資料１

2021年度 第１回 暗号技術検討会

令 和 ４ 年 ３ 月 ３ ０ 日
１ ４ ： ０ ０ ～
オ ン ラ イ ン 開 催

議 事 次 第

１．開会

２．議事
(1) 暗号技術検討会　開催要綱の改定について【報告】
(2) 2021年度暗号技術評価委員会 活動報告について【報告】
(3) 2021年度暗号技術活用委員会 活動報告について【報告】
(4) 利用実績による選定基準について【承認】
(5) 暗号強度要件に関する設定基準について【承認】
(6) 暗号鍵設定ガイダンスについて【承認】
(7) CRYPTREC暗号リストの改定について【承認】
(8) 暗号技術検討会 2021年度 報告書（案）について【承認】
(9) その他

３．閉会

配付資料一覧

資料１	議事次第・配付資料一覧
資料２	暗号技術検討会 開催要綱（構成員・オブザーバ名簿）
資料３－１	2021年度 暗号技術評価委員会 活動報告
資料３－２	監視状況報告
資料３－３	ディジタル署名EdDSAの評価結果について
資料３－４	2021年度暗号技術調査WG（耐量子計算機暗号）活動報告
資料３－５	2021年度暗号技術調査WG（高機能暗号）活動報告
資料３－６	軽量暗号に関する技術動向調査について
資料３－７	軽量暗号ガイドライン更新方針
資料４	2021年度 暗号技術活用委員会 活動報告
資料５	利用実績による選定基準（案）
資料６－１	暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準概要
資料６－２	暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準
資料７－１	暗号鍵設定ガイダンス概要
資料７－２	暗号鍵設定ガイダンスについて
資料８－１	CRYPTREC暗号リストの改定について
資料８－２	ディジタル署名EdDSAの推奨候補暗号リストへの追加について
資料８－３	CRYPTREC暗号リスト改訂案
資料８－４	CRYPTREC暗号リスト（現行）
資料９	暗号技術検討会 2021年度 報告書（案）

以上

資料２

「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、デジタル庁統括官、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、デジタル庁、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、デジタル庁デジタル社会共通機能グループ、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４年３月３０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

2022.3.30現在

構成員

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

（五十音順、敬称略）

オブザーバ

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

別紙２

暗号技術検討会の公開について

１　会議の公開について

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

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

２　検討会の資料の公開について

（１）検討会の資料については、原則公開とする。

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

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

３　議事概要の公開について

（１）議事概要については、原則公開とする。

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

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

資料３－１

2021 年度暗号技術評価委員会活動報告

1. 活動目的

CRYPTREC 暗号リストに掲載されている暗号技術や電子政府システム等で利用される暗号技術の安全性維持及び信頼性確保のために安全性及び実装に係る監視及び評価を行う。

2. 活動概要

(1) 暗号技術の安全性及び実装に係る監視及び評価

下記の通り、暗号技術の安全性に係る監視・評価 及び 実装に係る技術の監視・評価を実施した。

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 を通して報告することとした。

- 今年度時点では、電子政府推奨暗号リストの安全性に懸念を持たせるような事態は生じていない。今年度実施の監視報告の詳細については、CRYPTREC Report 2021 で報告。

（資料３－２参照）

② 電子政府推奨暗号リストからの運用監視暗号リストへの降格、並びに、推奨候補暗号リスト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こととした。

- そのような降格や削除が必要となる暗号技術は無かった。

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べく活動することとした。

- 注意喚起レポートの発行を要する事案は発生しなかった。

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こととした。

- 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 の実装性能評価を行うこととした。
  - ディジタル署名 EdDSA の実装性能評価を実施。実装性能に関して外部評価を実施し、評価レポートを踏まえ、暗号技術評価委員会としての見解をまとめた。昨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、EdDSA が十分な安全性および実装性能を有していると判断し、暗号技術検討会に「推奨候補暗号リスト(技術分類：「大分類：公開鍵暗号」、「中分類：署名」)」への追加を提案。
    （資料３－３参照）

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・性能評価を行った。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こととした。

- 耐量子計算機暗号に関するガイドラインを作成するため、耐量子計算機暗号に関するワーキンググループを設置した。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」の予測図の更新についても耐量子計算機暗号に関するワーキンググループで検討し、更新を行うこととした。
  - 暗号技術調査ワーキンググループ（耐量子計算機暗号）を開催し、ガイドライン及び、その根拠資料となる調査報告書の作成に関する方針（スケジュール、章立て、執筆担当者、執筆要項）をまとめ、ガイドラインの目次案を決定した。これらに基づき、2022 年度からガイドライン及び調査報告書の執筆を開始する。また、2020 年度に決定した「今後の予測図の取り扱い」に基づき、「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の更新を行った。
    （資料３－４参照）
- 高機能暗号に関するガイドラインを作成するため、高機能暗号に関するワーキンググループを設置することとした。
  - 暗号技術調査ワーキンググループ(高機能暗号)を開催し、ガイドラインで扱う「高機能暗号の定義」を行うとともに、「高機能暗号の分類」「ガイドラインに

記載する高機能暗号の種類」をまとめ、ガイドラインの目次案を決定した。これらに基づき、2022 年度からガイドラインの執筆を開始する。さらに、ガイドライン作成に向けて、個々の高機能暗号について、技術動向、応用事例、標準化動向の調査を 2022 年度に実施し、その結果をガイドラインに反映する。
（資料３－５参照）

- 2016 年度に作成した「CRYPTREC 暗号技術ガイドライン(軽量暗号)」の更新のため、掲載されている暗号方式に関わる安全性解析について、2017 年度以降の技術動向調査を行うこととした。
  - 現ガイドラインに掲載されている暗号方式の安全性について、2017 年度以降の技術動向調査を行い、報告書にまとめた。報告書は、CRYPTREC 技術報告書として公開予定。
    （資料３－６参照）
  - 現ガイドラインに新規情報を追加更新したものを 2023 年度ガイドラインとすることを更新方針とした。追加情報の対象は「NIST Lightweight コンペティション最終選考で採択された方式」及び「軽量な方式として ISO に近年採録されたもしくは採録される予定の方式」とした。
    （資料３－７参照）

(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・評価を行うこととした。

- (1)⑤による活動報告を参照。

3. 開催状況

表１ 暗号技術評価委員会の開催状況

回	開催日	議案
第 1 回	2021 年 7 月 6 日	● 暗号技術評価委員会活動計画の具体的な進め方についての審議 ● 暗号技術調査ワーキンググループの活動計画案の審議 ● 軽量暗号ガイドラインの更新についての審議 ● EdDSA の実装性能評価実施についての審議
第 2 回	2022 月 2 月 22 日	● EdDSA の実装性能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の活動内容の報告と審議 ● 軽量暗号に関する技術動向調査報告及び軽量暗号ガイドラインの更新の方針に関する審議

以上

暗号技術評価委員会委員名簿

（五十音順、敬称略）

委員長	高木　剛	東京大学　教授
委員	青木 和麻呂	文教大学　准教授
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	花岡　悟一郎	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　首席研究員
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	山村　明弘	秋田大学　教授

資料３－２

監視状況報告

1. 監視活動報告

2021 年度第 1 回暗号技術評価委員会（2021 年 7 月 6 日）から 2021 年度第 2 回暗号技術評価委員会（2021 年 2 月 22 日）までに、表 1 に示す国際会議に参加するとともに各種調査を行い、暗号解読技術等に関する研究動向を収集した。

表 1 国際会議への参加状況

学会名・会議名		開催国・都市	期間
PQCrypto 2021	The 12th International Conference on Post-Quantum Cryptography	(Virtual Conference)	2021 年 7 月 20 日～7 月 22 日
Crypto 2021	The 41st Annual International Cryptology Conference	(Virtual Conference)	2021 年 8 月 16 日～8 月 20 日
Eurocrypt 2021	The 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques	(Virtual Conference)	2021 年 10 月 17 日～10 月 21 日
TCC 2021	The Theory of Cryptography 19th International Conference	(Virtual Conference)	2021 年 11 月 8 日～11 月 11 日
Asiacrypt 2021	The 27th Annual International Conference on the Theory and Application of Cryptology and Information Security	(Virtual Conference)	2021 年 12 月 6 日～12 月 10 日

2. 解読技術等の動向

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

2.1. CRYPTREC 暗号リスト記載の暗号に直接関わる解読技術動向

CRYPTREC 暗号リスト（電子政府推奨暗号リスト）掲載の暗号に関して報告する。

AES については、2 本の暗号解析論文が見られた。まず、AES 鍵スケジュールに対する新しい表現と、それを活用した AES-128 に対する不可能差分攻撃（impossible-differential attacks）の改善が Eurocrypt 2021 で報告された。この結果は Mala 氏らが INDOCRYPT 2010 で報告して以来の改善である。本論文は Eurocrypt 2021 にて Best paper award を受賞している。また同じく Eurocrypt 2021 にて、AES-128 ハッシ

ュモードの 8 ラウンドに対する最初の攻撃が得られている。RSA については、部分的に秘密鍵がわかっている場合の素因数分解アルゴリズム（Partial Key Exposure Attack）として、新規のものが Asiacrypt 2021 によって提案された。SHA については、量子計算を用いた SHA-256 と SHA-512 に対する衝突攻撃が、CRYPTO 2021 にて提案された。

いずれも、未だ現実への脅威となるには至っていないが、今後動向を注視すべきである。

2.1.1. 共通鍵暗号に関する解読技術

・New Representations of the AES Key Schedule [Eurocrypt 2021, Awarded paper]

Gaëtan Leurent, Clara Pernot

本論文では、AES 鍵スケジュールの新しい表現と、AES ベースのスキームの安全性へのいくつかの示唆が提示される。特に、AES-128 鍵スケジュールは、32 ビットのチャンクで動作する 4 つの独立した並列計算に分割でき、線形変換まで可能であることが示される。この性質は 20 年以上にわたる AES の解析の結果、文献に記載されていなかった。さらに、この新しい表現が、AES ベースのスキームのこれまでの暗号解読結果を改善することを示す、2 つの結果が示される。まず著者らは、奇数回の鍵スケジュールラウンドを繰り返すと、短いサイクルを持つ関数が生成されることを確認した。これは、NIST Lightweight Cryptography コンペティションの第 2 ラウンド候補である mixFeed における Khairallah の観測を説明する。著者らの解析によれば、Khairallah の mixFeed に対する偽造攻撃が 0.44 の確率で成功し（データ量は 220GB）、実際にこの方式が破られることがわかった。また、同じ観測から、同じく AES ベースの AEAD 方式である ALE に対する新たな攻撃も発見された。また、著者らの新しい表現により、最初のサブキーの情報と最後のサブキーの情報を組み合わせて、対応するマスターキーを再構成する効率的な方法が示されている。特に、AES-128 に対する従来の不可能差分攻撃（impossible-differential attacks）を改善することができる。

・Automatic Search of Meet-in-the-Middle Preimage Attacks on AES-like Hashing [Eurocrypt 2021]

Zhenzhen Bao, Xiaoyang Dong, Jian Guo, Zheng Li, Danping Shi, Siwei Sun, Xiaoyun Wang

中間一致原像攻撃（MITM 原像攻撃）は、フル MD5、HAVAL、Tiger、縮小 SHA-0/1/2 など、多くのハッシュ関数の原像攻撃の耐性を破るのに極めて有効である。また、2011 年に Sasaki によって、AES のようなブロック暗号上に構築されたハッシュ関数に対する脅威であることが示された。近年、AES のハッシュモードに対するこうした攻撃は、単に内部状態の選択の自由度を利用したものから、メッセージの状態の選択の自由度も利用した

ものに発展している。しかし、このような攻撃、特に進化した亜種を検知することは困難である。従来の研究では、このような攻撃の構成の探索空間は限られており、手作業による解析が現実的であるため、最適な解が得られないという問題があった。

本論文では、先行研究における人為的な制限を取り除き、攻撃の構成に関する本質的なアイデアを明確に定式化し、最適な攻撃を探索する問題を混合整数-線形プログラミング（MILP）モデルにおける制約条件の下で最適化問題に変換する。このような MILP モデルを用い、市販のソルバーを用いることで、最適な攻撃を網羅的に探索することができる。その結果、Haraka-512 v2 の完全版（5 ラウンド）と拡張版（5.5 ラウンド）、および AES-128 ハッシュモードの 8 ラウンドに対する最初の攻撃、さらに Haraka-256 v2 および AES と Rijndael ハッシュモードの他のメンバーに対する改良版攻撃が得られた。

2.1.2. 公開鍵暗号に関する解読技術

・Partial Key Exposure Attack on Short Secret Exponent CRT-RSA [Asiacrypt 2021]

Alexander May, Julian Nowakowski, Santanu Sarkar

(N,e) を RSA 公開鍵とし、 N=pq をビットサイズの等しい素数 p,q の積とする。d_p, d_q は対応する秘密の CRT-RSA 指数とする。Coppersmith 型攻撃により、Takayasu, Lu and Peng（TLP）は最近、$d_p, d_q \leq N^{0.122}$ であれば、多項式時間で N の因数分解を得ることができることを示した。

本論文では、TLP 攻撃に基づいて、短い秘密指数を持つ CRT-RSA に対する最初の Partial Key Exposure 攻撃が示される。すなわち、$N^{0.122} \leq d_p, d_q \leq N^{0.5}$ のとき、d_p, d_q の両方の最下位ビット（LSB）の既知の分数で、多項式時間で N を因数分解するのに十分であることを示す。当然ながら、d_p, d_q が大きくなればなるほど、より多くの LSB が必要となる。例えば、d_p, d_q が $N^{0.13}$ のサイズであればその LSB の約 1/5、$N^{0.2}$ のサイズならその LSB の約 2/3、d_p, d_q がフルサイズ $N^{0.5}$ であればその LSB の全てを知る必要がある。この結果の副産物として、入力 (N, e, d_p, d_q) に対するヒューリスティックな決定論的多項式時間因数分解アルゴリズムが得られることに注目する。

2.1.3. ハッシュ関数に関する解読技術

・Quantum Collision Attacks on Reduced SHA-256 and SHA-512 [CRYPTO 2021]

Akinori Hosoyamada, Yu Sasaki

本論文では、SHA-256 と SHA-512 に対する専用の量子衝突攻撃法が初めて示される。

この攻撃はそれぞれ 38 ステップと 39 ステップに達し、古典的な 31 ステップと 27 ステップの攻撃を大幅に改善することができた。両攻撃とも、多数の semi-free-start

衝突を 2-ブロック衝突に変換する先行研究の枠組みを採用し、計算時間と計算空間の間のトレードオフのコスト指標において汎用攻撃より高速であることが確認された。必要な semi-free-start 衝突の数は、量子設定において削減できることが観測されており、これにより、従来の古典的な 38 ステップ、39 ステップの semi-free-start 衝突を一つの衝突に変換することが可能である。著者らは、攻撃の背後にある考え方は単純であり、他の暗号ハッシュ関数にも適用可能であると報告している。

2.2. その他の注視すべき技術動向

対称鍵暗号については、主に差分攻撃、線形攻撃、中間一致攻撃、キューブ攻撃に関する報告が大半を占める一方、機械学習や量子計算機による解読に関する論文も見られた。また公開鍵暗号については、解読報告のほとんどが耐量子暗号、特に NIST PQC Standardization と関わりのある格子ベースの暗号と超特異楕円曲線の同種を用いた暗号についてのものであった。署名に関しても同様の傾向が見られ、Picnic や Rainbow といった NIST PQC Standardization における候補に対する解読論文が見られた。また、暗号の安全性の根拠となる問題の研究についても、LWE（Learning with Errors）問題や SVP（Shortest Vector Problem）といった、耐量子暗号と関わりのある論文が大部を占めている。

より詳しくは、§2.1 で報告した論文以外にも、使用される機会が多い、もしくは今後多くなると予想される暗号に関する解析報告として、次の論文が発表された。

2.2.1. 対称鍵暗号に関する解読技術

・Linear Cryptanalysis of FF3-1 and FEA [CRYPTO 2021]

Tim Beyne

本論文は、ラウンド微調整を交互に行う汎用小領域 Feistel 暗号（generic small-domain Feistel cipher）に対する改良された攻撃を、線形暗号解析を用いて得ている。この結果、米国の形式保存暗号規格 FF3-1、韓国の規格 FEA-1、FEA-2 に対する実用的な識別攻撃とメッセージ回復攻撃を実現した。提案する FF3-1、FEA-1 に対する攻撃のデータ量は $O(N^{r/2-1.5})$である；ここで N^2 はドメインサイズ、r はラウンド数である。例えば、$N = 10^3$ の FF3-1 は、2^{23} の暗号化クエリを用いて、1/10 以上の成功率(advantage)で理想的な調整値付き（tweakable）ブロック暗号と区別することが可能である。同様の利点を持つメッセージの左半分を復元するためには、2^{24} 個のデータが必要である。FF3-1 の解析は、群$\mathbb{Z}/N\mathbb{Z}$上の（一般化）線形暗号解読の興味深い実世界への応用として役立っている。

・Differential-Linear Cryptanalysis from an Algebraic Perspective [CRYPTO 2021]

Meicheng Liu, Xiaojuan Lu, Dongdai Lin

差分-線形暗号解析（differential-linear cryptanalysis）は、暗号技術における重要な暗号解析手段であり、1994 年に Langford と Hellman によって発見されて以来、盛んに研究されている。それにもかかわらず、差分トレイルと線形トレイルが接続する中間部分を研究する方法は非常に少ない。

本論文では、代数学的な観点から差分-線形暗号解析を研究する。まず、差分-線形暗号解析のための DATF（Differential Algebraic Transitional Form）という技術を紹介し、次に差分-線形バイアスの推定に関する新しい理論と差分-線形暗号解析における鍵回復のための技術を開発する。

CAESAR と LWC の最終候補である ASCON、AES の最終候補である Serpent、eSTREAM の最終候補である Grain v1 に対して本技術を適用し、ASCON と Serpent に対する差分-線形近似のバイアスを推定した。バイアスの理論的な推定値は、差分-線形接続表（Differential-Linear Connectivity Table）（Bar-On et al., EUROCRYPT 2019）で得られる値よりも正確であり、ラウンド数が多くても適用可能な技術であることがわかる。著者らの一般的な技術は、差分-暗号解析における Grain v1 のバイアスを推定するためにも使用でき、暗号に合わせた Differential Engine ツールよりも明らかに優れた性能を持つ。次に、これらの暗号のラウンド数を削減した亜種に対する改良型鍵回復攻撃法も提案される。これらは、Serpent の暗号解析として、また、ASCON の差分線形暗号解析、Grain v1 の初期化解析として、現時点で最もよく知られているものである。特に、Serpent の安全性解析は、過去 20 年間における差分線形暗号解析の最も重要な応用例の 1 つである。本論文の結果は、2003 年の Biham, Dunkelman and Keller の研究の後、Serpent-128 と Serpent-256 の差分-線形暗号解読を 1 ラウンド増やして更新している。

・Cryptanalysis of Full LowMC and LowMC-M with Algebraic Techniques [CRYPTO 2021]

Fukang Liu, Takanori Isobe, Willi Meier

本論文では、LowMC の差分列挙（difference enumeration）の技術を再検討し、新しい代数的技術を開発して、無視できるほどのメモリ計算量で効率的な鍵回復攻撃を実現する。本技術により、ブロックサイズが鍵サイズよりはるかに大きい場合、LowMC に対する攻撃を大幅に改善し、そのようなパラメータで LowMC を破ることさえ可能となった。さらに新しい鍵回収技術により、ToSC 2018 で Rechberger らが興味深い質問として述べていた、入力と出力メッセージの単一のペアとそれらが取る差分トレイルのみが与えられた場合の、完全な鍵を回収する時間を大幅に改善に成功した。両方の技術を組み合わせることで、2 つの選ばれた平文のみで、ブロックサイズ 129、192、255 ビットのフル S-Box 層を採用した LowMC の 4 ラウンドがそれぞれ破られた。この 3 パラメータは、NIST のポスト量子暗号コンテストにおける代替第 3 ラウンド候補である Picnic3 の推奨 3 パラメータである。Picnic のユースケースは非常に異なっており、攻撃者は具体的な LowMC インスタンスに

対して暗号化する 2 つの平文を自由に選択することもできないため、著者らの攻撃は Picnic3 が壊れていることを示すものではない。しかし最新の LowMC では、このようなパラメータは安全であるとみなされていた。また、Peyrin と Wang が CRYPTO2020 で提案したバックドア暗号 LowMC-M の 7 インスタンスのうち、許可された 2^{64} データをフル活用することでバックドアを見つけることなくはるかに多くのラウンドを解読することが可能である。上記の攻撃は、いずれも無視可能なメモリ量で実現された。

・Improved Linear Approximations to ARX Ciphers and Attacks Against ChaCha [Eurocrypt 2021]

Murilo Coutinho Silva, Tertuliano C. de Souza Neto

本論文では、ARX 暗号においてより良い線形近似を求めるために用いることができる新しい技術が紹介される。この技術を用いることで、ChaCha の 3 ラウンドと 4 ラウンドに対して初めて明示的に導き出された線形近似を提示し、その結果として、ChaCha に対する最近の攻撃を改善することが可能となった。さらに、ChaCha の 3 ラウンドと 3.5 ラウンドに対する新しい差分を提示し、提案手法と組み合わせることで、ChaCha に対する差分線形攻撃の計算量をさらに向上させることに成功している。

・Rotational Cryptanalysis From a Differential-Linear Perspective - Practical Distinguishers for Round-reduced FRIET, Xoodoo, and Alzette [Eurocrypt 2021]

Yunwen Liu, Siwei Sun, Chao Li

差分線形識別器の偏りを評価する厳密な公式（JoC2017）から、差分部分と線形部分の切り替えの依存性を扱う差分線形接続表（DLCT）技術（EUROCRYPT2019）、そして ARX プリミティブの暗号解読の文脈での改良（CRYPTO2020）まで、この 4 年間で差分線形攻撃は大きな発展を見せている。本論文では、攻撃の差分部分を回転型 xor（rotational-xor）差分に置き換えることで、この枠組みをさらに拡張している。さらに、FRIET、Xoodoo、Alzette、SipHash に含まれる並べ換えに対して著者らの技術を適用した。これにより、既存の暗号解析結果を大幅に改善することができ、また、理論的根拠のない従来の実験的識別器の説明を行うことができる。本解析の妥当性を確認するため、実用的な計算量を持つすべての識別器の実験的検証も行われている。

・Meet-in-the-Middle Attacks Revisited: Key-recovery, Collision, and Preimage Attacks [CRYPTO 2021]

Xiaoyang Dong, Jialiang Hua, Siwei Sun, Zheng Li, Xiaoyun Wang, Lei Hu

EUROCRYPT 2021 で Bao らは、中間一致（MITM）原像攻撃の構成空間を系統的に探索する自動手法を提案した。

本論文は、それを制約ベースのフレームワークに拡張し、鍵回復攻撃と衝突攻撃の両方の

シナリオの微妙な特殊性を考慮することで、悪用可能な MITM 特性を見出す。さらに、従来にない非線形制約を持つ neutral words を用いた MITM 特性を利用した攻撃を行うために、対応する非線形方程式を解くことなく、また攻撃全体の時間的計算量を増すことなく、neutral words の解空間を導出する手順を提示する。本手法を、SKINNY、ForkSkinny、Romulus、Saturnin、Grostl、Whirlpool といった具体的な対称鍵プリミティブに適用した。その結果、単一鍵モデルにおいて、SKINNY-n-3n に対する初の 23 ラウンド鍵回復攻撃と ForkSkinny-n-3n に対する初の 24 ラウンド鍵回復攻撃を極めて少ないメモリで特定することができた。さらに、Whirlpool と Grostl に対する改良された（擬似）原像攻撃や衝突攻撃も得られた。これらの攻撃を生成するためのソースコードは公開されている。

・A Deeper Look at Machine Learning-Based Cryptanalysis[Eurocrypt 2021]

Adrien Benamira, David Gerault, Thomas Peyrin, Quan Quan Tan

機械学習による対称鍵暗号解析に関する論文である。

CRYPTO'19 で Gohr は、機械学習アルゴリズムの活用に基づく新たな暗号解析を提案した。ディープニューラルネットワークを利用し、よく研究されている NSA ブロック暗号 SPECK の 1 つのバージョンについて、最先端の暗号解読を驚くほど上回るニューラルベースの識別器（distinguisher）を構築することに成功した（この識別器は、今度はより大きな鍵回復攻撃にも使える可能性がある）。しかし、この識別器が実際にどのように機能するのか、機械学習アルゴリズムがどのような情報を推論しているのかといった問題は、ディープニューラルネットワークの解釈可能性はよく知られた困難な問題であることも加わり、まだ不明である。

本論文は、この新しい識別器の固有の仕組みについて、詳細な分析と徹底的な解説を行う。まず、分類済みセットを研究し、Gohr の結果をよりよく理解するための指針となるいくつかのパターンの発見を試みた。実験により、学習された識別器は一般に暗号文のペアに関する差分分布に依存しているが、ペナルティラウンドとアンチペナルティラウンド（penultimate and antepenultimate rounds）における差分分布にも依存していることを示した。この結果を検証するため、ニューラルネットワークを用いない純粋な暗号解析に基づく SPECK 暗号の識別器を構築し、Gohr のニューラル識別器と基本的に同じ精度と同じ効率（したがって従来のニューラルでない識別器よりも改善されている）を達成することに成功している。さらに別アプローチとして、Gohr のディープニューラルネットワークを必要最低限にまで減らした機械学習ベースの識別器を提供する。著者らは、標準的な機械学習ツールを用いて、Gohr の識別器に非常に近い精度を維持することができた。特に、Gohr の識別器は、実際には学習段階で暗号の差分分布表（DDT）の非常に優れた近似を構築し、その情報を使って暗号文ペアを直接分類していることを示す。この結果は、識別器の完全な解釈可能性を可能にし、それ自体、ディープニューラルネットワークの解釈可能性に向けた興味深い貢献となる。最後に、

Gohr の研究を改善する方法と、新しい識別器の設定の可能性を提案する。すべての結果は、SPECK ブロック暗号で実施した実験により確認されている。

・Three Third Generation Attacks on the Format Preserving Encryption Scheme FF3[Eurocrypt 2021]

Ohad Amon, Orr Dunkelman, Nathan Keller, Eyal Ronen, Adi Shamir

FPE（Format Preserving Encryption）方式は、社会保障番号や生年月日などの有限な値の集合から平文を受け取り、同じ集合に属する暗号文を生成する方式である。既存のデータベースや通信パケットの形式を変えずに暗号化できるため、実用上非常に有用である。業界の要望により、NIST は 2016 年に FF1 および FF3 と呼ばれる 2 つのこのような暗号化方式を標準化していた。これらは攻撃計算量の減少とともに、すぐに暗号解読の大きな注目を集めた。FF3 の Feistel 構築に対して現在知られている最高の攻撃は、入力がサイズ$N \times N$のドメインに属する場合、データとメモリの複雑さが$O(N^{11/6})$、時間の複雑さが$O(N^{17/6})$になる。

本論文では，FF3 に対する 3 つの改良型攻撃法を提案し，実験的に検証する．本論文で提案する攻撃法は、任意の$t \leq 0.5$に対し、トレードオフ曲線$D = M = \tilde{O}(N^{2-t}), T = \tilde{O}(N^{2+t})$を実現するものである。特に、データ量とメモリ量を実用的な$\tilde{O}(N^{1.5})$に低減し、同時に時間量を$\tilde{O}(N^{2.5})$に低減することが可能である。また、FPE 方式に対するもう一つの攻撃ベクトルである related-domain 攻撃を識別する。敵対者に異なるドメインで同じ鍵の暗号にアクセスさせることで強力な攻撃を行う方法を示し、FF3 インスタンスと FF3-1 インスタンスを効率的に区別するための適用方法を示す。

・Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2 [Eurocrypt 2021]

Christof Beierle, Patrick Derbez, Gregor Leander, Gaetan Leurent, Havard Raddum, Yann Rotella, David Rupprecht, Lukas Stennes

本論文では、GEA-1 および GEA-2 アルゴリズムに対する初めての公開された暗号解析攻撃を紹介する。64 ビットの完全なセキュリティを提供する代わりに、GEA-1 の初期状態を、わずか 65 ビットの（少なくとも 1 フレームごとに 24 ビットである）既知のキーストリームから、2^{40}回の GEA-1 評価と 44.5 GiB のメモリを使用して回復することができることを示した。GEA-1 への攻撃は、配置された LFSR と鍵の初期化との例外的な相互作用に基づいており、偶然に起こる可能性は極めて低いものである。この異常なパターンは、設計上セキュリティレベルを 40 ビットに制限するために、弱点を意図的に隠していることを示している。一方、GEA-2 については、同様の意図的な弱点は発見されなかった。しかし、代数的手法とリストマージアルゴリズムの組み合わせにより、依然として$2^{45.1}$回の GEA-2 評価で GEA-2 を破ることが可能である。主な実用上のハードルは、1600 バイトのキース

トリームの知識が要求される点となる。

・Mind the Middle Layer: The HADES Design Strategy Revisited [Eurocrypt 2021]

Nathan Keller, Asaf Rosemarin

HADES の設計方針は、古典的な SPN 構成と、暗号化ラウンドごとに状態の一部のみに非線形層を適用する部分 SPN（PSPN）構成を組み合わせたものである。統計的攻撃に対する HADES の安全性の議論は、PSPN ラウンドを無視し、SPN ラウンドのみを使用している。これにより、設計者は線形混合演算として使用する MDS 行列にいかなる制限も課さないことができる。

本論文では、MDS 行列の選択が HADES 設計のセキュリティレベルに大きく影響することを示す。さらに HADES の Starkad と Poseidon のインスタンスでの結果も紹介され、適切でない MDS 行列を選択した場合の、Starkad、Poseidon についての今まで主張されてきた安全性を破ることに成功している。本報告を受け、Starkad と Poseidon の設計者は、MDS 行列が適切に選択されていることを保証する要件を追加し、設計を修正済みである。

・QCB: Efficient Quantum-secure Authenticated Encryption [Asiacrypt 2021]

Ritam Bhaumik, Xavier Bonnetain, André Chailloux, Gaëtan Leurent, María Naya-Plasencia, André Schrottenloher, Yannick Seurin

対称鍵暗号は量子攻撃の影響を軽微にしか受けず、鍵長を 2 倍にすれば安全性が回復すると長い間考えられていた。 しかし、最近の研究により、敵がメッセージの量子重ね合わせで MAC/暗号化オラクルをクエリできる場合、Simon の量子周期発見アルゴリズムが多数の MAC/認証暗号化アルゴリズムを破ることが示された。特に、OCB 認証暗号モードはこの設定で破られ、同じ効率（レート 1、並列化可能）で量子安全なモードは知られていない。

本論文は、これまでの攻撃を一般化し、OCB に似た大規模な方式が重ね合わせクエリに対して安全でないことを示し、認証付き暗号化方式の量子安全性について議論する。また、TAE と OCB に着想を得た新しいレート 1 並列化可能なモード QCB を提案し、量子重ね合わせクエリに対する安全性を証明する。

・A Practical Key-Recovery Attack on 805-Round Trivium [Asiacrypt 2021]

Chen-Dong Ye, Tian Tian

キューブ攻撃（cube attack）は、Trivium に対する最も重要な暗号解読技術の一つである。キューブ攻撃に基づく鍵回復攻撃は数多く確立されている。しかし、80 ビットの完全な鍵情報を実用的に復元できる攻撃はほとんどない。特に、これまでの実用的な鍵復元攻撃は、FSE2013 で Fouque と Vannet が提案した 784 ラウンドの Trivium に対するものが最高だった。実用的な鍵回復攻撃を行うには、十分な数の低次の superpoly が必要となる。実

験的なキューブ攻撃でも、ランダムに選択したキューブを用いた分割特性に基づくキューブ攻撃でも、効率が悪いため困難である。

本論文では、線形 superpoly をターゲットとした候補キューブを構築するための新しいアルゴリズムが与えられる。実験により、構築したキューブを用いて線形 superpoly を見つける成功確率は 100%であることが示された。また、805 ラウンドの Trivium において、1000 以上の線形 superpoly を得ることができた。42 個の独立した線形 superpoly を用いて、805 ラウンドの Trivium に対して実用的な鍵回復攻撃を行い、攻撃ラウンド数を 21 ラウンド増加させた。攻撃の計算量は $2^{41.40}$ で、GTX-1080 GPU を搭載した PC で数時間以内に実行可能である。

・Algebraic Attacks on Rasta and Dasta Using Low-Degree Equations [Asiacrypt 2021]

Fukang Liu, Santanu Sarkar, Willi Meier, Takanori Isobe

Rasta と Dasta は、それぞれ CRYPTO 2018 と ToSC 2020 で提案された、完全準同型暗号になじむ共通鍵プリミティブである。

本論文では、Rasta と Dasta の設計者は、χ 演算の重要な特性を無視していたことが指摘される。この性質は、Rasta と Dasta の特殊な構造と相まって、代数的暗号解読の大幅な向上に直結する。特に、Rasta の攻撃的なバージョンであり、ブロックサイズがビット単位のセキュリティレベルよりわずかに大きい full Agrasta の 3 インスタンス中 2 インスタンスを理論的に破ることができる。さらに、Dasta は、刻々と変化するビット並べ換えと決定論的線形変換からなる線形層を用いるため、Rasta よりも著者らの攻撃に対して脆弱であることを明らかにした。この暗号解析により、パラメータ $(n, \kappa, r) \in \{(327,80,4), (1877,128,4), (3545,256,5)\}$ に対して、Dasta と Rasta のセキュリティマージンを 1 ラウンドに削減した。ここで、n,κ,r は、それぞれブロックサイズ、セキュリティレベル、ラウンド数を表す。これらのパラメータは、対応する ANDdepth が合理的な時間で実装でき、同じセキュリティレベルを目標とするものの中で最も小さいため、特に注目される。

・Automatic Classical and Quantum Rebound Attacks on AES-like Hashing by Exploiting Related-key Differentials [Asiacrypt 2021]

Xiaoyang Dong, Zhiyu Zhang, Siwei Sun, Congming Wei, Xiaoyun Wang, Lei Hu

AES によく似たハッシュ関数（有名な PGV モードやそれらの変種に AES によく似た暗号や置換を加味して作られたハッシュ関数）に対する衝突攻撃は、入力と出力の差が同じであるような AES によく似たプリミティブの、差分を表す入力の組を見つける問題に還元することが可能である。Mendel らによるリバウンド攻撃（rebound attack）は、この目標を達成するための強力なツールであり、その量子版は EUROCRYPT 2020 で Hosoyamada-

Sasaki によって初めて検討された。

本研究では、MILP に基づくアプローチにより、基礎となるブロック暗号の関連鍵の差分を考慮したリバウンド攻撃の構成を探索するプロセスを自動化することを目指す。量子環境において、著者らのモデルは、結果として得られるリバウンド攻撃のリソース（例えば、QRAM）と複雑さを最小化する特性に向かって探索を導く。本手法を Saturnin-hash、Skinny、Whirlpool に適用したところ、改善された結果が得られた。

・Clustering Effect in Simon and Simeck [Asiacrypt 2021]

Gaëtan Leurent, Clara Pernot, André Schrottenloher

Simon と Simeck は、単語の回転とビット単位の AND 演算のみを用いたシンプルなラウンド関数を持つ軽量ブロック暗号である。これまでの研究で、差分暗号や線形暗号には、同じ入出力を持つトレイルが多数存在するため、強いクラスタリング効果があることが示されている。

本論文では、アクティブビットが w ビットの固定ウィンドウに留まる高確率の微分・線形トレイルのクラスを示すことで、このクラスタリング効果を探索している。微分や線形近似に寄与する良いトレイルの集合を列挙する代わりに、クラス内の全てのトレイルを含む、この空間上の確率分布を計算する。この結果、従来提案されていたものより強力な識別器が実現され、Simon と Simeck に対する鍵回復攻撃について、従来の結果を最大 7 ラウンド向上したことが報告されている。特に、42 ラウンドの Simeck-64 に対しては 2 ラウンドのセキュリティマージンを残す攻撃、45 ラウンドの Simon-96/144 に対してはセキュリティマージンを 16 ラウンドから 9 ラウンドに減らす攻撃が得られている。

・New Attacks on LowMC instances with a Single Plaintext/Ciphertext pair [Asiacrypt 2021]

Subhadeep Banik, Khashayar Barooti, Serge Vaudenay, Hailun Yan

攻撃者が単一の既知の平文/暗号文のペアにアクセスできる場合の LowMC ブロック暗号の暗号解析は、数学的に困難な問題である。これは、攻撃者が線形暗号解析や差分暗号解析のような対称暗号の標準的な技術のほとんどを用いることができないためである。このシナリオは、LowMC ブロック暗号で生成された平文/暗号文のペアが公開鍵（検証鍵）となり、対応する LowMC 暗号鍵が署名方式の秘密鍵（署名鍵）にもなる Picnic 電子署名方式の安全性を論じる際に特に関連性が高い。Banik らの論文（IACR ToSC 2020）では、LowMC S-box の線形化技術を使って、ブロック暗号のいくつかのインスタンスに攻撃を仕掛けた。

本論文では、まず、線形化攻撃のより正確な計算量分析が行なわれる。そして、LowMC に対して 2 段階の中間一致攻撃を行う方法を示されている。第一段階では、マスターキーのキービットの何分の一かに相当するキー候補を削減する。この削減された候補セッ

トと残りのキービットの割合の間の 2 番目の中間一致攻撃のステージで、マスターキーの復元に成功する。これらのステージを合わせた計算量は、Banik らの ToSC 論文で報告された値よりも大幅に低いことも示される。

・Convexity of division property transitions: theory, algorithms and compact models [Asiacrypt 2021]

Aleksei Udovenko

積分暗号は対称暗号プリミティブを攻撃するための強力なツールであり、division property は積分識別器（integral distinguisher）を見つけるための最先端のフレームワークである。

本研究では、従来のビットベースの division property に対する新たな理論的・実用的な知見が述べられる。特に、division property の単調性・凸性の解析とその利用、およびグラフ指標との関連に焦点が当てられる。特に著者らの研究は、伝搬の新しいコンパクトな表現につながり、軽量ブロック暗号の 16 ビット Super-Sbox や 32 ビットランダム S-box のような、より大きな S-box の CNF/MILP モデリングを可能にするものである。これは、Derbez and Fouque (ToSC 2020)が提起した、16 ビット Super-Sbox の SAT/SMT/MILP モデリングの可能性に疑問を呈する課題を解決するものである。これまでのアプローチでは実現不可能であった、8 ラウンド LED の Super-Sboxes を CNF 式によるモデル化も行われる。

・Massive Superpoly Recovery with Nested Monomial Predictions [Asiacrypt 2021]

Kai Hu, Siwei Sun, Yosuke Todo, Meiqin Wang, Qingju Wang

あるキューブの superpoly の正確な代数構造または部分情報を決定することは、キューブ攻撃（秘密および公開の微調整可能な入力を持つ対称鍵プリミティブの汎用暗号解析技術）において必要なステップである。現在、superpoly の正確な復元には、division property に基づくアプローチが最も強力な手段となっている。しかし、ラウンド数の増加に伴い、対象となる出力ビットの代数的正規形（algebraic normal form、ANF）がますます複雑になるため、既存の superpoly 復元の手法はボトルネックを持つ。例えば、従来の方法は、Trivium、Grain、Kreyvium のそれぞれについて、ラウンド 842、190、892 で止まっていた。

本論文では、単項式予測法（monomial prediction technique、ASIACRYPT 2020、division property の代替）に基づき、大規模な superpoly の ANF を正確に復元する新しい枠組みが提案される。この新しいフレームワークは、Trivium, Grain, Kreyvium に適用された。その結果、843 ラウンドの Trivium、844 ラウンドの Grain、845 ラウンドの Kreyvium の superpoly の正確な ANF が復元される。さらにメビウス変換の助けを借りて、スパース構造を利用した全てのキービットを含む superpoly に基づく新しい

鍵回復技術を提示し、考察した対象に対して最良の鍵回復攻撃ができるようになった。

・Quantum Linearization Attacks [Asiacrypt 2021]

Xavier Bonnetain, Gaëtan Leurent, María Naya-Plasencia, André Schrottenloher

最近の研究により、量子周期探索を用いることで、重ね合わせクエリモデルでよく用いられる多くの構成（Even-Mansour などのいくつかのブロック暗号、複数の MAC や AE など）を破ることができることが示された。これまでに、解読された暗号はすべて強い代数的構造を示し、単一の入力ブロックの周期的関数を作成することが可能である。この周期を回復することで、鍵の回復や、これらのモードの機密性・真正性の保持を破ることができる。

本論文では、重ね合わせクエリモデルにおける MAC を標的とした Simon のアルゴリズムを用いた新しい方法である「量子線形化攻撃」（Quantum linearization attack）が紹介される。さらに量子暗号解析ではあまり用いられない、他の量子アルゴリズムを用いた本攻撃のバリエーションも紹介される：Deutsch、Bernstein-Vazirani、Shor の 3 種類である。これらのアルゴリズムが量子暗号解読や鍵回復攻撃に利用されたのは、著者らの知る限り今回が初めてである。この攻撃は、LightMac、PMAC などの並列化可能な MAC や、（古典的な）誕生日攻撃安全性を持っているもの（LightMAC+、PMAC+）、調整可能なブロック暗号を用いたもの（ZMAC）など、多くの変種を破ることができる。より一般的には、並列化可能な量子安全保障 PRF の構築が困難な課題であることを示している。

・Generic Framework for Key-Guessing Improvements [Asiacrypt 2021]

Marek Broll, Federico Canale, Antonio Florez-Gutierrez, Gregor Leander, Maria Naya-Plasencia

ブロック暗号に対するいくつかの攻撃において、鍵の推測ステップを改善する一般的な手法を提案する。これは、関連する S-box のいくつかの新しい特性を定義・研究し、それらを特殊なタイプの決定木として表現することによって達成されるもので、様々な攻撃ベクトルに対する細かい推測戦略を見つけるために重要である。 このような木を効率的に見つけるアルゴリズムを提案・実装し、それを用いて、NOKEON、GIFT、RECTANGLE に対する最もよく知られた攻撃を含む、このアプローチのいくつかの応用例を提供する。

2.2.2. 公開鍵暗号に関する解読技術

・SimS: a Simplification of SiGamal [PQCrypto 2021]

Tako Boris Fouotsa, Christophe Petit

Asiacrypt 2020 で Moriya らにより提案された、SiGamal と C-SiGamal に関する暗号解析論文である。これらは 2 つの新しい IND-CPA 安全な超特異性ベースの公開鍵暗

号化（PKE）プロトコルである。SIKE や CSIDH から正規化された PKE とは異なり、新しいプロトコルはランダムオラクルを用いずに IND-CPA の安全性を実現している。しかし、SiGamal と C-SiGamal は IND-CCA 安全ではない。また Moriya らは IND-CCA 安全性を持つ SiGamal の変種を提案したが、その研究は未解決のまま残された部分があった。

本論文では、Moriya らが提案したプロトコルを再検討する。まず、Moriya らが IND-CCA 安全性のために提案した SiGamal の変形が、実際には IND-CCA 安全性でないことを明らかにする。次に、SiGamal を単純化した InSIDH と名付けた新しい同種ベースの PKE プロトコルを提案する。In-SIDH は(C-)SiGamal よりも公開鍵、暗号文が小さく、効率的である。さらに、CSIDH の安全性仮定と、本論文で導入される Knowledge-of-Exponent 型の仮定の下で、InSIDH が IND-CCA 安全であることを証明する。興味深いことに、InSIDH は CSIDH プロトコルに非常に近く、SiGamal と CSIDH の比較を容易にする。

・A Practical Adaptive Key Recovery Attack on the LGM (GSW-like) Cryptosystem [PQCrypto 2021]

Prastudy Fauzi, Martha Norberg Hovd, Håvard Raddum

本論文では、Li, Galbraith and Ma (Provsec 2016) が提案した Leveled 準同型暗号に対する、適応的(adaptive)鍵回復攻撃が紹介される。この方式自体は、復号ごとに異なる秘密鍵の線形結合を使用することで鍵回復攻撃に抵抗するように設計された GSW 暗号の修正版である。著者らは、統計的な攻撃を用いて、現実的なパラメータの選択に対して、効率的に秘密鍵を復元することができた。これは特に、Li, Galbraith, Ma の戦略は適応的な鍵回復攻撃を防ぐことができないことを意味する。

・How to Meet Ternary LWE Keys [CRYPTO2021]

Alexander May

LWE 問題とその環を変えた変種は、量子コンピュータに耐える効率的な公開鍵暗号を構築するための最も有力な候補である。NTRU 暗号は、LWE 問題の変形で、最大ノルムの秘密が小さく、通常、集合 ${-1,0,1}$ の三項係数を使用する。これらの方式に対する最良の攻撃は、格子削減技術と Odlyzko の Meet-in-the-Middle アプローチを組み合わせたハイブリッド攻撃と推定される。Odlyzko のアルゴリズムは古典的な組み合わせ攻撃であり、鍵空間のサイズSに対して時間 $S^{0.5}$ で実行される。

本論文では、部分和アルゴリズムで開発された表現技法（representation technique）を用いて、この Meet-in-the-Middle アプローチが大幅に改善される。漸近的には、著者のヒューリスティックな Meet-in-the-Middle 攻撃はおよそ $S^{0.25}$ の時間で実行されるが、これは最もよく知られた量子アルゴリズムの $S^{1/3}$ 計算量を上回るものである。

NIST のラウンド 3 ポスト量子暗号 NTRU-Encrypt と NTRU-Prime に対しては、著者らの攻撃の非漸近的な実装を、計算量およそ $S^{0.35}$ で得ることができた。他の組み合わせ攻撃とは対照的に、著者らの攻撃はより大きな LWE フィールドサイズ q からアドバンテージを得ている。例えば、BLISS 署名では $S^{0.31}$ から $S^{0.35}$ の間で、GLP 署名では $S^{0.3}$ で非漸近的な組合せ攻撃が得られる。

著者の攻撃は、前述の方式の安全性の主張を無効化するものではない。しかし、その安全性に対して改善された組み合わせ論的な上界を確立している。著者の新しい Meet-in-the-Middle 攻撃と格子削減を組み合わせることで、ハイブリッド攻撃を高速化できるかどうかは未解決の問題である。

・Improved torsion-point attacks on SIDH variants [CRYPTO 2021]

Victoria de Quehen, Peter Kutas, Chris Leonardi, Chloe Martindale, Lorenz Panny, Christophe Petit, Katherine E. Stange

SIDH は、超特異楕円曲線間の同種写像を見つけることが困難であるという推定に基づく耐量子鍵交換アルゴリズムである。しかし、SIDH が依拠する厳密な困難性の仮定は純粋な同種写像問題ではない。攻撃者は実際に、秘密同種写像を曲線の部分群として与えるという制限を受ける。Petit はこの情報を利用して、SIDH の overstretched variants を多項式時間で破っており、ねじれ点の情報を利用することで、ある場合には効率的な攻撃ができることを実証している。

本論文の貢献は 2 つある。まず、Petit の手法を再検討し、双対とフロベニウス同種から来る情報を追加で利用する方法を示す。また、著者らの攻撃が適用されるパラメータの全範囲を示し、特に興味深い例として n-party group key agreement を挙げる。6 人以上のパーティの場合、本攻撃は多項式時間で実行され、3 人以上のパーティの場合、本量子攻撃は最もよく知られた漸近的計算量を向上させる。また、6 パーティに対する本攻撃の Magma 実装も提供する。

第二に、本攻撃に対して弱く設計された SIDH 変種を構築した。これには、開始曲線のトラップドアの選択と基礎体の標数のトラップドアの選択が含まれる。ただし著者らの結果は、NIST 提出の SIKE の弱点を明らかにしてはいない。

・On the hardness of the NTRU problem [Asiacrypt 2021, Award Paper]

Alice Pellet-Mary, Damien Stehlé

25 年前の NTRU 問題は、公開鍵暗号における重要な計算の前提となっている。しかし、ユークリッド格子上の他の問題と比較した場合、削減の観点からその相対的な難しさはよく分かっていない。その決定版は探索 Ring-LWE 問題に還元されるが、これは困難性の上界を与えるに過ぎない。

本論文は、NTRU 問題の困難性に関する漸化式の証拠を提供するという、長年の未

解決問題に対する 2 つの解答を提供する。まず、理想格子上の最悪ケースの近似最短ベクトル問題を、NTRU 問題の平均ケース探索変種問題に帰着する。次に、NTRU 問題の別の平均ケース探索変種問題を、決定 NTRU 問題に還元する.

・Fault-Injection Attacks against NIST's Post-Quantum Cryptography Round 3 KEM Candidates [Asiacrypt 2021]

Keita Xagawa, Akira Ito, Rei Ueno, Junko Takahashi, Naofumi Homma

NIST PQC ラウンド 3 *鍵カプセル*化メカニズムの全候補：Classic McEliece、Kyber、NTRU、Saber、BIKE、FrodoKEM、HQC、NTRU Prime、SIKE を、故障利用攻撃（fault injection attack）の観点から調査した。これらすべての KEM 方式は Fujisaki-Okamoto 変換の変種を使用しているため、カプセル化解除時の再暗号化との等価性テスト（equality test）が重要である。

本論文では、等値性判定を省略できる場合の有効な鍵回復攻撃について調査される。その結果、Kyber、NTRU、Saber、FrodoKEM、HQC、NTRU Prime の 2 つの KEM 方式のうちの 1 つ、および SIKE に対する既存の鍵回復攻撃があることがわかった。また、NTRU Prime に含まれるもう 1 つの KEM 方式に対する新しい鍵回復攻撃が提案される。また、BIKE に対して秘密鍵の情報漏えいを引き起こす攻撃が報告される。

オープンソースの pqm4 ライブラリには、Classic McEliece と HQC を除く全ての KEM スキームが含まれている。本論文では、Kyber, NTRU, Saber, BIKE, SIKE において、カプセル化解除の過程で 1 つの命令スキップ故障（instruction-skipping fault）を与えることで、仮想的に等値性テストがスキップされることが示されている。また、それらに対する攻撃の実験結果も報告される。また、NTRU Prime の実装では選択暗号文攻撃が自由に行えること、Guo, Johansson, and Nilsson (CRYPTO 2020) で報告された FrodoKEM のタイミングサイドチャネルが残っているが、彼らの NIST PQC Round 3 提出課題にはそのようなバグがないことも報告される。

・A formula for disaster: a unified approach to elliptic curve special-point-based attacks [Asiacrypt 2021]

Vladimir Sedlacek, Jesús-Javier Chi-Domínguez, Jan Jancar, Billy Bob Brumley

Refined Power Analysis、Zero-V*b*cy*e*b

完全なスカラーを回復させる。最後に、Explicit-Formulas データベースから楕円曲線点加算公式を系統的に解析し、すべての非自明な例外点を分類し、新しい公式でそれらを発見することに成功している。これらの結果は、公式の展開と特殊な点の発見に対する著者らのツールの有用性を示すものであり、将来的には独立した研究対象となる可能性がある。

・On the non-tightness of measurement-based reductions for key encapsulation mechanism in the quantum random oracle model [Asiacrypt 2021]

Haodong Jiang, Zhenfeng Zhang, Zhi Ma

弱く安全な（weakly-secure）PKE を IND-CCA 安全な KEM に変える Fujisaki-Okamoto（FO）変換（TCC 2017）の KEM 変種は、NIST ポスト量子暗号標準化プロジェクトの中で広く使われた。標準的な CPA の安全性仮定、すなわち OW-CPA と IND-CPA の下で、量子ランダムオラクルモデル（QROM）におけるこれらの変種の安全性は、例えば Jiang ら（CRYPTO 2018）、および非ブラックボックス帰着（EUROCRYPT 2020）により証明された。非ブラックボックス帰着は、セキュリティロスは線形だが、厳密な可逆実装を持つ特定の可逆敵対者にしか適用することができない。一方、既存のブラックボックス帰着は、任意の実装を持つ任意の敵対者に適用可能だが、安全性の損失が 2 倍となる。

本論文では、FO 変換の KEM バリエーションについて、まずブラックボックス帰着の厳密性の限界を示し、QROM において、基礎となる PKE の標準的な OW-CPA（または IND-CPA）安全性を破ることから、結果の KEM の IND-CCA 安全性を破ることへの測定ベース（measurement-based）の帰着は、必然的に安全性の二次損失を引き起こすことを証明する（「測定ベース」とは、攻撃者からのハッシュクエリーを測定し、測定結果を使用して PKE の基礎を破ろうとするものである）。特に、これらの FO 変換に似た KEM 変種に対するブラックボックス帰着のほとんどはこのタイプであり、我々の結果は、安全性損失の程度という点で、この帰着の厳密性の向上が進んでいないことの説明を示唆する。

さらに、探索問題を決定問題に変換するときに、量子ランダムオラクルを含む暗号システムの安全性を証明するために不可欠な技術として認識されているブラックボックス的な一方向秘匿技術を使う際、2 次的な安全性損失も避けられないことも示される。

・NTRU Fatigue: How Stretched is Overstretched? [Asiacrypt 2021]

Wessel van Woerden, Léo Ducas

最近まで、NTRU 格子の格子簡約攻撃は、同じパラメータを持つ(ring)-LWE 格子の場合と同様の挙動を示すと考えられていた。しかし、いくつかの研究（Albrecht-Bai-Ducas 2016, Kirchner-Fouque 2017）は、大きなモジュラス q、いわゆる NTRU の overstretched 領域に対して大きなギャップがあることを示した。NTRU スキームは NIST PQC コンペティシ

ョンの最終選考に残ったため、疲労点（fatigue point）がどこにあるのか、つまり、どの q で overstretched 領域が始まるのかを正確に理解することは、漸近的かつ具体的に重要である。

本論文では、Kirchner と Fouque の解析を漸近的に改善し、3 元 NTRU の疲労点を$q \leq n^{2.783+o(1)}$ から $q = n^{2.484+o(1)}$ まで絞り込み、最後にこの現象の背景を説明する新しい解析が提案される。この解析をさらに具体的に推し進め、疲労点を約 $q = 0.004 \cdot n^{2.484}$ に設定したとき、オーバーストレッチ領域における困難性の正確に予測することができるようになった。これらの予測は、広範な実験によって裏付けられている。

・Faster Dual Lattice Attacks for Solving LWE -- with applications to CRYSTALS [Asiacrypt 2021]

Qian Guo, Thomas Johansson

LWE 問題に基づく暗号システムには、LWE 問題を解くための汎用アルゴリズムのコストに関連するセキュリティレベルが割り当てられている。これには少なくとも、いわゆる格子攻撃と双対格子攻撃が含まれる。

本論文では、Bleichenbacher の研究に遡ることができるアイデアを用いて、双対格子攻撃の改良を提示する。提案手法では、格子簡約アルゴリズムにおける 2 つの最新技術、すなわち、「次元の自由化」と「1 回のふるい分けで多くの短いベクトルを生成する技術」を利用するが、この 2 つのトリックの非互換性が、双対格子攻撃が興味深くはない主な理由と考えられていた。そのため著者らの新しい削減戦略は、重要な暗号パラメータセットに対して、単純な格子攻撃よりも効率的な双対アプローチを可能にしている。

さらに、提案攻撃を NIST のポスト量子暗号プロジェクトの最終候補である CRYSTALS-Kyber と CRYSTALS-Dilithium に適用し、コア SVP モデルにおいて古典的および量子的に新しい低い計算量を与えることを示した。最も重要なことは、提案されたセキュリティパラメータについて、洗練された格子簡約戦略を用いた著者らの新しい双対攻撃が、古典的なゲートカウントメトリック（gate-count metric）、すなわち古典的 Random Access Machine（RAM）モデルにおける最先端の格子攻撃を大幅に改善したことである。具体的には、外挿モデルによる Kyber1024 では、改善係数が 15 ビットになる（Albrecht et al.at Eurocrypt 2019）。また、Kyber768 は、その主張するセキュリティレベル以下の古典的なゲート計算量で解くことができることを示す。さらに、Homomorphic Encryption Standard のドラフト版（https://homomorphicencryption.org 参照）の提案されたパラメータに提案攻撃が適用された。結果、例えば 192 ビットの安全性を目指すパラメータセットを、古典的な RAM モデルで $2^{187.0}$ 回の操作で解くことが可能となった。これらのパラメータは、よく知られた Fully Homomorphic Encryption ライブラリで展開されている。

・Lattice sieving via quantum random walks [Asiacrypt 2021]

Johanna Loyer, André Chailloux

格子暗号は、ポスト量子暗号の有力な提案の一つである。最短ベクトル問題（Shortest Vector Problem、SVP）は格子暗号の暗号解析において最も重要な問題であり、多くの格子暗号はその困難性に基づく安全性を主張している。SVP に対する最良の量子アルゴリズムは Laarhoven [Laa16 PhD]によるもので、（ヒューリスティックに）時間 $2^{0.2653d + o(d)}$ で実行される（d は格子の次元）。

本論文では、Laarhoven の結果を改良し、（ヒューリスティックに）時間 $2^{0.2570\,d + o(d)}$ で実行されるアルゴリズムが提示される。また、本アルゴリズムの量子メモリと量子ランダムアクセスメモリの量を定量化し、時間とメモリの間のトレードオフを提示する。

・A Systematic Approach and Analysis of Key Mismatch Attacks on Lattice-Based NIST Candidate KEMs [Asiacrypt 2021]

Yue Qin, Chi Cheng, Xiaohan Zhang, Yanbin Pan, Lei Hu, Jintai Ding

格子ベースの KEM に対する鍵不一致攻撃の研究は、現在進行中の NIST のポスト量子暗号の標準化における暗号評価の重要な部分である。このような攻撃は数多く存在しているが、しかしこれらの KEM の鍵不一致攻撃に対する耐性を評価する統一的な手法はまだない。効率性の重要な指標は、そのような攻撃を成功させるために必要なクエリ数である。

本論文では、そのような攻撃に必要な最小平均クエリ数の下界を求める体系的アプローチの提案、開発が行われる。基本的な考え方は、クエリの下限を求める問題を最適なバイナリ復元木（binary recovery tree、BRT）を見つけることに変換することである。この BRT において、下限の計算は、本質的には特定のシャノンエントロピーの計算となる。またこの最適 BRT のアプローチにより、いくつかの格子ベースの NIST 候補 KEM において、必要なクエリの数に関して、理論的な下限と実際の攻撃で観測された下限の間に大きなギャップがある理由を説明できる。さらにこれら既存攻撃に対する汎用的な改善方法が提案され、実験により確認された。提案された手法は、CCA 安全な NIST 候補 KEM に対するサイドチャネル攻撃を改善するために直接利用することができる。

