資料１

2020年度 第２回 暗号技術検討会

令 和 ３ 年 ３ 月 ３ ０ 日
１ ０ ： ０ ０ ～
オ ン ラ イ ン 開 催

議事次第

１．開会

２．議事
(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」の検討状況及び活動について【報告・審議】
(2) 2020年度暗号技術評価委員会 活動報告について【報告】
(3) 2020年度暗号技術活用委員会 活動報告について【報告】
(4) 暗号技術検討会 2020年度 報告書（案）について【承認】
(5) その他

３．閉会

配付資料一覧

資料１	議事次第・配付資料一覧
資料２－１	「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」の検討状況について
資料２－２	CRYPTREC暗号リストの３リスト構成について
資料３	2020年度 暗号技術評価委員会 活動報告
資料３別添１	監視状況報告
資料３別添２	ディジタル署名EdDSAの安全性評価結果(外部評価)
資料３別添３	2020年度 暗号技術調査WG（暗号解析評価）活動報告
資料３別添４	仕様書の参照先の変更について
資料３別添５	ガイドラインに関する今後の方針について
資料４	2020年度 暗号技術活用委員会 活動報告
資料５	暗号技術検討会 2020年度 報告書（案）
参考資料１	暗号技術検討会 開催要綱（構成員・オブザーバ名簿）
参考資料２	電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）

以上

資料２－１

「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」の検討状況について

１　設置の経緯

近年、耐量子計算機暗号（PQC）の研究開発・標準化が各国で進められており、大規模な量子コンピュータの出現に向けて、我が国においても耐量子計算機暗号について議論を行う必要性が高まっていた中で、量子コンピュータの動向や耐量子計算機暗号を含む新たな暗号技術の動向等を踏まえた次期CRYPTREC暗号リストの改定方針について、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を行った。

両委員会における議論及び2018年度暗号技術検討会での審議・承認を経て、次の事項を整理するため、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」（以下「検討TF」という。）を2019年度から設置（図１参照）することとした。

(1) 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等の検討

(2) その他新たな暗号技術の動向等（軽量暗号や秘密計算に利用される準同型暗号等）を踏まえた検討等

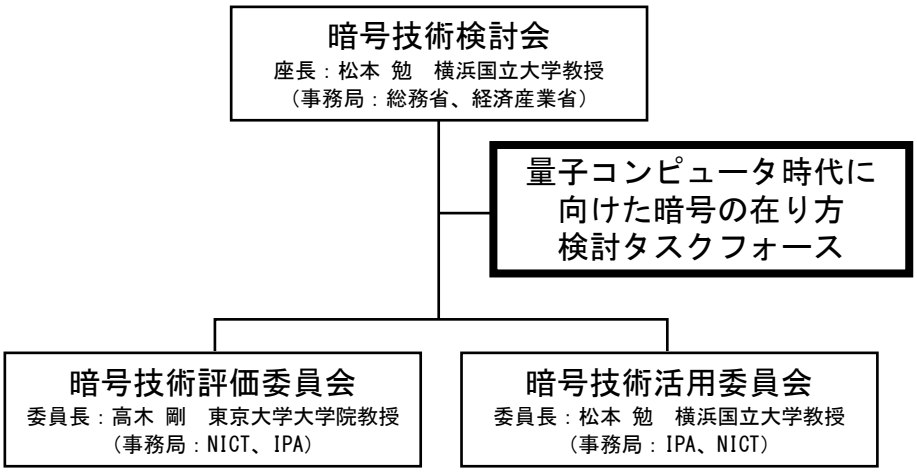


図１　検討TF

２　実施概要

２．１　体制（構成員・事務局）

検討TFの構成員は、2019年度に引き続き、暗号技術検討会並びに暗号技術評価委員会及び暗号技術活用委員会の構成員から表１のとおり構成した。

表１　検討TF　構成員

	宇根 正志	日本銀行金融研究所情報技術研究センター 情報技術研究グループ長
	國廣 昇	筑波大学システム情報系教授
	高木 剛	東京大学大学院情報理工学系研究科教授
	松井 充	三菱電機株式会社開発本部役員技監
(座長)	松本 勉	横浜国立大学大学院環境情報研究院教授
	松本 泰	セコム株式会社IS研究所 コミュニケーションプラットフォームディビジョンマネージャー
	満塩 尚史	内閣官房情報通信技術(IT)総合戦略室政府CIO補佐官

また、オブザーバーについても2019年度と同じく、内閣官房内閣サイバーセキュリティセンター、警察庁、個人情報保護委員会事務局、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、経済産業省、防衛省、警察大学校及び国立研究開発法人産業技術総合研究所の参加を得た。

事務局についても2019年度と同じく、暗号技術検討会の事務局である総務省及び経済産業省、並びに暗号技術評価委員会及び暗号技術活用委員会の事務局である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）の４者の共同により開催した。

２．２　開催実績

検討TFにおいて2019年度に検討した事項のうち、引き続き検討が必要とされたCRYPTREC暗号リストの３リスト構成の在り方について検討するとともに、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、表２のとおり、2020年度に会合を１回実施し、検討を行った。

表２　検討TF　開催実績

会合・実施日	主な議論内容
第４回会合 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　技術動向検討

３．１　量子コンピュータの動向について

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。

３．２　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の評価が行われ、2020年７月から表３の７（＋α）方式について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　Round 3 候補暗号

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)

３．３　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、$2^z \equiv 1 \ mod \ 3$ については良い出力を得られているものの、$2^z \equiv 2 \ mod \ 3$ 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。

４　CRYPTREC暗号リストでの３リスト構成について

４．１　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]

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。

４．２　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。

---

[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。

４．３　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。

移行ルールとしては次のとおり（図２を参照）。

＜「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。

[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。

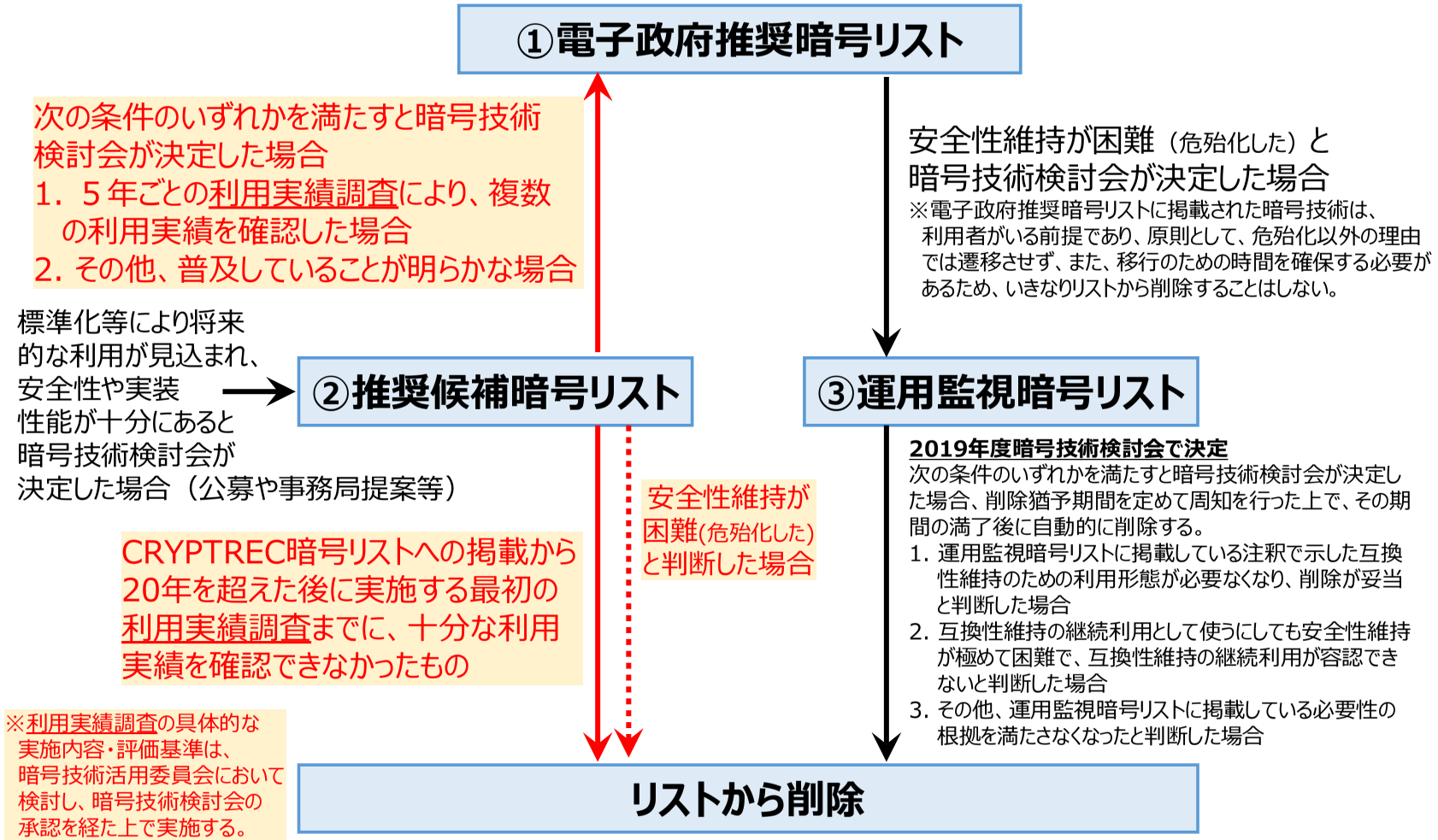


図２　CRYPTREC暗号リスト移行ルール

資料２－２

CRYPTREC暗号リストの３リスト構成について

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を踏まえ、CRYPTREC暗号リストについて３リスト構成を維持することとし、その移行ルールについて以下のように取り扱うこととしてよろしいか御審議いただきたい。

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

安全性維持が困難（危殆化した）と暗号技術検討会が決定した場合
※電子政府推奨暗号リストに掲載された暗号技術は、利用者がいる前提であり、原則として、危殆化以外の理由では遷移させず、また、移行のための時間を確保する必要があるため、いきなりリストから削除することはしない。

標準化等により将来的な利用が見込まれ、安全性や実装性能が十分にあると暗号技術検討会が決定した場合（公募や事務局提案等）

②推奨候補暗号リスト

③運用監視暗号リスト

（2019年度暗号技術検討会　決定事項）
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、削除猶予期間を定めて周知を行った上で、その期間の満了後に自動的に削除する。
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

安全性維持が困難(危殆化した)と判断した場合

CRYPTREC暗号リストへの掲載から20年を超えた後に実施する最初の利用実績調査までに、十分な利用実績を確認できなかったもの

※利用実績調査の具体的な実施内容・評価基準は、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。

リストから削除

資料３

2020 年度暗号技術評価委員会活動報告

1. 活動目的

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。

2. 活動概要

(1) 暗号技術の安全性及び実装に係る監視及び評価

下記の通り、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・評価を実施する。

① CRYPTREC 暗号等の監視

国際会議等で発表される CRYPTREC 暗号リストの安全性及び実装に係る技術（暗号モジュールに対する攻撃とその対策も含む）に関する監視を行い、会議や ML を通して報告する。

- 今年度実施の監視報告の詳細については、CRYPTREC Report 2020 で報告。（資料３別添１参照）

② 電子政府推奨暗号リスト及び推奨候補暗号リストからの運用監視暗号リストへの降格及び 運用監視暗号リストからの危殆化が進んだ暗号の削除

CRYPTREC 暗号リストの安全性に係る監視活動を継続的に行い、急速に危殆化が進んだ暗号技術やその予兆のある暗号技術の安全性について評価を行う。また、リストからの降格や削除、注釈の改訂が必要か検討を行う。

③ CRYPTREC 注意喚起レポートの発行

CRYPTREC 暗号リストの安全性及び実装に係る技術の監視活動を通じて、国際会議等で発表された攻撃等の概要や想定される影響範囲、対処方法について早期に公開することが望ましいと判断された場合、注意喚起レポートを発行する。

