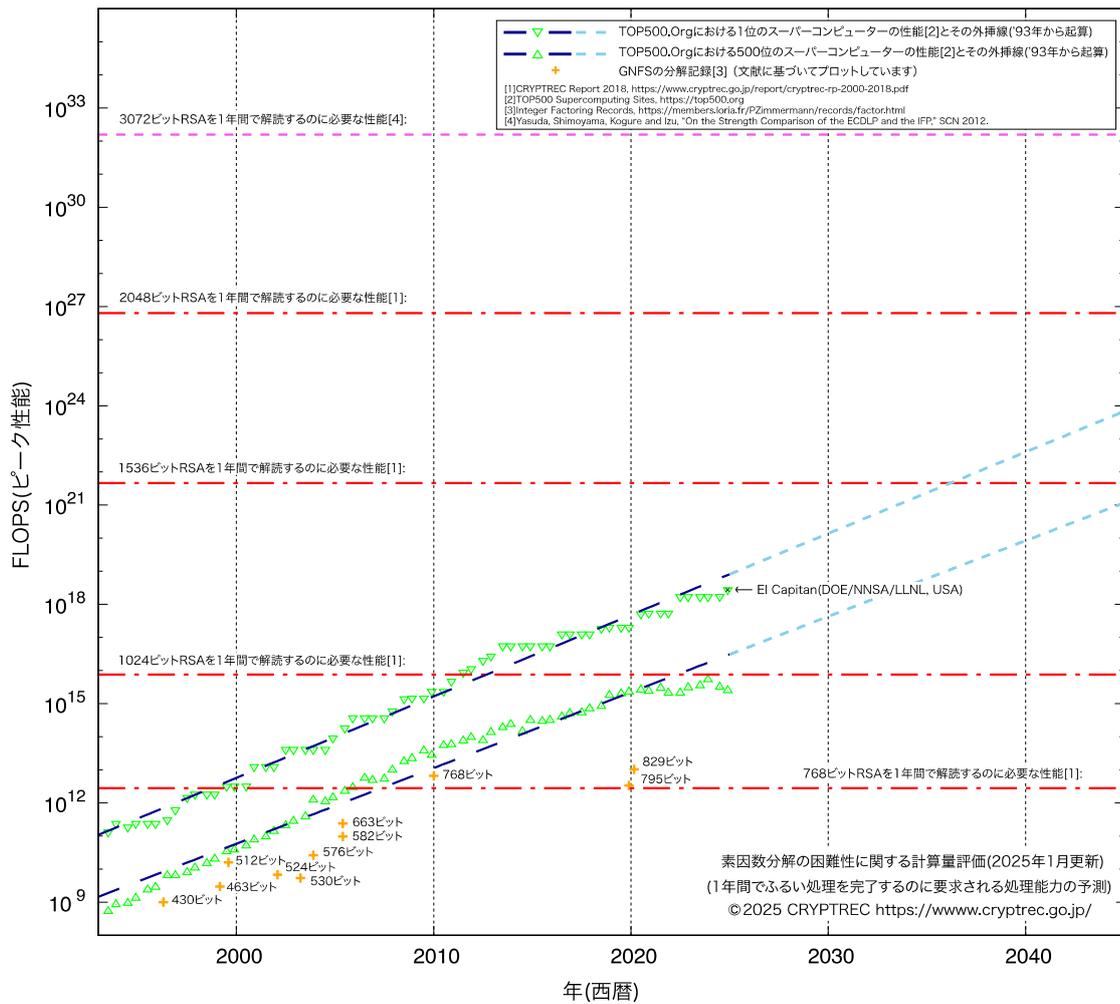


図3.1-1：素因数分解の困難性に関する計算量評価（2025年1月更新）¹

¹ スーパーコンピュータ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。

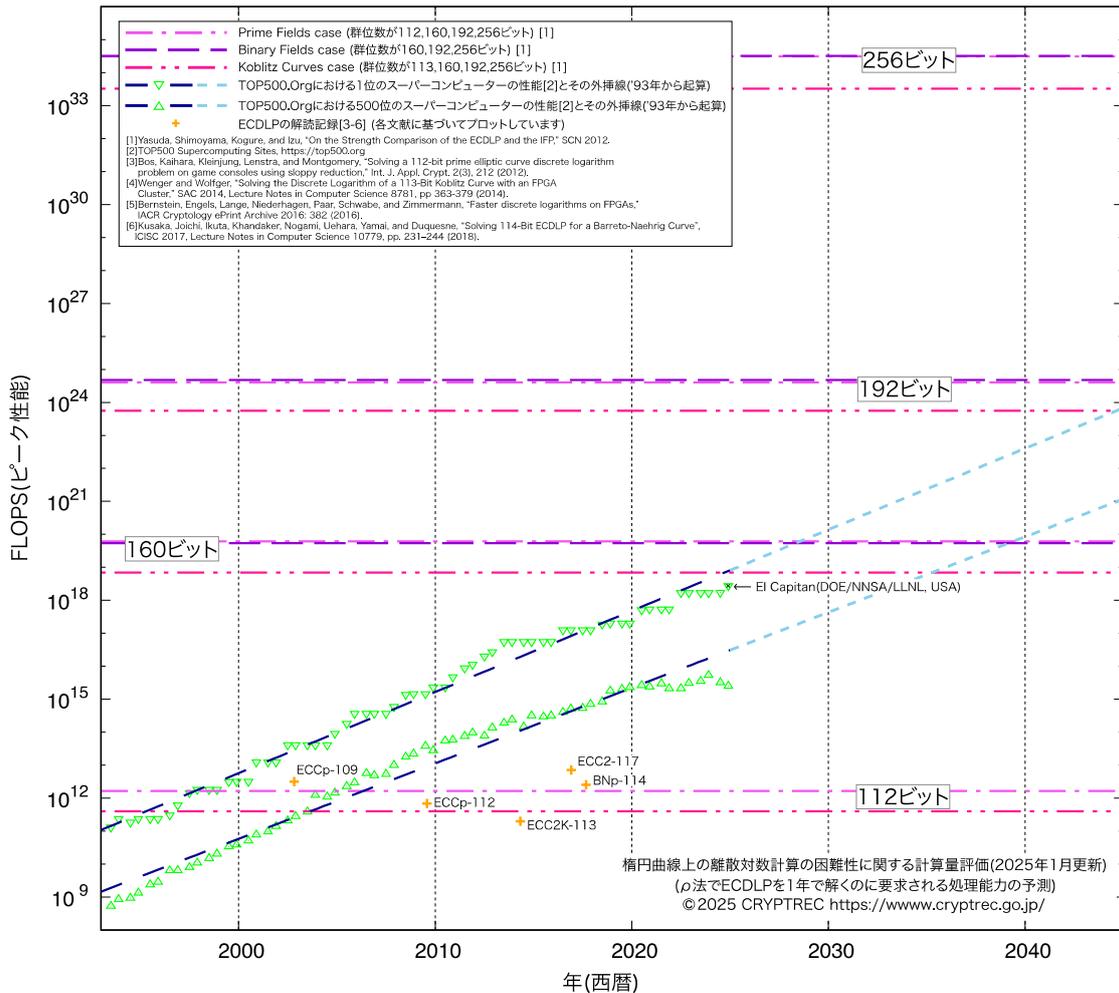


図3.1-2：楕円曲線上の離散対数計算の困難性に関する計算量評価（2025年1月更新）²

3.1.4. 外部評価「量子コンピュータが共通鍵暗号の安全性に及ぼす影響」

3.1.4.1. 背景

- (1) 2019年度、暗号技術調査ワーキンググループ（暗号解析評価）における活動として「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」を外部評価により実施し、本報告書（以下、「2019年度外部評価報告書（CRYPTREC EX-2901-2019）」という）をCRYPTRECの技術調査報告書として公開した。
- (2) 2022年度、PQC WGIにおける活動として「CRYPTREC暗号技術ガイドライン（耐量子計算機暗号）（CRYPTREC GL-2004-2022）」と「耐量子計算機暗号の研究動向調査報告書（CRYPTREC TR-2001-2022）」（以下、「PQCガイドライン等」という）を作成した。
- (3) 2019年度外部評価報告書が公開されていることを踏まえ、PQCガイドライン等ではPQCとして共通鍵暗号を含まず、公開鍵暗号のみを示す言葉としている。つまり、PQCガイドライン等では