2.2.3. ハッシュ関数に関する解読技術

・Attacks on Beyond-Birthday-Bound MACs in the Quantum Setting [PQCrypto 2021]

Tingting Guo, Peng Wang, Lei Hu, Dingfeng Ye

本論文では、攻撃者が MAC への量子クエリアクセスを持つ Q2 モデルにおいて、12 の誕生日攻撃耐性 MAC（BBB MAC）の安全性を系統的に研究している。その結果、

少なくとも $O(2^{2n/3})$クエリまでは安全であることが証明された（古典的な攻撃では$O(2^{3n/4})$クエリが必要)。さらに著者らは、SUM-ECBC および PMAC Plus に似た MAC に対する秘密状態回復と、PMAC Plus に似た MAC に対する鍵回復を検討し、どちらの攻撃も偽造を成功させた。これらは、BBB MAC に対する初の量子攻撃である。mPMAC+-f、mPMAC+-p1、mPMAC+-p2 のような最適安全 MAC に対しても、本攻撃は有効であると報告された。

・Revisiting the Security of DbHtS MACs: Beyond-Birthday-Bound in the Multi-User Setting [CRYPTO 2021]

Yaobin Shen, Lei Wang, Dawu Gu, Jian Weng

Double-block Hash-then-Sum (DbHtS) MACs は、誕生日攻撃耐性を目指す MACs で、 SUM-ECBC、PMAC_Plus、3kf9、LightMAC_Plus などがある。最近、Datta ら(FSE'19)と Kim ら(Eurocrypt'20)は、単一ユーザー設定において誕生日攻撃耐性を有することを証明した。しかし、一般的な簡約により、彼らの結果はマルチユーザー設定において成り立たないことがわかる。

本論文では、マルチユーザー設定における DbHtS の安全性が再検討され、誕生日攻撃耐性を証明するためのフレームワークが提案される。このフレームワークの有用性を、2k-SUM-ECBC、2k-PMAC_Plus、2k-LightMAC_Plus をはじめとした、鍵削減を施した DbHtS MACs のバリエーションに適用して実証する。これらの構成は、ユーザー数が増えても安全性が低下しないことが示された。一方、先行研究で解析を簡略化するために用いられている領域分離を追加することなく、シングルユーザーおよびマルチユーザーの設定において、これらの構成が誕生日攻撃耐性を持つことも示した。

さらに、Datta ら(FSE'19)が誕生日攻撃耐性を証明した 2kf9 に重大な欠陥があることを見いだした。問い合わせを一切行わず、確率 1 でタグの偽造に成功する。

・Simple Constructions from (Almost) Regular One-Way Functions [TCC 2021]

Noam Mazor, Jiapeng Zhang

一方向性関数から構成できる暗号プリミティブとして、擬似乱数生成器（pseudorandom generators、PRG）と普遍的一方向性ハッシュ関数（universal one-way hash functions、UOWHF）の 2 つが有用である。これらを実際に実装するためには、その構築の効率性を考慮する必要がある。効率性の指標としては、シード長、一方向性関数への呼び出し計算量、そしてこれらの呼び出しの適応性の 3 つが挙げられる。しかし、これらの構成における最適な効率はまだ十分に理解されておらず、ブラックボックス構成における既知の上限と既知の下限の間にギャップが存在する。未知の正則一方向性関数（unknown-regular one-way functions）と呼ばれる一方向性関数の特殊なクラスは、よりよく理解されている。Haitner, Harnik and Reingold (CRYPTO 2006)

は、ランダム化反復子と呼ばれる手法に基づき、半線形（semi-linear）シード長および線形呼び出し回数の PRG 構成について発表した。Ames, Gennaro and Venkitasubramaniam (TCC 2012)は、同様のパラメータで、同様のアイデアを用いた UOWHF の構築を示した。一方、Holenstein and Sinha (FOCS 2012) と Barhum and Holenstein (TCC 2013) は、一方向性関数から PRG と UOWHF のブラックボックス構成に対して、ほぼ線形な呼び出し計算量の下界を示した。したがって、Haitner らと Ames らは、通常の一方向性関数から PRG と UOWHF を（シード長と呼び出し回数の点から）厳密に構成することに成功した。しかしこれらの構成は適応的である。

本研究では、Holenstein と Sinha、Barhum と Holenstein が示した最適な呼び出し回数と一致する、両プリミティブの非適応的な構成法を提示する。構成は単純かつ非適応的であることに加え、ほぼ正則な一方向性関数に対してもロバストである。

・Cryptanalysis of an oblivious PRF from supersingular isogenies [Asiacrypt 2021]

Andrea Basso, Péter Kutas, Simon-Philipp Merz, Christophe Petit, Antonio Sanso

Boneh、Kogan、Woo が Asiacrypt'20 で提案した SIDH ベースの超特異楕円曲線同種に基づく擬似乱数関数（PRF）について暗号解析を行った。そのために、Boneh らが導入した補助的な仮定に対する攻撃を行い、これが紛失擬似乱数関数（OPRF）そのものに対する攻撃につながることを示す。この攻撃は、敵対者がいくつかの最初の OPRF 評価といくつかのオフライン計算の後、サーバーとそれ以上のやりとりをせずに OPRF を評価することを可能にするので、擬似ランダム性を破る。さらに、概念実証のための実装と、筆者らの攻撃のいくつかのタイミングを提供する。最後に、OPRF パラメータの 1 つの生成を検証し、証明可能なセキュリティを保証するためには、信頼できるサードパーティが必要であることを論じる。

2.2.4. 署名に関する解読技術

・On the Effect of Projection on Rank Attacks in Multivariate Cryptography [PQCrypto 2021]

Morten øygarden, Daniel Smith-Tone and Javier Verbel

多変数暗号方式 HFEv-は、かつてポスト量子署名システムの有望な候補とみなされていた。2000 年代初頭に初めて提案されたこの方式は、現在進行中の NIST のポスト量子標準化プロセスの第 3 ラウンドに進出している。2020 年後半、この方式は Tao, Petzoldt, そして Ding による効率的なランク攻撃を受けた。本論文では、この最近のランク攻撃がプロジェクション修正（projection modification）によってどのような影響を受けるかを検証している。この修正は、署名方式 PFLASH を先行者の攻撃から保護するために導入された。本論文では、著者らが行った実験では最も厳しいものであっ

た新しい攻撃の下での projected HFEv- (pHFEv-)と PFLASH のランクの上界が証明され、この最近の暗号解読から守るための有用なツールになりうると結論付ける。

・The Nested Subset Differential Attack: A Practical Direct Attack Against LUOV which Forges a Signature within 210 Minutes [Eurocrypt 2021]

Jintai Ding, Joshua Deaton, Vishakha, Bo-Yin Yang

2017 年、Ward Beullenset al.が Patarin による Unbalanced Oil and Vinegar を修正した耐量子署名スキーム Lifted Unbalanced Oil and Vinegar（LUOV）を提出した。その後 Ding らは Subfield Differential Attack を提案したが、これは NIST のポスト量子標準化コンペティションの第 2 ラウンドで LUOV の作者がパラメータを変更するきっかけとなった。

本論文では、提案されたパラメータセットの半分を完全に破る、Subfield Differential Attack を改良した Nested Subset Differential Attack を提案する。また、この攻撃が理論上の攻撃ではなく、レベル I のセキュリティパラメータに対して 210 分以内で実際に可能であることを実験により示す。Nested Subset Differential Attack は、Subfield Differential Attack を大きく改良したものであり、実環境で使用可能である。著者らは、LUOV の「lifted」構造と呼ばれるもののみを使用しており、その攻撃は「lifted」二次方程式を解くことの発展形と考えることができる。

・Improved cryptanalysis of UOV and Rainbow [Eurocrypt 2021]

Ward Beullens

本論文の貢献は 2 つある。一つに、Unbalanced Oil and Vinegar 方式（UOV）とその変形である Rainbow 方式の記述を簡略化し、既存の攻撃を理解しやすくしたことである。二つに、UOV と Rainbow の署名方式に対して、UOV と Rainbow の両方に適用できる交叉攻撃と、Rainbow のみに適用できる長方形 MinRank 攻撃という 2 つの新しい攻撃を与えたことである。これらは既存の攻撃よりも強力であり、特に、NIST PQC 標準化プロジェクトの第 2 ラウンドに提出された、セキュリティレベル I、III、V をそれぞれ対象とするパラメータセットに対して、従来知られている攻撃と比較して、鍵回復のコストを 2^{17}、2^{53}、2^{73} 倍削減すると推定している。第 3 ラウンドのパラメータでは、コストはそれぞれ 2^{20}、2^{40}、2^{55} で減少している。これらのパラメータセットはすべて、NIST が定めたセキュリティ要件を満たさない。

・Differential Power Analysis of the Picnic Signature Scheme [PQCrypto 2021]

Tim Gellersen, Okan Seker, Thomas Eisenbarths

本論文では、NIST 耐量子コンペティションの候補である Picnic 署名スキームの差分サイドチャネル解析を初めて行ったものである。LowMC ブロック暗号のマルチパーティ実装

（MPC-LowMC）のサイドチャネル解析に成功し、アルゴリズムの 2 つの異なる部分を利用することでサイドチャネル情報を利用して秘密鍵全体を復元する方法を示した。LowMC の鍵回復により、Picnic の署名を偽造することができる。本論文では、FRDM-K66F 開発ボードで実行される NIST 参照実装を対象とした。鍵の復元は 1000 以下の LowMC トレースで成功するが、これは観測された 30 以下の Picnic 署名から得ることができるものである。

・Efficient Key Recovery for all HFE Signature Variants [CRYPTO 2021]

Chengdong Tao, Albrecht Petzoldt, Jintai Ding

HFE 暗号は、最もよく知られた多変数暗号方式の一つである。特に電子署名の分野では、HFEv-亜種は短い署名と高い性能を提供する。最近、GeMSS と呼ばれる HFEv-署名方式のインスタンスが、NIST のポスト量子暗号（PQC）標準化プロジェクトの第 3 ラウンドで、署名方式の代替候補の 1 つに選出された。

本論文では、HFEv-署名方式に対する新たな鍵回復攻撃を提案される。本攻撃は、Minus と Vinegar の両修飾が基本 HFE 方式の安全性を大きく向上させないことを示す。このことは、HFE をベースとした安全かつ効率的な署名方式を構築することが非常に困難であることを示している。特に、提案した GeMSS 方式のパラメータが主張するほど安全でないことが示される。

2.2.5. サイドチャネル攻撃の解読技術

・Provable Security Analysis of FIDO2 [CRYPTO 2021]

Manuel Barbosa, Alexandra Boldyreva, Shan Chen, Bogdan Warinschi

本論文は、FIDO Alliance が提案するパスワードレスユーザー認証の標準規格である FIDO2 プロトコルについて、初めて証明可能な安全性解析を実施している。著者らの分析は、W3C の Web Authentication (WebAuthn) 仕様と新しい Client-to-Authenticator Protocol (CTAP2) という FIDO2 のコアコンポーネントを対象としている。

WebAuthn と CTAP2 について、順番に、意図されたセキュリティ目標を捕らえることを目的とした適切なセキュリティモデルを提案し、そのモデルを用いてセキュリティを分析する。最初に著者らは、WebAuthn の認証の安全性を証明することで確認する。次に、CTAP2 が弱い意味での安全性しか証明できないことを示す。その一方で、一連の設計上の欠陥を特定し、改善のための提案を提供する。さらに、より強力かつ現実的な敵に対抗するため、sPACA と呼ばれる汎用プロトコルを提案し、その強い安全性を証明する。適切なインスタンス化により、sPACA は CTAP2 よりも効率的である。最後に、FIDO2 と WebAuthn+sPACA が提供する全体的なセキュリティ保証を、それらの構成要素のセキュリティに基づいて分析する。著者らは、著者らのモデルと証明可能なセキュリティ結果によ

っていEUDO2 プロトコルのセキュリティ保証が明らかになることを期待している。また、CTAP2 の代替プロトコルとして、より強固なセキュリティと高い性能を両立する著者らによ[illegible]PACA [illegible]を採用することを提唱している。

・Advanced Lattice Sieving on GPUs, with Tensor Cores [Eurocrypt 2021]

Léo Ducas, Marc Stevens, Wessel van Woerden

本論文[illegible]Kernel (G6K, Albrecht et al. 2019)の内部で、格子のための様々な最先端のふるい分けアルゴリズム（Becker-Gama-Joux 2015, Becker-Ducas-Gama-Laarhoven 2016, Herold-Kirshanova 2017）の GPU 実装を研究している。特に、最近導入された Tensor Core（元々はレイトレーシングや機械学習用に設計されている）を広範囲に活用し、目下の暗号解読タスクへの適合性を実証する。また、G6K の重要な要素である短いリフトドベクトルの発見を高速化するために、「リフトに値する」(='lift-worthy'）ペアを効率的に検出する新しいデュアルハッシュ技術を提案する。筆者らは、SVP Darmstadt Challenge において、従来の 155 次元の記録を更新する 180 次元の計算量を達成し、新記録を達成した。この計算は、4 つの NVIDIA Turing GPU と 1.5TB の RAM を搭載したサーバーで 51.6 日間実行された。これは、実測時間やエネルギー効率の点で、これまでの記録より約 2 桁も優れている。

・Secure and Efficient Software Masking on Superscalar Pipelined Processors [Asiacrypt 2021]

probing model）における形式的な解析と、ゲートレベルタイミングシミュレーション（gate-level timing simulation）による経験的な解析の両面から明らかにした。次に、これらの問題をハードウェアで修正するか、ソフトウェアの制約として残すかの選択肢を議論する。これらのソフトウェア制約に基づき、より複雑な CPU 上でのマスクされたソフトウェアの設計のための一般規則を策定する。最後に、マスキング方式のいくつかの実装戦略を比較し、複雑な CPU のための安全なマスキングソフトウェアの設計が、13%という低いオーバーヘッドで可能であることをケーススタディで示す。

・Divided We Stand, United We Fall: Security Analysis of Some SCA+SIFA Countermeasures Against SCA-Enhanced Fault Template Attacks[Asiacrypt 2021]

Sayandeep Saha, Arnab Bag, Dirmanto Jap, Debdeep Mukhopadhyay, Shivam Bhasin

サイドチャネル攻撃（side-channel attack、SCA）と故障攻撃（fault attack、FA）に対する防御は、2 つのクラスの対策を同時に暗号実装に組み込む必要がある。SCA と FA の対策をストレートに組み合わせた場合、統計的非効率故障解析（ Statistical Ineffective Fault Analysis、SIFA）や故障テンプレート攻撃（Fault Template Attack、FTA）などの FA に対して脆弱であることが既に示されている。そのため、SIFA を防止し、SCA を防止するためのマスキングを含む新しいクラスの対策が提案されてきた。これらの対策は、SIFA や SCA に対して個別に安全である一方、SCA と FA を組み合わせた敵が存在する場合にも安全性の主張が成り立つかどうかが重要な問題である。しかし、このような実装では、両方の脅威に対する対策が含まれているため、複合攻撃に対する安全性が望まれている。

本論文では、最近提案された SIFA と SCA を組み合わせた対策の一部が、複合攻撃の対象になることが示される。そのために、故障注入時のサイドチャネル情報を考慮することで FTA 攻撃を強化する。提案する攻撃の成功は、S-Box の非自明な障害伝播特性に起因しており、これは元の FTA 提案では未解明な点である。また、SIFA で保護された χ5 S-Box をオープンソースのソフトウェアで実装し、レーザー故障注入とパワー計測を行い、SIFA で保護された χ3 S-Box をハードウェア実装し、ゲートレベルのパワートレースシミュレーションを行って、提案する攻撃を検証した。最後に、既存の対策を強化するためのいくつかの緩和策について述べる。

2.2.6. その他暗号解読に関する技術

・Decoding Supercodes of Gabidulin Codes and Applications to Cryptanalysis [PQCrypto 2021]

Maxime Bombar, Alain Couvreur

本論文は、Gabidulin 符号の復号化について述べ、復号化半径の大幅な減少と引き換え

に、通常の復号器を Gabidulin 符号の任意のスーパーコードに拡張する方法を示している。この復号器を用いて、ランクによる距離を用いた暗号化方式である RAMESSES と LIGA に対する多項式時間攻撃を提供する。

・Classical and Quantum algorithms for generic Syndrome Decoding problems and applications to the Lee metric [PQCrypto 2021]

Thomas Debris-Alazard, André Chailloux, Simona Etinski

コードベース暗号の安全性は、通常、ハミング重みに対するシンドローム復号（Syndrome Decoding、SD）問題の困難性に依存している。最も優れた汎用アルゴリズムは、いずれも Prange による古いアルゴリズムの改良版であり、Information Set Decoding (ISD) アルゴリズムの名で知られている。

本論文では、基礎となる重み関数と SD のアルファベットサイズを変更することにより、ISD アルゴリズムの適用範囲を拡大することが目的である。より正確には、ISD の枠組みで Wagner のアルゴリズムを使うことで、広範囲の重み関数に対する SD を解く方法が示される。また、ISD アルゴリズムの漸近的な複雑さを、古典的な場合と量子的な場合の両方について計算される。次に、現在注目されている Lee 測度に対して、著者らの結果が適用される。復号が最も困難と思われる Lee ウェイトに対する SD のパラメータを提供することにより、著者らの研究は、特に量子敵対者に対する符号ベースの暗号システムの設計とその安全性解析に対するいくつかの応用を持つことが報告される。

・Improving Thomae-Wolf Algorithm for Solving Underdetermined Multivariate Quadratic Polynomial Problem [PQCrypto 2021]

Hiroki Furue, Shuhei Nakamura and Tsuyoshi Takagi

多変数二次多項式問題（MQ 問題）は、ポスト量子暗号における基本的な計算問題である。有限体 Fq 上の n 変数における m 個の二次多項式の MQ 問題を MQ(q, n, m)と表す。PKC 2012 では、Thomae と Wolf により、劣決定（すなわち n>m の場合）の $MQ(2^r, n, m)$を解く効率的なアルゴリズムが提案された(TW アルゴリズム)。具体的には、α 個の二次多項式の交差積項を線形化により除去することで、$MQ(2^r, n, m)$は $MQ(2^r, m - k - \alpha, m - \alpha)$（k は TW アルゴリズム適用後のハイブリッドアプローチで固定される変数の数）に還元することが可能である。そして、このアルゴリズムは、α のうち最大の線形化係数$\alpha = \lfloor n/m \rfloor - 1$に対して最小の MQ 問題をもたらす。

本論文では、ハイブリッドアプローチと TW アルゴリズムを組み合わせることにより、線形化係数 α を改善するアルゴリズムが提案される。提案アルゴリズムは、$MQ(2^r, n, m)$を、線形化係数$\alpha_k = \lfloor (n-k)/(m-k) \rfloor - 1$で、$MQ(2^r, m\text{-}k\text{-}\alpha_k, m\text{-}\alpha_k)$に削減することが可能である。$\alpha_k \geq \alpha$ なので、提案アルゴリズムはいくつかのパラメータセットに対して TW ア

ルゴリズムよりも効率的である。さらにバイナリケース（r = 1）の場合に、自明ではない改良されたアルゴリズムを提供し、適切な k に対してより大きな線形化係数$\beta_k = \lfloor (n-1)/(m-k-1) \rfloor - 1$を与える。

・Quantum Key Search for Ternary LWE [PQCrypto 2021]

Iggy van Hoof, Elena Kir shanova, Alexander May

3 値 LWE（ternary LWE）、すなわち秘密と誤差ベクトルの係数を{-1, 0, 1}から取った LWE は、NTRU 型暗号や BLISS や GLP などの一部の署名方式でよく使われている。

本論文は、3 値 LWE に対する量子組み合わせ攻撃について検討する。提案アルゴリズムは、Magniez-Nayak-Roland-Santha の量子ウォークの枠組みをベースに、部分和問題のアルゴリズムに登場する表現技法（representation technique）と呼ばれる組合せ論的な手法を 3 値 LWE に適用している。LWE 鍵の探索空間を S で表すと、表現攻撃の漸近的計算量は $S^{0.24}$（古典）から $S^{0.19}$（量子）にまで低下する。これは、NTRU-HRSS [CHES'17]や NTRU Prime [SAC'17]などの具体的な NTRU インスタンスに対する顕著な攻撃速度の向上となる。提案されたアルゴリズムは、NTRU や他の 3 値 LWE ベースのスキームの現在の安全性を損なうものではないが、LWE に対するハイブリッド攻撃内部の組み合わせサブルーチンの改良のための基礎となりうる。

・A Fusion Algorithm for Solving the Hidden Shift Problem in Finite Abelian Groups [PQCrypto 2021]

Wouter Castryck, Ann Dooms, Carlo Emerencia, Alexander Lemmens

有限アーベル群 G における隠れシフト問題に関する論文である。

2014 年の Friedl, Ivanyos, Magniez, Santha and Sen による結果から、任意の（小さな）固定整数 m > 0 に対して、任意の有限アーベル群 G における隠れシフト問題を時間計算量$poly(log$ |

・Generating Cryptographically-Strong Random Lattice Bases and Recognizing Rotations of Z^n [PQCrypto 2021]

Tamar Blanks, Stephen Miller

格子暗号は、完全な簡約が困難なランダムな基底の生成に依存している。

本論文では、GL(n, Z)のランダムな要素をサンプリングする様々な方法の強さを比較し、Z^n 格子を回転として捉える問題に関して、ある方法が他の方法より強いことを発見した。特に、（Magma の RandomSLnZ コマンドで実装されている）ユニポテント行列を掛け合わせる標準的なアルゴリズムにより生成されるものは、1,500 に近い次元でもこの最後の問題のインスタンスで効率的に破ることができる。また、NIST のポスト量子暗号コンペティションに提出されたランダム基底生成法(DRS)も効率的に破ることができる。

・An Algebraic Approach to the Rank Support Learning Problem [PQCrypto 2021]

Magali Bardet, Pierre Briaud

階数距離符号ベースの暗号は、階数距離においてランダムな線形符号の復号が困難であることに依存している。その変種である階数サポート学習問題（Rank Support Learning, RSL）とは、同じサポートをエラーとして持つ N 個の復号インスタンスに攻撃者がアクセスし、そのうちどれか 1 つを解こうとするものである。この問題は Durandal 署名方式で用いられている。

本論文では、この問題を解くために、従来の攻撃を明らかに上回る RSL に対する代数的な攻撃を提案する。本論文では、MinRank と RD を解くために同様の技術を用いた既存研究を基に、RSL に対する代数的攻撃を提案する。しかしながら、著者らの分析はより単純であり、したがってその攻撃は標準的な Gröbner 基底攻撃と比較して非常に単純な仮定に依存する。また、Durandal に対する鍵回復攻撃は、これまで考えられていたよりもはるかに効率的であることも、本研究で示唆された。

・Towards faster polynomial-time lattice reduction [CRYPTO2021]

Paul Kirchner, Thomas Espitau, Pierre-Alain Fouque

LLL アルゴリズムは、指数関数的な近似係数を持つ d 次元格子を簡約する多項式時間アルゴリズムである。現在、最も効率の良い Neumaier and Stehl'e による LLL の変形は、$d^4 \cdot B^{1+o(1)}$ (B はエントリのビット長)の理論実行時間を持っているが、実装されてはいなかった。

本論文では、漸近的に高速な並列かつヒューリスティックな削減アルゴリズムとその最適化実装が紹介される。このアルゴリズムは再帰的であり、高速なブロック行列の乗算を十分に利用することができる。再帰的ステップで浮動小数点精度を注意深く制御す

ることにより、ランク d のユークリッド格子を時間 $\tilde{O}(d^{\omega c})$ 、すなわちほぼ一定数の行列乗算で削減できることを実験的に実証した。ここで、ω は行列の乗算の指数、C は行列の条件数の対数である。これにより、最新実装 fplll の実行時間が$d^2 \cdot B$のオーダー倍で改善される。さらに、ナップザック格子と呼ばれる構造的格子（structured lattice）を、漸近的な簡約により、時間 $\tilde{O}(d^{(\omega-1)c})$で削減することができることを示す。他にも著者らの実装は、4 百万ビットを持つ 2230 次元の大きな整数に基づく完全準同型暗号方式のいくつかのインスタンスを破ることができる。

・On Bounded Distance Decoding with Predicate: Breaking the "Lattice Barrier" for the Hidden Number Problem [Eurocrypt 2021]

Martin R. Albrecht, Nadia Heninger

暗号解読における格子ベースのアルゴリズムは、整数の線形制約を満たすターゲットベクトルを、ある格子における最短または最接近のベクトルとして探索することが多い。本研究では、これらの定式化が、ターゲットベクトルが一意に近い、あるいは短いとは言い難い場合でも、ターゲットベクトルを区別するために用いることができる基礎となるアプリケーションからの非線形情報を破棄する可能性があることを観察する。著者らは、ターゲットベクトルを区別する述語による格子問題の定式化を行い、これらの問題のインスタンスを解くためのアルゴリズムを提供する。本技術をサイドチャネル攻撃で DSA や ECDSA の秘密鍵を復元する際によく用いられる秘匿数問題の格子ベースの解法に適用し、これまで格子アプローチでは解けないと考えられていた事例でも本アルゴリズムが署名鍵の復元に成功することを実証する。また、著者らの推定・解法フレームワークを用いた広範な実験を行い、その結果も併せて公開する。

・On the ideal shortest vector problem over random rational primes [Eurocrypt 2021]

Yanbin Pan, Jun Xu, Nick Wadleigh, Qi Cheng

数体における非自明なイデアルは素イデアルの積に分解できる。本論文では、素イデアルの最短ベクトル問題（SVP）の計算量とその分解群の間の関係性について研究する。得られた結果を、二べきの円分体など、格子に基づく暗号システムでよく用いられる数体に適用したところ、有理素数（rational prime）の大部分は、SVP の多項式時間アルゴリズムを認める素イデアルに属することが示された。理想格子の最短ベクトル問題は Ring-LWE 暗号の安全性を支えているが、安全性の低下は最悪の場合の理想 SVP から平均的な場合の Ring-LWE への一方通行であるため、この研究は Ring-LWE を破るものではない。

・Relationships between quantum IND-CPA notions [TCC 2021]

Tore V. Carstens, Ehsan Ebrahimi, Gelo N. Tabia, Dominique Unruh

攻撃者が選んだ 2 つのメッセージの暗号を見分けることができない安全性、選択平文攻

撃に対する識別不可能性（indistinguishable under chosen plaintext attack、IND-CPA）と呼ばれる。この定義には他のバリエーションがあるが、古典的なケースではすべて等価であることがわかっている。

本論文では、対称型暗号化方式における IND-CPA の様々な定義について、量子環境下での包括的な概観を示している。また、これらの概念の関係を調査し、これらの概念の間の様々な等価性、含意、非等価性、非含意についての証明が行われる。

・A Geometric Approach to Linear Cryptanalysis [Asiacrypt 2021, Award Paper]

Tim Beyne

線形暗号解読の新解釈を提案する。「幾何学的アプローチ」（geometric approarch）は、線形暗号解読のすべての一般的なバリエーションを統一し、様々な特性の間のリンクを明らかにし、さらなる一般化を提案する。例えば、相関行列の非実数固有値に対応する不変量に対する新しい洞察や、ゼロ相関攻撃と積分攻撃の間のリンクの一般化が得られる。幾何学的直感は、固定鍵による piling-up 原理の動機付けにつながり、これは不変量と線形近似に関連する過去の結果の説明と一般化によって説明される。ランク 1 近似は、セル指向暗号（cell-oriented cipher）を分析するために提案され、FSE 2019 で Beierle、Canteaut、Leander によって提起された未解決問題を解決するために使用される。特に、そのような近似がリーマン最適化を用いて自動的に解析される方法を示す。

資料３－３

ディジタル署名アルゴリズム EdDSA について

１．　背景

2020 年度第 1 回暗号技術検討会において、 EdDSA の安全性評価を暗号技術評価委員会において行うことが審議・承認され、暗号技術評価委員会にて外部評価を実施し、2020 年度第 2 回暗号技術検討会にて報告された。安全性評価の結果としては、曲線に関する安全性および方式の構成に関する安全性いずれについても安全性に問題はないと報告されている。

2021 年度第 1 回暗号技術評価委員会にて、EdDSA について、事務局選出の暗号アルゴリズムとして CRYPTREC 暗号リストへの追加を視野に入れ、外部評価による実装性能評価を実施することが承認された。

２．　外部評価実施報告

- 本年度実施した外部評価

  ディジタル署名アルゴリズム EdDSA の実装性能調査

  内容：EdDSA 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等の調査

  依頼先：菅野　哲 様 (株式会社インフォーズ (現：株式会社イエラエセキュリティ))

外部評価報告書本体は、第 2 回暗号技術評価委員会配布資料 別紙４－１「ディジタル署名アルゴリズム EdDSA の実装性能調査」に掲載。

- 調査・評価概要
  - 特徴
    - EdDSA は ECDSA と同様に射影座標系を使用可能であるため、有限体上の乗法逆元の演算を用いずに演算可能であることから、高速な実装が可能である。
    - EdDSA で推奨される twisted-Edwards 曲線は無限遠点を例外的に扱うための分岐が不要なため、ECDSA で使われる Weierstrass 形式の楕円曲線と比較して実装しやすい。
    - EdDSA で推奨される Edwards 楕円曲線は，異なる点の加算と同一の点の加算(2 倍算)を同じ処理で計算できるため、実装するアルゴリズムが 1 つでよく、点が異なるかどうかの条件分岐を考慮する必要がないため，Weierstrass 形式の楕円曲線と比較して Side Channel Attack（SCA）対策に有利である。
  - 性能測定結果

    C 言語　4 種類、Java　2 種類の OSS の暗号ライブラリを Windows、Linux、Mac

の 3 つの OS 上でそれぞれ動かした計 18 種類の環境で実際に性能測定を行い、各環境の結果は以下のようになった。

- Ed25519
  - 鍵ペア生成
    - 17 環境で ECDSA P-256 より高スループットだった。
    - 1 環境では ECDSA P-256 より低スループットだったが 50%未満の極端な差はなかった。
  - 署名生成
    - 12 環境で ECDSA P-256 より高スループットだった。
    - 6 環境では ECDSA P-256 より低スループットだったが 50%未満の極端な差はなかった。
  - 署名検証
    - 15 環境で ECDSA P-256 より高スループットだった。
    - 3 環境では ECDSA P-256 より低スループットだったが 50%未満の極端な差はなかった。
- Ed448
  - 鍵ペア生成
    - 15 環境で ECDSA P-384 より高スループットだった。
    - 3 環境では ECDSA P-384 より低スループットだったが 50%未満の極端な差はなかった。
    - 18 環境で ECDSA P-521 より高スループットだった。
  - 署名生成
    - 15 環境で ECDSA P-384 より高スループットだった。
    - 3 環境では ECDSA P-384 より低スループットだったが 50%未満の極端な差はなかった。
    - 18 環境で ECDSA P-521 より高スループットだった。
  - 署名検証
    - 15 環境で ECDSA P-384 より高スループットだった。
    - 3 環境では ECDSA P-384 より低スループットだったが 50%未満の極端な差はなかった。
    - 18 環境で ECDSA P-521 より高スループットだった。

- 性能測定結果から得られた見解
  - 公開されている第三者の測定結果および本調査による測定結果の範囲では、

Ed25519 は ECDSA P-256 と同等の安全性でありながら高速であると評価でき、Ed448 は ECDSA P-384 より高い安全性でありながら同等または高速であると評価できる。

- 標準化での採用状況
  - RFC8032 [1]として標準化され，Draft 版を含め参照する標準も増えつつあることが明らかとなった。

EdDSA は、方式そのものに安全性担保、高速化、実装がしやすい特性があると評価でき、実際に OSS として実装された暗号ライブラリの性能は、同程度の安全性の ECDSA や高い安全性の ECDSA と比べても遜色のないものであった。実装された OSS の品質、高速化技法は洗練されているとは言い切れない部分もあるが、歴史のある ECDSA と比べても性能で劣ることはないと考えられる。

- 暗号技術評価委員会としての見解

  EdDSA は ECDSA と同様に射影座標を用いた計算効率の良い演算が用意されているなどの実装において有益な性質を持つと考えられる。また、ECDSA と比較しても遜色ない処理速度である。よって、ディジタル署名 EdDSA は、ECDSA と比較しても遜色ない十分な実装性能を有していると判断した。

３．　CRYPTREC 暗号リストへの追加について

CRYPTREC 暗号リストへ追加するためには、安全性評価および実装性能評価を実施する必要がある。ディジタル署名 EdDSA については、2020 年度に安全性評価を実施し、今年度実装性能評価を実施した。

3.1. 安全性評価

2020 年度に外部評価を実施し、暗号技術評価委員会として下記の見解を得ている。

- 曲線に関する安全性評価について

  EdDSA での使用が見込まれる二つの曲線 Curve25519 及び Curve448 における ECDLP に対する古典計算機（従来の計算機）を用いた現時点での最良のアルゴリズムは ρ 法であるため、その安全性は現在使用されている楕円曲線暗号の場合と同じく、結果として主に基礎体の大きさで決定される。従って、Curve25519 の場合はほぼ 128 ビットセキュリティ、 Curve448 の場合はほぼ 224 ビットセキュリティの安全性を持つと判断する。また、それらの曲線上の演算も効率よく実行できることを確認した。

- 方式の構成に関する安全性評価について

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

3.2. 実装性能評価

本年度、実装性能に関する調査・評価を実施した。詳細は２章に報告の通り。

3.3. 暗号技術評価委員会としての見解

ディジタル署名 EdDSA について 2020 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は、いずれの結果も CRYPTREC 暗号リストに追加するために必要となる要件を満たしていると判断し、下記のように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：文書番号 CRYPTREC LS-0001-2012R6、https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r6.pdf）に追加することを暗号技術検討会に提案することを決定した。

追加先：推奨候補暗号リスト

技術分類：「大分類：公開鍵暗号」、「中分類：署名」

以上

[参考文献]

[1] Internet Research Task Force (IRTF), “RFC8032 Edwards-Curve Digital Signature Algorithm (EdDSA),” 2017.

資料３－４

2021 年度暗号技術調査 WG（耐量子計算機暗号）活動報告

1. 2021 年度暗号技術調査 WG（耐量子計算機暗号）活動報告の概要

2020 年度第 2 回暗号技術検討会において、耐量子計算機暗号ガイドラインを作成するために暗号技術調査ワーキンググループ(耐量子計算機暗号)(以下:PQC WG)を設置することが承認された。2021 年度第 1 回暗号技術評価委員会において、PQC WG において下記 2 点について実施することが承認された。

(1) 耐量子計算機暗号の研究動向調査をもとに、主要な耐量子計算機暗号についてのガイドラインを 2021 年度から 2022 年度にかけて作成する。

(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」の予測図を更新する。

2. 委員構成（敬称略）

主査：國廣 昇（筑波大学）
委員：青木 和麻呂（文教大学）
委員：伊藤 忠彦 （セコム）
委員：草川 恵太（NTT）
委員：下山 武司（国立情報学研究所）
委員：高木 剛（東京大学）
委員：高島 克幸（早稲田大学）
委員：廣瀬 勝一 （福井大学）
委員：安田 貴徳（岡山理科大学）
委員：安田 雅哉（立教大学）

3. 耐量子計算機暗号ガイドラインの作成

3.1. スケジュール（第 1 回暗号技術評価委員会で承認）

年度	回	耐量子計算機暗号ガイドラインの議論・決定・報告
2021 年度	第 1 回 (9 月初旬頃を想定)	✓ 記載すべき項目及びその章立てを議論 ✓ 記載する暗号方式の選定基準を議論 ✓ 記載する暗号方式の候補を議論 ✓ 執筆担当者を議論
	第 2 回 (2 月を想定)	✓ 章立ての決定 ✓ 記載する暗号方式の選定基準の決定 ✓ 記載する暗号方式の候補の決定 ✓ 執筆担当者の決定
2022 年度	第 1 回 (8 月下旬頃を想定)	執筆内容の中間報告
	第 2 回 (2 月を想定)	執筆内容の最終報告

3.2. 第 1 回 WG（9/7）での実施内容及び決定事項

- ガイドライン及び調査報告書の作成

  ガイドラインは暗号理論に精通していない利用者を、調査報告書は暗号理論の研究者や技術者を対象とする。そのため、基本的にはガイドラインは調査報告書から技術的詳細を省き、その一部を抜粋したものする。ただし、暗号理論に精通していない利用者のために、PQC の活用方法をガイドラインでは記載し、調査報告書には記載しない。

- 記載すべき項目及び章立てと執筆担当者

	執筆担当者
i. はじめに	事務局（青野、篠原、高安）
ii. PQC の活用方法（ガイドラインのみ）	伊藤委員（ガイドラインのみ）
iii. 格子に基づく暗号技術	下山委員、安田（雅）委員、事務局（青野）
iv. 符号に基づく暗号技術	草川委員
v. 多変数多項式に基づく暗号技術	安田（貴）委員
vi. 同種写像に基づく暗号技術	高島委員
vii. ハッシュ関数に基づく署名技術	廣瀬委員

- ガイドライン及び調査報告書に記載する暗号方式の選定基準及び候補について

  公開鍵暗号を中心にまとめる。主要な暗号方式（NIST PQC 標準化への提案方式等）を記載するが、対象となる暗号方式は執筆担当者が選定する。

- 2021 年度第 2 回 PQC WG での調査内容の報告について
  各章の執筆担当者が 2021 年度第 2 回 PQC WG において、その時点までの調査内容を報告する。

3.3. 第 2 回 WG (1/28) での実施内容及び決定事項

- 調査内容の報告について
  各章の執筆担当者が 2021 年度第 2 回 PQC WG において、その時点までの調査内容を報告した。
- ガイドライン及び調査報告書の執筆方針について
  ガイドライン及び調査報告書の執筆方針が本 WG において決定された。
  - ガイドライン及び調査報告書の章立て
    i. 導入
    ii. PQC の活用方法（ガイドラインにのみ記載）
    iii. 格子に基づく暗号技術
    iv. 符号に基づく暗号技術
    v. 多変数多項式に基づく暗号技術
    vi. 同種写像に基づく暗号技術
    vii. ハッシュ関数に基づく署名技術
  - iii 章以降の構成（A 章の場合）
    A.1. 安全性の根拠となる問題の説明（例：LWE 問題、シンドローム復号問題）
    A.2. 代表的な暗号方式の構成法（例：Regev 暗号、McEliece 暗号）
    A.3. 主要な暗号方式
    A.3.1. 暗号方式 1（例：CRYSTALS-KYBER, Classic McEliece）
    A.3.2. 暗号方式 2
    A.3.3. 暗号方式 3
    ・・・
    A.4. まとめ

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」の予測図の更新

素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関する計算量評価に大幅な進展はなかったため、2021 年 6 月・11 月のベンチマーク結果を追加して予測図の更新を行った（図 1, 2）。

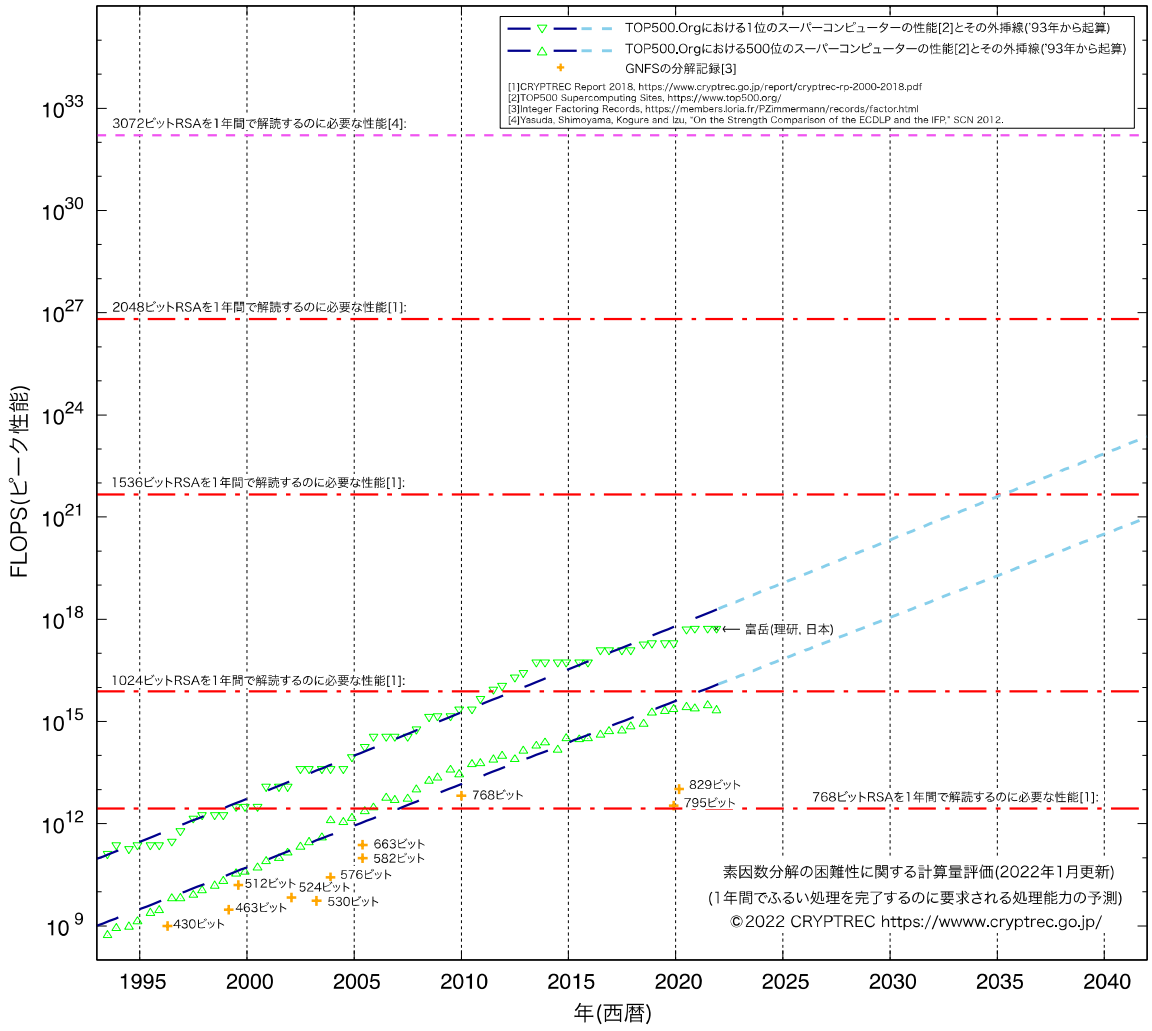


図 1：素因数分解の困難性に関する計算量評価（2022 年 1 月更新）

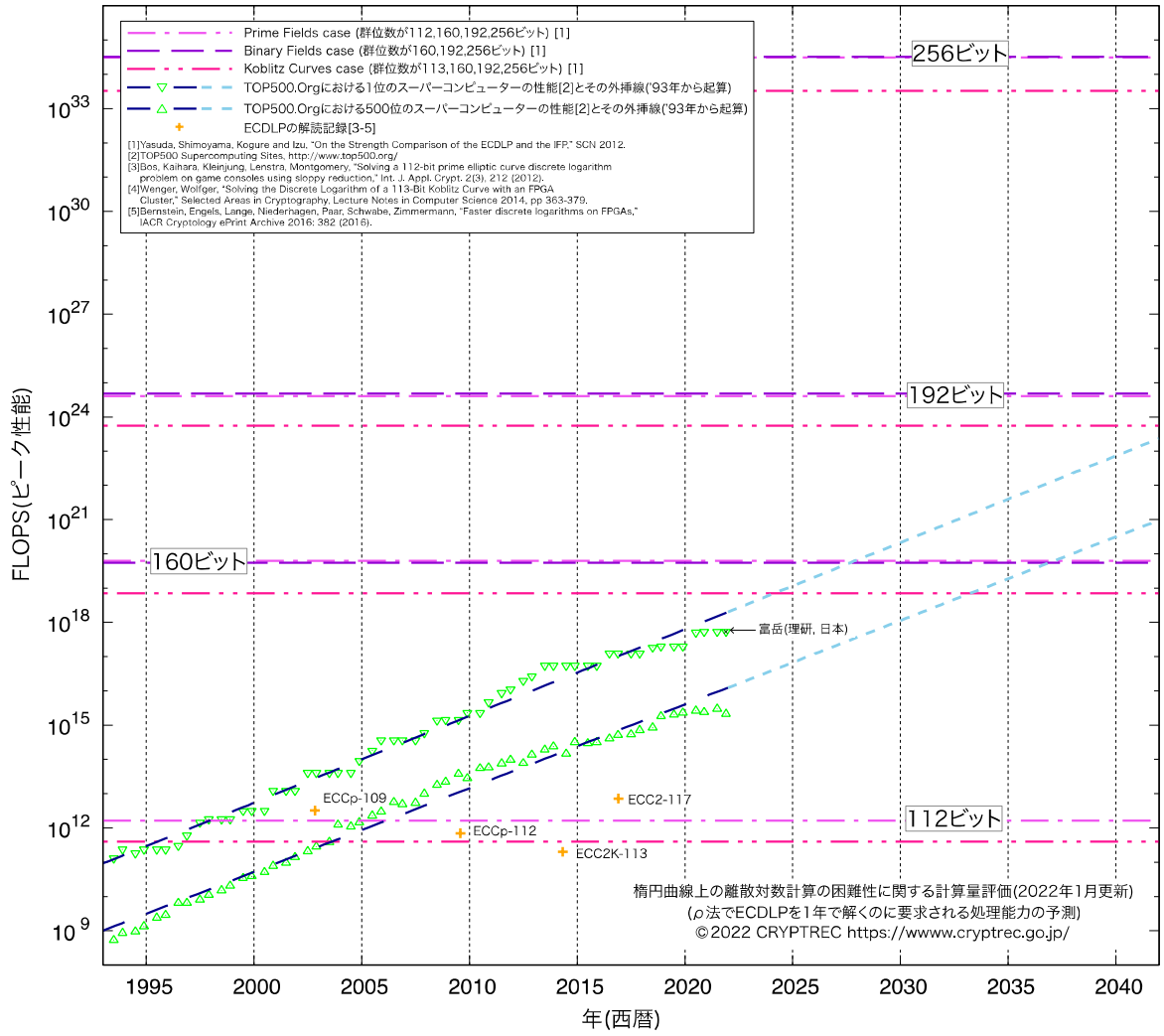


図 2：楕円曲線上の離散対数計算の困難性に関する計算量評価(2022 年 1 月更新)

以上

資料３－５

2021 年度暗号技術調査WG（高機能暗号）活動報告

1. 暗号技術調査WG（高機能暗号WG）の活動目的

高機能暗号の研究動向調査をもとに、高機能暗号ガイドラインを 2021 年度、2022 年度において作成する。

2. 委員構成（敬称略）

主査：四方 順司　　（横浜国立大学）
委員：金岡 晃　　（東邦大学）
委員：国井 裕樹　　（セコム）
委員：須賀 祐治　　（インターネットイニシアティブ）
委員：花岡 悟一郎　　（国立研究開発法人産業技術総合研究所）
委員：外園 康智　　（野村総合研究所）
委員：米山 一樹　　（茨城大学）

3. 2021 年度暗号技術調査WG（高機能暗号）活動報告の概要

3.1. 背景

公開鍵暗号は、アプリケーションが多様となりその活用が広まっている。その中で、従来の公開鍵暗号よりも機能が向上した高機能暗号を利用してアプリケーションに適用することが有効と考えられている。そこで、2020 年度第 2 回暗号技術検討会において高機能暗号ガイドラインを作成するために高機能暗号WGを設置することが承認された。

そして、2021 年度暗号技術評価委員会において、2021 年度の高機能暗号WGの活動として下記 3 点について実施する活動計画が承認された。

(1) 高機能暗号のスコープの明確化
(2) 高機能暗号技術に関する現状調査
(3) 高機能暗号のアプリケーションに関する調査

3.2. 活動概要

2021 年度活動計画に沿い、年 3 回の高機能暗号WGを以下の通り開催した。開催日と各WGでの活動内容は以下の通り。

(1) 第 1 回高機能暗号WG（2021 年 8 月 3 日）
　(ア) 高機能暗号のスコープの議論
　(イ) 高機能暗号技術に関する現状調査について作業方針・分担を議論
　(ウ) 高機能暗号のアプリケーションに関する現状調査について作業方針・分担を議論
　(エ) 高機能暗号のアプリケーションについて、エンドユーザのヒアリング先の検討
(2) 第 2 回高機能暗号WG（2021 年 12 月 8 日）
　(ア) 現状調査・アプリケーションに関する中間報告
　(イ) ヒアリングに関する中間報告
　(ウ) ガイドラインの目次案についての議論

(3) 第 3 回高機能暗号WG（2022 年 2 月 8 日）

(ア) 2021 年度高機能暗号WG報告資料の確認

(イ) 2021 年度調査内容の確認

(ウ) ガイドラインの執筆方針に関する確認

(エ) 2022 年度の検討項目の抽出および方針決定

4. 高機能暗号のスコープの明確化

「高機能暗号」に対して一般的に合意されている定義がない。そこで、本ガイドラインで記載する高機能暗号が何を指すものか定義する必要がある。このため、第 1 回高機能暗号WGにおいて、本ガイドラインで扱う高機能暗号のスコープを議論した。

そして、本ガイドラインでは、高機能暗号を「従来の暗号技術に対して、機能が追加・向上されるなどの優位性を主張する暗号、および、従来の暗号技術では困難であった事象を解決できるなどの新規機能を有することを主張する暗号技術」とした。ただし、今後の議論により修正が必要な場合は、WGにおいて議論し、修正することとした。

5. 高機能暗号の現状調査

高機能暗号に関する現在の活用事例、標準化動向、アルゴリズムを調査し、現状を情報共有するとともに、将来的に利用される可能性がある高機能暗号を精査する。

この調査のため、第 1 回高機能暗号WGにおいて、ガイドラインに掲載する可能性がある高機能暗号を列挙するとともに、高機能暗号を“守秘”、“認証・署名”、“その他”（表 1 分担表の第 1 列参照）に分類した。そして、調査すべき高機能暗号の対象を“ID ベース暗号”、“属性ベース暗号”、“放送型暗号”、“しきい値暗号”、“準同型暗号”、“プロキシ再暗号化”、“ID ベース署名”、“属性ベース署名”、“集約署名・MAC・マルチ署名”、“グループ署名”、“リング署名”、“しきい値署名”、“マルチパーティ計算－秘密分散ベース”、“ゼロ知識証明”、“検索可能暗号”、“Private Information Retrieval”、“Oblivious RAM”、“マルチパーティ計算－Garbled Circuit ベース”の１８項目（表 1 分担表の第 2 列参照）とし、それぞれに対し、“技術”、“活用事例”、“標準化”について調査することとした。

調査は、各WG委員が表 1 の分担表に応じた分担でおこなった。

表 1　分担表（敬称略）

技術分類	暗号技術	技術調査	活用事例調査	標準化調査
守秘	ID ベース暗号	金岡、四方	金岡、四方	金岡、四方
	属性ベース暗号	四方	四方	四方
	放送型暗号	花岡	花岡	花岡
	しきい値暗号	米山	米山	米山
	準同型暗号	四方	外園、四方	外園、四方
	プロキシ再暗号化	花岡	花岡	花岡
認証・署名	ID ベース署名	金岡、四方	金岡、四方	金岡、四方
	属性ベース署名	四方	四方	
	集約署名　MAC マルチ署名	四方	須賀、四方	須賀、四方
	グループ署名	米山	国井	国井
	リング署名	米山	須賀	須賀
	しきい値署名	国井	国井	国井
その他	マルチパーティ計算（秘密分散ベース＋汎用性）	花岡	須賀、花岡、外園	須賀、外園
	ゼロ知識証明	外園	国井、外園	国井、外園
	検索可能暗号（公開鍵・共通鍵）	米山	金岡	金岡
	Private Information Retrieval	須賀	須賀	須賀
	Oblivious RAM	米山	米山	米山
	マルチパーティ計算（Garbled Circuit ベース）	花岡	花岡	花岡

6.　高機能暗号のアプリケーションに関する調査

既存技術より効率的になる分野、既存技術でカバーできていない分野などで、高機能暗号の活用が期待される分野を整理する。このため、より深くアプリケーション、応用例を知るため、エンドユーザのヒアリングを検討する。そして、高機能暗号WG委員によるメール審議、および、第 3 回高機能暗号WGにおいて、以下の 4 件の候補を決定した。

① 秘密分散を利用した医療データ活用（NEC×大阪大学）
② 検索可能暗号&属性ベース暗号（三菱電機）
③ 属性ベース暗号を利用した放送サービスの拡張（JSAT）
④ マルチパーティ計算を利用した秘密情報秘匿したデータ分析（ZenmuTech）

このうち、2 件を選び、2022 年度にヒアリングを行うこととした。ヒアリングは、2022 年度の第 1 回、第 2 回高機能暗号WGにおいて、発表、質疑形式で行う予定である。

7. ガイドライン目次案

3回のWGを通じて、ガイドラインの目次に関する議論を行い、以下のように決定した。

目次案の議論において、現状調査の対象となった暗号技術の中で、ＩＤベース署名と、しきい値暗号については、関連する応用例、標準化等を考えたとき、その活動が少なく、それぞれ、ＩＤベース暗号と、しきい値署名の中にマージして扱うこととした。

この目次案については、今後の議論により修正が必要な場合は、WGにおいて議論し、修正することとした。

目次案

1. はじめに
2. 高機能暗号技術とその活用法
   - 2.1 高機能暗号とは
   - 2.2 高機能暗号の種類と分類
   - 2.3 高機能暗号はどこに使えるか、その有用性
   - 2.4 高機能暗号の活用例と効果
     - 2.4.1 守秘関連の活用事例
     - 2.4.2 認証・署名関連の活用事例
     - 2.4.3 その他の高機能暗号の活用事例
3. 主な高機能暗号技術のアルゴリズム・プロトコルとその性能
   - 3.1 守秘
     - 3.1.1 ＩＤベース暗号
     - 3.1.2 属性ベース暗号
     - 3.1.3 放送型暗号
     - 3.1.4 準同型暗号
     - 3.1.5 プロキシ再暗号化
   - 3.2 認証・署名
     - 3.2.1 属性ベース署名
     - 3.2.2 集約署名、ＭＡＣ、マルチ署名
     - 3.2.3 グループ署名
     - 3.2.4 リング署名
     - 3.2.5 しきい値署名
   - 3.3 その他
     - 3.3.1 マルチパーティ計算～秘密分散ベース～
     - 3.3.2 マルチパーティ計算～Garbled Circuit ベース～
     - 3.3.3 ゼロ知識証明
     - 3.3.4 検索可能暗号
     - 3.3.5 Private Information Retrieval（PIR）
     - 3.3.6 Oblivious RAM（ORAM）
4. おわりに

8. 2022 年度の活動予定

2022 年度は、2021 年度に設定した目次案に沿って、それぞれの項目の執筆を行う。このため年 3 回の高機能暗号WGを開催する。

第 1 回、第 2 回の高機能暗号WGでは、ヒアリングを行う。ヒアリング内容は、ガイドラインに反映する。

2021 年度に決定した高機能暗号ガイドライン執筆方針に従い、2022 年度末までに高機能暗号ガイドラインを作成する。

以上

資料３－６

軽量暗号に関する技術動向調査について

１．　目的

2020 年度第 2 回暗号技術検討会にて、2016 年度に作成した「CRYPTREC 暗号技術ガイドライン（軽量暗号）」の更新のため、2021 年度は、掲載されている暗号方式に関わる安全性解析について、2017 年度以降の技術動向調査を行い、2023 年度中を目途に現ガイドラインを更新することが承認された。

2021 年度第 1 回暗号技術評価委員会にて、2017 年度以降の技術動向調査の具体的な進め方について、2 章に示す調査対象および実施方法により行うことが承認された。

本資料では、上記承認された実施対象・実施方法により行った技術動向調査について報告する。

２．　実施概要

近年の軽量暗号に関わる技術動向調査を下記のとおり実施した。技術動向調査報告書については、３章を参照のこと。調査報告書レビューについては、４章を参照のこと。技術動向調査報告書本体は、第 2 回暗号技術評価委員会配布資料 別紙２－１に掲載。調査報告書レビュー本体は、第 2 回暗号技術評価委員会配布資料 別紙２－２に掲載。

- 調査対象
  - 2017 年 3 月に公開した「CRYPTREC 暗号技術ガイドライン（軽量暗号)」に掲載されている方式について、2017 年 3 月以降に大幅な安全性の劣化につながる脆弱性が見つかっているか否かについて調査。
  - 軽量暗号に関わる ISO/IEC 29192 シリーズに近年採録されたもしくは採録される予定の方式について、「CRYPTREC 暗号技術ガイドライン（軽量暗号)」における掲載の有無およびそれらの安全性について調査。
  - 「CRYPTREC 暗号技術ガイドライン（軽量暗号)」公開時に CAESAR プロジェクトが終了していなかったことから、CAESAR プロジェクトで最終的に選ばれたポートフォーリオ 6 方式について、「CRYPTREC 暗号技術ガイドライン（軽量暗号)」における掲載の有無およびそれらの安全性について調査。
- 実施方法
  - 調査報告書の執筆：事務局
  - 調査報告書レビュー：峯松　一彦　様（日本電気株式会社）

［選出理由］「CRYPTREC 暗号技術ガイドライン（軽量暗号）」作成時に主として認証暗号の分野をご担当頂いた方であり、認証暗号に関わる幅広い知識をお持ちであるため。

３．　「CRYPTREC 暗号技術ガイドライン（軽量暗号）」掲載の暗号方式に関する安全性評価の動向調査報告

３．１．　目的

2016 年度ガイドラインで紹介された暗号方式を中心とした代表的な軽量暗号の安全性評価に関する動向調査を行うことを目的とし、2021 年 9 月の時点でこれらの軽量暗号に対して脅威に繋がる脆弱性が指摘されているか否かを明らかにする。

