資料１

2020年度 第１回 暗号技術検討会

令 和 ２ 年 ６ 月 １ ９ 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) 2019年度暗号技術評価委員会 活動報告について【報告】
(3) 2019年度暗号技術活用委員会 活動報告について【報告】
(4) XTSの推奨候補暗号リストへの追加について【審議】
(5) 運用監視暗号リストからの削除ルール及びRC4の取扱いについて【審議】
(6) 暗号技術検討会　2019年度　報告書（案）について【承認】
(7) 2020年度暗号技術評価委員会 活動計画について【承認】

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	「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」の活動について
資料３	2019年度暗号技術評価委員会 活動報告
資料３別添１	現在の量子コンピュータによる暗号技術の安全性への影響
資料３別添２	暗号利用モードXTSについて
資料３別添３	2019年度暗号技術調査WG（暗号解析評価）活動報告
資料４	2019年度暗号技術活用委員会 活動報告
資料４別添１	EdDSAに関する安全性評価の必要性について
資料４別添２	暗号鍵管理システム設計指針（基本編）概要
資料４別添３	TLS暗号設定ガイドライン概要
資料５	XTSの推奨候補暗号リストへの追加について
資料６	運用監視暗号リストからの削除ルール及びRC4の取扱いについて
資料７	暗号技術検討会　2019年度　報告書（案）
資料８	2020年度暗号技術評価委員会 活動計画(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

(注)本会合の議事(1)～(6)については、2019 年度 暗号技術検討会が新型コロナウイルス感染症拡大防止の観点から延期となったものです。

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る。

こうした中、現行のCRYPTREC暗号リストの策定（2013年３月）から６年が経過することから、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。

両委員会において、改定方針に先立って次期CRYPTREC暗号リストに求められる要件等を明確にすべきとされたことから、2018年度暗号技術検討会での審議・承認を経て、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（図１参照）し、次の事項について整理することとした。

(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

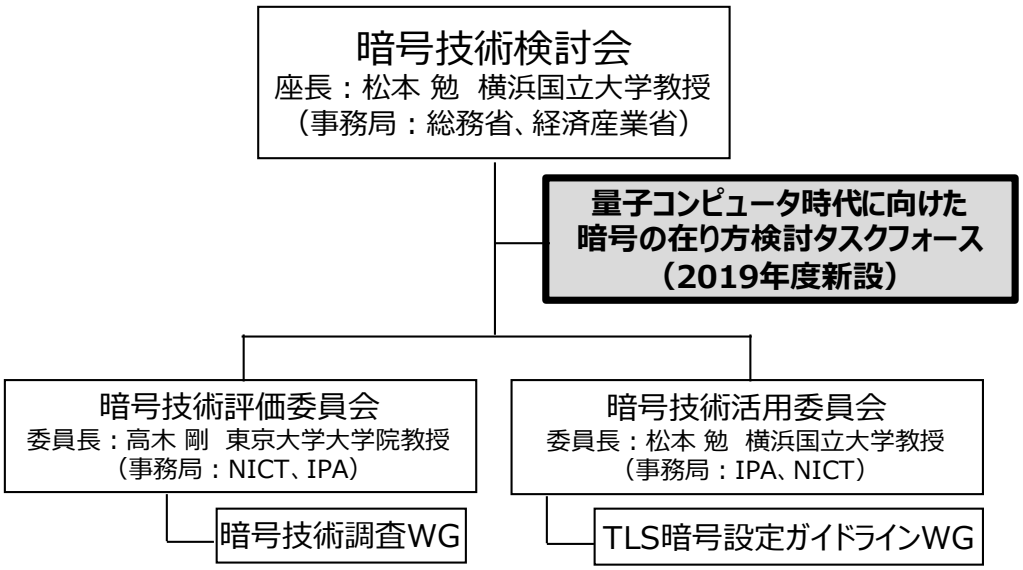


図１　検討TF

２　実施概要

２．１　体制（構成員・事務局）

検討TFの構成員は、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のとおり構成することとした。

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、オブザーバーとして、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。

事務局については、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は、表２のとおり2019年度に３回の会合を実施し、最新の技術動向等を踏まえ、次期CRYPTREC暗号リストに向けた検討を行った。

表２　検討TF　開催実績

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

３　技術動向検討

CRYPTREC暗号リストに関する検討に先立ち、最新の技術動向について次のとおり確認した。

また、３．１の内容については、2019年10月に量子コンピュータが量子超越を実現したという報告があり、暗号技術の危殆化が一部で懸念されている中で、CRYPTRECとして速やかに広く発信していくべきとされ、暗号技術評価委員会に対して注意喚起情報として発出を依頼した。

３．１　量子コンピュータの動向について

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

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ものでないことに留意が必要である。

しかしながら、そもそも量子コンピュータの量子ビット数が数千程度以上ないと、ノイズ等に関わらず（ノイズ等がないとしても）暗号解読はできないと見込まれているため、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は妥当である。

---

[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を実施したものではない。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の評価が行われ、2019年１月から表３の26方式がRound 2に進んで評価が行われている。今後、2020～2021年にRound 3を実施し、2022～2024年に標準化ドラフトが策定される予定[4]とされている。

表３　Round 2 候補暗号（26方式）

格子暗号	鍵交換・暗号化（９方式）: CRYSTALS-KYBER, Frodo-KEM, LAC, NewHope, NTRU, NTRU Prime, Round5, SABER, Three Bears デジタル署名（３方式）: CRYSTALS-DILITHIUM, FALCON, qTESLA
符号暗号	鍵交換・暗号化（７方式）: BIKE, Classic McEliece, HQC, ROLLO, LEDAenc, NTS-KEM, RQC
多変数多項式暗号	デジタル署名（４方式）: GeMSS, LUOV, MQDSS, Rainbow
ハッシュ関数署名	デジタル署名（１方式）: SPHINCS+
同種写像暗号	鍵交換・暗号化（１方式）: SIKE
その他	デジタル署名（１方式）: Picnic

（第１回会合資料４より作成）

３．３　耐量子計算機暗号の利活用について

３．２の動向を踏まえ、耐量子計算機暗号の利活用に関して次のような議論が行われた。

- ○　現在の暗号を使い続けながら、量子コンピュータに対しても準備をしておくことが必要。
- ○　大規模システムの更改には10年以上を要することもあり、データのライフサイクルも踏まえた議論も必要。
- ○　SHA-1等の危殆化に備えSHA-3が作られたがほとんど使われていない。耐量子計算機暗号についても実際にどの暗号方式が残っていくかという点に留意が必要。
- ○　耐量子計算機暗号の利用は、アプリケーションによって使用アルゴリズムを切り替えるようになる可能性も高いのではないか。
- ○　公開鍵暗号は、アプリケーションが広まったため活用も広まった。 耐量子計算機暗号を活用すると従来の暗号に比べてデータサイズが大きくなってしまうため、高機能暗号としてアプリケーションを広げ、それが耐量子性も持っているというような形が有効。

[4] https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline

３．４　軽量暗号の動向について

軽量暗号についても、米国NISTが標準化のための評価を実施している。2019年２月に暗号公募が締め切られ、56方式についてRound 1の評価が行われ、2019年８月から32方式がRound 2に進んで評価を受けている。今後、１年程度かけてRound 2が実施される予定である。

当該NISTの応募要項によれば、認証付き暗号は、鍵長は最低128ビット、攻撃に必要な計算量は2^112以上（古典計算機、単一鍵設定）で、サイズの制限（一つの鍵で処理できるデータ量）は2^50-1バイトを下回ってはならないとされている。また、短い入力に対する計算効率や、小型実装性能や省電力等実装への柔軟な対応のほか、サイドチャネル攻撃に対する耐性を求められるなど、非常に高い要求がされている。

また、学術コミュニティ主導の認証暗号のコンペティションとして、CAESAR（Competition for Authenticated Encryption: Security, Applicability, and Robustness）があり、2014年３月に57方式の応募を受け、2019年２月に６方式をポートフォリオとして公表している。このポートフォリオのUse Case 1が軽量暗号用途であり、AsconとACORNの２方式が掲げられている。

４　検討内容

３の技術動向を踏まえ、CRYPTREC暗号リストの改定に関連した検討を行い、その結果は次のとおりである。

４．１　CRYPTREC暗号リストにおける耐量子計算機暗号の位置づけについて

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

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

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

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

４．２　CRYPTREC暗号リストにおける軽量暗号・高機能暗号等の位置づけについて

現行のCRYPTREC暗号リストは、利用環境によらない暗号技術自体の安全性や利用実績を考慮した上でリスト化がされている。一方、利用が拡大すると想定される、IoT機器等に用いられる軽量暗号や、暗号状態で情報処理が可能な高機能暗号は、利用するアプリケーションやデータ取扱に関する要件が限定され、従来暗号とは取り扱いが異なるものであるため、軽量暗号及び高機能暗号については、CRYPTREC暗号リストとは別文書（ガイドライン等）を新たに作成することが適当である。

軽量暗号については、2016年に暗号技術ガイドラインを作成しているが、当該ガイドラインはCRYPTREC暗号リストを利用する者からその存在を確認しづらく、また、最新の技術動向については掲載されていないため、最新の技術動向を入れ込みつつ、利用者の視点を意識した文書となるよう工夫する必要がある。

４．３　CRYPTREC暗号リストの在り方について

CRYPTREC暗号リストの在り方について、「リスト構成」、「技術分類」、「暗号技術公募」の３点に分けて検討を行った。

４．３．１　リスト構成について

CRYPTREC暗号リストは、
①電子政府推奨暗号リスト[5]
②推奨候補暗号リスト[6]
③運用監視暗号リスト[7]
の３リスト構成となっている。

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

しかしながら、そもそも現行のCRYPTREC暗号リストの改定時に「②推奨候補暗号リスト」を含めた３リスト構成としたのは、国産暗号技術の普及展開を促進することもその目的の一つ[8]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ると、「②推奨候補暗号リスト」については、その意義・必要性について更なる検討を行う必要がある。このため、３リスト構成の望ましい在り方について、引き続き検討が必要である。

---

[5] 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。

[6] 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。

[7] 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。

[8] 2011年度第1回暗号技術検討会資料3-2

４．３．２　技術分類について

CRYPTREC暗号リストおいては、暗号技術を７つの技術分類（細分を含めると12分類）[9]に分けて管理している。

耐量子計算機暗号等をCRYPTREC暗号リストに含めるとした場合には、この技術分類の構成をどのようにするかが課題であったが、耐量子計算機暗号並びに軽量暗号及び高機能暗号については、前述のとおりCRYPTREC暗号リストとは別文書とすることとしたためその点は解消している。

また、現行の技術分類における暗号技術（耐量子計算機暗号等以外の暗号技術）については、十分成熟しており、現時点で特筆すべき動きはない。加えて現行のCRYPTREC暗号リストにおいても、改定後に必要に応じて技術分類の変更[10]を行っている[11]。

こうした状況を踏まえると、技術分類についてはCRYPTREC暗号リストの改定に当たって現在の構成を変更する必要はなく、維持することが適当である。

４．３．３　暗号技術公募について

2013年のCRYPTREC暗号リストの改定時には暗号技術の公募を行ったが、現行の技術分類における各暗号技術については、十分成熟しており、現時点で特筆すべき動きはない。

また、現行のCRYPTREC暗号リストにおいても、改定後に必要に応じて暗号技術の掲載内容の変更を行っている[12]。

こうした状況を踏まえると、2023年を目途に実施しようとしているCRYPTREC暗号リストの改定に当たって暗号技術の公募を実施する必要は認められない。

４．４　暗号技術のパラメータについて

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

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

---

[9] 公開鍵暗号（署名・守秘・鍵共有）／共通鍵暗号（64ビットブロック暗号・128ビットブロック暗号・ストリーム暗号）／ハッシュ関数／暗号利用モード（秘匿モード・認証付き秘匿モード）／メッセージ認証コード／認証暗号／エンティティ認証

[10] 2013年の「改定」後に実施してきたCRYPTREC暗号リストの修正は「変更」とし、2023年目途に実施しようとしている「改定」と分けて取り扱う。

[11] 平成30年3月29日付けで「認証暗号」の技術分類を追加する変更を実施。

[12] 平成30年3月29日付けで「ChaCha20-Poly1305」を追加する変更を実施。

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

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

４．５　CRYPTREC暗号リストの今後の改定について

2003年に「電子政府推奨暗号リスト」を作成し、2013年に現行のCRYPTREC暗号リストとして改定を行い、今般、2023年を目途とした改定作業を行っており、10年単位での改定を行っている。

CRYPTREC暗号リストの内容については、常に危殆化等の監視を行うとともに、必要に応じて新規の暗号技術を加えるなどの変更を行っている。このため、必ずしも10年単位で改定する必要もないことから、2023年目途の改定以後は、暗号技術や諸外国の動向を踏まえ、改定後５年以内[13]を目途に暗号技術検討会において改定是非を判断する（以後当該判断から５年以内に改めて判断を行う。）こととすることが適当である。

４．６　CRYPTRECの文書体系について

CRYPTRECの発行する文書は、現在、図２のような文書体系となっている。

４．１及び４．２で新たに作成することとした耐量子計算機暗号等に関する文書については「GL」に、４．４で新たに作成することとした推奨パラメータに係る文書についてはLSの下に、それぞれ位置づけることが適当である。

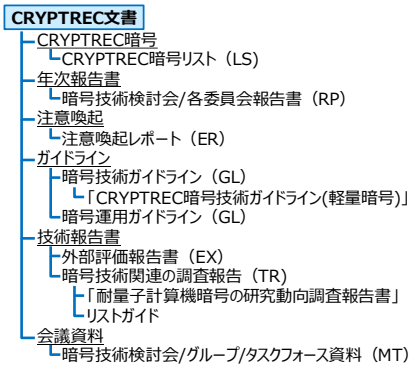


図２　現行のCRYPTREC文書体系

[13] 前回の改定では、枠組み等の検討開始から改定まで５年程度を要している。

４．７　検討TFについて

量子コンピュータや耐量子計算機暗号の動向についてはCRYPTRCとしてフォローしていく必要があり、その状況をフォローするため、また、４．３．１に示した３リスト構成の在り方について引き続き議論を行う必要があるため、2020年度以降も検討TFを継続設置することが必要である。

４．８　その他

そのほか、次のような議論が行われた。

- ○　耐量子計算機暗号についての安全性を長期的に検討していく体制を維持していくことが重要。
- ○　耐量子計算機暗号への移行がスムーズにできるよう、十分な体制構築や参考となる文書の検討が必要。
- ○　CRYPTREC暗号リストへの掲載有無によって、企業の暗号開発への注力の度合いも変わるのであれば、我が国の産業で使用されるものは、状況にあわせてCRYPTREC暗号リストに組み込んでいくことが必要。
- ○　量子コンピュータに備えるという文脈での、耐量子計算機暗号への移行や鍵長の増加等に関する記載は重要。一方で、従来のコンピュータの性能向上に備えるという文脈での、RSA2048からの移行を2030年頃までに行うこと[14]についても、利用者に示していくことが有用。

[14] RSA2048に相当する112bitセキュリティについて、NISTのロードマップでは2030年までには128bitセキュリティに移行すべきとしている。

資料２－２

「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」の活動について

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暗号リストの在り方及び暗号技術の動向等について、今後、次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　耐量子計算機暗号、軽量暗号、高機能暗号について、CRYPTREC暗号リストには含めず、それぞれ別の文書とする。また、当該文書の重要性がわかるよう、取りまとめたものとする。

２　2023年目途のCRYPTREC暗号リストの改定について、現行の３リスト構成の在り方については引き続き検討することとする。また、技術分類については現行のものを踏襲し、公募は行わない方針とする。

３　推奨される暗号のパラメータについて、CRYPTREC暗号リストから参照する形で別の文書としてまとめる方針とする。

４　１及び３に係る新たな文書も含め、CRYPTREC暗号リストを含むCRYPTRECの文書の位置付けを整理する。

５　量子コンピュータや耐量子計算機暗号の状況をフォローするため、及び引き続き継続検討とした内容の議論を行うため、2020年度以降もタスクフォースを継続設置する。

資料３

2019 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

下記のとおり、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 2019 で報告。

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。

- 「現在の量子コンピュータによる暗号技術の安全性への影響」について注意喚起レポートを発行 (資料３別添１参照)

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。

- 暗号利用モード XTS の実装性能評価を実施。2018 年度に実施した安全性評価および今年度実施した実装性能評価の結果に基づき、XTS モードが、安全性要件を満たす条件の下で秘匿モードとして十分な安全性および実装性能を有していると判断、暗号技術検討会に「推奨候補暗号リスト」への追加を提案。(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、主に、量子コンピュータによる共通鍵暗号の安全性への影響について調査し、技術報告書として公開する。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」の予測図の更新方法について近年の計算機の性能向上が鈍化傾向にあることを踏まえ、この傾向を予測図にどのように反映するかなど、以降の予測図の在り方について検討を行う。

量子コンピュータによる共通鍵暗号の安全性への影響については、外部専門家による外部評価による評価レポートを依頼する。

- 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」の予測図の更新方法を検討した。また、量子コンピュータによる共通鍵暗号の安全性への影響について、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。

- 電子政府推奨暗号リストに掲載されている RSA-PSS、RSASSA-PKCS1-v1_5、RSA-OAEP 及び運用監視暗号リストに掲載されている RSAES-PKCS1-v1_5 に関する仕様書の参照先の修正を行った。(表 1)

表１：RSA 暗号の新旧仕様書

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

3. 開催状況

表 2 暗号技術評価委員会の開催状況

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

以上

委員構成

［暗号技術評価委員会］

委員長	高木　剛	東京大学　教授
委員	岩田　哲	名古屋大学　准教授
委員	上原　哲太郎	立命館大学 教授
委員	大東　俊博	東海大学　准教授
委員	國廣　昇	筑波大学　教授
委員	四方　順司	横浜国立大学　教授
委員	手塚　悟	慶應義塾大学　教授
委員	藤崎　英一郎	北陸先端科学技術大学院大学　教授
委員	本間　尚文	東北大学　教授
委員	松本　勉	横浜国立大学　教授
委員	松本　泰	セコム株式会社　ディビジョンマネージャー
委員	盛合　志帆	国立研究開発法人情報通信研究機構　上席研究員
委員	山村　明弘	秋田大学　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研究センター　副研究センター長

［暗号技術調査ワーキンググループ(暗号解析評価)］

主査	國廣　昇	筑波大学　教授
委員	青木 和麻呂	日本電信電話株式会社　グループリーダ
委員	草川　恵太	日本電信電話株式会社　主任研究員
委員	桑門　秀典	関西大学　教授
委員	下山　武司	株式会社富士通研究所　主管研究員
委員	高木　剛	東京大学　教授
委員	高島　克幸	三菱電機株式会社　主管技師長
委員	峯松　一彦	日本電気株式会社　主幹研究員
委員	安田　貴徳	岡山理科大学　准教授
委員	安田　雅哉	九州大学　准教授

現在の量子コンピュータによる暗号技術の安全性への影響

2020 年(令和 2 年)2 月 17 日
CRYPTREC 暗号技術評価委員会

今般、ゲート型の量子コンピュータが量子超越を実現したという報告があり、暗号技術の危殆化が一部で懸念されております。しかし、現在の量子コンピュータの開発状況をふまえると、暗号解読には規模の拡大だけでなく量子誤り訂正などの実現が必要であるため、CRYPTREC としては、CRYPTREC 暗号リスト記載の暗号技術が近い将来に危殆化する可能性は低いと考えています。

今後も、本暗号リスト記載の暗号技術の監視活動を引き続き実施していきます。

今般、ゲート型の量子コンピュータが量子超越を実現したと主張する論文が Nature 誌に発表されました[1]。この論文では、ランダム量子回路からのサンプリング問題を、古典計算機を用いた場合には 1 万年かかるところ、量子コンピュータを用いると 200 秒で完了すると主張しています。この主張は、ランダム量子回路からのサンプリング問題を、量子コンピュータが古典計算機よりも高速に解くことを示しています。これにより、現在広く使用されている公開鍵暗号である RSA 暗号及び楕円曲線暗号などの安全性が大きく低下することが一部で懸念されています。その理由としては、それらの暗号技術が安全性の根拠として利用している素因数分解問題と離散対数問題が、大規模な量子コンピュータと Shor のアルゴリズムを使用することで高速に解読されることが知られているためです。

現在、CRYPTREC 暗号リストの電子政府推奨暗号リストに記載されている RSA-PSS、RSASSA-PKCS1-v1_5、RSA-OAEP は素因数分解問題を、DSA、ECDSA、DH、ECDH などは離散対数問題を安全性の根拠にしています。CRYPTREC では、以前より RSA 合成数の素因数分解などにおける安全なパラメータサイズについて、通常の計算機だけでなく、量子コンピュータによる影響に関しても評価を行っておりますが、今までの評価結果をふまえると、CRYPTREC としては、近い将来に CRYPTREC 暗号リスト記載の暗号技術が危殆化する可能性は低いと考えています。

論文[1]で使用されている量子コンピュータは 53 量子ビットであり、計算は合計 1543 回のゲート演算で構成されています。このとき、1 回当たりの計算時間は、1 マイクロ秒程度であると見積もられています。なお、ターゲットとする問題の性質上、量子誤り訂正は組み込まれていません。

その一方で、例えば、量子コンピュータを用いて 2048 ビット RSA 合成数の素因数分解

を行う場合には、量子誤りが一切ないという理想的な環境下でも、4098 量子ビットが必要であり、10^{12}〜10^{13}回のゲート演算が必要であると見積もられています[2, 3]。また、量子誤りがあるという現実的な環境下では、2000 万量子ビットが必要であるという見積もりもあります[4]。

このため、実現されている量子コンピュータと素因数分解を行うのに必要とされる量子コンピュータの性能に関しては、依然として大きな乖離があります。これは離散対数問題を利用する暗号についても同様です。量子コンピュータの性能を測る上での指標（量子ビット数、量子誤りの大きさ、演算可能回数など）や、量子コンピュータの開発状況もあわせて考慮にいれると、近い将来に、2048 ビットの素因数分解や 256 ビットの楕円曲線上の離散対数問題が解かれる可能性は低いと考えます。

しかしながら、革新的な技術の発展などにより、量子コンピュータで暗号解読を実現する可能性は否定できません。このため、CRYPTREC では、量子コンピュータによる暗号技術に対する影響、及び量子コンピュータ実現後にも安全な暗号技術（耐量子計算機暗号）に関する監視評価活動を継続していきます。

ご意見・コメントなどの問い合わせがございましたら、下記までお願いいたします。

CRYPTREC 事務局
E-mail: info@cryptrec.go.jp

参照

[1] Quantum supremacy using a programmable superconducting processor
https://www.nature.com/articles/s41586-019-1666-5

[2] National Academies of Sciences, Engineering, and Medicine. 2019. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press.
https://doi.org/10.17226/25196
日本語訳版：
E. Grumbling, M. Horowitz 編, 西森 秀稔 訳, “米国科学・工学・医学アカデミーによる量子コンピュータの進歩と展望,” 共立出版, 2020.

