暗号技術検討会
２０２０年度　報告書

２０２１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。

2020年度、CRYPTRECでは、前年度に暗号技術検討会の下に設置された「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、量子コンピュータの動向及び量子コンピュータに対する暗号技術の動向について確認するとともに、CRYPTREC暗号リストにおける推奨候補暗号リストの取扱いについて検討を行った。

2020年度の各委員会の活動として、暗号技術評価委員会では、新たにCRYPTREC暗号リストへの追加を検討するため、暗号技術（署名）であるEdDSAの安全性評価を行った。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」の予測図の更新や「Shorの量子アルゴリズムによる現代暗号への脅威」に関する調査報告、「耐量子計算機暗号（PQC）の技術動向に関する調査（PQCを導入する際の技術の調査）」についての調査報告を行った。暗号技術活用委員会では、「推奨鍵長ガイドライン（仮称）」の方針案、暗号鍵管理の参照プロファイルの作成の検討を行った。これらの2020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 2020」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年度の活動の一部が形式上2020年度に行ったため、暗号技術検討会2019年度報告書において報告した以降の活動を2020年度の活動として報告する。

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。

2021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、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。

2020年度のCRYPTRECにおいては、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において、量子コンピュータの動向及び量子コンピュータに対する暗号技術の動向について確認するとともに、CRYPTREC暗号リストにおける推奨候補暗号リストの取扱いについて検討を行った。暗号技術評価委員会では、新たにCRYPTREC暗号リストへの追加を検討するため、暗号技術（署名）であるEdDSAの安全性評価を行った。暗号技術活用委員会では、「推奨鍵長ガイドライン（仮称）」の方針案、暗号鍵管理の参照プロファイルの作成の検討を行った。

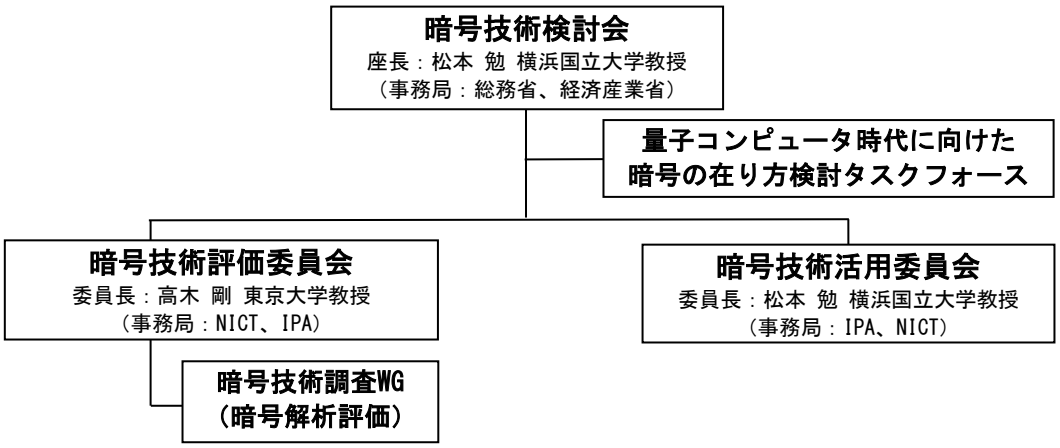

図2.2-1　2020年度CRYPTREC体制図

２．３．暗号技術検討会の開催実績

2020年度の暗号技術検討会は、2回開催した。第1回については、新型コロナウイルスの影響により2019年度の暗号技術検討会（当初は3月に開催予定）を6月に開催することとなったものであり、開催概要については「暗号技術検討会2019年度報告書(CRYPTREC RP-1000-2019)」を参照されたい。

また、第2回については、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、推奨候補暗号リストの取扱いに係る審議等を行うために開催した。

【第2回】2021年3月30日（火）10:00～11:30

（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
- 2020年度暗号技術評価委員会 活動報告について
- 2020年度暗号技術活用委員会 活動報告について
- 暗号技術検討会 2020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、CRYPTREC暗号リストについて3リスト構成を維持すること及び移行ルールを明確化することについて審議を行い、原案のとおり承認された。
- 2020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。
- 暗号技術検討会2020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．検討TF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。

３．１．２．2020年度の活動内容

2020年度、検討TFでは、量子コンピュータの動向及び量子コンピュータに対する暗号技術の動向について確認するとともに、CRYPTREC暗号リストにおける推奨候補暗号リストの取扱いについて検討を行った。

３．１．２．１．量子コンピュータの動向

2019年度の検討TFにおいて確認した次の状況に特段の変更がないことが確認された。

＜参考：暗号技術検討会2019年度報告書より抜粋＞

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。

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。

*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。
*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。

３．１．２．２．量子コンピュータに対する暗号技術の動向

耐量子計算機暗号の動向について

耐量子計算機暗号については、米国NIST（国立標準技術研究所）が標準化のための評価を実施している。耐量子計算機暗号について公募し、2017年12月から69方式についてRound 1の評価が、2019年1月から26方式についてRound 2の評価が、2020年7月から表3.1-1の7（＋α）方式についてRound 3の評価が行われている。今後、2022～2024年に標準化ドラフトが策定される予定とされている。

表3.1-1　Round 3

格子暗号	鍵交換・暗号化：CRYSTALS-KYBER、NTRU、SABER、(Frodo-KEM、NTRU Prime) デジタル署名：CRYSTALS-DILITHIUM、FALCON
符号暗号	鍵交換・暗号化：Classic McEliece、(BIKE、HQC)
多変数多項式暗号	デジタル署名：Rainbow、(GeMSS)
ハッシュ関数署名	デジタル署名：(SPHINCS+)
同種写像暗号	鍵交換・暗号化：(SIKE)
その他	デジタル署名：(Picnic)

量子コンピュータにおける素因数分解・離散対数問題について

量子コンピュータにおいてShorのアルゴリズムによる素因数分解を試みた結果として、適切に素因数分解されたと言える最大の数は21（＝3×7）であり、35（＝5×7）の素因数分解には失敗している。