④ 推奨候補暗号リストへの新規暗号（事務局選出）の追加

標準化動向に鑑み電子政府システム等での利用が見込まれると判断される暗号技術の追加を検討する。

- CRYPTREC 暗号リストへの追加を検討するため、IETF で標準化され、TLS 1.3 で実導入されるなど、今後、利用が見込まれる暗号技術（署名）である EdDSA の安全性評価を行う。
  - 利用する曲線の安全性および方式の構成の安全性について外部評価を実施し、評価レポートを踏まえ、暗号技術評価委員会としての見解をまとめた。(資料３別添２参照)

⑤ 新技術等に関する調査及び評価

将来的に有用になると考えられる技術やリストに関わる技術について、安全性・性能評価を行う。必要に応じて、暗号技術調査ワーキンググループによる調査・評価、または、外部評価による安全性・性能評価などを行う。

- 暗号技術調査ワーキンググループ(暗号解析評価)を継続し、耐量子計算機暗号(PQC)に関する技術動向及び 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を行う。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」の予測図の更新を行う。
  - 暗号技術調査ワーキンググループ(暗号解析評価)を開催し、「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」の予測図の更新を行った。また、Shor の量子アルゴリズムによる現代暗号への脅威について、事務局により評価を実施し、評価レポートを踏まえ、ワーキンググループとしての見解をまとめた。さらに、耐量子計算機暗号(PQC)に関する技術動向に関する調査(PQC を導入するための技術に関する調査) について、外部評価を実施し評価レポートを踏まえ、ワーキンググループとしての見解をまとめた。(資料３別添３参照)

(2) 暗号技術の安全な利用方法に関する調査（技術ガイドラインの整備、学術的な安全性の調査・公表等）

暗号技術を利用する際の技術面での注意点に関する調査、新技術の安全性・性能に関する調査・評価を行う。

- 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ため、アルゴリズムの部分に変更がないことを確認し、新しい仕様書へ参照先を変更した。(資料３別添４参照)

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の作成・更新を行う。

- 耐量子計算機暗号、高機能暗号、及び、軽量暗号のガイドラインに関する今後の方針を議論した。(資料３別添５参照)

3.開催状況

表１ 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

以上

資料３別添１

監視状況報告

1. 監視活動報告

2020 年度第一回暗号技術評価委員会（2020 年 7 月 17 日）から 2020 年度第二回暗号技術評価委員会（2021 年 3 月 9 日）までに、表 1 に示す国際会議に参加するとともに各種調査を行い、暗号解読技術等に関する研究動向を収集した。

表 1. 国際会議への参加状況

学会名・会議名		開催国・都市	期間
Crypto 2020	International Cryptology Conference	(Virtual Conference)	2020 年 8 月 17 日～8 月 21 日
FDTC 2020	Fault Tolerance and Diagnosis in Cryptography	(Virtual Conference)	2020 年 9 月 13 日
CHES 2020	Conference on Cryptographic Hardware and Embedded Systems	(Virtual Conference)	2020 年 9 月 14 日～2020 年 9 月 18 日
PQCrypto 2020	International Conference on Post-Quantum Cryptography	(Virtual Conference)	2020 年 9 月 21 日～2020 年 9 月 23 日
FSE 2020	Fast Software Encryption conference	(Virtual Conference)	2020 年 11 月 9 日～2020 年 11 月 13 日
Asiacrypt 2020	Annual International Conference on the Theory and Application of Cryptology and Information Security	(Virtual Conference)	2020 年 12 月 7 日～2020 年 12 月 11 日

2. 解読技術等の動向

各国際会議における報告等より、具体的な暗号の攻撃に関する発表を抽出し、CRYPTREC 暗号リスト記載の暗号の安全性に直接関わる技術動向（2.1）およびその他の注視すべき技術動向（2.2）について分析を行った。

2.1. CRYPTREC 暗号リスト記載の暗号に直接関わる解読技術動向

CRYPTREC 暗号リスト（電子政府推奨暗号リスト）掲載の暗号に関しては、公開鍵暗号および共通鍵暗号に対する攻撃研究が発表された。

公開鍵暗号に関しては、795 ビットの素因数分解および離散対数計算に対する新記録が報

告され、前者は約 1000 コア年、後者は約 3200 コア年の計算量見積もりとなっている *。これまでの記録はいずれも 768 ビットであったが、離散対数に関しては今回の篩フェーズは前回計算量よりも 25%削減され、かなりの高速化を実現しており、また素因数分解に対する計算量比率も約 3 倍とこれまでの見積もりほど差があるわけではないとしている。

共通鍵暗号に関しては、ChaCha に対するこれまでの記録を上回る鍵回復攻撃(7 ラウンド)が発表されたが、ChaCha20 のラウンド数 20 にはまだマージンがあり、早急な対策が必要となるものではないが今後の攻撃の進展には注意が必要である。

2.1.1. 公開鍵暗号に関する解読技術

・Comparing the Difficulty of Factorization and Discrete Logarithm: A 240-Digit Experiment [Crypto2020]

Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, and Paul Zimmermann

Peter L. Montgomery に捧ぐ

本論文では、2 つの新たな記録を報告する。795 ビットの数 RSA-240 の素因数分解と、795 ビット素体上の離散対数計算である。以前の記録は 2009 年の RSA-768 の素因数分解と 2016 年の 768 ビット離散対数計算であった。我々の 2 つの 795 ビットレベルの計算は同じハードウェアとソフトウェアを用いて行われ、離散対数を計算することは同じサイズの素因数分解よりも大きく難しくはないことを示している。更に、アルゴリズムの多様性と良く選ばれたパラメーターのおかげで、我々の計算は以前の記録から予想されるよりも遥かに効率的であった。

本論文の最後のページでは RSA-250 の素因数分解について報告している*。

2.1.2. 共通鍵暗号に関する解読技術

・ Improved Differential-Linear Attacks with Applications to ARX Ciphers [Crypto2020]

Christof Beierle, Gregor Leander, and Yosuke Todo

本論文では、ARX (Addition, Rotation and XOR) ベースの暗号に特に焦点を当てた差分線形解析のフレームワークに対する改良を数点提案している。このインパクトを検証する

---

* 分解記録 RSA-240(795 ビット)及び RSA-250(829 ビット)は 2019 年度暗号技術評価委員会活動報告として既に報告済みである。詳しくは、2020 年度第 1 回暗号技術検討会配布資料 3 別添 3 を参照のこと。https://www.cryptrec.go.jp/report/cryptrec-mt-1011-2020.pdf

ため、それらの改良を Chaskey と ChaCha に適用し、現在公開されている最良の攻撃を著しく改良することができた。6-round ChaCha では Time Complexity が $2^{77.4}$、Data Complexity が 2^{58}、7-round ChaCha では Time Complexity が $2^{230.86}$、Data Complexity が $2^{48.83}$ という結果になっている。

2.2. その他の注視すべき技術動向

使用される機会が多いか今後多くなると予想される暗号プリミティブに関して、上記以外に次の事項が発表された。

2.2.1. ハッシュ関数に関する解読技術

・Time-Space Tradeoffs and Short Collisions in Merkle-Damgård Hash Functions [Crypto2020]

Akshima, David Cash, Andrew Drucker, and Hoeteck Wee

ランダムオラクルモデルにおいてランダムオラクルに関する任意 S ビット補助情報の入力および T クエリを用いる攻撃者による、Merkle-Damgård 型ハッシュ関数に対する衝突発券攻撃を研究した。最近の結果では、このような攻撃者は n を出力長とするとアドバンテージ $\Omega(ST^2/2^n)$で(ランダム IV に関して)衝突を発見することができ、バースデイ境界を因子 S 分超えることができる。これらの攻撃は最適であることが示されている。

我々はこの攻撃により生成される衝突は T ブロックのオーダーになる非常に長いものであるため現実的な意義を制限しているものと考え、より短い衝突を発見する改良に関していくつかの結果を証明した。例えば、B ブロック長の衝突発見をアドバンテージ $\Omega(STB/2^n)$で達成する単純な攻撃を提示する。

・Out of Oddity – New Cryptanalytic Techniques Against Symmetric Primitives Optimized for Integrity Proof Systems [Crypto2020]

Tim Beyne, Anne Canteaut, Itai Dinur, Maria Eichlseder, Gregor Leander, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, Yu Sasaki, Yosuke Todo, and Friedrich Wiemer

SNARKs、STARKs、Bulletproofs のような多くの完全性証明システムの安全性と性能は、その元となるハッシュ関数に大きく依存する。このため、いくつかの新しい提案が最近開発されている。これらのプリミティブは、特に実装上の制限から標準的な設計アプローチに必ずしも沿っていないため詳細な安全性評価が必要である。

本論文では、最近のこのようなプリミティブの 2 つのファミリー、GMIMC と HADESMIMC の安全性を比較する。我々は、最近公開された STARK に適したハッシュ関数チャレンジで提案されたほとんどのパラメーターにおいて、GMIMC と HADESMIMC の置換に対する低計算量の識

別器を示す。ZK-STARK プロトコルで実用的な利用に対応するスポンジ構成のより具体的な設定において、GMIMC のラウンド削減版に対する実際的な衝突攻撃と HADESMIMC のいくつかの具体例に対する原像攻撃を提示する。これらの結果の達成のために、我々は奇標数体のいくつかの暗号的テクニックを一般化し採用した。

2.2.2. 軽量暗号に関する解読技術

・Automatic Verification of Differential Characteristics: Application to Reduced Gimli [Crypto2020]

Fukang Liu, Takanori Isobe, and Willi Meier

差分特性検索のための MILP もしくは SAT ベースモデルの多くにおいては、差分変化のみ取り入れており異なるラウンドにおいて独立と扱われているため、元となる置換において無効なものを発見する可能性がある。この障害を克服するため、我々は差分特性検索における不整合を自動的に避けるモデルを設計し、差分変化および値変化の両方を取り入れた。我々の新しいテクニックを CHES2017 で提案された Gimli 置換に適用し、その内の一つは Gimli 文書にも載っている縮退版 Gimli のいくつかの差分特性は実際に矛盾するものであることを示した。更に、NIST 軽量暗号標準化プロセスで第 2 ラウンド候補となっている Gimli 認証暗号スキームおよびハッシュスキームに対する包括的な研究を行い、ハッシュスキームに対しては、semi-free-start(SFS)衝突探索は途中のラウンドから開始して 8 ラウンドまで到達した。認証暗号スキームに対しては、状態回復攻撃が 9 ラウンドまで達成することを示した。ただし、我々の解析は Gimli の安全性を脅かすものではないことを強調しておく。

・Cryptanalysis Results on Spook: Bringing Full-Round Shadow-512 to the Light [Crypto2020]

Patrick Derbez, Paul Huynh, Virginie Lallemand, María Naya-Plasencia, Léo Perrin, and André Schrottenloher

Spook は NIST 軽量暗号標準化プロセスの 2 ラウンド 32 候補の 1 つであり、差分サイドチャネル体制を主張している点において特に興味深い。本論文では Spook の基盤となる置換フル 6 ステップ版、即ち Shadow-512 および Shadow-384 の実用的な識別器を示し、置換に関して設計者たちにより提案されたチャレンジ問題を解いた。更に、著者らにより考案された CIML2 セキュリティゲームにより許されるナンス誤用シナリオにおける SIP オペレーションモードの 4 ステップ Shadow に対する実用的な偽造を提示する。これらの結果は実装されている。

・New results on Gimli: full-permutation distinguishers and improved collisions

[Asiacrypt2020]

Antonio Flórez Gutiérrez, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, André Schrottenloher, and Ferdinand Sibleyras

Gimli は NIST 軽量暗号標準化コンペティションの第 2 ラウンドに選ばれた暗号プリミティブ(ハッシュ関数と認証暗号)のファミリーである。NIST コンペ候補である Gimli は、CHES2017 で提案された置換 Gimli に基づいている。本論文では、置換およびそれに基づいた構成の両方の安全性を研究する。我々は、Gimli における緩やかな拡散と内部の対称性を利用し、計算量 2^{64} のフル置換識別器を初めて構成した。また、フル 24 ラウンド Gimli の内 23 ラウンドに対する実用的な識別器を実装した。