[3] NICT サイバーセキュリティシンポジウム
https://www.pco-prime.com/2019cybersympo/

[4] How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits
https://arxiv.org/abs/1905.09749

資料３別添２

暗号利用モード XTS について

暗号技術評価委員会で審議を行った下記 3 点について報告する。
[1] 今年度実施した実装性能評価結果に基づく、XTS モードの実装性能に関する判断
[2] 昨年実施済みの安全性評価について、安全性要件を満たす条件の表現の改訂
[3] CRYPTREC 暗号リストに入る条件を満たしているか否かの判断

1　背景

暗号利用モード (秘匿モード)の一つである XTS モードは、2007 年にストレージデバイス上のデータの暗号化の規格として IEEE Standard 1619-2007 [1] で標準化され、NIST でも、2010 年に NIST SP 800-38E [2] として規定された。2018 年には IEEE Standard が更新され [3]、安全に使用するための条件が厳しくなった。大きな市場を持つ製品に搭載されるなどの実績があり、例えば、Microsoft Windows 搭載の BitLocker や macOS 搭載の FileVault 等のディスク暗号化機能に XTS モードが使われている。

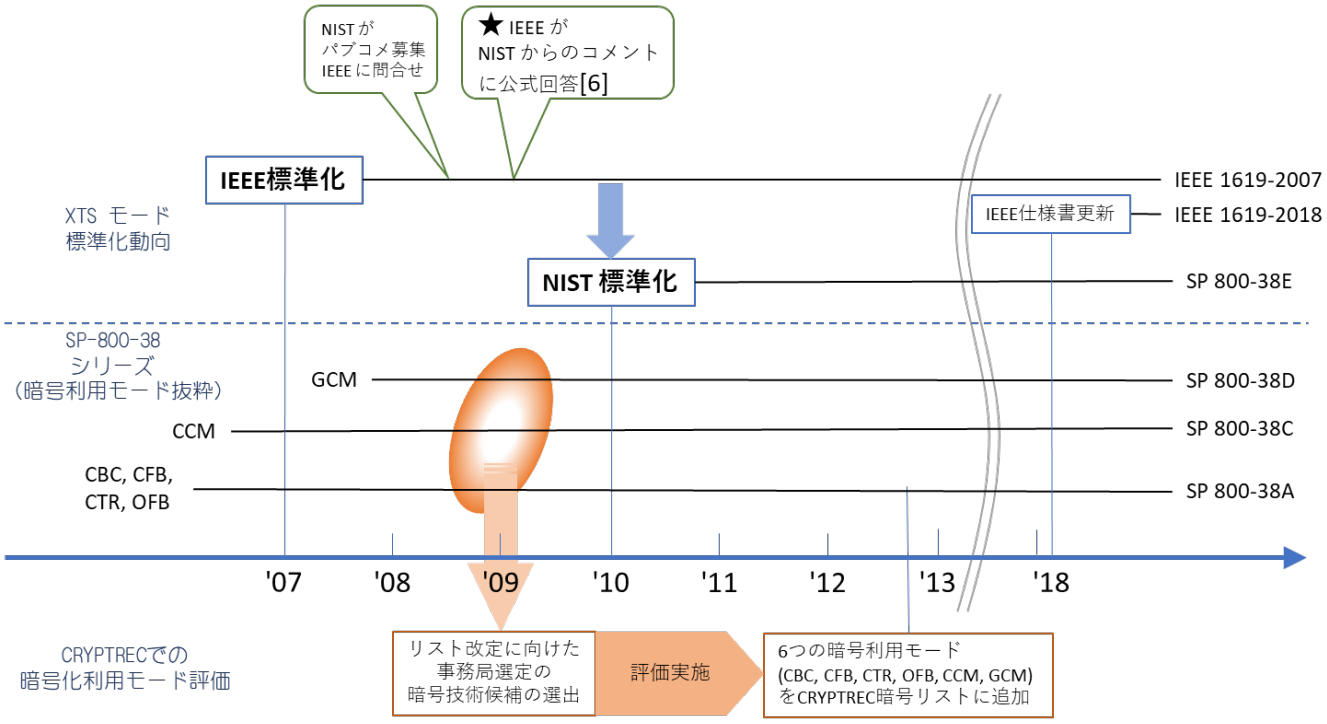


図 1 XTS に関する標準化動向

暗号利用モードは、2012 年度の CRYPTREC 暗号リスト改定に合わせて、2009 年度に事務局選出の暗号技術候補として複数の暗号利用モードを NIST SP 800-38 シリーズから選出して、安全性評価・実装性能評価を実施し [4] [5]、6 つの暗号利用モード (CBC, CFB, CTR, OFB, CCM, GCM) を CRYPTREC 暗号リストに追加した。 XTS モードは 、2009 年当時 NIST SP 800-38 シリーズにおいて規定されていない技術であったため、評価対象外であったが、昨今、情報漏えい対策として OS 搭載のディスク暗号化機能が一般的に利用されていることから、2018 年度外部評価として、安全性評価を実施した。また、今年度実装性能評価を実施した。

2　実装性能評価

第一回暗号技術評価委員会（2019 年 6 月 28 日)の承認を受け、下記のとおり外部評価を実施した。

依頼内容 : XTS モードの実装性能に関する調査及び公開されているベンチマーク実装評価の調査

依頼先：菅野　哲 様 (レピダム株式会社)

今年度の調査および評価結果に基づき、暗号技術評価委員会では、実装性能について、CRYPTREC 暗号リストに掲載するために十分な実装性能を有していると判断した。

3　安全性評価

Phillip Rogaway 氏による安全性評価レポート[5] および 2018 年度に峯松一彦氏に依頼し実施した外部評価による安全性評価レポート[7] の結果に基づき、2019 年度第二回暗号技術評価委員会(2019 年 3 月 11 日) にて、下記の判断を行った。

XTS モードは、下記 3 点の条件下では、暗号利用モード(秘匿モード)として CRYPTREC 暗号リストへ追加するための安全性要件を満たしている。

(条件 1) 利用用途は IEEE および NIST SP-800-38E の規格に沿ったストレージやディスクの暗号化に限る。

(条件 2) XTS 内のブロック暗号には、 CRYPTREC 暗号リスト掲載の 128 ビットブロック暗号を使う。

(条件 3) 同一の鍵を用いて暗号化する場合、2^{20} ブロックまでとする。

今年度、第二回暗号技術評価委員会(2020 年 2 月 18 日開催)の審議により、(条件 3) は表現が不明瞭であり、また、意図した内容は、参照先仕様書にその制限事項の記載があることから、(条件 1) に包含されるとの解釈の基、(条件 3) を安全性要件を満たす条件から削除することとした。また、(条件 1) は、冗長性が高かったため、表現の改善を行った。

以上より、安全性要件を満たす条件は下記のように改訂された。

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

4　CRYPTREC 暗号リストへの追加の可否

2018 年度に実施した安全性評価、および、今年度実施した実装性能評価の結果に基づき、暗号技術評価委員会では、XTS 利用モードは CRYPTREC 暗号リストに掲載するために十分な安全性および実装性能を満たしていると判断した。

上記判断に基づき、暗号技術評価委員会としては CRYPTREC 暗号リスト「推奨候補暗号リスト」に新たに掲載することを提言する。

CRYPTREC 暗号リストの追加先となる技術分類、および注釈表記については、下記 2 案について議論した。

A 案：[技術分類] 大分類「暗号利用モード」の中分類「秘匿モード」に追加する。
[注釈] 安全性要件を満たす条件 (条件 1) (条件 2) を注釈につける。

B 案：[技術分類] 大分類「暗号利用モード」に中分類として、
「ストレージデバイス暗号化用秘匿モード」を新設する。
[注釈] 安全性要件を満たす条件 (条件 2) を注釈につける。

現状の CRYPTREC 暗号リストの大分類「暗号利用モード」に属する中分類は、機能別に分類されているが、B 案の場合、中分類の分類方針が機能だけではなくなり、他の秘匿モードがストレージデバイス暗号化用に利用可能か否かなどにも配慮する必要が出てくる。A 案の場合、現状の分類方針を踏襲した扱いであり、また、(条件 1)を注釈につけることによりストレージデバイス暗号化用であることは明示できることから、暗号技術評価委員会としては、A 案を推薦する。

(参考)

各々の案に基づき追加した場合の推奨候補暗号リストのイメージは下記の通り。

【A 案イメージ図】(推奨候補暗号リスト)

暗号利用モード	秘匿モード	~~該当なし~~ XTS(注*)
	認証付き秘匿モード(注14)	該当なし

(注*) 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、NIST SP800-38E の規格に沿ったストレージデバイスの暗号化に限る。

【B 案イメージ図】(推奨候補暗号リスト)

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14)	該当なし
	ストレージデバイス用秘匿モード	XTS(注*)

(注*) 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。

電子政府推奨候補暗号リスト、運用監視暗号リスト、の枠には「該当なし」を記載。

【参考文献】

1. Institute of Electronical and Electronic Engineers, IEEE Std 1619-2007: IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices, IEEE Press, 2008.
2. Morris Dworkin, NIST Special Publication 800-38E: Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Device. NIST, 2010.
3. Institute of Electronical and Electronic Engineers, IEEE Std 1619-2018: IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices, IEEE Press, 2019. (Approved 2018/10/23. Published 2019/01/25)
4. 廣瀬勝一, 暗号利用モードおよびメッセージ認証コードに関する安全性評価, CRYPTREC 技術報告書(CRYPTREC EX-2011-2010), CRYPTREC, 2010.
5. Phillip Rogaway, Evaluation of Some Blockcipher Modes of Operation, CRYPTREC 技術報告書(CRYPTREC EX-2012-2010R1), CRYPTREC, 2010.
6. Matthew V. Ball, Sun Microsystems, Chair of IEEE Security in Storage Working Group (P1619), Follow-up to NIST's Consideration of XTS-AES as standardized by IEEE Std 1619-2007, Documents published by NIST, 2009.
   URL:https://csrc.nist.gov/csrc/media/projects/block-cipher-techniques/documents/bcm/comments/xts/follow-up_xts_comments-ball.pdf
7. 峯松 一彦, 暗号利用モードXTSの安全性に関する調査及び評価, CRYPTREC技術報告書(CRYPTREC EX-2801-2018), CRYPTREC, 2018.

以上

資料３別添３

2019 年度暗号技術調査 WG（暗号解析評価）活動報告

1. 2019 年度暗号技術調査 WG（暗号解析評価）活動報告の概要

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

・量子コンピュータによる共通鍵暗号の安全性への影響に関する調査及び評価

・「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の在り方についての検討

上記二件について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、実施した。

2. 委員構成（敬称略）

主査：國廣 昇（筑波大学）
委員：青木 和麻呂（NTT）
委員：草川 恵太（NTT）
委員：桑門 秀典（関西大学）
委員：下山 武司（富士通研究所）
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（九州大学）

3. 量子コンピュータによる共通鍵暗号の安全性への影響に関する調査及び評価

3.1. 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。特に米国では NIST が公開鍵暗号について PQC を公募し、現在では提案された暗号方式の安全性評価が進められている。また、欧州の ETSI や ISO/IEC でも標準化に向けた議論が始まっている。

国内では 2017 年度から 2018 年度にかけて、暗号解析評価 WG が公開鍵暗号について PQC の研究動向調査を行い、その調査結果を報告書としてまとめ、2019 年 4 月に公開した。また、2018 年度の暗号技術評価委員会において、量子コンピュータを使用した共通鍵暗号の解読に関する論文が近年、増加していることが委員から指摘されている。

3.2. 実施内容

量子コンピュータによる共通鍵暗号の安全性への影響の調査について、外部専門家による評価を依頼することが、第一回暗号技術評価委員会(2019 年 6 月 28 日）で承認され、具体的な評価価内容が、第一回暗号解析評価 WG（2019 年 7 月 29 日）にて承認された。

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

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

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

【依頼先】細山田 光倫 様（NTT セキュアプラットフォーム研究所）
【2019 年度のスケジュール】
・2019 年 7 月 29 日 第 1 回 暗号解析評価 WG：活動内容の審議・承認
・2020 年 1 月 24 日 第 2 回 暗号解析評価 WG：調査結果の報告の審議・承認

3.3. 外部評価報告書の見解（評価報告書のまとめ）

共通鍵暗号（ブロック暗号、ストリーム暗号)、ハッシュ関数、暗号利用モード（秘匿モード、認証付き秘匿モード)、メッセージ認証コードに対して、量子コンピュータを利用した下記の攻撃モデルが存在する。

- 攻撃モデル: 攻撃者は量子コンピュータを持っており、秘密鍵の埋め込まれた攻撃対象のオラクル（暗号化/復号オラクル、認証タグ生成オラクル）へクエリ可能である。このオラクルへのクエリに対して、古典クエリ攻撃モデル（Q1 モデル）と量子クエリ攻撃モデル(Q2 モデル)の二種類の攻撃モデルが存在する。
  - 古典クエリ攻撃モデル（Q1 モデル）
    - ✓ オラクルへのクエリが古典情報。
  - 量子クエリ攻撃モデル（Q2 モデル）
    - ✓ オラクルへのクエリが量子重ね合わせ状態。
- Q1 と Q2 の比較：Q2 では、秘密鍵が埋め込まれたオラクルが量子回路上に実装されており、攻撃者がその量子回路に量子重ね合わせ状態のクエリができる状況を想定しているため、Q1 より強い攻撃モデルである。CRYPTREC の電子政府推奨暗号リストにあるアルゴリズムは古典計算機向けであるため、通常は Q2 の攻撃モデルには該当しない。しかしながら、難読化処理等で秘密鍵を秘匿して埋め込んだこれらの暗号化処理プログラムを、量子コンピュータをもった攻撃者に渡した場合は、攻撃者は量子オラクルをシミュレート可能であるため Q2 モデルが成立する。

CRYPTREC の電子政府推奨暗号リストに掲載されている共通鍵暗号、暗号利用モード、メッセージ認証コード、ハッシュ関数に対する量子コンピュータを用いた場合の安全性については以下の通りである。

- **共通鍵暗号（ブロック暗号、ストリーム暗号）：** Q1、Q2 モデルにおいては、現行の CRYPTREC の電子政府推奨暗号リストに記載のアルゴリズムに対しては、Grover のアルゴリズムが最良の攻撃であり、k-bit 鍵の全数探索が $2^{k/2}$の計算量で可能である。長期保存を想定し、耐量子安全性を考慮する場合は、192-bit 鍵や 256-bit 鍵を使用することが賢明である。
- **暗号利用モード・メッセージ認証コード：**Q2 モデルでは認証付き秘匿モードである GCM とメッセージ認証コードである CMAC への偽造攻撃が多項式時間で実行可能になる。ただし、このモデルでの攻撃を実行するためには、攻撃対象の暗号技術が量子回路上に実装されている必要があり、そのような特殊な状況でない限り、Q2 モデルの攻撃が影響を及ぼすことは現状ではないと考えられる。Q1 モデルにおいては、耐量子安全性を考慮する場合は、暗号利用モードの内部で用いるブロック暗号の鍵を 192-bit 鍵や 256-bit 鍵にすればよい。
- **ハッシュ関数：**量子コンピュータを用いた場合、ハッシュ関数の原像探索に関して Grover のアルゴリズムが最良の攻撃であり、n-bit 出力のハッシュ関数の原像探索に必要な計算量は $2^{n/2}$である。衝突探索に必要な計算量は BHT のアルゴリズムを用いると $2^{n/3}$になるが、この攻撃は $2^{n/3}$のサイズという非常に多くの量子メモリの使用を必要とするため実際のハッシュ関数の安全性に影響を及ぼすか否かは不透明である。最も現実的に影響を及ぼすと思われるのは CNS のアルゴリズムであり $2^{2n/5}$の計算量で衝突を発見する。CNS のアルゴリズムは n の多項式オーダのサイズの量子計算機と $O(2^{n/5})$の古典メモリにて実行可能である。現行の CRYPTREC の電子政府推奨暗号リストに記載のハッシュ関数の出力は 256 ビット以上であり、n = 256 とした場合でも、原像探索の計算量は 2^{128}、衝突探索の計算量は CNS のアルゴリズムで $2^{102.4}$となるため現実的な脅威となるとは考えづらい。

3.4. 暗号解析評価 WG の見解

外部評価報告書の結論をもとに表 1 と表 2 に CRYPTREC の電子政府推奨暗号リストに掲載されている共通鍵暗号、暗号利用モード、メッセージ認証コード、ハッシュ関数に対する量子コンピュータを用いた場合の安全性について、古典計算機を用いた場合の比較とともに示す。表 2 では参考のため、$2^{n/3}$のサイズという多くの量子メモリを必要とする BHT のアルゴリズムが実行できる場合の計算量も併記している。

表 1 より共通鍵暗号および暗号利用モードに対して多項式時間で実行可能な攻撃は Q2 モデルにおける Kaplan らのアルゴリズムによる GCM や CMAC への偽造攻撃であるが、外部評価報告書の見解のとおり Q2 モデルは特殊な環境下での攻撃であり現実的な脅威となるとは考え難い。また、表 2 のハッシュ関数への攻撃では BHT のアルゴリズムが動作した場合に SHA-256 は $2^{85.3}$の計算量で衝突探索が可能であるが、$2^{85.3}$の量子メモリを必要とするため、直近で現実的な脅威となるとは考えづらい。

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

なお、今回の評価は電子政府推奨暗号リストに掲載されている共通鍵暗号を対象にしているが、

推奨候補暗号リストに掲載されている共通鍵暗号も Even-Mansour 暗号や FX 構成への攻撃をそのまま応用できるものではないことから同様の評価結果になると考えられる。

表 1： 共通鍵暗号、暗号利用モード、メッセージ認証コードに対する量子コンピュータを用いた場合の安全性（k: 鍵長、b: ブロック長）

	暗号技術	古典クエリ攻撃モデル (Q1 モデル)	量子クエリ攻撃モデル (Q2 モデル)
共通鍵暗号	AES	鍵回復攻撃 *1 $2^{k/2}$（古典 2^k）	鍵回復攻撃 *1 $2^{k/2}$（古典 2^k）
	Camellia		
	KCipher-2		
暗号利用モード (秘匿モード)	CBC	鍵回復攻撃 *1 $2^{k/2}$（古典 2^k）	鍵回復攻撃 *1 $2^{k/2}$（古典 2^k）
	CFB		
	CTR		
	OFB		
暗号利用モード (認証付き秘匿モード)	GCM	鍵回復攻撃 *1 $2^{k/2}$（古典 2^k）	鍵回復攻撃 *1 $2^{k/2}$（古典 2^k） 偽造攻撃 *2 多項式時間（古典 $2^{b/2}$）
メッセージ認証コード	CMAC	鍵回復攻撃 *1 $2^{k/2}$（古典 2^k）	鍵回復攻撃 *1 $2^{k/2}$（古典 2^k） 偽造攻撃 *2 多項式時間（古典 $2^{b/2}$）

*1 Grover のアルゴリズム

*2 Kaplan らのアルゴリズム

表 2：ハッシュ関数に対する量子コンピュータを用いた場合の安全性

ハッシュ関数	SHA-256	衝突探索: BHT*3 $2^{85.3}$, CNS*4 $2^{102.4}$, (古典 2^{128}) 原像探索 *5:2^{128}, (古典 2^{256})
	SHA-384	衝突探索: BHT*3 2^{128}, CNS*4 $2^{153.6}$, (古典 2^{192}) 原像探索 *5:2^{192}, (古典 2^{384})
	SHA-512	衝突攻撃: BHT*3 $2^{170.7}$, CNS*4 $2^{204.8}$, (古典 2^{256}) 原像探索 *5:2^{256}, (古典 2^{512})

*3 BHT のアルゴリズム（多くの量子メモリが必要な方式）

*4 CNS のアルゴリズム（使用量子ビット数の観点から現実的な方式）

*5 Grover のアルゴリズム

4. 「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の在り方についての検討

4.1. 背景

「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、予測図と略す）は 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)」[1]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。当該予測図は、これを踏まえ、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、RSA1024 の危殆化の様子を分かり易く示すために作成されたものである。

近年、計算機の性能向上が鈍化傾向にあることを踏まえ、以下について検討が必要である。

(1)今後の予測図の取り扱い

(2)今後の公開鍵暗号のパラメータ選択

4.2. 今後の予測図の取り扱いについて

これまでの暗号の鍵長の推奨値は、いわゆるムーアの法則（集積回路上のトランジスタ数が 18 ヶ月毎に 2 倍になる）を主な根拠として設定されてきた。ところが、近年、計算機の性能向上は以前と比べて鈍化してきている。今後の予測図のあり方に対して、下記のとおり、対応方針を決定した。

対応方針

<今後の予測図の取り扱い>

(1) 予測図を従来通り、いわゆるムーアの法則を仮定して外挿線を今まで引いていた範囲（2040 年[2]）まで直線で引き、評価に大きな変動がないと考えられる限りにおいては、安全サイドに倒した評価として当面の間更新していくことを本 WG として提案する。

なお、予測図は各国・国際標準化機関等により示されている主要な暗号技術の安全性基準と比較すると、より現状に則した評価であり、危殆化時期がそれらよりも先に延びるものとなっている。

