暗号技術検討会
２０１９年度　報告書

２０２０年６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。

2019 年度、CRYPTREC では、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、3 回の集中的な議論により、大規模な量子コンピュータの動向を踏まえた次期 CRYPTREC 暗号リストに求められる要件や、軽量暗号等の新たな暗号技術の動向等を踏まえた検討を行った。

2019 年度の各委員会の活動として、暗号技術評価委員会では、「現在の量子コンピュータによる暗号技術の安全性への影響に関する注意喚起レポート」の発行、新たに CRYPTREC 暗号リストに追加することとなった暗号利用モード XTS の評価等を行った。また、同委員会の下に設置された暗号技術調査 WG において、「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」の予測図の更新方法の検討や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ついての検討を行った。暗号技術活用委員会では、安全な暗号利用に係る運用ガイドラインを整備する観点から「暗号鍵管理システム設計指針（基本編）」及び「TLS 暗号設定ガイドライン」の作成を行った。これらの 2019 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 2019」を参照いただきたい。

なお、新型コロナウイルスの感染拡大防止の観点から 2019 年度末に予定していた暗号技術検討会を含む一部の活動を延期したため、それらの活動は形式上 2020 年度として行った。

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。

2020 年 6 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。

2019 年度の CRYPTREC においては、大規模な量子コンピュータの動向を踏まえた次期 CRYPTREC 暗号リストに求められる要件や、軽量暗号等の新たな暗号技術の動向等を踏まえた検討を行うため、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」（2019 年 7 月～）を設置し、議論を行った。

また、暗号技術評価委員会では、CRYPTREC 暗号リスト（推奨候補暗号リスト）に追加することとなった暗号利用モード XTS の実装性能評価や量子コンピュータによる共通鍵暗号の安全性への影響調査などを行い、暗号技術活用委員会では、鍵管理及び TLS に関する運用ガイドラインの整備を行った。

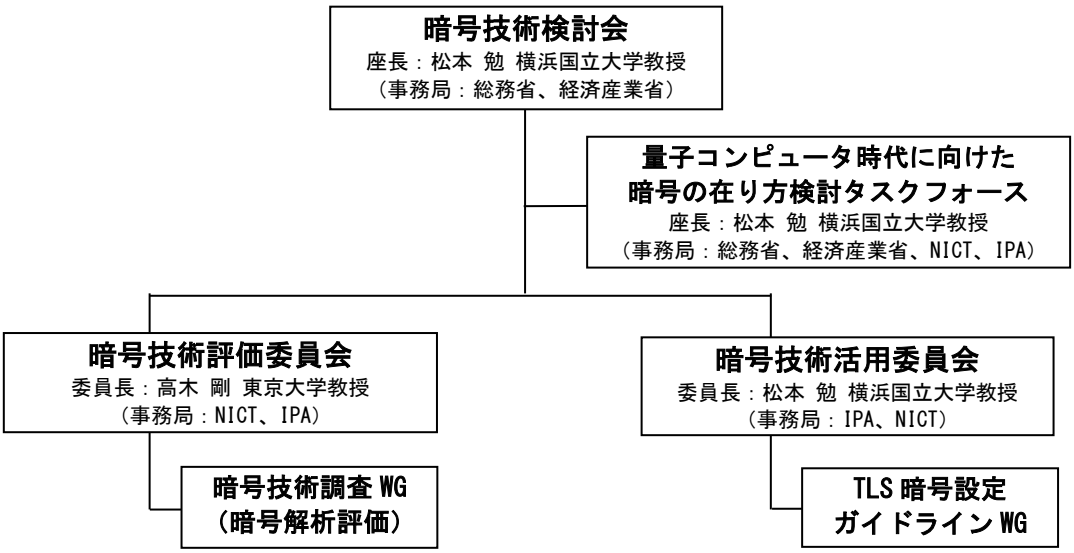

図 2.2.1　2019 年度 CRYPTREC 体制図

２．３．暗号技術検討会の開催実績

2019 年度の暗号技術検討会は、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、暗号技術評価委員会、暗号技術活用委員会の活動報告、運用監視暗号リストからの削除ルールに係る審議等を行うために 1 回開催した。なお、新型コロナウイルスの影響により当初予定の 3 月から 6 月に開催が延期されたため、形式上、2020 年度第 1 回暗号技術検討会の一部として開催された。

【第 1 回】2020 年 6 月 19 日（金）10:00～12:00

（主な議題）

- 「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」の検討状況及び活動について
- 2019 年度暗号技術評価委員会 活動報告について
- 2019 年度暗号技術活用委員会 活動報告について
- XTS の推奨候補暗号リストへの追加について
- 運用監視暗号リストからの削除ルール及び RC4 の取扱いについて
- 暗号技術検討会　2019 年度　報告書（案）について

（概要）

- 「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」の検討状況及び活動について事務局から説明があり、耐量子計算機暗号等については CRYPTREC 暗号リストには含めず別の文書とすること、2020 年度もタスクフォースを継続設置すること等について審議を行い、原案のとおり、承認された。
- 2019 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。
- XTS の推奨候補暗号リストへの追加について審議を行い、利用用途に係る記載ぶりについて一部修正の上で、推奨候補暗号リストへの追加が承認された。
- 運用監視暗号リストからの削除ルール及び RC4 の取扱いについて審議を行い、原案のとおり、

承認された。

- 暗号技術検討会 2019 年度報告書（案）について事務局より説明があり、後日、暗号技術検討会の議事概要を追記し、最終確認を行うことで承認を得た。

３．各委員会の活動報告

３．１．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

３．１．１．設置の経緯

現在の CRYPTREC 暗号リストの策定（2013 年 3 月 1 日）から 6 年が経過することもあり、量子コンピュータの動向や新たな暗号技術の動向を踏まえ、次期 CRYPTREC 暗号リストの改定方針の素案について、2018 年度の暗号技術評価委員会及び暗号技術活用委員会において議論したところ、両委員会の委員からは、改定方針よりも先に次期 CRYPTREC 暗号リストに求められる要件を明確にすべきという意見があった。