² スーパーコンピュータ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。

共通鍵暗号の耐量子安全性については触れていない。

- (4) 2023年度第2回暗号技術評価委員会で共通鍵暗号の耐量子安全性に関する議論が行われた。具体的には、共通鍵暗号の耐量子安全性に関する技術動向調査を実施し、2019年度外部評価報告書に調査内容を反映させる形で更新することはどうか、ということについて議論が行われた。本件について、事務局で対応を検討することが確認された。
- (5) 2024年度第1回暗号技術評価委員会において、量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価を外部評価で実施し、本結果を2019年度外部評価報告書に反映させる形で更新することが承認された。

3.1.4.2. 評価・調査実施概要

細山田 光倫 様（日本電信電話株式会社）に外部評価を依頼した。選出理由と依頼内容は以下のとおりである。

- (1) 選出理由
共通鍵暗号の耐量子安全性に関する広い知見をお持ちであり、当該分野に関する数多くの実績をお持ちであるとともに、2019年度外部評価報告書の執筆者であるため。
- (2) 依頼内容
量子コンピュータが共通鍵暗号の安全性に及ぼす影響について、公開されている解析手法やその影響範囲などについてまとめ、考察などを行い、2019年度外部評価報告書に最新の情報を反映させて、報告書（以下、「2024年度外部評価報告書」という）を作成する。