<今後の公開鍵暗号のパラメータ選択>

(2) 公開鍵暗号のパラメータ選択に関する対応方針については、安全性以外にも相互接続性など、運用上の観点もあるため、今後は、暗号技術評価委員会だけではなく、暗号技術検討会、暗号技術活用委員会や関係各所などを含めて検討することを本 WG として提案する。

---

[1] 現在は、米国 NIST では「NIST SP 800-57 Part 1 (Revision 4)(January,2016)」において暗号技術の鍵サイズに関して「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。

[2] 当該範囲については、ルート証明書の有効期限の長いものがあるため、第二回暗号技術評価委員会(2020 年 2 月 18 日開催)において、現在(2020 年)から 20 年後まで安全であることを分かり易く示すことが必要であると決定された。

4.3. 予測図の更新について

4.2 節の対応方針に基づいて、予測図の更新を下記の通り行った(図 1 及び図 2)。

- 篩処理の評価を 2006 年度版に基づく評価から 2018 年版(表 3)に基づくもの[1]に変更した。

表 3: 篩処理時間の推測結果 (単位は、Intel Xeon E5-2680 v3 2.5 GHz コア・年)

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

- 近年、ハードウェアを用いた新たな研究成果が無く、古い情報のみに依存した信頼性の低い評価となるため、「専用ハードウェアとソフトウェア処理との性能比較」に対応する外挿線は削除した。
- FactorWorld のサイト(http://www.crypto-world.com/FactorWorld.html)がなくなったので、Integer Factoring Records (https://members.loria.fr/PZimmermann/records/factor.html)に変更した。
- 3072 ビット RSA と 256 ビット ECDLP に関する計算量を表す横線(点線)を入れた。

なお、3072 ビット RSA に関する横線については他のビット長とは異なる評価方法であるため、より精度を高めるためにはさらなる検討が必要である。

参考文献

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

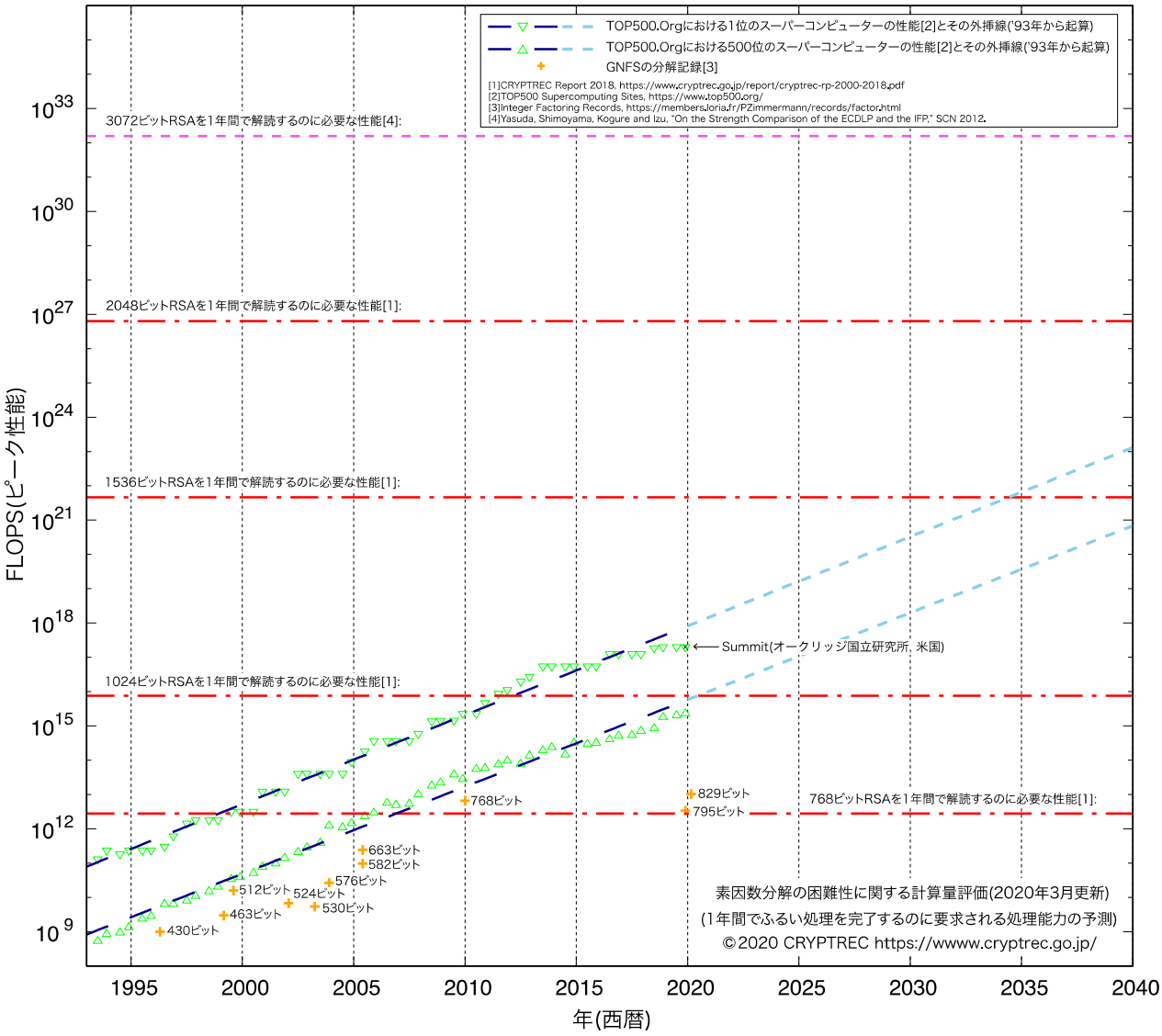


図 1：素因数分解の困難性に関する計算量評価

(1 年間でふるい処理を完了するのに要求される処理能力の予測、2020 年 3 月更新)[3]

[3] 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。

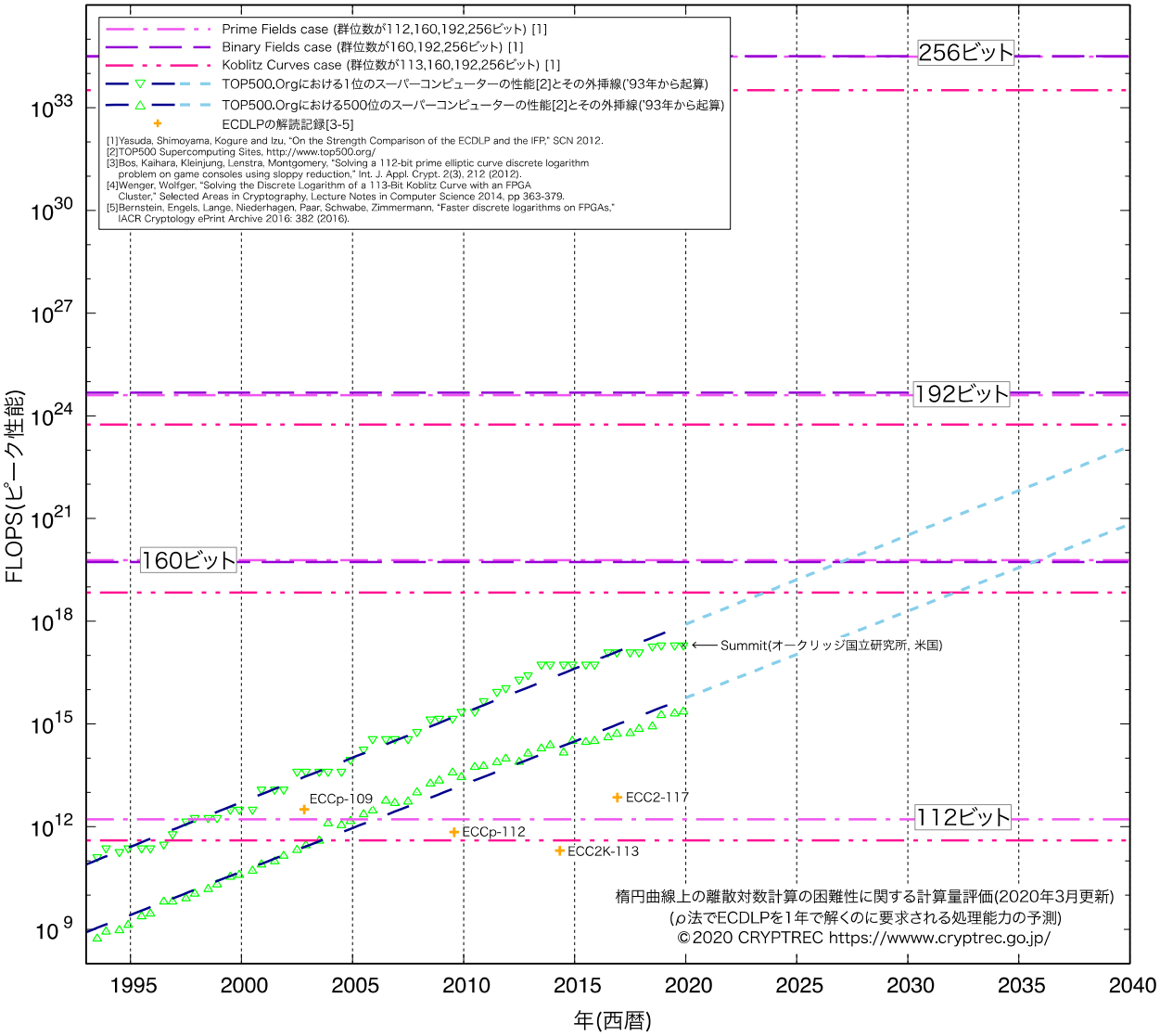


図 2：楕円曲線上の離散対数計算の困難性に関する計算量評価
（ρ 法で ECDLP を 1 年で解くのに要求される処理能力の予測、2020 年 3 月更新）[4]

以上

[4] 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。

資料４

2019 年度　暗号技術活用委員会活動報告

1.　2019 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。

2019 年度は、安全な暗号利用に係る運用ガイドラインを整備する観点から、「暗号鍵管理システム設計指針（基本編)」及び「TLS 暗号設定ガイドライン」の作成を行った。

（１）暗号鍵管理システム設計指針（基本編）の作成

2018 年度に作成した「暗号鍵管理システム設計指針（基本編)」のドラフト素案についてさらなる検討を進め、CRYPTREC シンポジウム 2019 の開催に合わせてドラフト版として公開した。

さらに、ドラフト版に対するパブリックコメントを実施して外部からの意見も踏まえつつ、暗号鍵管理の在り方・フレームワークを提示する初めての本格的な暗号鍵管理ガイドラインとなる「暗号鍵管理システム設計指針（基本編)」を完成させた。

（２）TLS 暗号設定ガイドラインの作成

2015 年に Ver1.0/Ver1.1、2018 年に Ver2.0 をリリースした「SSL/TLS 暗号設定ガイドライン（以下「現行ガイドライン」という。)」は累計で 20 万件以上のダウンロードがあるなど、TLS を利用する際の有用な運用ガイドラインとなっている。

このたび、SSL3.0 利用禁止及び TLS1.3 リリースなど、現行ガイドラインの利用環境とは大きく異なりつつある現状であることを踏まえて内容を大幅に見直すこととし、詳細な検討を行うため、TLS 暗号設定ガイドライン WG（以下「TLS ガイドライン WG」という。）を設置した。

TLS ガイドライン WG では、ガイドラインの位置づけ及び想定読者に関しては現行ガイドラインを踏襲し従来の有用性を維持する一方、技術的には 2020 年 3 月時点での TLS の現状を踏まえて全面的に記載内容の見直しを行った。なお、今回の改訂で SSL3.0 を全面的に禁止することになったため、ガイドラインの名称から「SSL」を削除し、「TLS 暗号設定ガイドライン」と呼ぶこととする。

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、2019 年度の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、新型コロナウイルスの影響により、2019 年度第二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 年度第一回活用委員会として開催された。

表 1-1 暗号技術活用委員会　委員構成

（**所属**：2020 **年** 3 **月末時点**）

委員長	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
委員	上原　哲太郎	立命館大学　情報理工学部　教授
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	清藤　武暢	日本銀行金融研究所　情報技術研究センター 主査[2019 年 8 月まで]
委員	宇根　正志	日本銀行　情報技術研究センター 情報技術研究グループ長[2019 年 9 月から]
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 NDIAS　自動車セキュリティ事業部　マネージャー
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 トラステッドシステム技術グループ　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
2019 年度 第一回	2019 年 6 月 12 日	■ 活用委員会活動計画について ■ TLS 暗号設定ガイドライン WG 活動計画について ■ 暗号鍵管理システム設計指針（基本編）ドラフト版について
2020 年度 第一回	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

1.3　成果概要

1.3.1　暗号鍵管理システム設計指針（基本編）の作成

あらゆる分野・あらゆる領域の全ての暗号鍵管理システム（以下「CKMS (Cryptographic Key Management System)」という。）を対象に、暗号鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として考慮すべき事項（Framework Requirements）を網羅的に提供し、設計時に考慮すべきトピックス及び設計書等に明示的に記載する要求事項を取りまとめた「暗号鍵管理システム設計指針（基本編)」を完成させた。

<u>位置づけ</u>

- 本設計指針は、セキュアな暗号アルゴリズムを利用する上で極めて重要な役割を果たす暗号鍵の管理に関する在り方を解説し、CKMS を設計・構築・運用する際に参考すべきドキュメントとして作成された。
  a) 「暗号鍵管理の在り方」（暗号鍵管理の位置づけと検討すべき枠組み）では、暗号鍵管理の必要性を認識してもらうための解説を記載した。これは、あらゆる暗号鍵管理を検討する際の基礎となる考え方を示したものである。
  b) 「暗号鍵管理についての技術的内容」では、包括的な CKMS 設計指針である NIST SP800-130 「A Framework for Designing Cryptographic Key Management Systems」の解説書・利用手引書として活用できるように構成した。本設計指針では、SP800-130 での Framework Requirements を『暗号鍵管理における目的に応じた』対象範囲に分類・再構成することによってそれぞれの検討項目の目的や必要性を明確化した。
- 本設計指針は、あらゆるユースケースにおける暗号鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として考慮すべき事項一覧を提供し、CKMS 設計時に考慮すべきトピックス及び設計書等に明示的に記載する要求事項を示している。
- ただし、本設計指針の中ではセキュリティ要求事項は定義せず、具体的な特定のセキュリティ機能の採用を義務づけることもしない。それぞれの要求事項に対してどのように対応（例えば、ポリシー、暗号アルゴリズム、デバイス等の選択）するかは CKMS 設計者に委ねられ、それらの対応方針が設計仕様書や運用マニュアル等に記載される。
- CKMS 設計者が選択した対応方針が適正かどうかの判断は運用管理者や調達責任者が行う。適切ではないと判断した場合には、CKMS 設計のやり直しを指示すべきである。確認にあたってはチェックリストも活用されたい。

<u>適用範囲</u>

- 本設計指針は、あらゆる分野・あらゆる領域の全ての CKMS を対象とする。CKMS は、暗号処理及びその処理で利用する暗号鍵を管理するシステム全体を包含する。ただし、暗号処理及び暗号鍵を管理・運用するのに必要な機能以外の部分は本設計指針の対象外である。

- 本設計指針の適用範囲に CKMS のシステム規模は問わない。もっとも小さい単純なものは一つのデバイス（の一部分）からなる場合もあるし、暗号鍵管理センタで複数のデバイスを集中管理するような大規模システムの場合もある。
- どの範囲を CKMS の対象とするのかは、「暗号鍵管理システムの設計原理と運用ポリシー」の中で CKMS 設計者によって具体的に定義される。

構成

本設計指針は、9 章で構成されており、章立ては以下のとおりである。

2 章では、イントロダクションとして暗号鍵管理の在り方や考え方について解説する。あらゆる暗号鍵管理における基礎をなすものである。

3 章では、本設計指針の活用方法について解説する。

4 章以降が CKMS の包括的な設計指針である SP800-130 の解説書・利用手引書として活用できるように、SP800-130 の内容を再構成したものである。暗号鍵管理における目的ごとに章分けをしている。

本設計指針の特長

本設計指針の最大の特長は、暗号鍵管理の考え方の枠組みを整理し、暗号鍵管理のための設計仕様書や運用マニュアルがどのように作られるべきかを明確にした点にある。大きくは 4 つの視点からなる。

第一の視点：暗号鍵管理の考え方の枠組み

国内外の暗号鍵管理に関するガイドラインの調査結果を基に、暗号鍵管理の考え方の枠組みを図 1-1 のように整理し、暗号鍵管理のための設計仕様書や運用マニュアルがどのように作られるべきかを明確にした。暗号鍵管理の構成要素は、「Framework Requirements」「Profile Requirements」「System Requirements」「Guidance」の 4 つからなり、暗号鍵管理に関する文書類はそれらの構成要素のいずれかに分類できる。

第二の視点：暗号鍵管理における検討項目

SP800-130 に記載されているトピックスや Framework Requirements を大きく以下の 6 つの『暗号鍵管理における目的（取り扱い項目）に応じた対象範囲』に分類・グループ化することによって、検討すべき項目の目的や必要性を明確化し、分かりやすく整理し直した。それら 6 つの目的の関係性を図 1-2 に示す。これにより、対象とする CKMS の利用環境に応じて本当に必要な検討項目をあらかじめ抽出することができ、効率よく CKMS 設計・構築に反映できると期待している。

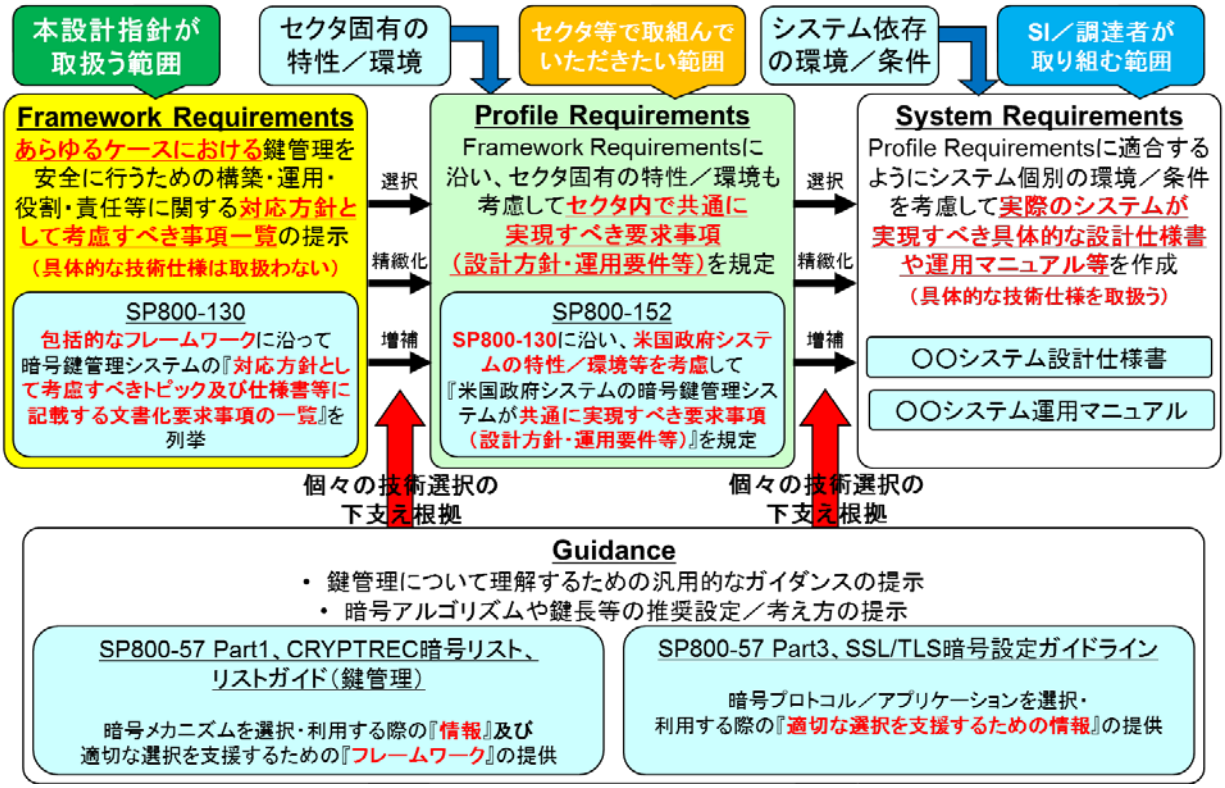


図 1-1　暗号鍵管理の考え方の枠組み

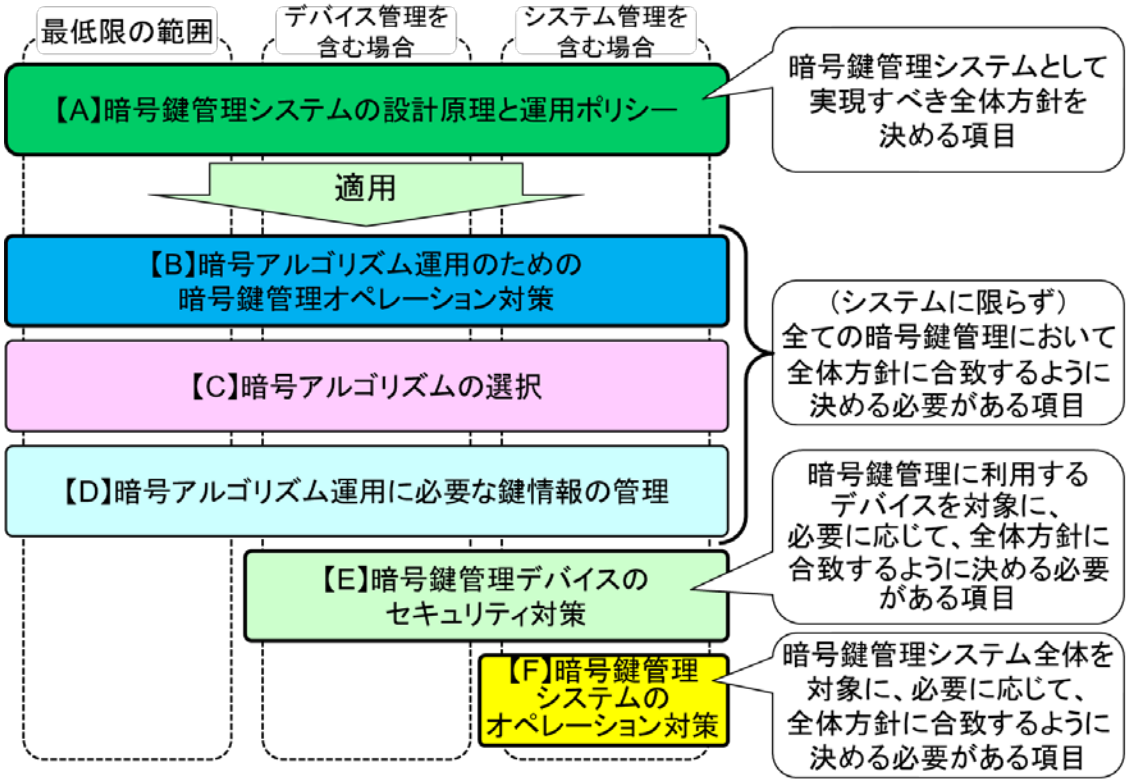


図 1-2　暗号鍵管理における目的別分類関係

第三の視点：暗号鍵管理における時間管理

暗号鍵管理においては「時間」の概念が非常に重要である。本設計指針では、時間管理の概念を図 1-3 のように整理した。これにより、時間管理の中で、いつまでに何を準備しなければならないのかを判断し、仕様書や運用マニュアルに組み入れることができるようになると考えている。