次に、我々は Gimli ハッシュに対して各々12/18 ラウンドに達する(フルステート)衝突攻撃/Semi-Free-Start(SFS)衝突攻撃を与えた。実際には 8 ラウンド Gimli ハッシュの衝突を計算した。量子設定ではこれらの攻撃はもう 2 ラウンド伸びる。最後に我々は置換における線型トレイルの研究を始めて行い、Gimli の 17 ラウンドに達する差分-線型暗号解析を提示する。

2.2.3. その他に関する解読技術

・Minerva: The curse of ECDSA nonces: Systematic analysis of lattice attacks on noisy leakage of bit-length of ECDSA nonces [CHES2020]

Ján Jančár, Vladimír Sedláček, Petr Švenda, and Marek Sýs

ECDSA の実装(FIPS140-2 認証されたスマートカード用 IC チップである Atmel 社製 AT90SC、および 5 個のソフトウェア暗号ライブラリ）に、サイドチャネル攻撃の一種であるタイミングアタックに対する脆弱性を発見した。ECDSA では、署名生成 1 回ごとに nonce が必要だが、nonce のビット長がサイドチャネル情報として（ノイズは大きいが）洩れる場合に、それを利用して秘密鍵を復元する手法を示し、実際の認証製品や暗号ライブラリに対する具体的な攻撃の結果も示している。EdDSA は、nonce が決定論的に生成され、また nonce が長いことから、この攻撃に耐性がある。

・Quantum Security Analysis of AES [FSE2020]

Xavier Bonnetain, María Naya-Plasencia and André Schrottenloher

本論文は、AES に関する初めてのポスト量子セキュリティの解析である。まず、ラウンド数を減らした AES に対する既知の最善の暗号解析の一般化・量子化バージョンを提示し、さらに量子計算機による計算速度向上の利点を受けないように見える攻撃についても議論する。本論文で提示する古典的・量子的の両方にわたる構造的な探索の新しいフレームワークを提案し、その攻撃の複雑性を効率的に計算することを可能にする。

本論文での最善の攻撃は、量子 Demirci-Selçuk meet-in-the-middle attack である。意

外にも、この設定原理の下になるアイディアを使用することで、新しい、直観に反する古典的 TMD trade-off を得ることが可能になる。特に、AES-256 及び AES-128 に対するある種の攻撃におけるメモリ消費を軽減することができる。

本論文の攻撃の要素のひとつは、AES の S-Box の差分方程式を、reversible S-Box の量子コストを考慮しながら、効率的に解くことである。現状で得られた結果から判断すると、AES は古典環境だけでなくポスト量子環境においても、量子一般攻撃に関して十分セキュリティマージンがある暗号プリミティブであるように見える。

・Finding Collisions in a Quantum World: Quantum Black-Box Separation of Collision-Resistance and One-Wayness [Asiacrypt2020]

Akinori Hosoyamada and Takashi Yamakawa

STOC1989 の Impagliazzo と Rudich の仕事により、多くのブラックボックス不可能性に関する結果が確立されたが、これらは暗号プリミティブ間の古典的なブラックボックス帰着を除外しただけであり、量子帰着を用いることにより可能となるかもしれなかった。これらの可能性をなくすために、量子設定の下でブラックボックス不可能性を研究した。

我々はまず初めに、TCC2004 の Reingold、Trevisan、Vadhan による定式化に従い、完全ブラックボックス帰着に対する量子版を定式化し、衝突耐性ハッシュ関数から一方向性置換（もしくは落とし戸置換でさえ）への量子完全ブラックボックス帰着はないことを証明した。我々は、古典・量子両方のプリミティブ実装を考慮し、この結果は古典設定において同様の結果を示した Eurocrypt 1998 における Simon の仕事の量子設定への拡張となっている。

An Algebraic Formulation of the Division Property: Revisiting Degree Evaluations, Cube Attacks, and Key-Independent Sums [Asiacrypt2020]

Kai Hu, Siwei Sun, Meiqin Wang, and Qingju Wang

我々は、ベクトルブール関数 f の座標関数の任意の席における単項式の有無を、その結合が f となるより単純な列にわたる所謂単項式地霊るの数を数えることにより決定する、分割プロパティの単純化とみなすことができる「単項式予測（monomial prediction）」と名付けたテクニックを導入する。単項式予測を用いて、我々は TRIVIUM の正確な代数的次数を 834 ラウンドまで初めて得ることができた。キューブ攻撃の文脈においては、より小さい次元でより多くのキューブを同定し、840、841、842 ラウンド TRIVIUM に対するほぼ最適な攻撃の改良を行った。

An Algebraic Attack on Ciphers with Low-Degree Round Functions: Application to Full MiMC [Asiacrypt2020]

Maria Eichlseder, Lorenzo Grassi, Reinhard Lüftenegger, Morten Øygarden, Christian

Rechberger, Markus Schofnegger, and Qingju Wang

我々は初めて、コードブックの半分を必要とする F_2^n 上の MiMC のすべてのフルラウンド版への鍵回復攻撃を記述する。選択暗号文攻撃シナリオにおいて、MiMC の n ビットフル版に対してこのデータから鍵を回復するのに、MiMC に対する $2^{n-\log_2(n)+1}$ 呼び出しと無視できる量のメモリを必要とする。本攻撃は MiMC のトイ版において実際に検証された。本攻撃は素体上の MiMC の安全性には影響しないことに注意されたい。

Improvements of Algebraic Attacks for solving the Rank Decoding and MinRank problems [Asiacrypt2020]

Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel

本論文では、多変数ベースあるいは階数距離符号ベース暗号においていたるところに現れる MinRank 問題を解く代数的手法を著しく改良する方法を示す。後者に現れる構造的 MinRank 問題の場合は、最近の Eurocrypt2020 における Canteaut、Ishai らのブレークスルーを更に改良し、これまで最良と考えられていた組み合わせ攻撃を代数攻撃が凌ぐことを示した。このアプローチを少し改良することにより、我々はあるパラメーターに関してはグレブナー基底計算を完全に避け、線型連立方程式を解くことが残されたのみであった。これは本質的に計算量を改良するのみならず、この場合になぜ代数的テクニックが機能するかの確信的議論を与えるものである。NIST PQC 第 2 ラウンド候補の ROLLO-I-128/192/256 に適用した場合、我々の新しい攻撃は、Eurocrypt2020 で得られたビット計算量 117、144、197 に対し、各々71、87、151 を与える。同様のアプローチにより通常の MinRank 問題に対し代数的的 MinRank ソルバーを改良した。NIST-PQC の第 2 ラウンド候補である GeMSS および Rainbow に適用した場合、我々の攻撃はこれまでに知られている最良攻撃に非常に近いもしくは少し良い計算量を持つ。

Lower Bounds on the Degree of Block Ciphers [Asiacrypt2020]

Phil Hebborn, Baptiste Lambin, Gregor Leander, and Yosuke Todo

ブロック暗号に対し代数的次数の上限を評価する手法はこれまでに知られているが、設計者にとって安全性を保証する役には立たない。本論文では現代的なブロック暗号の代数的次数の意味ある下限評価を与える。

2.2.4. 耐量子計算機暗号に関する動向

・NIST 耐量子計算機暗号(PQC: Post-Quantum Cryptography)標準化の動向

NIST PQC 標準化プロセスは 3 ラウンド目に入り、7 つの最終候補および 8 つの代替候補の評価が進められている。PQC Forum メーリングリストにおいて、NIST から「最近の暗号解

析が多変数署名 Rainbow および GeMSS に影響を与えたため、NIST はセキュリティおよびアプリケーションの観点から多様性欠如の懸念を持っている」旨のメールが投稿された。更に NIST は、2 ラウンド時のレポートから、SPHINCS+が 3 ラウンドの終わりの時点で標準のアルゴリズムになる可能性について言及した部分および標準化プロセスにないスキームを採用する可能性について言及した部分を議論のスタートポイントとして提示し、意見を募った。予断を許さない状況となったが、第 3 回標準化会議は 2021 年 6 月 7 日～9 日に開催される予定で論文募集が出されている（投稿締切り：4 月 23 日、採録通知：5 月 7 日)。

表 2. NIST PQC コンペティション応募暗号(第 3 ラウンド)

F: Finalist、A: Alternate

	電子署名	鍵カプセル化機構／暗号化	合計
格子ベース	2 Crystals-Dilithium(F), Falcon(F)	5 Crystals-Kyber(F), FrodoKEM(A), NTRU(F), NTRU Prime(A), Saber(F)	7
符号ベース	0	3 Classic McEliece(F), BIKE(A), HQC(A)	3
多変数	2 Rainbow(F), GeMSS(A)	0	2
ハッシュベース	2 Sphincs+(A), Picnic(A)	0	2
その他	0	1 SIKE(A)	1
合計	6(F:3, A:3)	9(F:4, A:5)	15

資料３別添２

ディジタル署名 EdDSA の安全性評価結果(外部評価)

1. 背景

ディジタル署名 EdDSA は、RFC8032[1] で規定され、TLS1.3 で採用された（RFC 8446 [2]）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 [3]）。TLS1.3 では楕円曲線暗号がベース仕様になると記載されており、また NIST は、2018 年以降、再三にわたり、米国政府ディジタル署名の次回改定版となる FIPS186-5 において EdDSA を追加する方針を明らかにしている[4][5]。実際、2019 年 11 月に公表された FIPS186-5 ドラフト版に EdDSA が追加されている[6]。このように EdDSA が広く一般に使われる環境が整いつつあり、その安全性が損なわれる場合甚大な影響を及ぼしかねない。2020 年度第一回暗号技術検討会の 2019 年度暗号技術活用委員会 TLS ワーキンググループ活動報告においても、その安全性評価の必要性が示されている(第一回暗号技術評価委員会配布資料資料 2-3 参照)。

2020 年度第一回暗号技術検討会において、EdDSA の安全性評価を暗号技術評価委員会において行うことが審議され承認された。

2. 外部評価概要

ディジタル署名 EdDSA について、事務局選出の暗号アルゴリズムとして CRYPTREC 暗号リストへの追加を視野に入れ、安全性評価を下記 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

I)に関する外部評価概要

［件名］：ディジタル署名 EdDSA が用いている曲線の安全性に関する調査及び評価

［依頼先］：安田雅哉 様（立教大学）
Steven Galbraith (University of Auckland)

［依頼内容］：

EdDSA で利用される曲線の安全性に関わる脆弱性について、公開されている攻撃方法の有無を調査し、存在する場合はその影響の範囲などについてまとめるなど、 対象となる曲線の安全性評価を実施する。報告書には以下の項目を含めることとする。

- EdDSA で利用される曲線に関する解説
- EdDSA で利用される曲線に関して公開されている攻撃・脆弱性の調査、および存在する場合は、その攻撃の適用条件や計算量等に関する解説
- EdDSA で利用される曲線の安全性評価
- ECDSA と比較した場合の曲線としての効率性に関する考察

なお、調査の範囲は、2020 年 8 月末までに公開された文献等を対象とする。

II)に関する外部評価概要

[件名]：ディジタル署名 EdDSA の構成の安全性に関する調査及び評価

[依頼先]：藤崎英一郎 様（北陸先端科学技術大学院大学）

Steven Galbraith（University of Auckland）

[依頼内容]：

EdDSA の構成に関わる脆弱性について、公開されている攻撃方法の有無を調査し、存在する場合はその影響の範囲などについてまとめ、また、安全性評価を実施する。報告書には以下の項目を含めることとする。

- EdDSA の構成の解説
- EdDSA の構成に関して公開されている攻撃・脆弱性の調査、および存在する場合は、その攻撃の有用性に関する解説
- EdDSA の構成としての安全性評価
- ECDSA と比較した場合の方式としての効率性に関する考察