3.1.4.3. 外部評価報告書の概要

- (1) 目次
2024年度外部評価報告書の目次は表3.1-2のとおり。表内において、2019年度版外部評価報告書から大きく加筆・修正した箇所を青字、追加された箇所を赤字で示す。

表3.1-2 2024年度外部評価報告書の目次

章	章タイトル	概要
1	はじめに	導入、 2019年度版との差異
2	準備	1. Grover のアルゴリズム 2. Simon のアルゴリズム
3	攻撃のモデル： 古典クエリと量子クエリ	1. 古典攻撃モデル 2. Q1 モデル（古典クエリ攻撃モデル） 3. Q2 モデル（量子クエリ攻撃モデル） 4. Q1 モデルと Q2 モデルの比較 5. ハッシュ関数への攻撃のモデル
4	攻撃コスト評価方法に 関する議論	1. 古典的衝突探索と誕生日のパラドクス 2. 最初の量子衝突探索アルゴリズム：BHT 3. BHT のアルゴリズムの効率性をめぐる議論 4. 量子ビット数の観点で効率的なアルゴリズム：CNS 5. その他の議論
5	汎用量子攻撃	1. Grover のアルゴリズムによる鍵回復・原像攻撃 2. 衝突探索および関連する問題

		3. 多重原像探索 4. タイムメモリトレードオフとレインボーテーブル 5. ノストラダムス攻撃 6. 汎用量子攻撃の具体的なコスト
6	量子クエリ攻撃 (Q2)	1. Even-Mansour (EM) 暗号への鍵回復攻撃 2. Feistel 暗号 (Luby-Rackoff 構成) への識別攻撃 3. Crypto 2016 における Kaplan らの結果 4. Grover のアルゴリズムと Simon のアルゴリズムの組み合わせ 5. 隠れシフト問題と Kuperberg のアルゴリズム 6. 線形化攻撃 7. その他の古典攻撃の高速化
7	古典クエリ攻撃 (Q1)	1. 桑門・森井による EM 暗号への鍵回復攻撃 2. オンライン-オフライン中間一致攻撃 3. 量子クエリ無しでの Simon のアルゴリズムの応用 4. 古典的に $2k$ ビット安全なら k ビット耐量子安全か? 5. その他の古典攻撃の高速化 6. 古典安全性証明の結果が Q1 モデルへ持ち上がる場合
8	ハッシュ関数への (汎用でない) 攻撃	1. 衝突攻撃 2. 原像攻撃
9	考察とまとめ	CRYPTREC暗号リスト、NIST LWC最終選考方式Asconの耐量子安全性に関する考察

(2) 調査結果の概要

調査結果について、主に新規追加事項 (表3. 1-2の赤字箇所) を概説する。

① 準備：攻撃モデル (3章)

攻撃者は量子計算機を持っており、秘密鍵が埋め込まれた攻撃対象のオラクル (暗号化／復号／認証タグ生成オラクル) へクエリ可能である。

- ・古典クエリ攻撃 (Q1) モデル：オラクルへのクエリが古典情報
- ・量子クエリ攻撃 (Q2) モデル：オラクルへのクエリが量子重ね合わせ状態

なお、ハッシュ関数への攻撃を考える場合はオラクルを使用する必要がないため、本資料では単に量子攻撃モデルと記載する。

② 汎用量子攻撃：タイムメモリトレードオフとレインボーテーブル (5. 4節)

ランダムな関数 $H: \{0,1\}^n \rightarrow \{0,1\}^n$ の原像探索にかかるオンライン計算量 T は、使用可能なメモリサイズ S によって変動することが知られている。最も有名な手法には、Hellmanのタイムメモリトレードオフ攻撃とOechslinのレインボーテーブルがある。いずれも、時間とメモリのトレードオフ $T = O((2^n/S)^2)$ が与えられる。

2024年にDunkelmanらは、量子計算機を用いることで時間とメモリのトレードオフを $T = O((2^n/S)^{1.5})$ まで改善できることを示した。攻撃アイデアの根幹はHellmanのタイムメモリトレードオフ攻撃とOechslinのレインボーテーブルと同じである。

量子計算リソースは、多項式サイズの小さい計算用量子プロセッサと指数的に大きなサイズのQRAMがある、と仮定している。

③ 汎用量子攻撃：ノストラダムス攻撃 (5. 5節)

Merkle-Damgard構造のハッシュ関数 H に対する汎用量子攻撃である。具体的には、攻撃者は以下の問題を解く。

Step 1. 攻撃者は何らかの値 y を事前に計算する。

Step 2. X が選ばれ、攻撃者に与えられる。

Step 3. 攻撃者は $H(X\parallel R) = y$ を満たす R を求める。

古典攻撃モデルでは、 n ビットハッシュ関数に対し、 $O(2^{2n/3})$ 回の圧縮関数評価で攻撃が実行可能であると知られている。2022年にBenediktらは、量子攻撃モデルにおいて評価回数を $O(2^{3n/7})$ 回まで削減できることを示した。