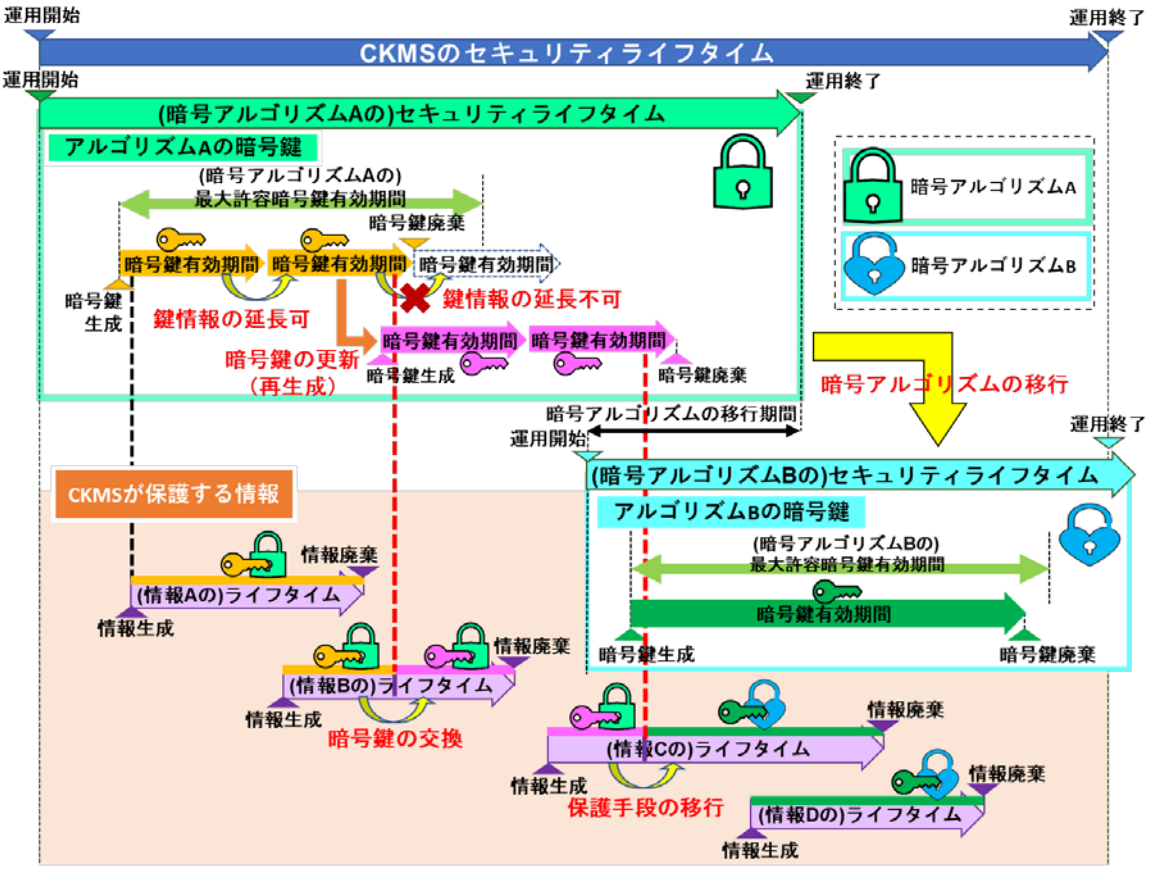


図 1-3　暗号鍵管理における時間管理の概念図

第四の視点：本設計指針の具体的な活用方法

CKMS の Profile Requirements や System Requirements を作成する設計者を対象に、具体的なプロファイルや仕様書等を作成する際に本設計指針を活用することを想定している。加えて、作成されたプロファイルや仕様書等が漏れなく適切な検討を踏まえて作成されたものであるかどうかをシステム管理責任者や調達責任者が確認・比較できるようにすること期待している。

- CKMS 設計者にとっての具体的な活用方法：
  a)　Framework Requirements の目的及びそれに続く概要に照らし合わせて、個々のト

ピックスが今回設計する CKMS が取り扱う対象範囲であるかどうかの判断を行う。対象範囲と判断すればb）に進み、対象範囲外と判断すればc）に進む。

b) 対象範囲の Framework Requirements ごとに、どのような要求仕様／設計方法を採用するか、あるいはどのような対応をとるかを決定し、その内容を要求事項として Profile Requirements や System Requirements に記載する。なお、一つの Framework Requirements に対して要求事項は一つとは限らず、複数となる場合もある。

c) 対象外と判断すればそのように判断した理由を明記したうえで当該 Framework Requirements は「対象外」と除外する。

- システム管理責任者や調達責任者等にとっての具体的な活用方法：

d) Framework Requirements ごとに、Profile Requirements や System Requirements に記載された要求事項の内容が適切であるかどうかを確認する。また、対象外と判断された項目については、対象外と判断した理由が適切であるかどうかを確認する。

1.3.2 TLS 暗号設定ガイドラインの作成

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

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

<u>位置づけ</u>

、「暗号技術以外の様々な利用上の判断材料も加味した合理的な根拠」を重視して現実的な利用方法を目指している。具体的には、実現すべき安全性と必要となる相互接続性とのトレードオフを考慮する観点から、安全性と相互接続性を踏まえたうえで設定すべき要求設定として3つの設定基準（「高セキュリティ型」「推奨セキュリティ型」「セキュリティ例外型」）を提示している。

実際にどの設定基準を採用するかは、安全性の確保と相互接続の必要性の両面を鑑みて、サーバ管理やサービス提供に責任を持つ管理者が最終的に決定すべきことではあるが、本ガイドラインでは、安全性もしくは相互接続性についての特段の要求がなければ「推奨セキュリティ型」の採用を強く勧める。本ガイドラインの作成時点（2020 年 3 月）では、「推奨セキュリティ型」がもっとも安全性と相互接続性のバランスが取れている要求設定であると考えている。

主な改訂内容

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

プロトコルバージョンの要求設定において TLS1.3 の採用及び SSL3.0 の禁止が行われた。これに伴い、各設定基準における要求設定についても大幅な変更が行われており、現行ガイドラインにおける設定基準から一段階高い安全性を求めるようになった項目も多い（図 1-4、表 1-3 参照）。例えば、推奨セキュリティ型で利用が認められていた TLS1.0 や TLS1.1 は、本ガイドラインではセキュリティ例外型のみで利用可能となった。また、鍵交換では Perfect Forward Secrecy の特性をもつ ECDHE や DHE をさらに強く推奨するようにした。

また、SSL3.0 の禁止と併せて、ガイドラインの名称を「SSL/TLS 暗号設定ガイドライン」から「SSL」を削除し、「TLS 暗号設定ガイドライン」とすることとした。

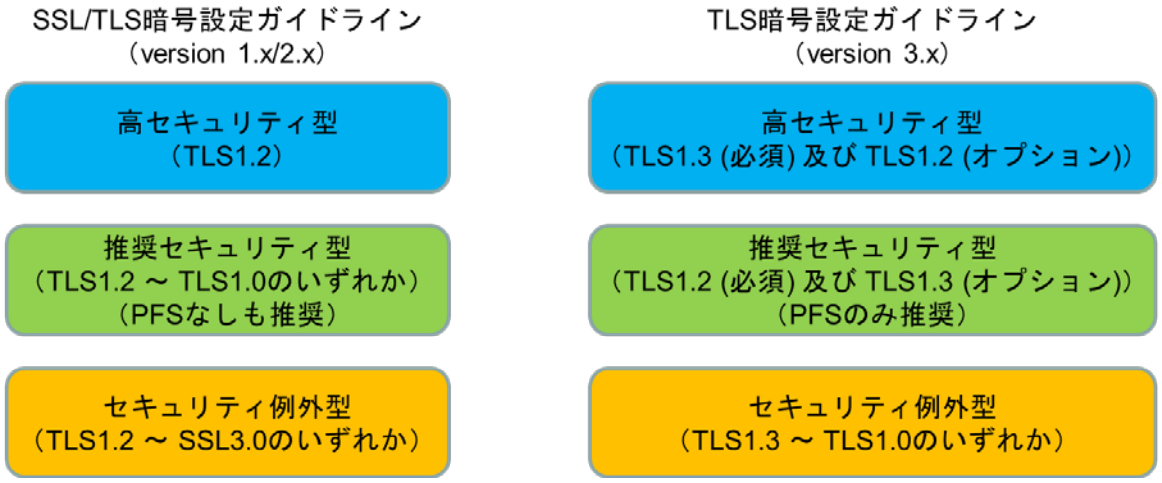


図 1-4　設定基準における要求設定の変更

B) 要求設定における「遵守項目」と「推奨項目」の区分けの新設

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

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

具体的な要求設定の区分けは表 1-4 の通りである。

表 1-3　要求設定の概要

要件		高セキュリティ型	推奨セキュリティ型	セキュリティ例外型
【遵守】想定対象		高い安全性の確保を必要とするケース	一般的な利用形態	推奨セキュリティ型への移行完了までの暫定運用
【遵守】暗号アルゴリズム		高セキュリティ型での利用禁止暗号を利用不可	推奨セキュリティ型での利用禁止暗号を利用不可	セキュリティ例外型での利用禁止暗号を利用不可
【遵守】バージョン		TLS1.3 (必須) 及び TLS1.2 (オプション)	TLS1.2 (必須) 及び TLS1.3 (オプション)	TLS1.3 ～ TLS1.0 のいずれか
【推奨】推奨暗号アルゴリズム設定	鍵交換	①256 ビット以上の ECDHE ②2048 ビット以上の DHE	①256 ビット以上の ECDHE ②2048 ビット以上の DHE	①1024 ビット以上の DHE 又は 256 ビット以上の ECDHE ②2048 ビット以上の RSA, 1024 ビット以上の DH, 256 ビット以上の ECDH のいずれか
	暗号化	128 ビット及び 256 ビットの AES 又は Camellia、もしくは ChaCha20-Poly1305		128 ビット及び 256 ビットの AES 又は Camellia、もしくは ChaCha20-Poly1305
	暗号利用モード	GCM, CCM, CCM_8 のいずれか	①GCM, CCM, CCM_8 のいずれか ②CBC	①GCM, CCM, CCM_8 のいずれか ②CBC
	ハッシュ関数	SHA-384 又は SHA-256	①SHA-384 又は SHA-256 ②SHA-1	SHA-384, SHA-256, SHA-1 のいずれか
【遵守】サーバ証明書	公開キー	鍵長 2048 ビット以上の RSA 又は 256 ビット以上の ECC		鍵長 2048 ビット以上の RSA
	署名アルゴリズム	鍵長 2048 ビット以上の RSA 又は 256 ビット以上の ECDSA		鍵長 2048 ビット以上の RSA
	ハッシュ関数	SHA-256 以上	SHA-256	SHA-256

凡例：　【遵守】遵守項目　　【推奨】推奨項目

表 1-4　要求設定における遵守項目と推奨項目

要求設定	遵守項目	プロトコルバージョン	利用禁止プロトコルバージョンを利用不可にする設定
		サーバ証明書	利用する暗号アルゴリズムと鍵長の設定
			発行・更新時の鍵情報の生成方法の明確化
			警告表示の回避方法の明確化
		暗号スイート	利用禁止暗号アルゴリズムを利用不可にする設定
			公開鍵暗号の鍵長の設定
	推奨項目	プロトコルバージョン	利用プロトコルバージョンの優先順位付け
		暗号スイート	利用推奨暗号アルゴリズムのみでの設定
			推奨暗号スイートの優先順位付け

C) 章構成の変更

現行ガイドラインでは、

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

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

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

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

の章構成とし、各章に「プロトコルバージョン」「サーバ証明書」「暗号スイート」の設定項目を記載した（図 1-5 参照）。これにより、選択した設定基準での該当章だけを参照すればよい構成とした。

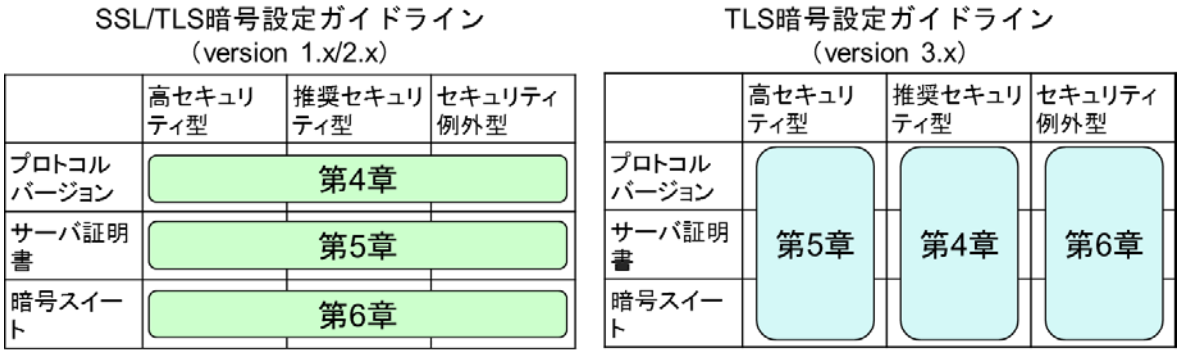


図 1-5　章構成の変更

1.3.3　EdDSA に関する安全性評価の必要性についての検討

EdDSA は、TLS1.3 で採用された署名アルゴリズムである（RFC 8446）。さらに、TLS1.2 以前では、ECDSA と同じ暗号スイートを使って EdDSA も利用可能となった（RFC8422）。

今後の利用状況によっては、早晩、TLS 暗号設定ガイドラインを改訂し EdDSA を推奨暗号スイートに含めるか否かを判断する必要に迫られると可能性があることから、暗号技術活用委員会では EdDSA に関する安全性評価の必要性について検討を行った。その結果、今後 EdDSA の利用が進み、TLS 暗号設定ガイドラインに EdDSA を推奨暗号スイートに含めるか否かの判断が迫られた際に速やかに対応できるように準備をしておく観点から、EdDSA に対して CRYPTREC 暗号リストへの掲載是非に資するレベルでの安全性評価を実施することが必要であるとの結論を取りまとめた。併せて、EdDSA では利用する楕円曲線パラメータが Ed25519 と Ed448 であるため、楕円曲線パラメータについて、Ed25519 が P-256 と、Ed448 が P-384 と同程度の安全性を有する楕円曲線パラメータであるかどうか評価することの必要性も指摘した。

1.3.4　RC4 の運用監視暗号リストからの削除についての検討

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

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

【運用監視暗号リストからの削除ルール（案)】

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

＜削除条件＞

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

【RC4 の運用監視暗号リストからの削除（案)】

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

資料４別添１

EdDSA に関する安全性評価の必要性について

現在、暗号技術活用委員会の傘下で活動している TLS 暗号設定ガイドラインワーキンググループ（主査：須賀祐治、以下「WG」という。）において、TLS 暗号設定ガイドライン（以下「ガイドライン」という。）を作成している。

今回のガイドラインでは EdDSA を推奨暗号スイートに含めることは安全性評価が必要であるため時期尚早と判断しているものの、今後の利用状況によっては、早晩ガイドラインを改訂し EdDSA を推奨暗号スイートに含めるか否かの判断が必要となる可能性が十分に考えられる。そのため、必要時に速やかに対応できるように準備をしておく観点から、EdDSA に対して CRYPTREC 暗号リストへの掲載に資するレベルでの安全性評価を実施することが必要であると判断した。

【背景】

EdDSA は、TLS1.3 で採用された署名アルゴリズムである（RFC 8446 [1]）。さらに、TLS1.2 以前では、ECDSA と同じ暗号スイートを使って EdDSA も利用可能となった（RFC8422 [2]）。

具体的には、TLS1.3 で採用された署名アルゴリズムは以下の通りであり、EdDSA は必須ではないもののオプションとして採用可能な唯一の署名アルゴリズムである。これらの署名アルゴリズムは、TLS でのサーバ認証及びクライアント認証で利用される。

- RSASSA-PKCS1-v1_5 （mandatory for certificates w/sha256）
- ECDSA （mandatory w/secp256r1_sha256）
- RSASSA-PSS （mandatory for CertificateVerify and certificates w/sha256）
- EdDSA

また、TLS1.2 以前では以下の通り拡張されており、ECDSA と同様の使い方ができるようになっている。

- ECDHE_ECDSA | Ephemeral ECDH with ECDSA or EdDSA signatures
  ※ 暗号スイートで区別するのではなく、extension での署名パラメータに ECDSA と EdDSA のどちらを利用するかの情報を記載して区別する

実装面でも 2018 年後半からオープンソースソフトウェアを中心に、Ed25519 曲線と一緒に EdDSA のサポートが進められている。下記に例を挙げる。

- OpenSSL 1.1.1d
- Bouncy Castle 1.64
- Thunderbird 68.2.0
- Android 10

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[3][4]。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[5]。

このように TLS で EdDSA を利用できる環境が整備されつつあるため、現状では楕円曲線暗号では ECDSA が使われることが多いものの、近いうちに EdDSA も TLS で利用されるようになる可能性が十分にあると WG では考えている。今後の利用状況によっては、早晩、ガイドラインを改訂し EdDSA を推奨暗号スイートに含めるか否かを判断する必要に迫られると思われる。

一方、ガイドラインで推奨暗号スイートに含める暗号アルゴリズムは CRYPTREC 暗号リスト（原則として「電子政府推奨暗号リスト」又は「推奨候補暗号リスト」）に掲載されるものとしているため、EdDSA を推奨暗号スイートに含めるためには、EdDSA が CRYPTREC 暗号リストに掲載されるか、少なくとも CRYPTREC 暗号リストに掲載されている暗号アルゴリズムと同程度の安全性を有していることを確認する必要がある。

【審議事項】

今後 EdDSA の利用が進み、ガイドラインに EdDSA を推奨暗号スイートに含めるか否かの判断が迫られた際に速やかに対応できるように準備をしておく観点から、EdDSA に対して CRYPTREC 暗号リストへの掲載に資するレベルでの安全性評価を実施することが必要である。

併せて、EdDSA では利用する楕円曲線パラメータが Ed25519 と Ed448 であるため、楕円曲線パラメータについて、Ed25519 が P-256 と、Ed448 が P-384 と同程度の安全性を有する楕円曲線パラメータであるかどうか評価することが望ましい。実際、Ed25519 と Ed448 は、P-224, P-256, P-384, P-521 と並び、楕円曲線パラメータに指定される予定である（SP800-186 ドラフト版で指定済[6]）。

【参考文献】

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

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

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

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

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

[6] NIST, “Recommendations for Discrete Logarithm-Based Cryptography: Elliptic Curve Domain Parameters,” NIST Special Publication 800-186 (Draft), 2019

以上

資料4別添2

暗号鍵管理システム設計指針（基本編）概要

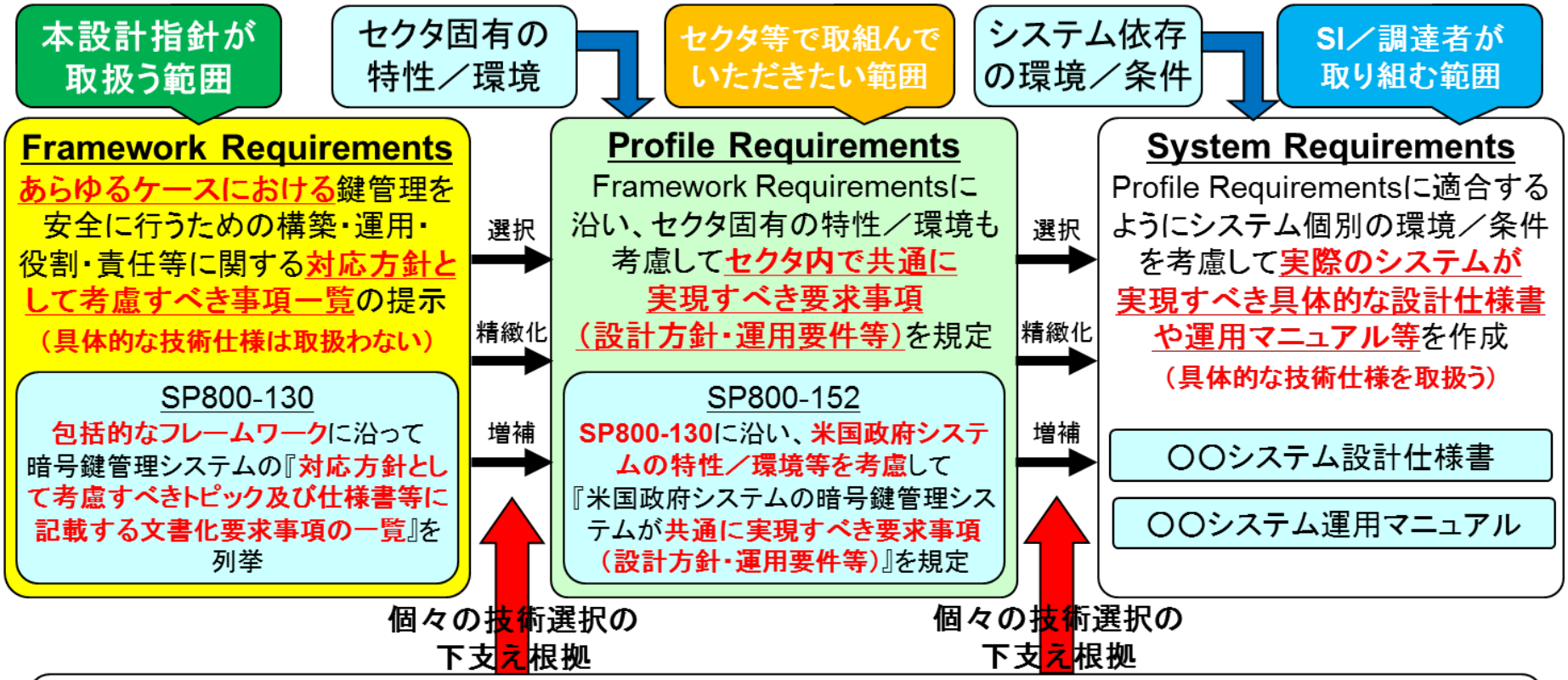
『暗号鍵管理システム設計指針（基本編）』とは

あらゆる分野・あらゆる領域の全ての暗号鍵管理システムを対象に暗号鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として**考慮すべき事項（Framework Requirements）を網羅的に提供**し、設計時に考慮すべきトピックス及び**設計書等に明示的に記載する要求事項を取りまとめた**ガイドライン