なお、調査の範囲は、2020 年 8 月末までに公開された文献等を対象とする。

3. 外部評価レポート概要

EdDSA は、有限体上のツイスト Edwards 曲線といわれる楕円曲線上の Schnorr 署名の署名内部乱数（ノンス）[1]を署名者の秘密情報と署名される平文のハッシュ値に置き換えた確定的(deterministic)な Schnorr 署名である。EdDSA で推奨されるツイスト Edwards 曲線は RFC7748[7]で規定されるものであり Ed25519, Ed448 と記述される。

3.1. 曲線に関する安全性評価レポート概要（第二回暗号技術評価委員会配布資料参考資料 2－1、2－3）

3.1.1. EdDSA で利用される曲線

EdDSA では Edwards 曲線と呼ばれる特殊な楕円曲線やそのツイスト曲線が利用され、これらの曲線上の点の加算と 2 倍算を効率的に計算することができる。RFC8032[1]によると、EdDSA では古典計算機による攻撃に対して約 128 ビットのセキュリティレベルの Ed25519 と約 224 ビットのセキュリティレベルの Ed448 の 2 種類が推奨されている。また、Ed25519 では Curve25519、Ed448 では Curve448 と呼ばれるツイスト Edwards 曲線パラメータを利用する。

3.1.2. EdDSA で利用される曲線に関して公開されている攻撃・脆弱性

EdDSA の安全性の根拠とされている楕円曲線離散対数問題(ECDLP)に対する攻撃法は、Pollard の ρ 法や指数計算法などの任意の楕円曲線に適用できる汎用攻撃アルゴリズムと、MOV 攻撃法や SSSA 攻撃などの特殊な楕円曲線にのみ適用可能な特殊攻撃アルゴリズムに大別される。Curve25519 や Curve448 では、これらの特殊な曲線に適した既存の攻撃方法

[1] 本来、ノンスという言葉は同じ値が用いられることのない 1 回のみ使用される値を意図して使われることが多く、その値が確率的に決められるか否かについては制約がない。一方、多くの文献(例えば[8][9][10]など)で確率的署名の内部乱数がノンスと呼ばれており、これを踏襲して Schnorr 署名や ECDSA の署名時の内部乱数も本資料ではノンスと呼ぶ。さらに、EdDSA の署名時に用いる確定的な値である「署名者の秘密情報と署名される平文のハッシュ値」も複数の論文(例えば[11]など)でノンスと呼ばれており、本資料においてもこれをノンスと呼ぶ。

が有効にならないような曲線パラメータが選択されているため、汎用攻撃アルゴリズムの中で最良のρ法がEdDSAに対する最良の攻撃法である。

3.1.3. EdDSAで利用される曲線の安全性評価

EdDSAに対する最良の攻撃法であるρ法は誕生日の逆理に基づく確率的アルゴリズムであるため、第二回暗号技術評価委員会配布資料参考資料2－1ではこの攻撃法に基づいて、Curve25519及びCurve448におけるECDLPを解くにはそれぞれ$2^{125.8257}$回と$2^{222.8257}$回の楕円加算が必要であると見積もっている。そのためそれぞれのECDLPはほぼ128ビットのセキュリティレベルとほぼ224ビットセキュリティレベルを持つとしている。

第二回暗号技術評価委員会配布資料参考資料 2－3 では、量子アルゴリズムによる脅威に関しても言及している。これまでの見積もりでは、256 ビット ECDLP を解くためには2000-3000 量子ビットが必要だと思われ、誤り訂正などを考慮に入れると 600 万量子ビットが必要だと考えられる。近年の量子コンピュータの実装の進展を考えると、今後の発展を注視する必要はあるものの、これから10年間EdDSAを使い続けて問題はないと考える。

3.1.4. ECDSAと比較した場合の曲線としての効率性

楕円曲線を利用したディジタル署名では、与えられた自然数nに対して署名生成時に楕円曲線の点Pのスカラー倍算[n]Pを行い、与えられた自然数n1、n2に対して署名検証時には楕円曲線の点P1、P2の複数スカラー倍算[n1]P1+[n2]P2を主に行う。

第二回暗号技術評価委員会配布資料参考資料2－1では、同じ基礎体を利用した場合に、通常の楕円曲線とEdwards曲線における上記2種類の演算のコストを比較している。その結果、Edwards 曲線の方がスカラー倍算の場合に最大約 33%、複数スカラー倍算は最大約28%効率的に計算できると見積もっている。

3.2. 方式の構成に関する安全性評価レポート概要(第二回暗号技術評価委員会配布資料参考資料2－2、2－3)

3.2.1. EdDSA構成の特徴

Schnorr 署名との一番大きな違いは署名内部乱数(ノンス)を署名者の秘密情報と平文のハッシュ値で生成し署名を確定的かつ異なる平文に対してノンスを衝突させにくくしたことであると述べている。そのほかの違いとしては、内部で使うハッシュ関数の出力長を長くし、群の位数で剰余を取っていること、Key-prexing を採用していること、さらに群要素チェックが通常の Schnorr 署名より緩くなっていることなどを挙げている。また、PureEdDSAとHashEdDSAのどちらかのオプションを選ぶ必要がある。

3.2.2. EdDSAの構成に関して公開されている攻撃・脆弱性

近年はサイドチャネル攻撃による解析結果などがいくつか示されているが、すぐさま現実的な脅威につながる結果などは報告されていない。

3.2.3. EdDSAの構成に関する安全性

- 総評：下記の観点から、EdDSAの構成に関わる安全性において、EdDSAがECDSAに劣ると考えられる点は無いと思われると述べている。

- ✓ Schnorr 署名をもとに EdDSA は構成されているため、ランダムオラクルモデルで安全性が証明されている Schnorr 署名に対する安全性評価を参考にすることができる。
- ✓ Schnorr 署名との大きな違いはノンスの生成方法であるが、EdDSA におけるノンスの生成方法は、署名の内部乱数を弱い疑似乱数生成器に委ねることによる危険を排除し、現実的な脅威を回避するための配慮が施されている。
- ✓ 比較対象となる ECDSA については、既存結果として generic group model でのみ安全性が証明されている。

➢ 証明可能安全性：ランダムオラクルモデルや generic group model での安全性証明に関する考察結果が示されている。

第二回暗号技術評価委員会配布資料参考資料 2－3 では、構成に用いられているハッシュ関数をランダムオラクルとみなし、ECDLP(Elliptic Curve Discrete Logarithm Problem)の計算量的困難性を仮定とするランダムオラクルモデルでの安全性証明を行い、その構成に問題がないことを示している。また、スタンダードモデルで安全性は示せないものの、EdDSA に用いるハッシュ関数に必要な性質を挙げ、EdDSA で利用される SHA-512 や SHA-3 はこれらの性質を満たしていると考えることが出来るだろうと述べている。

第二回暗号技術評価委員会配布資料参考資料 2－2 では、厳密に仕様書に規定されているハッシュ関数を考慮に入れた考察を行っている。仕様書では用いるハッシュ関数が規定されており、Ed25519 では SHA-512 を、Ed448 では SHAKE256 が使われる。Ed25519 で利用される SHA-512 は、その内部の Merkle-Damgard 構造によりランダム関数と識別がついてしまう。また、その出力値を疑似ランダム関数の出力値とみなすことが出来ない。よって、SHA-512 を利用した Ed25519 をランダムオラクルモデルや generic group model で安全性解析を行うことは難しいと述べている。一方、Ed448 で利用される SHAKE256 は、ランダム関数もしくは疑似ランダム関数とみなすことが許容される。よって、SHAKE256 を利用した Ed448 には、ランダムオラクルモデルや generic group model での Schnorr 署名の解析結果が利用でき、安全性にある程度の理論的根拠を与えることができると述べている。

➢ Key-prexing：EdDSA は key-prexing という署名者自身の公開鍵を平文と連結させ、公開鍵と平文に署名を付けさせる形を取っている。この仕様のため関連鍵攻撃のような攻撃を回避できるようになっていると述べている。

➢ 複数署名者での安全性：通常の署名方式は署名者が増えると署名者の数に応じて証明可能安全性で保障できるビットのセキュリティレベルは劣化するが、EdDSA は複数署名者の下でのセキュリティレベルが署名者の数に関係せず、単一署名者の Schnorr 署名のビットのセキュリティレベルで抑えることができると述べている。

➢ ノンスについて：Schnoor 署名との違いの一つに署名生成に用いるノンスの扱いが挙げられる。第二回暗号技術評価委員会配布資料参考資料 2－2 では、下記の考察を述べている。SHA-512 を利用した Ed25519 では、証明可能安全性の意味では証明がつかなくなっているが、現実の攻撃を考えると異なる平文に対するノンスの衝突こそが一番に回避しなければならないものであり、ハッシュ関数でノンスを生成することでこれを回避している。

➢ サイドチャネル攻撃耐性：EdDSA に関するサイドチャネル攻撃耐性として優位な点及び気を付けるべき点を挙げている。

第二回暗号技術評価委員会配布資料参考資料 2－2 では、EdDSA はノンスが漏洩しづらくする工夫をしているためノンスの漏洩を利用する攻撃（タイミング攻撃や電力解析攻撃な

ど)に対して ECDSA より安全と考えても良いと述べている。一方、ノンスを確定的にしたことに対する新たなフォールト攻撃も提案されており、サイドチャネル攻撃が可能な組み込みデバイスとして利用するような場合ではなんらかの対策をとることが望ましいということも述べている。

第二回暗号技術評価委員会配布資料参考資料 2－3 においても類似の見解を示している。

3.2.4. EdDSA に関する効率評価

- ECDSA との比較：署名検証の計算時間については、EdDSA についてはバッチ処理を適用することができるが、ECDSA については同様のバッチ処理が適用可能であるかは明らかではなく、EdDSA 署名ほどの高速化技法は知られていない。そのため、一般的にはバッチ処理を適用した場合の EdDSA の署名検証は、ECDSA に比べ高速になることが期待できると述べている。第二回暗号技術評価委員会配布資料参考資料 2－2 ではさらに厳密な下記の考察を示している。署名される平文がさほど長くない（平文をハッシュする時間が十分短い）場合、署名生成時間および検証時間いずれについても EdDSA が ECDSA よりやや短い。ただし平文が極めて長い(署名生成時間はほぼハッシュ関数の計算時間となってしまう)場合、EdDSA の署名生成時間の方が長く、署名検証時間は両方式でほぼ同程度である。

4. 暗号技術評価委員会としての見解

4.1. 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二つの曲線 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。

4.2. 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、3.2.3 の総論にて述べられているように 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、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。

評価報告書(第二回暗号技術評価委員会配布資料参考資料 2－1,2－2,2－3)により、EdDSA の曲線の安全性・方式構成の安全性に問題がないことを把握することができたことから、本報告書を CRYPTREC の外部評価報告書としてホームページにて公開する。

5. 今後の予定

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。このことから、「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。

【参考文献】

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

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

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

[4] NIST, “NIST Update (CHES version)”, CHES rump talk, 2018

[5] NIST, “NIST status update on Elliptic Curves and Post-Quantum Crypto”, NIST Threshold Cryptography Workshop 2019, 2019

[6] NIST, “Digital Signature Standard (DSS)”, FIPS PUB 186-5 (Draft), 2019

[7] RFC7748, “Elliptic Curves for Security”, Jan. 2016

[8] Phong Q. Nguyen, Igor E. Shparlinski, “The Insecurity of the Digital Signature Algorithm with Partially Known Nonces”, J. Cryptol. 15(3): 151-176 (2002)

[9] Phong Q. Nguyen, Igor E. Shparlinski,“The Insecurity of the Elliptic Curve Digital Signature Algorithm with Partially Known Nonces”, Des. Codes Cryptogr. 30(2): 201-217 (2003)

[10] Diego F. Aranha, Pierre-Alain Fouque, Benoît Gérard, Jean-Gabriel Kammerer, Mehdi Tibouchi, Jean-Christophe Zapalowicz, “GLV/GLS Decomposition, Power Analysis, and Attacks on ECDSA Signatures with Single-Bit Nonce Bias”, ASIACRYPT (1) 2014: 262-281