④ Q2モデルにおける量子クエリ攻撃：線形化攻撃（6.6節）

Q2モデルにおける量子クエリ攻撃のアイデアは、周期関数を作ってSimonのアルゴリズムを適用する、ということが大部分を占めている。例えば、EM暗号、Feistel暗号、GCMやCBC-MACを含むブロック暗号利用モード、などへの攻撃がある（報告書6.1-6.3節）。ブロック暗号利用モードへの攻撃は2016年のKaplanらによって報告されたが、ISO標準のLightMACを含むいくつかのブロック暗号利用モードには同様のアイデアを適用できないという問題があった。

2021年にBonnetainらは、量子線形化攻撃を提案してこの問題を解決した。攻撃手法の詳細は省略するが、既存のアイデアと同様、攻撃対象の内部構造を詳細に分析して周期関数を作り、Simonのアルゴリズムを適用することにより、多項式時間での識別攻撃を可能にした。

⑤ 古典攻撃モデルにて $2k$ ビット安全であれば k ビット耐量子安全か？（7.4節）

Groverのアルゴリズムにより、 k ビット鍵の全数探索に必要な計算量が 2^k から $2^{k/2}$ まで落ちることが知られている。量子計算機の実用化後に共通鍵暗号の安全性を現在と同程度に保つためには鍵長を2倍以上にする必要がある、と言われるのはこのためである。

一方、この逆の「古典攻撃モデルにて $2k$ ビット安全であればQ1/Q2モデルにて k ビット安全である」という主張について考察すると、必ずしもこの主張が成り立つとは限らない。例えば、Q2モデルではEM暗号に対する多項式時間攻撃（6.1節）があり、Q1モデルでもFX構成の拡張版である2XOR構成と呼ばれる構造のブロック暗号に対し、上記の主張を破る攻撃が2022年にBonnetainらによって報告された。

⑥ 古典的な安全性証明の結果がQ1モデルでもそのまま成り立つ場合（7.6節）

古典的な安全性証明がランダムオラクルモデルなどのプリミティブを理想化した条件で与えられるのではなく、反証可能な標準的仮定（CTRモードであればブロック暗号が擬似ランダム置換という仮定）のみに依存している場合、古典的な安全性証明の結果がQ1モデルでの安全性証明としてそのまま成り立つ。

⑦ ハッシュ関数に対する（汎用的でない）量子攻撃（8章）

衝突攻撃の攻撃可能段数に関して、古典攻撃モデルよりも量子攻撃モデルの方が優れている例がいくつか報告されている。例えば、電子政府推奨暗号リスト掲載のSHA-256、SHA-512、そしてSHA3-256が該当し、結果の詳細は表3.1-3の通りである。

表3. 1-3 古典・量子攻撃モデルでのSHA2とSHA3に対する衝突攻撃の比較

対象	出力長	段数	攻撃可能段数	
			古典	量子
SHA-256	256	64	31	38
SHA-512	512	80	31	39
SHA3-224	224	24	5	6
SHA3-256	256	24	5	6

一方、原像攻撃の攻撃可能段数に関して、現状において古典攻撃モデルよりも量子攻撃モデルの方が優れている例は報告されていない。

(3) 考察結果の概要

Q2モデルでの攻撃、Q1モデルでの攻撃、ハッシュ関数への攻撃に分け、種々の主要な方式の安全性への影響を考察する。より具体的には、CRYPTREC電子政府推奨暗号リスト掲載方式、そしてNIST標準軽量暗号Asconに焦点を当てる。

① Q2モデルでの攻撃

古典攻撃モデルにおいて安全性が保証されている共通鍵暗号技術（GCM、CBC-MAC、など）に対して多項式時間で実行可能な攻撃が存在するが、Q2モデルでは攻撃対象が量子回路上に実装されている必要がある。これは非常に特殊な状況であり、現状では既存の共通鍵暗号技術にQ2モデルでの攻撃の影響が及ぶことは無いと考えられる。特に、CRYPTREC電子政府推奨暗号リスト掲載方式やNIST標準軽量暗号Asconの安全性を評価する上でQ2モデルでの攻撃を考慮する必要はない。

② Q1モデルでの攻撃

Q2モデルでの攻撃とは異なり、古典攻撃モデルにおいて安全性が保証されている共通鍵暗号技術に対して多項式時間で実行可能な攻撃は存在しない。ただし、古典攻撃モデルにて $2k$ ビット以上の安全性があったとしても、Q1モデルでの安全性が k ビット以下になる例も示されているため、暗号技術ごとに確認が必要である。