これらの議論を受けて、2018 年度第 1 回暗号技術検討会での審議の結果、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」（以下「検討 TF」という。）を設置し、次期 CRYPTREC 暗号リストに求められる要件や課題等を整理することとなった。

３．１．２．2019 年度の検討の内容

2019 年度、検討 TF では、量子コンピュータ及び耐量子計算機暗号等の技術動向について確認した上で、次のテーマについて検討を行った。

- CRYPTREC 暗号リストにおける耐量子計算機暗号の位置づけについて
- CRYPTREC 暗号リストにおける軽量暗号・高機能暗号等の位置づけについて
- CRYPTREC 暗号リストの在り方について（リスト構成・技術分類・暗号技術公募）
- 暗号技術のパラメータについて
- CRYPTREC 暗号リストの今後の改定について
- CRYPTREC の文書体系について
- 検討 TF について

特に重点的に議論がなされた項目の内容は以下のとおり。

量子コンピュータの動向について

量子コンピュータ[1]の性能は、「量子ビット数」に加えて、「ノイズ（計算誤り）」や「演算可能回数」も重要な指標である。これは、古典コンピュータでは計算誤りの発生時に訂正する機能があるため何年でも計算させ続けられるが、量子コンピュータでは誤り訂正の実現の難易度が高いためである。現在の量子コンピュータでは誤り訂正をせずに計算を行う必要があるため、コヒーレンス時間（状態が保たれている時間；現状はミリ秒程度）の中で計算を終わらせる必要があり、演算可能回数も制限されている状況である。

[1] この場合はゲート型量子コンピュータ。ほかにアニーリング型量子コンピュータも存在するが、特定の組み合わせ最適化問題を解くことを目的としたものであるため、暗号の安全性への影響の観点からはゲート型量子コンピュータの方が脅威となる。

ノイズ（計算誤り）がある場合[2]でも、化学や金融の分野では活用できる想定だが、現状のノイズは暗号解読のための素因数分解に活用できる水準ではない。

また、一般的に、各社が開発している量子コンピュータについて、量子ビット数は公表されているが、ノイズや演算可能回数に関する情報はあまり公表されないため、計算性能に関する将来予測は困難であるが、現状、暗号解読ができるような（＝大規模でノイズの少ない）量子コンピュータ[3]の実現時期は見えていない。つまるところ、量子コンピュータによって従来暗号が破られる状況はすぐに到来する可能性は低いことに留意が必要である。

しかしながら、耐量子計算機暗号への移行には長期間を要することが想定されるため、量子コンピュータの開発の進展によって暗号が危殆化する時期を可能な限り把握する必要があることから、公表されている量子ビット数の動向を確認し続けることが必要である。

CRYPTREC 暗号リストにおける耐量子計算機暗号の位置づけについて

現行の CRYPTREC 暗号リスト（電子政府推奨暗号リスト）は、暗号技術の安全性等の評価に加え、利用実績や普及見込みも考慮した上でリスト化がされている。一方、耐量子計算機暗号は、現状、多数の方式が提案され、安全性等の検討が行われている状況であり、利用実績や普及見込みに言及できる段階にない。そのため、耐量子計算機暗号については、CRYPTREC 暗号リストとは別文書（ガイドライン等）を新たに作成することが適当である。ただし、新たに作成する文書（以下「ガイドライン」という。）は、ガイドラインの重要性がわかるようとりまとめるべきである。

ガイドラインとして別文書とすることで、利用者視点としても、量子コンピュータへの脅威がない場合の従来リストと、量子コンピュータへの脅威を考える必要がある場合の量子コンピュータ時代の安全性という観点でまとめたガイドラインとで、それぞれの用途に応じて分けて捉えられ、有効な使い方ができるものと考えられる。

ガイドラインの作成に当たっては、NIST 等の他のアクティビティが実施している取組も参考にしていくことが適当である。また、公開鍵暗号方式だけでなく、共通鍵暗号方式に対する影響についても言及すべきである。

なお、日常的に耐量子計算機暗号を使用することが必要となった場合は、CRYPTREC 暗号リスト本体に位置づけられることを妨げるものではない。

CRYPTREC 暗号リストにおけるリスト構成について

CRYPTREC 暗号リストは、

①電子政府推奨暗号リスト[4]

---

[2] NISQ（Noisy Intermediate-Scale Quantum Computer）。Google 社、IBM 社、Intel 社等が開発している。

[3] 素因数分解された最大の数は「21」であるが、その数に特化した方法で計算しており汎用的な素因数分解に適用できるものではない。暗号解読のためには、汎用的な方法により、数百桁程度の素因数分解が必要となる。

[4] CRYPTREC により安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

②推奨候補暗号リスト[5]

③運用監視暗号リスト[6]

の３リスト構成となっている。

「①電子政府推奨暗号リスト」については、安全性及び実装性能が確認された暗号技術を推奨するものであり、また、「③運用監視暗号リスト」については、危殆化等により推奨すべきではなくなった暗号技術を周知するものである。このため、両者については、それぞれの性質から引き続き維持（利用）していくことが望ましい。

しかしながら、そもそも現行の CRYPTREC 暗号リストの改定時に「②推奨候補暗号リスト」を含めた３リスト構成としたのは、国産暗号技術の普及展開を促進することもその目的の一つ[7]であったものの、現在の状況は３リスト構成とした意図が十分に活用されているとは言いがたい。

一方で、「②推奨候補暗号リスト」は、（利用実績等が十分でないものの）安全性及び実装性能が確認されていることから、将来的に「①電子政府推奨暗号リスト」に載る可能性がある暗号アルゴリズムの受け皿としての機能もある。