[11] Diego F. Aranha, Claudio Orlandi, Akira Takahashi, Greg Zaverucha, “Security of Hedged Fiat-Shamir Signatures Under Fault Attacks”, EUROCRYPT (1) 2020: 644-674

以上

資料３別添３

2020 年度暗号技術調査 WG（暗号解析評価）活動報告

1. 2020 年度暗号技術調査 WG（暗号解析評価）活動報告の概要

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。

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)の設置を継続して下記の調査を実施する。

(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

(2)Shor の量子アルゴリズムによる現代暗号[1]への脅威に関する調査

(3)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）

2. 委員構成（敬称略）

主査：國廣 昇（筑波大学）
委員：青木 和麻呂（文教大学）
委員：草川 恵太（NTT）
委員：桑門 秀典（関西大学）
委員：下山 武司（国立情報学研究所）
委員：高木 剛（東京大学）
委員：高島 克幸（三菱電機）
委員：峯松 一彦（NEC）
委員：安田 貴徳（岡山理科大学）
委員：安田 雅哉（立教大学）

3. 「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

3.1. 今後の予測図の取り扱いについて

2019 年度第 2 回暗号技術評価委員会にて決定した「今後の予測図の取り扱い」(下記の枠内左)の方針は、2020 年度第 1 回暗号技術検討会にて了承された。

今後はこの方針に従って予測図を更新する。ただし、外挿の範囲は年度末から 20 年後までとする（下記の枠内右)。

<今後の予測図の取り扱い>（昨年度からの抜粋)	<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）まで直線で引き、評価に大きな変	(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、評価に大きな変動がないと考え

[1] 本資料では、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。

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。	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。

【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
　予測図の取り扱いの報告

・2021 年 2 月 3 日　第 2 回 暗号解析評価 WG
　予測図の更新の報告・承認

3.2. 予測図の更新結果の報告

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、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 1, 2）。

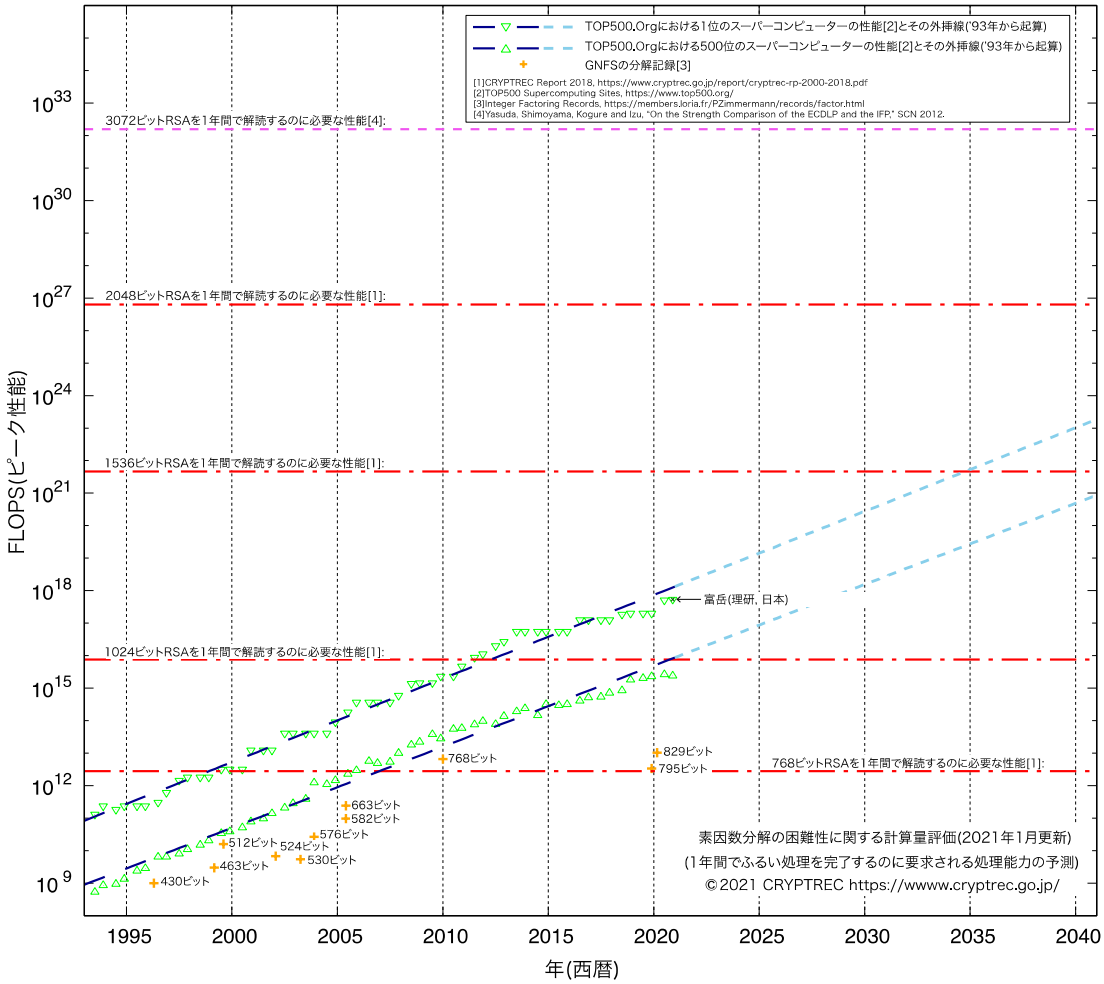


図 1：素因数分解の困難性に関する計算量評価(2021 年 1 月更新)

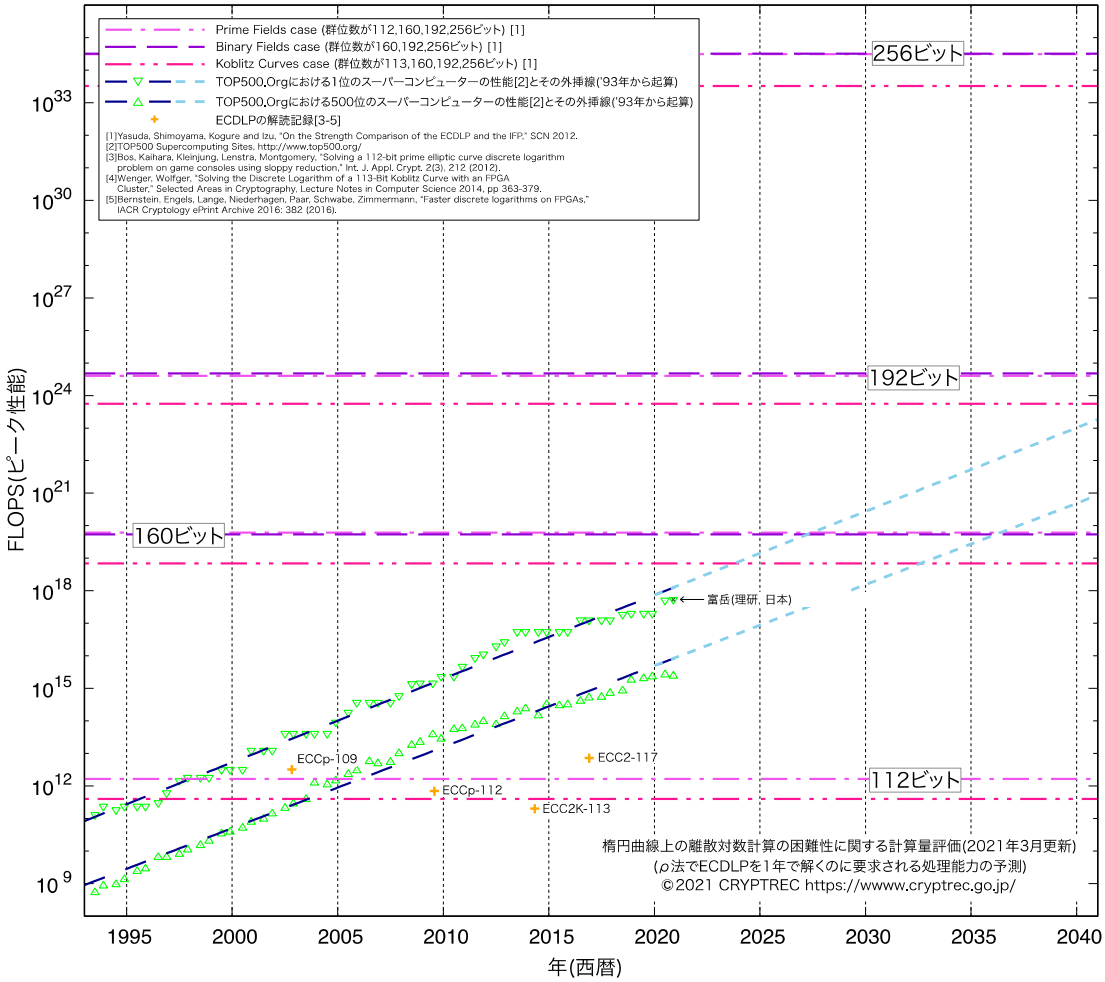


図 2：楕円曲線上の離散対数計算の困難性に関する計算量評価(2021 年 1 月更新)

4. 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

4.1. 背景及び調査の概要

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[2]。

4.2. 実施内容

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について、事務局が本件を担当すること及び具体的な調査内容が第一回暗号解析評価 WG（2020 年 8 月 26 日）にて承認された。

[2] 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。

【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。

【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
調査報告書（案）に対する WG の見解をまとめる。

4.3. WG としての見解

調査内容及び報告書の概要の項目 2)について、第 2 章で Shor のアルゴリズムの実装・リソース評価の把握の重要性をまとめている。Shor のアルゴリズムは、多項式時間で素因数分解や離散対数問題を解けるために理論的には大きな脅威だが、実験的に暗号で用いるような大きなパラメータに対してこれらの問題を解いたという報告はこれまで行われていない。そのため、現状どの程度のパラメータまで実験的に適用可能なのか、実際に暗号で用いるような大きなパラメータの問題を解くにはどの程度の性能の量子計算機が必要なのかを把握しておくことは重要である。

調査内容及び報告書の概要の項目 3)について、第 3 章で量子計算の基礎を、第 4 章で Shor のアルゴリズムの概要をまとめている。第 3 章では、量子ビット、測定の概念と Shor のアルゴリズムを理解するのに必要な量子ゲートをまとめている。第 4 章では、量子フーリエ変換や位数計算アルゴリズム、周期計算アルゴリズムを説明した後に素因数分解や離散対数問題のための Shor のアルゴリズムをまとめている。

調査内容及び報告書の概要の項目 4)について、第 5 章で既存の Shor のアルゴリズムの実装結果をまとめている。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、大半の実験では一般的な合成数に対しては適用できない大幅な量子ゲートの削減などを行うことで実験を成功させている。また、求めたい値を陽に利用した量子回路を用いた実験もあり、このような場合には任意の大きさの合成数が素因数分解可能であるが、一般の合成数に適用することはできない。また、他の実験と比べて極端な量子回路の効率化を行わずに 21 の素因数分解に成功した実験があるが、この論文では 35 の素因数分解にも試みており、このとき実験は成功しなかったと結論づけている。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。

調査内容及び報告書の概要の項目 5)について、第 6 章で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を行った研究をまとめている。一連の研究は、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。

5. 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）

5.1. 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[3]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[4][5]。

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。

5.2. 実施内容

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。

[件名]：PQC のハイブリッドモードに関する調査

[依頼先]：菅野 哲 様（株式会社レピダム）

選出理由：IEEE や IETF などの標準化団体での暗号技術に関する標準化活動の推進などに多くの実績があり、本件の調査対象であるハイブリッドモードの近年の標準化動向について広い知見をお持ちであり、本評価報告書をご執筆いただくために必要な情報収集や調査を実施可能な方であるため。

[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。

---

[3] 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。

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

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

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。

【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。

5.3. 評価報告書のまとめ(菅野氏による見解)