Q1モデルにおいて、ハッシュ関数を除くCRYPTREC電子政府推奨暗号リスト掲載方式やNIST標準軽量認証暗号のAscon-AEAD/Ascon-80pqの安全性に量子計算機が与える影響は、“Groverのアルゴリズムを用いると k ビット鍵の全数探索が $O(2^{k/2})$ で実行できるため、長期的に保護したいデータには鍵長が192ビットや256ビットの暗号技術を使用した方が賢明である”と考えられる。これらの暗号技術について、Q1モデルで安全性が期待できる範囲を表3. 1-4でまとめる。

③ ハッシュ関数への攻撃

SHA-256、SHA-512、SHA3-256では、量子計算機が使用可能になると衝突攻撃の攻撃可能段数が古典攻撃モデルと比べて伸びることが知られている。表3. 1-3で示すように、安全性マージンは十分に確保されているものの、今後の動向を注視する必要がある。その他、CRYPTREC電子政府推奨暗号リスト掲載のハッシュ関数やNIST標準軽量ハッシュ関数のAscon-Hash256/Ascon-XOF128の安全性に量子計算機が及ぼす影響は、汎用量子攻撃（特に、BHTのア

ルゴリズム)のみを考慮すれば十分である。これらの暗号技術について、BHTのアルゴリズムを適用するのに必要な計算時間と量子メモリの概算値を表3.1-5でまとめる。

表3.1-4 ハッシュ関数を除く電子政府推奨暗号リスト掲載方式、Ascon-AEAD、そしてAscon-80pqについて、Q1モデルで安全性が期待できる範囲 (Groverのアルゴリズム： $\leq 2^{k/2}$)

技術分類	方式名	鍵長 k (ビット)	安全性が期待できる範囲*
ブロック暗号	AES	128	時間 $\leq 2^{64}$
	Camellia	192	時間 $\leq 2^{96}$
		256	時間 $\leq 2^{128}$
ストリーム暗号	KCipher-2	128	時間 $\leq 2^{64}$
秘匿モード	CBC, CFB, CTR, OFB, XTS	k	時間 $\leq 2^{k/2}$ かつ 古典的に安全性が保証される範囲
認証付き 秘匿モード	CCM, GCM	k	時間 $\leq 2^{k/2}$ かつ 古典的に安全性が保証される範囲
メッセージ 認証コード	CMAC, HMAC	k	時間 $\leq 2^{k/2}$ かつ 古典的に安全性が保証される範囲
認証暗号	ChaCha20- Poly1305	256	時間 $\leq 2^{128}$ かつ 古典的に安全性が保証される範囲
	Ascon- AEAD128	128	時間 $\leq 2^{64}$ かつ 古典的に安全性が保証される範囲
	Ascon-80pq	160	時間 $\leq 2^{80}$ かつ 古典的に安全性が保証される範囲

* 計算時間：対象となる方式の呼び出し回数

表3.1-5 電子政府推奨暗号リスト掲載のハッシュ関数、Ascon-Hash256、Ascon-XOF128に対してBHTのアルゴリズムを適用するのに必要な計算時間と量子メモリの概算値： $\min(2^{c/3}, 2^{h/3})$

方式名	キャパシティ c	出力長 h	計算時間*	量子メモリ
SHA-256	-	-	-	-
SHA-512/256	-	256	$2^{85.3}$	$2^{85.3}$
SHA3-256	512	-	-	-
SHA-384	-	384	2^{128}	2^{128}
SHA3-384	768	-	-	-

SHA-512	-	512	$2^{170.7}$	$2^{170.7}$
SHA3-512	1024			
SHAKE128	256	$\ell \geq 256$	$\min(2^{85.3}, 2^{\ell/3})$	$\min(2^{85.3}, 2^{\ell/3})$
SHAKE256	512	$\ell \geq 256$	$\min(2^{170.7}, 2^{\ell/3})$	$\min(2^{170.7}, 2^{\ell/3})$
Ascon-Hash256	256	256	$2^{85.3}$	$2^{85.3}$
Ascon-XOF128	256	$\ell > 0$	$\min(2^{85.3}, 2^{\ell/3})$	$\min(2^{85.3}, 2^{\ell/3})$

* 計算時間：対象となる方式の呼び出し回数

(4) 2019年度外部評価報告書における結論との差異

具体的な方式の実用面での安全性評価について、2019年度外部評価執筆時からの大きな差異は、ハッシュ関数の衝突攻撃可能段数が古典攻撃モデルの場合に比べて量子攻撃モデルの場合に伸びることが明らかになってきたということである。