このため、現状の「②推奨候補暗号リスト」には、将来的に普及することが予想され「①電子政府推奨暗号リスト」に載る可能性がある暗号技術と、掲載から十分な期間を経てもあまり普及したとは言えない暗号技術とが混在している状況にあるが、「②推奨候補暗号リスト」から暗号技術を削除する際の基準や手続きが定まっていない。

こうした状況を踏まえると、「②推奨候補暗号リスト」については、その意義・必要性について更なる検討を行う必要がある。このため、３リスト構成の望ましい在り方について、引き続き検討が必要である。

暗号技術のパラメータについて

これまで、CRYPTREC では、推奨する暗号技術（暗号アルゴリズム）を CRYPTREC 暗号リストにより示してきたが、パラメータについては積極的な提示は行ってこなかった。

米国では、NIST SP800-57 や SP800-131A 等において、推奨パラメータを示しており、こうした推奨パラメータの明示は、危殆化対策としての安全なシステム構築や計画的な暗号技術の移行を促進するために有用である。

こうした状況を踏まえ、CRYPTREC においても、推奨パラメータについて提示していくこととし、この際、推奨パラメータを CRYPTREC 暗号リストに埋め込むのではなく、CRYPTREC 暗号リストは（引き続き）推奨する暗号技術（アルゴリズム）を規定するものとして用いることが適当である。つまり、推奨パラメータを規定する別の文書を新たに作成し、CRYPTREC 暗号リストから当該文書を参照する構成とすることが適当である。

なお、推奨パラメータについては、利用環境や技術の進展に依存すること、相互接続性などを踏まえて検討を行う必要があること、そして産業界をはじめとして多方面に影響を及ぼす重要なもの

---

[5] CRYPTREC により安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト。

[6] 実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったと CRYPTREC により確認された暗号技術のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。

[7] 2011 年度第 1 回暗号技術検討会資料 3-2

であることに留意が必要である。

３．１．３．検討結果概要

2019 年度、検討 TF における検討結果概要は以下のとおり。

○　耐量子計算機暗号、軽量暗号、高機能暗号は、CRYPTREC 暗号リストには含めず、それぞれ別の文書とする。また、当該文書の重要性がわかるよう、取りまとめたものとする。
○　2023 年目途の CRYPTREC 暗号リストの改定について、現行の３リスト構成の在り方については引き続き検討が必要であるものの、技術分類については現行のものを踏襲し、公募は行わない方針とする。
○　推奨される暗号のパラメータについて、CRYPTREC 暗号リストから参照する形で別の文書としてまとめる方針とする。
○　これらの新たな文書も含め、CRYPTREC 暗号リストを含む CRYPTREC の文書の位置付けを整理する。
○　量子コンピュータや耐量子計算機暗号の状況をフォローするため、及び引き続き継続検討とした内容の議論を行うため、2020 年度以降も検討 TF の継続設置を提案する。

３．１．４．2019 年度の開催状況

2019 年度、検討 TF は 3 回開催した。会合の概要は表 3.1 のとおり。

表 3.1　検討 TF の開催実績

回	年月日	主な議題
第 1 回	2019 年 6 月 24 日	・量子コンピュータの動向について ・耐量子計算機暗号の動向について
第 2 回	2019 年 9 月 6 日	・CRYPTREC 暗号リストにおける耐量子計算機暗号の扱いについて ・軽量暗号の動向について ・CRYPTREC 暗号リストにおける軽量暗号、高機能暗号の扱いについて
第 3 回	2019 年 12 月 24 日	・CRYPTREC 暗号リストに関する論点等について - CRYPTREC 暗号リストの在り方 - 暗号技術のパラメータ - CRYPTREC 暗号リストの今後の改定 - CRYPTREC の文書体系

３．２．暗号技術評価委員会

３．２．１．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
・新世代暗号に係る調査

これらの課題について 2019 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。

３．２．２．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 2019（暗号技術評価委員会報告）に掲載する。

３．２．３．暗号技術調査ワーキンググループ（暗号解析評価）

2019 年度暗号技術評価委員会活動計画における「新技術等に関する調査及び評価」の活動として下記二点について実施することが暗号技術検討会において承認された。

- 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
- 「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」の予測図の在り方についての検討

暗号技術評価委員会では暗号技術調査ワーキンググループ（暗号解析評価）（以下「暗号解析評価 WG」という。）を継続し、上記二件について実施した。それらの成果（３．２．３．１～３．２．３．２節）は 2019 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。

３．２．３．１．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

背景及び実施内容

近年、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）の調査・検討が各国で進められている。特に米国では NIST が公開鍵暗号について PQC を公募し、現在では提案された暗号方式の安全性評価が進められている。

2018 年度の暗号技術評価委員会において、量子コンピュータを使用した共通鍵暗号の解読に関する論文が近年、増加していることが委員から指摘されている。量子コンピュータによる共通鍵暗号の安全性への影響の調査について、外部専門家による評価を依頼することが、第 1 回暗号技術評価委員会（2019 年 6 月 28 日）で承認され、具体的な評価内容が、第 1 回暗号解析評価 WG（2019 年 7 月 29 日）にて承認された。

【件名】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

【依頼内容】大規模な量子コンピュータによる解析を想定した場合の共通鍵暗号の安全性への影響について、安全性評価及び調査を行う。具体的には以下の内容を評価レポートに入れる。

1) 本評価結果の概要（エグゼクティブサマリー）
2) 量子コンピュータを用いた共通鍵暗号に対する解析の重要性について
3) 量子コンピュータを用いた共通鍵暗号に対する攻撃モデルの解説
4) 量子コンピュータを用いた共通鍵暗号への攻撃について、公開されている攻撃の調査
5) 現在の電子政府推奨暗号リストに含まれる主要な方式や将来電子政府システム等で利用が見込まれる暗号方式への影響の考察