- 暗号鍵管理の考え方の枠組みを整理し、暗号鍵管理のための設計仕様書や運用マニュアルがどのように作られるべきかを明確化。4つの視点からなる
- 「暗号鍵管理の在り方」（暗号鍵管理の位置づけと検討すべき枠組み）では、暗号鍵管理の必要性を認識してもらうための解説を記載
- 「暗号鍵管理についての技術的内容」では、NIST SP800-130「A Framework for Designing Cryptographic Key Management Systems」の解説書・利用手引書として活用できるように構成
- セキュリティ要求事項は定義せず、具体的な特定のセキュリティ機能を義務づけない
  - どのように要求事項に対応するか＞設計者に委ねられる
  - 対応方針が適正かどうかの判断＞運用管理者や調達責任者が行う

第一の視点：暗号鍵管理の考え方の枠組み

■ 暗号鍵管理の設計仕様書や運用マニュアルをどのように作るべきかを明確化



Guidance

- 鍵管理について理解するための汎用的なガイダンスの提示
- 暗号アルゴリズムや鍵長等の推奨設定／考え方の提示

SP800-57 Part1、CRYPTREC暗号リスト、リストガイド（鍵管理）

暗号メカニズムを選択・利用する際の『情報』及び適切な選択を支援するための『フレームワーク』の提供

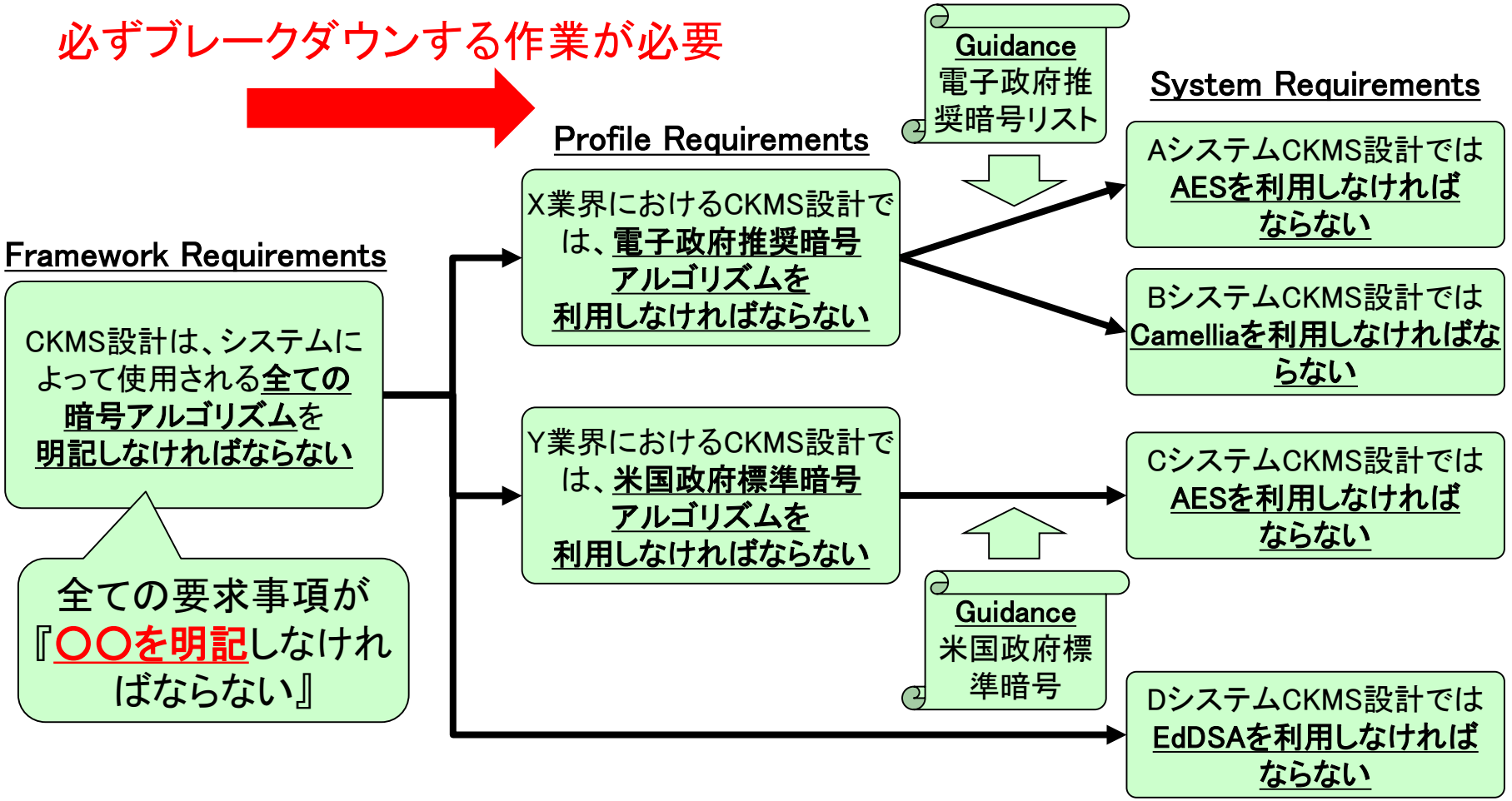
SP800-57 Part3、SSL/TLS暗号設定ガイドライン

暗号プロトコル／アプリケーションを選択・利用する際の『適切な選択を支援するための情報』の提供

第一の視点：暗号鍵管理の考え方の枠組み

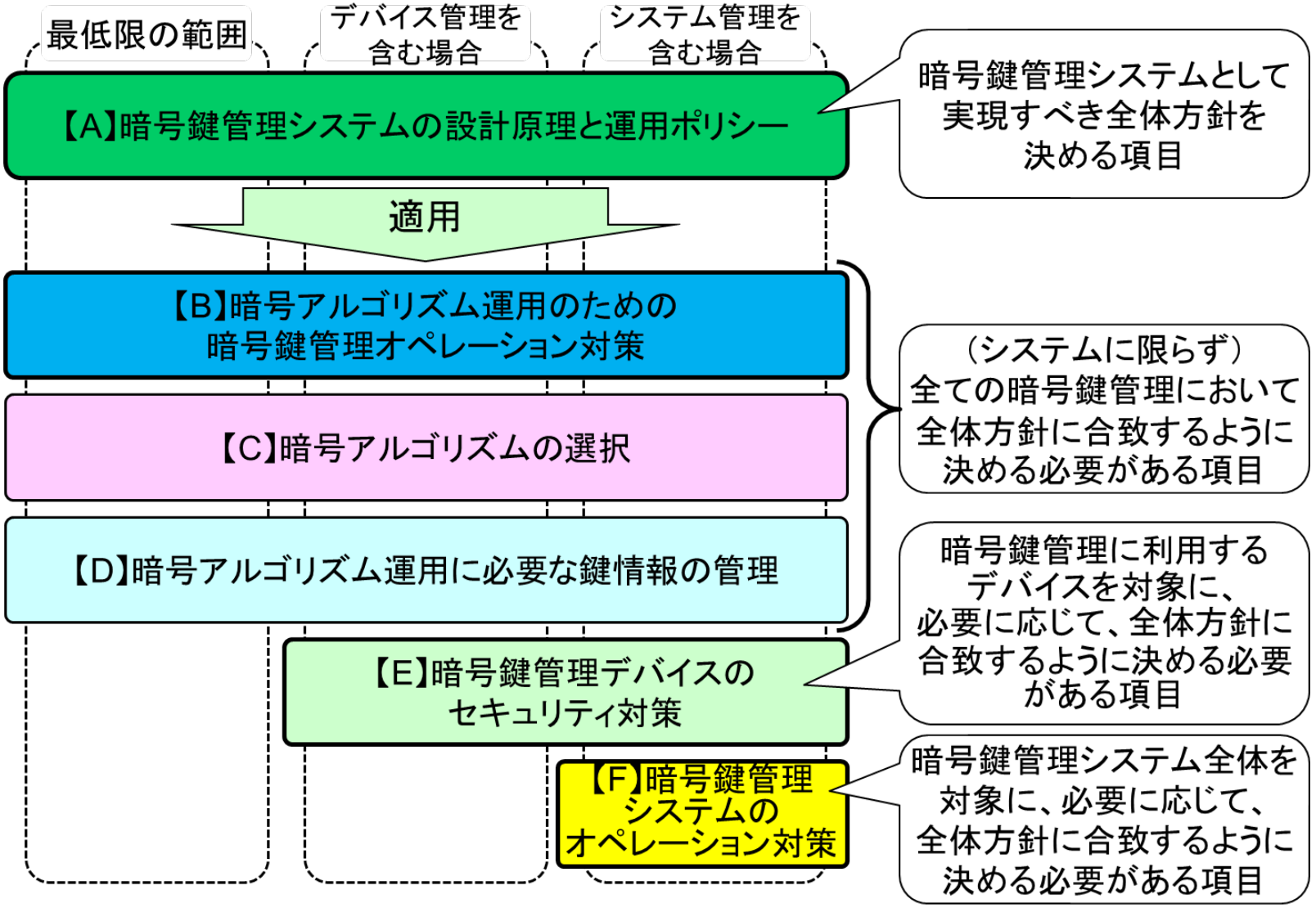
暗号鍵管理システムで検討すべき事項は同じでも実現方法は違う

Framework requirements　　Profile/System requirements



第二の視点：暗号鍵管理における検討項目

- 6つの『暗号鍵管理における目的（取り扱い項目）に応じた対象範囲』に分類・グループ化することによって、検討すべき項目の目的や必要性を明確化



第二の視点：暗号鍵管理における検討項目

【A】暗号鍵管理システムの設計原理と運用ポリシー

CKMSとして実現すべき全体方針を取り決める検討項目（69項目）

- CKMSをどのような方針（ポリシー）で運用するのか。そのために、どういった機能を用意しなければならないのか
- CKMSの利用者が誰でどういった権限を有しているのか
- CKMSの構築環境や実現目標はどういったものか
- 適合しなければならない法規制や標準化等があるのか
- 将来的な移行対策を準備しておく必要があるか

		SP800-130該当節
（4章）暗号鍵管理システム（CKMS）の設計原理と運用ポリシー	（4.1節） CKMSセキュリティポリシー	4.3, 4.4, 4.5
	（4.2節） 情報管理ポリシー等からの要求事項	4.6, 4.7
	（4.3節） セキュリティドメインポリシー	4.9
	（4.4節） CKMSにおける役割と責任	5
	（4.5節） 暗号鍵管理システムの構築環境／実現目標	2.10, 3.1, 3.2, 3.4, 3.5, 6.2, 7
	（4.6節） 標準／規制に対する適合性	3.3, 4.8
	（4.7節） 将来的な移行対策の必要性	7, 12

第二の視点：暗号鍵管理における検討項目

4. 暗号鍵管理システム（CKMS）の設計原理と運用ポリシー

4.1 CKMS セキュリティポリシー	①CKMSの設計にあたって、CKMSセキュリティポリシーを作成しなければならない。	A.01～A.02
	②CKMSセキュリティポリシーは、他のセキュリティポリシーや組織の様々なポリシーに依存することがあるので、それらを意識しなければならない。	A.03～A.04
	③CKMSセキュリティポリシーがCKMS内に電子的に保管され自動的に処理される場合には正しい処理が行われるように注意をしなければならない。	A.05
4.2 情報管理ポリシー等からの要求事項	①機微な情報を管理するために、「個人の説明責任（Personal accountability）」について情報管理ポリシー等の要求事項に記載される場合には、どのように対応するかを決めなければならない。	A.06
	②エンティティに対するプライバシーの提供、関連法令の遵守、又はセキュリティ強化のために、「匿名性」「連結不可能性」「観測不可能性」（のいずれか）の保証について情報管理ポリシー等に記載される場合には、どのように対応するかを決めなければならない。	A.07～A.13

検討番号A.01はCKMSセキュリティポリシーを作成することを、A.02はそのCKMSセキュリティポリシーに明記すべき内容及びその実現・利用方法について明確化することを要求したもの

A.01	FR4.1	CKMS設計は、実行するために設計した設定可能なオプションとサブポリシーを含むCKMSセキュリティポリシーを明記しなければならない。
A.02	FR4.2	CKMS設計は、CKMSセキュリティポリシーがCKMSによってどのように実行されるのか（例えば、ポリシーが要求する保護を提供するために使用されるメカニズム）を明記しなければならない。

第二の視点：暗号鍵管理における検討項目

【B】暗号アルゴリズム運用のための暗号鍵管理オペレーション対策

生成から廃棄までのライフサイクル全期間にわたって暗号鍵を管理するのに必要な機能や運用方法を決める検討項目（全7節 81項目）

【C】暗号アルゴリズムの選択

利用する暗号アルゴリズムの選択条件を決める検討項目（全2節 2項目）

【D】暗号アルゴリズム運用に必要な鍵情報の管理

具体的な鍵情報の設定方法や保管方法などを取り決める検討項目（全3節 10項目）

【E】暗号鍵管理デバイスのセキュリティ対策

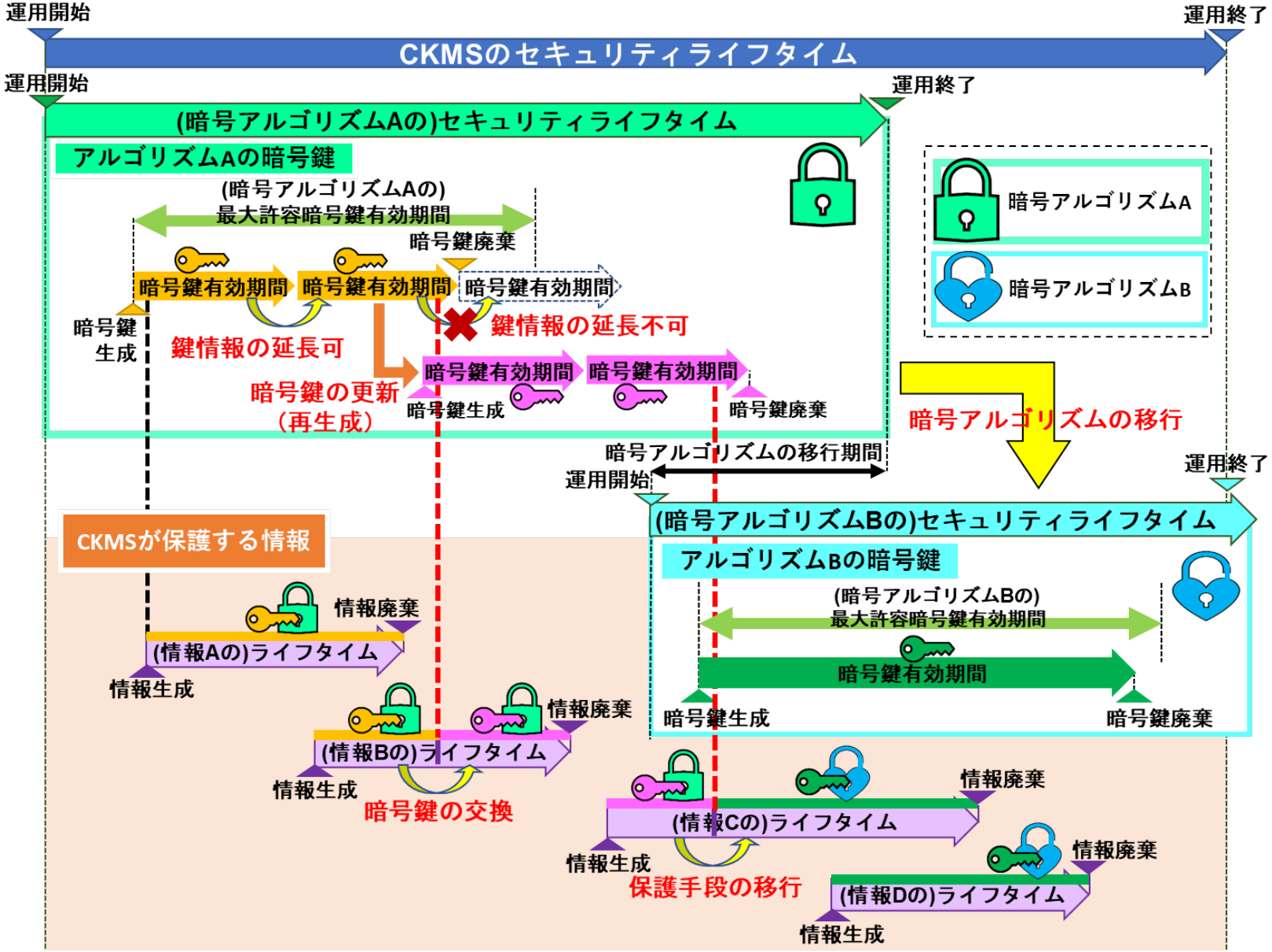
暗号鍵を管理するデバイスに対して、必要に応じて検討する項目（全3節 37項目）

【F】暗号鍵管理システムのオペレーション対策

CKMS全体に対して、必要に応じて検討する項目（5節全57項目）

第三の視点：暗号鍵管理における時間管理

- 暗号鍵管理における時間管理の概念を整理



第四の視点：本設計指針の具体的な活用方法

- CKMS設計者：具体的なプロファイルや仕様書等を作成する際に活用
- システム管理責任者や調達責任者：作成されたプロファイルや仕様書等が漏れなく適切な検討を踏まえて作成されたものであるかどうかを確認・比較

- Profile RequirementsやSystem Requirementsの作成にあたっては、CKMSの要求事項としてどの程度の強制力を持たせるのかを混同しないように明記しなければならない

【満たさなければ不適合となる要件】

- **【必須】**：必ず満たさなければならない要求事項を記述する際に利用する。「〇〇**しなければならない**。」
- **【禁止】**：絶対にしてはならない要求事項を記述する際に利用する。「〇〇**してはならない**。」

【満たすものを優先的に取り扱うべき要件】

- **【要望】**：できるだけ満たすように求める事項を記述する際に利用する。「〇〇**すべきである**。」

【上記以外の要件】

- **【オプション】**：満たすようにしてもよい事項を記述する際に利用する。「〇〇**してもよい**。」「〇〇することがあり得る。」

パブリックコメント対応

- コメントは1件のみ（以下、抜粋）

  第8章記載の暗号モジュールについて、安全な暗号鍵保管のソリューションとしては、「HSM: Hardware Security Module」が数十年前から存在しており、「HSM」という略語自体でGlobalにおいては1つのセキュリティマーケットを構成しております。

  鍵管理の方法はHSMよりセキュリティレベルの低い方法もありますが、より上位の鍵管理手法として、「HSM」について言及いただく事で、この指針を読まれるユーザー自身、鍵管理方法にどのようなものがあるかよりわかりやすく明示できると考えます。

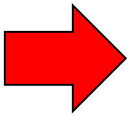
  既に海外では政府公官庁、防衛、銀行、クレジットカード業界では標準的なセキュリティソリューションであり、EUのGDPRでも推奨として扱われてますので、その点ご留意いただき、正式版においてはNISTと乖離がないよう、NIST SP800-57 Part2同等の記載をお勧めいたします。

【対応方針案】

内容としては、「暗号モジュール」の代わりに「HSM」を使うべき、というご意見だと解釈しました。

しかしながら、暗号モジュールには、HSM以外にも、暗号コプロ、SCU（セキュア暗号ユニット）、ソフトウェア暗号モジュールなど、様々な実装形態のものがあることから、本ガイドラインが対象とするFramework RequirementsのレベルでHSMに限定するのは適切ではないのではないかと考えます。

HSMを使うかどうかはProfile RequirementsやSystem Requirementsのレベルで判断すべきものであるとし、本コメントに対しては特にガイドラインに反映しないということにしたいと思いますが、いかがでしょうか。