2020年12月に、世界初となる量子コンピュータにおける離散対数問題の求解実験の成功について、当事者であるNICTより報告があり、2^z≡1 mod 3 については良い出力を得られているものの、2^z≡2 mod 3 については失敗している。

いずれも現在の量子コンピュータで、暗号で用いられるような大きなパラメータの問題が解けるとは考えにくい状況。

３．１．２．３．推奨候補暗号リストの取扱い

これまで（2019年度）の検討経緯

CRYPTREC暗号リストは、

①電子政府推奨暗号リスト[1]

②推奨候補暗号リスト[2]

③運用監視暗号リスト[3]

---

[1] 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] 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。

[3] 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。

の3リスト構成となっており、「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。

また、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、2019年度の検討においては、「②推奨候補暗号リスト」の意義・必要性について更なる検討を行う必要があるとされた。

推奨候補暗号リストの意義・必要性について

次の観点から、「②推奨候補暗号リスト」は維持することが適当とされた。

○　「②推奨候補暗号リスト」は、利用実績等が十分確認できていないものの、安全性及び実装性能を確認したものであることから、調達の状況（例：市場からの製品調達の際に選択性を確保する必要がない）によっては有用な場合も考えられる。

○　利用実績等の調査については、調査工数が大きく容易にできるものではないことを鑑みれば、利用実績調査までの間の予見可能性を高める観点からも、「①電子政府推奨暗号リスト」の予備軍として「②推奨候補暗号リスト」があることは有意義と考えられる。

推奨候補暗号リストの移行ルールについて

一方で、「②推奨候補暗号リスト」に長年掲載され続けている（利用実績等がない）ものもあり、掲載されている以上は、暗号技術の安全性に関する継続的な監視活動や再評価が必要となる。

今後、耐量子計算機暗号（PQC）や、軽量暗号、高機能暗号に関する評価・検討活動が必要となることから、活動リソースの最適化が必要なこともあり、「②推奨候補暗号リスト」から削除するルールを含めた、移行ルールを明確化する必要がある。

このため、移行ルールとしては次のとおり設定する。また、これを踏まえたCRYPTREC暗号リスト全体については図3.1-2のとおり。

＜「②推奨候補暗号リスト」→「①電子政府推奨暗号リスト」＞

次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

１　5年ごとの利用実績調査により、複数の利用実績を確認した場合

２　その他、普及していることが明らかな場合

＜「②推奨候補暗号リスト」→削除＞

CRYPTREC暗号リストへの掲載[4]から20年を超えた後に実施する最初の利用実績調査[5]までに、十

[4] 現行のCRYPTREC暗号リストにおいては、2003年から掲載されている暗号がある。

[5] 次回の利用実績調査は2022年を予定していることから、2003年に掲載された暗号が削除される可能性があるのは、その次の2027年の調査となる。

分な利用実績を確認できなかったもの

また、利用実績調査の具体的な実施内容・評価基準については、暗号技術活用委員会において検討し、暗号技術検討会の承認を経た上で実施する。

なお、暗号アルゴリズムの設計寿命は20年程度以上であることが期待されているが、実際にはセキュリティ向上のため、DES→TDES→AESの世代交代や公開鍵暗号の鍵長変更が20年程度で行われていることを踏まえると、20年超後に電子政府推奨暗号リストとなり活用される見込みが低いことから、削除する基準の年数として20年を設定した。