なお、4) については、2019 年 8 月末までに公開された攻撃を調査対象とする。5) については、網羅性は問わない。

【依頼先】細山田 光倫 様 （NTT セキュアプラットフォーム研究所）

【2019 年度のスケジュール】

・2019 年 7 月 29 日 第 1 回 暗号解析評価 WG：活動内容の審議・承認
・2020 年 1 月 24 日 第 2 回 暗号解析評価 WG：調査結果の報告の審議・承認

外部評価報告書に対する暗号解析評価 WG の見解

外部評価報告書の評価結果は妥当であると判断する。本評価結果により、CRYPTREC の電子政府推奨暗号リストにある共通鍵暗号、暗号利用モード、ハッシュ関数について、量子コンピュータを用いた攻撃による直近で現実的な脅威が生じる可能性は極めて低く、現状では CRYPTREC での具体的な対応は不要である。ただし、Even-Mansour 暗号への攻撃のように安全性に現実的な影響を及ぼす可能性がある攻撃が発見される可能性もあるため、攻撃手法および量子コンピュータの発展に関して継続的な監視・評価が必要である。

なお、今回の評価は電子政府推奨暗号リストに掲載されている共通鍵暗号を対象にしているが、推奨候補暗号リストに掲載されている共通鍵暗号も Even-Mansour 暗号や FX 構成への攻撃をそのまま応用できるものではないことから同様の評価結果になると考えられる。

３．２．３．２.「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」の予測図の在り方についての検討

「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 4)(January,2016)」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。これを踏まえ、以下について検討を行った。

(1) 今後の予測図の取り扱い
(2) 今後の公開鍵暗号のパラメータ選択

今後の予測図の取り扱いについて

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

〈今後の予測図の取り扱い〉

(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今まで引いていた範囲（2040 年[8]）まで直線で引き、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当面の間更新していくことを本 WG として提案する。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ことを本 WG として提案する。

予測図の更新について

上述の対応方針に基づいて、予測図の更新を下記の通り行った（図 3.2.1 及び図 3.2.2）。なお、主な変更点は以下の通りである。

- 篩処理の評価を 2006 年度版に基づく評価から 2018 年版（表 3.2.1）に基づく評価[9]に変更した。

表 3.2.1: 篩処理時間の推測結果（単位は、Intel Xeon E5-2680 v3 2.5GHz コア・年）

法サイズ（ビット）	768	1024	1536	2048
見積もり	561.99	1.52×10^{6}	0.92×10^{12}	1.28×10^{17}

- 近年、ハードウェアを用いた新たな研究成果が無く、古い情報のみに依存した信頼性の低い評価となるため、「専用ハードウェアとソフトウェア処理との性能比較」に対応する外挿線は削除した。
- FactorWorld のサイト[10]がなくなったので、Integer Factoring Records のサイト[11]に変更した。
- 3072 ビット RSA と 256 ビット ECDLP に関する計算量を表す横線（点線）を入れた。なお、3072 ビット RSA に関する横線については他のビット長とは異なる評価方法であるため、より精度を高めるためにはさらなる検討が必要である。

---

[8] 当該範囲については、ルート証明書の有効期限の長いものがあるため、第 2 回暗号技術評価委員会（2020 年 2 月 18 日開催）において、現在（2020 年）から 20 年後まで安全であることを分かり易く示すことが必要であると決定された。

[9] Evaluation of complexity of the sieving step of the general number field sieve, T. Kleinjung and A. K. Lenstra, December 5, 2018, https://www.cryptrec.go.jp/exreport/cryptrec-ex-2802-2018.pdf