評価報告書では、調査対象とした標準化団体・組織においては、PQC と現代暗号の双方を併用するハイブリッドモードについて明確に言及/定義している文書は見つからなかったことが報告されている。一方、調査によりハイブリッドモードに関わる以下の動向が明らかとなったと報告されている。

[動向 1] PQC と現代暗号の双方を併用するハイブリッドモードの導入が検討されている背景として、調査対象とした標準化団体・組織では 3 つの懸念を抱えている。

- 懸念 1) 従来の暗号技術の安全性への懸念:量子コンピュータによる暗号技術への脅威が現実的になった時には、従来の暗号技術が安全性を保てなくなることへの懸念。
- 懸念 2) PQC の安全性への懸念:従来の暗号技術と比較して、PQC そのものが長期間利用されていないことから PQC の安全性評価手法などが成熟していないために、今後、脆弱性が発見されることへの懸念。
- 懸念 3) PQC の運用上の懸念:ネットワーク上に配置されている機器が PQC に対応していない場合に通信できない可能性への懸念。および、PQC を利用できる製品や環境がないことへの懸念。

[動向 2] PQC と現代暗号の双方を併用するハイブリッドモードを検討している標準化団体・組織では、ハイブリッドモードを導入することによりこれらの懸念を解消し、下記を達成する方法が議論されている。

I. 安全性の確保:ハイブリッドモード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ハイブリッドモードとしての安全性を保つ。(懸念 1 及び懸念 2 への対策)
II. 後方互換性の確保:標準化やソフトウェア/ハードウェアへの実装のためのバッファ期間を確保し、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。(懸念 3 への対策)

PQC と現代暗号の双方を併用するハイブリッドモードの適用領域に関する評価報告書の記載概要は次のとおり。

- 暗号アルゴリズムとしては、ハイブリッドモードでの「鍵交換」と「ディジタル署名」での利用が有望であると多くの標準化団体・組織が述べている。ハイブリッドモードでの鍵交換については学術的な研究成果も発表されている。「鍵交換」と「ディジタル署名」については、ハイブリッドモードを適用することにより“I.安全性の確保”を達成することが模索されている。
- ネットワークプロトコルや証明書としては、「TLS」、「SSH」、「X.509 証明書」等を対象として、ハイブリッドモードでの鍵交換やハイブリッドモードでのディジタル署名の導入に向けた議論が IETF、Open Quantum-Safe(OQS)[6] などで行われている。例えば、IETF の TLS WG においては、TLS1.3 でハイブリッドモードを利用可能にするための Internet Draft が Working Group の検討項目として採択されるなど重要なテーマとしてコンセンサスが得られている。Open Quantum-Safe (OQS) では、NIST が主催している標準化会議で候補として残っている PQC を OpenSSL などに実装し、実際の世の中で利用されている TLS プロトコルや SSH プロトコルでの実現可能性を検討している。「TLS」、「SSH」、「X.509 証明書」等については、ハイブリッドモードでの鍵交換やハイブリッドモードでのディジタル署名の導入による“I.安全性の確保”を達成する方法が議論されている一方、“II.後方互換性の確保”の実現も併せて検討されている。

PQC と現代暗号の双方を併用するハイブリッドモードの構成に関わる安全性解析については、評価報告書では下記のようにまとめられている。

- 本調査の範囲において、ハイブリッドモードの脆弱性に関する文献は発見されなかった。しかし、ハイブリッドモードの安全性評価については現在のところ明らかになっていないところもある。

5.4. WG としての見解

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 の外部評価レポートとして HP に公開する。

5.3 節の評価報告書のまとめに記載した通り、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、以下の二つの要件について議論されることが多い。

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[1][2]。
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[1]。

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

[6] Waterloo 大学を中心とした「PQC の開発とプロトタイピングをサポートする」プロジェクト

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。

以上

[参考文献]

[1] 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.

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

資料３別添４

仕様書の参照先の変更について

１．　背景・目的

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ます[1]。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ため、参照先の変更が必要になっています。仕様書に変更がある場合は、新旧仕様書の差分を調査して、その内容が軽微な修正であると事務局にて判定できる場合には、CRYPTREC の Web サイトの仕様書の参照先の修正を行ってきています。

２．　報告内容

上記の暗号技術について、アルゴリズムの部分に変更がなかったので、新しい仕様書へ参照先の変更を行った（表 2）。

表１：ChaCha20-Poly1305 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 2：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

以上

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

資料３別添５

ガイドラインに関する今後の方針について

1. 目的

2020 年度第一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[1][2]。

このため、暗号技術評価委員会では、当該ガイドラインの作成を検討する必要がある。

2. 検討事項

（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。

以上

---

[1] 2020 年度 第 1 回 暗号技術検討会 議事概要 (CRYPTREC MT-1010-2020) https://www.cryptrec.go.jp/report/cryptrec-mt-1010-2020.pdf

[2] (第 1 回)【資料】(CRYPTREC MT-1011-2020) https://www.cryptrec.go.jp/report/cryptrec-mt-1011-2020.pdf

資料４

2020 年度　暗号技術活用委員会活動報告

1.　2020 年度の活動内容と成果概要

1.1　活動内容

活用委員会では、情報システム全般のセキュリティ確保に寄与することを目的として、暗号の取り扱いに関する観点から必要な活動を行っている。

2020 年度は、新型コロナウイルスの感染拡大防止の観点から延期とした 2019 年度第二回会合の代替会合を 2020 年 6 月 1 日に開催し、その後「TLS 暗号設定ガイドライン」及び「暗号鍵管理システム設計指針（基本編）」の公開（2020 年 7 月 7 日公開）に向けた作業を行ったなどの影響により、実質的に下期のみの活動となった。

このため、今年度の活動内容としては、2021 年度からの運用ガイドラインの整備に向けて、「鍵長ガイドライン（仮）」の作成方針の取りまとめ、及び「暗号鍵管理の参照プロファイル」の作成に向けた検討を開始することとした。

（1）鍵長ガイドライン（仮）の作成方針の取りまとめ

CRYPTREC 暗号リストでの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、2020 年度は作成方針案の取りまとめまでを行った。

（2）暗号鍵管理の参照プロファイルの作成に向けた検討

2020 年 7 月に、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。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、2020 年度は今後の進め方を取りまとめるところまでを行った。

1.2　暗号技術活用委員会の委員構成及び開催状況

暗号技術活用委員会の委員構成は表 1-1 のとおりである。

また、2020 年度に開催された暗号技術活用委員会での審議概要は表 1-2 のとおりである。なお、第一回は新型コロナウイルス感染拡大防止の観点から延期とした 2019 年度第二回会合の代替会合として開催したものである。

表 1-1 暗号技術活用委員会　委員構成

委員長	松本　勉	横浜国立大学　大学院環境情報研究院　教授
委員	上原　哲太郎	立命館大学　情報理工学部　情報理工学科　教授
委員	宇根　正志	日本銀行金融研究所　情報技術研究センター 情報技術研究グループ長［2020 年 9 月まで］
委員	田村　裕子	日本銀行金融研究所　情報技術研究センター 企画役補佐［2020 年 9 月から］
委員	垣内　由梨香	マイクロソフト株式会社　セキュリティレスポンスチーム セキュリティプログラムマネージャー
委員	菊池　浩明	明治大学　総合数理学部　先端メディアサイエンス学科　教授
委員	須賀　祐治	株式会社インターネットイニシアティブ セキュリティ本部セキュリティ情報統括室　シニアエンジニア
委員	杉尾　信行	株式会社 NTT ドコモ　情報セキュリティ部
委員	手塚　悟	慶應義塾大学　環境情報学部　教授
委員	寺村　亮一	株式会社イエラエセキュリティ　執行役員 高度解析部　部長
委員	松本　泰	セコム株式会社　IS 研究所　コミュニケーションプラットフォーム ディビジョン　マネージャー
委員	三澤　学	三菱電機株式会社　情報技術総合研究所 情報ネットワーク基盤技術部　主席研究員
委員	満塩　尚史	内閣官房　IT 総合戦略室　政府 CIO 補佐官
委員	山岸　篤弘	一般財団法人日本情報経済社会推進協会 電子署名・認証センター　客員研究員
委員	山口　利恵	国立大学法人東京大学　大学院情報理工学系研究科 ソーシャル ICT 研究センター　特任准教授
委員	渡邊　創	国立研究開発法人産業技術総合研究所 サイバーフィジカルセキュリティ研究センター　副研究センター長

表 1-2　暗号技術活用委員会　開催状況

回	開催日	議案
第一回	2020 年 6 月 1 日	■ TLS 暗号設定ガイドライン WG 活動及びガイドライン案について ■ 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 ■ 暗号鍵管理システム設計指針（基本編）について ■ 2020 年度暗号技術活用委員会活動案について
第二回	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
第三回	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（二回目） ■ 2020 年度暗号技術活用委員会活動報告案について

2. 成果概要

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、第二回と第三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

鍵長の選択にあたっては、「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、以下の表のとおりである。

	「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。

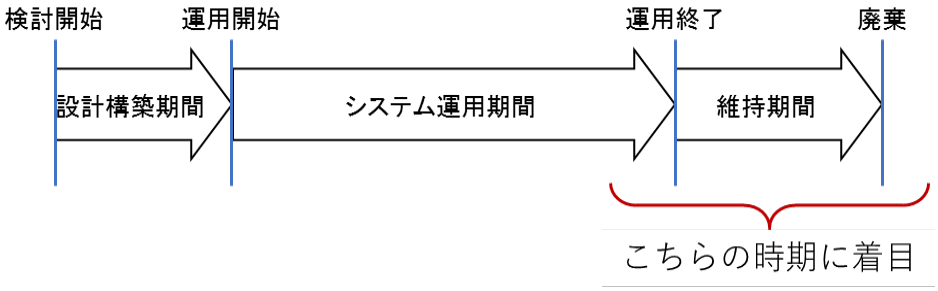
安全性基準の考え方

- **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。

- **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。



- **「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。

- **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。

- **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。

	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。

<u>ガイドラインで示すべき内容（項目）</u>

- 「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。

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、第三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あたり、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。

	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

資料5

暗号技術検討会
２０２０年度　報告書（案）

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。

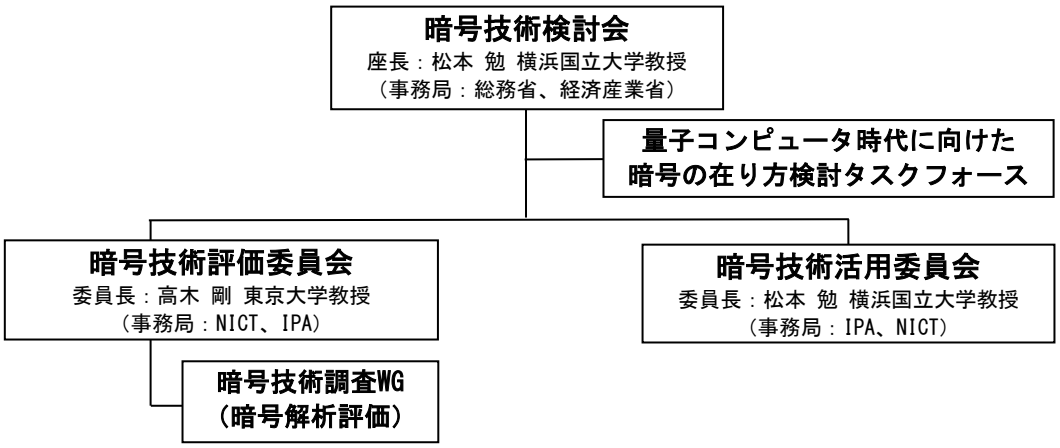


図2.2-1　2020年度CRYPTREC体制図

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～**:**（検討会の閉会時刻を記載）

（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）

検討会での議論を基に作成

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の評価が行われ、2020年７月から表3.1-1の７（＋α）方式について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 候補暗号