反対意見なし。ガイドラインには反映しない

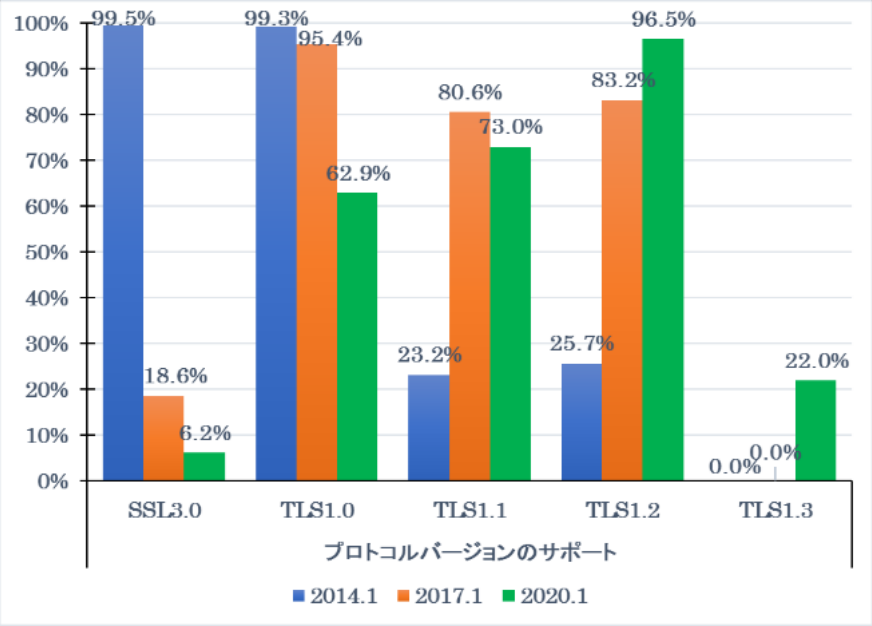
TLS暗号設定ガイドライン概要

環境の変化状況－SSL Pulseのデータ

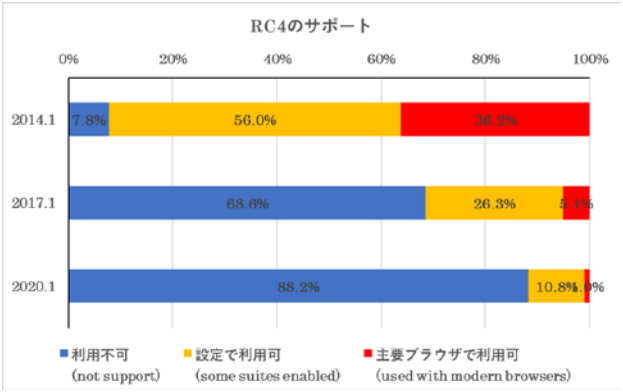
SSL Pulse

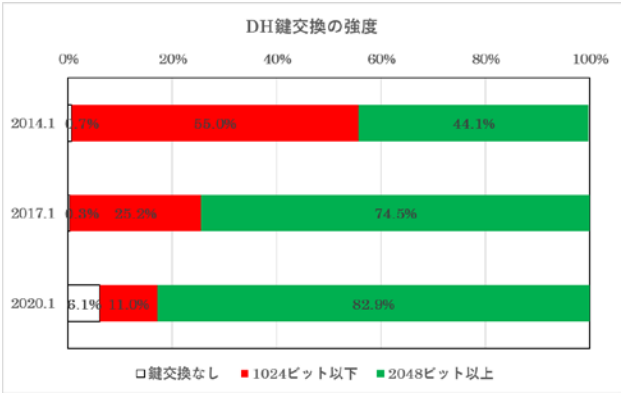
https://www.ssllabs.com/ssl-pulse/

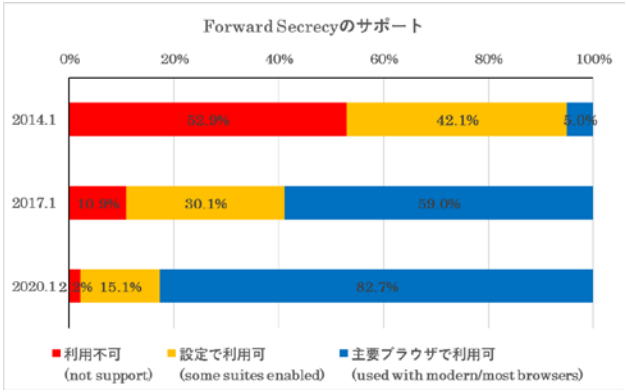
SSL Pulse is a continuous and global dashboard for monitoring the quality of SSL / TLS support over time across 150,000 SSL- and TLS-enabled websites, based on Alexa's list of the most popular sites in the world.



[RFC7465 (2015)] RC4禁止[Prohibiting]
[RFC7525 (2015)]
SSL2.0, SSL3.0, RC4禁止[MUST NOT]、
TLS1.0, TLS1.1, Triple DES非推奨[SHOULD NOT]
[RFC7568 (2015)] SSL3.0利用自粛[Deprecating]
[RFC8446 (2018)] TLS1.3発行
[ID] TLS1.0, TLS1.1利用自粛[Deprecating]







見直し方針

- 見直し方針
  ガイドラインの位置づけ及び想定読者に関しては現行ガイドラインと同様とするが、以下の論点項目を中心に見直しを行う
  - 位置づけ:
    TLSに関する「Best Practice集」
  - 想定読者:
    サーバ構築者、サーバ管理者、並びにシステム担当者
    一部の内容については、ブラウザを使う一般利用者への注意喚起も対象
- 論点項目一覧
  - タイトルの名称
  - 推奨プロトコルバージョンの見直し
  - 推奨暗号スイートの見直し
  - サーバ証明書の利用方法の見直し
  - ブラウザでの標記に関する留意点の追加
  - 常時HTTPS化に伴う留意点の追加
  - 現行ガイドラインでは情報提供として記載している内容(鍵生成、サーバ証明書の種類や有効期間、鍵管理など)についての見直し、要求事項への格上げ、あるいは削除
  - IoT機器やSSL-VPN、クラウド利用など、サーバ—ブラウザ以外の利用形態での利用方法の追加
  - 代表的な製品・OSSについて具体的な設定方法の見直し
  - その他、委員からの指摘項目

本バージョンで変えなかったところ－3段構成の概要

設定基準	概要	安全性	相互接続性の確保
高セキュリティ型	情報が漏えいした際、組織の運営や資産、個人の資産やプライバシー等に悪影響を及ぼすと予想される情報を、安全性を優先してTLS通信を行うような場合に採用する設定基準 ※ 高い安全性の確保を必要とするケースでの利用を想定している **＜利用例＞** **• 特にセキュリティが重要視されるシステムを構築する場合**	本ガイドライン作成時点（2020年3月）において、標準的な水準を大きく上回る高い安全性水準を達成している	本ガイドラインで対象とするブラウザが搭載されているPC、スマートフォン等であれば相互接続性を確保できると期待される。
推奨セキュリティ型	情報が漏えいした際、組織の運営や資産、個人の資産やプライバシー等に悪影響を及ぼすと予想される情報を、安全性確保と利便性（相互接続性）の実現をバランスさせてTLS通信を行うための標準的な設定基準 ※ほぼすべての一般的な利用形態で使うことを想定している **＜利用例＞** **• 電子申請など、企業・国民と役所等との電子行政サービスを提供する場合** **• 金融サービスや電子商取引サービス、多様な個人情報の入力を必須とするサービス等を広範囲（不特定多数）に提供する場合** **• 新規に社内システムを構築する場合**	本ガイドライン作成時点（2020年3月）における標準的な安全性水準を実現している	本ガイドラインで対象とするブラウザが搭載されているPC、スマートフォンを含め、多くの製品・システムで相互接続性を確保できると期待される。 ※サポートが終了しているバージョンが古いOSやブラウザ、発売開始から長期間経過している古い機器、IoT用途などの一部の機器類については接続できない可能性がある。
セキュリティ例外型	脆弱なプロトコルバージョンや暗号が使われるリスクを受容したうえで、安全性よりも相互接続性に対する要求をやむなく優先させてTLS通信を行う場合に採用する設定基準 ※推奨セキュリティ型への移行完了までの暫定運用を想定している **＜利用例＞** **• 利用するサーバやクライアントの実装上の制約、又は既存システムとの相互接続上の制約により、推奨セキュリティ型（以上）の設定が事実上できない場合**	本ガイドライン作成時点（2020年3月）において、標準的な安全性水準を満たしていないプロトコルバージョンや暗号スイート等が使用される可能性があることを認識する必要がある	既存システムを含め、ほぼすべての機器に対して相互接続性が確保されると期待される。

本バージョンでの大きな変更点(1)

- ガイドライン名称の変更
  「SSL/TLS暗号設定ガイドライン」→「TLS暗号設定ガイドライン」

- TLS1.3採用及びSSL3.0禁止に伴う各設定基準における要求設定の変更
  - 一段階高い安全性を求めるようになった項目も多い

SSL/TLS暗号設定ガイドライン（version 1.x/2.x）	TLS暗号設定ガイドライン（version 3.x）
高セキュリティ型（TLS1.2）	高セキュリティ型（TLS1.3 (必須) 及び TLS1.2 (オプション)）
推奨セキュリティ型（TLS1.2 ～ TLS1.0のいずれか）（PFSなしも推奨）	推奨セキュリティ型（TLS1.2 (必須) 及び TLS1.3 (オプション)）（PFSのみ推奨）
セキュリティ例外型（TLS1.2 ～ SSL3.0のいずれか）	セキュリティ例外型（TLS1.3 ～ TLS1.0のいずれか）

本バージョンでの大きな変更点(2)

- 要求設定における「遵守項目」と「推奨項目」の区分けの新設

要求設定	遵守項目	プロトコルバージョン	利用禁止プロトコルバージョンを利用不可にする設定
		サーバ証明書	利用する暗号アルゴリズムと鍵長の設定
			発行・更新時の鍵情報の生成方法の明確化
			警告表示の回避方法の明確化
		暗号スイート	利用禁止暗号アルゴリズムを利用不可にする設定
			公開鍵暗号の鍵長の設定
	推奨項目	プロトコルバージョン	利用プロトコルバージョンの優先順位付け
		暗号スイート	利用推奨暗号アルゴリズムのみでの設定
			推奨暗号スイートの優先順位付け

- 章構成の変更

SSL/TLS暗号設定ガイドライン
（version 1.x/2.x）

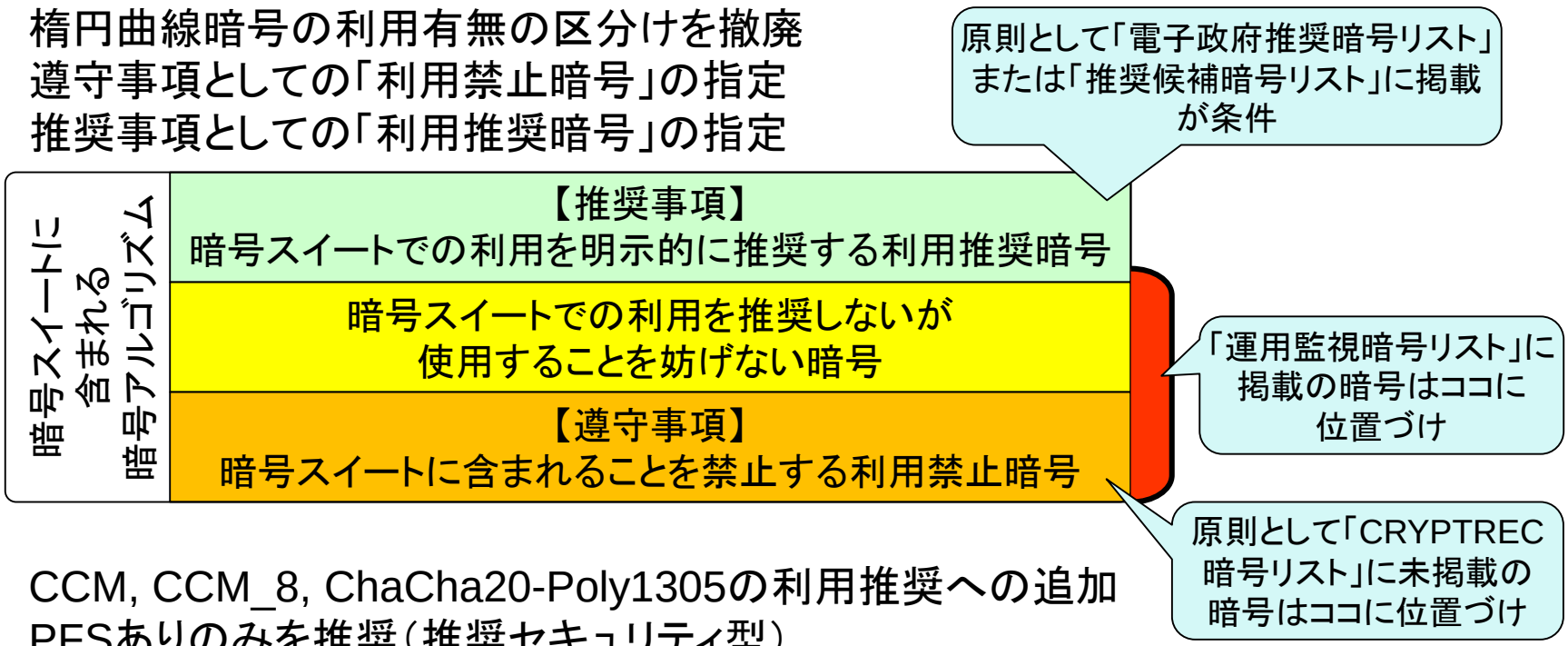
	高セキュリティ型	推奨セキュリティ型	セキュリティ例外型
プロトコルバージョン	第4章		
サーバ証明書	第5章		
暗号スイート	第6章		

TLS暗号設定ガイドライン
（version 3.x）

	高セキュリティ型	推奨セキュリティ型	セキュリティ例外型
プロトコルバージョン	第5章	第4章	第6章
サーバ証明書			
暗号スイート			

【推奨項目】利用推奨暗号＆【遵守項目】利用禁止暗号

- 主な変更点
  - 楕円曲線暗号の利用有無の区分けを撤廃
  - 遵守事項としての「利用禁止暗号」の指定
  - 推奨事項としての「利用推奨暗号」の指定



  - CCM, CCM_8, ChaCha20-Poly1305の利用推奨への追加
  - PFSありのみを推奨（推奨セキュリティ型）
  - Triple DES, RC4の利用禁止暗号への指定（セキュリティ例外型）
  - 楕円曲線暗号も利用推奨に含まれることを明確化（セキュリティ例外型）

- EdDSAの取扱い
  - 今回のバージョンでは「推奨しないが使用することを妨げない暗号」に位置づけ
  - 利用推奨の条件が整った段階でガイドラインの（マイナー）アップデートの実施を検討

【推奨項目】利用推奨暗号＆【遵守項目】利用禁止暗号

		高セキュリティ型	推奨セキュリティ型	セキュリティ例外型	共通の利用禁止暗号
鍵交換		DHE ECDHE	DHE ECDHE	DH DHE ECDH ECDHE RSAES-PKCS1-V1_5	なし
署名		ECDSA RSASSA-PKCS1-v1_5 RSASSA-PSS*2*3	ECDSA RSASSA-PKCS1-v1_5	ECDSA RSASSA-PKCS1-v1_5	GOST R 34.10-2012*1
暗号化	64ビットブロック暗号				RC2, EXPORT-RC2 IDEA DES, EXPORT-DES GOST 28147-89*1 Magma*1 3-key Triple DES
	128ビットブロック暗号	AES Camellia*4	AES Camellia*4	AES Camellia*4	Kuznyechik*1 ARIA SEED
	利用モード	CCM CCM_8 GCM	CBC CCM CCM_8 GCM	CBC CCM CCM_8 GCM	CTR_OMAC*1
	ストリーム	ChaCha20-Poly1305	ChaCha20-Poly1305	ChaCha20-Poly1305	RC4, EXPORT-RC4
ハッシュ関数(HMAC)		SHA-256 SHA-384	SHA-1 SHA-256 SHA-384	SHA-1 SHA-256 SHA-384	MD5 GOST R 34.11-2012*1
推奨しないが利用を妨げない		DSA EdDSA*2	RSAES-PKCS1-V1_5 DSA EdDSA*2	DSA EdDSA*2	凡例： *1 現在ID（RFCではない） *2 暗号スイートのIANA登録番号として管理されていない *3 TLS1.3でのみ利用可 *4 TLS1.2以前で利用可
追加の利用禁止暗号		DH ECDH RSAES-PKCS1-V1_5 CBC SHA-1	DH ECDH	なし	

【遵守項目】推奨プロトコルバージョン

- 主な変更点
  - TLS1.3の採用
  - SSL3.0の利用禁止（セキュリティ例外型）
  - TLS1.1及びTLS1.0の利用禁止（推奨セキュリティ型）

【高セキュリティ型】

TLS1.3	TLS1.2*	TLS1.1	TLS1.0	SSL3.0	SSL2.0
○	○	×	×	×	×

○：設定有効　×：設定無効化　ー：実装なし　*) 使わないことが明確な場合は設定無効にしてもよい

【推奨セキュリティ型】

	TLS1.3*	TLS1.2	TLS1.1	TLS1.0	SSL3.0	SSL2.0
2つのうちのいずれか	○	○	×	×	×	×
	ー	○	×	×	×	×

○：設定有効　×：設定無効化　ー：実装なし　*) 使わないことが明確な場合は設定無効にしてもよい

【セキュリティ例外型】

	TLS1.3	TLS1.2	TLS1.1	TLS1.0	SSL3.0	SSL2.0
4つのうちのいずれか	○	○	△	△	×	×
	ー	○	△	△	×	×
	ー	ー	△	△	×	×
	ー	ー	ー	△	×	×

○：設定有効　△：やむを得ず利用する場合に限り設定容認　×：設定無効化　ー：実装なし

【遵守項目】サーバ証明書推奨設定

- 主な変更点
  - SHA-1の削除（セキュリティ例外型）

	高セキュリティ型	推奨セキュリティ型	セキュリティ例外型
公開キー	2048ビット以上のRSA 256ビット以上のECC	2048ビット以上のRSA 256ビット以上のECC	2048ビット以上のRSA
署名 アルゴリズム	2048ビット以上のRSA 256ビット以上のECDSA	2048ビット以上のRSA 256ビット以上のECDSA	2048ビット以上のRSA
署名ハッシュ	SHA-256以上	SHA-256	SHA-256

【例：推奨セキュリティ型】

サーバ証明書の暗号アルゴリズムと鍵長	Subject Public Key Algorithmと鍵長としては、以下のいずれかを必須とする。 ● RSAEncryption（OID = 1.2.840.113549.1.1.1）で鍵長は2048ビット以上 ● ecPublicKey（OID = 1.2.840.10045.2.1）で鍵長256ビット以上（例：NIST P-256の場合のOID = 1.2.840.10045.3.1.7） Certificate Signature Algorithmと鍵長については、以下のいずれかを必須とする。 ● sha256WithRSAEncryption（OID = 1.2.840.113549.1.1.11）で鍵長2048ビット以上 ● ecdsa-with-SHA256（OID = 1.2.840.10045.4.3.2）で鍵長256ビット（NIST P-256）以上

【遵守項目】公開鍵暗号の鍵長設定

- 主な変更点
  - 楕円曲線暗号の利用有無の区分けを撤廃
  - DHEの鍵長を2048ビット以上に変更（推奨セキュリティ型）
  - RSAの記述を削除（推奨セキュリティ型）
  - 楕円曲線暗号の鍵長についても記載（セキュリティ例外型）

【高セキュリティ型】

設定すべき鍵長	鍵交換でECDHEを利用する場合には鍵長256ビット以上を、DHEを利用する場合には鍵長2048ビット以上での設定をしなければならない。 なお、DHEの鍵長を明示的に設定できない製品を利用する場合には、DHEを含む暗号スイートは選定すべきではない。

【推奨セキュリティ型】

設定すべき鍵長	鍵交換でECDHEを利用する場合には鍵長256ビット以上を、**DHEを利用する場合には鍵長2048ビット以上**での設定をしなければならない。 なお、DHEの鍵長を明示的に設定できない製品を利用する場合には、DHEを含む暗号スイートは選定すべきではない。

【セキュリティ例外型】

設定すべき鍵長	鍵交換でDHE・DHを利用する場合には鍵長1024ビット以上を、RSAを利用する場合には鍵長2048ビット以上を、**ECDHE・ECDHを利用する場合には鍵長256ビット以上**での設定をしなければならない。 なお、DHE・DHの鍵長を明示的に設定できない製品を利用する場合には、DHE・DHを含む暗号スイートは選定すべきではない。

【推奨項目】暗号スイート推奨設定

- 主な変更点
  - 楕円曲線暗号の利用有無の区分けを撤廃
  - 「推奨項目」に位置づけ変更
  - 優先順位付けの評価軸を「共通鍵暗号の鍵長」ベースから、「鍵交換」「暗号利用モード」ベースに変更

高セキュリティ型優先軸				
PFS特性	【第一】鍵交換	暗号利用モード	ハッシュ関数	共通鍵暗号鍵長
PFSあり	ECDHE	GCM CCM CCM_8	SHA-256 SHA-384	128ビット 256ビット
PFSあり	DHE	GCM CCM CCM_8	SHA-256 SHA-384	128ビット 256ビット

推奨セキュリティ型優先軸				
PFS特性	【第二】鍵交換	【第一】暗号利用モード	【第三】ハッシュ関数	共通鍵暗号鍵長
PFSあり	ECDHE	GCM CCM CCM_8	SHA-256 SHA-384	128ビット 256ビット
PFSあり	DHE	GCM CCM CCM_8	SHA-256 SHA-384	128ビット 256ビット
PFSあり	ECDHE	CBC	SHA-256 SHA-384	128ビット 256ビット
PFSあり	ECDHE	CBC	SHA-1*	128ビット 256ビット
PFSあり	DHE	CBC	SHA-256 SHA-384	128ビット 256ビット
PFSあり	DHE	CBC	SHA-1*	128ビット 256ビット

セキュリティ例外型優先軸				
【第二】PFS特性	鍵交換	【第一】暗号利用モード	ハッシュ関数	共通鍵暗号鍵長
PFSあり	ECDHE DHE	GCM CCM CCM_8	SHA-256 SHA-384	128ビット 256ビット
PFSなし	RSA DH ECDH	GCM CCM CCM_8	SHA-256 SHA-384	128ビット 256ビット
PFSあり	ECDHE DHE	CBC	SHA-256 SHA-384	128ビット 256ビット
PFSあり	ECDHE DHE	CBC	SHA-1	128ビット 256ビット
PFSなし	RSA DH ECDH	CBC	SHA-256 SHA-384	128ビット 256ビット
PFSなし	RSA DH ECDH	CBC	SHA-1	128ビット 256ビット