[10] http://www.crypto-world.com/FactorWorld.html

[11] https://members.loria.fr/PZimmermann/records/factor.html

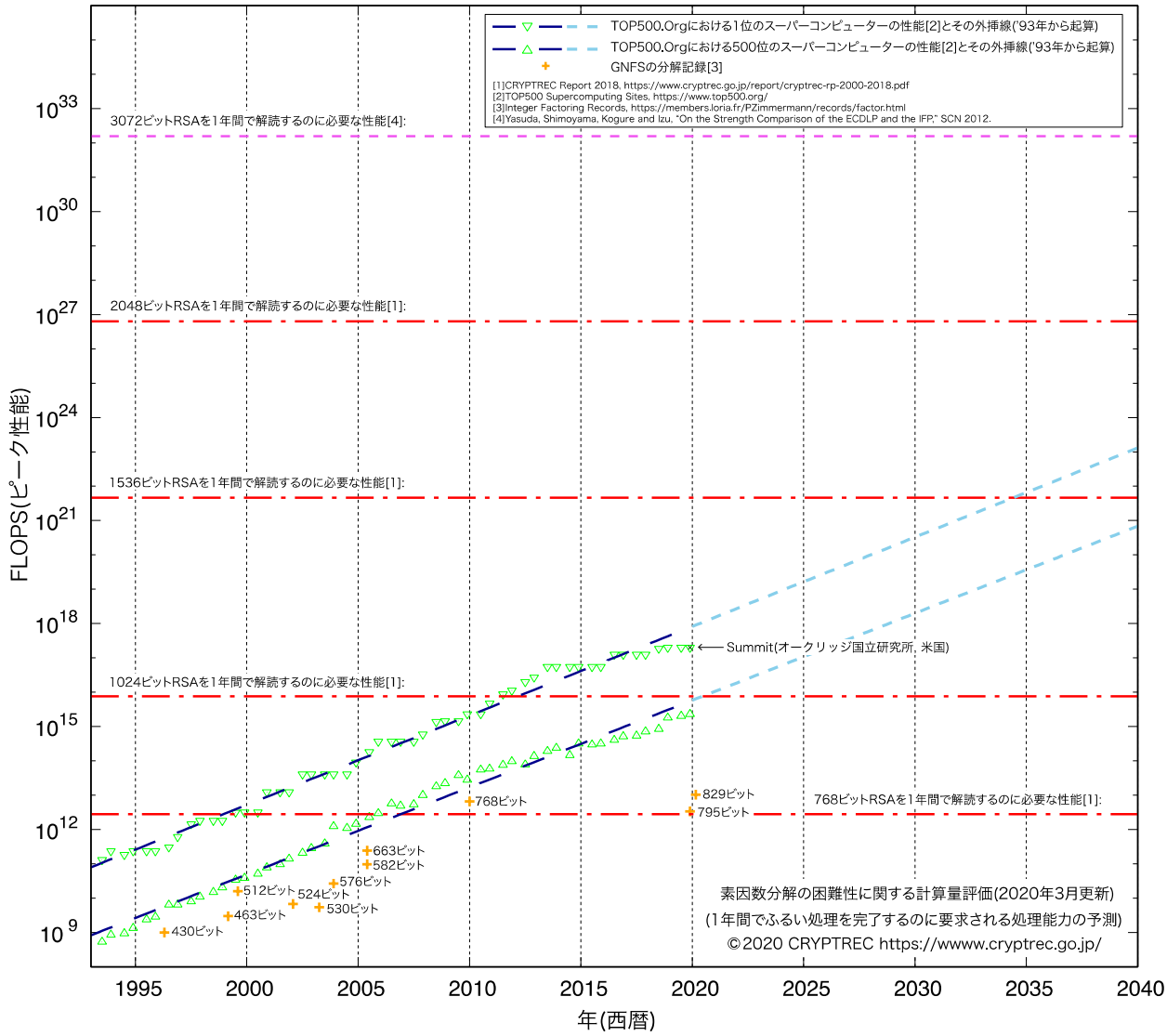

図 3.2.1：素因数分解の困難性に関する計算量評価
（1 年間でふるい処理を完了するのに要求される処理能力の予測、2020 年 3 月更新）[12]

[12] 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。

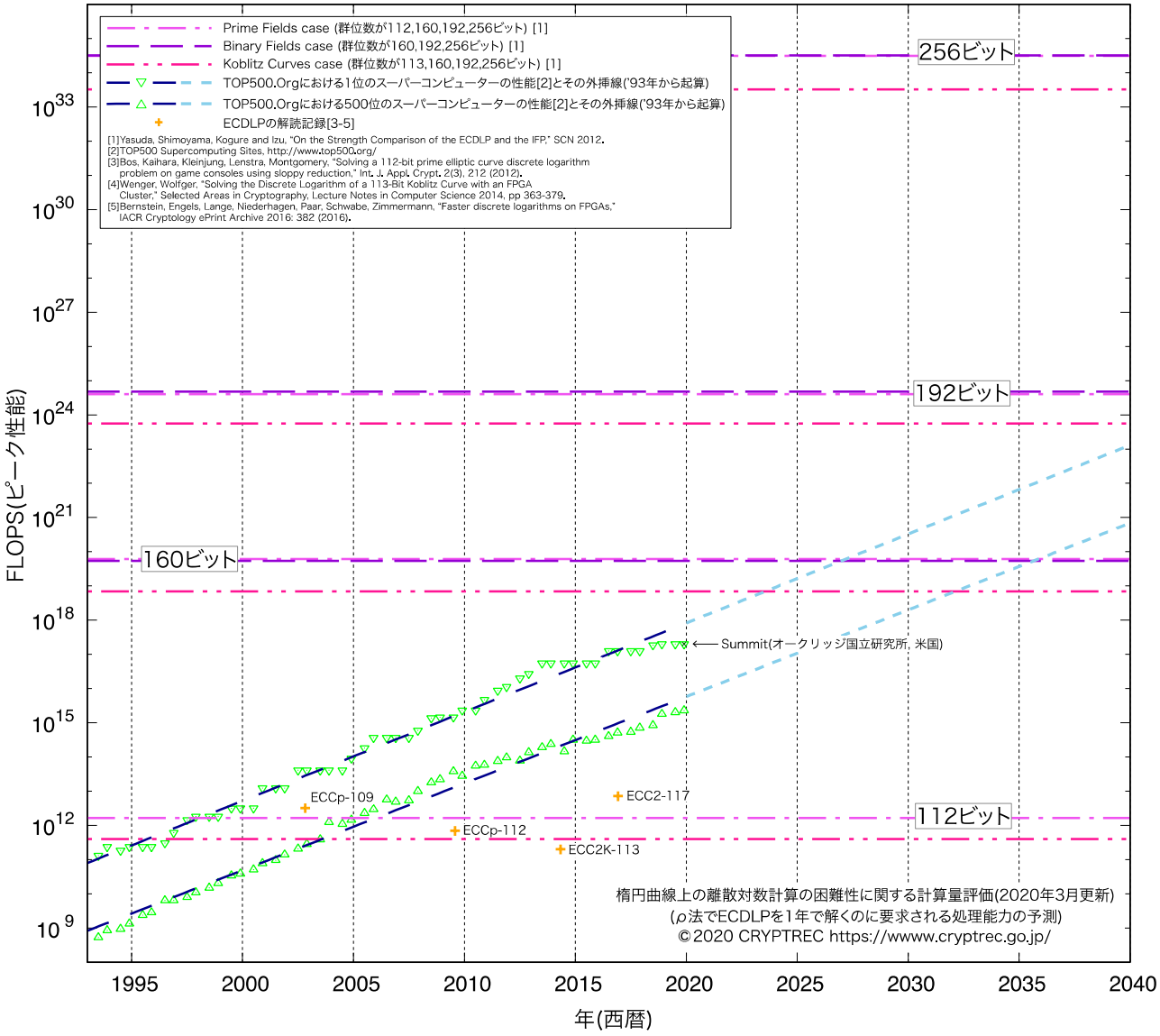

図 3.2.2：楕円曲線上の離散対数計算の困難性に関する計算量評価
（ρ法で ECDLP を 1 年で解くのに要求される処理能力の予測、2020 年 3 月更新）[13]