３．２．　本報告書の構成

第 1 章：本報告書の目的と構成概要
第 2 章：調査結果の概要
第 3 章：軽量ブロック暗号の安全性解析状況に関する調査結果（10 方式）
- CLEFIA、LED、Midori、Piccolo、PRESENT、PRINCE、Simon、Speck、TWINE、LEA

第 4 章：軽量ストリーム暗号の安全性解析状況に関する調査結果（5 方式）
- ChaCha、Enocoro、Grain v1、MICKEY 2.0、Trivium

第 5 章：軽量ハッシュ関数の安全性解析状況に関する調査結果（5 方式）
- Keccak、PHOTON、QUARK、SPONGENT、Lesamnta-LW

第 6 章：軽量 MAC の安全性解析状況に関する調査結果（4 方式）
- SipHash、Chaskey、LightMAC、Tsudik’s keymode

第 7 章：軽量認証暗号の安全性解析状況に関する調査結果（14 方式）
- ACORN、ASCON、AES-JAMBU、AES-OTR、CLOC and SILC、Deoxys、Joltik、Ketje、Minalpher、OCB、PRIMATEs、AEGIS、COLM、Grain-128A

３．３．　調査方法

（１）2016 年度ガイドラインの公開時点における安全性解析状況を明らかにした。
（２）代表的な軽量暗号の安全性評価に関する動向調査を行い、2021 年 9 月の時点で現実的な脅威に繋がる脆弱性が指摘されているか否かを明らかにした。
- 攻撃可能段数、攻撃種別、計算量、データ量、メモリ量、参考文献について表にまとめた。

- 表から、攻撃可能段数が多い、かつ、計算量が少ない攻撃を最良の攻撃とし、その攻撃方法の概要についてまとめた。

（3）2021 年 9 月現在における安全性解析状況についてまとめた。

３．４．　調査結果の概要

各方式の安全性解析状況について、次のとおり表にまとめた。

	分類１	分類２	分類３
ブロック暗号	CLEFIA、LED、Simon、Speck、LEA	Piccolo、Midori、PRESENT、PRINCE、TWINE	
ストリーム暗号	ChaCha、Enocoro、Trivium		Grain v1、MICKEY 2.0
ハッシュ関数	Keccak、PHOTON、QUARK、SPONGENT、Lesamnta-LW		
MAC	SipHash、Tsudik’s keymode	Chaskey、LightMAC	
認証暗号	ACORN、ASCON、AES-OTR、CLOC and SILC、Deoxys、Joltik、Ketje、Minalpher、OCB1、OCB3、PRIMATEs、AEGIS、$COLM_{127}$	$COLM_0$	OCB2、AES-JAMBU、Grain-128A

分類１：仕様段数において安全性を脅かす攻撃が存在しない方式

- 秘密鍵の全数探索よりも効率的に実行可能な攻撃が存在しない方式
- 安全性基準を脅かす攻撃が存在しない方式

分類２：特定の場合を除き、仕様段数において安全性を脅かす攻撃が存在しない方式

- 秘密鍵の全数探索よりも効率的に実行可能な攻撃が存在しない方式

分類３：仕様段数において安全性基準を満たさない方式

- 秘密鍵の全数探索よりも効率的に実行可能な攻撃が存在する方式
- 安全性基準を脅かす攻撃が存在する方式

４．　CRYPTREC 軽量暗号動向調査報告書に関するレビュー報告

いくつかの軽微な指摘事項を除き、全般的に評価内容は妥当であるとの結論を得た。主だった対応を記す。

- 軽量ブロック暗号の安全性評価において、Biclique 攻撃およびそれと類似した攻撃の扱いに関する懸念があり、妥当と思われる表現について考察
- 軽量ハッシュ関数の評価の表現における修正を提案
- いくつかの方式に関し、既存攻撃論文の評価について修正を提案

５．　調査報告書に対する評価委員会としての見解

調査報告書は、近年の軽量暗号に関わる技術動向調査として十分な内容を含んでいると考えられる。また、有識者によるレビュー内容も調査報告書の妥当性を評価していることから、本報告書を CRYPTREC の技術調査報告書する。

以上

資料３－７

軽量暗号ガイドライン更新方針

１．　背景

CRYPTREC では、2016 年度に「CRYPTREC 暗号技術ガイドライン (軽量暗号)」を公開している。他団体作成のガイドラインで参照された事例[1]などもあり、また今年に入ってからもガイドラインに関する問い合わせが来ていることなどを踏まえ、需要のあるガイドラインであると考えている。一方、軽量暗号に関わる世界の動向としては、いくつか注力すべき動きがある。例えば、CAESAR プロジェクトでは、2014 年の公募以降評価が進み、2019 年 2 月に最終選考に選ばれたポートフォーリオが発表され、3 つのケース各 2 方式、合計 6 方式が採択されている。そのうち 4 方式はすでに現在ガイドラインに掲載されている。また、NIST Lightweight コンペティションでは、2018 年に公募を開始し、1st ラウンド、2nd ラウンドを経て、2021 年 3 月にファイナリスト 10 方式が通過している。こののち、2022 年 5 月 9 日 ～ 11 日にかけて Lightweight Cryptography Workshop 2022 が予定されており、NIST としては、2022 年夏ごろまでを目途に最終結果を発表する予定であると公表している。そのほか、ISO では、軽量ブロック暗号・軽量ハッシュ関数・軽量メッセージ認証コード・軽量認証暗号の技術分類について、ここ数年で新しい方式が複数採択されている、もしシ

以下に更新方針を示す。

- 更新形態

2016 年度版ガイドラインに新規情報を追加・更新した文書を 2023 年度版ガイドラインとして公開する。

- 主たる追加は、2016 年度版ガイドラインの 4 章「代表的な軽量暗号」に相当する軽量暗号方式の紹介とする。
- 既に 4 章に掲載されている方式については、今年度実施した軽量暗号に関する技術動向調査(第 2 回暗号技術評価委員会配布資料 別紙２ - １）を基に更新する。
- 1 章～3 章は、2016 年度版ガイドラインをそのまま用いる。ただし、4 章に新規追加・更新する方式に関わる情報は、適切な章に節を追加し、掲載する。
- 付録を追加し、関連情報を掲載する。

- タイトル
  - 「CRYPTREC 暗号技術ガイドライン (軽量暗号)」2023 年度版

- 追加情報の対象
  - NIST Lightweight コンペティション最終選考で採択された方式
  - 軽量な方式として ISO に近年採録されたもしくは採録される予定の方式

- 主な追加内容
  - 1 章　はじめに
    - ✓ 追記箇所を説明する文章を追加する。
  - 2 章 軽量暗号とその活用法
    - ✓ 節を追加し、2017 年以降の標準化動向を掲載する。
  - 3 章 軽量暗号の性能比較
    - ✓ 節を追加し、 "追加情報の対象"　の方式に関する安全性や実装性能に関わる評価・調査結果 (2022 年度外部評価により実施予定) を掲載する。
  - 4 章 代表的な軽量暗号
    - ✓ 2016 年度版ガイドライン掲載暗号について、今年度実施した軽量暗号に関わる調査報告書（第 2 回暗号技術評価委員会配布資料 別紙２－１）を基に追記・更新する。
      ※更新イメージは、第2回暗号技術評価委員会配布資料 別紙３－１に掲載。
    - ✓ "追加情報の対象"の方式について、掲載方式と同等の情報を掲載する。

(2022 年度外部評価の実施結果を反映する)

※掲載イメージは、第 2 回暗号技術評価委員会配布資料 別紙３－１に掲載。

- 付録(新規)
  - ✓ NIST　Lightweight コンペティションファイナリスト(最終選考で採択されなかった方式)
  - ✓ CAESAR のスケジュールが後ろ倒しにずれ込み、最終選考が完結する前に 2016 年度版ガイドラインを公開することとなった。後に、CAESAR プロジェクトの最終選考により、3 ケース各 2 方式(計 6 方式) が選ばれた。Use case 1: Lightweight applications について選ばれた 2 方式はすでに掲載していたが、Use case 2: High-performance applications および Use case 3: Defense in depth については、2 方式中 1 方式は掲載しているが、各 1 方式は掲載していない。ここで、未掲載の 2 方式を紹介する。
    ※掲載イメージは、第 2 回暗号技術評価委員会配布資料 別紙３－１に掲載。

➢ 編集方法

- 事務局で取りまとめ・編集を行い、更新版を作成し、暗号技術評価委員会にて審議いただく。

３．　スケジュール案

[2021 年度]

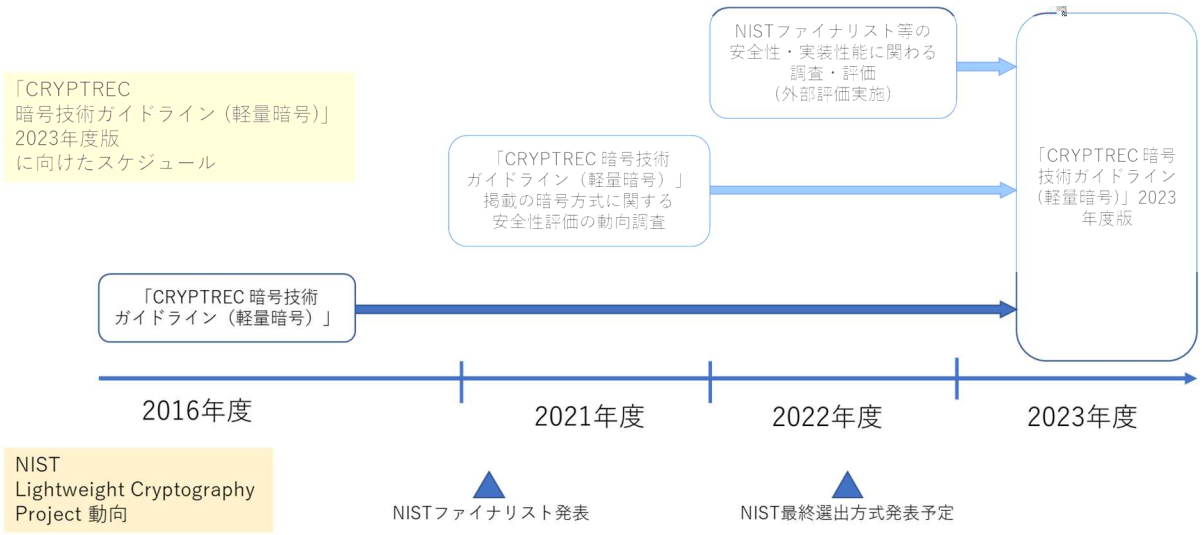
- (済) 2016 年度ガイドライン掲載暗号の 2017 年以降の脆弱性に関わる技術動向調査
- (済) "追加情報の対象"となる ISO に採録された、もしくは採録されることが決定している方式に関する安全性および実装性能に関わる調査
  実施内容については、第 2 回暗号技術評価委員会配布資料 資料２、別紙２－１、別紙２－２に掲載。

[2022 年度]

- NIST Lightweight コンペティションファイナリストを対象とした安全性および実装性能に関わる調査・評価(外部評価により実施)
  (今年度実施した軽量暗号に関する調査報告書に対するレビュー(第 2 回暗号技術評価委員会配布資料 別紙２-２）にて、峯松様から追加対象方式の一つである Tsudik's keymode について、世間での解析論文の少なさを言及頂いていることから、Tsudik's keymode も安全性に関する外部評価の対象方式に含める。)

[2023 年度]

・ 事務局によりガイドラインの更新案を編集し、ドラフト版について外部有識者にガイドラインとして、掲載内容の適切性や情報の過不足などについてレビュー頂き、完成版を暗号技術評価委員会に提出し、審議頂く



- NIST Lightweight ファイナリスト(2021 年 3 月公開)

技術分類	分類	名称
認証暗号&ハッシュ関数	Permutation	ASCON
認証暗号&ハッシュ関数	Permutation	PHOTON-Beetle
認証暗号&ハッシュ関数	Permutation	SPARKLE
認証暗号&ハッシュ関数	Permutation	Xoodyak
認証暗号のみ	Permutation	Elephant
認証暗号のみ	Permutation	ISAP
認証暗号のみ	Block cipher	GIFT-COFB
認証暗号のみ	Tweakable Block cipher	Romulus
認証暗号のみ	Block cipher	TinyJambu
認証暗号のみ	Stream Cipher	Grain-128AEAD

(色は、日本人が提案者に含まれる提案方式)

- ISO 採録方式（予定も含み）

技術分類	番号	名称	備考
ブロック暗号	(ISO/IEC 29192-2)	CLEFIA	
	(ISO/IEC 29192-2)	PRESENT	
	(ISO/IEC 29192-2)	LEA	現行の軽量暗号 GL には未掲載
ストリーム暗号	(ISO/IEC 29192-3)	Enocoro	
	(ISO/IEC 29192-3)	Trivium	
ハッシュ関数	(ISO/IEC 29192-5)	PHOTON	
	(ISO/IEC 29192-5)	SPONGENT	
	(ISO/IEC 29192-5)	Lesamnta-LW	現行の軽量暗号 GL には未掲載
メッセージ認証コード	(ISO/IEC 29192-6)	Chaskey	現行の軽量暗号 GL には未掲載
	(ISO/IEC 29192-6)	LightMAC	現行の軽量暗号 GL には未掲載
	(ISO/IEC 29192-6)	Tsudik's keymode	現行の軽量暗号 GL には未掲載
認証暗号	(ISO/IEC 29192-8)	Grain-128A	現行の軽量暗号 GL には未掲載

- CAESAR project ポートフォーリオ

分類	名称	
Use case 1: Lightweight applications	Ascon	
	ACORN	
Use case 2: High-performance applications	OCB	
	AEGIS	現行の軽量暗号 GL には未掲載
Use case 3: Defense in depth	Deoxys-II	
	COLM	現行の軽量暗号 GL には未掲載

以上

資料４

2021 年度　暗号技術活用委員会活動報告

1.　2021 年度の活動概要

1.1　活動目的

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。

1.2　活動概要

2021 年度の活動概要は以下の通りである。

(1) 利用実績に関する基準検討

CRYPTREC 暗号リストは、電子政府推奨暗号リスト、推奨候補暗号リスト、運用監視暗号リストの 3 つのリストで構成されている。2022 年度に CRYPTREC 暗号リストの改定が予定されており、その際、推奨候補暗号リストから電子政府推奨暗号リストへの昇格にあたって利用実績に基づいた選定が行われることが決まっている[1]。

そこで、昇格のための具体的な利用実績に関する選定基準案を検討・策定する。なお、策定した選定基準案は暗号技術検討会に報告され、改めて審議される。また、利用実績調査は 2022 年度上期に IPA にて実施する計画である。

(2) 「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準《(従来仮称）鍵長設定要件》」及び「暗号鍵設定ガイダンス《(従来仮称）鍵長設定ガイダンス（一般用)》」の作成

安全な暗号利用に係る運用ガイドラインとして、2020 年度の検討結果を踏まえて取りまとめた作成方針に基づき、2 つの鍵長に関するドキュメントを作成した。

一つは、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準《(従来仮称）鍵長設定要件》」である。これは、政府機関等のサイバーセキュリティ対策のための統一基準において適用対象となる情報システム（暗号化機能・電子署名機能の導入を行うものに限る。）の調達・開発にあたって、調達要件や開発要件として採用すべき暗号アルゴリズム及び鍵長を決定するためのガイドラインであり、CRYPTREC 暗号リストの一要素を成すものである。

もう一つは、「暗号鍵設定ガイダンス《(従来仮称）鍵長設定ガイダンス（一般用)》」である。これは、利用用途を特定せず、鍵長の選択方法や暗号鍵の設定に関する一般的な

[1] CRYPTREC, 暗号技術検討会２０２０年度報告書, https://www.cryptrec.go.jp/adv_board.html

ガイダンスを提供する。調達要件や開発要件などを具体的に定めるものではなく、鍵長の選択方法や暗号鍵の設定などについて考え方や留意点を示すものである。

(3) 暗号鍵管理プロファイルの作成ガイダンスの作成

暗号鍵管理ガイドラインの拡充を目的とし、2020 年度に公開した「暗号鍵管理システム設計指針（基本編）」の解説書となる「暗号鍵管理プロファイルの作成ガイダンス（仮称）」を作成する。

2020 年度に取りまとめた作業の進め方に基づき、暗号鍵管理ガイダンス WG を設置して検討を行う。なお、ガイダンス文書の完成時期は 2022 年度を予定する。

1.3 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 の通りである。また、2021 年度に開催された暗号技術活用委員会での議案は表 1-2 の通りである。

表 1-1 暗号技術活用委員会　委員構成

委員長	松本　勉	横浜国立大学　教授
委員	上原　哲太郎	立命館大学　教授
委員	垣内　由梨香	マイクロソフト株式会社　セキュリティプログラムマネージャー
委員	菊池　浩明	明治大学　教授
委員	佐藤　直之	SCSK 株式会社　シニアプロフェッショナルコンサルタント
委員	須賀　祐治	株式会社インターネットイニシアティブ　シニアエンジニア
委員	田村　裕子	日本銀行　企画役補佐
委員	手塚　悟	慶應義塾大学　教授
委員	寺村　亮一	株式会社イエラエセキュリティ　執行役員　兼　高度解析部　部長
委員	松本　泰	セコム株式会社　マネージャー
委員	三澤　学	三菱電機株式会社　主席研究員
委員	満塩　尚史	デジタル庁　セキュリティアーキテクト
委員	山岸　篤弘	一般財団法人日本情報経済社会推進協会　客員研究員
委員	山口　利恵	東京大学　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　副研究センター長

（2022 年 3 月 31 日現在）

表 1-2 暗号技術活用委員会　開催状況

回	開催日	議案
第一回	2021 年 6 月 30 日	● 2021 年度暗号技術活用委員会活動計画の確認 ● 暗号鍵管理ガイダンス WG 活動計画について ● 利用実績による選定基準について ● 鍵長設定要件（仮称）について ● 鍵長設定ガイダンス（一般用）（仮称）について
第二回	2021 年 12 月 13 日	● 利用実績による選定基準案について ● 鍵長設定要件（仮称）について ● 鍵長設定ガイダンス（一般用）（仮称）について
第三回	2022 年 3 月 1 日	● メール審議結果及び暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準について ● 暗号鍵設定ガイダンス（仮称）について ● 利用実績による選定基準（案）について ● 暗号鍵管理ガイダンス WG 活動報告 ● 2021 年度暗号技術活用委員会活動報告案について

2. 成果概要

2.1 利用実績による選定基準（案）について

利用実績に基づく選定基準（選定ルール）は、2012 年度に現在の CRYPTREC 暗号リストの形に改定された際に初めて導入されたものである。

2021 年度の活用委員会では 2012 年当時の選定基準をどのように見直すべきかの検討を行った結果、以下の理由により、選定基準（案）に電子政府推奨暗号リストへの昇格のための明確な選定基準・閾値は設けないとの結論に至った。また、今回作成した選定基準（案）は昇格の目安としてのものであり、実際の昇格判断は個々の状況を鑑みて個別に行うものとした。

- 暗号アルゴリズムの普及の仕方が、利用の前提・環境整備としての「標準化」を踏まえて**徐々に利用が広がっていく**以前の流れから、「有力ベンダが大規模採用」した影響を受けて**急速にその周辺に利用範囲が広がり**後から標準化につながっていく流れに変わってきていることに留意すべきである。
  - 5 年ごとの「利用実績」調査では急激な利用実績の変動に対応できず、判断の遅れにつながる
  - 有力ベンダの採用状況などから近い将来主流になっていく可能性が高いと判断できるような暗号アルゴリズムであれば、早いうちから採用できる環境を整えるべき
  - 結果として、今後の電子政府推奨暗号リストへの昇格は、**「1）5 年ごとの利用実績調査」に基づくケースよりも、「2）その他、普及していることが明らか又は急速な普及が大いに見込まれる」場合に随時昇格させるケースが主軸**になっていく可能性が高い

- 「2）その他、普及していることが明らか又は急速な普及が大いに見込まれる」場合に随時昇格させるケースを想定するならば、その際の普及状況として様々な場面が想定されるため、厳格な基準・閾値と定めたとしても適切な運用ができない可能性がある。
  - 昇格が適切と認められる状況であったとしても、定めた基準・閾値を満たさないという理由で昇格できないのでは本末転倒
  - 有力ベンダの今後の採用状況などの未来予測も加味して利用実績を判断すべき
- クローズドな利用（＝関係者外秘）での実績については、従来と同様、原則カウントしない。
  - ただし、電子政府システムや重要インフラ等、日本の基幹システムでの利用が確認された場合に限り、例外的に扱う
  - 利用実績がないことによる推奨候補暗号リストからの削除にあたっては、CRYPTREC暗号リストの主たる利用者である各府省庁に事前照会を行い、コメントを踏まえたうえで最終判断を行うものとする

【今回の選定基準（案)】

本選定基準は、暗号技術評価委員会で安全性及び実装性の評価を実施し、その評価結果により暗号技術検討会が推奨候補暗号リストに含めると決定した暗号技術に対して、電子政府推奨暗号リストへの昇格を決めるための基準である。昇格検討対象の暗号技術は、以下の考慮項目での目安に基づき、暗号技術活用委員会にて検討、選定し、暗号技術検討会に推薦する。

推薦された暗号技術について、暗号技術検討会では、その根拠となった利用実態を再度確認・審議を行い、電子政府推奨暗号リストへの昇格に問題がないと判断した場合に電子政府推奨暗号リストに選定する。

表　　利用実績による選定基準（案）

考慮項目		選定目安
採用実績	以下のいずれかを満たす場合、昇格の検討対象に含める。なお、採用実績は、 ● 5 年ごとに実施予定の大規模アンケート調査による「**利用実績調査**」 ● 必要に応じて、事務局が（大規模アンケート調査によらずに）情報収集する「**利用実態確認**」 により確認するものとする。	
	① **利用実績調査**の結果、電子政府推奨暗号リストに掲載されている（同一カテゴリの）暗号技術の採用実績と遜色がないことが確認された場合	**電子政府推奨暗号リスト掲載の（同一カテゴリの）暗号技術の採用実績と同等以上の採用実績がある推奨候補暗号リスト掲載の暗号技術を昇格検討対象とする。**

② 利用実績調査又は利用実態確認の結果、電子政府システムや

- さらに、標準化が進んで急速に利用が進展した場合であっても、採用実績の③や④などで対処することが可能

2.2 「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の作成

2020 年度活用委員会での議論を踏まえ、2021 年度の活用委員会では表 1-4 の通りに作成方針を定め、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」を作成した。作成にあたっては、以下の論点について主に検討を行い、検討結果を設定基準に反映させた。

表　「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の作成方針

文書体系	CRYPTREC 暗号リストの一要素を成すものとし、LS を附番
利用目的	政府機関等のサイバーセキュリティ対策のための統一基準において適用対象となる情報システム（暗号化機能・電子署名機能の導入を行うものに限る。）の調達又は開発にあたって、調達要件又は開発要件として採用すべき暗号アルゴリズム及び鍵長を決定する
想定読者	上記システムの調達又は開発に係る情報システムセキュリティ責任者・システム担当者・調達担当者、など。（その他の利用者は、ボランタリベースと位置付ける）
備考	「CRYPTREC 暗号リスト」と一体的に直接参照するものとし、「政府機関の情報セキュリティ対策のための統一基準」での利用を第一義とする
主な論点	● 「鍵長設定の要件」と「移行」に絞って記載してよいか ● 電子政府システムの運用期間として取り扱う範囲をどこまで想定するか ● ビットセキュリティの基準をどこまで区切るか ● 電子政府システムの運用寿命とセキュリティ強度要件の関係をどのように整理するか ● セキュリティ強度要件をどのように設定するか ● セキュリティ強度要件に付与するラベリング名を何にするか ● 情報の機微度、あるいはインパクトレベルによって要件に差をつけるか

<u>設定基準の位置づけ</u>

CRYPTREC 暗号リストに掲載されている暗号技術を利用する際に、適切なセキュリティ強度を実現するためのアルゴリズム及び鍵長の選択方法を規定したものであり、CRYPTREC 暗号リストとの関係を図 1-1 に示す。

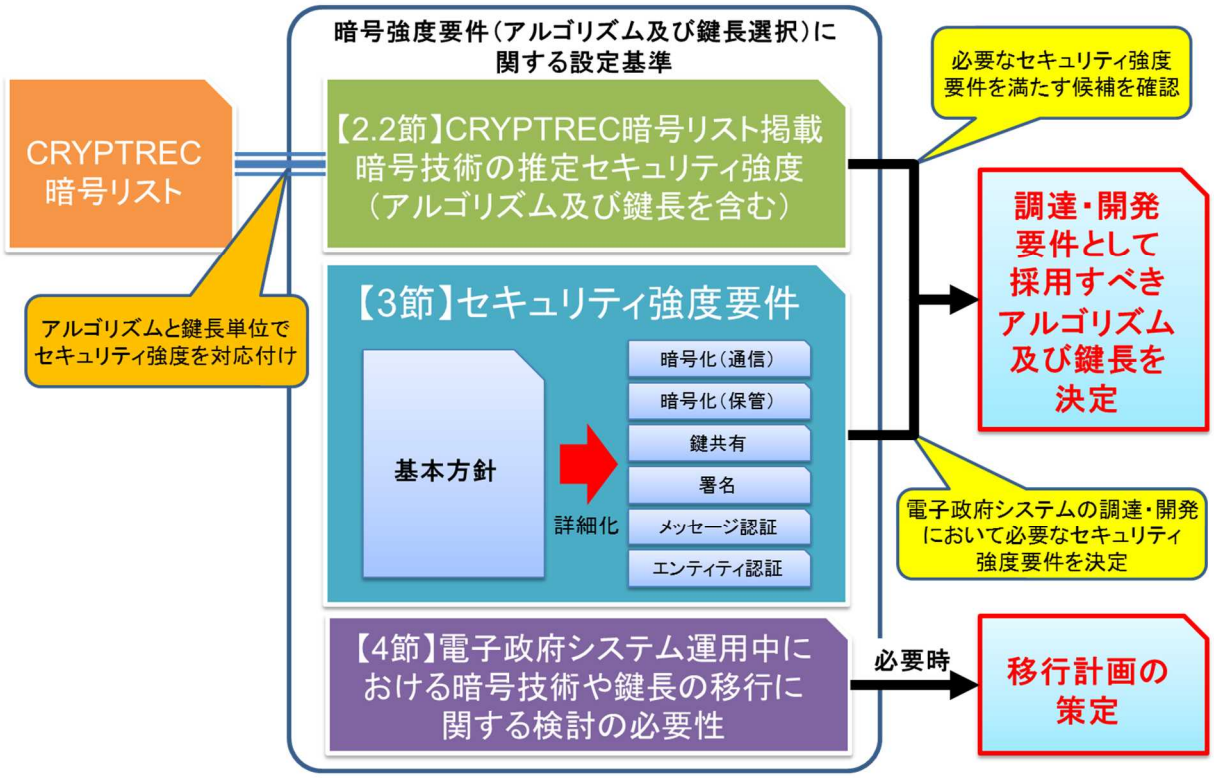


図 1-1 「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の位置づけ

<u>セキュリティ強度要件の基本設定方針概要</u>

電子政府システムを調達又は開発する際は、そのシステムの運用寿命全体と、その期間に実現するセキュリティ強度の関係を考慮してセキュリティ強度要件を設定し、その強度要件を満たすアルゴリズムと鍵長の組合せを調達・開発要件としなければならない。

必要なセキュリティ強度要件は表 1-5 をベースとして、電子政府システムの想定運用終了・廃棄年又は利用期間の終了年を基準に設定する。例えば、電子政府システムの運用終了・廃棄年が 2057 年予定であれば「2051～2060」の列を参照し、192 ビット以上のセキュリティ強度要件を設定する。

表　　セキュリティ強度要件の基本設定基準

想定運用終了・廃棄年／利用期間		2022～2030	2031～2040	2041～2050	2051～2060	2061～2070
112 ビットセキュリティ	新規生成[*1)]	移行完遂期間[*4)]	利用不可	利用不可	利用不可	利用不可
	処理[*2)]		許容[*3)]			
128 ビットセキュリティ	新規生成[*1)]	利用可	利用可	移行完遂期間[*4)]	利用不可	利用不可
	処理[*2)]				許容[*3)]	
192 ビットセキュリティ	新規生成[*1)]	利用可	利用可	利用可	利用可	利用可
	処理[*2)]					
256 ビットセキュリティ	新規生成[*1)]	利用可	利用可	利用可	利用可	利用可
	処理[*2)]					

*1) 新規に暗号処理を実行する場合（例：暗号化、署名生成）

*2) 処理済みのデータに対して処理を実行する場合（例：復号、署名検証）

*3) 処理済みのデータに対する正当性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合

*4) よりセキュリティ強度の高い暗号技術又は鍵長への移行を完遂させなければならない期間。利用する暗号処理が短期間で完結する場合（例：エンティティ認証）、又は既存の電子政府システムの継続利用やそれらとの互換性・相互接続性維持のための利用に限定

なお、本設定基準では量子コンピュータによる暗号技術の危殆化は将来的なリスク要因として位置づけ、推定セキュリティ強度の評価に量子コンピュータの影響は考慮していない。また、将来的なアルゴリズム及び鍵長の選択要件においてもその影響を考慮しないものとしている。

アルゴリズム及び鍵長の選択・実装要件及び利用要件の基本方針

- 設定されたセキュリティ強度要件と同じかそれ以上のセキュリティ強度を満たすアルゴリズム及び鍵長の組合せを推定セキュリティ強度の表から選択してサポート（実装）しなければならない。
- 設定したセキュリティ強度要件以下の安全性のアルゴリズム及び鍵長をサポート（実装）すること自体は妨げない。ただし、サポート（実装）されたアルゴリズム及び鍵長のすべてが常に利用されてよいわけではなく、その利用期間については、そのセキュリティ強度に応じて、セキュリティ強度要件に従って定めなければならない。
- データのセキュリティ寿命は利用するアルゴリズムのセキュリティ寿命に包含されなければならない。

CRYPTREC 暗号リスト上の暗号技術とセキュリティ強度との対応

本設定基準の中では、2021 年末時点での CRYPTREC 暗号リストに記載の暗号アルゴリズムごとの安全性評価の現状等を踏まえた推定セキュリティ強度を示している。これらは、今後、暗号解読手法の進展や大規模量子コンピュータの実現等により、推定セキュリティ強度が見直される可能性がある（少なくとも 5 年ごとに再確認される）。

運用中における暗号技術及び鍵長移行に関する検討の必要性

外部要因により、利用しているアルゴリズムや鍵長の移行に関する検討を行う必要が出てくるケースとして、以下のようなものがある。これらに該当する事象が発生した場合には、直ちに内容の確認を行い、必要に応じて移行計画を策定しなければならない。本設定基準では、これらに応じて移行計画を策定する際に考慮しなければならないポイントを示してい

	ように整理するか ● 求められるセキュリティ強度要件の考え方 ● 「暗号鍵のライフサイクル」「暗号鍵の（タイプごとの）利用期間」「鍵の保護」についての記載内容 ● 移行に関する検討の必要性についての記載内容

本書では、まず安全な暗号技術の導入の観点から、暗号技術を利用する際の鍵長の選択方法に関する一般的な考え方を解説する。また、暗号技術の安全な運用の観点から、適切に暗号鍵の管理を行うために必要となる項目についての技術的概要を示す。具体的には、暗号鍵を安全に設定し、運用していくために考慮すべき項目として以下の項目を解説している。

- 暗号鍵の鍵長
- 暗号鍵の鍵タイプ
- 暗号鍵のライフサイクル
- 運用中における鍵長移行に関する検討の必要性

なお、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」との最大の違いは求められるセキュリティ強度要件の考え方が違うことである。「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」では電子政府システムにおいて十分なセキュリティ強度を持たせるために必要な要件として予め規定しているのに対して、本ガイダンスでは実際の利用用途や利用期間、環境、コスト、その他様々な制約条件を踏まえて、読者が必要なセキュリティ強度を決めるように勧めている。

2.4　暗号鍵管理の参照プロファイルの作成に向けた検討結果について

情報を安全に取り扱うためには、通信情報や保管情報の暗号化に使う暗号アルゴリズムのみに注意を払うだけでは不十分であり、その暗号アルゴリズムに用いられる暗号鍵の管理が適切に行われる必要がある。そこで、2020 年度に鍵管理のフレームワークとなる「暗号鍵管理システム設計指針（基本編)」を公開したことに引き続き、暗号鍵管理ガイドラインの拡充を目的として暗号鍵管理ガイダンスを作成するため、暗号鍵管理ガイダンス WG を設置した。

2021 年度は、実際のガイダンス作成の進め方についての検討を行い、ガイダンス作成に向けた執筆方針の方向性を取りまとめることに注力した。なお、暗号鍵管理ガイダンスの位置づけと想定読者は以下の通りとする。

<u>位置づけ</u>

- 暗号鍵管理プロファイルを作成するためのガイダンスを作成する。ただし、特定の業界において使用する参照可能なプロファイルは含まれない点については注意されたい。
- 暗号鍵管理で必要となる項目について、シンプルなモデルを例示し説明する。

- シンプルなモデルを用いた説明においては、鍵管理における要求や思想が理解できるような記載を行う。
- 暗号鍵管理における特に注意すべきリスクや、発生しうる失敗例を説明する。

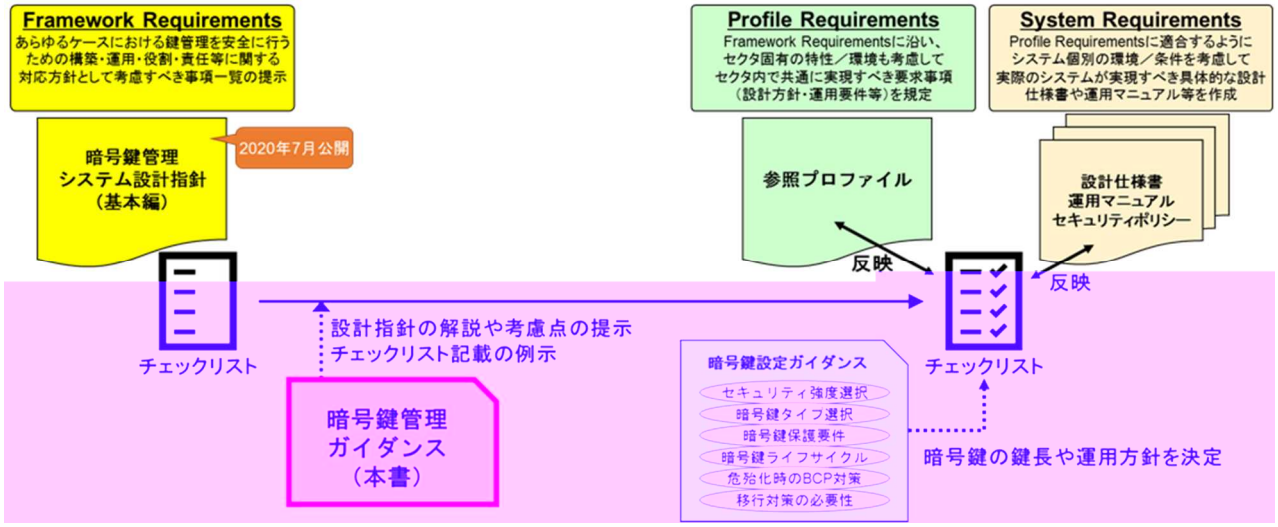


図 1-2 「暗号鍵管理ガイダンス」作成の位置づけ

想定読者

- 暗号鍵管理機能を持つシステム設計者
- 各業界において、暗号鍵管理の参照プロファイルを作成する担当者
- 一部の内容については、暗号鍵管理プロファイルの利用者、暗号鍵管理機能を持つシステム調達者等

【ガイダンス内容のイメージ】

本ガイダンスでは、要求内容については基本的に暗号鍵管理システム設計指針（基本編）の Frame Requirements の内容をそのまま転記し、「ガイダンスで記載する説明事項」と「チェックリストの記載例」を中心に説明を加筆する。

表　　「暗号鍵管理ガイダンス」の執筆内容

各節のフォーマット		
検討番号	*.**	―
要求内容	暗号鍵管理システム設計指針（基本編）の説明や Frame Requirements の内容を基本的に引用	● 目的・趣旨 ● 要求事項 ● 記載内容
ガイダンスで記載する説明事項	**1. 要求に対する判断理由に関する考え方を記載 2. 必要に応じて、要求に関する補足説明を記載**	**● 解説・考慮点**
チェックリストの記載例	**トイモデルを利用した判断理由の記載内容を例示**	**● トイモデルとチェックリストの記載例**

【ガイダンス作成の進め方】

暗号鍵管理システム設計指針（基本編）の要件（チェックリスト）の解説にあたって、参考例として「トイモデル」を使う。

- 暗号鍵管理システム設計指針（基本編）での 6 つの目的別分類ごとに、理解しやすいトイモデルを用意
- トイモデルを使ったガイダンスの中で CBP に該当する部分を参考
- 「ユースケースを例題・想定した記載」は本文中に想定しない

3. 今後に向けて

2022 年度に予定されている CRYPTREC 暗号リストの改定に向け、IPA と協力して暗号利用実績調査を実施し、策定された選定基準に照らし合わせた実績評価を行う。また、暗号鍵管理ガイダンス WG にて検討中の暗号鍵管理ガイダンスを完成させる予定である。

資料５

利用実績による選定基準（案）について

利用実績に基づく選定基準（選定ルール）は、2012 年度に現在の CRYPTREC 暗号リストの形に改定された際に初めて導入されたものであり、以下の（参考）のように定められた。

今年度の暗号技術活用委員会では、2012 年当時の選定基準をどのように見直すべきかの観点から、CRYPTREC 暗号リスト改定に伴う利用実績による選定基準案について検討し、以下のとおり基準案を取りまとめたので、ご審議願いたい。

（参考）【2012 年当時の選定基準の概要抜粋】

- 利用実績に基づく選定に関する知見があったわけではないので、暗号運用委員会（当時、現暗号技術活用委員会）にてゼロベースで検討した。
- 2009 年度に経済産業省が実施した「暗号モジュールの市場動向等に関する調査研究」における「暗号アルゴリズムの市場性」の調査結果をベースに、利用実績を評価するための閾値を検討した。
- 電子政府における競争調達性の確保を考慮し、電子政府推奨暗号リストに掲載するのは「利用実績が十分であり、今後も安定的に利用可能である（評価 A）」か、「利用実績は十分ではないが、今後の利用促進の可能性が高い（評価 B）」と判断できるような暗号アルゴリズムを選定することを目指した。特に、提案会社とは資本関係がない複数の企業から調達可能であることを重視した。

<table>
<tr><td></td><td colspan="2">評価 A</td><td colspan="2">評価 B</td></tr>
<tr><td>市販製品での採用実績
（販売会社数・種類・種別）</td><td>提案会社・グループ会社以外での採用、且つ採用割合 50%以上</td><td rowspan="4">うち、3 項目以上</td><td>提案会社・グループ会社以外での採用、且つ採用割合 50%以上</td><td rowspan="9">うち、3 項目以上</td></tr>
<tr><td>オープンソースプロジェクトでの採用実績</td><td>採用割合 50%以上</td><td>採用割合 50%以上</td></tr>
<tr><td>政府系システム規格での採用実績</td><td>採用割合 50%以上</td><td>採用割合 50%以上</td></tr>
<tr><td>国際的な民間メジャー規格での採用実績</td><td>採用割合 50%以上</td><td>採用割合 50%以上</td></tr>
<tr><td>利用促進を図る際の障壁の除去</td><td colspan="2"></td><td>特許無償ライセンスの付与</td></tr>
<tr><td>標準化・規格化の促進を図るハードルの低さ</td><td colspan="2"></td><td>技術的、標準化、採用実績のいずれかでアピールポイントがある</td></tr>
<tr><td>実装コスト低減を図るハードルの低さ</td><td colspan="2"></td><td>採用実績、オープンソースプロジェクトのいずれかでアピールポイント（採用割合 10%以上）がある</td></tr>
<tr><td>調達コスト低減を図るハードルの低さ</td><td colspan="2"></td><td>市販製品又は政府系システムでの採用実績（採用割合 10%以上）がある</td></tr>
</table>

1. 選定基準（案）についての考え方

以下の理由により、電子政府推奨暗号リストへの昇格のための明確な選定基準・閾値は設けない。今回作成する選定基準は昇格の目安としてのものであり、実際の昇格判断は個々の状況を鑑みて個別に行うものとする。

- 暗号アルゴリズムの普及の仕方が、利用の前提・環境整備としての「標準化」を踏まえて**徐々に利用が広がっていく**以前の流れから、「有力ベンダが大規模採用」した影響を受けて**急速にその周辺に利用範囲が広がり**後から標準化につながっていく流れに変わってきていることに留意すべきである。
  - 5年ごとの「利用実績」調査では急激な利用実績の変動に対応できず、判断の遅れにつながる
  - 有力ベンダの採用状況などから近い将来主流になっていく可能性が高いと判断できるような暗号アルゴリズムであれば、早いうちから採用できる環境を整えるべき
  - 結果として、今後の電子政府推奨暗号リストへの昇格は、**「1）5 年ごとの利用実績調査」に基づくケースよりも、「2）その他、普及していることが明らか又は急速な普及が大いに見込まれる」場合に随時昇格させるケースが主軸**になっていく可能性が高い
- 「2）その他、普及していることが明らか又は急速な普及が大いに見込まれる」場合に随時昇格させるケースを想定するならば、その際の普及状況として様々な場面が想定されるため、厳格な基準・閾値と定めたとしても適切な運用ができない可能性がある。
  - 昇格が適切と認められる状況であったとしても、定めた基準・閾値を満たさないという理由で昇格できないのでは本末転倒
  - 有力ベンダの今後の採用状況などの未来予測も加味して利用実績を判断すべき
- クローズドな利用（＝関係者外秘）での実績については、従来と同様、原則カウントしない。
  - ただし、電子政府システムや重要インフラ等、日本の基幹システムでの利用が確認された場合に限り、例外的に扱う
  - 利用実績がないことによる推奨候補暗号リストからの削除にあたっては、CRYPTREC 暗号リストの主たる利用者である各府省庁に事前照会を行い、コメントを踏まえたうえで最終判断を行うものとする

2. 選定基準（案）

＜選定基準＞

本選定基準は、暗号技術評価委員会で安全性及び実装性の評価を実施し、その評価結果により暗号技術検討会が推奨候補暗号リストに含めると決定した暗号技術に対して、電子政府推奨暗号リストへの昇格を決めるための基準である。昇格検討対象の暗号技術は、以下の考慮項目での目安に基づき、暗号技術活用委員会にて検討、選定し、暗号技術検討会に推薦する。

推薦された暗号技術について、暗号技術検討会では、その根拠となった利用実態を再度確認・審議を行い、電子政府推奨暗号リストへの昇格に問題がないと判断した場合に電子政府推奨暗号リストに選定する。

考慮項目		選定目安
採用実績	以下のいずれかを満たす場合、昇格の検討対象に含める。なお、採用実績は、 ● 5 年ごとに実施予定の大規模アンケート調査による「**利用実績調査**」 ● 必要に応じて、事務局が（大規模アンケート調査によらずに）情報収集する「**利用実態確認**」により確認するものとする。	
	① **利用実績調査**の結果、電子政府推奨暗号リストに掲載されている（同一カテゴリの）暗号技術の採用実績と遜色がないことが確認された場合	**電子政府推奨暗号リスト掲載の（同一カテゴリの）暗号技術の採用実績と同等以上の採用実績がある推奨候補暗号リスト掲載の暗号技術を昇格検討対象とする。**
	② **利用実績調査**又は**利用実態確認**の結果、**電子政府システムや重要インフラ等、日本の基幹システム**においてすでに利用されていることが確認された場合	**必要に応じて、利用実績調査に代わって、各府省庁等への照会を実施し、照会結果（クローズドな利用を含め）を基に昇格検討対象を選定する。**
	利用実績調査又は**利用実態確認**の結果、③～⑤のいずれかが確認された場合： ③ **利用者が多い主要な汎用製品群の複数**に搭載されるなど、明らかに採用が進展していると判断された場合 ④ **利用者が多い主要なオープンソースソフトウェアの複数**に搭載されるなど、明らかに採用が進展していると判断された場合 ⑤ **利用者が多い主要なサービスやプロトコルの複数**で利用されるなど、明らかに採用が進展していると判断された場合	**「複数」「利用者が多い（主要な）」というキーワードの両方を十分に満たし、明らかな採用促進が確認された場合には、必要に応じて、昇格検討対象とする。** **※「複数」の意味は、必要条件として「2 個以上が必要」ということであって、「2 個以上あればよい」という十分条件としての意味ではないことに留意**
標準化実績	以下を満たす場合、昇格の検討対象に含める。	
	⑥ **利用実績調査**の結果、電子政府推奨暗号リストに掲載されている（同一カテゴリの）暗号技術の採用実績と遜色がないことが確認された場合	**電子政府推奨暗号リスト掲載の（同一カテゴリの）暗号技術の採用実績と同等以上の採用実績がある推奨候補暗号リスト掲載の暗号技術は昇格検討対象とする。**

＜目安の理由＞

- ①は「利用実績調査」の結果に基づく基準として整備する。
  電子政府推奨暗号リストと推奨候補暗号リストの採用実績に著しい不整合が起きないようにするための指標とする。

- ②～⑤は「その他、普及していることが明らか又は急速な普及が大いに見込まれる」ケースに対応する基準として整備する。

  ①の場合と異なり、必ずしも利用実績調査を実施するわけではなく、利用実態確認だけで採用実績を確認する場合もあるので、採用割合での判断は行わない。象徴的な利用形態での採用実績がどれだけ進んだかを主な指標とする。

  - ②については、CRYPTRECの設置目的からして明らかに管理する必要があることへの対応。また、クローズドな利用での実績であったとしても、CRYPTREC暗号リストの主たる利用者である各府省庁に事前照会を踏まえた判断根拠になり得る。
  - ③～⑤については、「複数」「利用者が多い（主要）」というキーワードの両方を満たすことを例示しておくことで、「明らかな採用促進、又は急速な普及の可能性」の判断目安とすることを意図している。なお、実際に判断にあたっては、利用実態確認で収集した関連情報を基にした委員会での審議結果に基づく。
- 標準化実績については、標準化が進んだだけでは採用実績に直ちに結びつくわけではなく、また標準化されるまでに時間がかかる。このため、利用実績に急激な変化が起こりにくいことを考慮し、「利用実績調査」の結果に基づく基準のみを整備
  - さらに、標準化が進んで急速に利用が進展した場合であっても、採用実績の③や④などで対処することが可能

3. 「CRYPTREC暗号リスト移行ルール」の一部（表記上の）修正について

2020年度の暗号技術検討会にて、CRYPTREC暗号リスト移行ルールを別紙の通り決定したところである。

しかし、上で提案した選定基準（案）においては、実際には「利用実績を5年ごとの調査ベースを基本とすると、世の中のスピード感に対して遅れてしまう恐れがある。利用実績は未来予測をベースで考えたほうがいい。」との意見を反映し、「普及していることが明らか」な場合だけでなく、「急速な普及が大いに見込まれる」場合も含んだものとしている。

そのため、「CRYPTREC暗号リスト移行ルール」中の「②推奨候補暗号リスト」から「①電子政府推奨暗号リスト」への昇格ルールにおいて、「2. その他、普及していることが明らかな場合」を「2. その他、普及していることが明らか<u>又は急速な普及が大いに見込まれる</u>場合」に追記修正することを提案する。

以上

【別紙】

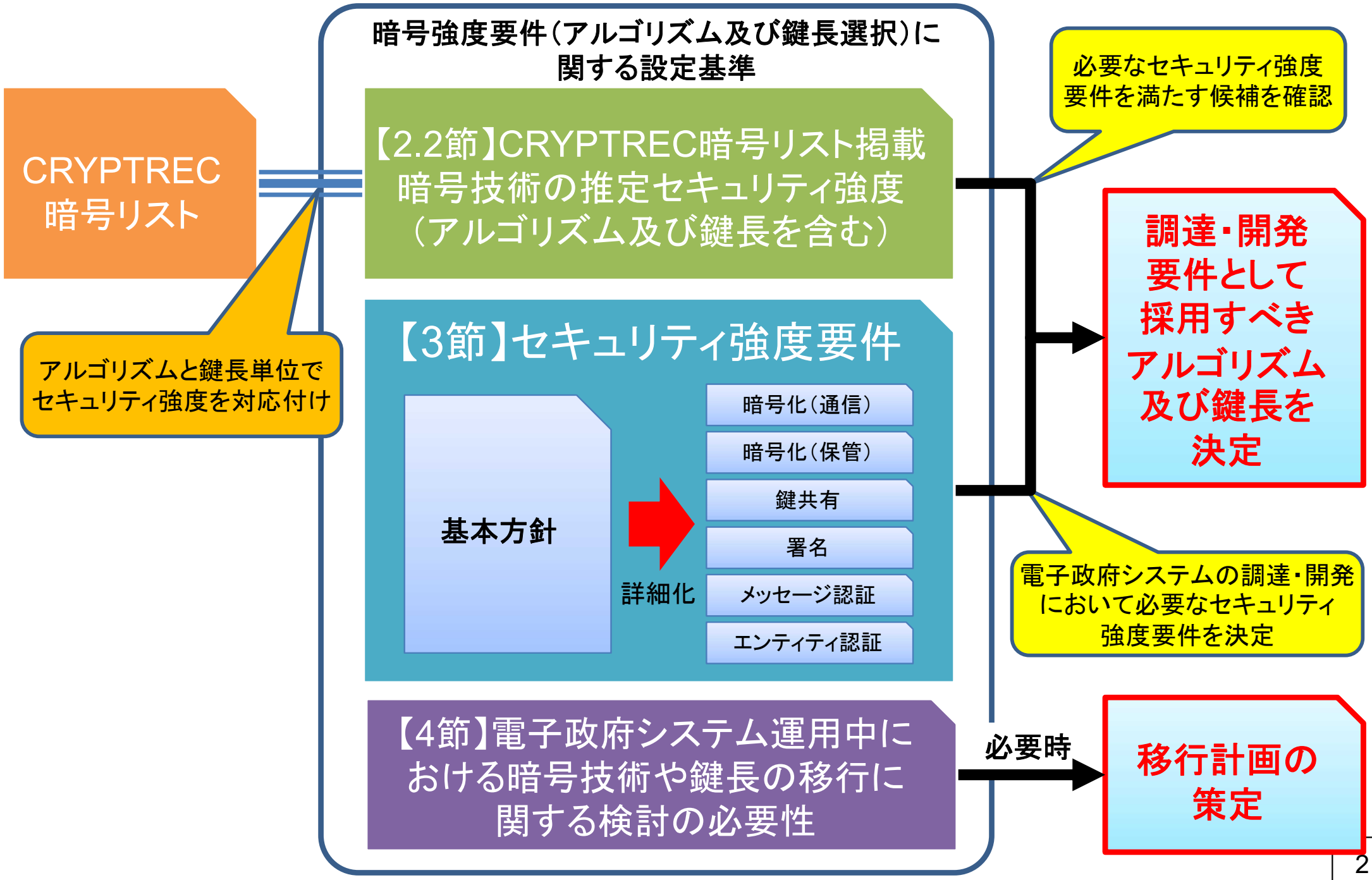
CRYPTREC 暗号リスト移行ルール

CRYPTREC LS-0003-2022附

資料６－１

暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準概要（Ver 0.99）

暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準概要



セキュリティ強度要件の基本設定方針概要(1/3)

電子政府システムを調達又は開発する際は、そのシステムの運用寿命全体と、その期間に実現するセキュリティ強度の関係を考慮してセキュリティ強度要件を設定し、その強度要件を満たすアルゴリズムと鍵長の組合せを調達・開発要件としなければならない。セキュリティ強度要件の設定にあたっては、電子政府システムの検討状況を踏まえ、以下の要件設定方法のいずれかを選択して行う。

【要件設定方法①】

電子政府システムの運用寿命全体を通して必要なセキュリティ強度要件を設定し、その強度要件を満たすアルゴリズムと鍵長の組合せをサポート(実装)しなければならない

- 利用終了時期を明確化し、それまでにより安全なアルゴリズム及び鍵長に移行することを条件に、その期間中は安全と期待されるアルゴリズムと鍵長の組合せを一緒にサポート(実装)してもよい

【要件設定方法②】

何らかの制約により、運用寿命全体を通して必要なセキュリティ強度要件を当初から設定することが困難である場合、セキュリティ強度要件を切り替える移行時期を明確化したスケジュールを立案することを条件としたうえで、その移行時期終了まで安全に運用するために必要なセキュリティ強度要件を設定し、その強度要件を満たすアルゴリズムと鍵長の組合せをサポート(実装)しなければならない

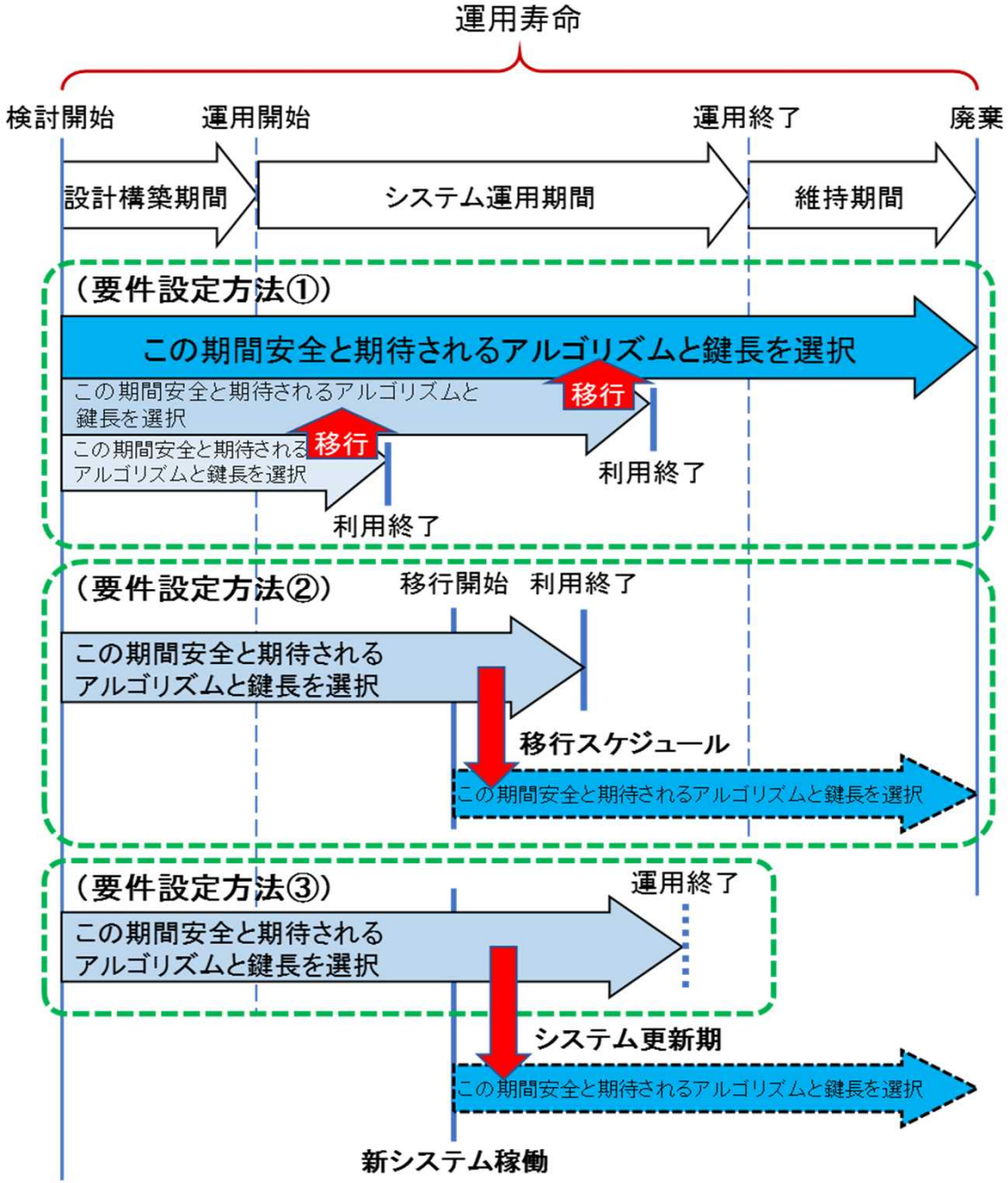
- 移行スケジュールには移行開始予定時期及び移行完了予定時期を明示すべき

【要件設定方法③】

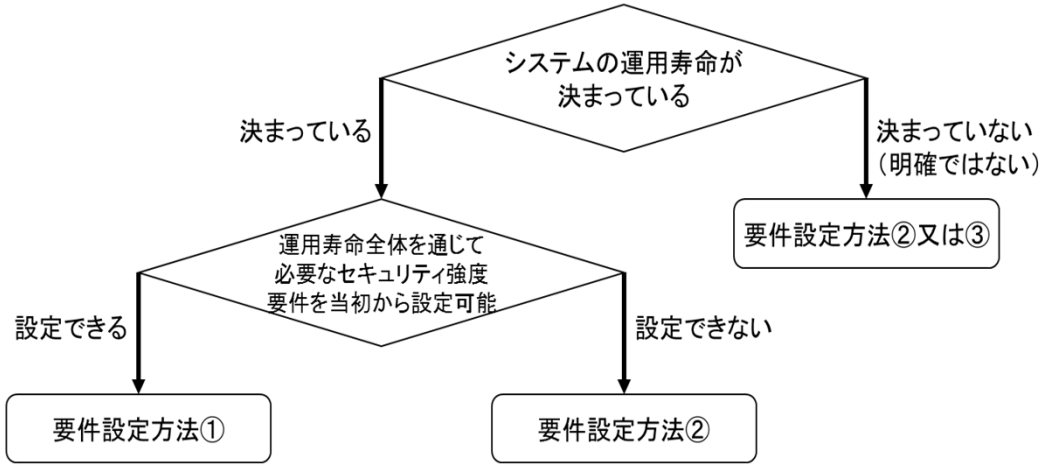
運用寿命が決まっていない(明確ではない)場合、システム更新期を明確化したスケジュールを立案することを条件としたうえで、その更新期まで安全に運用するために必要なセキュリティ強度要件を設定し、その強度要件を満たすアルゴリズムと鍵長の組合せをサポート(実装)しなければならない