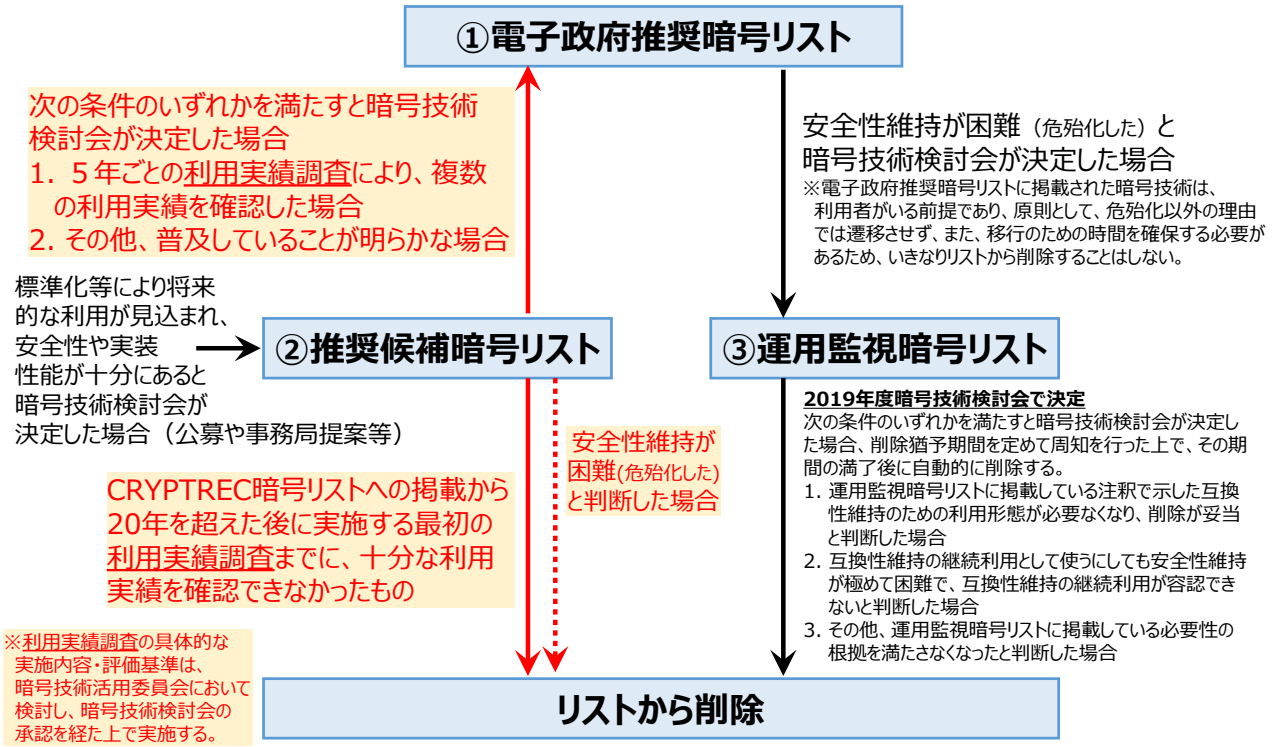

図3.1-2　CRYPTREC暗号リスト移行ルール

３．１．３．2020年度の開催状況

2020年度、検討TFは1回開催した。会合の概要は表3.1-3のとおり。

表3.1-3　検討TFの開催実績

回	年月日	主な議題
第4回	2021年3月3日	・量子コンピュータに関する動向等について ・量子コンピュータに対する暗号技術の動向等について ・CRYPTREC暗号リストでの推奨候補暗号リストの取扱いについて

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
- 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

これらの課題について2020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 2020（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）

2020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3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。

- 「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
- Shorの量子アルゴリズムによる現代暗号[6]への脅威に関する調査
- 耐量子計算機暗号(PQC)に関する技術動向に関する調査（PQCを導入する際の技術の調査）

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3点について実施した。それらの成果（３．２．３．１～３．２．３．３節）は2020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.「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

[6] 本書では、安全性が素因数分解や離散対数問題と関連する暗号方式を現代暗号と呼ぶ。

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[7]、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2020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）。

[7] 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。

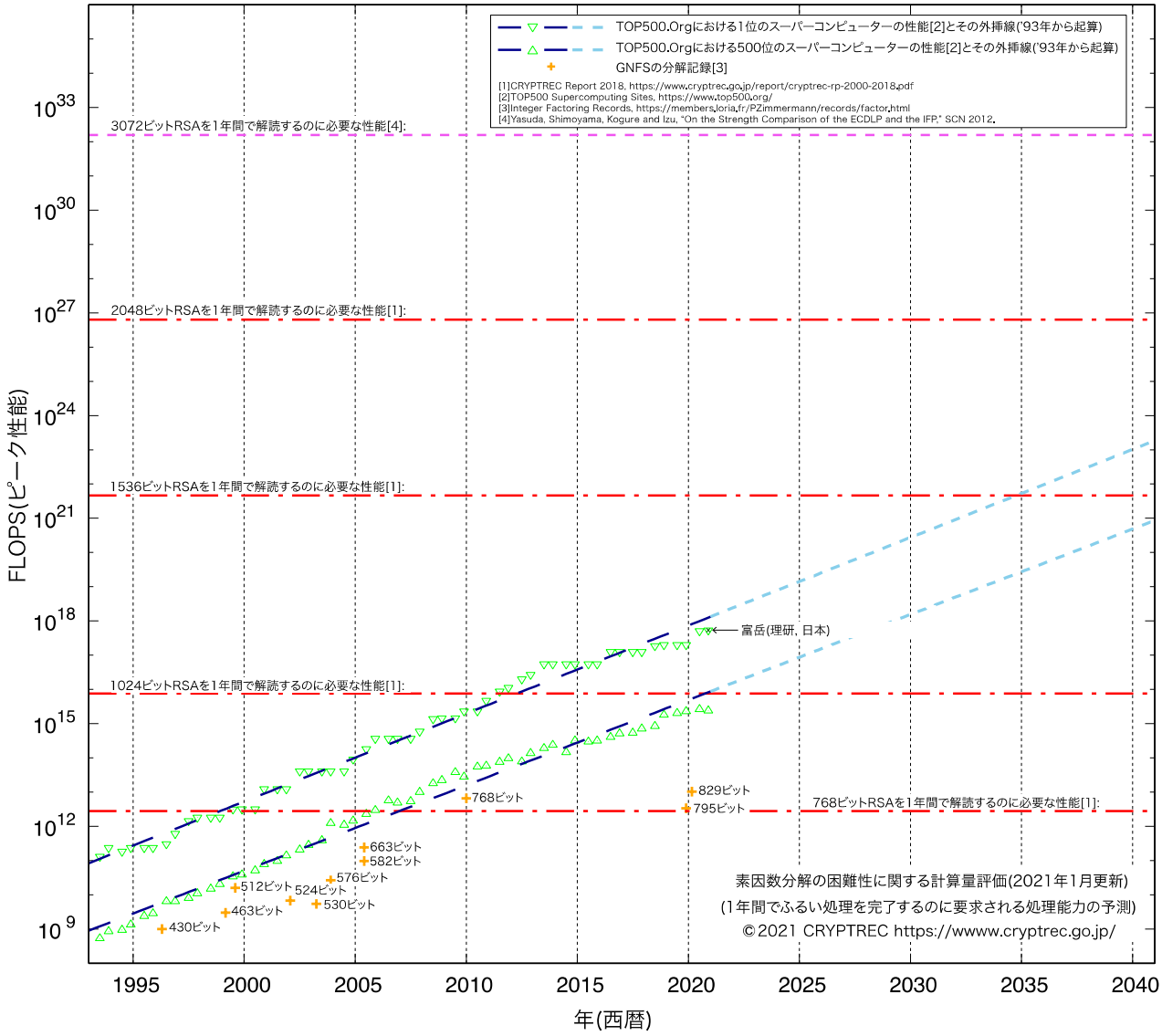

図3.2-1：素因数分解の困難性に関する計算量評価（2021年1月更新）[8]