このような状況の変化に応じ、2019年度版外部評価報告書の結論を表3.1-6で示すように変更した。その他の結論部分について大きな差異はない。

表3.1-6 ハッシュ関数に関する技術動向の変化

2019年度外部評価報告書執筆時	現在
古典的に128ビット安全性のあるハッシュ関数の安全性に量子攻撃が現実的な脅威を直接及ぼすとは現状考えづらい。	重要な用途に供するハッシュ関数の出力長（スポンジ構造の場合は出力長に加えてキャパシティ長）はBHTのアルゴリズムの計算量 $O(2^{n/3})$ を基準にして384ビットや512ビットのものをういた方が無難であると考えられる。

3.1.4.4. 外部評価報告書に対する暗号技術評価委員会の見解

2024年度外部評価報告書から、CRYPTREC電子政府推奨暗号リスト掲載方式とNIST標準軽量暗号Asconの安全性に量子計算機が及ぼす影響は、汎用量子アルゴリズム（特に、GroverのアルゴリズムとBHTのアルゴリズム）のみを考慮すれば十分であるという結論を得た。

以上より、2024年度外部評価報告書（案）を2024年度外部評価報告書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

2024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3.1-7のとおりである。

表3.1-7 暗号技術評価委員会の開催状況

回	開催日	議案
第1回	2024年7月9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

		<ul style="list-style-type: none"> ■ PQC WGの活動計画案の審議 ■ 「量子コンピュータが共通鍵暗号の安全性に及ぼす影響」について外部評価を行うことの審議 ■ 監視状況報告
第2回	2025月3月3日	<ul style="list-style-type: none"> ■ PQC WGの活動内容の報告 ■ 「量子コンピュータが共通鍵暗号の安全性に及ぼす影響」について外部評価についての報告と、本外部評価の公開に関する審議 ■ 監視状況報告 ■ CRYPTREC Report 2024作成について ■ CRYPTRECシンポジウム開催について

また、PQC WGは計2回開催した。さらに、メールによる審議を実施した。2023年度から2024年度のPQC WG各回、および、メール審議の概要は表3.1-8のとおりである。

表3.1-8 PQC WGの開催状況

年度	回	耐量子計算機暗号ガイドラインの議論・決定・報告
2023年度	第1回 2023/9/13	<ul style="list-style-type: none"> ✓ 追記・改定の方針について議論 ✓ 執筆担当者を議論
	第2回 2024/1/19	<ul style="list-style-type: none"> ✓ 追記・改定すべき項目及びその章立ての決定 ✓ 調査の中間報告
2024年度	第1回 2024/7/26	<ul style="list-style-type: none"> ✓ 中間報告、追加及び削除すべき暗号方式があれば議論
	第2回 2025/2/3	<ul style="list-style-type: none"> ✓ 内容の確定
	メール審議 2025/2/4~2/12	<ul style="list-style-type: none"> ✓ エディトリアルな部分の審議 <ul style="list-style-type: none"> ・ 「PQC」という単語の示す範囲 ・ 句読点の利用方針

3.2. 暗号技術活用委員会

3.2.1. 活動の概要

2024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 2024暗号技術活用委員会報告³を参照されたい。

(1) 暗号鍵管理ガイドランスの拡充

暗号鍵管理ガイドランスの拡充を目的として進めていた暗号鍵管理ガイドランスについて、2021年度から2023年度に引き続いて暗号鍵管理ガイドランスWGを設置し、2023年5月に発行したガイドランスでは記載を見送った部分の拡充を行う。2023年5月版の内容見直しも含め、2024年度完成を目標とする。

(2) 暗号利活用のための新たなガイドランスの作成

「クラウドにおける鍵管理ガイドランス」をテーマとする新たなガイドランスの作成に着手する。おおむね2年程度での完成を想定して執筆作業を行う。クラウド利用者が留意すべき鍵管理を解説することを目的とする。

3.2.2. 暗号鍵管理ガイドランスの拡充

2024年度は、2023年5月発行のガイドランスにおいて記載を見送った部分について追補版のガイドランスを作成した。分冊構成としたため、2023年5月発行のガイドランスを「暗号鍵管理ガイドランスPart 1」、今年度執筆した追補版を「暗号鍵管理ガイドランスPart 2」と呼ぶこととした。

表3.2-1 暗号鍵管理ガイドランスの章構成

暗号鍵管理システム設計指針 (基本編)	暗号鍵管理ガイドランスPart 1 (2023年5月発行)	暗号鍵管理ガイドランスPart 2 (2024年度執筆)
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の設計 原理と運用ポリシー		2. 暗号鍵管理システムの設計 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	

³ CRYPTREC Report 2024 暗号技術活用委員会報告, https://www.cryptrec.go.jp/promo_cmte.html

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のオペレーション対策		4. 暗号鍵管理システムのオペレーション対策

ガイダンスPart 1（2023年5月発行）では、「設計指針」の5章から7章に該当する項目に関して、項目の概説及びその記載例を提供している。これらの項目は、暗号鍵管理システム（CKMS）の利用環境に関わらず検討する必要がある共通項目であり、「狭義」の意味での暗号鍵管理に相当する。