[13] 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。

３．２．４．推奨候補暗号リストへの新規暗号（事務局選出）の追加

暗号利用モード XTS 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た。

安全性評価については、2018 年度に実施済みであり、2019 年度第 2 回暗号技術評価委員会（2019 年 3 月 11 日）にて、下記の見解を得ていた。

> XTS モードは、下記 3 点の条件下では、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。
>
> (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)同一の鍵を用いて暗号化する場合、2^{20}ブロックまでとする。

今年度、第 2 回暗号技術評価委員会（2020 年 2 月 18 日開催）の審議により、(条件 3)は表現が不明瞭であり、また、意図した内容は、参照先仕様書にその制限事項の記載があることから、(条件 1)に包含されるとの解釈のもと、(条件 3)を安全性要件を満たす条件から削除することした。また、(条件 1)は、冗長性が高かったため、表現の改善を行った。

最終的に、安全性要件を満たす条件は下記の通りとなった。

> 安全性要件を満たす条件：
>
> 1) 利用用途は NIST SP800-38E の規格に沿ったストレージデバイスの暗号化に限る。
>
> 2) XTS 内のブロック暗号には、CRYPTREC 暗号リスト掲載 128 ビットブロック暗号を使う。

以上の議論を踏まえ、2018 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、暗号利用モード XTS は、安全性要件を満たす条件の下で、暗号利用モード（秘匿モード）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。上記判断に基づき、XTS 利用モードは CRYPTREC 暗号リストに掲載するために十分な安全性および実装性能を満たしていると判断し、CRYPTREC 暗号リストへの追加を暗号技術検討会に提言した。併せて、追加先としては、大分類「暗号利用モード」_中分類「秘匿モード」とすること、安全性要件を満たす条件を注釈につけることを提言した。

2020 年度第 1 回暗号技術検討会（2020 年 6 月 19 日）の審議結果により、暗号技術評価委員会の提言が承認され、暗号利用モード XTS は、CRYPTREC 暗号リストに追加されることとなった。付随する注釈については、改善を図り下記の表現に確定した。

> XTS に添える注釈：
>
> ブロック暗号には、CRYPTREC 暗号リスト掲載 128 ビットブロック暗号を使う。
>
> 利用用途はストレージデバイスの暗号化に限り、実装方法は NIST SP800-38E に従うこと。

３．２．５．仕様書の参照先の変更

CRYPTREC の Web サイトでは、CRYPTREC 暗号リストに掲載している暗号技術の仕様書の参照先（https://www.cryptrec.go.jp/method.html）を記している。その中で、電子政府推奨暗号リストに掲載されている RSA 暗号（RSA-PSS、RSASSA-PKCS1-v1_5、RSA-OAEP 及び運用監視暗号リストに掲載されている RSAES-PKCS1-v1_5）に関する URL がリンク切れのため、新旧仕様書の差分が軽微な修正であると判定し（表 3.2.2）、参照先の変更を行った（表 3.2.3）。

表 3.2.2：RSA 暗号の新旧仕様書

暗号技術名	旧仕様書	新仕様書
RSA-PSS	EMC Corporation Public-Key Cryptography Standard (PKCS), PKCS #1 v2.2: RSA Cryptography Standard (October 27, 2012)	Internet Engineering Task Force (IETF) Request for Comments: 8017, PKCS #1: RSA Cryptography Specification Version 2.2 (November 2016)
RSASSA-PKCS1-v1_5		
RSA-OAEP		
RSAES-PKCS1-v1_5	http://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf	https://tools.ietf.org/html/rfc8017

表 3.2.3：判定結果とその理由

暗号技術名	判定結果	理由	備考
RSA-PSS	仕様書の参照先の変更を認める。	アルゴリズム部分に変更なし。	・誤記等の軽微な修正はいくつか存在するが、章・節の構成及び記述内容にほぼ変更はない。 ・旧版では、「F. Intellectual Property Considerations」があったが、新版ではなくなった。 ・新版では、「10. Security Considerations」、「Acknowledgements」と「Authors' Addresses」が出来た。
RSASSA-PKCS1-v1_5			
RSA-OAEP			
RSAES-PKCS1-v1_5			

３．２．６．暗号技術評価委員会の開催実績

2019 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 3.2.1 のとおりである。

表 3.2.1　暗号技術評価委員会の開催状況

回	開催日	議案
第 1 回	2019 年 6 月 28 日	■ 暗号技術調査ワーキンググループ（暗号解析評価）の活動計画案の審議 ■ 外部評価（暗号利用モード XTS の実装性能に関する調査及び評価）実施についての審議 ■ 監視状況報告
第 2 回	2020 月 2 月 18 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 ■ 外部評価（暗号利用モード XTS の実装性能に関する調査及び評価）実施報告 ■ 注意喚起レポート発行の報告 ■ 仕様書参照先変更の報告 ■ 監視状況報告

３．３．暗号技術活用委員会

３．３．１．活動の概要

2019 年度は、安全な暗号利用に係る運用ガイドラインを整備する観点から、主に以下の活動を行った。

- 「暗号鍵管理システム設計指針（基本編)」の作成
- 「TLS 暗号設定ガイドライン」の作成

３．３．２．2019 年度の活動内容

暗号鍵管理システム設計指針（基本編）の作成

あらゆる分野・あらゆる領域の全ての暗号鍵管理システム（以下「CKMS(Cryptographic Key Management System)」という。）を対象に、暗号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（Framework Requirements）を網羅的に提供し、設計時に考慮すべきトピックス及び設計書等に明示的に記載する要求事項を取りまとめた「暗号鍵管理システム設計指針（基本編)」を完成させた。