[8] 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。

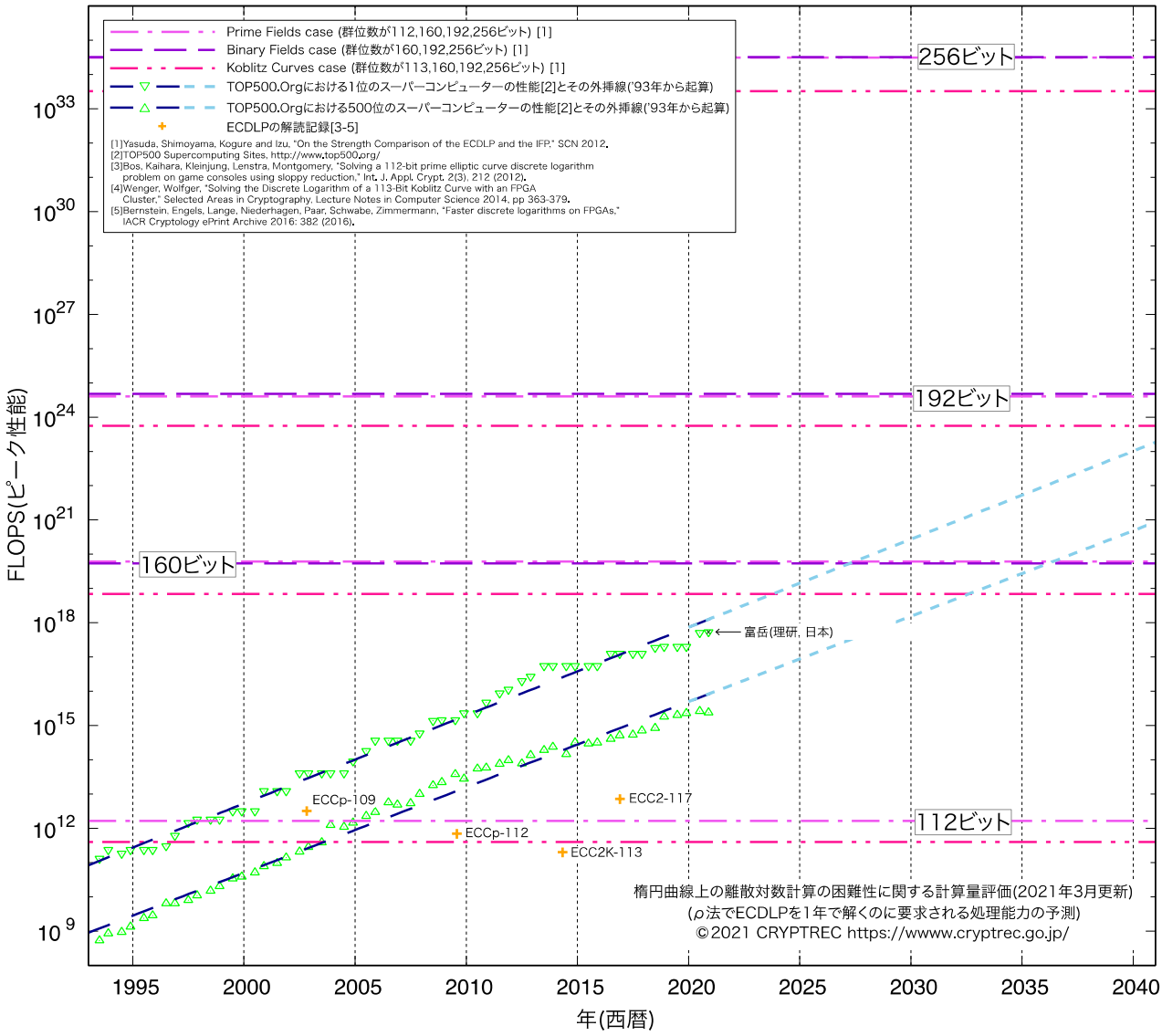

図3.2-2：楕円曲線上の離散対数計算の困難性に関する計算量評価（2021年1月更新）[9]

[9] 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。

３．２．３．２．Shorの量子アルゴリズムによる現代暗号への脅威に関する調査

背景及び実施内容

Shorの量子アルゴリズムにより、理論的には素因数分解問題や離散対数問題を効率的に解くことができ、RSA暗号や楕円曲線暗号等の安全性が危殆化することは広く知られている。そのため、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。CRYPTREC でもPQCの導入について議論が進められており、PQCの必要性を明確にするためにもShorのアルゴリズムを量子コンピュータ上で実装した研究動向を把握する必要性があるとの指摘を暗号技術調査WGの委員からうけている。

以上より、Shorの量子アルゴリズムによる現代暗号への脅威を正確に把握するために、上記の研究及び暗号で実際に利用される大きさのパラメータを攻撃するために必要なリソース評価の研究について調査する[10]。

調査内容及び報告書の構成

1) 本評価結果の概要（エグゼクティブサマリー）
2) Shorのアルゴリズムの実装・リソース評価の把握の重要性について
3) Shorの量子アルゴリズムの解説
4) Shorの量子アルゴリズムについて報告されている実装結果の調査
5) 暗号で用いるようなパラメータに対してShorの量子アルゴリズムを実行する際のリソース評価

なお、4) と5) については、2020年9月末までに公開された結果（特にPQCrypto2020で講演されるものを含む）を調査対象とする。ただし、確認されたものについては2020年10月以降の論文も調査している。

暗号解析評価WGの見解

既存のShorのアルゴリズムの実装について、これまでの実装結果では基本的に15, 21などの小さな合成数が対象とされており、いずれの実験においてもこれらの合成数に特化した効率化を行った量子回路を用いている。そのため、現状の量子コンピュータでは暗号で用いるほど大きなパラメータの合成数を素因数分解することは困難であり、暗号で用いるパラメータの問題を解くためには量子ビット数やゲート計算のエラー率など量子コンピュータの性能の大幅な向上が必要であると考える。素因数分解や離散対数問題を実行する際のリソース評価について、Shorのアルゴリズム自体の改良や実装する際の計算の簡略化手法の提案も行っており、それまで2048ビットの合成数を素因数分解するためには1.7億個の量子ビットを用いて1日かかるとされていたが、2000万個の量子ビットを用いて5時間程度で終わるという結果が2019年に報告されており、離散対数問題においても同様に様々な改良が報告されている。そのため、今後も様々な効率化が提案される可能性があるため、量子コンピュータの進歩に合わせて実装法の改良やそれに基づいたリソース評価は今後注視する必要があると考えられる。