ガイダンスPart 2（2024年度執筆）では、「設計指針」の4章、8章、9章に該当する項目に関して、項目の概説及びその記載例を提供している。Part 2の2章はCKMSの全体方針を定める項目である。また、Part 2の3章はCKMSに利用するデバイス管理を含む場合に検討すべき項目であり、Part 2の4章はCKMSのシステム管理を含む場合に検討すべき項目である。これらのPart 2における3章や4章までを含む場合、「広義」の意味での暗号鍵管理に相当する内容となる。

ガイダンスPart 2の各章の記載概要は以下のとおりである。

1. はじめに

イントロダクションとして、ガイダンスPart 2の位置づけについて、「設計指針」やガイダンスPart 1との関係を含めて記載した。また、ガイダンスPart 2におけるトイモデルとして設定した「IoT機器（家電製品）向けに公開鍵証明書を発行するプライベートCAシステム」の概要を説明した。

2. 暗号鍵管理システムの設計原理と運用ポリシー

「設計指針」での「暗号鍵管理システムの設計原理と運用ポリシー」における検討項目について解説・考慮点を記載した。CKMSのセキュリティポリシー、CKMSに関わるエンティティの定義、CKMSを構成するデバイスやコンポーネントの一覧、CKMSでの実現目標、CKMSに関わる法規制や標準化技術、将来的な移行対策などの検討項目から構成される。トイモデルとしてプライベートCAのセキュリティポリシーや運用の想定例を設定して、各検討項目の対応例を説明した。

3. 暗号鍵管理デバイスへのセキュリティ対策

「設計指針」での「暗号鍵管理デバイスへのセキュリティ対策」における検討項目について解説・考慮点を記載した。CKMSにおけるセキュアな暗号鍵管理・保管の中核となる暗号鍵管理デバイスへのアクセスコントロールに対する検討事項、暗号鍵管理デバイス内の暗号モジュールに対する検討項目、暗号鍵管理デバイス及びCKMSのセキュリティ評価・試験に関する検討項目、暗号鍵管理デバイスにおける障害発生時のBCP対策に関わる検討項目などで構成される。トイモデルとして、プライベートCAで用いるハードウェア・セキュリティモジュールに関わる具体例として各検討項目の対応例を説明した。

4. 暗号鍵管理システムのオペレーション対策

「設計指針」での「暗号鍵管理システムのオペレーション対策」における検討項目について解

説・考慮点を記載した。CKMSにおける物理的セキュリティコントロール及びコンピュータシステムやネットワークにおけるセキュリティコントロールとそれらが危殆化した場合のBCP対策、システム及びデバイスの開発プロセスやセキュリティメンテナンスに関わる検討項目、セキュリティアセスメントに関わる検討項目、CKMS全体に関わる災害時のBCP対策などの検討項目で構成される。トイモデルとして、プライベートCAの設置環境や入退室管理、プライベートCAを構成するサーバシステムでのセキュリティコントロール、セキュリティアセスメントにおける実施項目、プライベートCAの災害復旧対策を想定して各検討項目の対応例を説明した。

3.2.3. 暗号利活用のための新たなガイダンスの作成

新たなガイダンスとして「クラウドにおける鍵管理ガイダンス（仮称）」を設定し、作成方針を議論した。委員会での議論を経た検討結果を以下の観点で説明する。

- ① 目的・想定読者・スコープについて
- ② 記載内容のポイントについて
- ③ 作成スケジュールおよび検討体制について

① 目的・想定読者・スコープについて

本ガイダンス執筆の目的については以下のように整理した。

クラウドサービスを活用して効率的に情報システムを構築することは一般的になっている。一方で、クラウドサービスの活用には、クラウドサービスに預けた情報が漏洩すること、設定不備やクラウドサービスにおける障害波及のリスクがあること、等の懸念事項も生じる。クラウドサービスにおける暗号鍵管理システムを適切に選択・構築・運用することによって、そうした懸念事項に対処できる部分がある。クラウドサービスにおける暗号鍵管理の仕組みや注意事項を解説したガイダンスを作成し、クラウド環境で安全に暗号を運用するための一つのガイダンスとする。

本ガイダンスの想定読者については以下とした。

クラウドサービスを利用した情報システムの構築者（SI 事業者）、運用者、利用者。

本ガイダンスのスコープは以下のように整理した。

IaaS や PaaS のクラウドサービスを利用して、情報システムのプラットフォーム構築を行うケースを対象に、どのような鍵管理サービスを提供すべきかをターゲットとする。暗号機能による保護の対象はクラウドサービスに預けたデータ及び鍵情報の機密性と完全性の確保、並びに暗号化消去とする。

② 記載内容のポイントについて

本ガイダンス記載内容のポイントとなる事項について、以下の点を設定した。ただし、詳細はガイダンス作成の過程で再度議論する。

- ・ クラウド鍵管理サービスの分類
クラウドサービスプロバイダ(GSP)が提供する鍵管理サービスを体系化し、ユースケースに応じてどのような鍵管理サービスを利用すべきかを判断できる情報を提供する。