- 新システムの稼働開始予定時期及び新旧システムの併用運用想定期間も示しておくことが望ましい

セキュリティ強度要件の基本設定方針概要(2/3)



システムの運用寿命と求められるセキュリティ強度



要件設定方法の選択フロー

セキュリティ強度要件の基本設定方針概要(3/3)

- 必要なセキュリティ強度要件は以下の表をベースとして、システムの想定運用終了・廃棄年又は利用期間の終了年を基準に設定する
  - システムの**運用終了・廃棄年**が2057年予定であれば「2051～2060」の列を参照 ➡ 192ビット以上のセキュリティ強度要件
  - 署名を利用するシステムの場合、利用期間の終了年は、署名生成を行わなくなる年ではなく、すべての署名検証が必要なくなる年で判断
  - **移行期間**を2041～2045年とするシステムならば、「2041年移行開始2045年移行完了予定」の移行スケジュールを立案するとともに、当初は「2041～2050」の列を参照 ➡ 128ビット以上のセキュリティ強度要件
  - 次期システムの想定運用開始が2040年前半である場合、併用運用期間が5年間であれば2040年前半から5年間の、10年間であれば10年間のシステム更新スケジュールを立案するとともに、それぞれ当初は「2041～2050」「2051～2060」の列を参照

想定運用終了・廃棄年／利用期間		2022～2030	2031～2040	2041～2050	2051～2060	2061～2070
112ビットセキュリティ	新規生成*1)	移行完遂期間*4)	利用不可	利用不可	利用不可	利用不可
	処理*2)		許容*3)			
128ビットセキュリティ	新規生成*1)	利用可	利用可	移行完遂期間*4)	利用不可	利用不可
	処理*2)				許容*3)	
192ビットセキュリティ	新規生成*1)	利用可	利用可	利用可	利用可	利用可
	処理*2)					
256ビットセキュリティ	新規生成*1)	利用可	利用可	利用可	利用可	利用可
	処理*2)					

*1) 新規に暗号処理を実行する場合（例：暗号化、署名生成）

*2) 処理済みのデータに対して処理を実行する場合（例：復号、署名検証）

*3) 処理済みのデータに対する正当性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合

*4) よりセキュリティ強度の高い暗号技術又は鍵長への移行を完遂させなければならない期間。利用する暗号処理が短期間で完結する場合（例：エンティティ認証）、又は既存の電子政府システムの継続利用やそれらとの互換性・相互接続性維持のための利用に限定

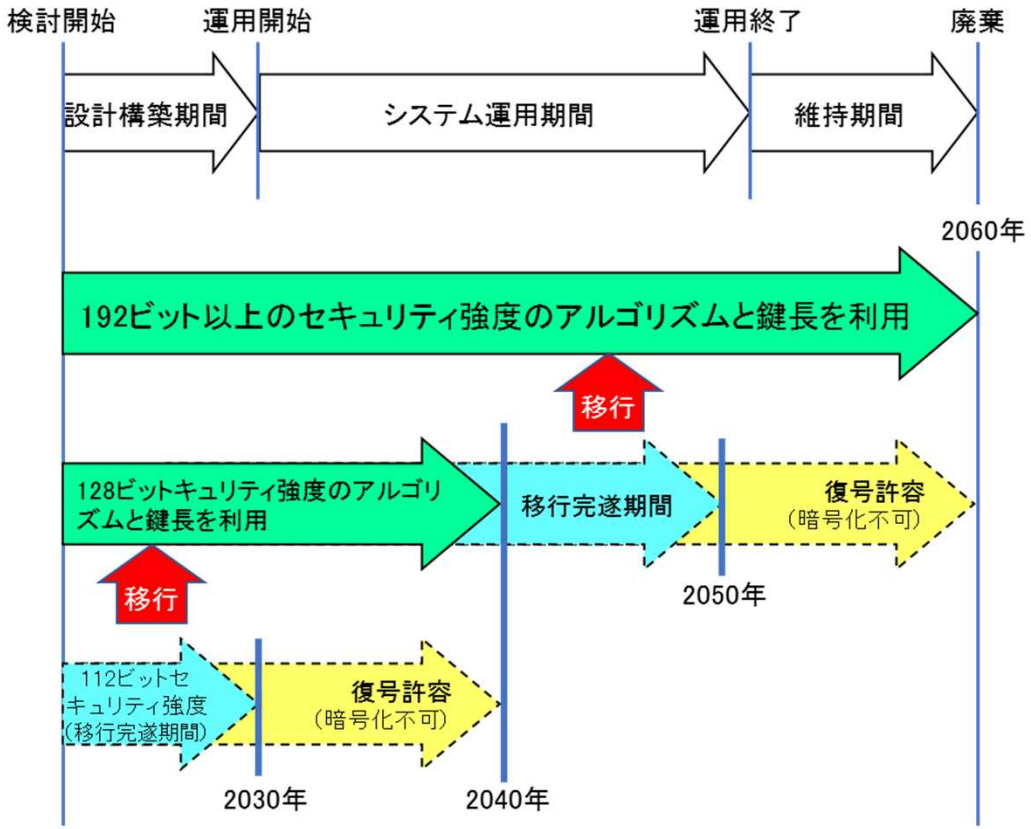
注) 2021年末時点での暗号技術の安全性評価の現状等を踏まえたうえで、2070年までの予測可能なセキュリティマージンを持った基準として定めたものである。
したがって、精度の高い実現時期の予測が困難な、画期的な暗号解読手法の発明や大規模量子コンピュータの実現によるアルゴリズムの危殆化等については考慮していない。

実際の調達・開発・運用にあたっては、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準（3節）」を参照願います。

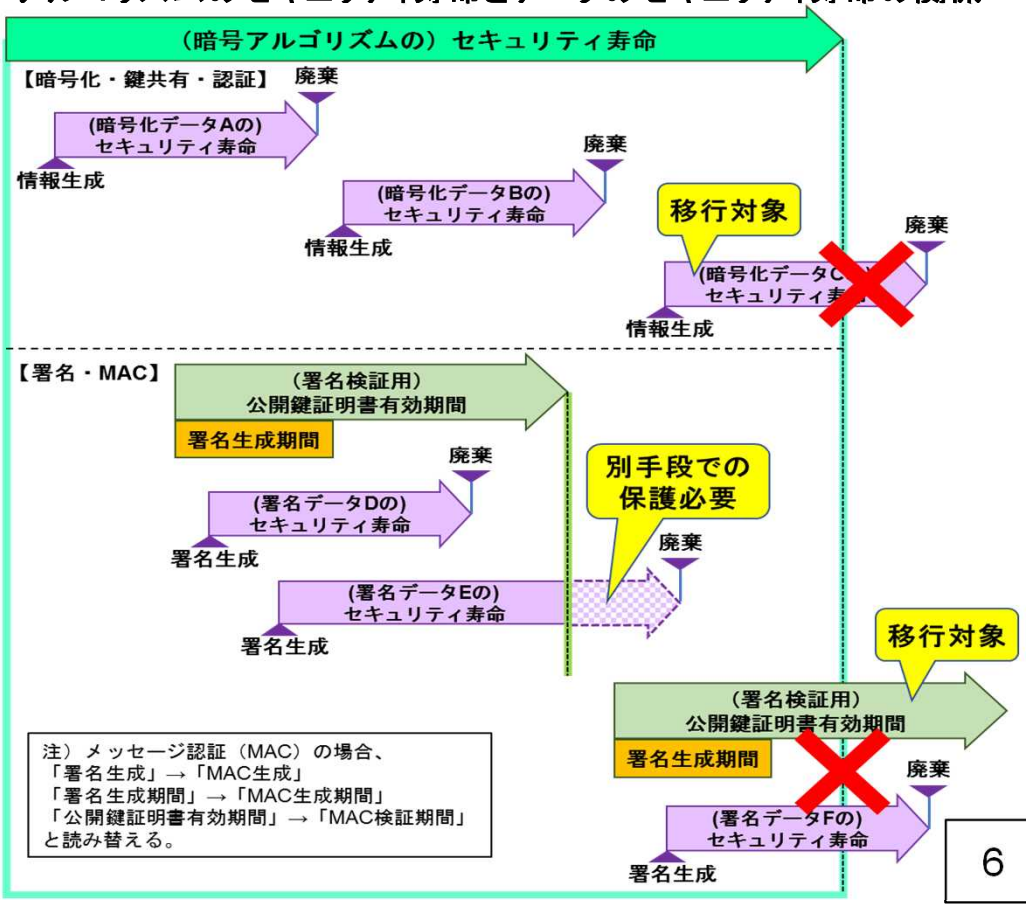
アルゴリズム及び鍵長の選択・実装及び利用の基本方針

- 設定されたセキュリティ強度要件と同じかそれ以上のセキュリティ強度を満たすアルゴリズム及び鍵長の組合せを推定セキュリティ強度の表から選択してサポート(実装)しなければならない
- 設定したセキュリティ強度要件以下の安全性のアルゴリズム及び鍵長をサポート(実装)すること自体は妨げない。ただし、サポート(実装)されたアルゴリズム及び鍵長のすべてが常に利用されてよいわけではなく、その利用期間については、そのセキュリティ強度に応じて、セキュリティ強度要件に従って定めなければならない
- データのセキュリティ寿命は利用するアルゴリズムのセキュリティ寿命に包含されなければならない

想定廃棄年を2060年に予定しているシステムにおける保管時の暗号化の場合



アルゴリズムのセキュリティ寿命とデータのセキュリティ寿命の関係



（参考）CRYPTREC暗号リスト上の暗号技術とセキュリティ強度との対応

注) この表は2021年末時点での暗号アルゴリズムごとの安全性評価の現状等を踏まえた推定セキュリティ強度を示したものである。
したがって、**今後、暗号解読手法の進展や大規模量子コンピュータの実現等により、暗号アルゴリズム及び鍵長によっては推定セキュリティ強度が見直される可能性がある（少なくとも5年ごとに再確認される）**。

	ビットセキュリティ			
	112	**128**	**192**	**256**
公開鍵暗号	**RSA系**[*1)](鍵長2048ビット) **DSA(鍵長2048ビット/224ビット)** **ECDSA(P-224,B-233,K-233)** **DH(鍵長2048ビット/224ビット)** **ECDH(P-224,B-233,K-233)** PSEC-KEM(P-224,B-233,K-233)	**RSA系**[*1)](鍵長3072ビット) **DSA(鍵長3072ビット/256ビット)** **ECDSA(P-256,B-283,Ed25519等)** **DH(鍵長3072ビット/256ビット)** **ECDH(P-256,B-283,Ed25519等)** PSEC-KEM(P-256,B-283,Ed25519等)	**RSA系**[*1)](鍵長7680ビット) **DSA(鍵長7680ビット/384ビット)** **ECDSA(P-384,B-409,Ed448等)** **DH(鍵長7680ビット/384ビット)** **ECDH(P-384,B-409,Ed448等)** PSEC-KEM(P-384,B-409,Ed448等)	**RSA系**[*1)](鍵長15360ビット) **DSA(鍵長15360ビット/512ビット)** **ECDSA(P-521,B-571,K-571)** **DH(鍵長15360ビット/512ビット)** **ECDH(P-521,B-571,K-571)** PSEC-KEM(P-521,B-571,K-571)
共通鍵暗号	3-key Triple DES	**ブロック暗号**[*2)](鍵長128ビット) **KCipher-2** Enocoro-128v2 MUGI	**ブロック暗号**[*2)](鍵長192ビット)	**ブロック暗号**[*2)](鍵長256ビット) MULTI-S01
ハッシュ関数		**SHA-256** SHA-512/256 SHA3-256 SHAKE128 SHAKE256(ハッシュ長256ビット)	**SHA-384** SHA3-384 SHAKE256(ハッシュ長384ビット)	**SHA-512** SHA3-512 SHAKE256(ハッシュ長512ビット)
ハッシュ関数(HMAC利用時)		SHAKE128 RIPEMD-160 SHA-1		**ハッシュ関数**[*3)]
認証暗号				ChaCha20-Poly1305

*1) 次の公開鍵暗号
- **RSA-PSS**
- **RSASSA-PKCS1-v1_5**
- **RSA-OAEP**
- RSAES-PKCS1-v1_5

*2) 次の共通鍵暗号（ブロック暗号）
- **AES**
- CIPHERUNICORN-E
- MISTY1
- CLEFIA
- SC2000
- **Camellia**
- Hierocrypt-L1
- CIPHERUNICORN-A
- Hierocrypt-3

*3) 次のハッシュ関数
- **SHA-256**
- **SHA-512**
- SHA3-256
- SHA3-512
- **SHA-384**
- SHA-512/256
- SHA3-384
- SHAKE256

［文字色の凡例］
- **電子政府推奨暗号リスト**
- 推奨候補暗号リスト
- 運用監視暗号リスト

運用中における暗号技術及び鍵長移行に関する検討の必要性

- 新しいアルゴリズム及び鍵長に移行するのは、多くの場合、非常に時間とコストがかかる作業であることを念頭に置いておく必要がある。
  - 実際、過去にあったアルゴリズムや鍵長における大規模な移行（例：DESからAESへの移行、RSAでの鍵長1024ビットから2048ビットへの移行、SHA-1からSHA-256への移行など）では、移行準備から移行完了までに5年から10年単位の時間がかかっている
- そのため、利用しているアルゴリズムや鍵長がセキュリティ寿命を迎える少なくとも5年前までには、より強力なアルゴリズム及び鍵長への移行計画を策定すべき。その移行計画を立てる際には、いつからどのくらいの期間をかけてどのアルゴリズムや鍵長に移行するのかを明確にすべき。
- 外部要因により、利用しているアルゴリズムや鍵長の移行に関する検討を行う必要が出てくるケースとして、以下のようなものがある。これらに該当する事象が発生した場合には、直ちに内容の確認を行い、必要に応じて移行計画を策定しなければならない。
  - 電子政府システムの運用寿命の延長に伴う対応
  - セキュリティ強度要件の設定変更に伴う対応
  - 暗号技術の推定セキュリティ強度の変更に伴う対応
  - 運用監視暗号リストに掲載されたアルゴリズムの継続利用にあたっての対応
  - 突発的な理由に伴う緊急移行にあたっての対応
  - 量子コンピュータの実現リスクへの対応

実際の移行計画作成の検討についても、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準（4節）」を参照願います。

CRYPTREC LS-0003-2022

資料６－２

暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準

2022 年 3 月

（Ver. 0.99）

目次

【修正履歴】

修正日	修正内容
2022.xx.xx (Ver.1.0)	初版発行

1. はじめに

1.1 本書の内容及び位置付け

CRYPTREC 暗号リスト[1]に掲載されている多くの暗号技術では一つのアルゴリズムで複数の鍵長が利用可能であり、利用する鍵長によってセキュリティ強度と処理効率などが変わることに留意する必要がある。アルゴリズムの中には（特に RSA などの公開鍵暗号では）必要以上に長い鍵長を使用すると処理効率などに悪影響が出る場合がある一方、短すぎる鍵長を使用すると十分なセキュリティ強度を提供しない。

本書は、**CRYPTREC 暗号リストに掲載されている暗号技術を利用する際に、適切なセキュリティ強度を実現するためのアルゴリズム及び鍵長の選択方法を規定**したものであり、CRYPTREC 暗号リストとの関係を図 1 に示す。

したがって、**政府機関等のサイバーセキュリティ対策のための統一基準[2]において適用対象となる情報システム（暗号化機能・電子署名機能の導入を行うものに限る。）（以下、「電子政府システム」という。）に対して CRYPTREC 暗号リストに掲載されているアルゴリズムを採用していたとしても、本書の規定に合致しない鍵長を用いた場合には統一基準の遵守事項を満たしているとは見なされない**ことに留意されたい。

本書は 4 節で構成されており、節立ては以下の通りである。

1 節では、イントロダクションとして、本書の位置づけや想定読者を示す。
2 節では、本書を理解する上での技術的な基礎知識を説明する。また、暗号技術ごとの推定セキュリティ強度をまとめる。
3 節では、電子政府システムに求められる運用寿命とセキュリティ強度要件の設定方針の関係の考え方を示し、暗号処理ごとにセキュリティ強度要件の設定方針を記載する。
4 節では、運用中における暗号技術及び鍵長移行に関する検討の必要性を示し、その際の論点等を記載する。
Appendix では、本書を作成する上で考慮した参考情報を紹介する。

---

1 総務省・経済産業省、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)、https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r6.pdf

2 内閣サイバーセキュリティセンター（NISC）、政府機関等のサイバーセキュリティ対策のための統一基準（令和 3 年度版）、https://www.nisc.go.jp/active/general/pdf/kijyunr3.pdf

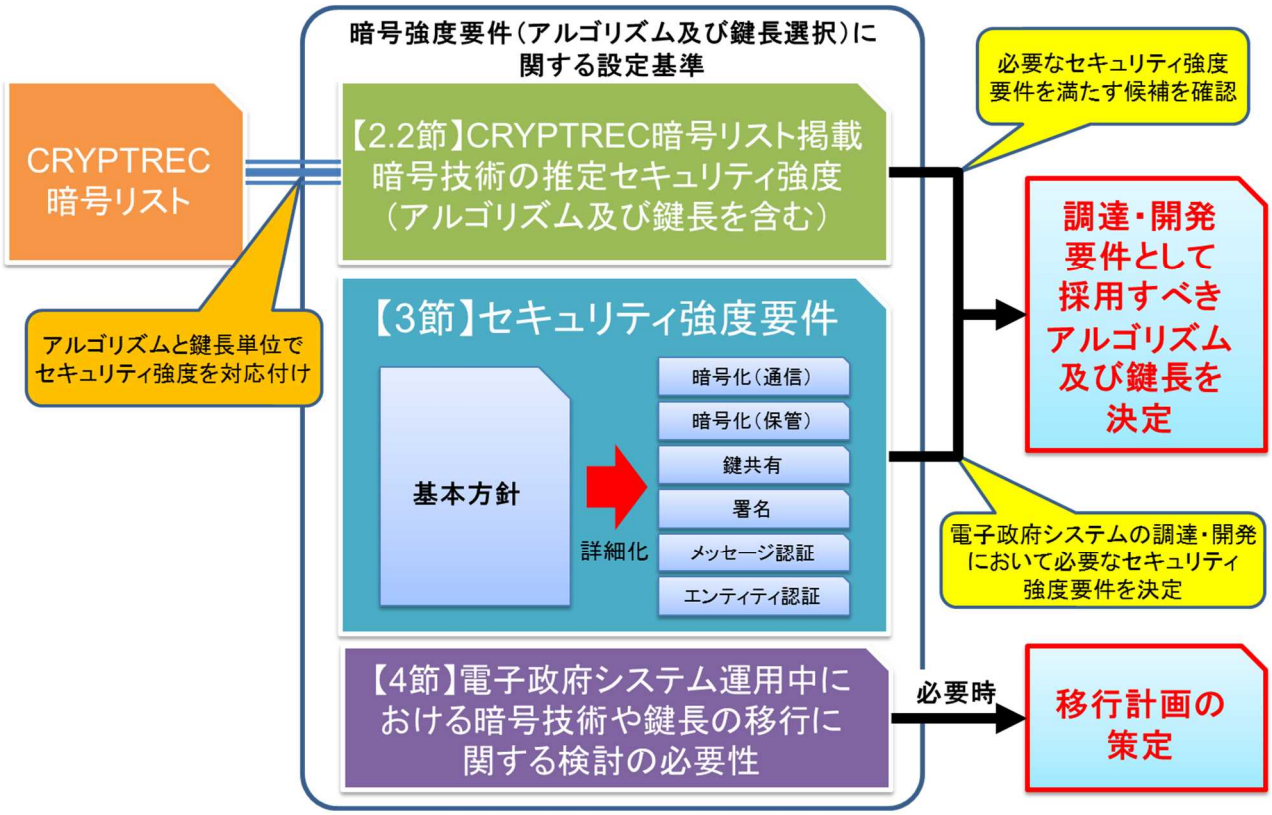


図 1　CRYPTREC 暗号リストと本書の関係

1.2 本書が対象とする読者

本書は、**政府機関等のサイバーセキュリティ対策のための統一基準において適用対象となる電子政府システム（暗号化機能・電子署名機能の導入を行うものに限る。）の調達・開発・運用に関わる責任者及び担当者を対象**とする。

その他の読者については、ボランタリベースで参照・活用してもらうことを歓迎する。

2. 技術的な基礎知識

2.1 暗号処理の種類

本書で取り上げる暗号処理は、表 1の通りである。アルゴリズム及び鍵長の選択にあたっては利用する暗号処理に依存することに留意されたい。

表 1　暗号処理の種類

暗号処理		概要
暗号化（守秘）	通信時	2つ又はそれ以上のエンティティ（ユーザやデバイス等）間の通信路上での盗聴を防止することを目的とした処理のこと。「暗号通信」ともいう。 送信者がデータの暗号化を行うタイミングと受信者が暗号化された通信データを復号するタイミングは時間的にそれほど離れていないことを前提とする。つまり、暗号化された通信データがそのまま長期間保存されることは想定しない。
	保管時	データベースやストレージデバイスなどに保管されるデータの機密性保護を目的とした処理のこと。 長期にわたって安全な保管ができるようにすることが期待され、データの暗号化を実施するタイミングと、復号してデータを取り出すタイミングが大きく異なることが想定される。
	鍵共有	共通鍵暗号を用いた暗号通信に先立ち、2つ又はそれ以上のエンティティ間で、盗聴されずにセッション鍵の共有・確立・合意を行い、当該エンティティ間でセッション鍵を安全に共有することを目的とした処理のこと。
署名		対象データの完全性及び署名者の検証を行い、当該データの完全性を確保することを目的とした処理のこと。当該データの否認防止の確認にも寄与する。 有効な（失効していない）署名検証用の公開鍵証明書の有効期間（*NotBefore* から *NotAfter* の期間）内では、当該データの完全性及び署名者の正当性が確保されることが期待される。
メッセージ認証		通信データや保管データの完全性検証を行い、当該データが変更されていないことを確認することを目的とした処理のこと。
エンティティ認証		正規のエンティティであることを確認することを目的とした処理のこと。

2.2 暗号技術の推定セキュリティ強度表現－ビットセキュリティ

技術分類が異なる暗号技術のアルゴリズムについて、同じ程度のセキュリティ（暗号学的安全

性）[3]を有するかどうかを判断する目安として、“ビットセキュリティ”（等価安全性ということもある）という指標がある。具体的には、評価対象とするアルゴリズムに対して最も効果的な攻撃手法を用いたときに、どの程度の計算量があれば解読できるか（解読計算量[4]）に関連付けられた値で、鍵長とは別に求められる。表記上、解読計算量が 2^x である場合に“x ビットセキュリティ”という。

表 2～表 4 に、CRYPTREC 暗号リストに掲載されている暗号技術について、一般的に使用されているビットセキュリティ（112 ビット、128 ビット、192 ビット及び 256 ビット）を実現していると評価（推定）されている鍵長をアルゴリズムごとに示す。

ビットセキュリティによる評価では、技術分類に関わらず、どのアルゴリズムであっても、解読計算量が大きければセキュリティ（暗号学的安全性）が高く、逆に小さければセキュリティ（暗号学的安全性）が低い。また、解読計算量が実現可能と考えられる計算機能力を大幅に上回っていれば、少なくとも現在知られているような攻撃手法ではそのアルゴリズムを破ることは現実的に不可能であると期待される。

ただし、これらのビットセキュリティの推定値は、本書の発行時点で知られている最良の攻撃方法を用いた際の研究結果に基づいている。そのため、数体篩法、指数計算法、ρ 法といった素因数分解問題や（楕円）離散対数問題の解法アルゴリズムの進展はもとより、全く新しい解法アルゴリズムの登場や大規模な量子コンピュータの実用化などによって、ビットセキュリティの推定値が今後見直される可能性があることに留意されたい。推定値の妥当性を確認する観点から、本書は少なくとも 5 年ごとに（必要があれば適宜）記載内容の再レビューを実施するものとし、必要に応じて適切な修正を加えることを計画している。

【重要な注意】

大規模な量子コンピュータが利用可能になった場合、Shor のアルゴリズムにより多項式時間で素因数分解問題や（楕円）離散対数問題が解けることが知られており、とりわけ CRYPTREC 暗号リストの公開鍵暗号（守秘、署名、鍵共有）に掲載されている全てのアルゴリズムにとって理論的には大きな脅威になっている[5]。

しかし、2021 年 3 月時点の CRYPTREC 調査[6]では、35（＝5×7）の素因数分解が成功しなかったという研究発表などを踏まえ、「現状の量子コンピュータでは暗号で用いるほど大きなパラメータの合成数を素因数分解することは困難であり、暗号で用いるパラメータの問題を解くためには量子ビット数やゲート計算のエラー率など量子コンピュータの性能の大幅な向上が必要であ

---

3 一般には「(暗号の) 安全性」と表現されることが多いが、「安全性」には「物理的な安全性」や「人命などに対する安全性」といった意味で使われることもある。そのため、本書では、「(暗号の) 安全性」のことを「セキュリティ」又は「暗号学的安全性」と表記する。

4 1 つの候補が正しい秘密鍵であるかを判定するために必要な計算量を 1 として、どの程度の候補数を調べれば正しい秘密鍵を確実に（又は高い確率で）求められるかを表した値である。

5 共通鍵暗号、暗号利用モード、メッセージ認証コードに対しては、おおむね鍵長の半分程度のセキュリティ強度に低下するが、公開鍵暗号ほど大きな影響は受けないと評価されている。つまり、鍵長を 256 ビットにするなどの対策で対処可能である。詳細については、CRYPTREC Report 2019「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」を参照されたい。
https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2019r1.pdf

6 CRYPTREC Report 2020「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」を参照されたい。https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2020.pdf

ると考える。」と結論付けている。このことは、**現時点で実現されている量子コンピュータと実際の暗号解読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る**ことを意味している。加えて、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を考慮すると、本書の発行時点（2022 年 3 月）において量子コンピュータによる公開鍵暗号の危殆化時期を予測することは困難である。

したがって、**本書では量子コンピュータによる暗号技術の危殆化は将来的なリスク要因として位置づけ、推定セキュリティ強度の評価に量子コンピュータの影響は考慮していない**。また、**将来的なアルゴリズム及び鍵長の選択要件においてもその影響を考慮しないものとする**。4.7 節も参照されたい。

2.2.1　公開鍵暗号の推定セキュリティ強度

CRYPTREC 暗号リストに掲載されている公開鍵暗号については、アルゴリズムに依存して、数体篩法、指数計算法、ρ 法といった解法アルゴリズムによる攻撃が最も効果的な攻撃方法である。そこで、これらの攻撃方法に基づいて推定される公開鍵暗号のセキュリティ強度をビットセキュリティで表現する。

以上を踏まえ、それぞれのビットセキュリティに対応するアルゴリズムの鍵長を示したのが表 2 である。2 行目のアルゴリズム名は、CRYPTREC 暗号リストに掲載されている公開鍵暗号のアルゴリズムを示している。

- 2 列目は、素因数分解問題ベースの公開鍵暗号（IFC：Integer Factorization Cryptography）を使用する場合の 1 列目で示したビットセキュリティを提供する鍵長（パラメータ）を示す。k は鍵長である。
- 3 列目は、有限体上の離散対数問題ベースの公開鍵暗号（FFC：Finite Field Cryptography）を使用する場合の 1 列目で示したビットセキュリティを提供する鍵長（パラメータ）を示す。L は公開鍵の鍵長、N はプライベート鍵の鍵長である。
- 4 列目は、楕円曲線暗号（ECC：Elliptic Curve Cryptography）を使用する場合の 1 列目で示したビットセキュリティを提供する曲線（パラメータ）を示す。一般に数字部分が鍵長に相当する（ただし、数字部分が 25519 の場合には鍵長 255 ビットに相当する）。例えば、P-256 は鍵長 256 ビットの素体曲線、B-283 は鍵長 283 ビットの拡大体（バイナリ）曲線、Edwards25519 は鍵長 255 ビットのエドワード曲線であることを示す。

表 2　公開鍵暗号の推定セキュリティ強度

セキュリティ強度 （ビットセキュリティ）	IFC RSA-PSS RSASSA-PKCS1-v1.5 RSA-OAEP RSAES-PKCS1-v1_5	FFC DSA DH	ECC ECDSA ECDH PSEC-KEM
112	k = 2048	(L, N) = (2048, 224)	P-224 B-233 K-233
128	k = 3072	(L, N) = (3072, 256)	P-256 B-283 K-283 W-25519 Curve25519 Edwards25519
192	k = 7680	(L, N) = (7680, 384)	P-384 B-409 K-409 W-448 Curve448 Edwards448
256	k = 15360	(L, N) = (15360, 512)	P-521 B-571 K-571

※ P: curve over Prime fields（素体曲線）、B: curve over Binary fields（拡大体（バイナリ）曲線）、K: Koblitz-curve（コブリッツ曲線）、W: Weierstrass-curve（ワイエルシュトラス曲線）、Curve: Montgomery-curve（モンゴメリ曲線）、Edwards: Edwards-curve（エドワード曲線）

2.2.2　共通鍵暗号の推定セキュリティ強度

CRYPTREC 暗号リストの「電子政府推奨暗号リスト」及び「推奨候補暗号リスト」に掲載されている共通鍵暗号については、鍵全数探索法が最も効果的な攻撃方法であるため、鍵全数探索法を用いた時のセキュリティ強度をビットセキュリティで表現する。一方、「運用監視暗号リスト」に掲載されている共通鍵暗号については、鍵全数探索法よりも効果的な攻撃方法（ショートカット攻撃法）が存在することが分かっているため、ショートカット攻撃法を用いた時の推定セキュリティ強度をビットセキュリティで表現する。

以上を踏まえ、それぞれのビットセキュリティに対応するアルゴリズム（及び鍵長）を示したのが表 3 である。

- 2 列目は、1 列目で示したビットセキュリティを提供するブロック暗号のアルゴリズム（及び鍵長）を示す。
- 3 列目は、1 列目で示したビットセキュリティを提供するストリーム暗号のアルゴリズムを示す。
- ブロック暗号を利用する暗号利用モード及びメッセージ認証コードのビットセキュリティは、ベースとなるブロック暗号のアルゴリズム（及び鍵長）に準拠する。

表 3　共通鍵暗号の推定セキュリティ強度

セキュリティ強度（ビットセキュリティ）	ブロック暗号※	ストリーム暗号	認証暗号
112	3-key Triple DES	－	－
128	鍵長 128 ビットを利用する CRYPTREC 暗号リスト掲載のブロック暗号	KCipher-2 Enocoro-128v2 MUGI	－
192	鍵長 192 ビットを利用する CRYPTREC 暗号リスト掲載のブロック暗号		－
256	鍵長 256 ビットを利用する CRYPTREC 暗号リスト掲載のブロック暗号	MULTI-S01	ChaCha20-Poly1305

※ ブロック暗号のセキュリティ強度はブロック長にも依存[7]するため、ブロック暗号を選択する際にはブロック長も併せて**考慮しなければならない**。

2.2.3　ハッシュ関数の推定セキュリティ強度

ハッシュ関数については、利用方法によって要求される特性が異なるため、どちらのセキュリティ強度の推定値を使うのかは利用用途に応じて慎重に**判断すべきである**。特に、署名のように衝突困難性[8]を必要とするアプリケーションで使う場合（衝突困難性に対するセキュリティ強度に依存するケース）と、メッセージ認証コード（HMAC）や鍵導出（KDF）などのように衝突困難性を必要としないアプリケーションで使う場合（原像計算困難性[9]に対するセキュリティ強度に依

7　一般にブロック長が長いほどセキュリティ（暗号学的安全性）が向上する。特にブロック暗号を使ってメッセージ認証を行う場合はその影響が大きい。現在では、128 ビットのブロック長を使うアルゴリズムが一般的である。

8　衝突困難性とは、同じハッシュ値を生成する 2 つのメッセージを見つけることが困難である性質のことをいう。効果的な攻撃方法が見つかっていないハッシュ関数では、ハッシュ長に対するバースデーパラドックスを基にしたセキュリティ強度となり、具体的にはハッシュ長の半分の値で表現される。例えば、ハッシュ長が 256 ビットである場合、バースデーパラドックスを基にしたセキュリティ強度は 128 ビットセキュリティとなる。

9　原像計算困難性とは、与えられたハッシュ値を生成するメッセージを構築したり見つけたりすることが困難である性質のことをいう。効果的な攻撃方法が見つかっていないハッシュ関数では、ハッシュ長に対する全数探索を基にしたセキュリティ強度となり、具体的にはハッシュ長の値で表現される。

存するケース）とを分けて考える必要がある。

衝突困難性に対するセキュリティ強度については、CRYPTREC 暗号リストの「電子政府推奨暗号リスト」及び「推奨候補暗号リスト」に掲載されているハッシュ関数のいずれにおいてもバースデーパラドックスよりも効率的に衝突するメッセージ組を求める効果的な攻撃方法が見つかっていないため、バースデーパラドックスによる衝突困難性に対するセキュリティ強度をビットセキュリティで表現する。なお、「運用監視暗号リスト」に掲載されているハッシュ関数 SHA-1 と RIPEMD-160 は、ハッシュ長が 160 ビットであるため、衝突困難性に対して 80 ビット以下[10]のセキュリティ強度しかない。このため、表 4 には含まれていない。

原像計算困難性に対するセキュリティ強度については、CRYPTREC 暗号リストに掲載されているハッシュ関数のいずれもが全数探索法よりも効果的な攻撃方法が見つかっていないため、全数探索法を用いた時のセキュリティ強度をビットセキュリティで表現する。

表 4　ハッシュ関数の推定セキュリティ強度

セキュリティ強度 （ビットセキュリティ）	衝突困難性に対するセキュリティ強度に依存するケース （署名と組み合わせて利用する場合）	原像計算困難性に対するセキュリティ強度に依存するケース （HMAC や KDF に使う場合）
112	－	－
128	SHA-256 SHA-512/256 SHA3-256 SHAKE128 SHAKE256（ハッシュ長 256 ビット）	SHAKE128 SHA-1※ RIPEMD-160※
192	SHA-384 SHA3-384 SHAKE256（ハッシュ長 384 ビット）	－
256	SHA-512 SHA3-512 SHAKE256（ハッシュ長 512 ビット）	SHA-1、RIPEMD-160 及び SHAKE128 を除く CRYPTREC 暗号リスト掲載のハッシュ関数全て
備考	※SHA-1 及び RIPEMD-160 は、112 ビットのセキュリティ強度に達しないので、記載していない	※SHA-1 及び RIPEMD-160 は、192 ビットのセキュリティ強度に達しないので、128 ビットセキュリティに置いている

以上を踏まえ、それぞれのハッシュ関数のビットセキュリティを表現したのが表 4 である。

- 2 列目は、衝突困難性に対するセキュリティ強度に依存するケースにおいて、1 列目で示したビットセキュリティを提供するハッシュ関数のアルゴリズムを示す。署名と組み合わせてハッシュ関数を使う場合は、この列を参照すること。

[10] SHA-1 については、衝突困難性に対してバースデーパラドックスよりも効果的な攻撃方法が見つかっているため、衝突困難性に対するセキュリティ強度は 80 ビットセキュリティにも達しない。

- 3 列目は、原像計算困難性に対するセキュリティ強度に依存するケースにおいて、1 列目で示したビットセキュリティを提供するハッシュ関数のアルゴリズムを示す。メッセージ認証コード（HMAC）や鍵導出（KDF）にハッシュ関数を使う場合は、この列を参照すること。なお、利用する鍵のエントロピーがそのビットセキュリティ以上のエントロピーを有していることを前提とする。

2.3 暗号技術の組合せによるセキュリティ強度の考え方

電子政府システムによっては、2.1 節に記載された暗号処理のいくつかを組み合わせて実現することが求められる。このような場合、異なる種類の暗号処理に対して異なる暗号技術のアルゴリズムと鍵を使用する（例えば、暗号化に AES を使用し、署名に RSA を使用する）やり方もあれば、同じアルゴリズムと同じ鍵、又は同じアルゴリズムと異なる鍵で使用する（例えば、AES を使用して暗号化とメッセージ認証を実行する）やり方もある。また、利用するアルゴリズムも複数のアルゴリズムから選択できる場合もある（例えば、鍵共有において、公開鍵暗号なら RSA、Diffie-Hellman（DH）、ECDH などから、共通鍵暗号ならブロック暗号のいずれかのアルゴリズムを使った鍵ラッピング法から選択できる）。

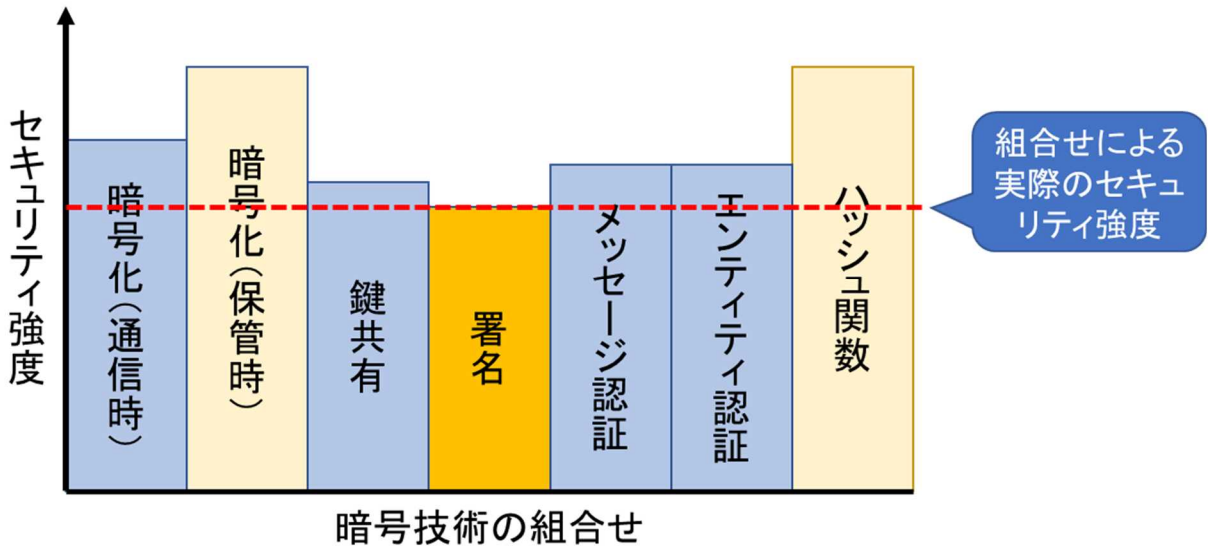


図 2　暗号技術の組合せによるセキュリティ強度（イメージ図）

そのため、電子政府システムでは、異なるセキュリティ強度を有する複数のアルゴリズムと鍵長を組み合わせて実現されることも多い。このような場合、最終的なセキュリティ強度は、最も弱いセキュリティ強度である暗号技術のアルゴリズムと鍵長の組合せによって決定される[11]（図

[11] 「樽理論」等とも呼ばれる。

2 参照)。

以下に、いくつかの暗号技術の組合せ例を用いてセキュリティ強度の考え方を示す。

- 暗号通信において、セッション鍵の確立を公開鍵暗号で行い、データの暗号化は共通鍵暗号で行うハイブリット暗号化方式の場合、そのセキュリティ強度はより弱い方のアルゴリズムと鍵長の組合せによって決定される。例えば、256 ビット鍵の AES でデータの暗号化をする場合、通常であれば 256 ビットのセキュリティ強度を提供する。しかし、256 ビットのセッション鍵を確立するために P-256 ビット鍵（素体曲線での鍵長 256 ビットの鍵）の ECDH が使用される場合、P-256 ビット鍵の ECDH は 128 ビットセキュリティに該当するため（2.2.1 節参照）、そのセッション鍵で保護されたデータに対しては（256 ビットセキュリティではなく）128 ビットのセキュリティ強度しか提供されない。
- ハッシュ関数と署名アルゴリズムを組み合わせて署名を計算する場合、署名のセキュリティ強度はより弱い方のアルゴリズムによって決定される。例えば、SHA-256 を 2048 ビット鍵の RSA 署名と組み合わせて使用する場合、2048 ビット鍵の RSA 署名は 112 ビットセキュリティに該当するため（2.2.1 節参照）、その署名に対して（128 ビットセキュリティではなく）112 ビットのセキュリティ強度しか提供されない。

所定のセキュリティ強度をサポートするためには、アルゴリズム及び鍵長を慎重に**選択しなければならない**。例えば、通信されるデータを保護するために 128 ビットセキュリティ強度で暗号化、署名及び鍵共有を行う場合、以下のような暗号技術の選択の組合せが考えられる。

i) 暗号化：共通鍵暗号で 128 ビットセキュリティ強度を有するアルゴリズム（と鍵長）のなかから選択する（例えば、128 ビット鍵の AES）。
ii) 署名：SHA-256 を署名生成前のデータハッシュに使用する。署名アルゴリズムは、128 ビットセキュリティ強度を有するアルゴリズム及び鍵長のなかから選択する（例えば、3072 ビット鍵の RSA 署名）。なお、同一のビットセキュリティ強度で複数のアルゴリズムと鍵長が利用可能な場合、アルゴリズムの性能、メモリ要件などに基づいて選択してよい。
iii) 鍵共有：128 ビットセキュリティ強度を有するアルゴリズム及び鍵長のなかから選択する。例えば、ECDH が利用可能な場合は、ECDH と 128 ビットセキュリティ強度の楕円曲線（P-256 など）を使用する。

3. セキュリティ強度要件の設定

本節では、保護対象のデータに対して電子政府システムが適切な保護を提供するために、CRYPTREC 暗号リストに掲載された暗号技術のなかから、適切なアルゴリズム及び鍵長を選択するための要件を提示する。なお、選択にあたっては利用する暗号処理の種類に依存することにも留意されたい。

【重要な注意】

2.2 節に記載の通り、量子コンピュータによる暗号技術の危殆化は将来的なリスク要因として位置づけ、本書でのアルゴリズム及び鍵長の選択要件においてはその影響を考慮していない。そのため、運用寿命が長期にわたる電子政府システムであって、特にその中で公開鍵暗号や署名を利用している場合には、将来的に耐量子計算機暗号（PQC: Post-Quantum Cryptography）の採用も視野に入れた移行計画が必要となる場合があることに留意されたい（4.7 節参照）。

3.1 電子政府システムに求められる運用寿命とセキュリティ強度要件の関係

電子政府システムを調達又は開発する際は、そのシステムの検討・設計開始から構築、運用、さらに運用終了・廃棄までの運用寿命全体と、その期間に実現するセキュリティ強度の関係を考慮してセキュリティ強度要件を設定し、その強度要件を満たすアルゴリズム及び鍵長を調達・開発要件としなければならない。これは、時間の経過とともに解読計算能力が向上するため、運用開始時と比較して安全性が低下し、攻撃が成功する可能性が高まるリスクがあるためである。

結果として、電子政府システムの運用途中でより安全なアルゴリズム及び鍵長への移行が必要となる場合があることにも留意されたい。また、システム運用中における予期しない危殆化等への対処のため、アルゴリズムと鍵長を容易に変更できるように配慮した移行計画を考慮すべきであり（4 節参照）、特に運用寿命が長期にわたるシステムの場合には重要な視点である。

本書では、電子政府システムの運用寿命の期間と求められるセキュリティ強度要件の関係から 3 つの要件設定方法を示す（図 3 参照）。電子政府システムの検討状況を踏まえ、適切な要件設定方法を選択されたい（図 4 参照）。

【要件設定方法①】

電子政府システムの運用寿命全体を通して必要なセキュリティ強度要件を設定し、その強度要件を満たすアルゴリズム及び鍵長を**サポート（実装）しなければならない**。その際、必要なセキュリティ強度を過小評価又は過大評価しないように**注意すべきである**。

なお、利用終了時期を明確化し、それまでにより安全なアルゴリズム及び鍵長に移行することを条件に、その期間中は安全と期待されるアルゴリズム及び鍵長を一緒にサポート（実装）してもよい。

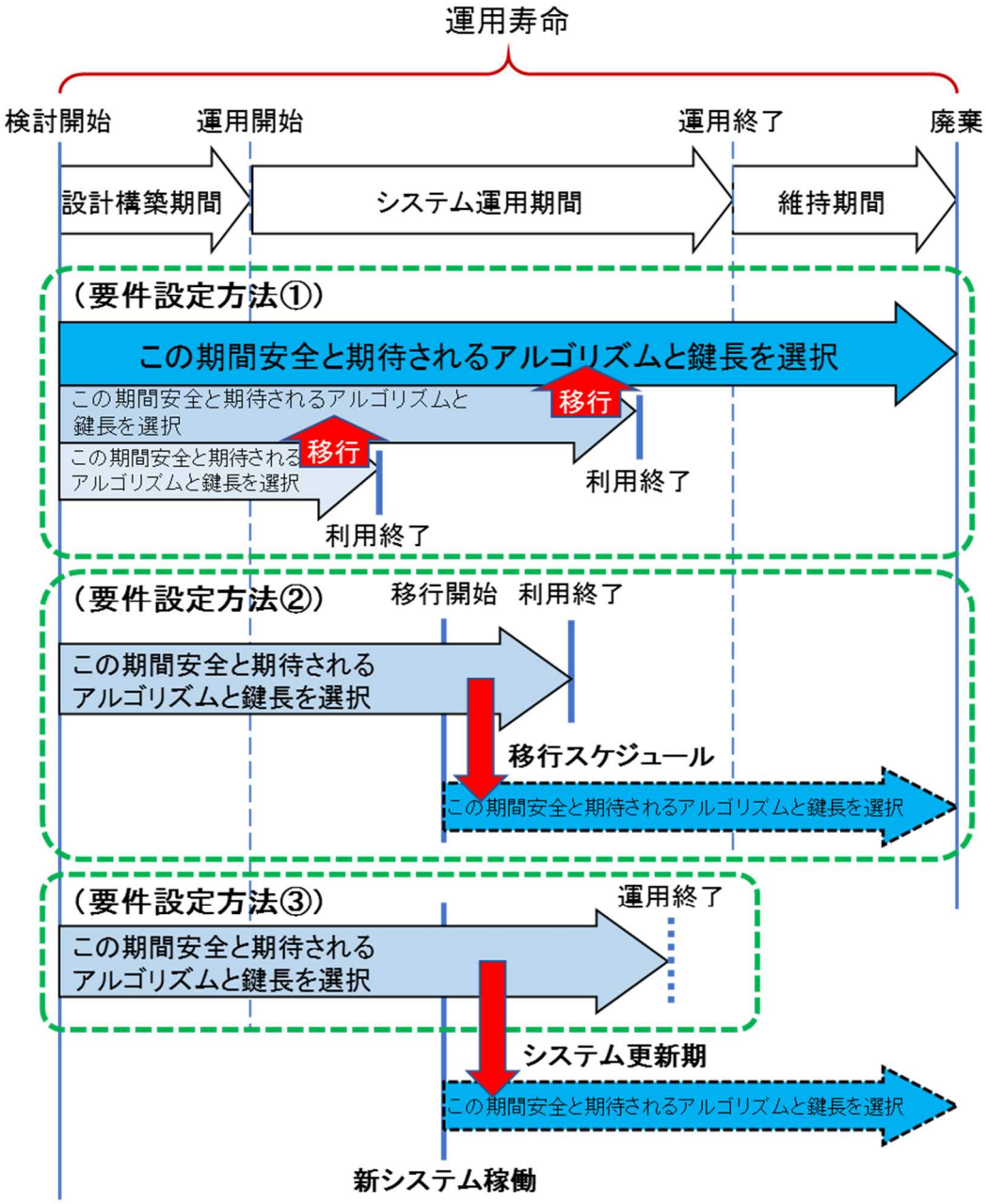


図 3　システムの運用寿命と求められるセキュリティ強度要件

【要件設定方法②】

対象となる電子政府システムの調達や開発における何らかの制約により、運用寿命全体を通して必要なセキュリティ強度要件を当初から設定することが困難である場合には、セキュリティ強度要件を切り替える移行時期を明確化したスケジュールを立案することを条件としたうえで、その移行時期終了まで安全に運用するために必要なセキュリティ強度要件を設定し、その強度要件を満たすアルゴリズム及び鍵長を**サポート（実装）しなければならない**。その際、そのスケジュールには移行開始予定時期及び移行完遂予定時期を明示すべきである。

【要件設定方法③】

対象となる電子政府システムにおいて、運用寿命が決まっていない（明確ではない）場合には、システム更新期を明確化したスケジュールを立案することを条件としたうえで、その更新期まで安全に運用するために必要なセキュリティ強度要件を設定し、その強度要件を満たすアルゴリズム及び鍵長を**サポート（実装）しなければならない**。なお、そのスケジュールにおいて、新システムの稼働開始予定時期及び新旧システムの併用運用想定期間を示しておくことが望ましい。

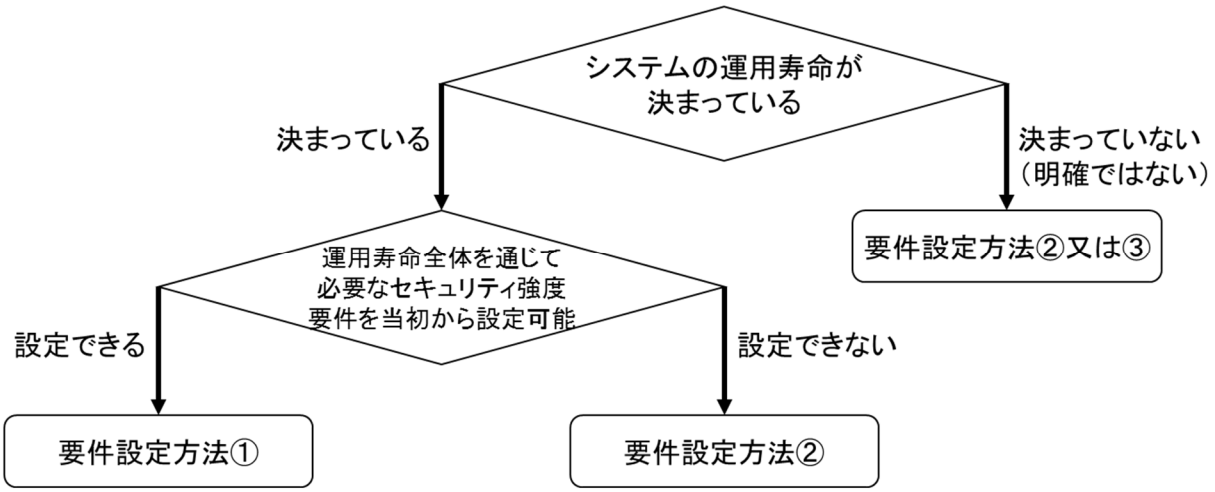


図 4　要件設定方法の選択フロー

3.2 セキュリティ強度要件の基本設定方針

電子政府システムの調達・開発にあたっての基本方針として、3.1 節の考え方に基づき、**最低限のセキュリティ強度要件を以下の方針で設定し、その強度要件を満たすアルゴリズム及び鍵長を選択（3.3 節参照）することを調達・開発要件としなければならない**。

なお、本書では、標準文書保存期間基準[12]を参考に、最長想定運用終了・廃棄年を 2070 年（本書発行後、約 50 年間）とした。

- 必要なセキュリティ強度要件は表 5 をベースとして**設定しなければならない**。
  なお、表 5 はセキュリティ強度要件の基本方針を示したものであり、実際には暗号処理の種類に依存して、具体的な要件は微妙に異なることに留意されたい。3.4 節以降の表 6～表 9 に、暗号処理ごとの詳細なセキュリティ強度要件を規定しているので、それらも参照すること。
- 表 5 では、システムの想定運用終了・廃棄年又は利用期間の終了年を基準に必要なセキュリティ強度要件を設定する。

[12] https://www.kantei.go.jp/jp/singi/genshiryoku_bousai/pdf/hozonhyou.pdf

例 1）システムの運用終了・廃棄年を 2037 年に予定しているであれば「2031～2040」の列を、2053 年に予定しているのであれば「2051～2060」の列を参照してセキュリティ強度要件を設定する。システムの運用開始年が 2023 年であっても「2022～2030」の列を参照するわけではないことに留意すること。

例 2）署名を利用するシステムの場合、利用期間の終了年は署名生成を行わなくなる年ではなく、全ての署名検証が必要なくなる年で**判断しなければならない**。例えば、署名生成を 2040 年まで行うシステムにおいて、署名検証用の公開鍵証明書の有効期間が 5 年の場合であれば、利用期間の終了年は 2040 年ではなく 2045 年である。

例 3）運用終了・廃棄年が 2060 年であり、移行期間を 2041～2045 年と想定するシステムならば、2041 年移行開始 2045 年移行完遂予定の移行スケジュールを立案するとともに、当初は「2041～2050」の列を参照してセキュリティ強度要件を設定する。

例 4）想定運用開始時期が 2040 年前半を想定する次期システムである場合、新旧システムの併用運用期間が 5 年間であれば 2040 年前半から 5 年間のシステム更新スケジュールを立案するとともに、当初は「2041～2050」の列を参照してセキュリティ強度要件を設定する。10 年程度との併用運用期間ならば、10 年間のシステム更新スケジュールを立案するとともに、当初は「2051～2060」の列を参照する。

- 様々な暗号処理を統合して利用するシステムを調達や開発する際には、個別の暗号処理でのセキュリティ強度だけでなく、システム全体として必要なセキュリティ強度要件が達成されているかも**確認すべきである**。

表 5　セキュリティ強度要件の基本設定方針

<table>
<tr><th colspan="2">想定運用終了・廃棄年／
利用期間</th><th>2022～2030</th><th>2031～2040</th><th>2041～2050</th><th>2051～2060</th><th>2061～2070</th></tr>
<tr><td rowspan="2">112 ビット
セキュリティ</td><td>新規生成
((a)参照)</td><td rowspan="2">移行完遂
期間
((c)参照)</td><td>利用不可</td><td rowspan="2">利用不可</td><td rowspan="2">利用不可</td><td rowspan="2">利用不可</td></tr>
<tr><td>処理
((b)参照)</td><td>許容</td></tr>
<tr><td rowspan="2">128 ビット
セキュリティ</td><td>新規生成
((a)参照)</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">移行完遂
期間
((c)参照)</td><td>利用不可</td><td rowspan="2">利用不可</td></tr>
<tr><td>処理
((b)参照)</td><td>許容</td></tr>
<tr><td rowspan="2">192 ビット
セキュリティ</td><td>新規生成
((a)参照)</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td></tr>
<tr><td>処理
((b)参照)</td></tr>
<tr><td rowspan="2">256 ビット
セキュリティ</td><td>新規生成
((a)参照)</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td></tr>
<tr><td>処理
((b)参照)</td></tr>
</table>

(a) ***新規に暗号保護を適用***する（例えば、暗号化や署名生成を実行する）際は、原則として、2040年までは128ビット以上のセキュリティ強度のものを**選択すべきである**。2041年以降は192ビット以上のセキュリティ強度のものを**選択すべきである**。

(b) ***保護済みのデータに対して処理を実行***する（例えば、復号や署名検証を実行する）際は、2040年までは128ビット以上、2041年以降は192ビット以上のセキュリティ強度のものを**選択すべきである**。ただし、保護済みのデータに対する正当性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合に、2031年以降も2040年までの必要な範囲内で112ビットセキュリティ強度のものを選択することを許容する。同様に、2051年以降も2060年までの必要な範囲内で128ビットセキュリティ強度のものを選択することを許容する。

(c) 移行完遂期間内に、よりセキュリティ強度の高い暗号技術又は鍵長への移行を完遂させることを前提として、利用する暗号処理が短期間で完結する場合（例：エンティティ認証）、又は既存の電子政府システムの継続利用やそれらとの互換性・相互接続性維持などの必要がある場合には、2030年までは112ビットセキュリティ強度のものを、2050年までは128ビットセキュリティ強度のものを選択することを許容する。

凡例：

- 1列目はビットセキュリティ強度を示し、2つのサブ行に分割されている。上段のサブ行は「新規生成」であり、新規データに対して新たな暗号保護を施す場合に参照する（(a)に該当）。下段のサブ行は「処理」であり、過去に暗号保護が施された保護済みのデータに対して復号や検証などの処理を行う場合に参照する（(b)に該当）。
- “利用可”とは、そのセキュリティ強度を満たす暗号技術であれば安全であると期待される期間であることを示す。新規調達や更新調達を行うシステムにおけるセキュリティ強度要件として設定することができる。
- “利用不可”とは、そのセキュリティ強度の暗号技術では必要なセキュリティ（暗号学的安全性）を確保できないと見なされており、もはや利用すべきではない期間であることを示す。新規調達や更新調達を行うシステムはもとより、**既存の電子政府システムでも利用してはならない**。
- “許容”とは、そのセキュリティ強度の暗号技術では必要なセキュリティ（暗号学的安全性）を確保するには必ずしも十分ではないレベルであると想定され得るが、その正当性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合に、過去に暗号保護が施された保護済みのデータに対して復号や検証の処理を行うことを許容する期間であることを示す。なお、3.4節以降では、処理の違いにより、“復号許容”又は“検証許容”と示す。
- “移行完遂期間”とは、そのセキュリティ強度の暗号技術では必要なセキュリティ（暗号学的安全性）を確保するには必ずしも十分ではないレベルになりつつあると想定され、この期間中に、**よりセキュリティ強度の高い暗号技術及び鍵長への移行を完遂させなければならない**期間であることを示す。そのため、利用する暗号処理が短期間で完結する場合（例：エンティティ認証）、又は既存の電子政府システムの継続利用やそれらとの互換性・相互接続性維持のための利用に**限定すべき**であり、新規調達や更新調達を行うシステムにおい

て、**既存の電子政府システムとの互換性・相互接続性維持が必要でない場合や代替手段がある場合には、利用を許容すべきではない**ことに留意されたい。

【重要な注意】

表 5 は、2021 年末時点での暗号技術のセキュリティ（暗号学的安全性）評価の現状、及び今後のコンピュータ性能の向上予測（具体的にはムーアの法則[13]）を主とした暗号解読の可能性予測、並びに世界各国での類似の文書類の記載内容など（Appendix 参照）を踏まえたうえで、2021 年時点で 2070 年までの予測可能なセキュリティマージンを持った基準として定めたものである。今後、予測の妥当性を確認する観点から、本書は少なくとも 5 年ごとに記載内容の再レビューを実施するものとし、必要に応じて適切な修正を加えることを計画している。