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。

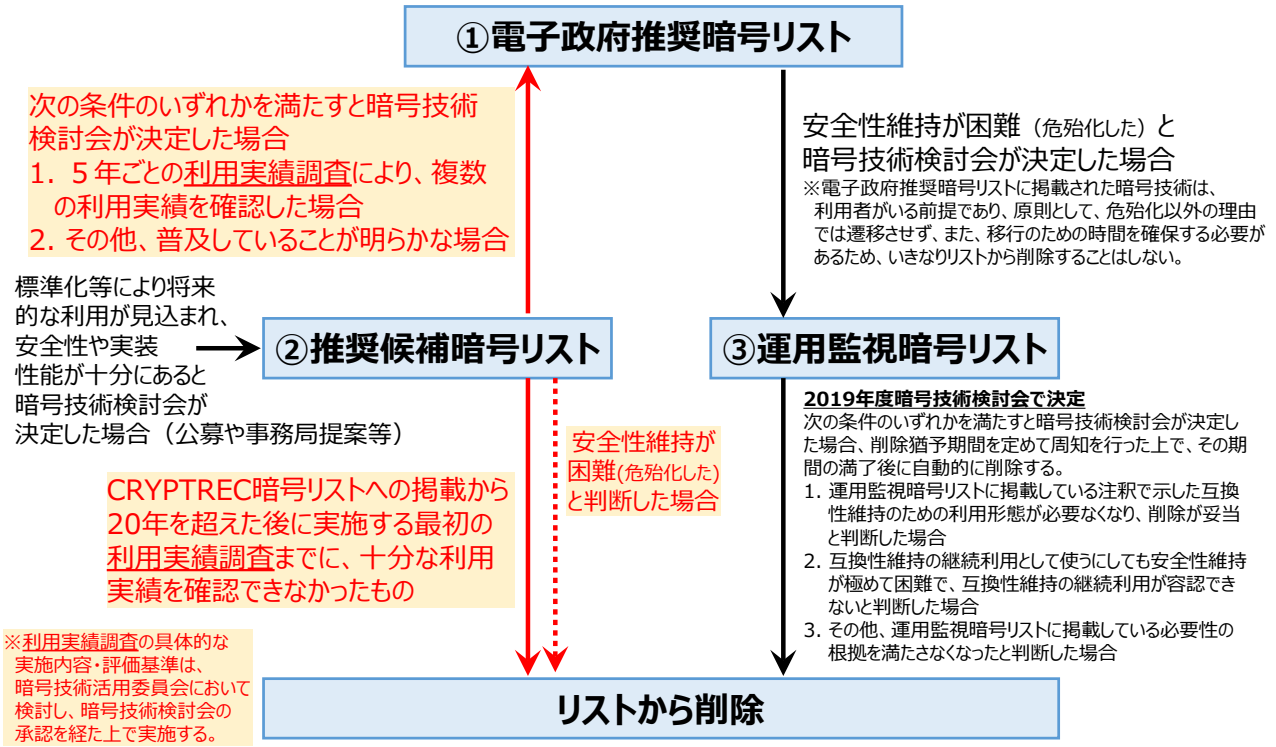


図3.1-2　CRYPTREC暗号リスト移行ルール

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。

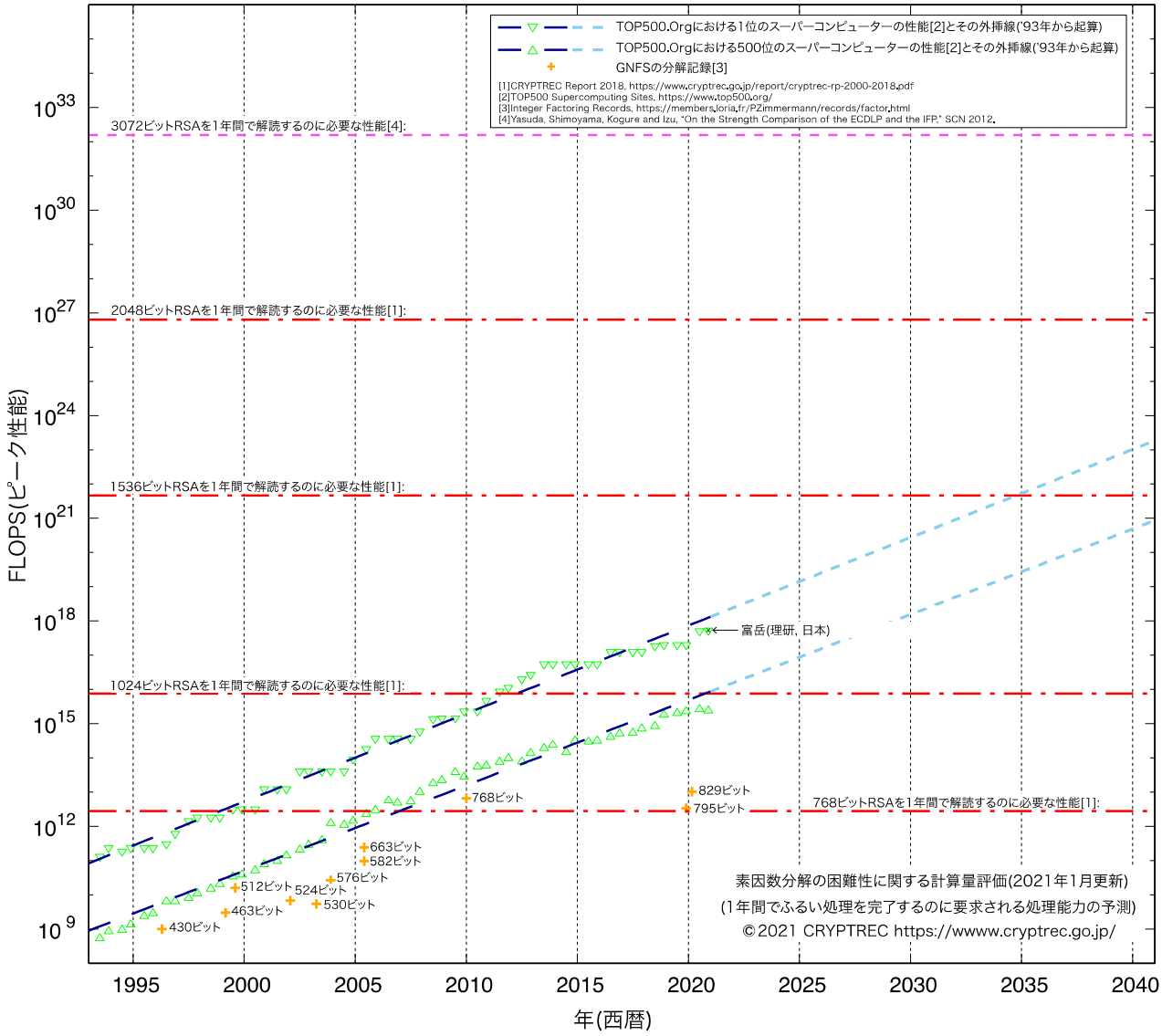


図3.2-1：素因数分解の困難性に関する計算量評価（2021年1月更新）[8]

[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。

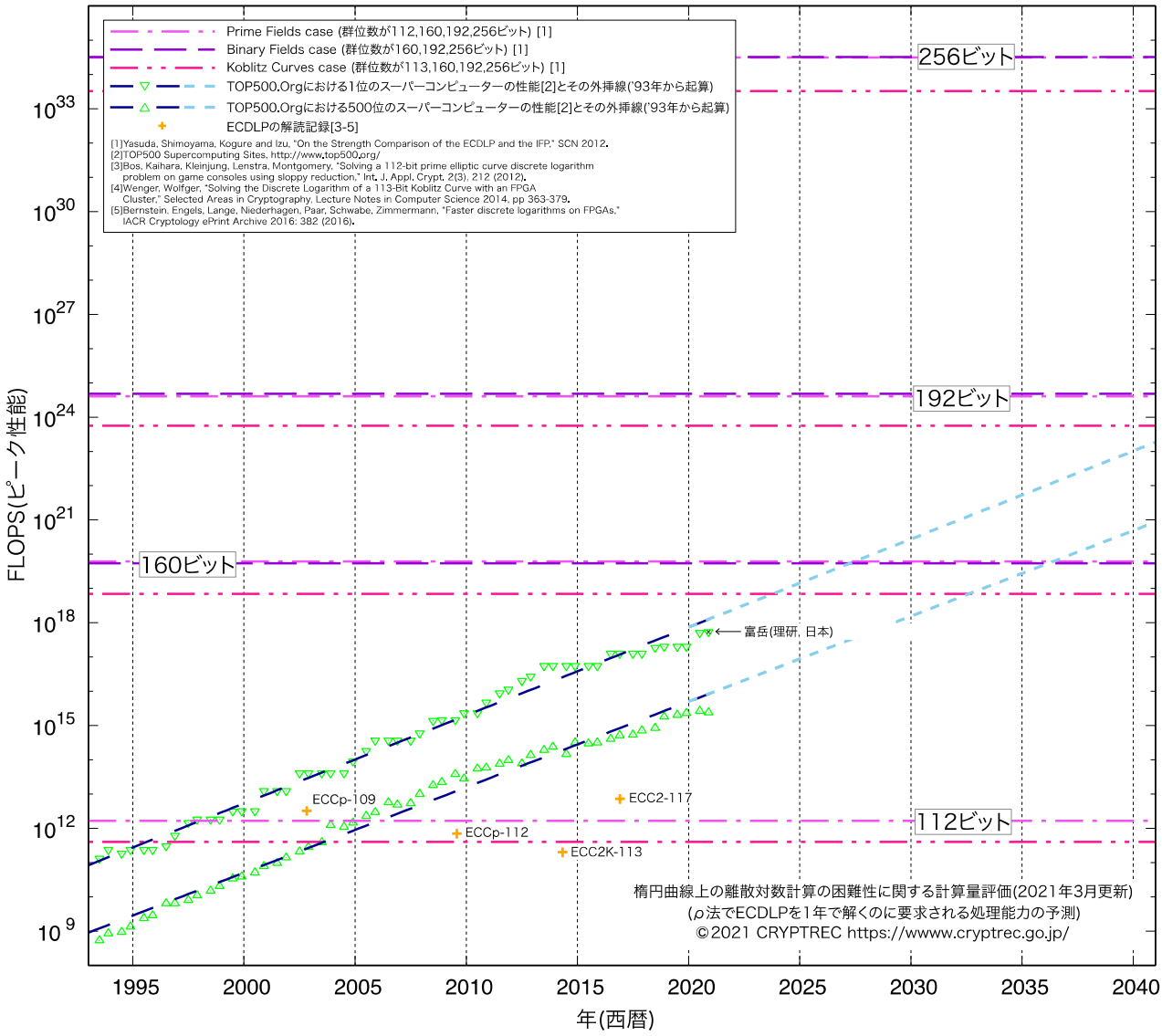


図3.2-2：楕円曲線上の離散対数計算の困難性に関する計算量評価（2021年1月更新）[9]