[10] 調査対象はShor のオリジナルの量子アルゴリズム及びその変種を含む。

３．２．３．３．耐量子計算機暗号(PQC)の技術動向に関する調査（PQCを導入する際の技術の調査）

背景

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。しかし、現代暗号を解読可能な量子コンピュータが実現される時期は不明瞭であるため、PQCの使用が必須となる時期を具体的に定めることは難しい。PQCが必要になった際にそれを利用する方法として、PQCと現代暗号の双方を併用するいわゆるハイブリッドモード[11]がNISTをはじめ、様々な企業・組織で世界的に議論されている[12][13]。

CRYPTRECでは暗号技術検討会においてPQCに関する技術動向調査を実施することが承認されている。また、「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PQCのガイドラインの作成について議論されており、ハイブリッドモードをガイドラインに含めるべきかを検討する必要性が生じている。その検討の準備として、PQCのハイブリッドモードの動向を把握しておく必要がある。

耐量子計算機暗号(PQC)と現代暗号の双方を併用するハイブリッドモードに関する標準化動向を中心とした技術調査について、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（2020年7月17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（2020年8月26日）にて承認された。

調査内容

外部評価により耐量子計算機暗号(PQC)の技術動向に関する調査（PQCを導入する際の技術の調査）を実施した。

【依頼内容】ハイブリッドモードの標準化動向についてまとめ、評価報告書を作成する。評価報告書には、以下の内容を含める。

a) ハイブリッドモードの標準化動向調査

b) ハイブリッドモードの構成方法の解説、および、安全性の解析・評価などについて公開されている文献などの調査およびそれらの解説

なお、調査は2020年8月末までに公開された標準化に関わる文献などを主たる対象とし、それ以降、評価報告書の提出時期までに公開された文献については可能な範囲で評価報告書に含めることとする。

【依頼先】：菅野 哲 様 （株式会社レピダム）

【2020年度のスケジュール】

2020年8月26日第1回 暗号解析評価WG：調査の内容についてWGで説明する。（事務局担当）

2021年2月3日第2回 暗号解析評価WG：評価報告書（案）に対する WG の見解をまとめる。

暗号解析評価WGの見解

評価報告書により、主要な標準化団体・組織によるPQCと現代暗号の双方を併用するハイブリッ

---

[11] 今回の調査でハイブリッドモードという用語については合意の取れた定義は定まっていないことが確認された。

[12] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/faqs

[13] https://csrc.nist.gov/Events/2019/second-pqc-standardization-conference

ドモードに関する現在の検討状況を把握できたため、本報告書をCRYPTREC外部評価報告書としてホームページに公開する。

ハイブリッドモードという用語については合意の取れた定義はなく、ハイブリッドモードが持つべきさまざまな要件が議論されている。特に、以下の2つの要件について議論されることが多い。（詳細は、CRYPTREC外部評価報告書「PQCのハイブリッドモードに関する調査」参照）

I. 安全性の確保：（システム・プロトコル・方式などの）中で利用されているいくつかの暗号技術の安全性に問題があったとしても、問題のない他の暗号技術によって全体としての安全性を保つ[14][15]。

II. 後方互換性の確保：暗号技術の移行やシステムマイグレーションを円滑に行う一助となる。

ハイブリッドモードの安全性評価について現在のところ明らかになっていないところがある。また、ハイブリッドモードを含めて、PQCの実社会システムへの導入に関しては議論している段階にあり、今後も新たな定義や達成すべき要件などが提案される可能性がある。そのため、本WGはそれらの技術動向について引き続き把握する必要があると結論する。

３．２．４．推奨候補暗号リストへの新規暗号（事務局選出）の追加に向けた検討

ディジタル署名EdDSAは、RFC8032[16]で規定され、TLS1.3で採用された（RFC 8446[17]）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[18]）。

ディジタル署名 EdDSA の安全性評価について、下記2点の観点による評価を実施した。

I. EdDSAで使われている曲線の安全性評価（安全性の根拠となる仮定の強度）

II. 方式の構成そのものの安全性評価

評価結果より下記の見解を得た。尚、評価レポートは CRYPTREC ホームページにて公開する。

- 曲線に関する安全性評価について
  EdDSAでの使用が見込まれる2つの曲線Curve25519及びCurve448におけるECDLPに対する量子アルゴリズムを含む現時点での最良のアルゴリズムはρ法であるため、その安全性は現在使用されている楕円曲線暗号の場合と同じく、結果として主に基礎体の大きさで決定される。従って、Curve25519の場合はほぼ128ビットセキュリティ、Curve448の場合はほぼ224ビット

[14] E. Crockett, C. Paquin, D. Stebila: Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH, NIST 2nd Post- Quantum Cryptography Standardization Conference 2019.

[15] N. Bindel, J. Brendel, M. Fischlin, B. Goncalves, D. Stebila: Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange, PQCrypto 2019: 206-226

[16] RFC8032, “Edwards-Curve Digital Signature Algorithm (EdDSA) ”, Jan. 2017

[17] RFC8446, “The Transport Layer Security (TLS) Protocol Version 1.3”, Aug. 2018

[18] RFC8422, “Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier”, Aug. 2018

セキュリティの安全性を持つと判断する。また、それらの曲線上の演算も効率よく実行できることを確認した。

- 方式の構成に関する安全性評価について
  評価報告書において、現実的な脅威に結びつくような脆弱性は指摘されておらず、また、ECDSAと比較してもその安全性に劣る点はないと考えられる。他、評価報告書では複数の観点から安全性に関わる考察が示されており、いずれも安全性に問題を与える点はないと考えられる。以上より、評価報告書により示された評価結果を総合し、EdDSAの構成については、現実的な利用シーンにおける安全性に問題はないと判断する。

また、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、実装性能評価も行うこととする。

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を記している[19]。その中で、推奨候補暗号リストの認証暗号ChaCha20-Poly1305のChaCha20に関する仕様書に変更があった。新旧仕様書の差分が軽微な修正であると判定し、CRYPTRECのWebサイトの仕様書の参照先の修正を行った（表3.2-3、表3.2-4）。