* 暗号スイートとしてのSHA-1はHMACの構成部品として利用されており、2020年時点においてもHMAC-SHA1の安全性について問題はない。しかしながら、実運用上は、HMACの構成部品であってもSHA-1の利用を避けるなどの世の中の動きもあり、今後の動向次第では推奨から外す可能性があることに留意されたい。

【参考】ガイドライン目次

【参考】ガイドライン目次

<table>
<tr><td colspan="2">7. TLSを安全に使うために考慮すべきこと</td></tr>
<tr><td colspan="2">7.1 最新セキュリティパッチの適用</td></tr>
<tr><td rowspan="6">7.2 サーバ証明書の作成・管理について注意すべきこと</td><td>7.2.1 サーバ証明書での脆弱な鍵ペアの使用の回避</td></tr>
<tr><td>7.2.2 サーバ証明書を発行・更新する際に新しい鍵情報を生成する重要性</td></tr>
<tr><td>7.2.3 サーバ証明書の更新忘れ防止に対する対策例</td></tr>
<tr><td>7.2.4 サーバで使用する鍵ペアの適切な管理</td></tr>
<tr><td>7.2.5 推奨されるサーバ証明書の種類</td></tr>
<tr><td>7.2.6 DNSのCAA設定による証明書不正発行の防止</td></tr>
<tr><td></td><td>7.2.7 複数サーバに同一のサーバ証明書（ワイルドカード証明書／マルチドメイン証明書）を利用する場合の注意点</td></tr>
<tr><td></td><td>7.2.8 プライベート認証局の利用の注意点</td></tr>
<tr><td colspan="2">7.3 委託先のサーバ（PaaS／SaaS）を利用する場合の注意点</td></tr>
<tr><td rowspan="3">7.4 さらに安全性を高めるために</td><td>7.4.1 HTTP Strict Transport Security（HSTS）の設定有効化</td></tr>
<tr><td>7.4.2 OCSP Staplingの設定有効化</td></tr>
<tr><td>7.4.3 Public Key Pinningのサポート終了について</td></tr>
</table>

<table>
<tr><td colspan="2">8. ブラウザを利用する際に注意すべきポイント</td></tr>
<tr><td colspan="2">8.1 本ガイドラインが対象とするブラウザ</td></tr>
<tr><td rowspan="2">8.2 設定に関する確認項目</td><td>8.2.1 基本原則</td></tr>
<tr><td>8.2.2 設定項目</td></tr>
<tr><td colspan="2">8.3 ブラウザ利用時の注意点</td></tr>
<tr><td colspan="2">9. その他のトピック</td></tr>
<tr><td colspan="2">9.1 リモートアクセスVPN over SSL（いわゆるSSL-VPN）</td></tr>
<tr><td colspan="2">コラム
① 常時HTTPS化に伴う留意点
② インターネット越しではないTLSの使い方—HTTPS in Local Network
③ サーバ証明書の自動発行・更新プロトコル
④ TLSではフィッシングが防げない？ーTLSで守られる限界を知ろう
⑤ サーバ証明書解析からフィッシングサイトを見つけ出せるか？</td></tr>
</table>

【参考】ガイドライン目次

Appendix	
A. チェックリスト	A.1. チェックリストの利用方法
	A.2. 推奨セキュリティ型のチェックリスト
	A.3. 高セキュリティ型のチェックリスト
	A.4. セキュリティ例外型のチェックリスト
B. サーバ設定編 ＊)「サーバ設定編」本体は、アップデートのうえ差し替え	
C. 暗号スイートの設定例 ＊)「暗号スイート設定編」本体は、アップデートのうえ差し替え	
D.ルートCA証明書の取り扱い	D.1.ルートCA証明書の暗号アルゴリズムおよび鍵長の確認方法
	D.2. Active Directoryを利用したプライベートルートCA証明書の自動更新
E：version 1.x/2.xとversion 3.xの大きな差分	

【参考】グループ優先順位ー高セキュリティ型推奨設定

	TLS1.2	TLS1.3
グループA	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	
	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	
	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	
	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	
	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8	
	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256
	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	
	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	
	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	
	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	TLS_AES_128_CCM_SHA256
	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8	TLS_AES_128_CCM_8_SHA256
グループB	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	
	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	
	TLS_DHE_RSA_WITH_AES_256_CCM	
	TLS_DHE_RSA_WITH_AES_256_CCM_8	
	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	
	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	
	TLS_DHE_RSA_WITH_AES_128_CCM	
	TLS_DHE_RSA_WITH_AES_128_CCM_8	

【参考】グループ優先順位ー推奨セキュリティ型推奨設定

	TLS1.2	TLS1.3
グループA	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	
	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	
	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	
	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	TLS_AES_128_CCM_SHA256
	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8	TLS_AES_128_CCM_8_SHA256
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	
	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	
	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	
	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	
	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8	
	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256
	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	
グループB	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	
	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	
	TLS_DHE_RSA_WITH_AES_128_CCM	
	TLS_DHE_RSA_WITH_AES_128_CCM_8	
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	
	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	
	TLS_DHE_RSA_WITH_AES_256_CCM	
	TLS_DHE_RSA_WITH_AES_256_CCM_8	
	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	

【参考】グループ優先順位ー推奨セキュリティ型推奨設定

	TLS1.2	TLS1.3
グループC	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	
グループD	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	
グループE	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	
グループF	TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	

【参考】グループ優先順位ーセキュリティ例外型推奨設定

	TLS1.2	TLS1.3
グループX	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	
	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	
	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	
	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	
	TLS_DHE_RSA_WITH_AES_128_CCM	TLS_AES_128_CCM_SHA256
	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	
	TLS_DHE_RSA_WITH_AES_128_CCM_8	TLS_AES_128_CCM_8_SHA256
	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8	
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	
	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	
	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	
	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	
	TLS_DHE_RSA_WITH_AES_256_CCM	
	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	
	TLS_DHE_RSA_WITH_AES_256_CCM_8	
	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8	
	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256
	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	
	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	

【参考】グループ優先順位ーセキュリティ例外型推奨設定

	TLS1.2	TLS1.3
グループY	TLS_RSA_WITH_AES_128_GCM_SHA256	
	TLS_DH_RSA_WITH_AES_128_GCM_SHA256	
	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	
	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	
	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256	
	TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256	
	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	
	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256	
	TLS_RSA_WITH_AES_128_CCM	
	TLS_RSA_WITH_AES_128_CCM_8	
	TLS_RSA_WITH_AES_256_GCM_SHA384	
	TLS_DH_RSA_WITH_AES_256_GCM_SHA384	
	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	
	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	
	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384	
	TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384	
	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	
	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384	
	TLS_RSA_WITH_AES_256_CCM	
	TLS_RSA_WITH_AES_256_CCM_8	

【参考】グループ優先順位ーセキュリティ例外型推奨設定

	TLS1.2	TLS1.3
グループZ	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	
	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	
	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	
	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	
	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	

【参考】グループ優先順位ーセキュリティ例外型推奨設定

グループZ（cont.）	TLS_RSA_WITH_AES_128_CBC_SHA256
	TLS_DH_RSA_WITH_AES_128_CBC_SHA256
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256
	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256
	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256
	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_DH_RSA_WITH_AES_128_CBC_SHA
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA
	TLS_RSA_WITH_AES_256_CBC_SHA256
	TLS_DH_RSA_WITH_AES_256_CBC_SHA256
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256
	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384
	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384
	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_DH_RSA_WITH_AES_256_CBC_SHA
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA

資料５

XTS の推奨候補暗号リストへの追加について

1. 暗号技術評価委員会の審議について

暗号技術評価委員会において、ディスク暗号化等で利用されている XTS の安全性（2018 年度）及び実装性能評価（2019 年度）が実施された。評価結果はそれぞれ下記の通りである。

- **安全性**

次の条件の下で、暗号利用モード(秘匿モード)として CRYPTREC 暗号リストに追加するための安全性要件を満たしていると判断した。

（条件 1）利用用途は NIST SP800-38E の規格に沿ったストレージデバイスの暗号化に限る。

（条件 2）XTS 内のブロック暗号には、CRYPTREC 暗号リスト掲載 128 ビットブロック暗号を使う。

- **実装性能**

暗号利用モード(秘匿モード)として、CRYPTREC 暗号リストに追加するための実装性能を有していると判断した。

以上から、2019 年度第 2 回暗号技術評価委員会において、XTS を次の通り CRYPTREC 暗号リストに追加することが望ましいという結論に至った。

- 推奨候補暗号リストの秘匿モード
- 注釈として、（条件１）、（条件２）を付与

2. 審議事項

暗号技術評価委員会からの提案通り、暗号利用モード XTS を CRYPTREC 暗号リストの中の "推奨候補暗号リスト" に追加することを審議いただきたい。

（推奨候補暗号リストへの追加のイメージ）

暗号利用モード	**秘匿モード**	**XTS(注*)**
	認証付き秘匿モード(注14)	**該当なし**

（注*）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、NIST SP800-38E の規格に沿ったストレージデバイスの暗号化に限る。

資料６

運用監視暗号リストからの削除ルール及び RC4 の取扱いについて

現在、暗号技術活用委員会の傘下で活動している TLS 暗号設定ガイドラインワーキンググループ（主査：須賀祐治、以下「WG」という。）において、TLS 暗号設定ガイドライン（以下「ガイドライン」という。）を作成している。

今回のガイドラインでは、セキュリティ例外型においても SSL3.0 を利用禁止にすることに伴い、RC4 についても利用禁止暗号アルゴリズムに位置付けるものとした。

このため、暗号技術活用委員会としては、RC4 を運用監視暗号リストに掲載しておく必要性がなくなったと判断し、同リストからの削除を提案する。併せて、運用監視暗号リストからの削除ルールの策定を提案する。

【背景】

RC4 は運用監視暗号リストに掲載されており、かつ（注 10）として「互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。SSL/TLS での利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。」と記載されている。

また、平成 15 年～平成 25 年に使われていた前の電子政府推奨暗号リストにおいても、「128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。」との注釈が付記されている。

このことから、RC4 が運用監視暗号リストに掲載されていた大きな理由は、「（CRYPTREC 暗号リスト作成当時）SSL/TLS において実際に利用されていた」ためであると理解すべきである。

したがって、今回のガイドラインにおいて RC4 が TLS での利用禁止暗号アルゴリズムに指定された以上、注釈が想定している例外的な利用形態そのものが存在しなくなると判断される。

【審議事項 1】　運用監視暗号リストからの削除ルール（案）

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

＜削除条件＞

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

【審議事項 2】　RC4 の運用監視暗号リストからの削除（案）

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

以上

資料７

暗号技術検討会
２０１９年度　報告書（案）

２０２０年６月

目次

１．はじめに

情報通信技術の急速な発展により、自動車、家電、医療、農業、工場など様々な分野で、あらゆるモノがネットワークに繋がる IoT 社会が到来し、サイバー空間と実空間の高度な融合により、多様なニーズにきめ細やかに対応したモノやサービスを提供できる社会への産業構造の変化が進みつつある。一方で、IoT 機器の普及に伴うサイバー攻撃の起点の増加や、サイバー攻撃自体の巧妙化・複雑化が続く中で、サイバー攻撃の影響が実空間にまで到達するリスクも増していくと考えられる。このような産業構造、社会の変化に伴うサイバー攻撃の脅威の増大に対応したセキュリティ確保が求められる中、暗号技術は既に様々な製品やサービスに組み込まれ、セキュリティを支える基盤技術として欠かせないものであるが、IoT 機器から得られる大量のデータの流通・連携を支える上でも、その重要性は一層増すと考えられる。

このような社会の変化に伴い、CRYPTREC においても、これまで取り組んできた暗号アルゴリズムのセキュリティ確保を引き続き推進することに加えて、暗号アルゴリズムを利用したプロトコルのセキュリティ確保のための活動拡大や、情報システム全体のセキュリティ確保に向けた暗号技術の利活用のための情報提供等の貢献が求められている。

2019 年度、CRYPTREC では、暗号技術検討会の下に「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」を新たに設置し、3 回の集中的な議論により、大規模な量子コンピュータの動向を踏まえた次期 CRYPTREC 暗号リストに求められる要件や、軽量暗号等の新たな暗号技術の動向等を踏まえた検討を行った。

2019 年度の各委員会の活動として、暗号技術評価委員会では、「現在の量子コンピュータによる暗号技術の安全性への影響に関する注意喚起レポート」の発行、新たに CRYPTREC 暗号リストに追加することとなった暗号利用モード XTS の評価等を行った。また、同委員会の下に設置された暗号技術調査 WG において、「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の更新方法の検討や量子コンピュータによる共通鍵暗号の安全性への影響についての検討を行った。暗号技術活用委員会では、安全な暗号利用に係る運用ガイドラインを整備する観点から「暗号鍵管理システム設計指針（基本編）」及び「TLS 暗号設定ガイドライン」の作成を行った。これらの 2019 年度の活動の詳細については、国立研究開発法人情報通信研究機構及び独立行政法人情報処理推進機構が取りまとめる「CRYPTREC Report 2019」を参照いただきたい。

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

今後も暗号技術を用いた情報システム及び情報社会全体のセキュリティ確保のために、成果物の検討や情報発信等を行っていく所存である。

末筆であるが、暗号技術検討会及び関係委員会等に御協力いただいた構成員、オブザーバの方々をはじめ、関係者の皆様に心から謝意を表する次第である。

2020 年 6 月

暗号技術検討会
座長　松本　勉

２．暗号技術検討会開催の背景及び開催状況

２．１．暗号技術検討会開催の背景

暗号技術は情報セキュリティの基盤技術であり、その安全性を暗号技術の専門家により技術的、専門的な見地から客観的に評価することが重要である。電子政府のセキュリティ確保のためには、安全性に優れた暗号技術を利用することが不可欠である。

このため、総務省及び経済産業省は、客観的な評価により安全性及び実装性に優れると判断される暗号技術をリスト化し、各府省に対してその利用を推奨することにより、高度な安全性と信頼性に支えられ、国民が安心して利用できる電子政府の構築に貢献することを目指し、2001 年 5 月に最初の暗号技術検討会を開催した。

暗号技術検討会において 2003 年 2 月に策定された電子政府推奨暗号リストは、2013 年 3 月に 10 年ぶりの改定が行われ、CRYPTREC 暗号リストとして発表されたが、その後においても、電子政府推奨暗号等の安全性を評価・監視し、暗号技術の更なる普及促進を行うため、総務省及び経済産業省は、継続的に暗号技術検討会を開催している。

２．２．CRYPTREC の体制

CRYPTREC とは、Cryptography Research and Evaluation Committees の略であり、総務省及び経済産業省が共同で開催する暗号技術検討会（座長：松本勉横浜国立大学教授）と、国立研究開発法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で開催する委員会から構成される暗号技術評価プロジェクトをいう。

2019 年度の CRYPTREC においては、大規模な量子コンピュータの動向を踏まえた次期 CRYPTREC 暗号リストに求められる要件や、軽量暗号等の新たな暗号技術の動向等を踏まえた検討を行うため、暗号技術検討会の下に、「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」（2019 年 7 月～）を設置し、議論を行った。

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

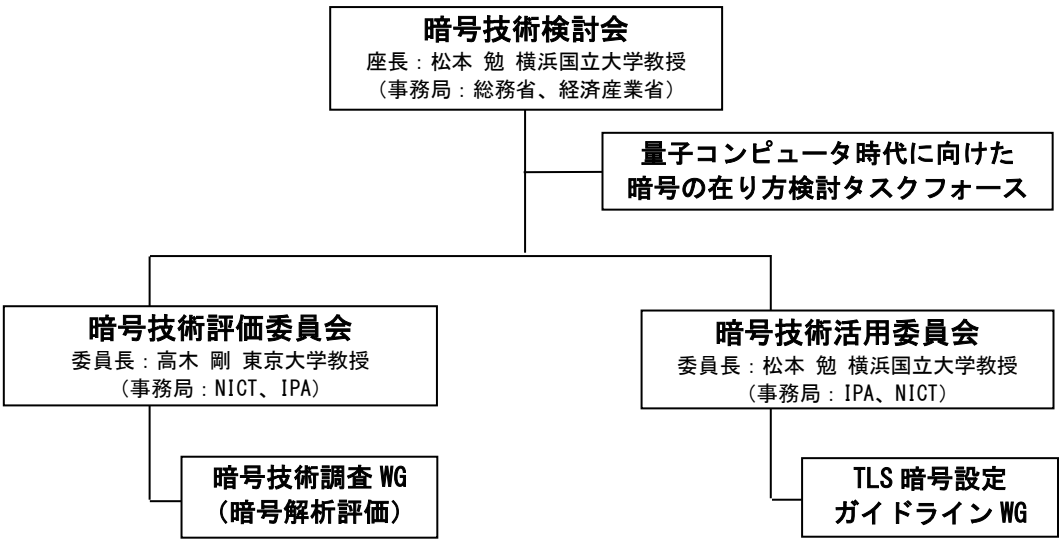


図 2.2.1　2019 年度 CRYPTREC 体制図

２．３．暗号技術検討会の開催実績

2019 年度の暗号技術検討会は、量子コンピュータ時代に向けた暗号の在り方検討タスクフォース、暗号技術評価委員会、暗号技術活用委員会の活動報告、運用監視暗号リストからの削除ルールに係る審議等を行うために 1 回開催した。なお、新型コロナウイルスの影響により当初予定の 3 月から 6 月に開催が延期されたため、形式上、2020 年度第 1 回暗号技術検討会の一部として開催された。

【第 1 回】2020 年 6 月 19 日（金）10:00～**:**（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
- 2019 年度暗号技術評価委員会 活動報告について
- 2019 年度暗号技術活用委員会 活動報告について
- XTS の推奨候補暗号リストへの追加について
- 運用監視暗号リストからの削除ルール及び RC4 の取扱いについて
- 暗号技術検討会　2019 年度　報告書（案）について

（概要）
- 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．設置の経緯

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

これらの議論を受けて、2018 年度第 1 回暗号技術検討会での審議の結果、暗号技術検討会の下に「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」（以下「検討 TF」という。）を設置し、次期 CRYPTREC 暗号リストに求められる要件や課題等を整理することとなった。

３．１．２．2019 年度の検討の内容

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

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

特に重点的に議論がなされた項目の内容は以下のとおり。

量子コンピュータの動向について

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

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

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

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

しかしながら、そもそも量子コンピュータの量子ビット数が数千程度以上ないと、ノイズ等に関わらず（ノイズ等がないとしても）暗号解読はできないと見込まれているため、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は妥当である。

CRYPTREC 暗号リストにおける耐量子計算機暗号の位置づけについて

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

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

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

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

CRYPTREC 暗号リストにおけるリスト構成について

CRYPTREC 暗号リストは、

①電子政府推奨暗号リスト[4]

---

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

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

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

②推奨候補暗号リスト[5]

③運用監視暗号リスト[6]

の３リスト構成となっている。

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

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

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

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

暗号技術のパラメータについて

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

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

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

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

---

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

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

[7] 2011 年度第 1 回暗号技術検討会資料 3-2

であることに留意が必要である。

３．１．３．検討結果概要

2019 年度、検討 TF における検討結果概要は以下のとおり。

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

３．１．４．2019 年度の開催状況

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

表 3.1　検討 TF の開催実績

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

３．２．暗号技術評価委員会

３．２．１．活動の概要

暗号技術評価委員会は、CRYPTREC 暗号リストに掲載されている暗号技術や電子政府システム等で利用される暗号技術の安全性維持及び信頼性確保のために安全性及び実装に係る監視及び評価を行う。主要な検討課題は以下のとおりである。

・暗号技術の安全性及び実装に係る監視及び評価
・暗号技術の電子政府推奨暗号リストからの降格
・暗号技術に関する注意喚起レポートの CRYPTREC ホームページへの公表
・新世代暗号に係る調査

これらの課題について 2019 年度に行った具体的な検討内容を、以下のとおり報告する。

３．２．２．暗号技術の安全性及び実装に係る監視及び評価

学会等での情報収集に基づく CRYPTREC暗号等の監視活動を行った。監視報告の詳細については、CRYPTREC Report 2019（暗号技術評価委員会報告）に掲載する。

３．２．３．暗号技術調査ワーキンググループ（暗号解析評価）

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

- 量子コンピュータによる共通鍵暗号の安全性への影響に関する調査及び評価
- 「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の在り方についての検討

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

３．２．３．１．量子コンピュータによる共通鍵暗号の安全性への影響に関する調査及び評価

背景及び実施内容

近年、量子コンピュータが実用化されても安全性を保てると期待される暗号（耐量子計算機暗号:PQC）の調査・検討が各国で進められている。特に米国では NIST が公開鍵暗号について PQC を公募し、現在では提案された暗号方式の安全性評価が進められている。

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

【件名】量子コンピュータによる共通鍵暗号の安全性への影響に関する調査及び評価

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

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

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

【依頼先】細山田 光倫 様 （NTT セキュアプラットフォーム研究所）

【2019 年度のスケジュール】

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

外部評価報告書に対する暗号解析評価 WG の見解

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

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

３．２．３．２.「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の在り方についての検討

「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図（以下単に「予測図」という。）は公開鍵暗号方式のセキュリティパラメータの選択について検討を行うため、2006 年度に設置された暗号技術調査 WG（公開鍵暗号）において作成された。当時、米国 NIST は「NIST SP 800-57 Part 1 (Revised)(May,2006)」[8]において暗号技術の鍵サイズに関して「80 ビットセキュリティの利用期限を 2010 年まで」と推奨していた。現在では「NIST SP 800-57 Part 1 (Revision 4)(January,2016)」において「112 ビットセキュリティの利用期限を 2030 年まで」と推奨している。これを踏まえ、以下について検討を行った。

(1) 今後の予測図の取り扱い

[8] 現在は、米国 NIST では「NIST SP 800-57 Part 1 (Revision 4)(January,2016)」において暗号技術の鍵サイズに関して「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。