[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[14]。

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。

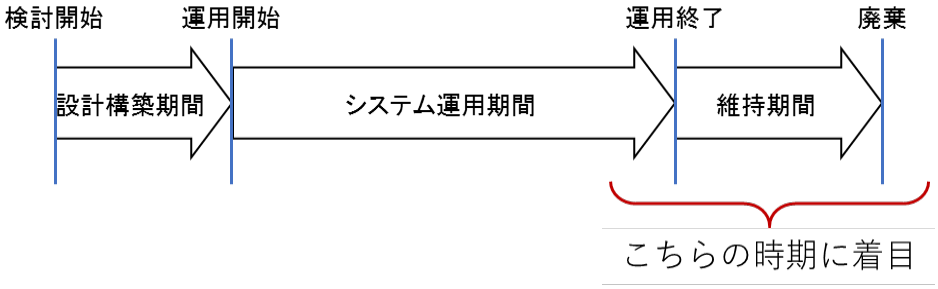


図3.3-2： システムのライフサイクル

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。

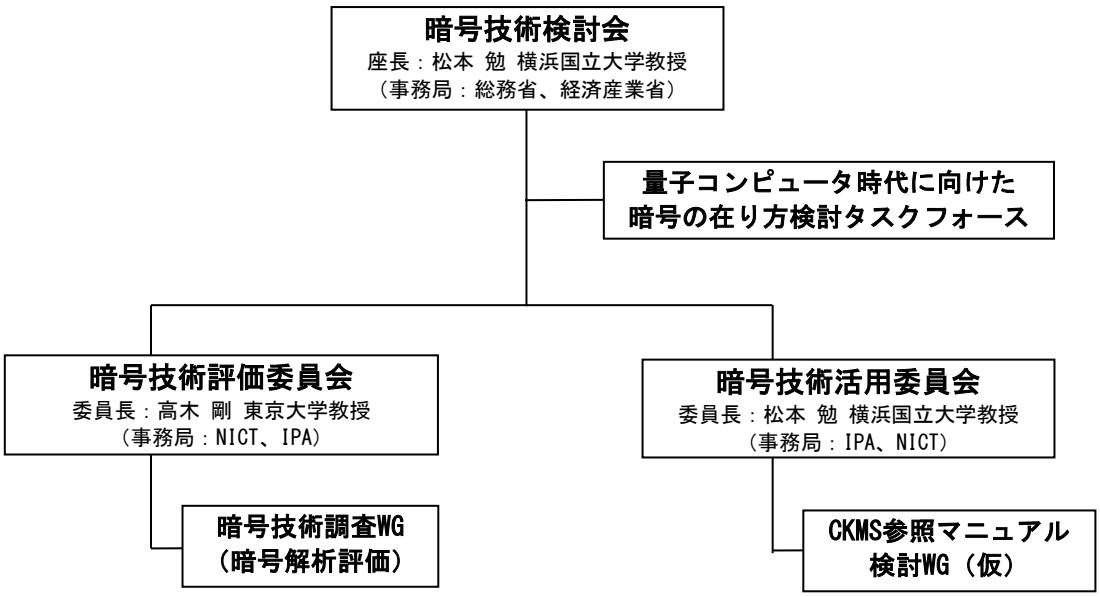


図4-1 2021年度CRYPTRECの体制図（予定）

参考資料１

「暗号技術検討会」開催要綱

１　名　称

本検討会は「暗号技術検討会」（以下「検討会」という。）と称する。

２　開催の趣旨・目的

検討会は、総務省サイバーセキュリティ統括官及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、総務省及び経済産業省における施策の検討に資することを目的として開催する。

３　検討事項

（１）CRYPTREC暗号リスト掲載暗号技術の監視

（２）CRYPTREC暗号リスト掲載暗号技術の安全性及び信頼性確保のための調査・検討

（３）CRYPTREC暗号リストの改定に関する調査・検討

（４）CRYPTREC暗号リスト掲載暗号技術の普及促進及び暗号技術の利用促進・産業化に向けた取組の検討

（５）その他、システム全体のセキュリティ確保のために必要となる活動の検討等、暗号技術の評価及び利用に関すること

４　構成等

（１）検討会の構成は、別紙１のとおりとする。

（２）検討会には、座長１名を置く。

（３）座長は、構成員の互選により定める。

（４）座長は、検討会構成員の中から顧問及び座長代理を指名できる。

（５）構成員の任期は委嘱時に定めるものとし、再任を妨げないものとする。

５　運営

（１）座長は、検討会の議事を掌握する。

（２）座長が、緊急の理由によりやむを得ず不在となった場合、座長代理が座長に代わり議事を掌握する。

（３）関係する政府機関等で、座長が特に認めたものについては、オブザーバとして検討会に出席することができる。

（４）座長が必要と認めるときは、暗号技術の提案者、関連する利害関係者その他の参考人から意見を聴取することができる。

（５）座長は、検討会が調査する事項について特に専門的な調査を行う必要があると認めるときは、委員会等を置くことができる。
（６）座長は、必要があると認めるときは電子メールによる審議を行うことができる。なお、この審議を行った場合は、次の検討会において当該審議の結果を報告するものとする。
（７）その他検討会の運営に関し必要な事項は、座長が定めるところによる。

６　スケジュール

検討会は、年度内に１回以上開催する。

７　開催方法

検討会は、集合開催を原則とするが、必要に応じ、その一部又は全部をオンラインにより開催することができることとする。

８　議事・資料等の取扱い

別紙２のとおりとする。

９　庶　務

検討会の庶務は、総務省サイバーセキュリティ統括官室及び経済産業省商務情報政策局サイバーセキュリティ課において処理する。

（令和２年６月１９日　最終改訂）

別紙１

暗号技術検討会　構成員・オブザーバ名簿

2021.3.30現在

構成員

今井　正道	一般社団法人情報通信ネットワーク産業協会　常務理事
上原哲太郎	立命館大学　情報理工学部　教授
宇根　正志	日本銀行　金融研究所　情報技術研究センター　情報技術研究グループ長
太田　和夫	国立大学法人電気通信大学　名誉教授
高木　　剛	国立大学法人東京大学大学院　情報理工学系研究科　教授
近澤　　武	独立行政法人情報処理推進機構　セキュリティセンター セキュリティ技術評価部暗号グループ　主任研究員
手塚　　悟	慶應義塾大学　環境情報学部　教授
本間　尚文	国立大学法人東北大学　電気通信研究所　教授
松井　　充	三菱電機株式会社　開発本部　役員技監
松浦　幹太	国立大学法人東京大学 生産技術研究所　教授
松本　　勉	国立大学法人横浜国立大学大学院　環境情報研究院　教授
松本　　泰	セコム株式会社　IS研究所 コミュニケーションプラットフォームディビジョン　マネージャー
向山　友也	一般社団法人テレコムサービス協会　技術・サービス委員会　副委員長
渡邊　　創	国立研究開発法人産業技術総合研究所 サイバーフィジカルセキュリティ研究センター 副研究センター長

（五十音順、敬称略）

オブザーバ

内閣官房内閣サイバーセキュリティセンター　内閣参事官（政府機関総合対策担当）
個人情報保護委員会事務局　参事官
警察庁　情報通信局　情報管理課　情報セキュリティ対策官
総務省　行政管理局　調査官
総務省　自治行政局　住民制度課長
法務省　民事局　商事課長
外務省　大臣官房　情報通信課長
財務省　大臣官房　文書課　業務企画室長
文部科学省　大臣官房　政策課　サイバーセキュリティ・情報化推進室長
厚生労働省　大臣官房参事官（サイバーセキュリティ・情報システム管理担当）
経済産業省　産業技術環境局　国際電気標準課長
防衛省　整備計画局　情報通信課　AI・サイバーセキュリティ推進室長
国立研究開発法人情報通信研究機構　サイバーセキュリティ研究所長
国立研究開発法人産業技術総合研究所　サイバーフィジカルセキュリティ研究センター　高機能暗号研究チーム長
独立行政法人情報処理推進機構　技術本部セキュリティセンター長
一般財団法人日本情報経済社会推進協会　電子署名・認証センター長
公益財団法人金融情報システムセンター　監査安全部長

別紙２

暗号技術検討会の公開について

１　会議の公開について

（１）民間企業の暗号技術（既製品を含む）の解読方法等について議論を行う可能性があり、当事者又は第三者の権利、利益や公共の利益を害するおそれがあるため、検討会は原則非公開とする。

（２）検討会の出席者は、検討会において知り得た情報で、当事者又は第三者の権利、利益や公共の利益を害するおそれがあるものについては、検討会の出席者及び座長が特に認めた者以外に漏えいしてはならないものとする。

２　検討会の資料の公開について

（１）検討会の資料については、原則公開とする。

（２）ただし、検討会の資料を公開することにより、当事者又は第三者の権利、利益や公共の利益を害するおそれがある場合は、検討会は資料の公開を延期又は非公開とすることができる。

（３）資料は、ホームページ（cryptrec.go.jp）への掲載その他の方法により公開するものとする。

３　議事概要の公開について

（１）議事概要については、原則公開とする。

（２）ただし、議事概要を公開することにより、当事者又は第三者の権利、利益や公共の利益を害するおそれがある場合は、議事概要の該当部分を削除した上で公開することができる。

（３）議事概要は、ホームページ（cryptrec.go.jp）への掲載その他の方法により公開するものとする。

電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）

平成25年3月1日
総務省・経済産業省
（最終更新：令和2年12月21日）

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]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。

技術分類		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号(注2)	該当なし
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード(注13)	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
認証暗号		該当なし
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

[1] 総務省サイバーセキュリティ統括官及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、総務省及び経済産業省における施策の検討に資することを目的として開催。

[2] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

（注1） 「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」（平成20年４月情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
https://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成25年３月１日現在）

（注2） CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注4） 初期化ベクトル長は96ビットを推奨する。

（注13） CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

推奨候補暗号リスト

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[3]のリスト。

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM(注5)
共通鍵暗号	64ビットブロック暗号(注6)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128ビットブロック暗号	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
		SC2000
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01(注7)
ハッシュ関数		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128(注12)
		SHAKE256(注12)
暗号利用モード	秘匿モード	XTS(注17)
	認証付き秘匿モード(注14)	該当なし
メッセージ認証コード		PC-MAC-AES
認証暗号		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-4

（注5） KEM (Key Encapsulating Mechanism) - DEM (Data Encapsulating Mechanism) 構成における利用を前提とする。

（注6） CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注7） 平文サイズは64ビットの倍数に限る。

（注12） ハッシュ長は256ビット以上とすること。

（注14） CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

（注17） 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] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

運用監視暗号リスト

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[4]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。

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5(注8)(注9)
	鍵共有	該当なし
共通鍵暗号	64ビットブロック暗号(注15)	3-key Triple DES
	128ビットブロック暗号	該当なし
	ストリーム暗号	128-bit RC4(注10)
ハッシュ関数		RIPEMD-160
		SHA-1(注8)
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード(注16)	該当なし
メッセージ認証コード		CBC-MAC(注11)
認証暗号		該当なし
エンティティ認証		該当なし

（注8） 「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」（平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
https://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成25年3月1日現在）

（注9） TLS 1.0, 1.1, 1.2で利用実績があることから当面の利用を認める。

（注10） 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。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。

（注11） 安全性の観点から、メッセージ長を固定して利用すべきである。

（注15） CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注16） CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

[4] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

変更履歴情報

変更日付	変更箇所	変更前の記述	変更後の記述
平成27年3月27日	（注10）	128-bit RC4は、SSL（TLS1.0以上）に限定して利用すること。	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。
平成28年3月29日	推奨候補暗号リスト（技術分類：ハッシュ関数）	該当なし	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256（注12）
	（注12）	[新規追加]	ハッシュ長は256ビット以上とすること。
平成29年3月30日	推奨候補暗号リスト（技術分類：ハッシュ関数）	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256（注12）	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE128（注12） SHAKE256（注12）
平成30年3月29日	（注2） （注6）	より長いブロック長の暗号が利用できるのであれば、128ビットブロック暗号を選択することが望ましい。	CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。
	（注15）	[新規追加]	
	電子政府推奨暗号リスト（技術分類：共通鍵暗号）	3-key Triple DES（注3）	該当なし
	（注3）	3-key Triple DESは、以下の条件を考慮し、当面の利用を認める。 1） NIST SP 800-67として規定されていること。 2） デファクトスタンダードとしての位置を保っていること。	[削除]
	運用監視暗号リスト（技術分類：共通鍵暗号）	該当なし	3-Key Triple DES（注15）
	電子政府推奨暗号リスト	[技術分類の新設]	技術分類：認証暗号 暗号技術：該当なし
	推奨候補暗号リスト		技術分類：認証暗号 暗号技術：ChaCha20-Poly1305
	運用監視暗号リスト		技術分類：認証暗号 暗号技術：該当なし

	（注13） （注14） （注16）	[新規追加]	CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。
	電子政府推奨暗号リスト（見出し）	名称	暗号技術
	推奨候補暗号リスト（見出し）		
	運用監視暗号リスト（見出し）		
令和２年12月21日	推奨候補暗号リスト（技術分類：暗号利用モード　秘匿モード）	該当なし	XTS（注17）
	（注17）	[新規追加]	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。