ダウンロード先:

https://www.cryptrec.go.jp/op_guidelines.html

https://www.ipa.go.jp/security/vuln/ckms.html

位置づけ

- 本設計指針は、セキュアな暗号アルゴリズムを利用する上で極めて重要な役割を果たす暗号鍵の管理に関する在り方を解説し、CKMS を設計・構築・運用する際に参考すべきドキュメントとして作成された。
  - 「暗号鍵管理の在り方」(暗号鍵管理の位置づけと検討すべき枠組み）では、暗号鍵管理の必要性を認識してもらうための解説を記載した。これは、あらゆる暗号鍵管理を検討する際の基礎となる考え方を示したものである。
  - 「暗号鍵管理についての技術的内容」では、包括的な CKMS 設計指針である NIST SP800-130「A Framework for Designing Cryptographic Key Management Systems」の解説書・利用手引書として活用できるように構成した。本設計指針では、SP800-130 での Framework Requirements を『暗号鍵管理における目的に応じた』対象範囲に分類・再構成することによってそれぞれの検討項目の目的や必要性を明確化した。
- 本設計指針は、あらゆるユースケースにおける暗号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一覧を提供し、CKMS 設計時に考慮すべきトピックス及び設計書等に明示的に記載する要求事項を示している。
- ただし、本設計指針の中ではセキュリティ要求事項は定義せず、具体的な特定のセキュリティ機能の採用を義務づけることもしない。それぞれの要求事項に対してどのように対応（例えば、ポリシー、暗号アルゴリズム、デバイス等の選択）するかは CKMS 設計者に委ねられ、それらの対応方針が設計仕様書や運用マニュアル等に記載される。

- CKMS 設計者が選択した対応方針が適正かどうかの判断は運用管理者や調達責任者が行う。適切ではないと判断した場合には、CKMS 設計のやり直しを指示すべきである。確認にあたってはチェックリストも活用されたい。

本設計指針の特長

本設計指針の最大の特長は、暗号鍵管理の考え方の枠組みを整理し、暗号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点にある。大きくは 4 つの視点からなる。

詳細については、本ガイドライン及び CRYPTREC Report 2019 暗号技術活用委員会報告を参照されたい。

TLS 暗号設定ガイドラインの作成

SSL/TLS 暗号設定ガイドライン（version 1.x/2.x）発行以降、TLS1.3 発行[RFC8446]及び SSL3.0 禁止[RFC7525]、ChaCha20-Poly1305 追加[RFC7905]及び RC4 禁止[RFC7465]など、現行ガイドラインに記載の内容に大きく影響する規格化が相次いで行われており、それに伴い SSL/TLS の利用環境も大きく変化した。

そこで、TLS 暗号設定ガイドライン WG を設置して、ガイドラインの中身を 2020 年 3 月時点における TLS 通信での安全性と相互接続性のバランスを踏まえた TLS サーバの暗号設定方法に大幅な見直しを行い、TLS 暗号設定ガイドラインを完成させた。

ダウンロード先：

https://www.cryptrec.go.jp/op_guidelines.html

https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

位置づけ

- 「暗号技術以外の様々な利用上の判断材料も加味した合理的な根拠」を重視して現実的な利用方法を目指している。具体的には、実現すべき安全性と必要となる相互接続性とのトレードオフを考慮する観点から、安全性と相互接続性を踏まえたうえで設定すべき要求設定として 3 つの設定基準（「高セキュリティ型」「推奨セキュリティ型」「セキュリティ例外型」）を提示している。
- 実際にどの設定基準を採用するかは、安全性の確保と相互接続の必要性の両面を鑑みて、サーバ管理やサービス提供に責任を持つ管理者が最終的に決定すべきことではあるが、本ガイドラインでは、安全性もしくは相互接続性についての特段の要求がなければ「推奨セキュリティ型」の採用を強く勧める。本ガイドラインの作成時点（2020 年 3 月）では、「推奨セキュリティ型」がもっとも安全性と相互接続性のバランスが取れている要求設定であると考えている。

主な改訂内容

主な改訂内容は以下の通り。詳細については、本ガイドライン及び CRYPTREC Report 2019 暗号

技術活用委員会報告を参照されたい。

A) TLS1.3 の採用及び SSL3.0 の禁止に伴う各設定基準における要求設定の変更

プロトコルバージョンの要求設定において TLS1.3 の採用及び SSL3.0 の禁止が行われた。これに伴い、各設定基準における要求設定についても大幅な変更が行われており、現行ガイドラインにおける設定基準から一段階高い安全性を求めるようになった項目も多い。例えば、推奨セキュリティ型で利用が認められていた TLS1.0 や TLS1.1 は、本ガイドラインではセキュリティ例外型のみで利用可能となった。また、鍵交換では Perfect Forward Secrecy の特性をもつ ECDHE や DHE をさらに強く推奨するようにした。

B) 要求設定における「遵守項目」と「推奨項目」の区分けの新設

現行ガイドラインでは、全ての設定項目について一律に「要求設定」と位置付けていた。

今回は、設定項目のおける安全性への寄与度を考慮し、TLS 暗号設定ガイドライン（version 3.x）では、選択した設定基準としての最低限の安全性を確保するために必ず満たさなければならない「遵守項目」と当該設定基準としてよりよい安全性を実現するために満たすことが望ましい「推奨項目」とに分け、より現実的かつ実効性が高い要求設定とした。

C) 章構成の変更

現行ガイドラインでは、

- プロトコルバージョンの設定（4 章）
- サーバ証明書の設定（5 章）
- 暗号スイートの設定（6 章）

の章構成とし、各章に「高セキュリティ型」「推奨セキュリティ型」「セキュリティ例外型」の設定項目を記載していた。

今回、章構成を見直し、TLS 暗号設定ガイドライン（version 3.x）では、

- 推奨セキュリティ型の要求設定（4 章）
- 高セキュリティ型の要求設定（5 章）
- セキュリティ例外型の要求設定（6 章）

の章構成とし、各章に「プロトコルバージョン」「サーバ証明書」「暗号スイート」の設定項目を記載した。これにより、選択した設定基準での該当章だけを参照すればよい構成とした。

EdDSA に関する安全性評価の必要性についての検討

EdDSA は、TLS1.3 で採用された署名アルゴリズムである（RFC 8446）。さらに、TLS1.2 以前では、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）。