(2) 今後の公開鍵暗号のパラメータ選択

今後の予測図の取り扱いについて

これまでの暗号の鍵長の推奨値は、いわゆるムーアの法則（集積回路上のトランジスタ数が 18 ヶ月毎に 2 倍になる）を主な根拠として設定されてきた。ところが、近年、計算機の性能向上は以前と比べて鈍化してきている。今後の予測図のあり方に対して、下記のとおり、対応方針を決定した。

対応方針

〈今後の予測図の取り扱い〉

(1) 予測図を従来通り、いわゆるムーアの法則を仮定して外挿線を今まで引いていた範囲（2040 年[9]）まで直線で引き、評価に大きな変動がないと考えられる限りにおいては、安全サイドに倒した評価として当面の間更新していくことを本 WG として提案する。なお、予測図は各国・国際標準化機関等により示されている主要な暗号技術の安全性基準と比較すると、より現状に則した評価であり、危殆化時期がそれらよりも先に延びるものとなっている。

〈今後の公開鍵暗号のパラメータ選択〉

(2) 公開鍵暗号のパラメータ選択に関する対応方針については、安全性以外にも相互接続性など、運用上の観点もあるため、今後は、暗号技術評価委員会だけではなく、暗号技術検討会、暗号技術活用委員会や関係各所などを含めて検討することを本 WG として提案する。

予測図の更新について

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

- 篩処理の評価を 2006 年度版に基づく評価から 2018 年版（表 3.2.1）に基づく評価[10]に変更した。

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

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

- 近年、ハードウェアを用いた新たな研究成果が無く、古い情報のみに依存した信頼性の低い評価となるため、「専用ハードウェアとソフトウェア処理との性能比較」に対応する外挿線は削除した。

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

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

- FactorWorld のサイト[11]がなくなったので、Integer Factoring Records のサイト[12]に変更した。
- 3072 ビット RSA と 256 ビット ECDLP に関する計算量を表す横線（点線）を入れた。なお、3072 ビット RSA に関する横線については他のビット長とは異なる評価方法であるため、より精度を高めるためにはさらなる検討が必要である。

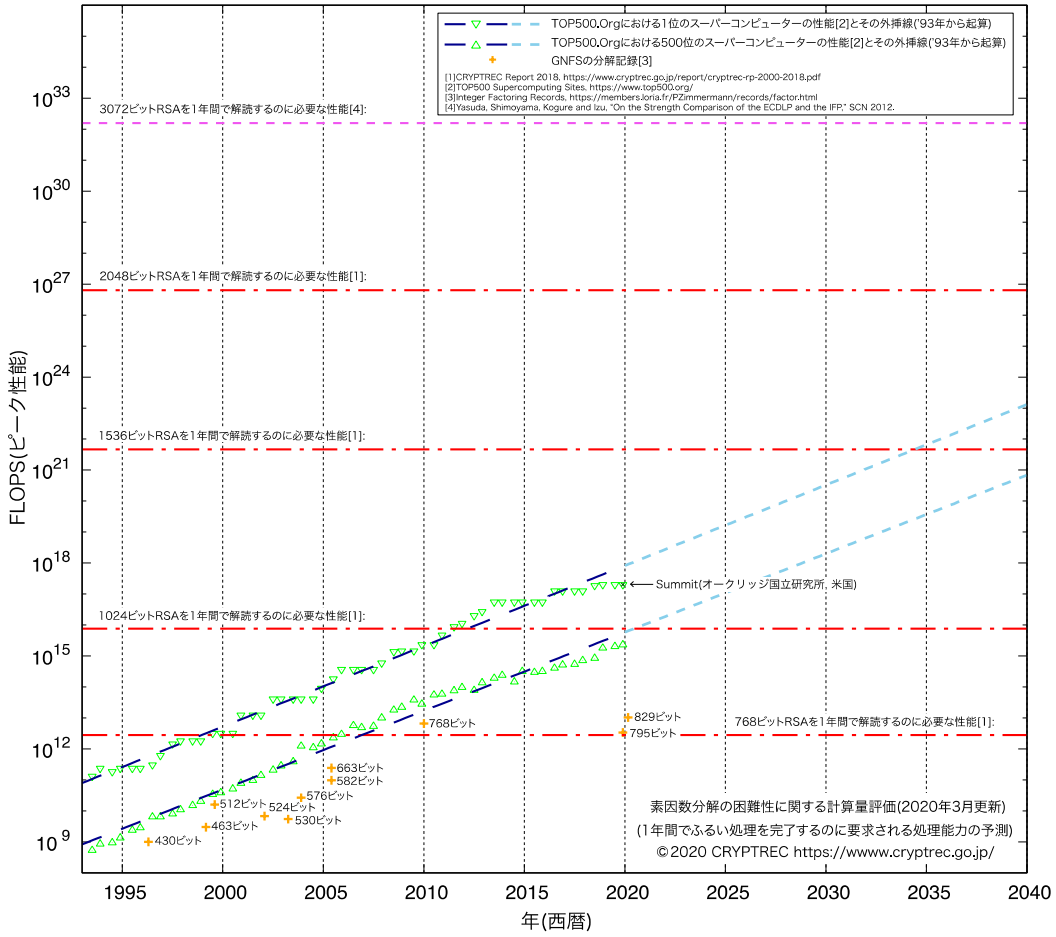


図 3.2.1：素因数分解の困難性に関する計算量評価
（1 年間でふるい処理を完了するのに要求される処理能力の予測、2020 年 3 月更新）[13]

[11] http://www.crypto-world.com/FactorWorld.html
[12] https://members.loria.fr/PZimmermann/records/factor.html
[13] スーパーコンピューターの性能の伸びに関する外挿線は僅かであるが鈍化してきている。

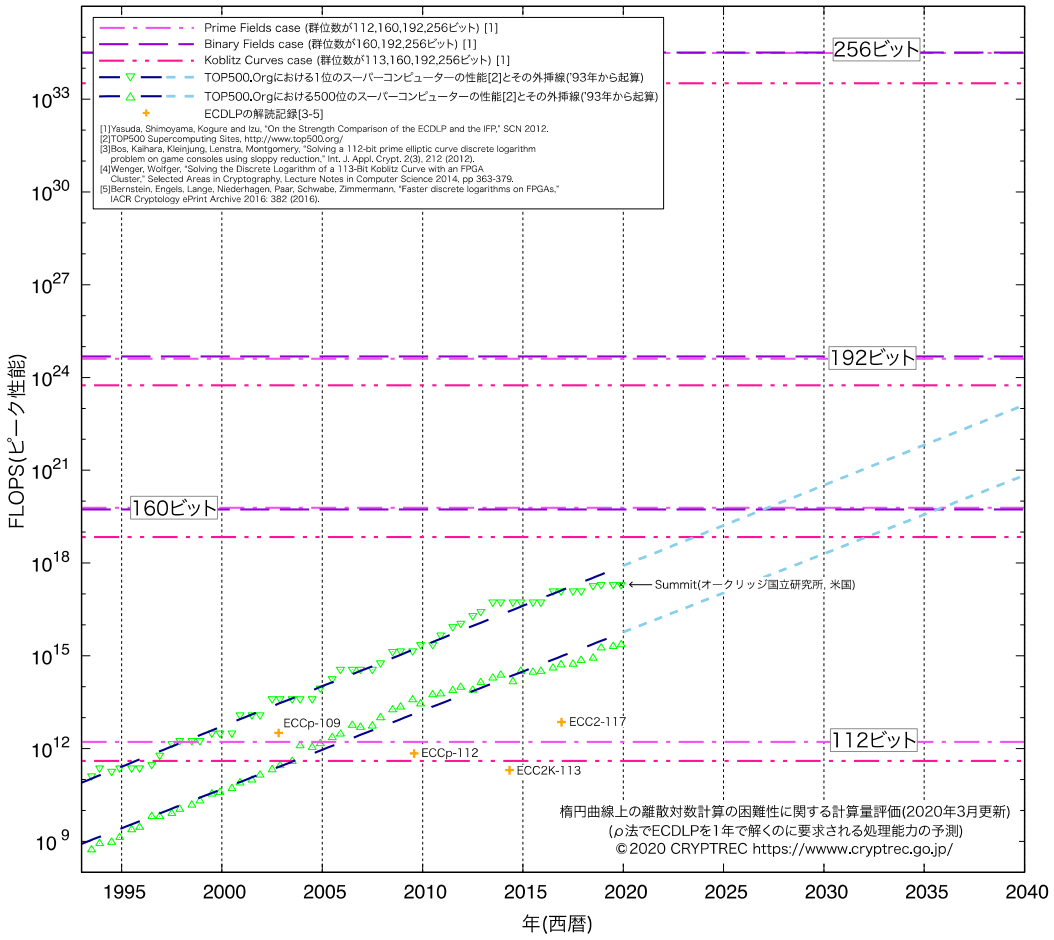


図 3.2.2：楕円曲線上の離散対数計算の困難性に関する計算量評価
（ρ 法で ECDLP を 1 年で解くのに要求される処理能力の予測、2020 年 3 月更新）[14]

３．２．４．推奨候補暗号リストへの新規暗号（事務局選出）の追加

暗号利用モード XTS の実装性能評価を行い、十分な実装性能があることを確認した。

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

> XTS モードは、下記 3 点の条件下では、暗号利用モード（秘匿モード）として CRYPTREC 暗号リストへ追加するための安全性要件を満たしている。
>
> (条件 1) 利用用途は IEEE および NIST SP-800-38E の規格に沿ったストレージやディスクの暗号化に限る。
>
> (条件 2) XTS 内のブロック暗号には、CRYPTREC 暗号リスト掲載の 128 ビットブロック暗号を使う。
>
> (条件 3) 同一の鍵を用いて暗号化する場合、220 ブロックまでとする。

今年度、第 2 回暗号技術評価委員会（2020 年 2 月 18 日開催）の審議により、(条件 3) は表現が不明瞭であり、また、意図した内容は、参照先仕様書にその制限事項の記載があることから、(条件

[14] 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。

1)に包含されるとの解釈の基、(条件 3)を安全性要件を満たす条件から削除することした。また、(条件 1)は、冗長性が高かったため、表現の改善を行った。

最終的に、安全性要件を満たす条件は下記の通りとなった。

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

以上の議論を踏まえ、2018 年度に実施した安全性評価および今年度実施した実装性能評価の結果に基づき、暗号利用モード XTS は、安全性要件を満たす条件の下で、暗号利用モード（秘匿モード）として十分な安全性及び実装性能を有していると判断した。上記判断に基づき、XTS 利用モードは CRYPTREC 暗号リストに掲載するために十分な安全性および実装性能を満たしていると判断し、CRYPTREC 暗号リストへの追加を暗号技術検討会に提言した。併せて、追加先としては、大分類「暗号利用モード」_中分類「秘匿モード」とすること、安全性要件を満たす条件を注釈につけることを提言した。

(仮)2019 年度暗号技術検討会（2020 年 6 月 19 日）の審議結果により、暗号技術評価委員会の提言が承認され、提言内容の通り XTS 利用モードは、CRYPTREC 暗号リストに追加されることとなった。

３．２．５．仕様書の参照先の変更

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

表 3.2.2：RSA 暗号の新旧仕様書

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

表 3.2.3：判定結果とその理由

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

３．２．６．暗号技術評価委員会の開催実績

2019 年度、暗号技術評価委員会は計 2 回開催した。各回会合の概要は表 3.2.1 のとおりである。

表 3.2.1　暗号技術評価委員会の開催状況

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

３．３．暗号技術活用委員会

３．３．１．活動の概要

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

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

３．３．２．2019 年度の活動内容

暗号鍵管理システム設計指針（基本編）の作成

あらゆる分野・あらゆる領域の全ての暗号鍵管理システム（以下「CKMS(Cryptographic Key Management System)」という。）を対象に、暗号鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として考慮すべき事項（Framework Requirements）を網羅的に提供し、設計時に考慮すべきトピックス及び設計書等に明示的に記載する要求事項を取りまとめた「暗号鍵管理システム設計指針（基本編)」を完成させた。

ダウンロード先　※後ほど追記

位置づけ

- 本設計指針は、セキュアな暗号アルゴリズムを利用する上で極めて重要な役割を果たす暗号鍵の管理に関する在り方を解説し、CKMS を設計・構築・運用する際に参考すべきドキュメントとして作成された。
  - 「暗号鍵管理の在り方」（暗号鍵管理の位置づけと検討すべき枠組み）では、暗号鍵管理の必要性を認識してもらうための解説を記載した。これは、あらゆる暗号鍵管理を検討する際の基礎となる考え方を示したものである。
  - 「暗号鍵管理についての技術的内容」では、包括的な CKMS 設計指針である NIST SP800-130「A Framework for Designing Cryptographic Key Management Systems」の解説書・利用手引書として活用できるように構成した。本設計指針では、SP800-130 での Framework Requirements を『暗号鍵管理における目的に応じた』対象範囲に分類・再構成することによってそれぞれの検討項目の目的や必要性を明確化した。
- 本設計指針は、あらゆるユースケースにおける暗号鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として考慮すべき事項一覧を提供し、CKMS 設計時に考慮すべきトピックス及び設計書等に明示的に記載する要求事項を示している。
- ただし、本設計指針の中ではセキュリティ要求事項は定義せず、具体的な特定のセキュリティ機能の採用を義務づけることもしない。それぞれの要求事項に対してどのように対応（例えば、ポリシー、暗号アルゴリズム、デバイス等の選択）するかは CKMS 設計者に委ねられ、それらの対応方針が設計仕様書や運用マニュアル等に記載される。

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

本設計指針の特長

本設計指針の最大の特長は、暗号鍵管理の考え方の枠組みを整理し、暗号鍵管理のための設計仕様書や運用マニュアルがどのように作られるべきかを明確にした点にある。大きくは 4 つの視点からなる。

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

TLS 暗号設定ガイドラインの作成

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

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

ダウンロード先　※後ほど追記

位置づけ

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

主な改訂内容

主な改訂内容は以下の通り。詳細については、本ガイドライン及び CRYPTREC Report 2019 暗号技術活用委員会報告を参照されたい。

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

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

B) 要求設定における「遵守項目」と「推奨項目」の区分けの新設

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

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

C) 章構成の変更

現行ガイドラインでは、

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

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

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

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

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

EdDSA に関する安全性評価の必要性についての検討

EdDSA は、TLS1.3 で採用された署名アルゴリズムである（RFC 8446）。さらに、TLS1.2 以前では、ECDSA と同じ暗号スイートを使って EdDSA も利用可能となった（RFC8422）。

暗号技術活用委員会では、今後 EdDSA の利用が進み、TLS 暗号設定ガイドラインに EdDSA を推奨暗号スイートに含めるか否かの判断が迫られた際に速やかに対応できるように準備をしておく観点から、EdDSA に対して CRYPTREC 暗号リストへの掲載是非に資するレベルでの安全性評価を実施することが必要であるとの結論を取りまとめた。併せて、EdDSA では利用する楕円曲線パラメータが Ed25519 と Ed448 であるため、楕円曲線パラメータについて、Ed25519 が P-256 と、Ed448 が P-384 と同程度の安全性を有する楕円曲線パラメータであるかどうか評価することの必要性も指摘した。

RC4 の運用監視暗号リストからの削除についての検討

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

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

【運用監視暗号リストからの削除ルール（案)】

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

＜削除条件＞

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

【RC4 の運用監視暗号リストからの削除（案)】

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

３．３．３．暗号技術活用委員会の開催状況

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

表 3.3.1　暗号技術活用委員会の開催状況

回	開催日	議案
2019 年度 第 1 回	2019 年 6 月 12 日	■ 活用委員会活動計画について ■ TLS 暗号設定ガイドライン WG 活動計画について ■ 暗号鍵管理システム設計指針（基本編）ドラフト版について
2020 年度 第 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

４．今後の CRYPTREC の活動について

CRYPTREC では、暗号アルゴリズムの安全性確保やその利活用に係る議論のみならず、鍵管理の安全な運用に向けた取組など、暗号をとりまく環境変化に応じた新たなニーズへの対応などに取り組むこととしている。

量子コンピュータ時代に向けた暗号の在り方検討タスクフォースにおいては、引き続き、量子コンピュータや耐量子計算機暗号の状況を注視しつつ、CRYPTREC 暗号リストの次回改定に向け継続検討とした内容の議論を行う。暗号技術評価委員会においては、引き続き、暗号技術の安全性に係る監視・評価及び実装に係る技術の監視・評価を行うとともに、暗号技術の安全な利用方法に関する調査を行う。暗号技術活用委員会においては、「暗号鍵管理システム設計指針（基本編）」及び「TLS 暗号設定ガイドライン」の公開を行うとともに、新たな運用ガイドラインの作成に向けた検討を行う。なお、両委員会の範囲を超えるものについては、必要に応じて、暗号技術検討会で審議・判断する。

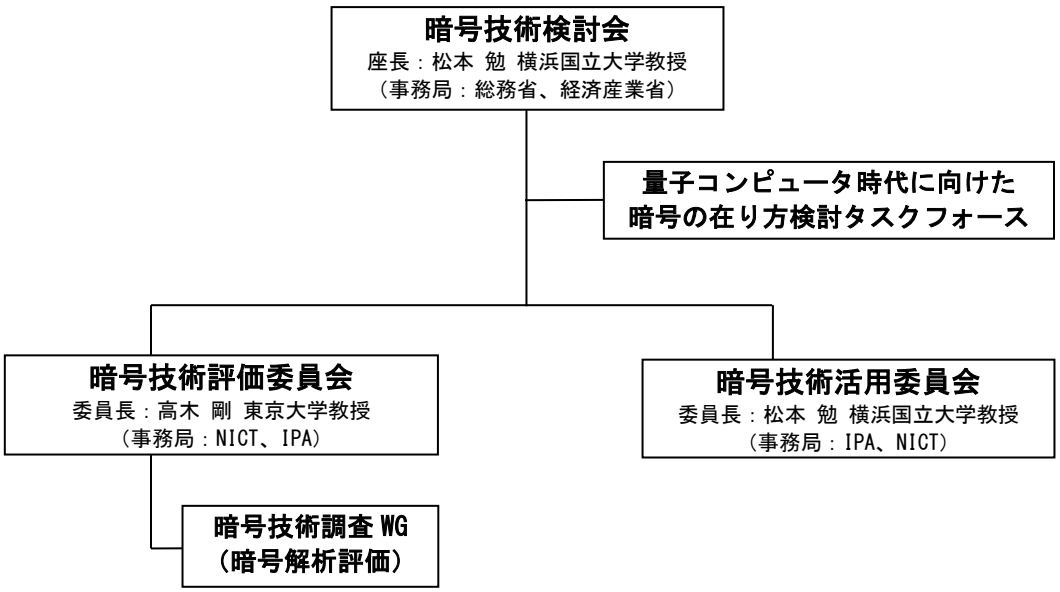


図 4.1.1 2020 年度 CRYPTREC の体制図（予定）

資料８

2020 年度暗号技術評価委員会活動計画(案)

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。

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。

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。

(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。

3. 活動スケジュール

暗号技術評価委員会は、2 回の開催を予定する。

回	開催日	議案
第 1 回	2020 年 7 月中旬	● 暗号技術評価委員会活動計画の具体的な進め方についての審議 ● 暗号技術調査ワーキンググループ(暗号解析評価)の活動計画案の審議
第 2 回	2021 月 2 月下旬～3 月上旬	● 暗号技術評価委員会活動報告(案)についての審議 ● EdDSA の安全性評価結果の報告と審議 ● 暗号技術調査ワーキンググループ(暗号解析評価)の活動内容の報告と審議

以上

（参考）

委員構成

暗号技術評価委員会委員名簿

委員長	高木　剛	東京大学　教授
委員	岩田　哲	名古屋大学　准教授
委員	上原　哲太郎	立命館大学 教授
委員	大東　俊博	東海大学　准教授
委員	國廣　昇	筑波大学　教授
委員	四方　順司	横浜国立大学　教授
委員	手塚　悟	慶應義塾大学　教授
委員	藤崎　英一郎	北陸先端科学技術大学院大学　教授
委員	本間　尚文	東北大学　教授
委員	松本　勉	横浜国立大学　教授
委員	松本　泰	セコム株式会社　ディビジョンマネージャー
委員	盛合　志帆	国立研究開発法人情報通信研究機構　上席研究員
委員	山村　明弘	秋田大学　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研究センター　副研究センター長

［暗号技術調査ワーキンググループ(暗号解析評価)］

主査	國廣　昇	筑波大学　教授
委員	青木 和麻呂	文教大学　准教授
委員	草川　恵太	日本電信電話株式会社　主任研究員
委員	桑門　秀典	関西大学　教授
委員	下山　武司	国立情報学研究所 特任研究員
委員	高木　剛	東京大学　教授
委員	高島　克幸	三菱電機株式会社　主管技師長
委員	峯松　一彦	日本電気株式会社　主管研究員
委員	安田　貴徳	岡山理科大学　准教授
委員	安田　雅哉	立教大学　准教授

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

2020.6.19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大学院　情報理工学研究科　教授
高木　　剛	国立大学法人東京大学大学院　情報理工学研究科　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	慶應義塾大学大学院　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　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

一ノ瀬宏昭	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）
三原　祥二	個人情報保護委員会事務局　参事官
吉田　和彦	警察庁　情報通信局　情報管理課　情報セキュリティ対策官
小高　久義	総務省　行政管理局　行政情報システム企画課　情報システム管理室長
阿部　知明	総務省　自治行政局　住民制度課長
宮崎　拓也	法務省　民事局　商事課長
髙橋　良明	外務省　大臣官房　情報通信課長
下井　善博	財務省　大臣官房　文書課　業務企画室長
竹田　和彦	文部科学省　大臣官房　政策課　情報システム企画室長
原口　剛	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）
中野　宏和	経済産業省　産業技術環境局　国際電気標準課長
大橋　洋一	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
久保田　実	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
寶木　和夫	国立研究開発法人産業技術総合研究所 情報技術研究部門 副研究部門長
瓜生　和久	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
大澤　昭彦	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
和田　雅昭	公益財団法人金融情報システムセンター　監査安全部長

（敬称略）

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

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] 総務省政策統括官（情報セキュリティ担当）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。
http://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	該当なし
	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。

[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。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成25年 3 月 1 日 現在）

（注9） SSL 3.0 / 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。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。

（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	[削除]

		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。	
	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）		