3.3 アルゴリズム及び鍵長の選択・実装及び利用の基本方針

電子政府システムの調達・開発においては、3.2 節及び 3.4～3.7 節を踏まえて設定したセキュリティ強度要件と同じかそれ以上のセキュリティ強度を満たすアルゴリズム及び鍵長を推定セキュリティ強度の表（2.2 節表 2～表 4 参照）から選択して**サポート（実装）しなければならない**。例えば、セキュリティ強度要件として 128 ビットセキュリティが設定された時、公開鍵暗号であれば鍵長 3072 ビットの RSA（2.2.1 節表 2 参照）、共通鍵暗号であれば鍵長 128 ビットの CRYPTREC 暗号リスト掲載のブロック暗号（2.2.2 節表 3 参照）、ハッシュ関数であれば SHA-256（2.2.3 節表 4 参照）などが選択肢となる。

なお、設定したセキュリティ強度要件以下のセキュリティ（暗号学的安全性）のアルゴリズムや鍵長をサポート（実装）すること自体は妨げない。

ただし、サポート（実装）されたアルゴリズム及び鍵長の全てが常に利用されてよいわけでないことに**留意しなければならない**。**サポート（実装）されたアルゴリズム及び鍵長の利用期間については、そのセキュリティ強度に応じて、暗号処理ごとのセキュリティ強度要件（3.4 節表 6～3.7 節表 9）に従って定めなければならない**。

具体的には、特定のアルゴリズム及び鍵長について、保護されたデータが安全であり続けると評価されて「利用可」とされた期間は「当該アルゴリズムのセキュリティ寿命」と呼ばれ、その期間中はどの対象データに対しても適切な保護を提供することが期待される。一方、特定のデータに対して暗号保護が適用されてから最終的に処理をする必要がなくなるまでの期間（つまり、機密性や完全性を保持する必要がある期間）は「当該データのセキュリティ寿命」と呼ばれ、その期間中は当該データに対して適切な保護を提供することが期待される。

このため、**「データのセキュリティ寿命」は利用する「アルゴリズムのセキュリティ寿命」に包含されるように扱わなければならない**（図 5 参照）。

---

[13] 「集積回路上のトランジスタ数が 18 ヶ月ごとに 2 倍になる」という経験法則のこと

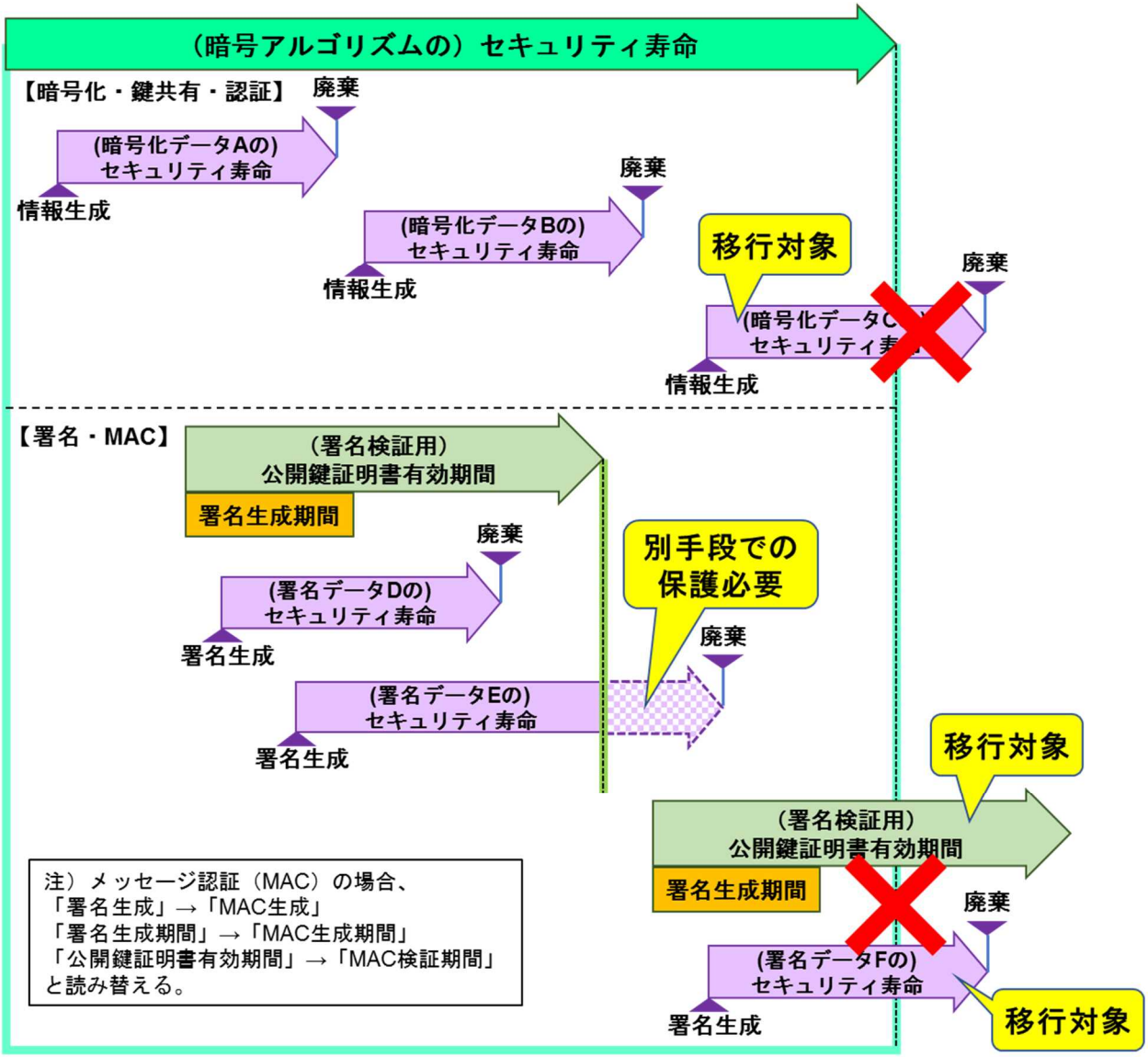


図 5　アルゴリズムのセキュリティ寿命とデータのセキュリティ寿命の関係

例えば、保管時の暗号化（3.5 節参照）の場合、以下のように定められる。

- 想定運用終了・廃棄年を 2060 年に予定しているシステムの場合（図 6 参照）、最終的には 192 ビット以上のセキュリティ強度のアルゴリズム及び鍵長を**サポート（実装）しなければならない**。なお、112 ビット及び 128 ビットのセキュリティ強度のアルゴリズムや鍵長のものを**サポート（実装）してもよい**。
- 新規にデータを暗号化する時は、原則として 2040 年までは 128 ビット以上のセキュリティ強度で、2041 年以降は 192 ビット以上のセキュリティ強度で**暗号化を行うべきである**。ただし、移行完遂期間中に移行スケジュールを完遂することを条件に、既存の電子政府システムの継続利用やそれらとの互換性・相互接続性維持のための利用に限定して 2030 年

までは 112 ビットセキュリティ強度、2050 年までは 128 ビットセキュリティ強度での暗号化が許容される。

- 112 ビットセキュリティ強度で既に暗号化されたデータは、機密性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合に、2040 年までの継続利用（復号）が許容される。同様に、128 ビットセキュリティ強度で暗号化されたデータは、2051 年以降も 2060 年までの継続利用（復号）が許容される。
- 112 ビットセキュリティ強度で既に暗号化されたデータを 2041 年以降も利用する場合には、2040 年までによりセキュリティ強度の高いアルゴリズム及び鍵長で再暗号化するか、別の保護手段によって**保護し直さなければならない**。

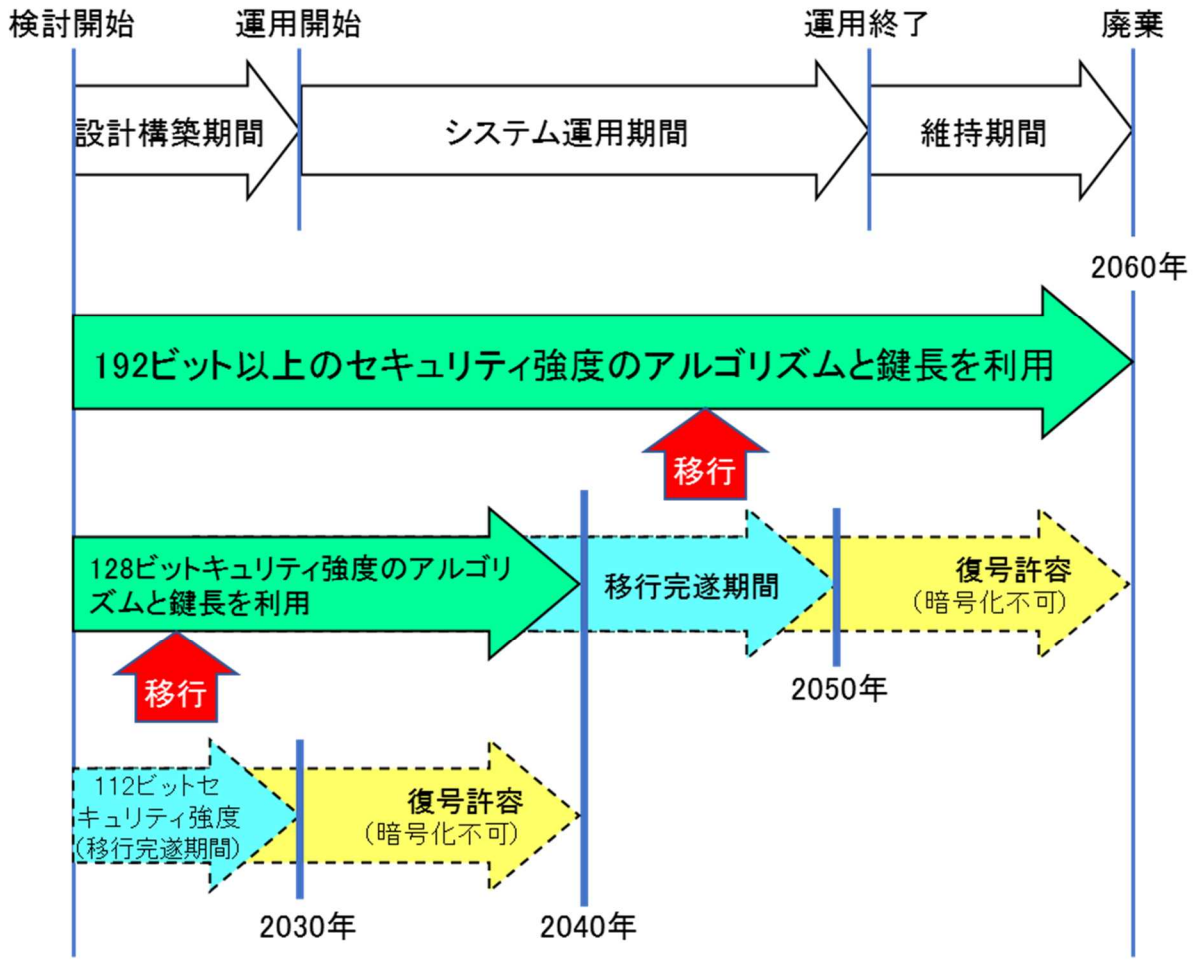


図 6　保管時の暗号化の例

3.4 通信時及び鍵共有の暗号化におけるセキュリティ強度要件

通信時及び鍵共有における暗号化処理では、通常、送信者がデータ暗号化を行うタイミングと

受信者が暗号化データを復号するタイミングは時間的にそれほど離れていないと考えられる。このため、通信時及び鍵共有におけるセキュリティ強度要件を、3.2 節及び 3.3 節を踏まえ、以下の通りとする。システムの調達や開発にあたっては、それらの**要件を全て満たすようにしなければならない**。

① 通信時におけるセキュリティ強度要件は表 6 に**従わなくてはならない**。

表 6 通信時及び鍵共有の暗号化におけるセキュリティ強度要件

想定運用終了・廃棄年／利用期間		2022～2030	2031～2040	2041～2050	2051～2060	2061～2070
112 ビットセキュリティ	新規生成(暗号化)	移行完遂期間	利用不可	利用不可	利用不可	利用不可
	処理(復号)					
128 ビットセキュリティ	新規生成(暗号化)	利用可	利用可	移行完遂期間	利用不可	利用不可
	処理(復号)					
192 ビットセキュリティ	新規生成(暗号化)	利用可	利用可	利用可	利用可	利用可
	処理(復号)					
256 ビットセキュリティ	新規生成(暗号化)	利用可	利用可	利用可	利用可	利用可
	処理(復号)					

【サポート（実装）要件】

- 最終的には、想定運用終了・廃棄年が 2040 年までならば 128 ビット以上のセキュリティ強度の、2041 年以降なら 192 ビット以上のセキュリティ強度のアルゴリズム及び鍵長を**サポート（実装）しなければならない**。
- 対象となる電子政府システムの調達や開発における何らかの制約により、運用寿命全体を通じた必要なセキュリティ強度要件を設定することが困難である場合には、セキュリティ強度を切り替える移行時期を明確化したスケジュールを立案したうえで、その移行時期終了まで安全に運用するために必要なセキュリティ強度要件を満たすアルゴリズム及び鍵長を**サポート（実装）しなければならない。**例えば、移行時期を 2041～2045 年とする場合、当初は 128 ビット以上のセキュリティ強度のものを**サポート（実装）しなければならない**。

- 運用寿命が定まっていない場合には、システム更新期を明確化したスケジュールを立案することを条件としたうえで、その更新期まで安全に運用するために必要なセキュリティ強度要件を満たすアルゴリズム及び鍵長を**サポート（実装）しなければならない**。例えば、新システムの稼働開始予定時期が 2043 年である場合、新旧システムの併用運用想定期間が 5 年間であれば 128 ビット以上のセキュリティ強度のものを、10 年間であれば 192 ビット以上のセキュリティ強度のものを**サポート（実装）しなければならない**。

【利用要件】

- 原則として、2040 年までは 128 ビット以上のセキュリティ強度で、2041 年以降は 192 ビット以上のセキュリティ強度で**暗号化・復号とも行わなければならない**。
  ただし、移行完遂期間中に移行スケジュールを完遂することを条件に、既存の電子政府システムの継続利用やそれらとの互換性・相互接続性維持のための利用に限定して、2030 年までは 112 ビットセキュリティ強度で、2050 年までは 128 ビットセキュリティ強度で暗号化・復号を行ってもよい。
- データ暗号化を行うタイミングと暗号化データを復号するタイミングは時間的にそれほど離れていないので、「新規生成」において「利用不可」の期間では「処理」においても「利用不可」とする。

② 鍵共有におけるセキュリティ強度要件は、表 6 を満たすだけでなく、鍵共有後に利用する暗号処理で必要とされるセキュリティ強度と同等以上のセキュリティ強度で**暗号化・復号とも行うべきである**。
例えば、通信データの暗号化を 256 ビットセキュリティの強度で行うのであれば、その際のセッション鍵の鍵共有においても 256 ビットセキュリティの強度で行うべきである。

③ 受信した暗号化データをそのまま**長期間保存すべきではない**。もし当該データを長期間保存する必要がある場合には、3.5 節の要件に準拠しているかどうかを確認しなければならない。準拠していない場合には、再暗号化など、3.5 節の要件に準拠させるのに必要な処理を**行うべきである**。

④ 表 6 では、攻撃者が暗号化された通信データを先に窃取しておいて解読が可能になった時期に復号を行う攻撃（Store (Harvest)-then-decrypt、Store now & decrypt later、Retrospective Decryption ともいう）は対象外である。この攻撃を考慮する必要がある場合には、通信や鍵共有における場合であっても、当初から 3.5 節の要件を**準用すべきである**。その際、想定する利用期間は、通信や鍵共有を行うタイミングではなく、当該通信データの機密性を保護しておくべき期間全体に広がることに**留意しなければならず**、その広がった期間において必要なセキュリティ強度が求められることに**注意すべきである**。例えば、通信自体は 2025 年に行われたとしてもその内容が 2065 年まで秘匿すべき機密情報である場合、表 6 の「2022～2030 年」ではなく、3.5 節表 7 の「2061～2070」を参照してセキュリティ強度を設定する。

なお、この種の攻撃に対しては後から防ぐことができないため、電子政府システムの調達・開発時点で対策の必要性について十分に**検討すべきである**。

⑤ ブロック暗号を利用する際は、アルゴリズム及び鍵長の選択と合わせ、CRYPTREC 暗号リストに記載の暗号利用モードを**使用しなければならない**。

3.5 保管時の暗号化におけるセキュリティ強度要件

保管時における暗号化処理では、暗号化されたデータを長期間にわたって継続的に利用する場面や、法令等のルールにより機密性を保持したまま長期間保管する必要がある場面が考えられる。つまり、データ暗号化を実施するタイミングと、その暗号化データを復号してデータを取り出すタイミングが大きく異なる場合があることが想定される。また、同一システム内に短期間のみセキュリティ（暗号学的安全性）を確保して保管できればよいデータと長期にわたって安全に保管する必要があるデータが混在する可能性もある。

このようにデータの保管方法はいろいろなケースが考えられるが、本書では、長期にわたって安全に保管できることを前提として保管時におけるセキュリティ強度要件を定めるものとし、その要件を、3.2 節及び 3.3 節を踏まえ、以下の通りとする。システムの調達や開発にあたっては、それらの**要件を全て満たすようにしなければならない**。

① 保管時におけるセキュリティ強度要件は表 7 に**従わなくてはならない**。

表 7 保管時の暗号化におけるセキュリティ強度要件

<table>
<tr><th colspan="2">想定運用終了・廃棄年／利用期間</th><th>2022～2030</th><th>2031～2040</th><th>2041～2050</th><th>2051～2060</th><th>2061～2070</th></tr>
<tr><td rowspan="2">112 ビット
セキュリティ</td><td>新規生成
(暗号化)</td><td rowspan="2">移行完遂
期間</td><td>利用不可</td><td rowspan="2">利用不可</td><td rowspan="2">利用不可</td><td rowspan="2">利用不可</td></tr>
<tr><td>処理
(復号)</td><td>復号許容</td></tr>
<tr><td rowspan="2">128 ビット
セキュリティ</td><td>新規生成
(暗号化)</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">移行完遂
期間</td><td>利用不可</td><td rowspan="2">利用不可</td></tr>
<tr><td>処理
(復号)</td><td>復号許容</td></tr>
<tr><td rowspan="2">192 ビット
セキュリティ</td><td>新規生成
(暗号化)</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td></tr>
<tr><td>処理
(復号)</td></tr>
<tr><td rowspan="2">256 ビット
セキュリティ</td><td>新規生成
(暗号化)</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td></tr>
<tr><td>処理
(復号)</td></tr>
</table>

【サポート（実装）要件】

- 最終的には、想定運用終了・廃棄年が 2040 年までならば 128 ビット以上のセキュリティ強度の、2041 年以降なら 192 ビット以上のセキュリティ強度のアルゴリズム及び鍵長を**サポート（実装）しなければならない**。
- 対象となる電子政府システムの調達や開発における何らかの制約により、運用寿命全体を通じた必要なセキュリティ強度要件を設定することが困難である場合には、セキュリティ強度を切り替える移行時期を明確化したスケジュールを立案したうえで、その移行時期終了まで安全に運用するために必要なセキュリティ強度要件を満たすアルゴリズム及び鍵長を**サポート（実装）しなければならない**。例えば、移行時期を 2041～2045 年とする場合、当初は 128 ビット以上のセキュリティ強度のものを**サポート（実装）しなければならない**。
- 運用寿命が定まっていない場合には、システム更新期を明確化したスケジュールを立案することを条件としたうえで、その更新期まで安全に運用するために必要なセキュリティ強度要件を満たすアルゴリズム及び鍵長を**サポート（実装）しなければならない**。例えば、新システムの稼働開始予定時期が 2043 年である場合、新旧システムの併用運用想定期間が 5 年間であれば 128 ビット以上のセキュリティ強度のものを、10 年間であれば 192 ビット以上のセキュリティ強度のものを**サポート（実装）しなければならない**。

【利用要件】

- 原則として、2040 年までは 128 ビット以上のセキュリティ強度で、2041 年以降は 192 ビット以上のセキュリティ強度で**暗号化・復号とも行わなければならない。**
  ただし、移行完遂期間中に移行スケジュールを完遂することを条件に、既存の電子政府システムの継続利用やそれらとの互換性・相互接続性維持のための利用に限定して、2030 年までは 112 ビットセキュリティ強度で、2050 年までは 128 ビットセキュリティ強度で暗号化・復号を行ってもよい。
- 112 ビットセキュリティ強度で既に暗号化されたデータは、データの機密性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合に、2040 年までの継続利用（復号）が許容される。同様に、128 ビットセキュリティ強度で暗号化されたデータは、2051 年以降も 2060 年までの継続利用（復号）が許容される。
- 112 ビットセキュリティ強度で既に暗号化されたデータを 2041 年以降も利用する場合には、2040 年までによりセキュリティ強度の高いアルゴリズム及び鍵長によって再暗号化するか、別の保護手段によって**保護し直さなければならない**。128 ビットセキュリティ強度で既に暗号化されたデータを 2061 年以降も利用する場合も同様に 2060 年までに対応する必要がある。

② ブロック暗号を利用する際は、アルゴリズム及び鍵長の選択と合わせ、CRYPTREC 暗号リストに記載の暗号利用モードを**使用しなければならない**。

3.6 署名及びメッセージ認証におけるセキュリティ強度要件

署名では、署名検証用の公開鍵証明書の有効期間（*NotBefore* から *NotAfter* の期間）中は生成された署名の検証が常に行われる可能性がある。そのため、署名検証用の公開鍵証明書の有効期間内では署名の正当性が確保され続けることが望まれる。

また、メッセージ認証は、保管時のデータの完全性を確認するために用いられることもあることから、保管時におけるデータに要求されるセキュリティ強度と同等の強度が求められる。

そこで、署名及びメッセージ認証におけるセキュリティ強度要件を、3.2 節、3.3 節及び 3.5 節を踏まえ、以下の通りとする。システムの調達や開発にあたっては、それらの**要件を全て満たすようにしなければならない**。

① 署名及びメッセージ認証におけるセキュリティ強度要件は表 8 に**従わなくてはならない**。

表 8 署名及びメッセージ認証におけるセキュリティ強度要件

<table>
<tr><th colspan="2">想定運用終了・廃棄年／
利用期間</th><th>2022～2030</th><th>2031～2040</th><th>2041～2050</th><th>2051～2060</th><th>2061～2070</th></tr>
<tr><td rowspan="2">112 ビット
セキュリティ</td><td>新規生成
(生成)</td><td rowspan="2">移行完遂
期間</td><td>利用不可</td><td rowspan="2">利用不可</td><td rowspan="2">利用不可</td><td rowspan="2">利用不可</td></tr>
<tr><td>処理
(検証)</td><td>検証許容</td></tr>
<tr><td rowspan="2">128 ビット
セキュリティ</td><td>新規生成
(生成)</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">移行完遂
期間</td><td>利用不可</td><td rowspan="2">利用不可</td></tr>
<tr><td>処理
(検証)</td><td>検証許容</td></tr>
<tr><td rowspan="2">192 ビット
セキュリティ</td><td>新規生成
(生成)</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td></tr>
<tr><td>処理
(検証)</td></tr>
<tr><td rowspan="2">256 ビット
セキュリティ</td><td>新規生成
(生成)</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td></tr>
<tr><td>処理
(検証)</td></tr>
</table>

【サポート（実装）要件】

- 最終的には、想定運用終了・廃棄年が 2040 年までならば 128 ビット以上のセキュリティ強度の、2041 年以降なら 192 ビット以上のセキュリティ強度のアルゴリズム及び鍵長を**サポート（実装）しなければならない**。
- 対象となる電子政府システムの調達や開発における何らかの制約により、運用寿命全体を通じた必要なセキュリティ強度要件を設定することが困難である場合には、セキ

ュリティ強度を切り替える移行時期を明確化したスケジュールを立案したうえで、その移行時期終了まで安全に運用するために必要なセキュリティ強度要件を満たすアルゴリズム及び鍵長を**サポート（実装）しなければならない**。例えば、移行時期を 2041～2045 年とする場合、当初は 128 ビット以上のセキュリティ強度のものを**サポート（実装）しなければならない**。

- 運用寿命が定まっていない場合には、システム更新期を明確化したスケジュールを立案することを条件としたうえで、その更新期まで安全に運用するために必要なセキュリティ強度要件を満たすアルゴリズム及び鍵長を**サポート（実装）しなければならない**。例えば、新システムの稼働開始予定時期が 2043 年である場合、新旧システムの併用運用想定期間が 5 年間であれば 128 ビット以上のセキュリティ強度のものを、10 年間であれば 192 ビット以上のセキュリティ強度のものを**サポート（実装）しなければならない**。

【署名における利用要件】

- 署名において実際に利用できるセキュリティ強度は、署名生成の日付と署名検証用の公開鍵証明書の有効期限（*NotAfter* の日付）に依存することに留意する。つまり、原則として、新規のデータに対して署名する時点（「新規生成」）で「利用可」の期間内であり、且つ有効期限での「処理」が「利用可」又は「移行完遂期間」となっているセキュリティ強度のものを**利用すべきである**。例えば、2040 年までに署名生成する場合、有効期限が 2045 年であれば 128 ビット以上のセキュリティ強度があればいいが、有効期限が 2055 年であれば 192 ビット以上のセキュリティ強度で署名生成することが求められる。
- 署名検証用の公開鍵証明書の有効期限（*NotAfter* の日付）での「処理」が「検証許容」となっているセキュリティ強度のものは、署名の正当性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合に、「新規生成」が「利用可」の期間内で新規のデータに対する署名生成が許容される。例えば、有効期限が 2055 年である場合に、2040 年までに 128 ビットセキュリティ強度で署名生成することがそれに該当する。
- 署名検証用の公開鍵証明書の有効期限（*NotAfter* の日付）での「処理」が「利用不可」にかかるような公開鍵証明書を**発行してはならない**。また、署名検証用の公開鍵証明書の有効期限（*NotAfter* の日付）での「処理」が「利用不可」にかかるセキュリティ強度のものは、新規のデータに対する署名生成に**利用してはならない**。
- 署名検証を行ってよいのは署名検証用の公開鍵証明書の有効期限（*NotAfter* の日付）までである。署名検証用の公開鍵証明書の有効期限（*NotAfter* の日付）を超えて署名検証する必要性が出てきた場合には、別の安全な保護手段により**保護し直さなければならない**。
- 「移行完遂期間」については、その期間中に移行スケジュールを完遂することを条件に、既存の電子政府システムの継続利用やそれらとの互換性・相互接続性維持のための利用に限定して、署名検証用の公開鍵証明書の有効期限（*NotAfter* の日付）が 2030 年以内である場合は 112 ビットセキュリティ強度での署名生成･検証を行ってもよい。

また、有効期限が 2040 年以内であり、且つ署名の正当性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合には、2030 年までは 112 ビットセキュリティ強度での署名生成と検証の両方を、2031 年以降は有効期限満了まで継続利用（検証のみ）を許容する。
同様に、有効期限が 2050 年以内である場合は 128 ビットセキュリティ強度での署名生成・検証を行ってもよい。また、有効期限が 2060 年以内である場合には、2050 年までは 128 ビットセキュリティ強度での署名生成と検証の両方を、2051 年以降は有効期限満了まで継続利用（検証のみ）を許容する。

【メッセージ認証における利用要件】

- 原則として、2040 年までは 128 ビット以上のセキュリティ強度で、2041 年以降は 192 ビット以上のセキュリティ強度でメッセージ認証コードを**生成・検証しなければならない**。
  ただし、移行完遂期間中に移行スケジュールを完遂することを条件に、既存の電子政府システムの継続利用やそれらとの互換性・相互接続性維持のための利用に限定して、2030 年までは 112 ビットセキュリティ強度で、2050 年までは 128 ビットセキュリティ強度でメッセージ認証コードの生成・検証を行ってもよい。
- 112 ビットセキュリティ強度で既に生成されたメッセージ認証コードに対して、対応するデータの完全性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合に、2040 年までメッセージ認証の継続利用（検証）を行うことを許容する。同様に、128 ビットセキュリティ強度でのメッセージ認証コードに対して、2051 年以降も 2060 年までメッセージ認証の継続利用（検証）を行うことを許容する。
- 112 ビットセキュリティ強度で既に生成されたメッセージ認証コードによるメッセージ認証を 2041 年以降も利用する場合には、2040 年までによりセキュリティ強度の高いアルゴリズム及び鍵長によってメッセージ認証コードを**再生成しなければならない**。128 ビットセキュリティ強度で既に生成されたメッセージ認証コードを 2061 年以降に利用する場合も同様に 2060 年までに対応する必要がある。

② 署名の利用にあたっては、以下の点にも**留意しなければならない**。

- 署名で利用するハッシュ関数は、その署名のセキュリティ強度と同等以上の衝突困難性に対するセキュリティ強度を有するものから**選択しなければならない**（2.2.3 節表 4 の 2 列目参照）。
- 署名の検証期間が 5 年を超えるような電子政府システムであれば、タイムスタンプサービスや長期署名システムなど、別の保護手段の利用も**検討すべきである**。

③ メッセージ認証の利用にあたっては、以下の点にも**留意しなければならない**。

- ブロック暗号を用いてメッセージ認証を行う場合（つまり、CMAC や CBC-MAC など）又は認証暗号を用いる場合には、表 8 で必要とされるセキュリティ強度と同等以上のセキュリティ強度を有する共通鍵暗号から**選択しなければならない（2.2.2 節表 3 参**

照）。さらに、ブロック暗号を利用する場合は、アルゴリズム及び鍵長の選択と合わせ、CRYPTREC 暗号リストに記載された認証付き秘匿モード又はメッセージ認証コードを**使用しなければならない**。

- ハッシュ関数を用いてメッセージ認証を行う場合（つまり、HMAC）には、表 8 で必要とされるセキュリティ強度と同等以上の原像困難性に対するセキュリティ強度を有するものから**選択しなければならない（2.2.3 節表 4 の 3 列目参照）**。

3.7 エンティティ認証におけるセキュリティ強度要件

エンティティ認証は、送受信が行われるその場で処理が完了することから、エンティティ認証におけるセキュリティ強度要件を、3.2 節及び 3.3 節を踏まえ、以下の通りとする。システムの調達や開発にあたっては、それらの**要件を全て満たすようにしなければならない**。

① エンティティ認証におけるセキュリティ強度要件は表 9 に**従わなくてはならない**。

表 9 エンティティ認証におけるセキュリティ強度要件

想定運用終了・廃棄年／利用期間		2022～2030	2031～2040	2041～2050	2051～2060	2061～2070
112 ビットセキュリティ	新規生成（被検証）	移行完遂期間	利用不可	利用不可	利用不可	利用不可
	処理（検証）					
128 ビットセキュリティ	新規生成（被検証）	利用可	利用可	移行完遂期間	利用不可	利用不可
	処理（検証）					
192 ビットセキュリティ	新規生成（被検証）	利用可	利用可	利用可	利用可	利用可
	処理（検証）					
256 ビットセキュリティ	新規生成（被検証）	利用可	利用可	利用可	利用可	利用可
	処理（検証）					

【サポート（実装）要件】

- 最終的には、想定運用終了・廃棄年が 2040 年までならば 128 ビット以上のセキュリティ強度の、2041 年以降なら 192 ビット以上のセキュリティ強度のアルゴリズム及び鍵長を**サポート（実装）しなければならない**。
- 対象となる電子政府システムの調達や開発における何らかの制約により、運用寿命全体を通じた必要なセキュリティ強度要件を設定することが困難である場合には、セキュリティ強度を切り替える移行時期を明確化したスケジュールを立案したうえで、その移行時期終了まで安全に運用するために必要なセキュリティ強度要件を満たすアルゴリズム及び鍵長を**サポート（実装）しなければならない。**例えば、移行時期を 2041～2045 年とする場合、当初は 128 ビット以上のセキュリティ強度のものを**サポート（実装）しなければならない**。
- 運用寿命が定まっていない場合には、システム更新期を明確化したスケジュールを立案することを条件としたうえで、その更新期まで安全に運用するために必要なセキュリティ強度要件を満たすアルゴリズム及び鍵長を**サポート（実装）しなければならない**。例えば、新システムの稼働開始予定時期が 2043 年である場合、新旧システムの併用運用想定期間が 5 年間であれば 128 ビット以上のセキュリティ強度のものを、10 年間であれば 192 ビット以上のセキュリティ強度のものを**サポート（実装）しなければならない**。

【利用要件】

- 原則として、2040 年までは 128 ビット以上のセキュリティ強度で、2041 年以降は 192 ビット以上のセキュリティ強度でエンティティ認証を**行わなければならない**。
  ただし、移行完遂期間中に移行スケジュールを完遂することを条件に、既存の電子政府システムの継続利用やそれらとの互換性・相互接続性維持のための利用に限定して、2030 年までは 112 ビットセキュリティ強度で、2050 年までは 128 ビットセキュリティ強度でエンティティ認証を行ってもよい。
- 認証用データの生成と当該認証用データの検証は極めて短い時間差で行われるので、「新規生成」において「利用不可」の期間では「処理」においても「利用不可」とする。
- 署名によるエンティティ認証の場合、検証用の公開鍵証明書の有効期限（*NotAfter* の日付）が「処理」において「利用不可」にかかるような公開鍵証明書を**発行してはならない**。また、検証用の公開鍵証明書の有効期限（*NotAfter* の日付）が「処理」において「利用不可」にかかるセキュリティ強度のものを**利用してはならない**。

② エンティティ認証を行った際のデータは、必要がなくなったら速やかに**破棄しなければならない**。

③ ブロック暗号を利用する際は、アルゴリズム及び鍵長の選択と合わせ、CRYPTREC 暗号リストに記載の暗号利用モードを**使用しなければならない**。

4. 運用中における暗号技術及び鍵長移行に関する検討の必要性

電子政府システムに必要な暗号処理ごとに、システムの想定運用終了・廃棄年、アルゴリズムのセキュリティ寿命、及び保護すべき対象データのセキュリティ寿命を考慮し、2.2 節表 2～表 4 及び 3.2 節表 5～3.7 節表 9 を使用して、セキュリティ強度要件を満たすアルゴリズム及び鍵長を選択して**利用すべきである**。

ただ、電子政府システムの運用開始時点での利用環境等によっては、将来的に必要となる高いセキュリティ強度のアルゴリズムや鍵長を当初から選択すると、対応製品がない、導入コストが許容できないほど高くなる、処理が許容できないほど遅くなるなど、パフォーマンスや導入スケジュール等に悪影響を及ぼす可能性がある。このような場合、セキュリティ強度を切り替える移行時期を明確化したスケジュールを立案したうえで、電子政府システムの運用寿命の前半に対して適切なセキュリティ強度を有するアルゴリズム及び鍵長を選択して利用するといったことが考えられる。

また、電子政府システムの運用開始時点は想定できなかった（もしくはあえて考慮対象から外した）暗号解読の向上や大規模な量子コンピュータの実現などが現実化し、想定していたよりも早期に使用しているアルゴリズムや鍵長が適切なセキュリティ（暗号学的安全性）を提供できなくなることも起こり得る。

これらのケースでは、電子政府システムの運用寿命の途中で、利用しているアルゴリズムのセキュリティ寿命が尽きつつあることを意味するため、そのセキュリティ寿命が尽きる前に、その後に必要となるセキュリティ強度を有する新しいアルゴリズム及び鍵長へ**移行しなければならない**。もし、アルゴリズムのセキュリティ寿命が尽き、もはや情報に対して望ましい保護を提供しないと判断された（例えば、“解読された”可能性がある）場合、そのアルゴリズム及び鍵長によって保護されている情報は疑わしいと見なされることになる（例えば、当該データの機密性が損なわれていたり、完全性が保証できなくなったりする）。

なお、移行にあたっては、移行先となるアルゴリズム及び鍵の取扱いだけでなく、使用中のアルゴリズム及び鍵の取扱いにも**注意を払わなければならない**。その際、重要なのは、利用している様々な鍵に対するライフサイクルを正しく運用管理することである。鍵のライフサイクルについては、暗号鍵設定ガイダンス（一般用）[14]の 4 節を参照されたい。

4.1 移行計画策定における論点

新しいアルゴリズム及び鍵長へ移行するのは、電子政府システムの規模や移行対象のアルゴリズムや鍵長の種類、代替するアルゴリズムや鍵長の実装状況、データフォーマットやプログラムインタフェースの差異による移行容易性の違いなどにもよるが、多くの場合、非常に時間とコストがかかる作業であることを念頭に置いておく必要がある。実際、過去にあったアルゴリズムや

[14] 暗号鍵設定ガイダンス（一般用）、https://

鍵長における大規模な移行（例：DES/Triple DES から AES への移行、RSA での鍵長 1024 ビットから 2048 ビットへの移行、SHA-1 から SHA-256 への移行など）では、移行準備から移行完遂までに 5 年から 10 年単位の時間がかかっている[15]。

そのため､利用しているアルゴリズムのセキュリティ寿命を迎える少なくとも 5 年前までには、より安全なアルゴリズム及び鍵長への移行計画を**策定すべきである**。その移行計画を立てる際には、いつからどのくらいの期間をかけてどのアルゴリズム及び鍵長に移行するのかを**明確にすべきである**。

以下では、移行のための論点のいくつかを述べる。

4.1.1 通信時及び鍵共有の暗号化における論点

送信側と受信側の両方でより安全な新しいアルゴリズム及び鍵長が実装され利用可能になった時点以降であれば、新しいアルゴリズム及び鍵長だけを使うように切り替えることで移行対策は実現可能である。

なお、移行前に行われた通信や鍵共有について、攻撃者が通信中の暗号化された情報や鍵[16]を収集・保存している可能性を強く想定する必要がある場合、それらの通信内容が解読され、当該情報の機密性が危殆化する可能性がある[17]と考えるべきであることに留意されたい。この場合、別の鍵やアルゴリズムを用いて再暗号化したとしてもセキュリティ上の必要な効果が得られるかどうかは不明である。

このような攻撃に対しては後から防ぐことができないため、こういった攻撃に対する対策が必要であるかどうかについても、移行計画を立てる際に十分に**検討すべきである**。

4.1.2 保管時の暗号化における論点

保管するデータに対して期待されるセキュリティ寿命（当該データの機密性を保持する期間）を考慮に入れることが非常に重要である。

新規のデータのセキュリティ寿命がアルゴリズムのセキュリティ寿命を超えている(すなわち、当該アルゴリズムや鍵長のセキュリティ強度が 3.5 節表 7 の「新規生成」において「利用不可」となる時間枠内に入っている）ならば、そのアルゴリズム及び鍵長を当該データの暗号保護に**適用してはならない**。つまり、データのセキュリティ寿命全体をカバーするより安全なアルゴリズム及び鍵長を使って**暗号化を行わなければならない**。もしそのようなアルゴリズム及び鍵長がサ

---

15 政府機関の情報システムで使用されていた SHA-1 及び RSA-1024 を SHA-2 及び RSA-2048 に移行する際には、2008 年 4 月情報セキュリティ政策会議決定を皮切りに、各府省庁に対して 2008 年度中の移行計画の立案を要請、2009 年度に検証システム構築、2010 年度から 2013 年度までのシステム移行期間が設けられた。また、米国では DES の米国政府標準暗号からの削除方針を 1993 年に NIST が表明した後、実際に削除されたのは 2005 年であった。SHA-1 及び RSA-1024 を SHA-256 及び RSA-2048 へ 2010 年までに移行する方針を表明したのも 2005 年である。

16 鍵共有が行われた際のセッション鍵が危殆化した場合、当該セッション鍵を利用した暗号通信も同時に危殆化したものと判断すべきである。

17 Store (Harvest)-then-decrypt、Store now & decrypt later、Retrospective Decryption ともいう。

ポート（実装）されていないのであれば、より安全なアルゴリズム及び鍵長が実装され利用可能になった後に再暗号化を行うことができるようになるまでは、復号に利用するアルゴリズムのセキュリティ寿命が尽きる期日と同じになるように当該データのセキュリティ寿命を短縮**しなければならない**。

保管時の暗号化における移行対策では、新しいアルゴリズム及び鍵長が実装され利用可能となった後の切り替えだけではなく、すでに暗号化された形で保管されているデータについての取扱いも検討し、必要な処置を**行わなくてはならない**。

例えば、すでに暗号化された上で保管されているデータのセキュリティ寿命を延長した場合や何らかの理由で暗号化に利用したアルゴリズムや鍵長のセキュリティ強度が低下した場合、本来必要とされるセキュリティ強度よりも低い状態で当該データが暗号化されている状態になり得る。とりわけ、そのままだと当該データの機密性が危殆化するかもしれないリスクがある期間（3.5 節表 7 の「処理」において「復号許容」又は「利用不可」となる時間枠内）にかかってしまうケースの場合が問題となる。そのような状況を避けるために、データの機密性が保たれている間に、より安全なアルゴリズム及び鍵長で当該データの再暗号化をして**保護し直さなければならない**。

なお、「復号許容」に該当する期間中であれば、すでに暗号化された形で保管されているデータに対する機密性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合には、特に移行対策を取ることなく、暗号化されたデータを継続利用（復号）することが許容される。

4.1.3 署名における論点

署名するデータに対して期待されるセキュリティ寿命（当該データの完全性及び署名者の検証が行える期間）を考慮に入れることが非常に重要である。

署名の署名検証期間全体（すなわち、署名検証用の公開鍵証明書の有効期間）がアルゴリズムのセキュリティ寿命を超えている（すなわち、当該アルゴリズムや鍵長のセキュリティ強度が 3.6 節表 8 の「処理」において「利用不可」となる時間枠内に入っている）ならば、そのアルゴリズム及び鍵長を当該データの署名生成に**適用してはならない**。つまり、データの署名検証期間全体をカバーする、より安全なアルゴリズム及び鍵長を使って署名生成を**行わなければならない**。もしそのようなアルゴリズム及び鍵長がサポート（実装）されていないのであれば、より安全なアルゴリズム及び鍵長が実装され利用可能になるまでは、署名検証に利用するアルゴリズムのセキュリティ寿命が尽きる期日と同じになるように署名検証期間を**短縮しなければならない**。

署名における移行対策では、新しいアルゴリズム及び鍵長が実装され利用可能となった後の切り替えだけではなく、有効期間が残っている公開鍵証明書の取扱い、及びすでに署名された形で保管されているデータについての取扱いも検討し、必要な処置を**行わなくてはならない**。

例えば、すでに署名された形で保管されているデータのセキュリティ寿命を延長した場合や何らかの理由で署名生成に利用したアルゴリズムや鍵長のセキュリティ強度が低下した場合、本来必要とされるセキュリティ強度よりも低い状態で当該データの署名が生成されている状態になり得る。とりわけ、そのままだと当該データの完全性が危殆化したり、否認防止の確認ができなく

なったりするかもしれないリスクがある期間（3.6 節表 8 の「処理」において「検証許容」又は「利用不可」となる時間枠内）にかかってしまうケースが問題となる。そのような状況を避けるために、署名の検証が正しく行えている間に、より安全なアルゴリズム及び鍵長を使用した署名を再適用する方法のほか、暗号学的タイムスタンプを採用した保存機能や長期署名システムなどを利用するなどの方法により、署名を**保護し直さなければならない**。また、関連する公開鍵証明書について、有効期間が残っている場合には、失効処理などの**対応が必要となる**。

なお、「検証許容」に該当する期間中であれば、すでに署名された形で保管されているデータに対する正当性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合には、特に移行対策を取ることなく、当該データの署名検証を継続することが許容される。

4.1.4 メッセージ認証における論点

署名の場合と同様に、認証するデータに対して期待されるセキュリティ寿命（当該データの完全性検証が行える期間）を考慮に入れることが非常に重要である。

データの検証期間（すなわち、データの完全性を保護する必要がある期間）がアルゴリズムのセキュリティ寿命を超えている（すなわち、当該アルゴリズムや鍵長のセキュリティ強度が 3.6 節表 8 の「処理」において「利用不可」となる時間枠内に入っている）ならば、そのアルゴリズム及び鍵長を当該データのメッセージ認証コードの生成に**適用してはならない**。つまり、データの検証期間をカバーする、より安全なアルゴリズム及び鍵長を使ってメッセージ認証コードの生成を**行わなければならない**。もしそのようなアルゴリズム及び鍵長がサポート（実装）されていないのであれば、より安全なアルゴリズム及び鍵長が実装され利用可能になるまでは、メッセージ認証コードの検証に利用するアルゴリズムのセキュリティ寿命が尽きる期日と同じになるように検証期間を**短縮しなければならない**。

メッセージ認証における移行対策では、新しいアルゴリズム及び鍵長が実装され利用可能となった後の切り替えだけではなく、すでにメッセージ認証コードとともに保管されているデータについての取扱いも検討し、必要な処置を**行わなくてはならない**。

例えば、すでにメッセージ認証コードとともに保管されているデータのセキュリティ寿命を延長した場合や何らかの理由でメッセージ認証コードの生成に利用したアルゴリズムや鍵長のセキュリティ強度が低下した場合、本来必要とされるセキュリティ強度よりも低い状態で当該データのメッセージ認証コードが生成されている状態になり得る。とりわけ、そのままだと当該データの完全性が危殆化するかもしれないリスクがある期間（3.6 節表 8 の「処理」において「検証許容」又は「利用不可」となる時間枠内）にかかってしまうケースが問題となる。そのような状況を避けるために、データの完全性検証が正しく行えている間に、より安全なアルゴリズム及び鍵長を使用して当該データのメッセージ認証コードを再生成して**保護し直さなければならない**。

なお、「検証許容」に該当する期間中であれば、すでに生成されたメッセージ認証コードとともに保管されているデータに対する完全性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合には、特に移行対策を取ることなく、当該データの完全性検証を継続することが許容される。

4.1.5　エンティティ認証における論点

送信側と受信側の両方でより安全な新しいアルゴリズム及び鍵長が実装され利用可能になった時点以降であれば、新しいアルゴリズム及び鍵長だけを使うように切り替えることで移行対策は実現可能である。

なお、署名によるエンティティ認証の場合で、移行前の公開鍵証明書の有効期間が残っている場合には、失効処理などの**対応が必要となる**。

4.2 電子政府システムの運用寿命の延長に伴う移行にあたっての対応

電子政府システムの運用中の状況の変化により、当該システムの調達又は開発段階で当初想定した運用寿命どおりには運用を終了せず、延長して運用を継続する必要性が生じる場合があり得る。

このような場合、延長の必要性が判明した時点で、直ちに、新たに設定される運用寿命をもとに、3.2 節表 5～3.7 節表 9 から必要なセキュリティ強度要件を**再評価しなければならない**。再評価の結果、

- 求められるセキュリティ強度要件に変化がなく、現在利用中のアルゴリズム及び鍵長でも同じように必要なセキュリティ強度を維持できる場合は、そのまま継続して利用してよい。
- より強力なセキュリティ強度が求められ、現在利用中のアルゴリズムや鍵長では必要なセキュリティ強度要件を満たすことができない場合には、4.1 節の論点を踏まえ、速やかにより安全なアルゴリズム及び鍵長への移行計画を**策定し**、その計画に則って新しいアルゴリズム及び鍵長への移行を**完了しなければならない。**その際、現在利用中のアルゴリズム及び鍵長での新規のデータに対する暗号保護（つまり、「新規生成」）において「利用不可」の期間に移行完遂時期が**入らないようにしなければならない**。

4.3 セキュリティ強度要件の設定変更に伴う移行にあたっての対応

3 節に記載された必要なセキュリティ強度要件の予測の妥当性を確認する観点から、5 年ごとに 3.2 節表 5～3.7 節表 9 のセキュリティ強度要件のレビューを実施し、必要に応じて適切な修正を加えることとしている。例えば、画期的な暗号解読手法の発明や大規模な量子コンピュータの実現予測時期の精緻化などに伴い、必要なセキュリティ強度要件の設定が変更になる可能性がある。

電子政府システムの運用者は、本書が改訂されるタイミングで変更内容を確認し、セキュリティ強度要件の変更有無及びその影響を**確認しなければならない**。

セキュリティ強度要件の変更により、より強力なセキュリティ強度が求められ、現在利用中のアルゴリズムや鍵長では必要なセキュリティ強度要件を満たすことができないことが判明した時

は、4.1 節の論点を踏まえ、速やかにより安全なアルゴリズム及び鍵長への移行計画を**策定し**、その計画に則って新しいアルゴリズム及び鍵長への移行を**完了しなければならない**。その際、現在利用中のアルゴリズム及び鍵長での新規のデータに対する暗号保護（つまり、「新規生成」）において「利用不可」の期間に移行完遂時期が**入らないようにしなければならない**。

4.4 暗号技術の推定セキュリティ強度の変更に伴う移行にあたっての対応

2.2 節に記載された暗号技術の推定セキュリティ強度の予測の妥当性を確認する観点から、5 年ごと又は必要に応じて、2.2 節表 2～表 4 の暗号技術の推定セキュリティ強度のレビューを実施し、適宜適切な修正を加えることを計画している。例えば、画期的な暗号解読手法の発明や大規模な量子コンピュータの実現予測時期の精緻化などに伴い、アルゴリズムや鍵長によってはその推定セキュリティ強度の結果が変更になる可能性がある。

電子政府システムの運用者は、本書が改訂されるタイミングで変更内容を確認し、利用しているアルゴリズムや鍵長についての推定セキュリティ強度が変更されていないかどうかを**確認しなければならない**。

利用しているアルゴリズムや鍵長についての推定セキュリティ強度が変更され、当該アルゴリズムや鍵長では必要なセキュリティ強度要件を満たすことができないことが判明した時は、4.1 節の論点を踏まえ、より安全なアルゴリズム及び鍵長への移行計画を速やかに**策定し**、その計画に則って新しいアルゴリズム及び鍵長への移行を**完了しなければならない**。その際、変更後の推定セキュリティ強度を基準として、3.2 節表 5～3.7 節表 9 での新規のデータに対する暗号保護（つまり、「新規生成」）において「利用不可」の期間に移行完遂時期が**入らないようにすべきである**。例えば、ある鍵長の推定セキュリティ強度が 192 ビットセキュリティから 112 ビットセキュリティに低下した場合、2030 年までに移行完遂する計画を**策定し、実行すべきである**。

もし推定セキュリティ強度の低下が著しく、すでに「利用不可」の期間に入ってしまっている場合には、可能な限り早期に移行を完了させる計画を速やかに**策定し、**その計画に則って新しいアルゴリズム及び鍵長への移行を**完了すべきである**。

なお、移行に向けた対処方針が別途提示されたアルゴリズムや鍵長を利用している場合には、その対処方針に従って移行計画を**策定しなければならない**。

4.5 運用監視暗号リストに掲載されたアルゴリズムの継続利用にあたっての対応

電子政府推奨暗号リストに掲載されているアルゴリズムに対する画期的な暗号解読手法が発明された結果、アルゴリズムとしてのセキュリティ（暗号学的安全性）が低下し、互換性維持以外の目的での利用は推奨しないと CRYPTREC にて判断された場合、当該アルゴリズムは運用監視

暗号リストに適宜移行する。

電子政府システムの運用者は、適宜 CRYPTREC 暗号リストが変更されていないかどうかを確認し、変更があった場合には利用しているアルゴリズムが運用監視暗号リストに移行していないかどうかを**確認しなければならない**。

利用しているアルゴリズムが運用監視暗号リストに移行した場合でも継続して利用する場合には、以下の対応を**行うべきである**。

- 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ていて、必要なセキュリティ強度要件を満たす代替可能な別のアルゴリズム（代替アルゴリズム）がサポート（実装）されていなければ、できる限り速やかにサポートする。
- 代替アルゴリズムがサポート（実装）されたら、新たなデータに対する暗号保護にあたって、互換性維持が必要ないデータから順次代替アルゴリズムを利用する。
- 新たなデータに対する暗号保護であっても、互換性維持が必要なものは（当面）今まで利用していたアルゴリズムを継続して利用してもよい。ただし、互換性維持が必要な場合であっても、代替アルゴリズムで対応可能な場合には代替アルゴリズムを利用する。
- 運用監視暗号リストに掲載されたアルゴリズムを継続利用している最中に、当該アルゴリズムの代替アルゴリズムへの移行に向けた対処方針が別途提示された場合、運用監視暗号リストに記載されている当該アルゴリズムに付記された注釈を満たさなくなった場合、又は運用監視暗号リストからの削除が示唆された場合には、4.1 節の論点を踏まえ、代替アルゴリズムへの移行計画を速やかに**策定し、実行すべきである**。なお、移行に向けた対処方針が提示されている場合には、その対処方針に従って、移行計画を**策定しなければならない**。

4.6 突発的な理由に伴う緊急移行にあたっての対応

可能性は低いものの、あるアルゴリズムに対する極めて画期的な暗号解読手法が発明され、当該アルゴリズムや鍵長の推定セキュリティ強度の急速な低下を引き起こす可能性はゼロではない。そのため、CRYPTREC では、CRYPTREC 暗号リスト掲載のアルゴリズム及び鍵長に対するセキュリティ（暗号学的安全性）を常時監視しており、セキュリティ（暗号学的安全性）が大きく懸念されるような学会発表やニュース報道などに対して、必要に応じて注意喚起情報を発表している。

注意喚起一覧：https://www.cryptrec.go.jp/er.html

利用しているアルゴリズムや鍵長についての注意喚起情報が発表されたとしても、緊急対応を求める旨の記述がなければ、直ちに何らかの対処を求めるというものではない。ただし、内容によっては、その後、CRYPTREC 暗号リスト又は本書での推定セキュリティ強度やセキュリティ強度要件などの見直しに反映されることがあるので、それらが改訂された際には 4.3 節、4.4 節

及び 4.5 節に従って対処するのが原則である。

なお、可能性は極めて低いものの、全く想定できなかった推定セキュリティ強度の著しい低下により大きな被害の発生が懸念される場合[18]には、緊急対応を求める旨の発表がなされる可能性がある。その際の対処方針によっては、移行対象となったアルゴリズムや鍵長を利用している場合、移行を極めて短期間で終えるための緊急移行計画を**速やかに策定し、実行しなければならない**場合もあることに留意されたい。

4.7 量子コンピュータの実現リスクへの対応

現在、大規模な量子コンピュータが実現しても安全な耐量子計算機暗号（PQC: Post-Quantum Cryptography）の標準化選定プロセス[19]を NIST が進めている。また、CRYPTREC 暗号技術評価委員会でもその傘下に暗号技術調査 WG（耐量子計算機暗号）を設置し、PQC の研究動向調査をもとに主要な PQC についてのガイドライン策定を進めている。

今後、これらの活動の進捗状況及び量子コンピュータの進展状況によっては、本書にその成果が取り込まれ、内容が大きく更新される可能性があることに留意されたい。その場合、将来標準化される PQC も代替アルゴリズムの有力な選択肢の一つとなり得る。

その一方、現在の CRYPTREC 暗号リストに掲載されているアルゴリズムの鍵長と PQC の鍵長とでは大きくサイズが異なるため、移行にあたってアプリケーションやインタフェース、データフォーマット、プロトコルなどに大幅な変更が必要となる可能性が高い。その場合、移行のための準備や開発コスト、実際の移行に必要な期間などが従来以上に大きく膨らむ可能性があることに留意されたい。加えて、現在主流の暗号技術とは違い、PQC に特化した暗号解読手法や安全性評価の蓄積、実装脆弱性を回避するための PQC を実装する際のセキュリティ対策（例えば、サイドチャネル攻撃[20]対策）の蓄積といったものが十分に進んでいるとはいえない状況である点も考慮しておく必要がある。

したがって、PQC への移行については、ガイドライン等を参考に、移行の必要性や方法などについても予め十分に検討し、移行計画を慎重に策定したうえで**実施すべきである**。利用環境によっては、PQC への完全な移行ではなく、PQC と現在主流の暗号技術との併用を視野に入れることも考えられる。

---

18 ちなみに、2000 年の CRYPTREC 発足以来、今までにそのようなケースが発生したことは一度もない。

19 NIST Post-Quantum Cryptography Standardization, https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization

20 暗号技術が実装された暗号モジュールやプログラム、チップなどから、実際に暗号保護を行う際に漏えいする物理的情報（消費電力、処理時間、電磁波など）を測定することによって、内部の動作状況を推定し、暗号鍵などの秘密情報を入手する攻撃手法のこと。電力解析攻撃、タイミング攻撃などが有名。アルゴリズムではなく実装物への攻撃なので、アルゴリズムそのものは安全であったとしても、実装された暗号モジュールやプログラム、チップが脆弱であったために暗号解読されたというケースは多い。

Appendix　参考情報

[1] Cryptographic Mechanisms: Recommendations and Key Lengths, TR-02102-1 v2020-01, BSI, 03/2020.
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html

表 10　BSI（独）のセキュリティ強度選択基準（1.1 節、1.2 節）

2020～2022	（要件）100 ビット以上のセキュリティ強度であること （推奨）共通鍵暗号：128 ビットセキュリティ メッセージ認証コード：128 ビットセキュリティ 楕円曲線以外の公開鍵暗号（RSA, DH など）：100 ビットセキュリティ（鍵長 2000 ビット） 楕円曲線の公開鍵暗号（ECDSA など）：120 ビットセキュリティ（鍵長 250 ビット）
2023～2026	（要件）　120 ビット以上のセキュリティ強度であること （推奨）共通鍵暗号：128 ビットセキュリティ メッセージ認証コード：128 ビットセキュリティ 楕円曲線以外の公開鍵暗号（RSA, DH など）：120 ビットセキュリティ（鍵長 3000 ビット） 楕円曲線の公開鍵暗号（ECDSA など）：120 ビットセキュリティ（鍵長 250 ビット）

[2] Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 5, NIST, 05/2020.
https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