表3.2-3：ChaCha20-Poly1305の暗号の新旧仕様書

暗号技術名	旧仕様書	新仕様書
ChaCha20-Poly1305	Request for Comments: 7539, ChaCha20 and Poly1305 for IETF Protocols (May 2015)	Request for Comments: 8439, ChaCha20 and Poly1305 for IETF Protocols (June 2018)

表3.2-4：判定結果とその理由

暗号技術名	判定結果	理由	備考
ChaCha20-Poly1305	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。	https://www.rfc-editor.org/errata_search.php?rfc=7539

３．２．６．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の作成・更新の検討

第1回暗号技術検討会において、次期CRYPTREC暗号リストとは別文書として、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を作成することが決定された。このため、当該

[19] https://www.cryptrec.go.jp/method.html

ガイドラインの作成方針について第2回暗号技術評価委員会にて下記のとおり決定し、第2回暗号技術検討会にて了承された。

（１） 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、次年度に、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。
（２） 高機能暗号に関するガイドラインを作成するため、次年度に、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。
（３） 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、次年度は、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。

３．２．７．暗号技術評価委員会の開催実績

2020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	2020年7月17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の安全性評価）実施についての審議 ■ 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
第2回	2021月3月9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の安全性評価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（暗号解析評価）の活動内容の報告 ■ 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の今後について審議

３．３．暗号技術活用委員会

３．３．１．活動の概要

2020年度は、2021年度からの運用ガイドラインの整備に向け、主に以下の活動を行った。

- 鍵長ガイドライン（仮）の作成方針の取りまとめ
- 暗号鍵管理の参照プロファイルの作成に向けた検討

３．３．２．2020年度の活動内容

３．３．２．１．鍵長ガイドライン（仮）の作成方針の取りまとめについて

CRYPTREC暗号リストとして安全な暗号アルゴリズムを選定してきたが、安全に利用する推奨鍵長について明示したものはなかったため、中長期的な推奨鍵長をガイダンスすることにより、情報システム設計時に必要な対策を検討することを促すためのガイドラインを2021年度に作成することとした。そこで、第2回と第3回の委員会で検討を行い、ガイドライン作成に向けた方針案を取りまとめた。

＜ガイドラインの位置づけ＞

鍵長の選択に当たっては、「鍵そのものの有効期間」「対象システムの寿命や利用環境」「対象データの機微度や保護期間」などの要因を総合的に勘案する必要がある。一方、CRYPTREC暗号リストの一要素としての鍵長の選択ということであれば、電子政府システム用途での安全な利用を前提としたものとなる。

以上を踏まえ、「用途を限定して満たすべき鍵長の要件を規定する」という考え方に基づく文書（「鍵長設定要件（仮）」）と「用途を限定せずに鍵長の設定方法に関するガイダンスを提供する」という考え方に基づく文書（「鍵長設定ガイダンス（仮）（一般用）」）とに明確に分離し、両方の文書の検討を進める。

両者の利用目的などの違いは、表3.3-1のとおりである。

表3.3-1　鍵長ガイドライン（仮）の位置づけの整理

	「鍵長設定要件（仮）」	「鍵長設定ガイダンス（仮）（一般用）」
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。	運用ガイドラインの一つと位置付け。 CRYPTRECで作成するならGLを附番
利用目的	電子政府システム用途で利用する場合の鍵長選択に関する要件を規定	用途を特定せず、鍵長やアルゴリズムの選択方法に関するガイダンスを提供
想定読者	電子政府システム用途での情報システム調達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、等 （その他の利用者は、ボランタリベースと位置付ける）	システム又はアプリケーションの所有者や管理者、設計者、開発者、運用担当者、利用者、等
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。	SP800-57 Part 1に記載がある「鍵長やアルゴリズムの選択以外の鍵管理に関する事項（鍵状態遷移や保護手段等）」は「鍵管理ガイダンス（仮）」に分ける。

＜安全性基準の考え方＞

〇様々なドキュメントで使われている「ビットセキュリティ（セキュリティレベル、セキュリティ強度）」を基本単位として鍵長を定める

　具体的には、コンセンサスが得やすく、かつ合理的な判断を行うことを目的とするため、基準とするビットセキュリティをある程度の間隔をもって設定することとする。

〇対象システムの「想定運用終了年」を基準とした、採用すべき「ビットセキュリティ」を表現したものとする

　システムの設計・構築・運用の開始時期ではなく、システムの運用終了・廃棄までの「システム寿命」に着目する。つまり、システムの運用終了・廃棄まで安全に運用できる鍵長を選択できるようにすることを基本とする。

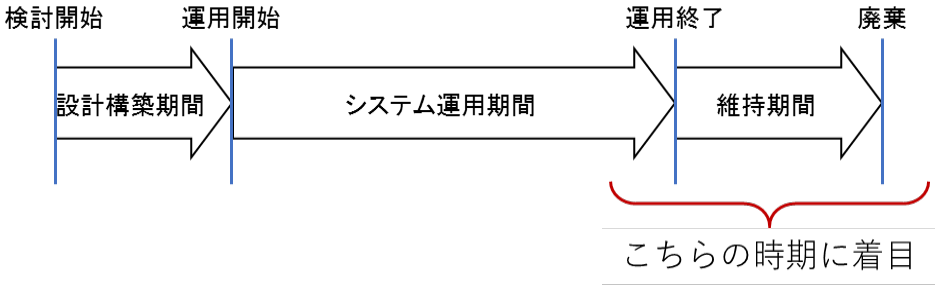

図3.3-2： システムのライフサイクル

〇「移行（Transition）」の考え方や必要性について言及する

　運用中のシステムから新しいシステムに瞬時に切り替えるということは大変困難である。このため、とりわけ長期運用のシステムでは、予め「暗号アルゴリズムや鍵長の移行」についての対応策を検討しておくことが望ましい。

〇原則として5年周期で「要求するビットセキュリティ」の内容を再確認する

　前提として長期は「現時点」での判断結果に基づくものであって、最後まで保証するものではない。そのため、5年ごとにその時々の最新の知見を考慮して内容を再確認し、必要に応じて変更するルールを導入する。