暗号技術活用委員会では、今後 EdDSA の利用が進み、TLS 暗号設定ガイドラインに EdDSA を推奨暗号スイートに含めるか否かの判断が迫られた際に速やかに対応できるように準備をしておく観点から、EdDSA に対して CRYPTREC 暗号リストへの掲載是非に資するレベルでの安全性評価を実施することが必要であるとの結論を取りまとめた。併せて、EdDSA では利用する楕円曲線パラメータが Ed25519 と Ed448 であるため、楕円曲線パラメータについて、Ed25519 が P-256 と、Ed448 が P-

384 と同程度の安全性を有する楕円曲線パラメータであるかどうか評価することの必要性も指摘した。

RC4 の運用監視暗号リストからの削除についての検討

RC4 は運用監視暗号リストに掲載されており、かつ（注 10）として「互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。SSL/TLS での利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。」と記載されている。また、平成 15 年～平成 25 年に使われていた前の電子政府推奨暗号リストにおいても、「128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。」との注釈が付記されている。

今回、TLS 暗号設定ガイドラインにおいて RC4 が TLS での利用禁止暗号アルゴリズムに指定された以上、暗号技術活用委員会としては、RC4 を運用監視暗号リストに掲載しておく必要性がなくなったと判断し、同リストからの削除についての検討を行った。併せて、運用監視暗号リストからの削除ルール（案）の検討も行った。

【運用監視暗号リストからの削除ルール（案)】

運用監視暗号リストに掲載されている暗号アルゴリズムについて、以下の条件のいずれかを満たすと暗号技術検討会が決定した場合、同リストからの削除猶予期間を定めて周知を行ったうえで、その期間の満了後に同リストから自動的に削除する。

＜削除条件＞

1. 運用監視暗号リストに掲載している注釈で示した互換性維持のための利用形態が必要なくなり、削除が妥当と判断した場合
2. 互換性維持の継続利用として使うにしても安全性維持が極めて困難で、互換性維持の継続利用が容認できないと判断した場合
3. その他、運用監視暗号リストに掲載している必要性の根拠を満たさなくなったと判断した場合

【RC4 の運用監視暗号リストからの削除（案)】

- RC4 は削除条件 1.を満たすと判断する。RC4 を運用監視暗号リストから令和 3 年 3 月 31 日に削除する。
- CRYPTREC ホームページ等を活用し、削除する旨の周知を強化する。

３．３．３．暗号技術活用委員会の開催状況

2019 年度の暗号技術活用委員会での審議概要は表 3.3.1 のとおりである。なお、新型コロナウイルスの影響により、2019 年度第 2 回活用委員会は当初予定の 3 月から 6 月に開催が延期されたため、形式上、2020 年度第 1 回活用委員会として開催された。この他、暗号技術活用委員会とは別に、暗号設定ガイドライン WG を開催した。

表 3.3.1　暗号技術活用委員会の開催状況

回	開催日	議案
2019 年度 第 1 回	2019 年 6 月 12 日	■ 活用委員会活動計画について ■ TLS 暗号設定ガイドライン WG 活動計画について ■ 暗号鍵管理システム設計指針（基本編）ドラフト版について
2020 年度 第 1 回	2020 年 6 月 1 日	■ TLS 暗号設定ガイドライン案について ■ 暗号鍵管理システム設計指針（基本編）案について ■ EdDSA に関する安全性評価の必要性について ■ 運用監視暗号リストからの削除について

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。

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は、引き続き、量子コンピュータや耐量子計算機暗号の状況を注視しつつ、CRYPTREC 暗号リストの次回改定に向け継続検討とした内容の議論を行う。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、暗号技術の安全な利用方法に関する調査を行う。暗号技術活用委員会においては、「暗号鍵管理システム設計指針（基本編）」及び「TLS 暗号設定ガイドライン」の公開を行うとともに、新たな運用ガイドラインの作成に向けた検討を行う。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。

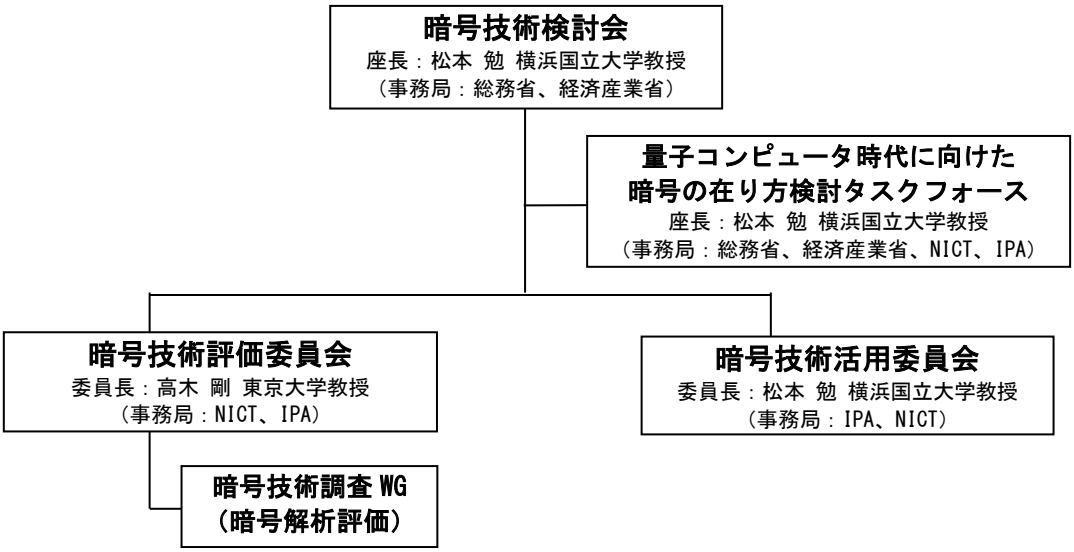

図 4.1.1 2020 年度 CRYPTREC の体制図（予定）