- クラウド鍵管理サービスに関わる責任分界について
クラウドサービス利用時の鍵管理システムに関わる CSP との責任分界について、クラウド鍵管理サービスの種類に応じて原則となる考え方を整理する。その際、クラウドサービスモデルに依存する部分があるかについても現状を整理する。
- 暗号鍵管理ガイダンス（NIST SP 800-130）の Framework Requirement との関係
暗号鍵管理ガイダンスにおいて解説している検討項目（Framework Requirement）について、クラウドサービス利用時はどのように検討されるべきかを記載する。現在の暗号鍵管理ガイダンスでは、オンプレミスに構築した CKMS をトイモデルに設定して検討項目への対応例を記載しているため、クラウドサービスを利用した場合に重点的に検討すべき項目や対応例がどのように変わるかを説明する。

③ 作成スケジュールおよび検討体制

本ガイダンスの作成にあたって、2025 年度より WG を新しく設置することとなった。WG 委員として CSP 事業者、SI 事業者・SaaS 事業者、クラウド HSM ベンダ、クラウドサービス利用者、大学や関連団体などの有識者にそれぞれ参画いただき、事務局を中心に委員の知見をまとめる形で作成を進める。

作成スケジュールについては、WG の任期である 2 年間で遅くとも本ガイダンスの作成を行う計画である。ただし、技術やサービスの進展が早い領域でもあるため、計画は柔軟に捉えることとする。

3.2.4. 暗号技術活用委員会の開催状況

2024年度の暗号技術活用委員会での審議概要は表3.2-2の通りである。

表3.2-2 暗号技術活用委員会の開催状況

回	開催日	議案
メール	2024年6月	● 2024 年度暗号鍵管理ガイダンス WG 活動計画の審議
第一回	2024年10月28日	● 2024 年度暗号技術活用委員会活動計画の確認 ● 2024 年度暗号鍵管理ガイダンス WG 活動計画の確認 ● 暗号鍵管理ガイダンス WG 進捗報告 ● クラウドにおける鍵管理ガイダンスについて
第二回	2025年3月4日	● 2024 年度暗号鍵管理ガイダンス WG 活動報告及びガイダンス案の審議 ● クラウドにおける鍵管理ガイダンスについて ● 2024 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、2025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に鑑み、引き続き暗号技術調査ワーキンググループ（耐量子計算機暗号）を設置して、耐量子計算機暗号に関する最新動向を把握するとともに、社会的動向を踏まえてNIST標準として公開されたFIPS-203, 204, 205について安全性評価・実装性能評価関連の活動を開始する予定である。

暗号技術活用委員会においては、新たなガイダンスとして作成方針を検討した「クラウドにおける鍵管理ガイダンス（仮称）」について、新たなWGを設置して同ガイダンスの作成を本格的に開始する予定である。また、暗号技術検討会に応じて、耐量子計算機暗号をめぐる社会的動向を踏まえ、耐量子計算機暗号の取扱い基準や運用ガイドライン／ガイダンスにおける耐量子計算機暗号の位置づけ・記載内容等についての検討を開始する予定である。

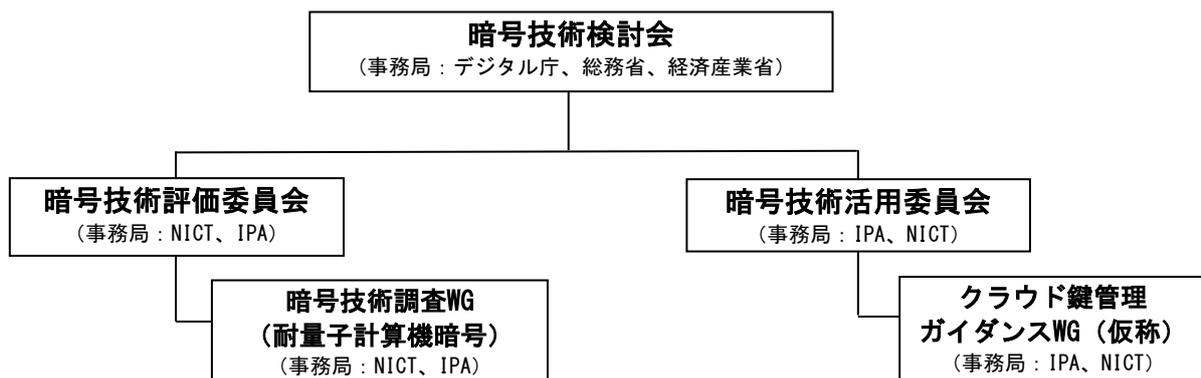


図4-1 CRYPTREC体制図（2025年度）（予定）