〇今回は、量子コンピュータによる危殆化は原則的に想定しない

　暗号技術評価委員会傘下の暗号調査WG（暗号解析評価）での報告において「現状の量子コンピュータでは暗号で用いるほど大きなパラメータの合成数を素因数分解することは困難であり、量子ビット数やゲート計算のエラー率など量子コンピュータの性能の大幅な向上がない限りは現代暗号の脅威にはならないと考えることができる。」との見解が出されている。

　このため、今回は量子コンピュータによる危殆化は想定しないこととし、注意喚起として「Quantum Safe Security」について何らかの形で記載するものとする。今後、暗号解読が実際

に扱える量子コンピュータの実現時期について十分に信頼できる予測がされるなど、状況の変化が明確になった時点で、内容を再考する。

○以下のラベリングをつける方向で検討する

暗号化や署名などでは、新規に暗号化や署名などを行う「新規データの生成」のタイミングと、生成済のデータに対して復号や署名検証などを行う「生成済データの処理」のタイミングが大きく異なる場合がある。一方、鍵交換やエンティティ認証では、通常、送信者が行う「新規データの生成」のタイミングと受信者が行う「生成済データの処理」のタイミングはほぼ同じである。

このような特性の違いを考慮して、利用可否を整理するのがこのラベリングの役目である。

表3.3-3　ラベリングの整理（たたき台案）

	新規データの生成	生成済データの処理
暗号化（通信時）	利用可（＝acceptable）	利用可（＝acceptable）
	利用不可（＝disable/disallowed）	利用不可（＝disable/disallowed）
		＜復号を認めるかは要検討＞
暗号化（保管時）	利用可（＝acceptable）	利用可（＝acceptable）
	利用不可（＝disable/disallowed）	復号のみ可（＝deprecated/legacy use）
		利用不可(注)（＝disable/disallowed）
鍵交換	利用可（＝acceptable）	利用可（＝acceptable）
	利用不可（＝disable/disallowed）	利用不可（＝disable/disallowed）
		＜再構成を認めるかは要検討＞
署名	利用可（＝acceptable）	利用可（＝acceptable）
	利用不可（＝disable/disallowed）	検証のみ可（＝deprecated/legacy use）
		利用不可(注)（＝disable/disallowed）
MAC	利用可（＝acceptable）	利用可（＝acceptable）
	利用不可（＝disable/disallowed）	検証のみ可（＝deprecated/legacy use）
		利用不可(注)（＝disable/disallowed）
エンティティ認証	利用可（＝acceptable）	利用可（＝acceptable）
	利用不可（＝disable/disallowed）	利用不可（＝disable/disallowed）

（注）:「暗号化（保管時）」「署名」「MAC」の生成済データの処理については、暗号技術以外の手段で何らかのリスク低減措置が取られていれば、（期限を決めずに）リスク受容を条件に利用不可とまではしなくてもよいかもしれない。

＜ガイドラインで示すべき内容（項目）＞

○「鍵長設定要件（仮）」の作成方針

CRYPTREC暗号リスト記載の暗号アルゴリズムを電子政府システム用途で利用する場合を前提とした鍵長やアルゴリズムの**選択に関する要件**、及び「移行（Transition）」の考え方や必要性に絞って記載するものとする。すなわち、CRYPTREC暗号リストに記載がない暗号アルゴリズム

（例：軽量暗号、高機能暗号）や電子政府システム用途以外（例：自動車、IoTデバイス、制御システム）は考慮しない。

- 112ビットセキュリティ以上を対象とする。

また、「取り扱う期間」は、30年程度以上、又は電子政府システム用途や法令上で最も長い運用期間を目安として検討していく。その際、強めの要件を意図し、「最小」＞「レガシーシステム・ユース」の区分けを採用する。

- 「最小」：新規調達・更新調達で使う際の基準
- 「レガシーシステム・ユース」：既存システムや暗号化済・署名済データを使う際の基準

○「鍵長設定ガイダンス（仮）（一般用）」の作成方針

用途を特定せず、鍵長やアルゴリズムの**選択方法に関するガイダンス**として、「鍵長設定の考え方」、「移行の考え方や必要性」、「鍵タイプ」及び「（鍵タイプごとの）推奨暗号利用期間」について記載するものとする。「鍵長設定の考え方」では、CRYPTREC暗号リスト記載の暗号アルゴリズムに限定せず、目的に応じた鍵長設定の考え方を示す。また、CRYPTREC暗号リストに記載がない暗号アルゴリズム（例：軽量暗号、高機能暗号）についても含める。

- 80ビットセキュリティ、又は100ビットセキュリティ（96ビットセキュリティ）以上を対象とする。

「取り扱う期間」は、暗号技術評価委員会が作成している素因数分解及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の予測図における対象範囲が発行年＋20年までであることを考慮し、20～30年程度を目途に適切な期間を検討していく。

また、用途を限定しない以上、どの程度のセキュリティを求めるかの判断は読者が行うことを原則とし、要件としての意図は求めないこととする。その代わりの対策として、鍵長以外でのセキュリティ確保の考え方も示す。例えば、「移行に向けた事前準備」「鍵利用期間の制限」「危殆化発生時対応計画」の組合せ、など。

３．３．２．２．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

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、具体的な参照プロファイルの作成を2021年度から開始することとしている。

そこで、以下の論点について、第3回の委員会で検討を行い、今後の進め方を取りまとめるところまでを行った。

＜位置づけの整理＞

参照プロファイルは、詳細なシステムやサービスを想定するほど、厳密なプロファイルを作成することが可能になると考えられるが、その他のシステムやサービスへの転用が難しくなると思