表 11　NIST（米）のセキュリティ強度選択基準（5.6.3 節）

2020～2030	（要件）新規データの保護（暗号化、署名生成など）は 112 ビット以上のセキュリティ強度であること。但し、2024 年以降は、3-key Triple DES は利用不可 保護済データの処理（復号、署名検証など）は 2-key Triple DES、1024 ビット RSA、SHA-1 相当以上のセキュリティ強度であること
2031～	（要件）新規データの保護（暗号化、署名生成など）は 128 ビット以上のセキュリティ強度であること 保護済データの処理（復号、署名検証など）は 2-key Triple DES、1024 ビット RSA、SHA-1 相当以上のセキュリティ強度であること

[3] Mécanismes cryptographiques - Règles et recommandations, Rev. 2.03, ANSSI, 02/2014
https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf

表 12　ANSSI（仏）のセキュリティ強度選択基準（2.1 節、2.2 節、2.3 節）

2014～2030	（要件）共通鍵暗号：128 ビット以上のセキュリティ強度。なお、ブロック暗号のブロック長は 128 ビット 楕円曲線以外の公開鍵暗号（RSA, DH など）：112 ビット以上のセキュリティ強度（鍵長 2048 ビット以上） 楕円曲線の公開鍵暗号（ECDSA など）：128 ビット以上のセキュリティ強度（鍵長 256 ビット以上） ハッシュ関数：128 ビット以上のセキュリティ強度（ハッシュ長 256 ビット以上） （推奨）楕円曲線以外の公開鍵暗号（RSA, DH など）：128 ビット以上のセキュリティ強度（鍵長 3072 ビット以上）
2031～	（要件）共通鍵暗号：128 ビット以上のセキュリティ強度。なお、ブロック暗号のブロック長は 128 ビット 楕円曲線以外の公開鍵暗号（RSA, DH など）：128 ビット以上のセキュリティ強度（鍵長 3072 ビット以上） 楕円曲線の公開鍵暗号（ECDSA など）：128 ビット以上のセキュリティ強度（鍵長 256 ビット以上） ハッシュ関数：128 ビット以上のセキュリティ強度（ハッシュ長 256 ビット以上）

* ビットセキュリティ自体の表示はなし。鍵長・ハッシュ長からの推定

[4] Commercial National Security Algorithm, National Security Agency (NSA), 01/2016.
https://apps.nsa.gov/iad/programs/iad-initiatives/cnsa-suite.cfm

表 13　NSA（米）のセキュリティ強度選択基準

TOP SECRET までの保護	（要件）共通鍵暗号：256 ビットセキュリティ 楕円曲線以外の公開鍵暗号（RSA, DH など）：128 ビット以上のセキュリティ強度（鍵長 3072 ビット以上） 楕円曲線の公開鍵暗号（ECDSA など）：192 ビットセキュリティ（鍵長 384 ビット） ハッシュ関数：192 ビットセキュリティ（ハッシュ長 384 ビット）

[5] Algorithms, Key Size and Protocols Report (2018), H2020-ICT-2014 – Project 645421, D5.4, ECRYPT-CSA, 02/2018.
https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf

表 14　ECRYPT（欧州）のセキュリティ強度選択基準（4.6 節）

互換性維持	
2018 ～ 2028 (near term use) 短期の利用	（要件）共通鍵暗号：128 ビットセキュリティ 楕円曲線以外の公開鍵暗号（RSA, DH など）：128 ビットセキュリティ（鍵長 3072 ビット） 楕円曲線の公開鍵暗号（ECDSA など）：128 ビットセキュリティ（鍵長 256 ビット） ハッシュ関数：128 ビットセキュリティ（ハッシュ長 256 ビット）
2018 ～ 2068 (long term use) 長期の利用	（要件）共通鍵暗号：256 ビットセキュリティ 楕円曲線以外の公開鍵暗号（RSA, DH など）：256 ビットセキュリティ（鍵長 15360 ビット） 楕円曲線の公開鍵暗号（ECDSA など）：256 ビットセキュリティ（鍵長 512 ビット） ハッシュ関数：256 ビットセキュリティ（ハッシュ長 512 ビット）

[6] Selecting Cryptographic Key Sizes, Arjen K. Lenstra and Eric R. Verheul, Journal of Cryptology, vol. 14, p. 255-293, 2001.
https://link.springer.com/content/pdf/10.1007/s00145-001-0009-4.pdf
[7] Key Lengths, Arjen K. Lenstra, The Handbook of Information Security, 06/2004.
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.694.8206

表 15　1982 年の DES と同等のセキュリティを提供すると推定される（＝その後 10～15 年程度なら完全解読が困難と期待される）ビットセキュリティ
([3] Figure 6、[6] Table 1、[7] 2 節式(2))

	1982	2030	2040	2050	2060	2070
[3] ANSSI（2014）	56	81 ～ 96	86 ～ 104	91 ～ 112	96 ～ 120	101 ～ 128
[6] Lenstra（2001）	56	93	101	109	－	－
[7] Lenstra（2004）	56	88	95	102	－	－

[8] CRYPTREC Report 2020

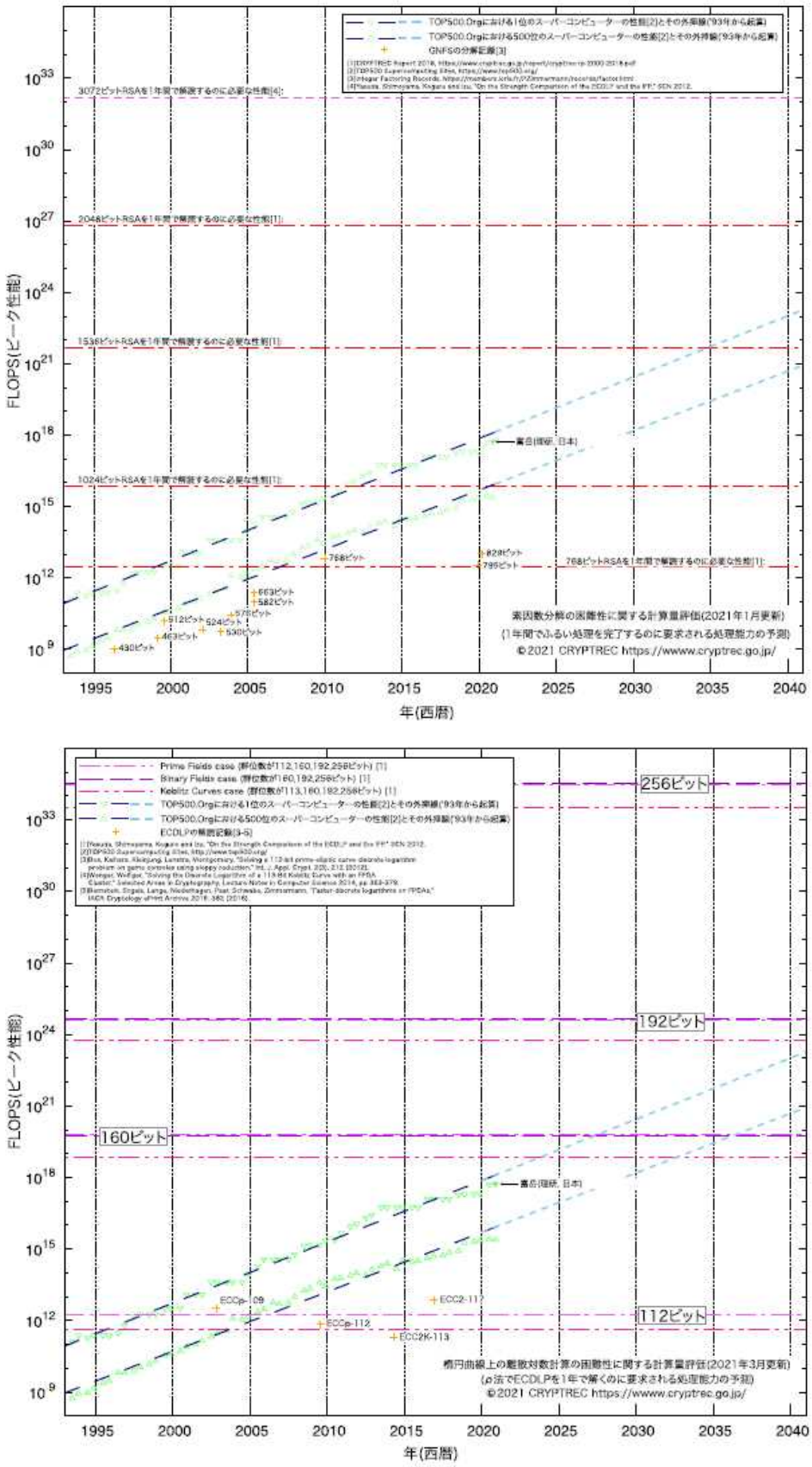


図 7　1 年で解読するのに必要な性能が達成できると見込まれる時期（図 3.1、図 3.2）

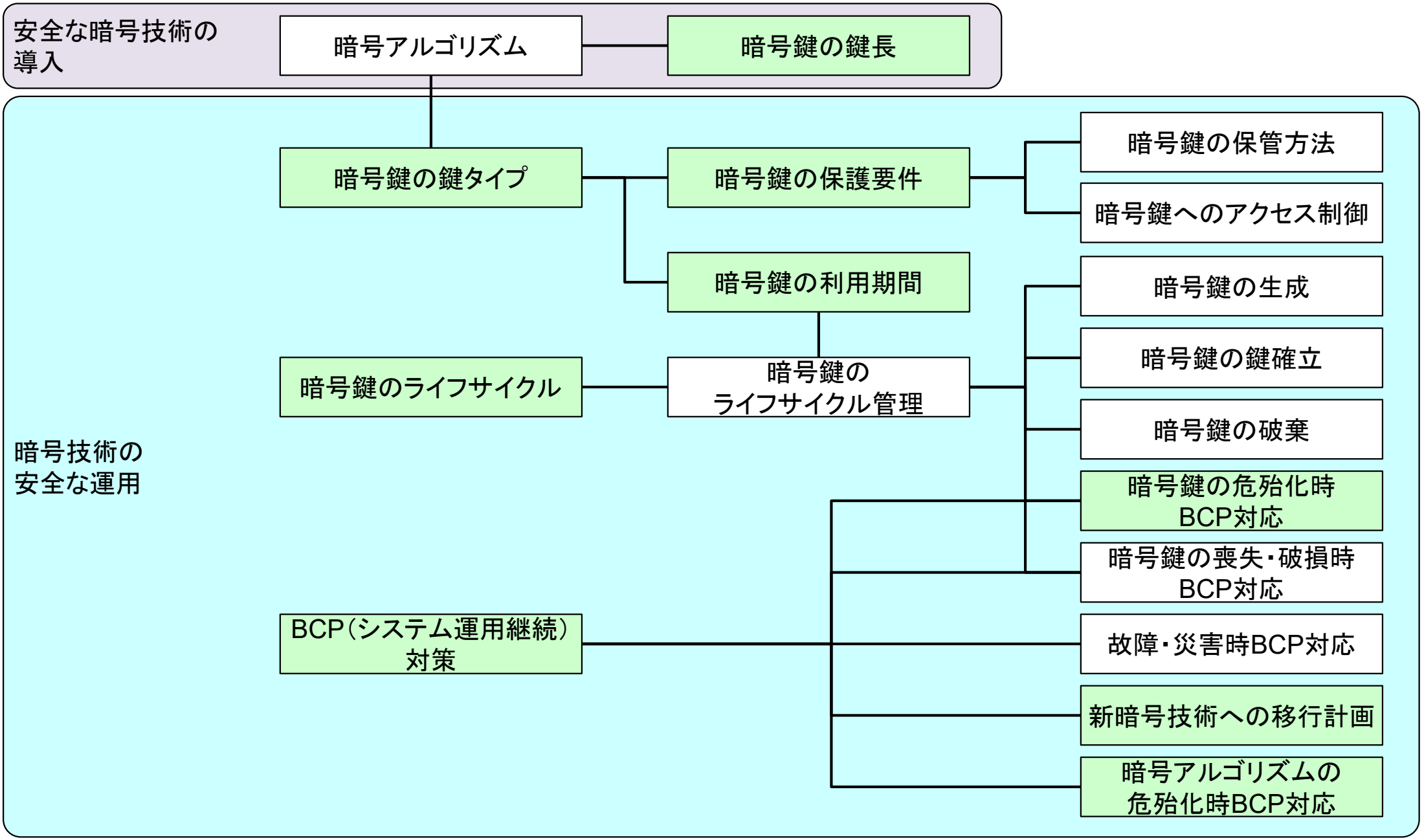
資料７－１

暗号鍵設定ガイダンス概要
（2022年3月3日版）

暗号鍵設定ガイダンスの位置づけ

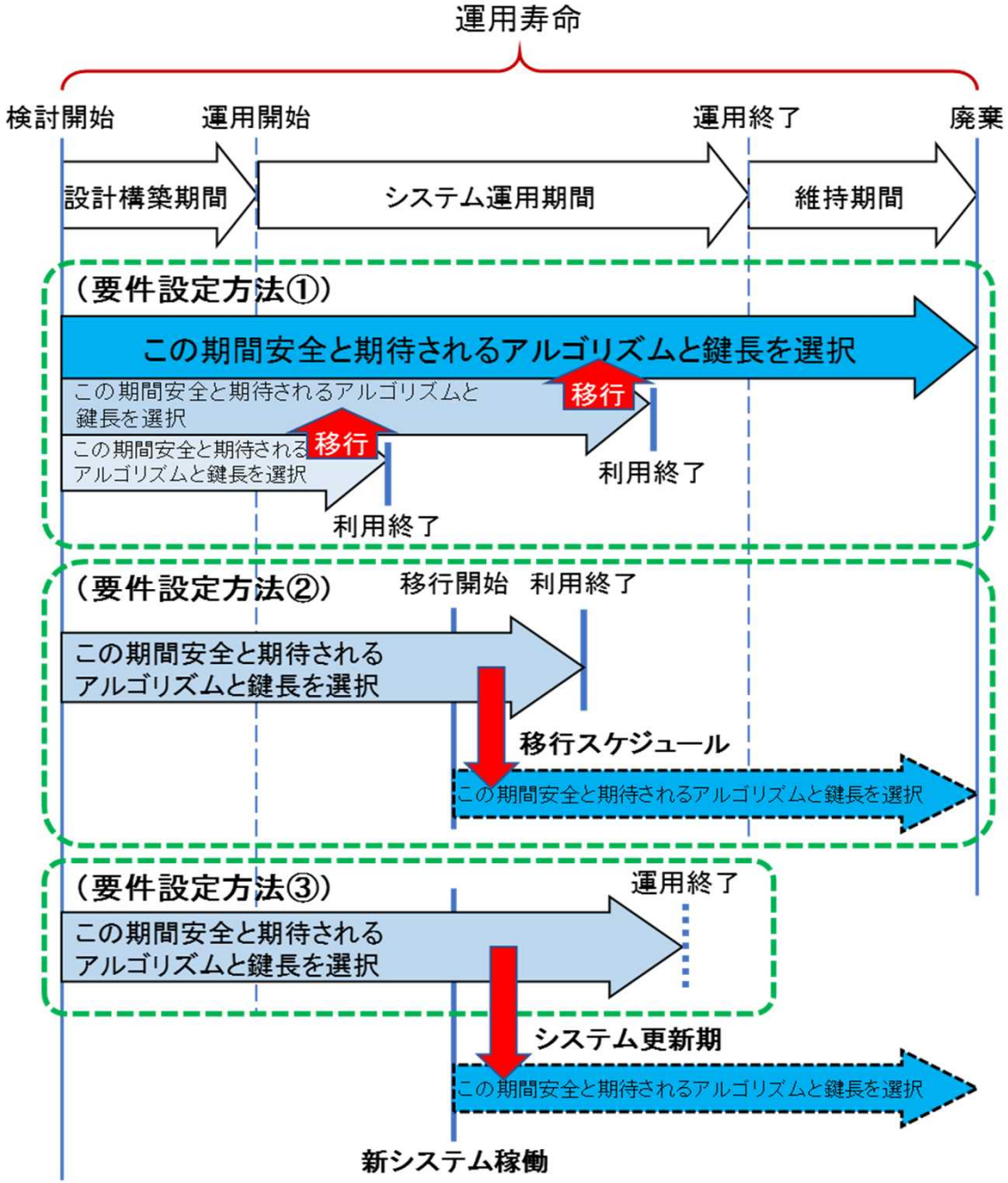
文書体系	運用ガイドラインの一つと位置付け。GLを附番
利用目的	暗号技術に用いられる暗号鍵に対して適切に鍵長を設定し、さらに適切に鍵管理を行って安全に運用していくための技術的ガイダンスを提供する
想定読者	暗号技術を組込んだシステム又はアプリケーションの設計・開発・運用・提供にあたって、安全な暗号技術の選定、及び暗号技術の安全な運用方針・対策の作成や決定などに携わる管理者、設計者、開発者など
備考	SP800-57 Part 1に記載がある「アルゴリズムや鍵長の設定以外の鍵管理に関する事項（保護手段など）」は「暗号鍵管理ガイダンス」に分ける
主な論点	● 「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」との位置づけの違いの明確化 ◆ 暗号技術を利用する際の鍵長設定の考え方を解説するもので、強制的な要求（～しなければならない／～してはならない）は原則として使わない ◆ 政府機関等のサイバーセキュリティ対策のための統一基準において適用対象となる情報システムにおいて、CRYPTREC暗号リストに記載のアルゴリズムを利用する場合には本ガイダンスの対象外 ● ビットセキュリティの基準をどこまで区切るか ● システムやアプリケーションの運用寿命とセキュリティ強度要件の関係をどのように整理するか ● 求められるセキュリティ強度要件の考え方 ● 「暗号鍵のライフサイクル」「暗号鍵の（タイプごとの）利用期間」「鍵の保護」についての記載内容 ● 移行に関する検討の必要性についての記載内容

暗号鍵設定ガイダンスの取り扱い項目



凡例：本ガイダンスで取り扱っている項目

暗号鍵のセキュリティ強度要件の考え方



システムの運用寿命と求められるセキュリティ強度

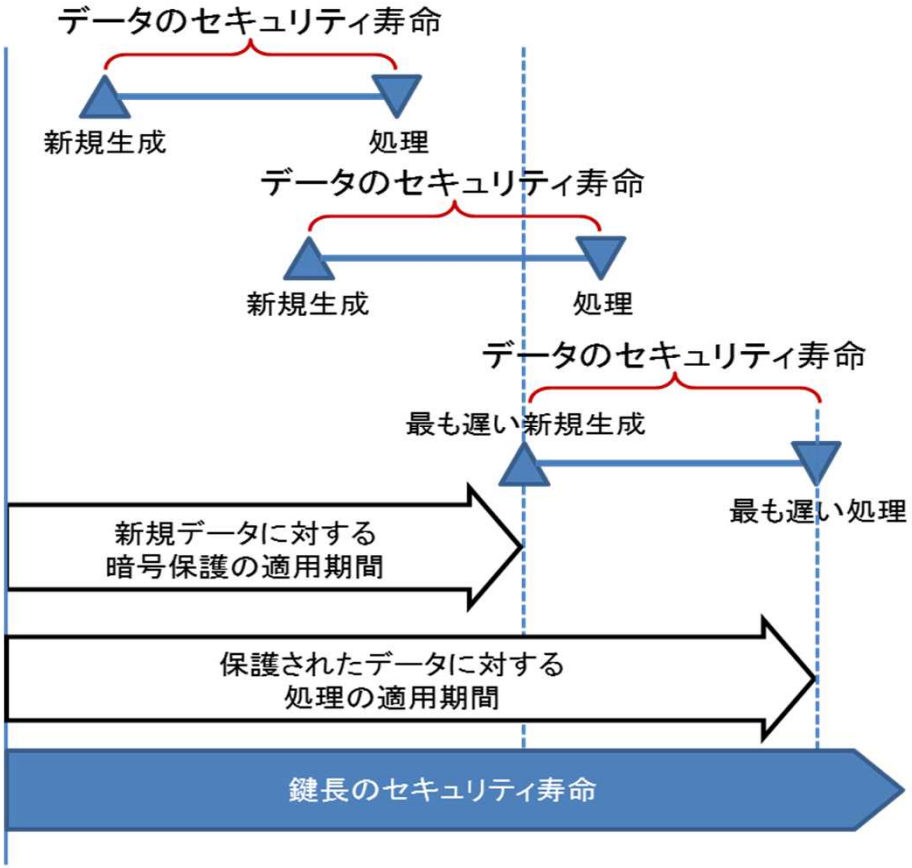
■ 下限のビットセキュリティ強度（＝その年から後10～15年程度なら安全と期待される強度）を提示

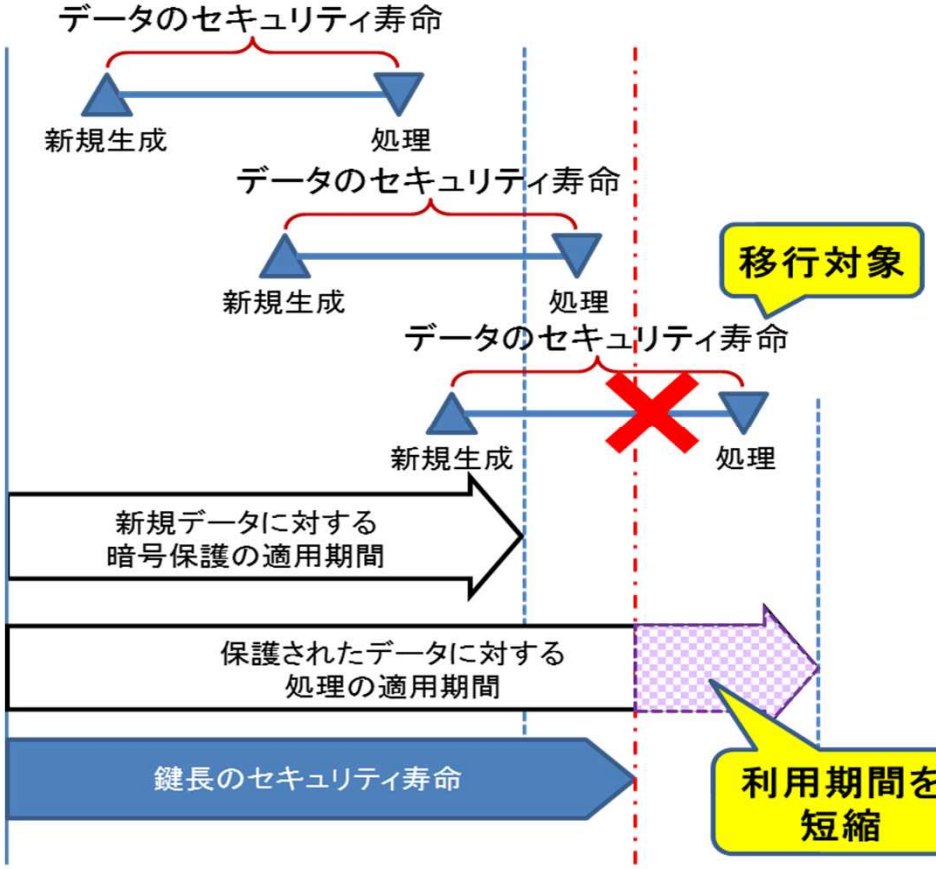
- 一定のセキュリティマージンを追加したそれ以上のセキュリティ強度で設定するようアドバイス
- Appendixに各国の推奨状況を記載

年	ANSSI (2014)	Lenstra (2001)	Lenstra (2004)
1982	56	56	56
2030	81 ～ 96	93	88
2040	86 ～ 104	101	95
2050	91 ～ 112	109	102
2060	96 ～ 120	—	—
2070	101 ～ 128	—	—

鍵長の選択及び利用期間の考え方

データのセキュリティ寿命		
暗号化	通信時	（鍵共有後から）通信が終了するまでの期間
	保管時	データが暗号化されてから、復号する必要がなくなるまでの期間
	鍵共有	鍵共有を行っている期間
署名		署名生成してから、当該署名の署名検証を行う必要がなくなるまでの期間
メッセージ認証		MACを生成してから、当該データの完全性検証を行う必要がなくなるまでの期間
エンティティ認証		エンティティ認証を行っている期間



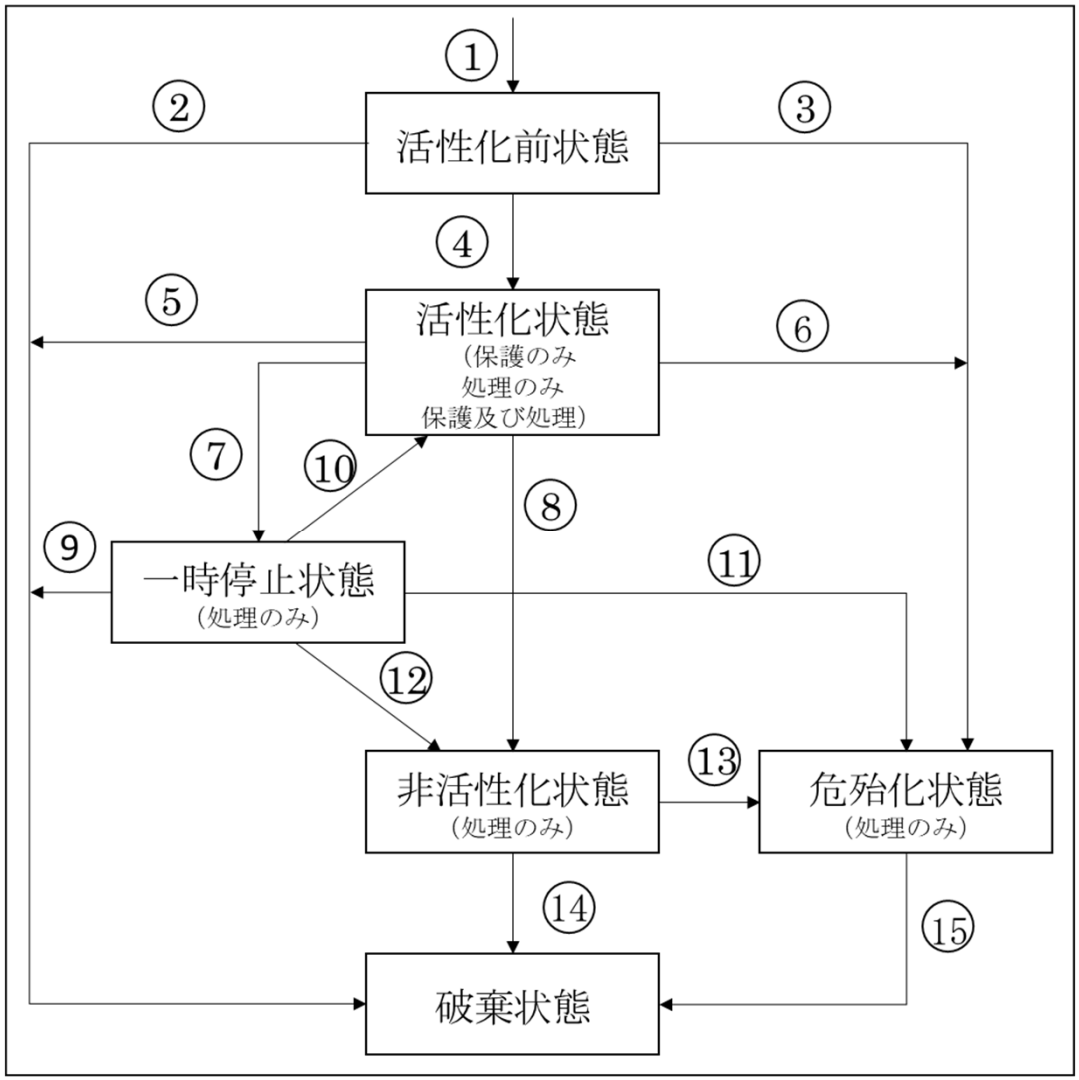


暗号鍵の鍵タイプ

鍵タイプ	セキュリティ特性	関連性保護	保証の必要性	保護期間
データ暗号化対称鍵	機密性 完全性 可用性	● 当該鍵を共有しているエンティティ ● 暗号化データ	ー	当該鍵の生成から、データのセキュリティ寿命が尽きる又は利用期間が終わるまでのいずれか遅い方の期間
鍵共有対称鍵	機密性 完全性 可用性	● 当該鍵を共有しているエンティティ ● 暗号化された鍵	ー	当該鍵の生成から、利用期間が終わる又は暗号化された鍵が保護を必要としなくなるまでのいずれか遅い方の期間
鍵共有プライベート鍵	機密性 完全性 可用性	● 鍵共有公開鍵 ● 暗号化された鍵	保有	当該鍵の生成から交換した全ての鍵の保護期間が終了するまで
鍵共有公開鍵	完全性	● 鍵共有プライベート鍵	有効性	当該鍵の生成から利用期間終了まで
署名プライベート鍵	機密性 完全性	● 署名検証公開鍵	保有	当該鍵の生成から利用期間終了まで
署名検証公開鍵	完全性 可用性	● 署名プライベート鍵 ● 署名データ	有効性	当該鍵の生成から署名データの検証が不要になるまで
認証対称鍵	機密性 完全性 可用性	● 当該鍵を共有しているエンティティ ● 認証データ	ー	当該鍵の生成から認証データの検証が不要になるまで
認証プライベート鍵	機密性 完全性	● 認証公開鍵	保有	当該鍵の生成から利用期間終了まで
認証公開鍵	完全性 可用性	● 認証プライベート鍵 ● 認証データ	有効性	当該鍵の生成から認証データの検証が不要になるまで

暗号鍵のライフサイクル／BCP対策

■ 暗号鍵のライフサイクル



■ 暗号鍵の危殆化対策

1. 鍵の利用期間を制限
2. 一つの鍵で保護されるデータ量を制限
3. 暗号処理ごとに異なる鍵を使用
4. 対称鍵やプライベート鍵が平文形式で存在する時間を制限
5. 平文の対称鍵やプライベート鍵を人間が閲覧できないようにする
6. 平文の対称鍵やプライベート鍵が配置される場所を物理的に保護されたコンテナ内に制限
7. 完全性チェックを使用して、鍵の完全性や他のデータとの関連性が危殆化していないことを確認
8. 鍵が不要になったらすぐに当該鍵を破棄

■ 鍵長移行に関する検討

1. システムやアプリケーションの運用寿命の延長に伴う対応
2. 暗号技術の推定セキュリティ強度の変更に伴う対応
3. 突発的な理由に伴う緊急移行にあたっての対応
4. 量子コンピュータの実現リスクへの対応

CRYPTREC GL-3010-1.0

資料７－２

暗号鍵設定ガイダンス

2022 年 x 月

（2022 年 3 月 3 日版）

独立行政法人 情報処理推進機構

国立研究開発法人 情報通信研究機構

目次

【修正履歴】

修正日	修正内容
2022.xx.xx (Ver.1.0)	初版発行

1. はじめに

1.1 本書の内容及び位置付け

情報を安全に取り扱うためには、通信情報や保管情報の暗号化や署名などに使う暗号技術のみに注意を払うだけでは不十分であり、その暗号技術に用いられる暗号鍵に対して適切に鍵長を設定し、さらに適切に鍵管理を行って安全に運用していくことが必要である。

図 1は、安全な暗号技術の導入にあたって考慮すべき項目と暗号技術の安全な運用にあたって考慮すべき項目の代表的なものを示しており、線でそれらの項目間での関連性を示している。本書では、このうち、緑色でハッチングされている項目を取り上げている。

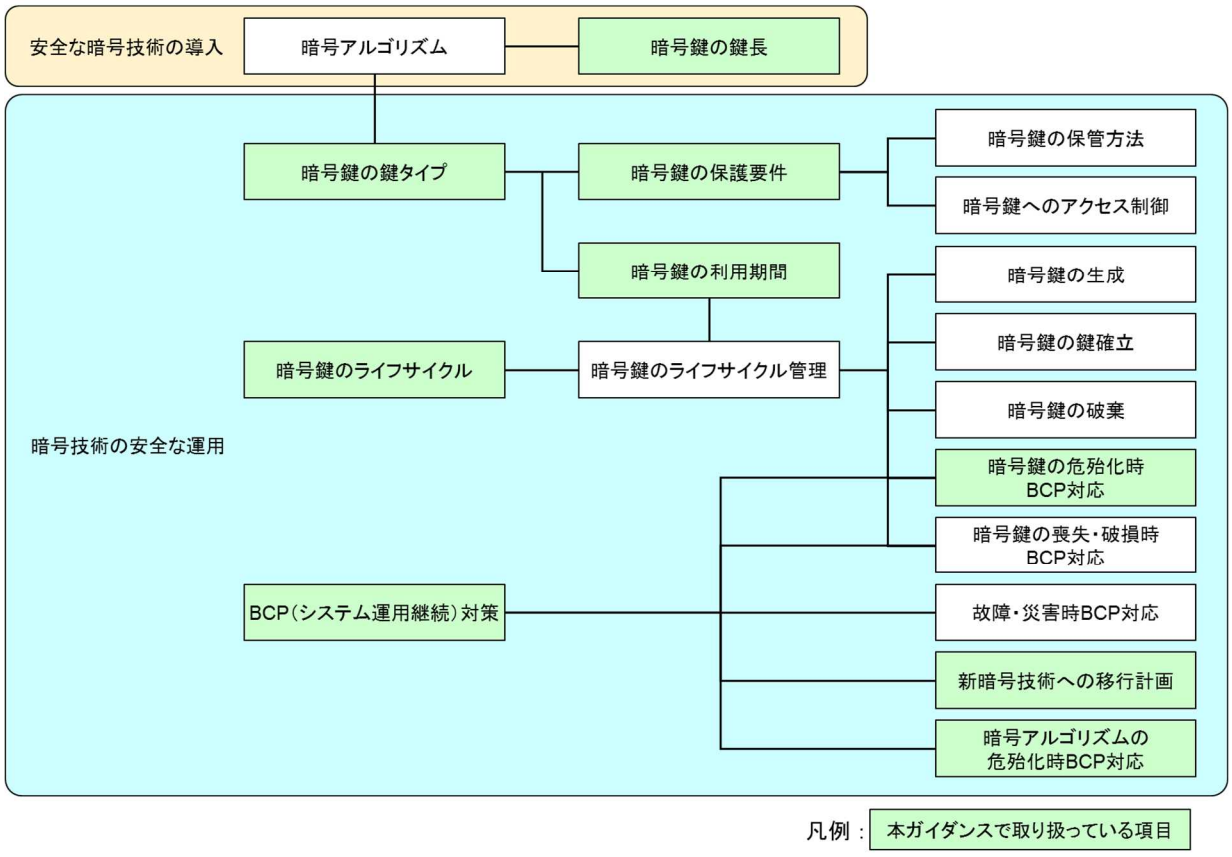


図 1　暗号技術の導入・運用にあたって考慮すべき代表的な項目

本書では、まず安全な暗号技術の導入の観点から、暗号技術を利用する際の鍵長の選択方法に関する一般的な考え方を解説する。

本書で示すセキュリティ強度は暗号技術のセキュリティ（暗号学的安全性）[1]を判断する上での

1　一般には「(暗号の）安全性」と表現されることが多いが、「安全性」には「物理的な安全性」や「人命などに対する安全性」といった意味で使われることもある。そのため、本書では、「(暗号の）安全性」のことを「セキュリティ」又は「暗号学的安全性」と表記する。

目安となるものであり、利用する鍵長によってセキュリティ強度と処理効率などが変わることに留意する必要がある。アルゴリズムの中には（特に RSA などの公開鍵暗号では）必要以上に長い鍵長を使用すると処理効率などに悪影響が出る場合がある一方、短すぎる鍵長を使用すると十分なセキュリティ強度を提供しないので、システムやアプリケーションの設計・開発にあたっては、適切なセキュリティ強度を満たすように鍵長を定めることが重要である。なお、実際の設計・開発にあたっては、鍵長以外の対策を適切に併用することによってシステム全体としてのセキュリティ確保を図るという方針を採用するも可能である。

本書を参考に、実際の利用用途や利用期間、環境、コスト、その他様々な制約条件を踏まえて、必要なセキュリティ強度を満たすように鍵長を**設定すべきである**。

次に、暗号技術の安全な運用の観点から、適切に暗号鍵の管理を行うために必要となる項目についての技術的概要を示す。なお、本書では具体的な対策方法や実現方法などについて説明しないので、より詳細な情報が必要であれば、NIST SP800-57 パート 1 改訂 5 版[2]などを参考にされたい。

本書は 7 節で構成されており、節立ては以下の通りである。

1 節では、イントロダクションとして、本書の位置づけや想定読者を示す。
2 節では、本書を理解する上での技術的な基礎知識を説明する。また、暗号技術ごとの推定セキュリティ強度をまとめる。
3 節では、鍵長選択の考え方を記載する。
4 節では、鍵を安全に運用するために重要な、鍵の生成から破棄までのライフサイクルについて説明する。
5 節では、鍵の利用期間について考え方を提示する。
6 節では、鍵の保護について考慮すべきポイントを提示する。
7 節では、運用中における鍵長移行に関する検討の必要性を示し、その際の論点等を記載する。

【重要な注意①】

政府機関等のサイバーセキュリティ対策のための統一基準[3]において適用対象となる情報システム（暗号化機能・電子署名機能の導入を行うものに限る。）に対して CRYPTREC 暗号リスト[4]に記載のアルゴリズムを利用する場合、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準[5]」に従ってセキュリティ強度を**設定しなければならない**。そのセキュリティ強度を満たすアルゴリズム及び鍵長の組合せを採用しなければ、統一基準の遵守事項を満たしているとは見なされないことに留意されたい。

---

2 NIST SP800-57 Part 1 Revision5 の日本語訳、https://www.ipa.go.jp/files/000090943.pdf
3 内閣サイバーセキュリティセンター（NISC）、政府機関等のサイバーセキュリティ対策のための統一基準（令和 3 年度版）、https://www.nisc.go.jp/active/general/pdf/kijyunr3.pdf
4 総務省・経済産業省、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)、https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r6.pdf
5 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準、https://・・・

【重要な注意②】

大規模な量子コンピュータが利用可能になった場合、Shor のアルゴリズムにより多項式時間で素因数分解問題や（楕円）離散対数問題が解けることが知られており、とりわけ CRYPTREC 暗号リストの公開鍵暗号（守秘、署名、鍵共有）に掲載されている全てのアルゴリズムにとって理論的には大きな脅威になっている[6]。

しかし、2021 年 3 月時点の CRYPTREC 調査[7]では、35（＝5×7）の素因数分解が成功しなかったという研究発表などを踏まえ、「現状の量子コンピュータでは暗号で用いるほど大きなパラメータの合成数を素因数分解することは困難であり、暗号で用いるパラメータの問題を解くためには量子ビット数やゲート計算のエラー率など量子コンピュータの性能の大幅な向上が必要であると考える。」と結論付けている。このことは、現時点で実現されている量子コンピュータと実際の暗号解読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ることを意味している。加えて、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を考慮すると、本書の発行時点（2022 年 3 月）において量子コンピュータによる公開鍵暗号の危殆化時期を予測することは困難である。

したがって、**本書では量子コンピュータによる暗号技術の危殆化は将来的なリスク要因に位置づけている**。7.5 節も参照されたい。

1.2 本書が対象とする読者

本書は、暗号技術を組込んだシステム又はアプリケーションの設計・開発・運用・提供にあたって、安全な暗号技術の選定、及び暗号技術の安全な運用方針・対策の作成や決定などに携わる管理者、設計者、開発者などを主な想定読者とする。

---

6 共通鍵暗号、暗号利用モード、メッセージ認証コードに対しては、おおむね鍵長の半分程度のセキュリティ強度に低下するが、公開鍵暗号ほど大きな影響は受けないと評価されている。つまり、鍵長を 256 ビットにするなどの対策で対処可能である。詳細については、CRYPTREC Report 2019「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」を参照されたい。
https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2019r1.pdf

7 CRYPTREC Report 2020「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」を参照されたい。https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2020.pdf

2. 技術的な基礎知識

暗号鍵を安全に設定し、運用していくために考慮すべき項目として以下のものがある。

- 暗号鍵の鍵長（2.2 節、3 節）
  システムやアプリケーションなどのセキュリティ（暗号学的安全性）に直接影響する項目である。どのような暗号処理に使う鍵なのか（鍵タイプ）、どのぐらいの期間利用するものなのかに依存して適切な鍵長を選択する必要がある。
- 暗号鍵の鍵タイプ（2.1 節）
  どのような暗号処理に使う暗号鍵なのかによって決まる項目である。鍵タイプの種類によって、暗号鍵に求められるセキュリティ要件は異なる（5 節、6 節参照）。
- 暗号鍵のライフサイクル（4 節）
  個々の暗号鍵の生成から破棄までの鍵状態とその間の遷移を示す項目である。暗号鍵の取扱いで重要なのは、利用する様々な鍵に対して、この鍵のライフサイクルを正しく運用管理することである。とりわけ、利用期間が経過した暗号鍵を利用停止・破棄することや、暗号鍵の危殆化が起きた又は疑われる場合の当該鍵の利用を制限・破棄することなどを適切に行うことによって、暗号鍵そのものの安全性を確保することが必要である。

2.1 暗号処理及び鍵タイプの種類

本書で取り上げる暗号処理及び鍵タイプは、表 1 及び

表 2 の通りである。

表 1　暗号処理の種類及び鍵タイプの種類

暗号処理		概要	利用する鍵タイプ
暗号化	通信時	2 つ又はそれ以上のエンティティ（ユーザやデバイス等）間の通信路上での盗聴を防止することを目的とした処理のこと。「暗号通信」ともいう。 送信者がデータの暗号化を行うタイミングと受信者が暗号化された通信データを復号するタイミングは時間的にそれほど離れていないことを前提とする。つまり、暗号化された通信データがそのまま長期間保存されることは想定しない。	データ暗号化対称鍵
	保管時	データベースやストレージデバイスなどに保管されるデータの機密性保護を目的とした処理のこと。 長期にわたって安全な保管ができるようにすることが期待され、データの暗号化を実施するタイミングと、復	

		号してデータを取り出すタイミングが大きく異なることが想定される。	
	鍵共有	共通鍵暗号を用いた暗号通信に先立ち、2 つ又はそれ以上のエンティティ間で、盗聴されずにセッション鍵の共有・確立・合意を行い、当該エンティティ間でセッション鍵を安全に共有することを目的とした処理のこと。	鍵共有対称鍵 鍵共有公開鍵 鍵共有プライベート鍵
署名		対象データの完全性及び署名者の検証を行い、当該データの完全性を確保することを目的とした処理のこと。当該データの否認防止の確認にも寄与する。 有効な（失効していない）署名検証用の公開鍵証明書の有効期間（*NotBefore* から *NotAfter* の期間）内では、当該データの完全性及び署名者の正当性が確保されることが期待される。	署名プライベート鍵 署名検証公開鍵
メッセージ認証		通信データや保管データの完全性検証を行い、当該データが変更されていないことを確認することを目的とした処理のこと。	認証対称鍵
エンティティ認証		正規のエンティティであることを確認することを目的とした処理のこと。	認証対称鍵 認証プライベート鍵 認証公開鍵

表 2　鍵タイプの種類

鍵タイプ	概要
データ暗号化対称鍵	共通鍵暗号を用いて、データの機密性保護に適用（平文データを暗号化）するために使用される。また、同じ鍵が、機密性保護を解除（暗号文データを復号）するためにも使用される。 この鍵は、暗号化したデータの機密性保護が必要な期間、秘密に**保持されなければならない**。
鍵共有対称鍵	共通鍵暗号を用いて、セッション鍵等の鍵情報を暗号化するために使用される。また、同じ鍵が暗号化された鍵情報を復号するためにも使用される。 この鍵は、暗号化した鍵情報の機密性保護が必要な期間、秘密に**保持されなければならない**。 鍵の名称については、鍵暗号化鍵、鍵ラッピング鍵、鍵合意対称鍵、鍵交換対称鍵と呼ばれることがある。
鍵共有公開鍵 鍵共有プライベート鍵	公開鍵暗号を用いて、セッション鍵等の鍵情報を交換するために使用される。鍵情報は、鍵共有プライベート鍵に対応する鍵共有公開鍵で暗号化され、当該鍵共有プライベート鍵で復号される。 鍵共有プライベート鍵は、鍵情報の交換が有効な期間中、秘密に**保持**

	されなければならない。 同じデータを暗号化すると同じ暗号文になるやり方で鍵共有を行う静的（長期的）な方式と、同じデータを暗号化しても異なる暗号文になるやり方で鍵共有を行う一時的（短期的）な方式とがある。 また、鍵共有の形式により、鍵合意、鍵配送、鍵交換などと呼ばれることがある。鍵の名称についても、鍵交換プライベート鍵、鍵交換公開鍵と呼ばれることもある。
署名プライベート鍵 署名検証公開鍵	公開鍵暗号を用いて、署名生成及び署名検証を行うために使用される。署名は、署名プライベート鍵を使って生成され、それに対応する署名検証公開鍵を使って検証される。 署名検証公開鍵は公開鍵証明書により、対応する署名プライベート鍵との関係が保証され、当該公開鍵証明書の有効期間中は署名検証に用いることができる。 署名プライベート鍵は、署名生成が許可されている期間中、秘密に**保持されなければならず**、同期間終了後は遅滞なく**破棄されなければならない**。もし、その期間中に漏えい・紛失等をした場合には、直ちに対応する署名検証公開鍵の公開鍵証明書を**失効させるべきである**。
認証対称鍵	共通鍵暗号（多くの場合、ブロック暗号）を用いて、データの完全性認証、又は ID 認証／エンティティ認証を行うために使用される。認証するデータに対する認証コードの生成及び検証に同じ鍵が用いられる。 この鍵は、認証が必要な期間、秘密に**保持されなければならない**。
認証プライベート鍵 認証公開鍵	公開鍵暗号を用いて、ID 認証／エンティティ認証を行うために使用される。一般にチャレンジ&レスポンス方式での認証が行われ、レスポンスを生成する際に認証プライベート鍵を利用し、当該レスポンスの正当性を確認する際に対応する認証公開鍵が利用される。 認証公開鍵は公開鍵証明書により、対応する認証プライベート鍵との関係が保証され、当該公開鍵証明書の有効期間中は ID 認証／エンティティ認証に用いることができる。 認証プライベート鍵は、認証が必要な期間、秘密に**保持されなければならない**。もし、その期間中に漏えい・紛失等をした場合には、直ちに対応する認証公開鍵の公開鍵証明書を**失効させるべきである**。

2.2 暗号技術の推定セキュリティ強度表現－ビットセキュリティ

技術分類が異なる暗号技術のアルゴリズムについて、同じ程度のセキュリティ（暗号学的安全性）を有するかどうかを判断する目安として、“ビットセキュリティ”（等価安全性ということもある）という指標がある。具体的には、評価対象とするアルゴリズムに対して最も効果的な攻撃

手法を用いたときに、どの程度の計算量があれば解読できるか（解読計算量[8]）に関連付けられた値で、鍵長とは別に求められる。表記上、　解読でき　き

表 3　公開鍵暗号の推定セキュリティ強度

セキュリティ強度 （ビットセキュリティ）	IFC RSA-PSS RSASSA-PKCS1-v1.5 RSA-OAEP RSAES-PKCS1-v1_5	FFC DSA DH	ECC ECDSA ECDH PSEC-KEM
112	k = 2048	(L, N) = (2048, 224)	P-224 B-233 K-233
128	k = 3072	(L, N) = (3072, 256)	P-256 B-283 K-283 W-25519 Curve25519 Edwards25519
192	k = 7680	(L, N) = (7680, 384)	P-384 B-409 K-409 W-448 Curve448 Edwards448
256	k = 15360	(L, N) = (15360, 512)	P-521 B-571 K-571

※ P: curve over Prime fields（素体曲線）、B: curve over Binary fields（拡大体（バイナリ）曲線）、K: Koblitz-curve（コブリッツ曲線）、W: Weierstrass-curve（ワイエルシュトラス曲線）、Curve: Montgomery-curve（モンゴメリ曲線）、Edwards: Edwards-curve（エドワード曲線）

以上を踏まえ、それぞれのビットセキュリティに対応するアルゴリズムの鍵長を示したのが表 3 である。2 行目のアルゴリズム名は、CRYPTREC 暗号リストに掲載されている公開鍵暗号のアルゴリズムを示している。

- 2 列目は、素因数分解問題ベースの公開鍵暗号（IFC：Integer Factorization Cryptography）を使用する場合の 1 列目で示したビットセキュリティを提供する鍵長（パラメータ）を示す。k は鍵長である。
- 3 列目は、有限体上の離散対数問題ベースの公開鍵暗号（FFC：Finite Field Cryptography）を使用する場合の 1 列目で示したビットセキュリティを提供する鍵長（パラメータ）を示す。L は公開鍵の鍵長、N はプライベート鍵の鍵長である。

- 4 列目は、楕円曲線暗号（ECC：Elliptic Curve Cryptography）を使用する場合の 1 列目で示したビットセキュリティを提供する曲線（パラメータ）を示す。一般に数字部分が鍵長に相当する（ただし、数字部分が 25519 の場合には鍵長 255 ビットに相当する）。例えば、P-256 は鍵長 256 ビットの素体曲線、B-283 は鍵長 283 ビットの拡大体（バイナリ）曲線、Edwards25519 は鍵長 255 ビットのエドワード曲線であることを示す。

2.2.2 共通鍵暗号の推定セキュリティ強度

CRYPTREC 暗号リストの「電子政府推奨暗号リスト」及び「推奨候補暗号リスト」に掲載されている共通鍵暗号については、鍵全数探索法が最も効果的な攻撃方法であるため、鍵全数探索法を用いた時のセキュリティ強度をビットセキュリティで表現する。一方、「運用監視暗号リスト」に掲載されている共通鍵暗号については、鍵全数探索法よりも効果的な攻撃方法（ショートカット攻撃法）が存在することが分かっているため、ショートカット攻撃法を用いた時の推定セキュリティ強度をビットセキュリティで表現する。

以上を踏まえ、それぞれのビットセキュリティに対応するアルゴリズム（及び鍵長）を示したのが表 4 である。

- 2 列目は、1 列目で示したビットセキュリティを提供するブロック暗号のアルゴリズム（及び鍵長）を示す。
- 3 列目は、1 列目で示したビットセキュリティを提供するストリーム暗号のアルゴリズムを示す。
- ブロック暗号を利用する暗号利用モード及びメッセージ認証コードのビットセキュリティは、ベースとなるブロック暗号のアルゴリズム（及び鍵長）に準拠する。

表 4 共通鍵暗号の推定セキュリティ強度

セキュリティ強度（ビットセキュリティ）	ブロック暗号※	ストリーム暗号	認証暗号
112	3-key Triple DES	－	－
128	鍵長 128 ビットを利用する CRYPTREC 暗号リスト掲載のブロック暗号	KCipher-2 Enocoro-128v2 MUGI	－
192	鍵長 192 ビットを利用する CRYPTREC 暗号リスト掲載のブロック暗号		－
256	鍵長 256 ビットを利用する CRYPTREC 暗号リスト掲載のブロック暗号	MULTI-S01	ChaCha20-Poly1305

※ ブロック暗号のセキュリティ強度はブロック長にも依存[9]するため、ブロック暗号を選択する際にはブロック長も併せて**考慮すべきである**。

2.2.3 ハッシュ関数の推定セキュリティ強度

ハッシュ関数については、利用方法によって要求される特性が異なるため、どちらのセキュリティ強度の推定値を使うのかは利用用途に応じて慎重に**判断すべきである**。特に、署名のように衝突困難性[10]を必要とするアプリケーションで使う場合（衝突困難性に対するセキュリティ強度に依存するケース）と、メッセージ認証コード（HMAC）や鍵導出（KDF）などのように衝突困難性を必要としないアプリケーションで使う場合（原像計算困難性[11]に対するセキュリティ強度に依存するケース）とを分けて考える必要がある。

衝突困難性に対するセキュリティ強度については、CRYPTREC 暗号リストの「電子政府推奨暗号リスト」及び「推奨候補暗号リスト」に掲載されているハッシュ関数のいずれにおいてもバースデーパラドックスよりも効率的に衝突するメッセージ組を求める効果的な攻撃方法が見つかっていないため、バースデーパラドックスによる衝突困難性に対するセキュリティ強度をビットセキュリティで表現する。なお、「運用監視暗号リスト」に掲載されているハッシュ関数 SHA-1 と RIPEMD-160 は、ハッシュ長が 160 ビットであるため、衝突困難性に対して 80 ビット以下[12]のセキュリティ強度しかない。このため、表 5 には含まれていない。

原像計算困難性に対するセキュリティ強度については、CRYPTREC 暗号リストに掲載されているハッシュ関数のいずれもが全数探索法よりも効果的な攻撃方法が見つかっていないため、全数探索法を用いた時のセキュリティ強度をビットセキュリティで表現する。

以上を踏まえ、それぞれのハッシュ関数のビットセキュリティを表現したのが表 5 である。

- 2 列目は、衝突困難性に対するセキュリティ強度に依存するケースにおいて、1 列目で示したビットセキュリティを提供するハッシュ関数のアルゴリズムを示す。署名と組み合わせてハッシュ関数を使う場合は、この列を参照すること。
- 3 列目は、原像計算困難性に対するセキュリティ強度に依存するケースにおいて、1 列目で示したビットセキュリティを提供するハッシュ関数のアルゴリズムを示す。メッセージ認証コード（HMAC）や鍵導出（KDF）にハッシュ関数を使う場合は、この列を参照するこ

---

9 一般にブロック長が長いほどセキュリティ（暗号学的安全性）が向上する。特にブロック暗号を使ってメッセージ認証を行う場合はその影響が大きい。現在では、128 ビットのブロック長を使うアルゴリズムが一般的である。

10 衝突困難性とは、同じハッシュ値を生成する 2 つのメッセージを見つけることが困難である性質のことをいう。効果的な攻撃方法が見つかっていないハッシュ関数では、ハッシュ長に対するバースデーパラドックスを基にしたセキュリティ強度となり、具体的にはハッシュ長の半分の値で表現される。例えば、ハッシュ長が 256 ビットである場合、バースデーパラドックスを基にしたセキュリティ強度は 128 ビットセキュリティとなる。

11 原像計算困難性とは、与えられたハッシュ値を生成するメッセージを構築したり見つけたりすることが困難である性質のことをいう。効果的な攻撃方法が見つかっていないハッシュ関数では、ハッシュ長に対する全数探索を基にしたセキュリティ強度となり、具体的にはハッシュ長の値で表現される。

12 SHA-1 については、衝突困難性に対してバースデーパラドックスよりも効果的な攻撃方法が見つかっているため、衝突困難性に対するセキュリティ強度は 80 ビットセキュリティにも達しない。

と。なお、利用する鍵のエントロピーがそのビットセキュリティ以上のエントロピーを有していることを前提とする。

表 5　ハッシュ関数の推定セキュリティ強度

セキュリティ強度 （ビットセキュリティ）	衝突困難性に対するセキュリティ強度に依存するケース （署名と組み合わせて利用する場合）	原像計算困難性に対するセキュリティ強度に依存するケース （HMAC や KDF に使う場合）
112	－	－
128	SHA-256 SHA-512/256 SHA3-256 SHAKE128 SHAKE256（ハッシュ長 256 ビット）	SHAKE128 SHA-1※ RIPEMD-160※
192	SHA-384 SHA3-384 SHAKE256（ハッシュ長 384 ビット）	－
256	SHA-512 SHA3-512 SHAKE256（ハッシュ長 512 ビット）	SHA-1、RIPEMD-160 及び SHAKE128 を除く CRYPTREC 暗号リスト掲載のハッシュ関数全て
備考	※SHA-1 及び RIPEMD-160 は、112 ビットのセキュリティ強度に達しないので、記載していない	※SHA-1 及び RIPEMD-160 は、192 ビットのセキュリティ強度に達しないので、128 ビットセキュリティに置いている

2.3 暗号技術の組合せによるセキュリティ強度の考え方

システムやアプリケーションによっては、2.1 節に記載された暗号処理のいくつかを組み合わせて実現することが求められる。このような場合、異なる種類の暗号処理に対して異なる暗号技術のアルゴリズムと鍵を使用する（例えば、暗号化に AES を使用し、署名に RSA を使用する）やり方もあれば、同じアルゴリズムと同じ鍵、又は同じアルゴリズムと異なる鍵で使用する（例えば、AES を使用して暗号化とメッセージ認証を実行する）やり方もある。また、利用するアルゴリズムも複数のアルゴリズムから選択できる場合もある（例えば、鍵共有において、公開鍵暗号なら RSA、Diffie-Hellman（DH）、ECDH などから、共通鍵暗号ならブロック暗号のいずれかのアルゴリズムを使った鍵ラッピング法から選択できる）。

そのため、システムやアプリケーションによっては、異なるセキュリティ強度を有する複数のアルゴリズムと鍵長を組み合わせて実現されることも多い。このような場合、最終的なセキュリティ強度は、最も弱いセキュリティ強度である暗号技術のアルゴリズムと鍵長によって決定され