われる。一方、具体的なシステムやサービスを想定しないと、プロファイルの作成そのものが難しい。

そこで、具体的な参照プロファイルの作成方法を検討するに当たり、まず出来上がりの文書の位置づけの整理を以下のように整理した。

表3.3-4　出来上がり文書の位置づけの整理

	考え方1	考え方2	考え方3
目標	CKMSチェックリスト（の一部項目）に、そのまま流用、もしくは少々の改変で利用可能な形になっている**参照プロファイルを作成**	CKMSチェックリストの中で「必要最小限の統一的条件（ベースライン)」を取りまとめた**参照プロファイルを作成**	参照プロファイルそのものではなく、参照プロファイルの**作成マニュアルを作成**
想定システム・サービス	具体的なシステムモデル／サービスモデル	一般的・汎用的なシステムモデル／サービスモデル	システム・サービスは例示（シンプルなモデル、トイモデル）
期待点	うまく当てはまるケースであれば、個々の設計仕様書やプロファイルの作成の効率化がかなり図れる	想定範囲内に含まれる様々なシステム／サービスでの個々の設計仕様書やプロファイルの作成において、一定程度の安全性の底上げが期待できる（項目がある）	暗号鍵管理システム設計指針（基本編）の理解や、仕様書やプロファイルへの落とし込み方の理解が進むと期待できる。 各業界の業界団体等が、該当の業態の実態に即したプロファイルを作る事が期待できる。
懸念点	●想定したシステムモデル／サービスモデルがそもそも現実的であるか不明 ●想定から外れたシステムモデル／サービスモデルではほとんど使えない可能性が高い ●他の（上位）ポリシーなどと整合しない可能性もある（現状の整合性、将来の相互運用性、両方で課題が発生する可能性がある） ●一般企業が調査対象に含まれる場合、企業機密に近い情報が必要となる可能性もある	●参照プロファイルに記載できるのはCKMSチェックリストのごく一部にとどまると予想される ●想定範囲内に含まれる様々なシステムモデル／サービスモデルでの条件の公約数的なものしかプロファイルに記載できない可能性が高い ●多くの機関の情報を得る必要があることが予想される ●「ベースライン」のスコープ定義においては、各機関の利害調整が必要となる可能性が高い	●参照プロファイルではないので、個々の設計仕様書やプロファイルの作成のための流用はほぼ不可能 ●体系的な理想形や推奨を提示しているわけではない

＜作成方針＞

○「考え方3」で参照プロファイルの作成方法を整理するところから始める

「考え方1」では多くのシステムが使用できるプロファイル作成が難しく、さらに対象とする具体的なシステムの選定に時間がかかる可能性が高い。また、「考え方2」では必要最小限の統一的条件の決め方が難しいことが予想される。

○作業スケジュールとしては2年計画とし、WGを発足させて検討を進める

2021年度は、重点的に説明が必要な項目の精査、及び各分野から情報を収集し記載するモデルの検討を行う。その後、本文のドキュメント化を進め、2022年度に作成マニュアルを完成させる予定で作業を進める。

例示としてのシンプルなモデルの候補は以下のものを含め、WGで検討を行う。

- オンプレミスHSMを利用した鍵へのアクセスコントロール（デバイス向け鍵管理、Web用証明書）
- リモート管理された鍵へのアクセスコントロール（リモート署名、暗号化鍵のクラウド管理、等）
- クラウドデータに対するアクセスコントロール
- 失敗事例

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3.3-5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3.3-5　暗号技術活用委員会の開催状況

回	開催日	議案
第1回 （2020年度 第2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 ■　2020年度暗号技術活用委員会活動案について
第2回	2021年1月15日	■　2020年度活用委員会活動計画の確認 ■　推奨鍵長ガイドライン（仮）についての検討 ■　暗号鍵管理の参照プロファイルについての検討
第3回	2021年3月2日	■　鍵長ガイドライン（仮）（方向案）についての検討 ■　暗号鍵管理の参照プロファイルについての検討（2回目） ■　2020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。

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、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、鍵長ガイドライン（仮）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。

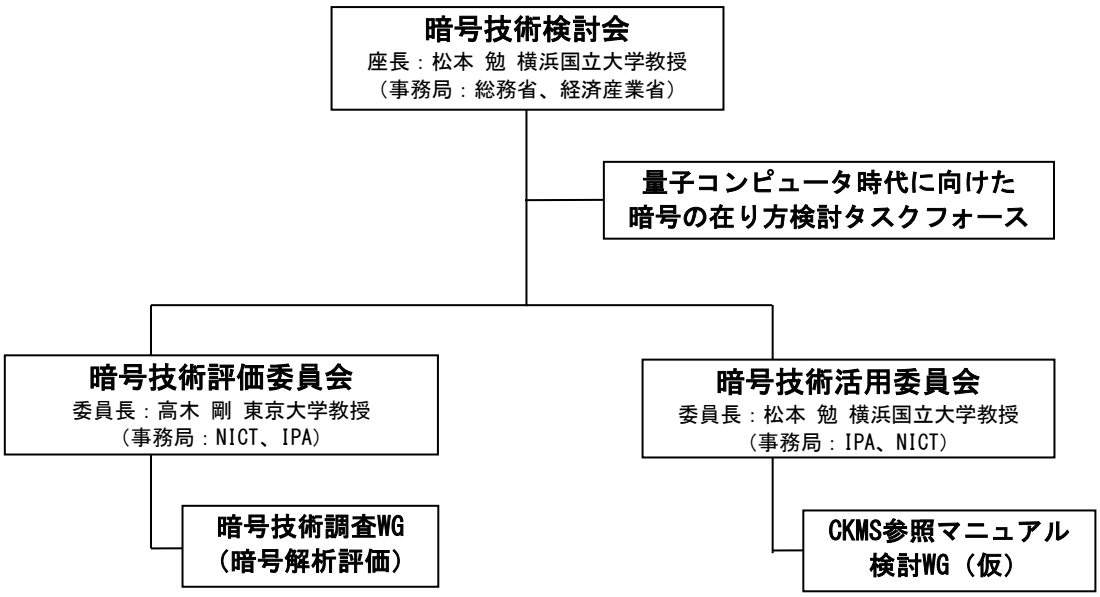

図4-1 2021年度CRYPTRECの体制図（予定）