る[13]（図 2 参照）。

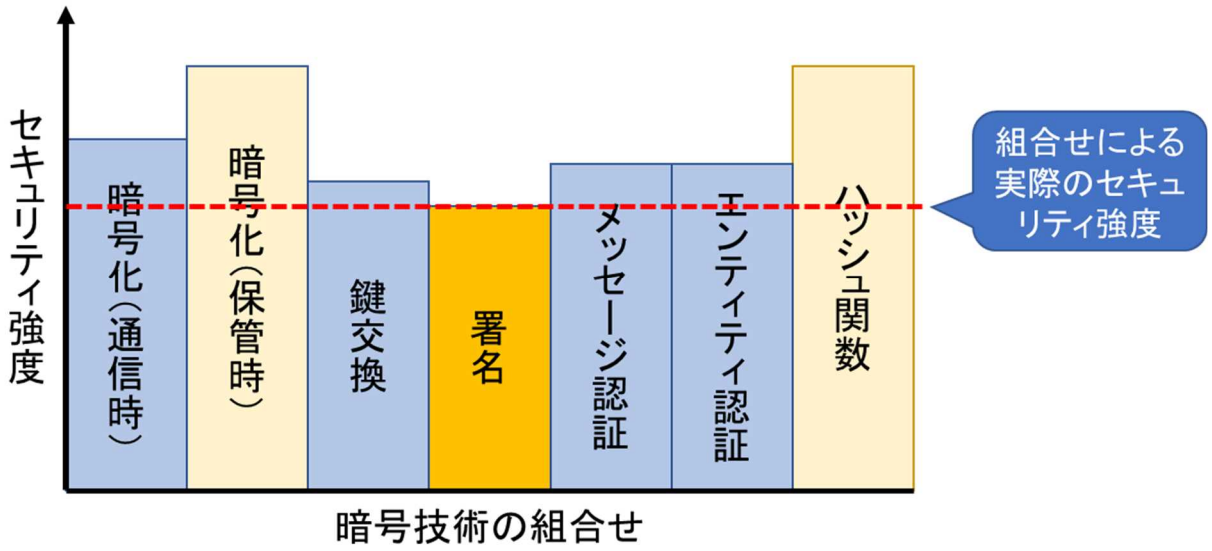


図 2　暗号技術の組合せによるセキュリティ強度（イメージ図）

以下に、いくつかの暗号技術の組合せ例を用いてセキュリティ強度の考え方を示す。

- 暗号通信において、セッション鍵の確立を公開鍵暗号で行い、データの暗号化は共通鍵暗号で行うハイブリット暗号化方式の場合、そのセキュリティ強度はより弱い方のアルゴリズムと鍵長によって決定される。例えば、256 ビット鍵の AES でデータの暗号化をする場合、通常であれば 256 ビットのセキュリティ強度を提供する。しかし、256 ビットのセッション鍵を確立するために P-256 ビット鍵（素体曲線での鍵長 256 ビットの鍵）の ECDH が使用される場合、P-256 ビット鍵の ECDH は 128 ビットセキュリティに該当するため（2.2.1 節参照）、そのセッション鍵で保護されたデータに対しては（256 ビットセキュリティではなく）128 ビットのセキュリティ強度しか提供されない。
- ハッシュ関数と署名アルゴリズムを組み合わせて署名を計算する場合、署名のセキュリティ強度はより弱い方のアルゴリズムによって決定される。例えば、SHA-256 を 2048 ビット鍵の RSA 署名と組み合わせて使用する場合、2048 ビット鍵の RSA 署名は 112 ビットセキュリティに該当するため（2.2.1 節参照）、その署名に対して（128 ビットセキュリティではなく）112 ビットのセキュリティ強度しか提供されない。

所定のセキュリティ強度をサポートするためには、アルゴリズムと鍵長の組合せを慎重に**選択すべきである**。例えば、通信されるデータを保護するために 128 ビットセキュリティ強度で暗号化、署名及び鍵共有を行う場合、以下のような暗号技術の選択の組合せが考えられる。

13 「樽理論」等とも呼ばれる。

i) 暗号化：共通鍵暗号で 128 ビットセキュリティ強度を有するアルゴリズム（と鍵長）のなかから選択する（例えば、128 ビット鍵の AES）。

ii) 署名：SHA-256 を署名生成前のデータハッシュに使用する。署名アルゴリズムは、128 ビットセキュリティ強度を有するアルゴリズムと鍵長の組合せのなかから選択する（例えば、3072 ビット鍵の RSA 署名）。なお、同一のビットセキュリティ強度で複数のアルゴリズムと鍵長が利用可能な場合、アルゴリズムの性能、メモリ要件などに基づいて選択してよい。

iii) 鍵共有：128 ビットセキュリティ強度を有するアルゴリズムと鍵長の組合せのなかから選択する。例えば、ECDH が利用可能な場合は、ECDH と 128 ビットセキュリティ強度の楕円曲線（P-256 など）の組合せを使用する。

3. 鍵長選択の考え方

本節では、保護対象のデータに対してシステムやアプリケーションが適切な保護を提供するための鍵長選択の考え方を提示する。鍵長の選択にあたっては利用する暗号処理の種類に依存することにも留意されたい。

3.1 運用寿命とセキュリティ強度要件の関係

システムやアプリケーションを設計・開発する際は、そのシステムやアプリケーションの検討・設計開始から構築、運用、さらに運用終了・廃棄までの運用寿命全体と、その期間に実現するセキュリティ強度の関係を考慮して適切なセキュリティ強度要件を設定し、その強度要件を満たす鍵長を**選択すべきである**。これは、時間の経過とともに解読計算能力が向上するため、運用開始時と比較して安全性が低下し、攻撃が成功する可能性が高まるリスクがあるためである。

結果として、システムやアプリケーションの運用途中でより安全な鍵長（又はより安全なアルゴリズム）への移行が必要となる場合があることにも留意されたい。また、システムやアプリケーションの運用中における予期しない危殆化等への対処のため、鍵長を容易に変更できるように配慮した移行計画を考慮するのが望ましく（7 節参照）、特に運用寿命が長期にわたるシステムやアプリケーションの場合には重要な視点である。

【重要な注意】

1.1 節に記載の通り、量子コンピュータによる暗号技術の危殆化は将来的なリスク要因に位置づけている。そのため、運用寿命が長期にわたるシステムやアプリケーションであって、特にその中で公開鍵暗号や署名を利用している場合には、将来的に耐量子計算機暗号（PQC: Post-Quantum Cryptography）の採用も視野に入れた移行計画が必要となる場合があることに留意されたい（7.5 節参照）。

本書では、システムやアプリケーションの運用寿命の期間と求められるセキュリティ強度要件の関係から 3 つの要件設定方法を示す（図 3 参照）。システムやアプリケーションの検討状況を踏まえ、適切な要件設定方法を選択されたい（図 4 参照）。

【要件設定方法①】

システムやアプリケーションの運用寿命全体を通して必要なセキュリティ強度要件を設定し、その強度要件を満たす鍵長を**サポート（実装）すべきである**。その際、必要なセキュリティ強度を過小評価又は過大評価しないように**注意すべきである**。

なお、利用終了時期を明確化し、それまでにより安全な鍵長に移行することを条件に、その期間中は安全と期待される鍵長を一緒にサポート（実装）してもよい。

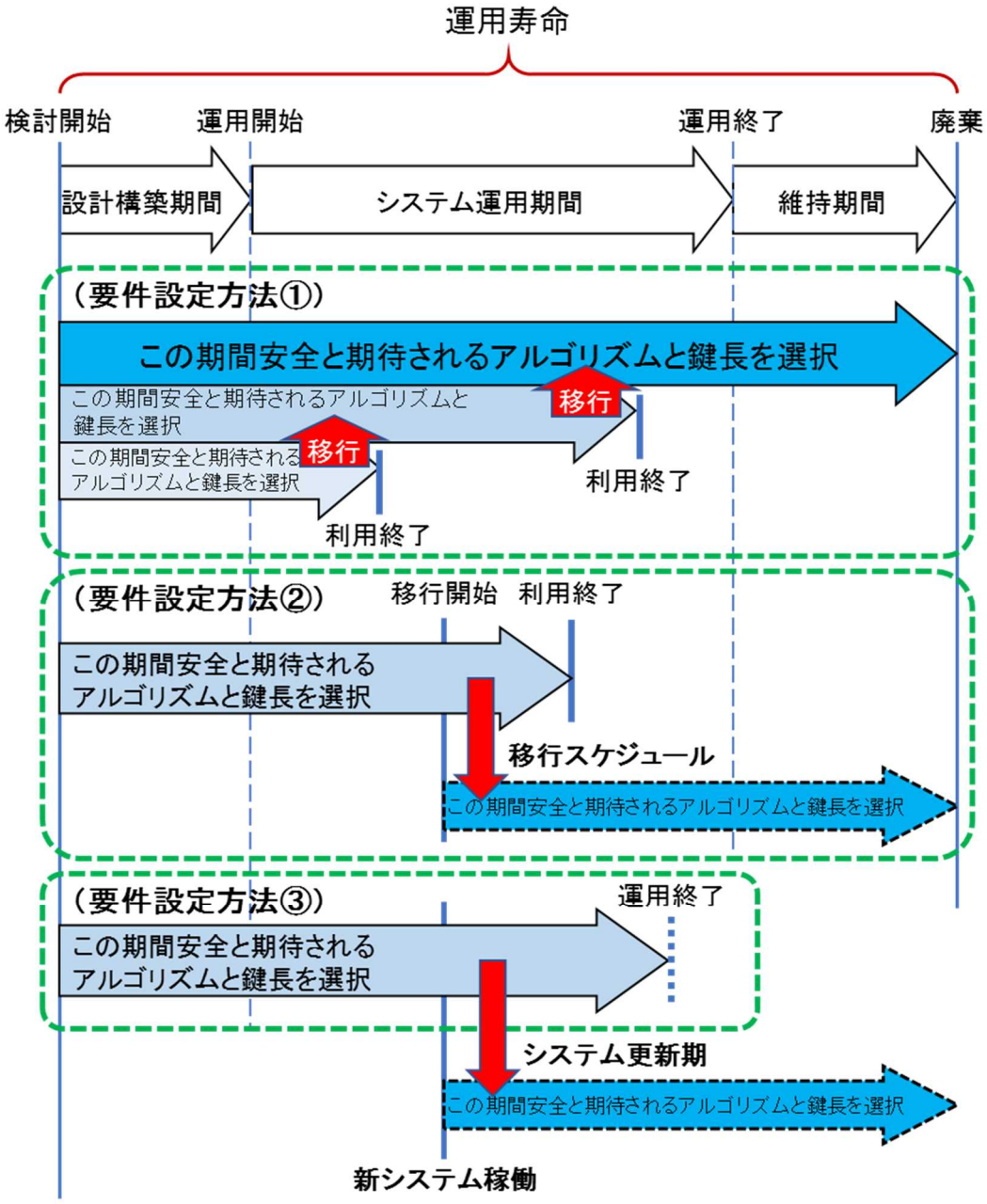


図 3　システムの運用寿命と求められるセキュリティ強度要件

【要件設定方法②】

対象となるシステムやアプリケーションの設計・開発における何らかの制約により、運用寿命全体を通して必要なセキュリティ強度要件を当初から設定することが困難である場合には、セキュリティ強度要件を切り替える移行時期を明確化したスケジュールを立案したうえで、その移行時期終了まで安全に運用するために必要なセキュリティ強度要件を設定し、その強度要件を満たす鍵長を**サポート（実装）すべきである**。その際、そのスケジュールには移行開始予定時期及び移行完了予定時期を明示することが望ましい。

【要件設定方法③】

対象となるシステムやアプリケーションにおいて、運用寿命が決まっていない（明確ではない）場合には、システムやアプリケーションの更新期を明確化したスケジュールを立案したうえで、その更新期まで安全に運用するために必要なセキュリティ強度要件を設定し、その強度要件を満たす鍵長を**サポート（実装）すべきである**。なお、そのスケジュールにおいて、新システムや新アプリケーションの稼働開始予定時期及び併用運用想定期間を示しておくことが望ましい。

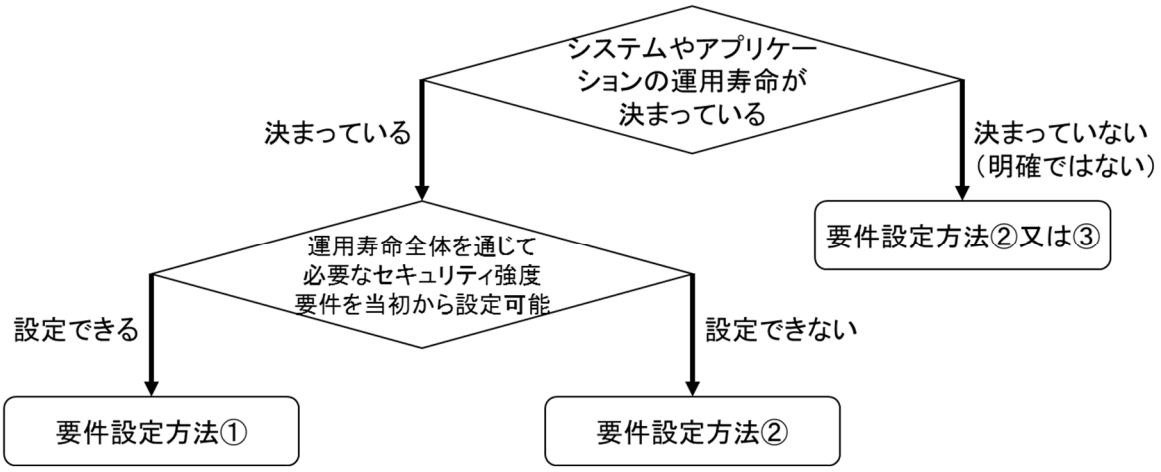


図 4　要件設定方法の選択フロー

3.2 求められるセキュリティ強度要件の考え方

必要なセキュリティ強度を設定する場合、システムやアプリケーションの運用開始年ではなく、予定している運用終了・廃棄年又は利用期間の終了年を基準として、表 6 を参考に考えることが望ましい。例えば、システムの運用終了・廃棄年を 2037 年に予定しているであれば「2040」の列を、2053 年に予定しているのであれば「2060」の列を参照してセキュリティ強度を設定する。システムの運用開始年が 2023 年であっても「2030」の列を参照するわけではない。

表 6 は 1982 年当時に DES が有していたのと同程度のセキュリティ強度を実現するために必要と推定されるビットセキュリティを表している。これは、解読能力の向上が計算機能力の向上だけにほぼ比例する（いわゆるムーアの法則[14]に従って向上していく）と仮定した場合にその後 10～15 年程度であれば解読が困難を期待される状態であることを意味する。ただし、未知の攻撃手法に対するセキュリティ（暗号学的安全性）の余裕度（“セキュリティマージン”という）がほとんどない状態なので、画期的な新たな解読手法が見つかるなどして解読能力が急激に向上した場合には、10～15 年持たずに解読される可能性があることに留意されたい。

[14] 「集積回路上のトランジスタ数が 18 ヶ月ごとに 2 倍になる」という経験法則のこと

したがって、**表 6 でのビットセキュリティを下限のセキュリティ強度として、一定のセキュリティマージン（数十ビット）を追加したそれ以上のセキュリティ強度で設定することが望ましい。**例えば、「2040」の列であれば最低で 104 ビット以上、できれば 128 ビット以上のセキュリティ強度を設定するのがよい。

このほかに、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」や Appendix に記載の情報を参照してセキュリティ強度を設定してもよい。

表 6　1982 年の DES と同等のセキュリティを提供すると推定される（＝その後 10～15 年程度安全と期待される）ビットセキュリティ

年	1982	2030	2040	2050	2060	2070
ANSSI（2014）[15]	56	81 ～ 96	86 ～ 104	91 ～ 112	96 ～ 120	101 ～ 128
Lenstra（2001）[16]	56	93	101	109	－	－
Lenstra（2004）[17]	56	88	95	102	－	－

ちなみに、CRYPTREC では、「素因数分解の困難性に関する計算量評価」と「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図を作成[18]している（Appendix 図 7 参照）。これは、公開鍵暗号の鍵長の選択について検討するために、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。

この予測図では、世界最速及び世界 500 位のスーパーコンピュータの計算機能力がムーアの法則に従って向上していくと仮定して外挿線を直線で引いたものである。極めて画期的な暗号解読手法が発明され、全く想定外のセキュリティ強度の低下が生じるような事象が生じない限り、この直線と所定のセキュリティ強度が交わる時期に解読可能になると見込まれるため、信頼性の高い下限のセキュリティ強度を表す指標として活用できる。

3.3 鍵長の選択及び利用期間の考え方

システムやアプリケーションの設計・開発においては、3.2 節を踏まえて設定したセキュリティ強度と同じかそれ以上のセキュリティ強度を満たす鍵長を選択して**サポート（実装）すべきである**。例えば、必要なセキュリティ強度として 128 ビットセキュリティが設定された時、公開鍵

---

15 Mécanismes cryptographiques - Règles et recommandations, Rev. 2.03, ANSSI , 02/2014 https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf

16 Selecting Cryptographic Key Sizes, Arjen K. Lenstra and Eric R. Verheul, Journal of Cryptology, vol. 14, p. 255-293, 2001. https://link.springer.com/content/pdf/10.1007/s00145-001-0009-4.pdf

17 Key Lengths, Arjen K. Lenstra, The Handbook of Information Security, 06/2004. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.694.8206

18 CRYPTREC Report 2020 暗号技術評価委員会報告、https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2020.pdf

暗号であれば鍵長 3072 ビットの RSA（2.2.1 節表 3 参照）、共通鍵暗号であれば鍵長 128 ビットの CRYPTREC 暗号リスト掲載のブロック暗号(2.2.2 節表 4 参照)、ハッシュ関数であれば SHA-256（2.2.3 節表 5 参照）などが選択肢となる。

なお、設定したセキュリティ強度以下のセキュリティ（暗号学的安全性）の鍵長をサポート（実装）してもよい。ただし、サポート（実装）された鍵長の全てが常に利用されてよいわけではないことに**留意すべきである**。サポート（実装）された鍵長の利用期間については、そのセキュリティ強度に応じて適切に**定めるべきである**。

具体的には、特定の鍵長について、保護されたデータが安全であり続けると評価された期間は「当該鍵長のセキュリティ寿命」と呼ばれ、その期間中はどの対象データに対しても適切な保護を提供することが期待される。一方、特定のデータに対して暗号保護が適用されてから最終的に処理をする必要がなくなるまでの期間（つまり、機密性や完全性を保持する必要がある期間）は「当該データのセキュリティ寿命」と呼ばれ、その期間中は当該データに対して適切な保護を提供することが期待される。なお、データのセキュリティ寿命は暗号処理の違いにより異なる（表 7 参照）。

一般に「鍵長のセキュリティ寿命」と「データのセキュリティ寿命」の間には、以下のような関係性が成り立つように**設定すべきである**（図 5 参照）。特に、「データのセキュリティ寿命」は利用する鍵の「鍵長のセキュリティ寿命」に包含されるように**扱うべきであり**、包含されないような場合には、鍵長の移行を**検討すべきである**（7 節参照）。

「新規データに対する暗号保護の適用期間[19]」＋「データのセキュリティ寿命」
≦「保護されたデータに対する処理の適用期間[20]」
≦「鍵長のセキュリティ寿命」

表 7　データのセキュリティ寿命

暗号化	通信時	（鍵共有後から）通信が終了するまでの期間
	保管時	データが暗号化されてから、復号する必要がなくなるまでの期間
	鍵共有	鍵共有を行っている期間
署名		データに署名生成してから、当該署名の署名検証を行う必要がなくなるまでの期間。多くの場合、法令や規則などで定められる期間、又は署名検証用の公開鍵証明書の有効期間に依存する
メッセージ認証		データに対するメッセージ認証コード（MAC）を生成してから、当該データの完全性検証を行う必要がなくなるまでの期間
エンティティ認証		エンティティ認証を行っている期間

19 データ暗号化対称鍵（暗号化）、鍵共有対称鍵（暗号化）、鍵共有公開鍵、署名プライベート鍵、認証対称鍵（MAC 生成）、認証プライベート鍵の利用期間に一致する

20 データ暗号化対称鍵（復号）、鍵共有対称鍵（復号）、鍵共有プライベート鍵、署名検証公開鍵、認証対称鍵（MAC 検証）、認証公開鍵の利用期間に一致する

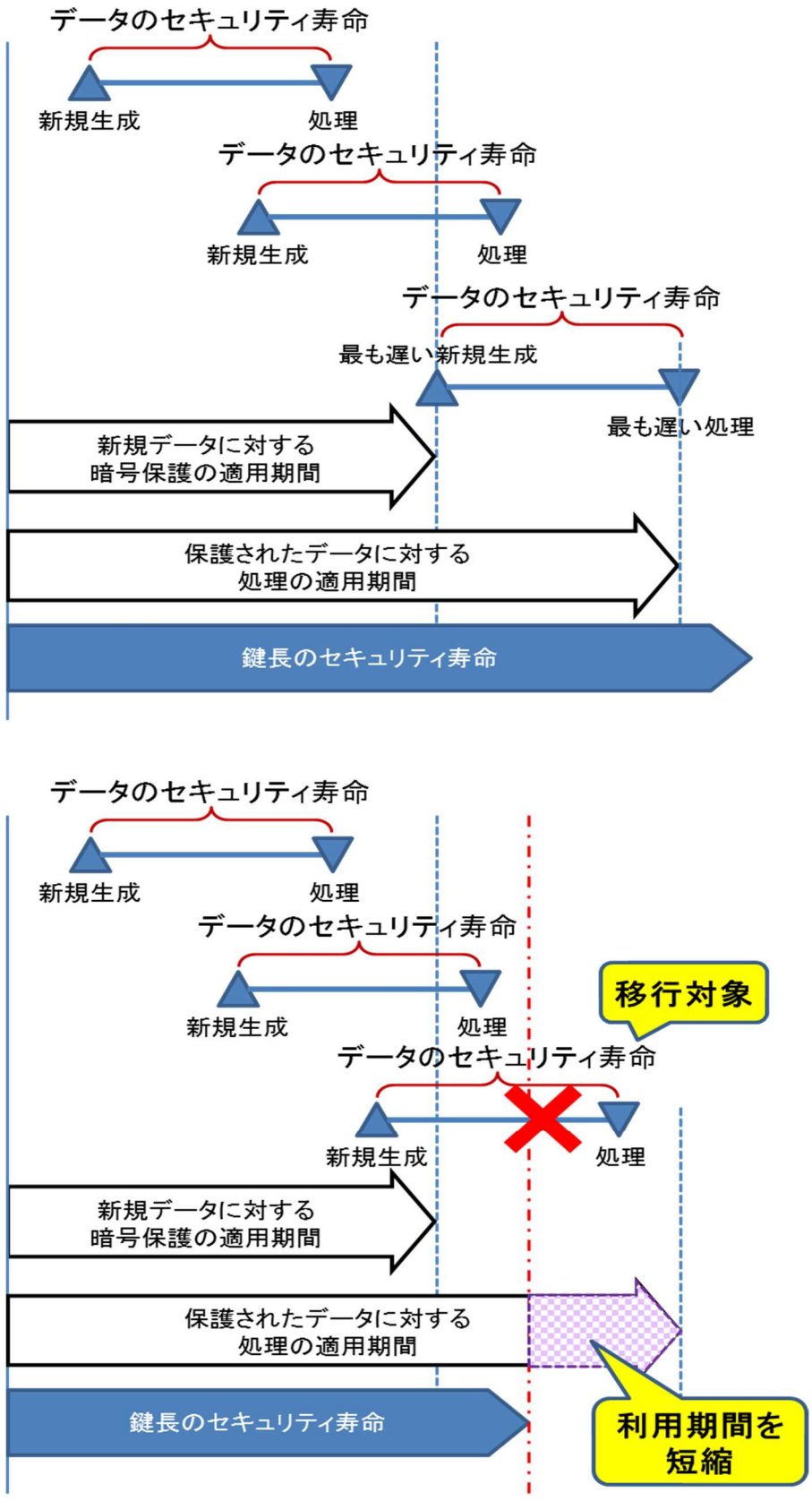


図 5　鍵長のセキュリティ寿命とデータのセキュリティ寿命の関係性

状態遷移①：

- 鍵は、生成された時点で直ちに活性化前状態に入る。

状態遷移②：

- 鍵が活性化前状態にあり、将来的にその鍵が必要ないと判断された場合、当該鍵は、活性化前状態から破棄状態に直接**遷移しなければならない**。
  なお、公開鍵暗号又は署名の場合には、鍵ペア（公開鍵とプライベート鍵の組）の両方の鍵が破棄状態に**遷移しなければならない**。

状態遷移③：

- 鍵が活性化前状態にあり、機密性保護が必要な鍵の機密性、又は鍵の完全性が疑われる場合には、当該鍵は、活性化前状態から危殆化状態に**遷移しなければならない**。
  なお、公開鍵暗号又は署名の場合には、鍵ペア（公開鍵とプライベート鍵の組）の両方の鍵が危殆化状態に**遷移しなければならない**。
- 危殆化状態に遷移する鍵が複数のエンティティに知られている場合、失効通知が**行われなければならない**。

状態遷移④：

- 対称鍵の利用期間、又は公開鍵とプライベート鍵の両方の利用期間が始まると、活性化前状態から活性化状態に**遷移しなければならない**。この遷移は、活性化する日付になった時に実行されてもよいし、外部イベントにより実行されてもよい。鍵がすぐに使用できるように生成された場合は、活性化前状態に入った直後に遷移が行われる。
- 証明書に関連付けられた鍵ペア（公開鍵とプライベート鍵の組）の場合、当該鍵ペアの公開鍵に対して最初に発行された証明書内に記載される *notBefore* の日付になったら、鍵ペアの両方の鍵が活性化状態に遷移する。

4.2 活性化状態

鍵が、新規データに対する暗号保護の適用、保護されたデータの処理、又はその両方に使用される状態である。なお、暗号保護の適用に利用できる期間は、活性化状態にある場合に限られる（5 節参照）。

状態遷移⑤：

- 鍵共有公開鍵、署名プライベート鍵、及び認証プライベート鍵と認証公開鍵については、鍵が危殆化することなく、その鍵の利用期間が終了した場合、活性化状態から破棄状態に直接**遷移しなければならない**。なお、対応する鍵共有プライベート鍵及び署名検証公開鍵は、この時点で活性化状態から非活性化状態に遷移することに留意されたい。

状態遷移⑥：

- 対称鍵又はプライベート鍵の危殆化が疑われた場合、又はそれが確認された場合、当該鍵（対応する公開鍵も）は活性化状態から危殆化状態に**遷移しなければならない**。
- 危殆化状態に遷移する鍵が複数のエンティティに知られている場合、失効通知が**行われなければならない**。

状態遷移⑦：

- 何らかの理由により、対称鍵又はプライベート鍵が一定期間使用されないのであれば、活性化状態から一時停止状態に**遷移しなければならない**。例えば、署名プライベート鍵は、当該鍵に関連付けられたエンティティが長期休暇中である、又はその鍵が危殆化した疑いがあるといった理由で、一時停止されることがある。後者の場合、失効及び交換のプロセスを開始する前に、鍵の状態を調査することができる。
  なお、公開鍵暗号又は署名の場合には、公開鍵とプライベート鍵の両方を同時に活性化状態から一時停止状態に**遷移しなければならない**。
- 一時停止状態に遷移する鍵が複数のエンティティに知られている場合、一時停止とその理由を示す通知が**行われなければならない**。

状態遷移⑧：

- 対称鍵については、新規データに対して暗号保護を適用する必要がなくなった場合、活性化状態から非活性化状態に**遷移しなければならない**。
- 鍵共有公開鍵又は署名プライベート鍵が活性化状態から破棄状態に直接遷移した場合、対応する鍵共有プライベート鍵及び署名検証公開鍵は、この時点で活性化状態から非活性化状態に**遷移しなければならない**。

4.3 一時停止状態

鍵の使用を一時的に中断させる状態である。この状態にある間は、新規データに対する暗号保護の適用を**行ってはならない**。

一時停止の理由には大きく 2 つある。一つは、鍵の危殆化が疑われる場合、当該鍵の失効及び交換のプロセスを開始する前に、状況を調査するための時間を確保する目的で行われるケースであり、もう一つは、鍵を所有するエンティティが当該鍵を利用できない場合（例えば、長期休暇中）に当人に無断で新規データに対する暗号保護の適用や保護されたデータの処理が行われないようにするためのケースである。

一時停止された鍵は、理由に応じて、活性化状態、非活性化状態、破棄状態、又は危殆化状態に遷移しうる。

状態遷移⑨：

- 一時停止状態中に利用期間が終了した鍵は、一時停止状態から破棄状態に**遷移しなければならない**。

状態遷移⑩：

- 鍵が危殆化しておらず、一時停止の理由が存在しなくなり、且つ暗号保護の適用の利用期間が残っている場合、一時停止状態にある鍵は、一時停止状態から活性化状態に**遷移しなければならない**。
  なお、公開鍵暗号又は署名の場合には、公開鍵とプライベート鍵の両方を同時に一時停止状態から活性化状態に**遷移しなければならない**。

状態遷移⑪：

- 対称鍵又はプライベート鍵の危殆化が疑われた場合、又はそれが確認された場合、当該鍵（対応する公開鍵も）は一時停止状態から危殆化状態に**遷移しなければならない**。
- 危殆化状態に遷移する鍵が複数のエンティティに知られている場合、失効通知が**行われなければならない**。

状態遷移⑫：

- 鍵が危殆化しておらず、一時停止の理由が存在しなくなった場合であって、新規データに対する暗号保護の適用の利用期間は残っていないが、保護されたデータの処理の利用期間が残っている場合、一時停止状態から非活性化状態に**遷移しなければならない**。一般に、データ暗号化対称鍵、認証対称鍵、及び署名検証公開鍵が対象となり得る。

4.4 非活性化状態

鍵が、新規データに対する暗号保護を適用するために**使用されてはならない**が、保護されたデータを処理するために使用できる状態である。一般に、データ暗号化対称鍵、認証対称鍵、及び署名検証公開鍵が対象となり得る。

状態遷移⑬：

- データ暗号化対称鍵又は認証対称鍵の危殆化が疑われた場合、又はそれが確認された場合、当該鍵は非活性化状態から危殆化状態に**遷移しなければならない**。
- 危殆化状態に遷移する鍵が複数のエンティティに知られている場合、失効通知が**行われなければならない**。

状態遷移⑭：

- 保護されたデータの処理に対する鍵の利用期間が終了した場合、又は保護されたデータを処理することが不要になった場合、非活性化状態から破棄状態に**遷移しなければならない**。

4.5 危殆化状態

対称鍵又はプライベート鍵の危殆化が疑われたり、確認されたりした状態である。危殆化した

鍵は、新規データに対する暗号保護を適用するために**使用されてはならない**。

一方、場合によっては、セキュリティ（暗号学的安全性）が担保されない可能性があるというリスクを受容し、高度に管理された条件下[21]において、保護されたデータを処理するために使用することがある。例えば、危殆化する前に生成された署名であり、署名後はずっと物理的に保護されていた場合、又は信頼できるタイムスタンプが署名データに含まれている場合であれば、署名データの完全性を判断するために検証されてもよい。

このように、危殆化した鍵の継続使用は、既に保護されているデータの処理に**限定されなければならず**、またその処理の結果に対して包含される危険性を十分に**認識すべきである**。

状態遷移⑮：

- 必要とされなくなったりした時点で、危殆化状態から破棄状態に**遷移すべきである**。

4.6 破棄状態

この状態の鍵は、いかなる暗号処理にも**使用されてはならない**。

対称鍵及びプライベート鍵は、コピーを含めて、当該鍵の痕跡を全て除去する方法で破棄して、物理的又は電子的な手段では**復元できない[22]ようにすべきである**（NIST SP800-88 改訂 1 版[23]参照）。公開鍵は、必要に応じて保持又は破棄することができる。

21 例えば、情報の機密性や完全性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合のことを指す。

22 単純な削除では、鍵を完全には消去できない場合があることに留意されたい。

23 NIST SP800-88 Revision1 の日本語訳、https://www.ipa.go.jp/files/000094547.pdf

5. 鍵タイプごとの鍵の利用期間

5.1 鍵の利用期間

利用する鍵は鍵のライフサイクルを踏まえて運用することが必要である（4 節参照）。

鍵の利用期間とは、その鍵に対して正規のエンティティが使用することを認められている期間、又はあるシステムやアプリケーションにおいてその鍵が有効である期間のことである。すなわち、4 節図 6 の*活性化状態*に存在することができる期間（データ暗号化対称鍵、認証対称鍵、及び署名検証公開鍵については*非活性化状態*の期間も含む）のことである。

鍵の利用期間の長さと、鍵の危殆化リスクやインシデントに伴う影響度とはトレードオフの関係にあるので、利用期間は慎重に検討して適切に**決定すべきである**。なお、鍵が危殆化した場合、それ以降の利用期間は有効と**見なすべきではない**。

また、以下の理由により、暗号処理ごとに異なる鍵を**使用すべきである**。

1. 鍵が危殆化した場合に被害が発生する可能性のある範囲を限定する
2. 2 つ以上の異なる暗号処理に同じ鍵を使用すると、一部又は全ての暗号処理で提供されるセキュリティ強度が低下する可能性がある
3. 暗号処理の違いにより、鍵管理上の要件が干渉することがある。例えば、署名プライベート鍵は署名生成が許可されている期間が経過したら直ちに**破棄すべきである**が、鍵共有プライベート鍵は、鍵共有が続く限り、破棄できない。

5.2 鍵の利用期間に影響を与える要因

一般に、鍵の利用期間が短いほど、その鍵に対するセキュリティ（暗号学的安全性）が向上する。しかしその一方で、鍵更新を頻繁に行うことが必要になるので、鍵の更新方法によっては人為的なエラーや設定ミスなどによる鍵の漏えいリスクが高まる可能性も想定し得る。

また、ビットセキュリティ強度のより高い鍵長を選択すれば、将来的な危殆化に対する耐性が向上すると期待されるので、そのアルゴリズムで使う鍵の利用期間を延ばすことが容易になる。ただし、その場合は、暗号解読による攻撃リスクよりも、システムへの侵入や破壊など、暗号解読以外の攻撃方法によって、より少ない時間とコストで鍵に直接アクセスされるリスクのほうが大きくなる可能性があることに**留意すべきである**。このため、鍵の保護が非常に重要になる（6 節参照）。

このように、鍵の利用期間は、当該鍵が使用されるシステムやアプリケーションの状況、利用環境等に大きく影響されるので、それらの状態に応じて適切に**設定されるべきである**。鍵の利用期間の長さに影響を与える要因の中には、以下のようなものがある（これらに限るわけではない）。

1. 暗号処理の種類

2. アルゴリズムのセキュリティ強度（例：鍵長、ブロック長など）
3. アルゴリズムの使用に必要な制限（例：ノンスの再利用を避けるための最大呼び出し回数）
4. 動作環境（アクセスが限定された安全な施設か、オープンオフィス環境か、一般にアクセス可能な端末や攻撃者が入手可能なデバイスか、など）
5. 同一の鍵で処理するデータ量又はトランザクション数（例：同一の鍵で暗号化された平文と暗号文のペア数など）
6. データのセキュリティ寿命
7. 秘密に保持する鍵の保護方法（例：物理的又は論理的なアクセス制御やセキュリティ対策など）及び保護環境（例：耐タンパーモジュール（TPM、HSM、SIM など）の使用など）
8. 秘密に保持する鍵のコピー数、及びそのコピーの配付先（例：鍵のバックアップ／アーカイブ、共有するエンティティなど）
9. 想定攻撃者の能力（例：想定される技術的攻撃能力や資金力など）
10. 新技術（例：量子コンピュータなど）による暗号解読成功確率の向上
11. 鍵が漏えいした場合や保護されている情報の機密性が失われた場合に想定されるインパクト（例えば、不正なエンティティへの情報漏えい、署名の偽造など）
12. 鍵の更新方法（例：自動更新か手動更新か、など）
13. 鍵の更新に関連するコスト（例：大規模データベースや分散型データベースの再暗号化、一度に非常に多くの鍵の交換が必要になるケースなど）

5.3 鍵タイプごとの鍵の利用期間の考え方

5.3.1 公開鍵暗号及び署名の鍵ペアの利用期間

公開鍵暗号及び署名の鍵ペア（公開鍵とプライベート鍵の組）では、ペアの鍵ごとに自身の利用期間を独立して設定する。鍵ペアの一方の鍵は、新規データに対する暗号保護の適用に使用され、もう一方の鍵は保護されたデータの処理に使用される。

- 鍵共有での鍵ペア（鍵共有公開鍵と鍵共有プライベート鍵）では、鍵配送スキーム[24]を使う場合、通常、鍵を配送するために暗号化する鍵共有公開鍵の利用期間よりも、鍵を復号する鍵共有プライベート鍵の利用期間のほうが長くなる。鍵合意スキーム[25]を使う場合、両方の鍵の利用期間は通常同じである。
- 署名での鍵ペア（署名プライベート鍵と署名検証公開鍵）の場合、通常、署名生成をするための署名プライベート鍵の利用期間よりも、署名検証をするための署名検証公開鍵の利用期間のほうが長くなる。なお、署名検証公開鍵が公開鍵証明書で配付される場合、その鍵の利用期間は当該公開鍵証明書の *notBefore* と *notAfter* の日付で示される期間（つまり、当該公開鍵証明書の有効期間）となる。また、署名生成できる利用期間が経過した場合、当該署名プライベート鍵は**破棄されなければならない**。

[24] 鍵生成者が送信者となり、受信者に当該鍵を送付する一方向での鍵共有になる
[25] 双方が鍵導出に必要な情報を相互に送付し、各自が鍵導出することで秘密鍵を共有する鍵共有になる

- 認証での鍵ペア（認証プライベート鍵と認証公開鍵）の場合、多くは、両方の鍵の利用期間は同じである。通常、認証プライベート鍵がチャレンジ情報の署名に使用されなくなった場合には、認証公開鍵も不要となる。

5.3.2 共通鍵暗号の鍵の利用期間

共通鍵暗号では、新規データに対する暗号保護の適用と保護されたデータの処理の両方で同じ対称鍵が使われる。

- 通信の暗号化に使用される場合、発信者がデータを暗号化してから受信者が復号するまでの時間は比較的短いと考えられる。この場合、暗号化に使える利用期間と復号に使える利用期間とは通常同じである。
  なお、攻撃者が暗号化された通信データを先に窃取しておいて解読が可能になった時期に復号を行う攻撃（Store (Harvest)-then-decrypt、Retrospective Decryption ともいう）を強く想定する必要がある場合には、通信時だけを考慮するのではなく、初めから保管を想定した暗号化の方法を**準用すべきである**。この攻撃に対しては後から防ぐことができないため、こういった攻撃に対する対策が必要であるかどうかについても、予め十分に**検討すべきである**。
- 保管データの機密性（暗号化）又は完全性（メッセージ認証）を保護するために使用される場合、通常、新規データに対して暗号保護に適用するための利用期間よりも、保護されたデータを処理するための利用期間のほうが長くなる。しかし、同じ対称鍵を使うことが必要となる関係上、新規データに対する暗号保護の適用のための利用期間を経過した後は、新たな暗号保護に適用しないように、運用による対策を**立てるべきである**。
- エンティティ認証のために使用される場合、被認証者がチャレンジ情報を暗号化してから検証者が復号して当該チャレンジ情報を得るまでの時間は比較的短いと考えられる。この場合、暗号化に使える利用期間と復号に使える利用期間とは通常同じである。

5.3.3 SP800-57 に記載されている推奨利用期間

様々な鍵タイプに対する推奨利用期間が NIST SP800-57 パート 1 改訂 5 版に記載されており、表 8 に示す。なお、この推奨利用期間の多くは、米国政府での運用効率を最大化したいという要望と、使用環境の最低基準を想定したものを基準としている。

したがって、この内容はあくまでも大まかなガイダンスであると**理解すべきであり**、この通りにすることを要求しているわけではない。実際には当該鍵が使用されるシステムやアプリケーション、利用環境等に依存して、より長い利用期間やより短い利用期間を設定することが適切とされる場合があることに注意されたい。

5.2 節の要因を踏まえ、利用期間の長さを適切に**設定すべきである**。

表 8　鍵タイプごとの SP800-57 に記載されている推奨利用期間

鍵タイプ	推奨利用期間	
	新規生成	処理
データ暗号化対称鍵	2 年以内	新規生成の利用期間終了後、3 年以内
鍵共有対称鍵	2 年以内	新規生成の利用期間終了後、3 年以内
鍵共有プライベート鍵	―	2 年以内
鍵共有公開鍵	1～2 年	―
署名プライベート鍵	1～3 年	–
署名検証公開鍵	―	数年（鍵長に依存）
認証対称鍵	2 年以内	新規生成の利用期間終了後、3 年以内
認証プライベート鍵	1～2 年	―
認証公開鍵	―	対応する認証プライベート鍵の利用期間と同じ

6. 鍵の保護について

6.1 鍵の保護要件

鍵は、対象とする暗号処理で使う必要がある限り、適切に利用できることが求められる。そのために当該鍵が満たすべき保護要件として考慮すべき項目は以下の通りである。ただし、表 9 に示すように、必要な保護要件は鍵タイプによって異なることに留意されたい。

セキュリティ特性

鍵に要求されるセキュリティ特性（すなわち、機密性や完全性、可用性）のことである。

- 機密性は、秘密にしておくことを意図した全ての鍵に要求される。一般に、適切なセキュリティレベルの CMVP[26]認証済暗号モジュールの利用、適切なセキュリティ強度での暗号化の実施、又は秘密情報への適切なアクセス制御下にある領域での保管などによって実現される。
- 完全性は、全ての鍵に要求される。
- 可用性は、保護されたデータの処理（復号や検証など）を行う際に必要となる全ての鍵に要求される。これは、鍵のコピーやバックアップ、アーカイブなどによって実現する場合もある。

関連性保護

ある鍵を使って暗号処理を正しく実行する際に、(当該鍵以外に) 適正に保護されていることが求められる鍵やデータのことを表す。

例えば、署名検証公開鍵を使って署名を検証しようとする際には、当該鍵に対応する署名プライベート鍵を使って署名が行われていることと、その署名プライベート鍵で署名された署名データ自体が必要である。そのため、署名検証公開鍵では、署名プライベート鍵と署名データが関連性保護の対象となる。

保証の必要性

- 有効性の保証とは、公開鍵暗号や署名で使用されるパラメータ、及び公開鍵とそれに対応するプライベート鍵との関係が算術的に正しいことを保証することである。この保証がない場合、公開鍵とプライベート鍵の対応関係が成り立っていないことになる。

保護期間

鍵が保護されている必要がある期間のことである。なお、機密性が求められる鍵は、保護期間終了後直ちに**破棄されるべきである**。

表 9　鍵の保護要件

鍵タイプ	セキュリティ特性	関連性保護	保証の必要性	保護期間
データ暗号化対称鍵	機密性 完全性 可用性	● 当該鍵を共有しているエンティティ ● 暗号化データ	ー	当該鍵の生成から、データのセキュリティ寿命が尽きる又は利用期間が終わるまでのいずれか遅い方の期間
鍵共有対称鍵	機密性 完全性 可用性	● 当該鍵を共有しているエンティティ ● 暗号化された鍵	ー	当該鍵の生成から、利用期間が終わる又は暗号化された鍵が保護を必要としなくなるまでのいずれか遅い方の期間
鍵共有プライベート鍵	機密性 完全性 可用性	● 鍵共有公開鍵 ● 暗号化された鍵	保有	当該鍵の生成から交換した全ての鍵の保護期間が終了するまで
鍵共有公開鍵	完全性	● 鍵共有プライベート鍵	有効性	当該鍵の生成から利用期間終了まで
署名プライベート鍵	機密性 完全性	● 署名検証公開鍵	保有	当該鍵の生成から利用期間終了まで
署名検証公開鍵	完全性 可用性	● 署名プライベート鍵 ● 署名データ	有効性	当該鍵の生成から署名データの検証が不要になるまで
認証対称鍵	機密性 完全性 可用性	● 当該鍵を共有しているエンティティ ● 認証データ	ー	当該鍵の生成から認証データの検証が不要になるまで
認証プライベート鍵	機密性 完全性	● 認証公開鍵	保有	当該鍵の生成から利用期間終了まで
認証公開鍵	完全性 可用性	● 認証プライベート鍵 ● 認証データ	有効性	当該鍵の生成から認証データの検証が不要になるまで

6.2 鍵の危殆化対策

保護されたデータは、アルゴリズムが安全であったとしても、鍵が危殆化していない場合にのみ安全である。

鍵の危殆化とは、当該鍵の機密性、完全性、又は鍵の所有者との関連付けが喪失した、もしくは喪失したと疑われる状態（4.5 節参照）になることである。例えば、鍵の危殆化が起きると以下のような影響が起こり得る。

- 鍵の機密性が喪失することは、別のエンティティ（不正なエンティティ）が当該鍵を使用して、その鍵を必要とする処理が実行できる可能性があることを意味する。例えば、データ暗号化対称鍵が危殆化した場合、不正なエンティティは、当該鍵を利用して、過去から将来にわたって暗号化された情報を復号（すなわち、情報が正規のエンティティ間の機密ではなくなる）したり、虚偽の情報を暗号化して正規のエンティティに送りつけたりする可能性がある。また、署名プライベート鍵が危殆化した場合は、不正なエンティティが虚偽の情報に署名した可能性が生じるため、当該鍵で署名された全てのデータの完全性と否認防止の特性が疑われる余地が出てくることを意味する。
- 鍵の完全性が喪失することは、鍵が（意図的か偶発的かにかかわらず）変更されたか、別の鍵が置き換えられたかのいずれかであり、当該鍵が正しくない（本来の鍵とは異なるものになっている）ことを意味する。
- 所有者との鍵の関連性が喪失することは、当該鍵を持つエンティティの身元が保証されない（すなわち、当該鍵の所有者が実際に誰であるかわからない）ことを意味する。

鍵の危殆化の可能性や影響を最小限に抑えるために、以下のような危殆化対策を考慮することが望ましい。特に、プライベート鍵及び対称鍵については、所有者に当該鍵の機密性を保護する責任がある。

1. 鍵の利用期間を制限する
2. 一つの鍵で保護されるデータの量を制限する
3. 暗号処理ごとに異なる鍵を使用する
4. 対称鍵やプライベート鍵が平文形式で存在する時間を制限する
5. 平文の対称鍵やプライベート鍵を人間が閲覧できないようにする
6. 平文の対称鍵やプライベート鍵が配置される場所を物理的に保護された“コンテナ”内に制限する
7. 完全性チェックを使用して、鍵の完全性や他のデータとの関連性が危殆化していないことを確認する
8. 鍵が不要になったらすぐに当該鍵を破棄する

7. 運用中における鍵長移行に関する検討の必要性

システムやアプリケーションに必要な暗号処理ごとに、システムやアプリケーションの想定運用終了・廃棄年、鍵長のセキュリティ寿命、及び保護すべき対象データのセキュリティ寿命を考慮し、必要なセキュリティ強度要件を満たす鍵長を選択して**利用すべきである**。

ただ、システムやアプリケーションの運用開始時点での利用環境等によっては、将来的に必要となる高いセキュリティ強度の鍵長を当初から選択すると、対応製品がない、導入コストが許容できないほど高くなる、性能が許容できないほど遅くなるなど、パフォーマンスや導入スケジュール等に悪影響を及ぼす可能性がある。このような場合、例えば、セキュリティ強度を切り替える移行時期を明確化したスケジュールを立案したうえで、システムやアプリケーションの運用寿命の前半に対して適切なセキュリティ強度を有する鍵長を選択して利用するといったことが考えられる。

また、システムやアプリケーションの運用開始時点は想定できなかった（もしくはあえて考慮対象から外した）暗号解読の向上や大規模な量子コンピュータの実現などが現実化し、想定していたよりも早期に使用している鍵長が適切なセキュリティ（暗号学的安全性）を提供できなくなることも起こり得る。

これらのケースでは、システムやアプリケーションの運用寿命の途中で、利用している鍵長のセキュリティ寿命が尽きつつあることを意味するため、そのセキュリティ寿命が尽きる前に、その後に必要となるセキュリティ強度を有する新しい鍵長へ**移行すべきである**。もし、鍵長のセキュリティ寿命が尽き、もはや情報に対して望ましい保護を提供しないと判断された（例えば、“解読された”可能性がある）場合、その鍵長によって保護されている情報は疑わしいと見なされることになる（例えば、当該データの機密性が損なわれていたり、完全性が保証できなくなったりする）。

なお、鍵長の移行だけでは必要なセキュリティ強度が達成できず、利用しているアルゴリズムそのものも同時に移行する必要がある場合には、鍵長だけの移行で必要となるコストや時間よりも多くのコストや時間がかかる可能性があるなど、さらに多くの検討課題が出てくることに留意されたい。

7.1 移行計画策定における論点

新しい鍵長へ移行するのは、システムやアプリケーションの規模や移行対象の鍵長の種類、代替する鍵長の実装状況、データフォーマットやプログラムインタフェースの差異による移行容易性の違いなどにもよるが、多くの場合、非常に時間とコストがかかる作業であることを念頭に置いておく必要がある。実際、過去にあった鍵長における大規模な移行（例：RSA での鍵長 1024 ビットから 2048 ビットへの移行）では、移行準備から移行完了までに 5 年から 10 年単位の時間

がかかっている[27]。

そのため、利用している鍵長のセキュリティ寿命を迎える少なくとも 5 年前までには、より安全な鍵長への移行計画を**策定すべきである**。その移行計画を立てる際には、いつからどのくらいの期間をかけてどの鍵長に移行するのかを**明確にすべきである**。

以下では、移行のための論点のいくつかを述べる。

7.1.1 通信時及び鍵共有の暗号化における論点

送信側と受信側の両方でより安全な新しい鍵長が実装され利用可能になった時点以降であれば、新しい鍵長だけを使うように切り替えることで移行対策は実現可能である。

なお、移行前に行われた通信や鍵共有について、攻撃者が通信中の暗号化された情報や鍵[28]を収集・保存している可能性を強く想定する必要がある場合、それらの通信内容が解読され、当該情報の機密性が危殆化する可能性がある[29]と**考えるべきである**ことに留意されたい。この場合、別の鍵やアルゴリズムを用いて再暗号化したとしてもセキュリティ上の必要な効果が得られるかどうかは不明である。

このような攻撃に対しては後から防ぐことができないため、こういった攻撃に対する対策が必要であるかどうかについても、移行計画を立てる際に十分に**検討すべきである**。

7.1.2 保管時の暗号化における論点

保管するデータに対して期待されるセキュリティ寿命（当該データの機密性を保持する期間）を考慮に入れることが非常に重要である。

データのセキュリティ寿命全体が鍵長のセキュリティ寿命を超えない範囲にある場合に、当該鍵長のデータ暗号化対称鍵を使って暗号化を**行うべきである**。もしそのような鍵長がサポート（実装）されていないのであれば、より安全な鍵長が実装され利用可能になった後に再暗号化を行うことができるようになるまでは、復号に利用する鍵長のセキュリティ寿命が尽きる期日と同じになるように当該データのセキュリティ寿命を**短縮すべきである**。

保管時の暗号化における移行対策では、新しい鍵長が実装され利用可能となった後の切り替えだけではなく、すでに暗号化された形で保管されているデータについての扱いも検討し、必要な処置を**行うべきである**。

---

[27] 政府機関の情報システムで使用されていた SHA-1 及び RSA-1024 を SHA-2 及び RSA-2048 に移行する際には、2008 年 4 月情報セキュリティ政策会議決定を皮切りに、各府省庁に対して 2008 年度中の移行計画の立案を要請、2009 年度に検証システム構築、2010 年度から 2013 年度までのシステム移行期間が設けられた。また、米国でも SHA-1 及び RSA-1024 を SHA-256 及び RSA-2048 へ 2010 年までに移行する方針が表明されたのも 2005 年である。

[28] 鍵共有が行われた際のセッション鍵が危殆化した場合、当該セッション鍵を利用した暗号通信も同時に危殆化したものと**判断すべきである**。

[29] Store (Harvest)-then-decrypt、Store now & decrypt later、Retrospective Decryption ともいう。このような攻撃は後から防ぐことができないため、システムやアプリケーションの設計・開発時点で必要性について十分に**検討すべきである**。

例えば、すでに暗号化された上で保管

ュリティ寿命を超えない範囲にある場合に、当該鍵長の認証対称鍵を使ってメッセージ認証コードの生成を**行うべきである**。もしそのような鍵長がサポート（実装）されていないのであれば、より安全な鍵長が実装され利用可能になるまでは、メッセージ認証コードの検証に利用する鍵長のセキュリティ寿命が尽きる期日と同じになるように検証期間を短縮**すべきである**。

メッセージ認証における移行対策では、新しい鍵長が実装され利用可能となった後の切り替えだけではなく、すでにメッセージ認証コードともに保管されているデータについての扱いも検討し、必要な処置を**行うべきである**。

例えば、すでにメッセージ認証コードとともに保管されているデータのセキュリティ寿命を延長した場合や何らかの理由でメッセージ認証コードの生成に利用した鍵長のセキュリティ強度が低下した場合、本来必要とされるセキュリティ強度よりも低い状態で当該データのメッセージ認証コードが生成されている状態になり得る。その場合は、データの完全性検証が正しく行えている間に、より安全な鍵長で当該データのメッセージ認証コードを再生成して**保護し直すべきである**。

なお、本来必要とされるセキュリティ強度よりも低い状態であっても、すでに生成されたメッセージ認証コードとともに保管されているデータに対する完全性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合には、特に移行対策を取ることなく、当該データの完全性検証を継続することを考慮してもよい。

7.1.5　エンティティ認証における論点

送信側と受信側の両方でより安全な新しい鍵長が実装され利用可能になった時点以降であれば、新しい鍵長だけを使うように切り替えることで移行対策は実現可能である。

なお、署名によるエンティティ認証の場合で、移行前の公開鍵証明書の有効期間が残っている場合には、失効処理などの**対応が必要となる**。

7.2 システムやアプリケーションの運用寿命の延長に伴う移行にあたっての対応

システムやアプリケーションの運用中の状況の変化により、当該システムやアプリケーションの設計・開発段階で当初想定した運用寿命どおりには運用を終了せず、延長して運用を継続する必要性が生じる場合があり得る。

このような場合、延長の必要性が判明した後、できるだけ早期に、新たに設定される運用寿命をもとに、必要なセキュリティ強度要件を**再評価すべきである**。再評価の結果、

- 求められるセキュリティ強度要件に変化がなく、現在利用中の鍵長でも同じように必要なセキュリティ強度を維持できる場合は、そのまま継続して利用してよい。

- より強力なセキュリティ強度が求められ、現在利用中の鍵長では必要なセキュリティ強度要件を満たすことができない場合には、7.1 節の論点を踏まえ、より安全な鍵長への移行計画をできるだけ早期に策定し、その計画に則って新しい鍵長への移行を**完了すべきである。**

7.3 暗号技術の推定セキュリティ強度の変更に伴う移行にあたっての対応

2.2 節に記載された暗号技術の推定セキュリティ強度の予測の妥当性を確認する観点から、5 年ごと又は必要に応じて、表 3～表 5 の暗号技術の推定セキュリティ強度のレビューを実施し、適宜適切な修正を加えることを計画している。例えば、画期的な暗号解読手法の発明や大規模な量子コンピュータの実現予測時期の精緻化などに伴い、鍵長によってはその推定セキュリティ強度の結果が変更になる可能性がある。

システムやアプリケーションの運用者は、本書が改訂されるタイミングで変更内容を確認し、利用している鍵長についての推定セキュリティ強度が変更されていないかどうかを**確認すべきである**。

利用している鍵長についての推定セキュリティ強度が変更され、当該鍵長では必要なセキュリティ強度要件を満たすことができないことが判明した時は、7.1 節の論点を踏まえ、より安全な鍵長への移行計画をできるだけ早期に策定し、その計画に則って新しい鍵長への移行を**完了すべきである。**

なお、移行に向けた対処方針が別途提示された鍵長を利用している場合には、その対処方針も参考にして移行計画を**検討すべきである**。

7.4 突発的な理由に伴う緊急移行にあたっての対応

可能性は低いものの、あるアルゴリズムに対する極めて画期的な暗号解読手法が発明され、当該アルゴリズムや鍵長の推定セキュリティ強度の急速な低下を引き起こす可能性はゼロではない。そのため、CRYPTREC では、CRYPTREC 暗号リスト掲載のアルゴリズム及び鍵長に対するセキュリティ（暗号学的安全性）を常時監視しており、セキュリティ（暗号学的安全性）が大きく懸念されるような学会発表やニュース報道などに対して、必要に応じて注意喚起情報を発表している。

注意喚起一覧：https://www.cryptrec.go.jp/er.html

利用しているアルゴリズムや鍵長についての注意喚起情報が発表されたとしても、緊急対応を求める旨の記述がなければ、直ちに何らかの対処を求めるというものではない。ただし、内容によっては、その後、CRYPTREC 暗号リスト又は本書での推定セキュリティ強度やセキュリティ

強度要件などの見直しに反映されることがあるので、それらが改訂された際には 7.3 節に従って対処することが望ましい。

Appendix　参考情報

[1] Cryptographic Mechanisms: Recommendations and Key Lengths, TR-02102-1 v2020-01, BSI, 03/2020.
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html

表 10　BSI（独）のセキュリティ強度選択基準（1.1 節、1.2 節）

2020～2022	（要件）100 ビット以上のセキュリティ強度であること （推奨）共通鍵暗号：128 ビットセキュリティ メッセージ認証コード：128 ビットセキュリティ 楕円曲線以外の公開鍵暗号（RSA, DH など）：100 ビットセキュリティ（鍵長 2000 ビット） 楕円曲線の公開鍵暗号（ECDSA など）：120 ビットセキュリティ（鍵長 250 ビット）
2023～2026	（要件）　120 ビット以上のセキュリティ強度であること （推奨）共通鍵暗号：128 ビットセキュリティ メッセージ認証コード：128 ビットセキュリティ 楕円曲線以外の公開鍵暗号（RSA, DH など）：120 ビットセキュリティ（鍵長 3000 ビット） 楕円曲線の公開鍵暗号（ECDSA など）：120 ビットセキュリティ（鍵長 250 ビット）

[2] Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 5, NIST, 05/2020.
https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

表 11　NIST（米）のセキュリティ強度選択基準（5.6.3 節）

2020～2030	（要件）新規データの保護（暗号化、署名生成など）は 112 ビット以上のセキュリティ強度であること。但し、2024 年以降は、3-key Triple DES は利用不可 保護済データの処理（復号、署名検証など）は 2-key Triple DES、1024 ビット RSA、SHA-1 相当以上のセキュリティ強度であること
2031～	（要件）新規データの保護（暗号化、署名生成など）は 128 ビット以上のセキュリティ強度であること 保護済データの処理（復号、署名検証など）は 2-key Triple DES、1024 ビット RSA、SHA-1 相当以上のセキュリティ強度であること

[3] Mécanismes cryptographiques - Règles et recommandations, Rev. 2.03, ANSSI, 02/2014
https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf

表 12　ANSSI（仏）のセキュリティ強度選択基準（2.1 節、2.2 節、2.3 節）

2014～2030	（要件）共通鍵暗号：128 ビット以上のセキュリティ強度。なお、ブロック暗号のブロック長は 128 ビット 楕円曲線以外の公開鍵暗号（RSA, DH など）：112 ビット以上のセキュリティ強度（鍵長 2048 ビット以上） 楕円曲線の公開鍵暗号（ECDSA など）：128 ビット以上のセキュリティ強度（鍵長 256 ビット以上） ハッシュ関数：128 ビット以上のセキュリティ強度（ハッシュ長 256 ビット以上） （推奨）楕円曲線以外の公開鍵暗号（RSA, DH など）：128 ビット以上のセキュリティ強度（鍵長 3072 ビット以上）
2031～	（要件）共通鍵暗号：128 ビット以上のセキュリティ強度。なお、ブロック暗号のブロック長は 128 ビット 楕円曲線以外の公開鍵暗号（RSA, DH など）：128 ビット以上のセキュリティ強度（鍵長 3072 ビット以上） 楕円曲線の公開鍵暗号（ECDSA など）：128 ビット以上のセキュリティ強度（鍵長 256 ビット以上） ハッシュ関数：128 ビット以上のセキュリティ強度（ハッシュ長 256 ビット以上）

* ビットセキュリティ自体の表示はなし。鍵長・ハッシュ長からの推定

[4] Commercial National Security Algorithm, National Security Agency (NSA), 01/2016.
https://apps.nsa.gov/iad/programs/iad-initiatives/cnsa-suite.cfm

表 13　NSA（米）のセキュリティ強度選択基準

TOP SECRET までの保護	（要件）共通鍵暗号：256 ビットセキュリティ 楕円曲線以外の公開鍵暗号（RSA, DH など）：128 ビット以上のセキュリティ強度（鍵長 3072 ビット以上） 楕円曲線の公開鍵暗号（ECDSA など）：192 ビットセキュリティ（鍵長 384 ビット） ハッシュ関数：192 ビットセキュリティ（ハッシュ長 384 ビット）

[5] Algorithms, Key Size and Protocols Report (2018), H2020-ICT-2014 – Project 645421, D5.4, ECRYPT-CSA, 02/2018.
https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf

表 14　ECRYPT（欧州）のセキュリティ強度選択基準（4.6 節）

互換性維持	
2018 ～ 2028 (near term use) 短期の利用	（要件）共通鍵暗号：128 ビットセキュリティ 楕円曲線以外の公開鍵暗号（RSA, DH など）：128 ビットセキュリティ（鍵長 3072 ビット） 楕円曲線の公開鍵暗号（ECDSA など）：128 ビットセキュリティ（鍵長 256 ビット） ハッシュ関数：128 ビットセキュリティ（ハッシュ長 256 ビット）
2018 ～ 2068 (long term use) 長期の利用	（要件）共通鍵暗号：256 ビットセキュリティ 楕円曲線以外の公開鍵暗号（RSA, DH など）：256 ビットセキュリティ（鍵長 15360 ビット） 楕円曲線の公開鍵暗号（ECDSA など）：256 ビットセキュリティ（鍵長 512 ビット） ハッシュ関数：256 ビットセキュリティ（ハッシュ長 512 ビット）

[6] Selecting Cryptographic Key Sizes, Arjen K. Lenstra and Eric R. Verheul, Journal of Cryptology, vol. 14, p. 255-293, 2001.
https://link.springer.com/content/pdf/10.1007/s00145-001-0009-4.pdf
[7] Key Lengths, Arjen K. Lenstra, The Handbook of Information Security, 06/2004.
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.694.8206

表 15　1982 年の DES と同等のセキュリティを提供すると推定される（＝その後 10～15 年程度なら完全解読が困難と期待される）ビットセキュリティ
([3] Figure 6、[6] Table 1、[7] 2 節式(2))

	1982	2030	2040	2050	2060	2070
[3] ANSSI（2014）	56	81 ～ 96	86 ～ 104	91 ～ 112	96 ～ 120	101 ～ 128
[6] Lenstra（2001）	56	93	101	109	－	－
[7] Lenstra（2004）	56	88	95	102	－	－

[8] CRYPTREC Report 2020

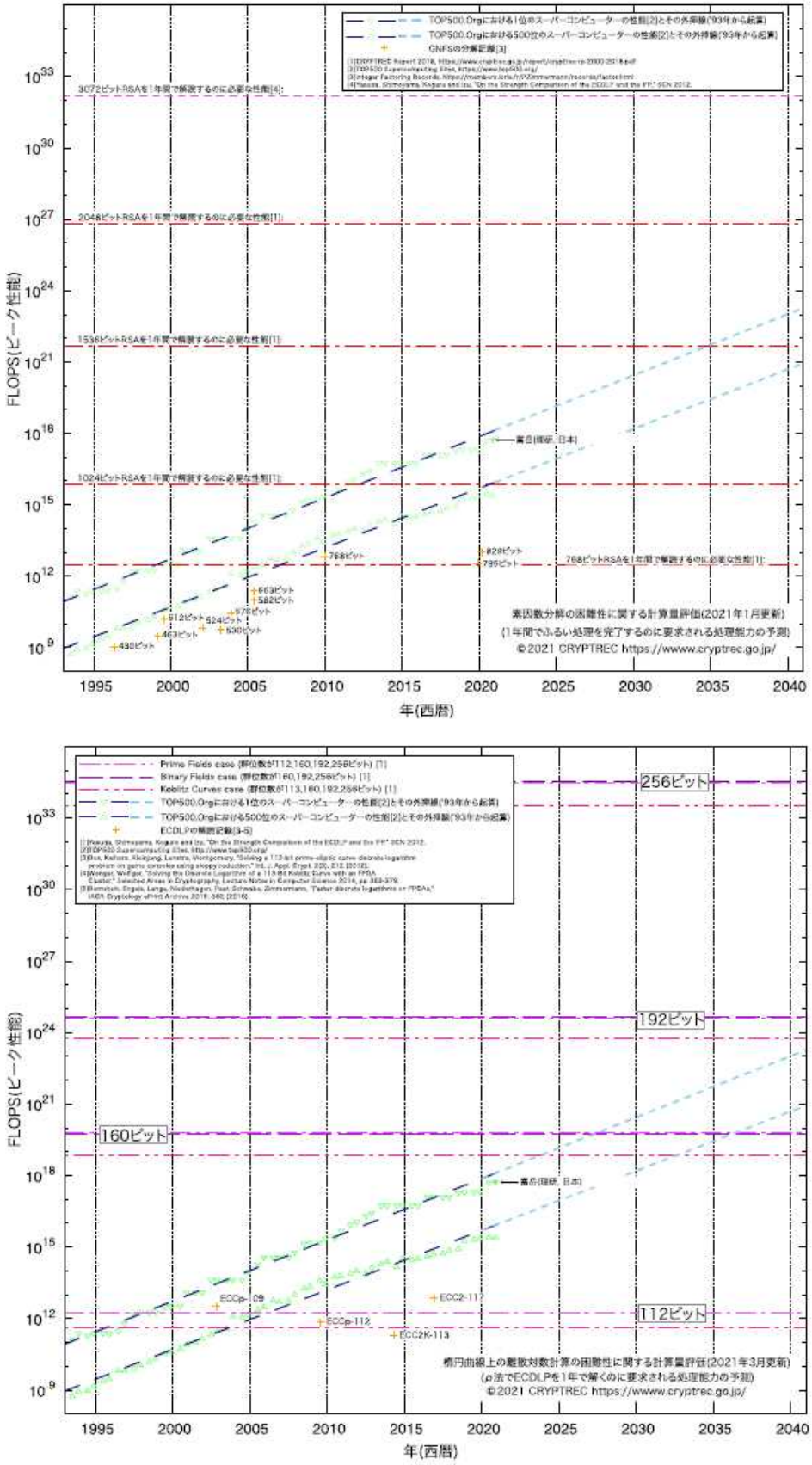


図 7　1 年で解読するのに必要な性能が達成できると見込まれる時期（図 3.1、図 3.2）

発行日　2022 年 xx 月 xx 日　第 1.0 版

発行者

・〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
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　暗号グループ）
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
2-28-8 HONKOMAGOME, BUNKYO-KU
TOKYO, 113-6591 JAPAN

・〒184-8795
東京都小金井市貫井北町四丁目 2 番 1 号
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　セキュリティ基盤研究室）
NATIONAL INSTITUTE OF
INFORMATION AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI, KOGANEI
TOKYO, 184-8795 JAPAN

資料８－１

CRYPTREC 暗号リストの改定について

CRYPTREC 暗号リストの改定に関する以下の項目について御審議いただきたい。なお、事務局の提案する CRYPTREC 暗号リスト改定案を資料８－３に、現行の CRYPTREC 暗号リストを資料８－４にそれぞれ示す。

１．ディジタル署名 EdDSA の推奨候補暗号リストへの追加

暗号技術評価委員会において実施されたディジタル署名 EdDSA に対する 2020 年度の安全性評価及び 2021 年度の実装性能評価に基づく暗号技術評価委員会からの提案（資料８－２参照）により、ディジタル署名 EdDSA を CRYPTREC 暗号リストの「推奨候補暗号リスト」に新たに掲載する。
追加先の技術分類は、公開鍵暗号　署名。

２．各暗号リストの本文に「暗号強度要件に関する設定基準」を参照する旨を追記

CRYPTREC 暗号リストに掲載されている暗号技術を利用する際に、適切なセキュリティ強度を実現するためのアルゴリズム及び鍵長の選択方法を規定した「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」を作成したことを踏まえ、電子政府推奨暗号リスト・推奨候補暗号リスト・運用監視暗号リストのそれぞれにおいて参照することを追記。
それぞれの記載への追記案は以下下線部太字のとおり。

電子政府推奨暗号リスト
暗号技術検討会及び関連委員会（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。**なお、利用する鍵長について、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。**

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のリスト。**なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の規定に合致する鍵長を用いることが求められることに留意すること。**

資料８－１

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。**なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の規定に合致する鍵長を用いることが求められることに留意すること。**

３．運用監視暗号リストの本文に脚注を追加

本文中の「互換性維持」について、趣旨を明確にするため、以下のとおり脚注を追加。

[7]既に稼働中のシステムやアプリケーション等との間での相互運用を継続すること

資料８－２

ディジタル署名 EdDSA の推奨候補暗号リストへの追加について

[暗号技術評価委員会の審議結果]

ディジタル署名 EdDSA について 2020 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は、いずれの結果も CRYPTREC 暗号リストに追加するために必要となる要件を満たしていると判断し、下記のように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：文書番号 CRYPTREC LS-0001-2012R6、https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r6.pdf）に追加することを暗号技術検討会に提案することを決定した。

- 安全性に関する見解
  - 曲線に関する安全性評価

    EdDSA での使用が見込まれる二つの曲線 Curve25519 及び Curve448 における ECDLP に対する古典計算機（従来の計算機）を用いた現時点での最良のアルゴリズムは ρ 法であるため、その安全性は現在使用されている楕円曲線暗号の場合と同じく、結果として主に基礎体の大きさで決定される。従って、Curve25519 の場合はほぼ 128 ビットセキュリティ、 Curve448 の場合はほぼ 224 ビットセキュリティの安全性を持つと判断する。また、それらの曲線上の演算も効率よく実行できることを確認した。
  - 方式の構成に関する安全性評価

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

EdDSA は ECDSA と同様に射影座標を用いた計算効率の良い演算が用意されているなどの実装において有益な性質を持つと考えられる。また、ECDSA と比較しても遜色ない処理速度である。よって、ディジタル署名 EdDSA は、ECDSA と比較しても遜色ない十分な実装性能を有していると判断した。

- CRYPTREC 暗号リストへの追加案

追加先：推奨候補暗号リスト

技術分類：「大分類：公開鍵暗号」、「中分類：署名」

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　改定案
（CRYPTREC暗号リスト）

平成２５年３月１日
デジタル庁・総務省・経済産業省
（最終更新：令和4年3月30日）

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。なお、利用する鍵長について、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[5]の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。

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

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

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

[5] CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, https://www.cryptrec.go.jp/list.html

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

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

（注4） 初期化ベクトル長は96ビットを推奨する。

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

推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術[3]のリスト。なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[6]の規定に合致する鍵長を用いることが求められることに留意すること。

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

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

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

（注7） 平文サイズは64ビットの倍数に限る。

（注12） ハッシュ長は256ビット以上とすること。

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

（注17） ブロック暗号には、CRYPTREC暗号リスト掲載128ビットブロック暗号を使う。利用用途はストレージデバイスの暗号化に限り、実装方法はNIST SP800-38Eに従うこと。

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

[6] CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, https://www.cryptrec.go.jp/list.html

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[7]以外の目的での利用は推奨しない。なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[8]の規定に合致する鍵長を用いることが求められることに留意すること。

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	該当なし
ハッシュ関数		RIPEMD-160
		SHA-1（注8）
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード（注16）	該当なし
メッセージ認証コード		CBC-MAC（注11）
認証暗号		該当なし
エンティティ認証		該当なし

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

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

（注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。
[7] 既に稼働中のシステムやアプリケーション等との間での相互運用を継続すること
[8] CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, https://www.cryptrec.go.jp/list.html

変更履歴情報

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

	（注13） （注14） （注16）	[新規追加]	CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。
	電子政府推奨暗号リスト（見出し）	名称	暗号技術
	推奨候補暗号リスト（見出し）		
	運用監視暗号リスト（見出し）		
令和２年12月21日	推奨候補暗号リスト（技術分類：暗号利用モード　秘匿モード）	該当なし	XTS（注17）
	（注17）	[新規追加]	ブロック暗号には、CRYPTREC暗号リスト掲載128ビットブロック暗号を使う。利用用途はストレージデバイスの暗号化に限り、実装方法はNIST SP800-38Eに従うこと。
令和３年4月1日	運用監視暗号リスト（技術分類：共通鍵暗号）	128-bit RC4（注10）	該当なし
	（注10）	互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。TLSでの利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。	[削除]
令和4年3月30日	文書クレジット	総務省・経済産業省	デジタル庁・総務省・経済産業省
	推奨候補暗号リスト（技術分類：公開鍵暗号　署名）	該当なし	EdDSA
	電子政府推奨暗号リスト（本文）	暗号技術検討会及び関連委員会（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。	暗号技術検討会及び関連委員会（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。なお、利用する鍵長について、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。

	電子政府推奨暗号リスト（本文）	「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」	「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[5]
	電子政府推奨暗号リスト（脚注）	該当なし	[5] CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, https://www.cryptrec.go.jp/list.html
	推奨候補暗号リスト（本文）	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。	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。なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の規定に合致する鍵長を用いることが求められることに留意すること。
	推奨候補暗号リスト（本文）	「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」	「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[6]
	推奨候補暗号リスト（脚注）	該当なし	[6] CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, https://www.cryptrec.go.jp/list.html
	運用監視暗号リスト（本文）	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。	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。なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の規定に合致する鍵長を用いることが求められることに留意すること。
	運用監視暗号リスト（本文）	互換性維持	互換性維持[7]
	運用監視暗号リスト（脚注）	該当なし	[7] 既に稼働中のシステムやアプリケーション等との間での相互運用を継続すること
	運用監視暗号リスト（本文）	「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」	「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[8]
	運用監視暗号リスト（脚注）	該当なし	[8] CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, https://www.cryptrec.go.jp/list.html

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

平成２５年３月１日
総務省・経済産業省
（最終更新：令和3年4月1日）

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

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

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

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

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

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

（注4） 初期化ベクトル長は96ビットを推奨する。

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

推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術[3]のリスト。

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

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

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

（注7） 平文サイズは64ビットの倍数に限る。

（注12） ハッシュ長は256ビット以上とすること。

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

（注17） ブロック暗号には、CRYPTREC暗号リスト掲載128ビットブロック暗号を使う。利用用途はストレージデバイスの暗号化に限り、実装方法はNIST SP800-38Eに従うこと。

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

運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったとCRYPTRECにより確認された暗号技術[4]のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。

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

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

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

（注11） 安全性の観点から、メッセージ長を固定して利用すべきである。

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

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

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

変更履歴情報

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

	（注13） （注14） （注16）	[新規追加]	CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。
	電子政府推奨暗号リスト（見出し）	名称	暗号技術
	推奨候補暗号リスト（見出し）		
	運用監視暗号リスト（見出し）		
令和２年12月21日	推奨候補暗号リスト（技術分類：暗号利用モード　秘匿モード）	該当なし	XTS（注17）
	（注17）	[新規追加]	ブロック暗号には、CRYPTREC暗号リスト掲載128ビットブロック暗号を使う。利用用途はストレージデバイスの暗号化に限り、実装方法はNIST SP800-38Eに従うこと。
令和３年4月1日	運用監視暗号リスト（技術分類：共通鍵暗号）	128-bit RC4（注10）	該当なし
	（注10）	互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。TLSでの利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。	[削除]

資料９

暗号技術検討会
２０２１年度　報告書（案）

２０２２年３月

１．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。

2021年度の各委員会の活動として、暗号技術評価委員会では、暗号技術（署名）であるEdDSAのCRYPTREC暗号リスト（推奨候補暗号リスト）への追加を検討するため、2020年度の安全性評価に引き続き実装性能評価を行った。また、同委員会の下に暗号技術調査WG（耐量子計算機暗号）及び暗号技術調査WG（高機能暗号）を設置して、それぞれ耐量子計算機暗号及び高機能暗号に関するガイドラインを作成するための執筆方針を決定した。また、軽量暗号に関するガイドラインの作成については、2016年度版の軽量暗号ガイドラインを更新するための基となる調査報告を行い、今後の作成方針を決定した。また、暗号技術調査WG（耐量子計算機暗号）では、「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図を更新した。暗号技術活用委員会では、CRYPTREC暗号リストの改定に向けた利用実績に関する選定基準の検討、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」及び「暗号鍵設定ガイダンス」の作成を行った。また、同委員会の下に設置された暗号鍵管理ガイダンスWGにおいて、「暗号鍵管理ガイダンス」の作成方針を決定した。なお、「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」は2021年度開催しなかった。これらの2021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 2021」を参照いただきたい。

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

末筆であるが、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。

2022年3月

暗号技術検討会
座長　松本　勉

２．暗号技術検討会開催の背景及び開催状況

２．１．暗号技術検討会開催の背景

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

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

暗号技術検討会において2003年2月に策定された電子政府推奨暗号リストは、2013年3月に10年ぶりの改定が行われ、CRYPTREC暗号リストとして発表されたが、その後においても、電子政府推奨暗号等の安全性を評価・監視し、暗号技術の更なる普及促進を行うため、2021年9月に発足したデジタル庁、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、デジタル庁、総務省及び経済産業省が共同で開催する暗号技術検討会（座長：松本勉横浜国立大学教授）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。

2021年度のCRYPTRECにおいては、暗号技術評価委員会では、暗号技術（署名）であるEdDSAのCRYPTREC暗号リスト（推奨候補暗号リスト）への追加を検討するため、2020年度の安全性評価に引き続き実装性能評価を行った。また、同委員会の下に暗号技術調査WG（耐量子計算機暗号）及び暗号技術調査WG（高機能暗号）を設置して、それぞれ耐量子計算機暗号及び高機能暗号に関するガイドラインを作成するための執筆方針を決定した。また、軽量暗号に関するガイドラインの作成については、2016年度版の軽量暗号ガイドラインを更新するための基となる調査報告を行い、今後の作成方針を決定した。また、暗号技術調査WG（耐量子計算機暗号）では、「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図を更新した。暗号技術活用委員会では、CRYPTREC暗号リストの改定に向けた利用実績に関する選定基準の検討、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」及び「暗号鍵設定ガイダンス」の作成を行った。また、同委員会の下に設置された暗号鍵管理ガイダンスWGにおいて、「暗号鍵管理ガイダンス」の作成方針を決定した。

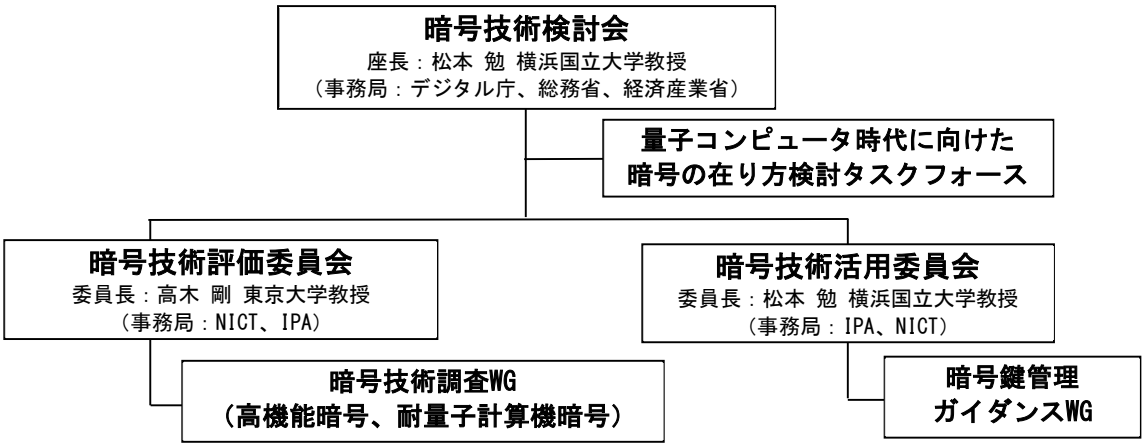


図2.2-1　2021年度CRYPTREC体制図

２．３．暗号技術検討会の開催実績

2021年度の暗号技術検討会は、暗号技術評価委員会、暗号技術活用委員会の活動報告、次期CRYPTREC暗号リストの改定に向けた検討に係る審議、暗号技術検討会2021年度報告書に係る承認等を行うために開催した。

【第 1 回】2022年3月30日（火）14:00～16:00
（主な議題）
- 2021年度暗号技術評価委員会 活動報告について
- 2021年度暗号技術活用委員会 活動報告について
- 利用実績による選定基準について
- 暗号強度要件に関する設定基準について
- 暗号鍵設定ガイダンスについて
- CRYPTREC暗号リストの改定について
- 暗号技術検討会 2021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．暗号技術評価委員会

３．１．１．活動の概要

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

- 暗号技術の安全性及び実装に係る監視及び評価
- 暗号技術の電子政府推奨暗号リストからの降格
- 暗号技術に関する注意喚起レポートのCRYPTRECホームページへの公表
- 推奨候補暗号リストへの新規暗号（事務局選出）の追加
- 新世代暗号に係る調査

また、次期CRYPTREC暗号リストとは別文書として、耐量子計算機暗号、軽量暗号、及び、高機能暗号に関するガイドラインを作成する。基本方針は以下のとおりである。

- 耐量子計算機暗号に関するガイドラインを作成するため、2021年度に、耐量子計算機暗号に関するワーキンググループを設置する。2022年度中に当該ガイドラインを作成する。
- 高機能暗号に関するガイドラインを作成するため、2021年度に、高機能暗号に関するワーキンググループを設置する。2022年度中に当該ガイドラインを作成する。
- 軽量暗号に関するガイドラインについては、2016年度に作成した「CRYPTREC暗号技術ガイドライン（軽量暗号)」の更新のため、2021年度は、掲載されている暗号方式に関わる安全性解析について、2017年度以降の技術動向調査を行う。2023年度中を目途に現ガイドラインを更新する。

これらの課題について2021年度に行った具体的な検討内容を、以下のとおり報告する。

３．１．２．暗号技術の安全性及び実装に係る監視及び評価

学会等での情報収集に基づくCRYPTREC暗号等の監視活動を行った。監視報告の詳細については、CRYPTREC Report 2021（暗号技術評価委員会報告）に掲載する。

３．１．３．推奨候補暗号リストへの新規暗号（事務局選出）の追加に向けた検討

ディジタル署名EdDSAは、RFC8032[1]で規定され、TLS1.3で採用された（RFC 8446[2]）署名アルゴリズムである。さらに、TLS1.2のようなTLS1.3 より前のバージョンでは、ECDSAと同じ暗号スイートを使ってEdDSAも利用可能となった（RFC8422[3]）。

[1] RFC8032, “Edwards-Curve Digital Signature Algorithm (EdDSA) ”, Jan. 2017
[2] RFC8446, “The Transport Layer Security (TLS) Protocol Version 1.3”, Aug. 2018
[3] RFC8422, “Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier”, Aug. 2018

ディジタル署名 EdDSA の安全性評価について、2020年度に評価を行い、EdDSAの曲線および方式の構成いずれについても安全性に問題は見つからなかったことから、「国際標準化等の実績がある」ことを根拠とした事務局で選出する暗号アルゴリズムの候補として、CRYPTREC暗号リストへの追加を視野に入れて評価を行うことが承認された。

2021年度は、EdDSA 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、2020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、EdDSA はディジタル署名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ので、CRYPTREC暗号リストの推奨候補暗号リストへ追加することを提案した。

３．１．４．暗号技術調査ワーキンググループ（耐量子計算機暗号）

大規模な量子コンピュータが実用化され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）の研究開発及び標準化などが各国で進められている。そこで、2021年度、暗号技術評価委員会では、耐量子計算機暗号に関するガイドライン（以下「耐量子計算機ガイドライン」という）を作成するためにワーキンググループを設置することが承認されていたことから、「新技術等に関する調査及び評価」の活動として暗号技術調査ワーキンググループ（耐量子計算機暗号）（以下「耐量子計算機暗号WG」という）を設置した。以下が主な検討項目である。

- 耐量子計算機暗号の研究動向調査をもとに、主要な耐量子計算機暗号についてのガイドラインを2021年度から2022年度にかけて作成する。
- 「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」の予測図の更新する

それらの成果（３．１．４．１～３．１．４．２節）は2021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。

３．１．４．１．耐量子計算機暗号に関するガイドラインの作成方針

ガイドライン及び調査報告書の作成

耐量子計算機暗号ガイドラインは、暗号理論に精通していない利用者を対象とし、耐量子計算機暗号に関する調査報告書は、暗号理論の研究者や技術者を対象とし、基本的には耐量子計算機暗号ガイドラインは調査報告書から技術的詳細を省き、その一部を抜粋したものする。ただし、暗号理論に精通していない利用者のために、耐量子計算機暗号の活用方法を耐量子計算機暗号ガイドラインでは記載し、調査報告書には記載しない。

ガイドライン及び調査報告書に記載する暗号方式の選定基準及び候補について

主要な公開鍵暗号方式（NIST PQC標準化への提案方式等）を記載するが、対象となる暗号方式は執筆担当委員が選定する。

記載すべき項目及び章立て

i. 導入
ii. PQC の活用方法（ガイドラインにのみ記載）
iii. 格子に基づく暗号技術
iv. 符号に基づく暗号技術
v. 多変数多項式に基づく暗号技術
vi. 同種写像に基づく暗号技術
vii. ハッシュ関数に基づく署名技術

- iii 章以降の構成（A 章の場合）

A.1. 安全性の根拠となる問題の説明（例：LWE問題、シンドローム復号問題）
A.2. 代表的な暗号方式の構成法（例：Regev暗号、McEliece暗号）
A.3. 主要な暗号方式
A.3.1. 暗号方式1（例：CRYSTALS-KYBER, Classic McEliece）
A.3.2. 暗号方式2
A.3.3. 暗号方式3
・・・
A.4. まとめ

３．１．４．２．「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図の更新

「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の予測図（以下単に「予測図」という。）は公開鍵暗号方式のセキュリティパラメータの選択について検討を行うため、2006年度に設置された暗号技術調査WG（公開鍵暗号）において作成された。当時、米国NISTは「NIST SP 800-57 Part 1 (Revised)(May,2006)」において暗号技術の鍵サイズに関して「80ビットセキュリティの利用期限を2010年まで」と推奨していた。現在では「NIST SP 800-57 Part 1 (Revision 5)(May,2020)」において「112ビットセキュリティの利用期限を2030年まで」と推奨している。

これらの状況を踏まえて、2019年度暗号技術評価委員会において、今後の予測図の取扱いについて審議し、下記のとおりの対応方針を決定していた。

今後の予測図の取扱いについて

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

対応方針
〈今後の予測図の取扱い〉
(1) 予測図を従来通り、いわゆるムーアの法則を仮定して外挿線を年度末から20年後まで直線で引

き[4]、評価に大きな変動がないと考えられる限りにおいては、安全サイドに倒した評価として当面の間更新していく。なお、予測図は各国・国際標準化機関等により示されている主要な暗号技術の安全性基準と比較すると、より現状に則した評価であり、危殆化時期がそれらよりも先に延びるものとなっている。

〈今後の公開鍵暗号のパラメータ選択〉

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

予測図の更新について

素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関する計算量評価に大幅な進展はなかったため、TOP500.orgにおける2021年6月・11月のベンチマーク結果を追加して予測図の更新を行った（図3.2-1及び図3.2-2）。

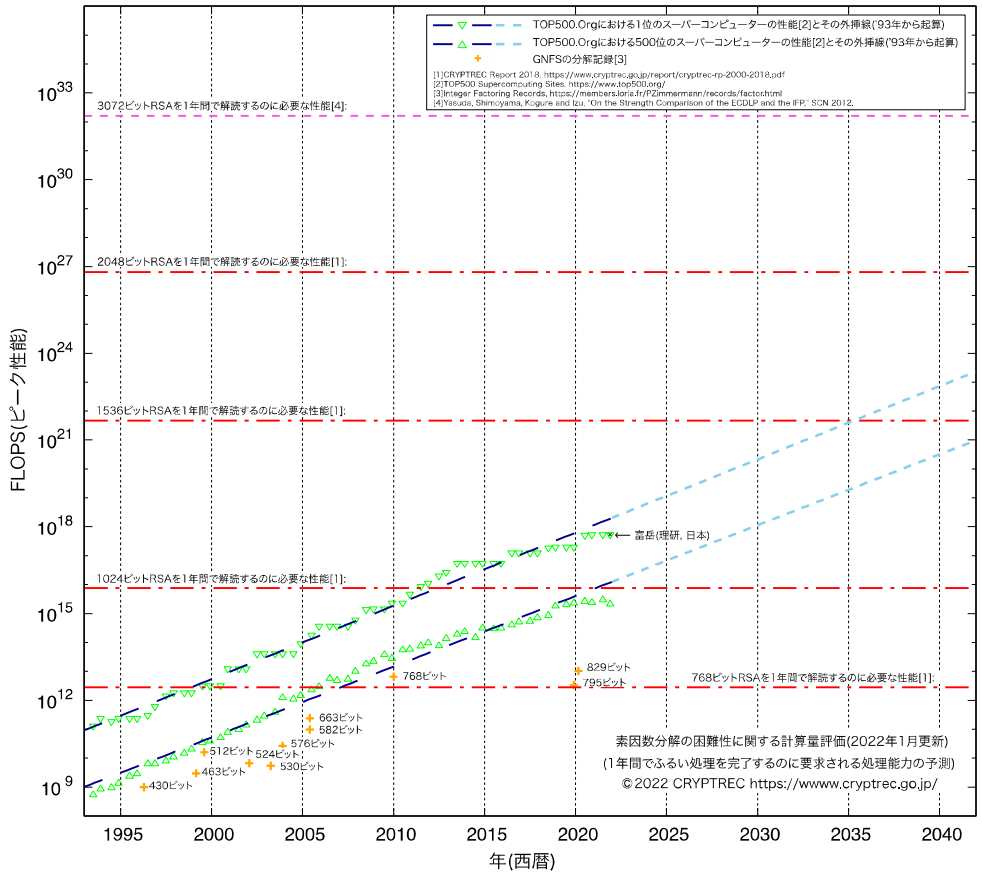


図3.2-1：素因数分解の困難性に関する計算量評価（2022年1月更新）[5]

[4] 2020年度暗号技術評価委員会にて、直線の外挿範囲を「年度末から20年後」と変更した。

[5] 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。

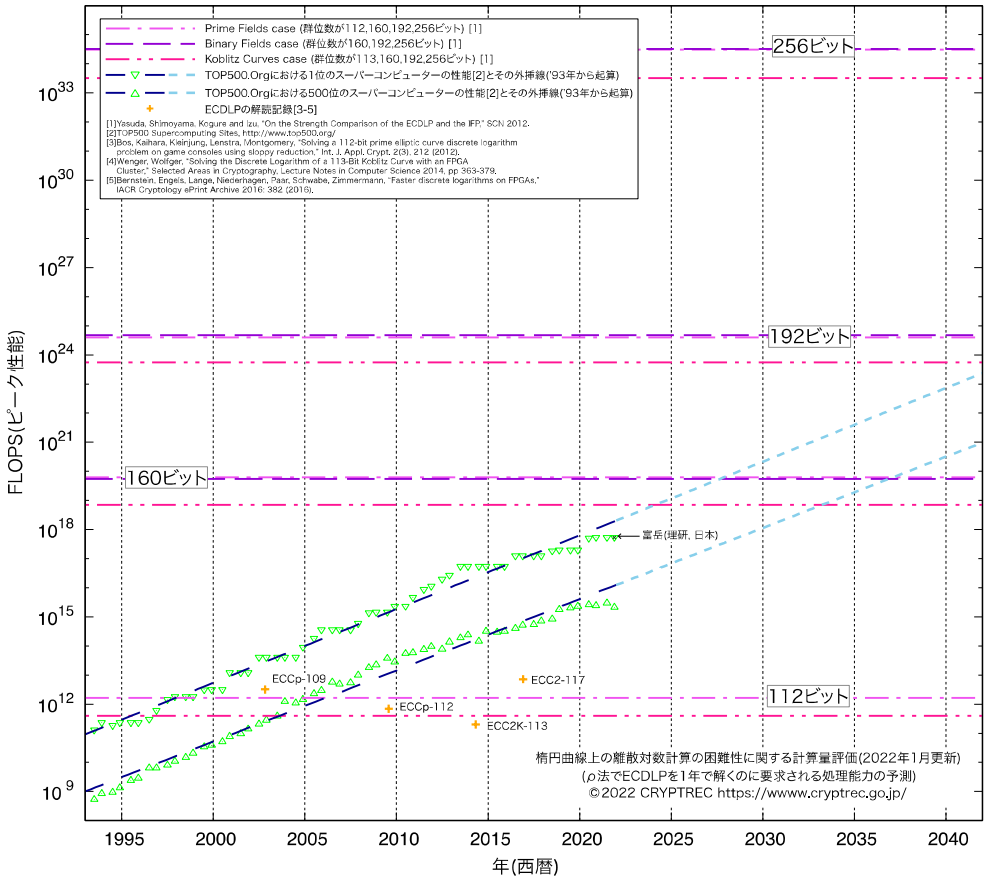


図3.2-2：楕円曲線上の離散対数計算の困難性に関する計算量評価（2022年1月更新）[6]

[6] スーパーコンピューターの性能の伸びに関する外挿線は僅かであるが鈍化してきている。

３．１．５．暗号技術調査ワーキンググループ（高機能暗号）

公開鍵暗号は、アプリケーションが多様となりその活用が広まっている。その中で、従来の公開鍵暗号よりも機能が向上した高機能暗号を利用してアプリケーションに適用することが有効と考えられている。そこで、2020年度第2回暗号技術検討会において高機能暗号ガイドラインを作成するために暗号技術調査ワーキンググループ（高機能暗号）（以下「高機能暗号WG」という）を設置することが承認された。

そして、2021年度暗号技術評価委員会において、2021年度の高機能暗号WGの活動として下記3点について実施する活動計画が承認された。

- 高機能暗号のスコープの明確化
- 高機能暗号技術に関する現状調査
- 高機能暗号のアプリケーションに関する調査

高機能暗号WGでは、上記3点について実施した。それらの成果（３．１．５．１～３．１．５．３節）は2021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。

３．１．５．１．高機能暗号のスコープの明確化

「高機能暗号」に対して一般的に合意されている定義がない。そこで、高機能暗号に関するガイドライン（以下「本ガイドライン」という）で記載する高機能暗号が何を指すものか定義する必要がある。このため、本ガイドラインで扱う高機能暗号のスコープを議論した。

そして、本ガイドラインでは、高機能暗号を「従来の暗号技術に対して、機能が追加・向上されるなどの優位性を主張する暗号、および、従来の暗号技術では困難であった事象を解決できるなどの新規機能を有することを主張する暗号技術」とした。ただし、今後の議論により修正が必要な場合は、高機能暗号WGにおいて議論し、修正することとした。

３．１．５．２．高機能暗号技術に関する調査

高機能暗号に関する現在の活用事例、標準化動向、アルゴリズムを調査し、現状を情報共有するとともに、将来的に利用される可能性がある高機能暗号を精査する。

この調査のため、第1回高機能暗号WGにおいて、本ガイドラインに掲載する可能性がある高機能暗号を列挙するとともに、高機能暗号を

- 守秘
- 認証・署名
- その他

に分類した。そして、調査すべき高機能暗号の対象を

- 守秘
  - IDベース暗号、属性ベース暗号、放送型暗号、しきい値暗号、準同型暗号、プロキシ再暗号化
- 認証・署名
  - IDベース署名、属性ベース署名、集約署名・MAC・マルチ署名、グループ署名、リング

署名、しきい値署名

- その他
  - マルチパーティ計算－秘密分散ベース、マルチパーティ計算－Garbled Circuitベース、ゼロ知識証明、検索可能暗号、Private Information Retrieval、Oblivious RA

の１８項目とし、それぞれに対し、“技術”、“活用事例”、“標準化”についてＷＧ委員が分担し調査した。

３．１．５．３．高機能暗号のアプリケーションに関する調査

既存技術より効率的になる分野、既存技術でカバーできていない分野などで、高機能暗号の活用が期待される分野を整理する。この活動の一環として、より深くアプリケーション、応用例を知るためにエンドユーザのヒアリングを検討する。そして、審議により、以下の4件の候補を決定した。

① 秘密分散を利用した医療データ活用
② 検索可能暗号＆属性ベース暗号
③ 属性ベース暗号を利用した放送サービスの拡張
④ マルチパーティ計算を利用した秘密情報秘匿したデータ分析

このうち、2件を選び、2022年度にヒアリングを行うこととした。ヒアリングは、2022年度の第1回、第2回高機能暗号WGにおいて、発表、質疑形式で行う予定である。

このヒアリング内容は、本ガイドラインの応用事例に掲載することとするが、ヒアリング先である企業、団体、個人の宣伝とはならないように、できるだけ、企業、団体、個人名などを削除できるようにし、ヒアリング先に了解を得ることとした。

３．１．５．４．高機能暗号に関するガイドラインの作成方針

ガイドラインの作成

高機能暗号ガイドラインは、高機能暗号を導入することを考えられている技術開発者や、コンソーシアム・標準化団体に関与する技術者などを読者として想定し、暗号理論に精通していない方々を対象として執筆する。

ガイドラインに記載する暗号方式の選定基準及び候補について

主要な高機能暗号方式として、対象となる暗号方式は執筆担当委員が選定する。

ガイドラインの章立て

2021年度の調査項目を本ガイドラインの目次とし、2022年度に執筆を行う。

１．　はじめに
２．　高機能暗号技術とその活用法
　２．１　高機能暗号とは
　２．２　高機能暗号の種類と分類
　２．３　高機能暗号はどこに使えるか、その有用性
　２．４　高機能暗号の活用事例と標準化動向

２．４．１　守秘関連の暗号技術の活用事例と標準化動向
２．４．２　認証・署名関連の技術の活用事例と標準化動向
２．４．３　その他の技術の活用事例と標準化動向
参考文献
３．　主な高機能暗号技術のアルゴリズム・プロトコルとその性能
３．１　守秘関連の高機能暗号技術
３．１．１　IDベース暗号
３．１．２　属性ベース暗号
３．１．３　放送型暗号
３．１．４　準同型暗号
３．１．５　プロキシ再暗号化
参考文献
３．２　認証・署名を目的とした高機能暗号技術
３．２．１　属性ベース署名
３．２．２　集約署名、集約MAC、マルチ署名
３．２．３　グループ署名
３．２．４　リング署名
３．２．５　閾値署名
参考文献
３．３　その他の高機能暗号技術
３．３．１　マルチパーティ計算－秘密分散ベース
３．３．２　マルチパーティ計算－Garbled Circuitベース－
３．３．３　ゼロ知識証明
３．３．４　検索可能暗号
３．３．５　Private Information Retrieval (PIR)
３．３．６　Oblivious RAM (ORAM)
参考文献
４．おわりに

３．１．６．軽量暗号に関するガイドラインの作成に関する活動

2020年度第2回暗号技術検討会にて、2016年度に作成した「CRYPTREC暗号技術ガイドライン（軽量暗号）」（以下、2016年度版ガイドラインと呼ぶ）の更新のため、2021年度は、掲載されている暗号方式に関わる安全性解析について、2017年度以降の技術動向調査を行い、2023年度中を目途に現ガイドラインを更新することが承認された。

2016年度版ガイドラインに掲載されている暗号方式に関わる安全性解析について、2017年度以降の技術動向調査を行った。また、現ガイドラインの更新方針を決定した。

３．１．６．１．軽量暗号に関する技術動向調査

2021年9月の時点で脅威に繋がる脆弱性が指摘されているか否かについて調査を実施した。調査報告書は、技術調査報告書として CRYPTREC ホームページに公開する。

調査概要は下記の通り。

- 調査対象
  - 2017 年 3 月に公開した「CRYPTREC 暗号技術ガイドライン（軽量暗号)」に掲載されている方式について、2017 年 3 月以降に大幅な安全性の劣化につながる脆弱性が見つかっているか否かについて調査。
  - 軽量暗号に関わる ISO/IEC 29192 シリーズに近年採録されたもしくは採録される予定の方式について、「CRYPTREC 暗号技術ガイドライン（軽量暗号)」における掲載の有無およびそれらの安全性について調査。
  - 「CRYPTREC 暗号技術ガイドライン（軽量暗号)」公開時に CAESAR プロジェクトが終了していなかったことから、CAESAR プロジェクトで最終的に選ばれたポートフォーリオ 6 方式について、「CRYPTREC 暗号技術ガイドライン（軽量暗号)」における掲載の有無およびそれらの安全性について調査。
- 実施方法
  - 事務局により調査を行い、調査報告書を執筆し、外部有識者による調査報告書のレビューを実施した。
- 調査結果概要

  各方式の安全性解析状況について、次のとおり表にまとめた。

	分類１	分類２	分類３
ブロック暗号	CLEFIA、LED、Simon、Speck、LEA	Piccolo、Midori、PRESENT、PRINCE、TWINE	
ストリーム暗号	ChaCha、Enocoro、Trivium		Grain v1、MICKEY 2.0
ハッシュ関数	Keccak 、 PHOTON 、 QUARK 、SPONGENT、Lesamnta-LW		
MAC	SipHash、Tsudik’s keymode	Chaskey、LightMAC	
認証暗号	ACORN、ASCON、AES-OTR、CLOC and SILC、Deoxys、Joltik、Ketje、Minalpher、OCB1、OCB3、PRIMATEs、AEGIS、$COLM_{127}$	$COLM_0$	OCB2 、 AES-JAMBU 、Grain-128A

分類１：仕様段数において安全性を脅かす攻撃が存在しない方式

- ✧ 秘密鍵の全数探索よりも効率的に実行可能な攻撃が存在しない方式
- ✧ 安全性基準を脅かす攻撃が存在しない方式

分類２：特定の場合を除き、仕様段数において安全性を脅かす攻撃が存在しない方式

- ✧ 秘密鍵の全数探索よりも効率的に実行可能な攻撃が存在しない方式

分類３：仕様段数において安全性基準を満たさない方式

- ✧ 秘密鍵の全数探索よりも効率的に実行可能な攻撃が存在する方式
- ✧ 安全性基準を脅かす攻撃が存在する方式

３．１．６．２．軽量暗号ガイドライン更新方針

下記の通り更新を行うことを決定した。

- ➢ 更新形態

  2016 年度版ガイドラインに新規情報を追加・更新した文書を 2023 年度版ガイドラインとして公開する。

  - ・ 主たる追加は、2016 年度版ガイドラインの 4 章「代表的な軽量暗号」に相当する軽量暗号方式の紹介とする。
  - ・ 既に 4 章に掲載されている方式については、今年度実施した軽量暗号に関する技術動向調査(３．１．６．１参照)を基に更新する。
  - ・ 1 章～3 章は、2016 年度版ガイドラインをそのまま用いる。ただし、4 章に新規追加・更新する方式に関わる情報は、適切な章に節を追加し、掲載する。
  - ・ 付録を追加し、関連情報を掲載する。
- ➢ タイトル
  - ・ 「CRYPTREC 暗号技術ガイドライン（軽量暗号)」2023 年度版
- ➢ 追加情報の対象
  - ・ NIST Lightweight コンペティション最終選考で採択された方式
  - ・ 軽量な方式として ISO に近年採録されたもしくは採録される予定の方式
- ➢ 主な追加内容
  - ・ 1 章　はじめに
    - ✓ 追記箇所を説明する文章を追加する。
  - ・ 2 章 軽量暗号とその活用法
    - ✓ 節を追加し、2017 年以降の標準化動向を掲載する。
  - ・ 3 章 軽量暗号の性能比較
    - ✓ 節を追加し、 ″追加情報の対象″ の方式に関する安全性や実装性能に関わる評価・調査結果（2022 年度外部評価により実施予定）を掲載する。
  - ・ 4 章 代表的な軽量暗号
    - ✓ 2016 年度版ガイドライン掲載暗号について、今年度実施した軽量暗号に関わる調査報告書（３．１．６．１参照)を基に追記・更新する。
    - ✓ ″追加情報の対象″の方式について、掲載方式と同等の情報を掲載する。(2022 年度外部評価の実施結果を反映する)
  - ・ 付録(新規)
    - ✓ NIST Lightweight コンペティションファイナリスト(最終選考で採択されなかった方式)
    - ✓ CAESAR のスケジュールが後ろ倒しにずれ込み、最終選考が完結する前に 2016 年度版ガイドラインを公開することとなった。後に、CAESAR プロジェクトの最

終選考により、3 ケース各 2 方式(計 6 方式) が選ばれた。Use case 1: Lightweight applications について選ばれた 2 方式はすでに掲載していたが、Use case 2: High-performance applications および Use case 3: Defense in depth については、2 方式中 1 方式は掲載しているが、各 1 方式は掲載していない。ここで、未掲載の 2 方式を紹介する。

- 編集方法
  - 事務局で取りまとめ・編集を行い、更新版を作成し、暗号技術評価委員会にて審議いただく。
- 今後のスケジュール
  - 2022年：
    NIST Lightweight コンペティションファイナリストを対象とした安全性および実装性能に関わる調査・評価
  - 2023年：

事務局によりガイドラインの更新案を編集し、ドラフト版について外部有識者にガイドラインとして、掲載内容の適切性や情報の過不足などについてレビュー頂き、完成版を暗号技術評価委員会にて審議する

３．１．７．暗号技術評価委員会の開催実績

2021年度、暗号技術評価委員会は計2回開催した。各回会合の概要は表3.2-5のとおりである。

表3.2-5　暗号技術評価委員会の開催状況

回	開催日	議案
第1回	2021年7月6日	■ 暗号技術評価委員会活動計画の具体的な進め方についての審議 ■ 外部評価（ディジタル署名EdDSAの実装性能に関する調査）実施についての審議 ■ 暗号技術調査ワーキンググループ（耐量子計算機暗号）の活動計画案の審議 ■ 暗号技術調査ワーキンググループ（高機能暗号）の活動計画案の審議 ■ 軽量暗号に関するガイドライン係る技術動向調査及び更新方針案の審議
第2回	2022月2月22日	■ 暗号技術評価委員会活動報告（案）についての審議 ■ ディジタル署名EdDSAの実装性能に関する調査結果の報告と暗号技術評価委員会としての見解について審議 ■ 暗号技術調査ワーキンググループ（耐量子計算機暗号）の活動内容の報告

		■ 暗号技術調査ワーキンググループ（高機能暗号）の活動内容の報告 ■ 軽量暗号ガイドラインに係る技術動向調査結果の報告及び更新方針の決定

３．２．暗号技術活用委員会

３．２．１．活動の概要

2021年度の活動概要は以下の通りである。詳細については、CRYPTREC Report 2021暗号技術活用委員会報告[7]を参照されたい。

(1) 利用実績に関する選定基準の検討

CRYPTREC暗号リストは、電子政府推奨暗号リスト、推奨候補暗号リスト、運用監視暗号リストの3つのリストで構成されている。2022年度にCRYPTREC暗号リストの改定が予定されており、その際、推奨候補暗号リストから電子政府推奨暗号リストへの昇格にあたって利用実績に基づいた選定が行われることが決まっている[8]。
そこで、昇格のための具体的な利用実績に関する選定基準案を検討・策定する。なお、策定した選定基準案は暗号技術検討会に報告され、改めて審議される。また、利用実績調査は2022年度上期にIPAにて実施する計画である。

(2) 「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準《(従来仮称）鍵長設定要件》」及び「暗号鍵設定ガイダンス《(従来仮称）鍵長設定ガイダンス（一般用)》」の作成

安全な暗号利用に係る運用ガイドラインとして、2020年度の検討結果を踏まえて取りまとめた作成方針に基づき、2つの鍵長に関するドキュメントを作成する。
一つは、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準《(従来仮称）鍵長設定要件》」である。これは、政府機関等のサイバーセキュリティ対策のための統一基準において適用対象となる情報システム（暗号化機能・電子署名機能の導入を行うものに限る。）の調達・開発にあたって、調達要件や開発要件として採用すべき暗号アルゴリズム及び鍵長を決定するためのガイドラインであり、CRYPTREC暗号リストの一要素を成すものである。
もう一つは、「暗号鍵設定ガイダンス《(従来仮称）鍵長設定ガイダンス（一般用)》」である。これは、利用用途を特定せず、鍵長の選択方法や暗号鍵の設定に関する一般的なガイダンスを提供する。調達要件や開発要件などを具体的に定めるものではなく、鍵長の選択方法や暗号鍵の設定などについて考え方や留意点を示すものである。

(3) 暗号鍵管理プロファイルの作成ガイダンスの作成

暗号鍵管理ガイドラインの拡充を目的とし、2020年度に公開した「暗号鍵管理システム設計指針（基本編)」の解説書となる「暗号鍵管理プロファイルの作成ガイダンス（仮称)」を作成する。
2020年度に取りまとめた作業の進め方に基づき、暗号鍵管理ガイダンスWGを設置して検討を行う。なお、ガイダンス文書の完成時期は2022年度を予定する。

---

[7] CRYPTREC Report 2021 暗号技術活用委員会報告, https://www.cryptrec.go.jp/promo_cmte.html
[8] CRYPTREC, 暗号技術検討会２０２０年度報告書, https://www.cryptrec.go.jp/adv_board.html

３．２．２．2021年度の活動内容

３．２．２．１．利用実績による選定基準（案）について

利用実績に基づく選定基準（選定ルール）は、2012年度に現在のCRYPTREC暗号リストの形に改定された際に初めて導入されたものである。

2021年度の活用委員会では2012年当時の選定基準をどのように見直すべきかの検討を行った結果、以下の理由により、選定基準（案）に電子政府推奨暗号リストへの昇格のための明確な選定基準・閾値は設けないとの結論に至った。また、今回作成した選定基準（案）は昇格の目安としてのものであり、実際の昇格判断は個々の状況を鑑みて個別に行うものとした。

- 暗号アルゴリズムの普及の仕方が、利用の前提・環境整備としての「標準化」を踏まえて**徐々に利用が広がっていく**以前の流れから、「有力ベンダが大規模採用」した影響を受けて**急速にその周辺に利用範囲が広がり**後から標準化につながっていく流れに変わってきていることに留意すべきである。
  - 5年ごとの「利用実績」調査では急激な利用実績の変動に対応できず、判断の遅れにつながる
  - 有力ベンダの採用状況などから近い将来主流になっていく可能性が高いと判断できるような暗号アルゴリズムであれば、早いうちから採用できる環境を整えるべき
  - 結果として、今後の電子政府推奨暗号リストへの昇格は、**「1）5年ごとの利用実績調査」に基づくケースよりも、「2）その他、普及していることが明らか又は急速な普及が大いに見込まれる」場合に随時昇格させるケースが主軸**になっていく可能性が高い
- 「2）その他、普及していることが明らか又は急速な普及が大いに見込まれる」場合に随時昇格させるケースを想定するならば、その際の普及状況として様々な場面が想定されるため、厳格な基準・閾値と定めたとしても適切な運用ができない可能性がある。
  - 昇格が適切と認められる状況であったとしても、定めた基準・閾値を満たさないという理由で昇格できないのでは本末転倒
  - 有力ベンダの今後の採用状況などの未来予測も加味して利用実績を判断すべき
- クローズドな利用（＝関係者外秘）での実績については、従来と同様、原則カウントしない。
  - ただし、電子政府システムや重要インフラ等、日本の基幹システムでの利用が確認された場合に限り、例外的に扱う
  - 利用実績がないことによる推奨候補暗号リストからの削除にあたっては、CRYPTREC暗号リストの主たる利用者である各府省庁に事前照会を行い、コメントを踏まえたうえで最終判断を行うものとする

【今回の選定基準（案）】

本選定基準は、暗号技術評価委員会で安全性及び実装性の評価を実施し、その評価結果により暗号技術検討会が推奨候補暗号リストに含めると決定した暗号技術に対して、電子政府推奨暗号リストへの昇格を決めるための基準である。昇格検討対象の暗号技術は、以下の考慮項目での目安に基づき、暗号技術活用委員会にて検討、選定し、暗号技術検討会に推薦する。

推薦された暗号技術について、暗号技術検討会では、その根拠となった利用実態を再度確認・審議を行い、電子政府推奨暗号リストへの昇格に問題がないと判断した場合に電子政府推奨暗号リストに選定する。

表3.2-1 利用実績による選定基準（案）

考慮項目		選定目安
採用実績	以下のいずれかを満たす場合、昇格の検討対象に含める。なお、採用実績は、 ● 5 年ごとに実施予定の大規模アンケート調査による「**利用実績調査**」 ● 必要に応じて、事務局が（大規模アンケート調査によらずに）情報収集する「**利用実態確認**」により確認するものとする。	
	① **利用実績調査**の結果、電子政府推奨暗号リストに掲載されている（同一カテゴリの）暗号技術の採用実績と遜色がないことが確認された場合	**電子政府推奨暗号リスト掲載の（同一カテゴリの）暗号技術の採用実績と同等以上の採用実績がある推奨候補暗号リスト掲載の暗号技術を昇格検討対象とする。**
	② **利用実績調査**又は**利用実態確認**の結果、**電子政府システムや重要インフラ等、日本の基幹システム**においてすでに利用されていることが確認された場合	**必要に応じて、利用実績調査に代わって、各府省庁等への照会を実施し、照会結果（クローズドな利用を含め）を基に昇格検討対象を選定する。**
	利用実績調査又は**利用実態確認**の結果、③～⑤のいずれかが確認された場合： ③ **利用者が多い主要な汎用製品群の複数**に搭載されるなど、明らかに採用が進展していると判断された場合 ④ **利用者が多い主要なオープンソースソフトウェアの複数**に搭載されるなど、明らかに採用が進展していると判断された場合 ⑤ **利用者が多い主要なサービスやプロトコルの複数**で利用されるなど、明らかに採用が進展していると判断された場合	**「複数」「利用者が多い（主要な）」というキーワードの両方を十分に満たし、明らかな採用促進が確認された場合には、必要に応じて、昇格検討対象とする。** **※「複数」の意味は、必要条件として「2 個以上が必要」ということであって、「2 個以上あればよい」という十分条件としての意味ではないことに留意**
標準化実績	以下を満たす場合、昇格の検討対象に含める。	
	⑥ **利用実績調査**の結果、電子政府推奨暗号リストに掲載されている（同一カテゴリの）暗号技術の採用実績と遜色がないことが確認された場合	**電子政府推奨暗号リスト掲載の（同一カテゴリの）暗号技術の採用実績と同等以上の採用実績がある推奨候補暗号リスト掲載の暗号技術は昇格検討**

		対象とする。

＜目安の理由＞

- ①は「利用実績調査」の結果に基づく基準として整備する。
  電子政府推奨暗号リストと推奨候補暗号リストの採用実績に著しい不整合が起きないようにするための指標とする。
- ②～⑤は「その他、普及していることが明らか又は急速な普及が大いに見込まれる」ケースに対応する基準として整備する。①の場合と異なり、必ずしも利用実績調査を実施するわけではなく、利用実態確認だけで採用実績を確認する場合もあるので、採用割合での判断は行わない。象徴的な利用形態での採用実績がどれだけ進んだかを主な指標とする。
  - ②については、CRYPTRECの設置目的からして明らかに管理する必要があることへの対応。また、クローズドな利用での実績であったとしても、CRYPTREC暗号リストの主たる利用者である各府省庁に事前照会を踏まえた判断根拠になり得る
  - ③～⑤については、「複数」「利用者が多い（主要）」というキーワードの両方を満たすことを例示しておくことで、「明らかな採用促進、又は急速な普及の可能性」の判断目安とすることを意図している。なお、実際に判断にあたっては、利用実態確認で収集した関連情報を基にした委員会での審議結果に基づく
- 標準化実績については、標準化が進んだだけでは採用実績に直ちに結びつくわけではなく、また標準化されるまでに時間がかかる。このため、利用実績に急激な変化が起こりにくいことを考慮し、「利用実績調査」の結果に基づく基準のみを整備する。
  - さらに、標準化が進んで急速に利用が進展した場合であっても、採用実績の③や④などで対処することが可能

３．２．２．２．「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の作成

2020年度活用委員会での議論を踏まえ、2021年度の活用委員会では表3.2-2の通りに作成方針を定め、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」を作成した。作成にあたっては、以下の論点について主に検討を行い、検討結果を設定基準に反映させた。

詳細は、暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準[9]を参照されたい。

表3.2-2 「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の作成方針

文書体系	CRYPTREC暗号リストの一要素を成すものとし、LSを附番
利用目的	政府機関等のサイバーセキュリティ対策のための統一基準において適用対象となる情報システム（暗号化機能・電子署名機能の導入を行うものに限る。）の調達又は開発にあたって、調達要件又は開発要件として採用すべき暗号アルゴリズム及び鍵長を決定する
想定読者	上記システムの調達又は開発に係る情報システムセキュリティ責任者・システム担当

[9] CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, https://www.cryptrec.go.jp/list.html

	者・調達担当者、など。（その他の利用者は、ボランタリベースと位置付ける）
備考	「CRYPTREC暗号リスト」と一体的に直接参照するものとし、「政府機関の情報セキュリティ対策のための統一基準」での利用を第一義とする
主な論点	● 「鍵長設定の要件」と「移行」に絞って記載してよいか ● 電子政府システムの運用期間として取り扱う範囲をどこまで想定するか ● ビットセキュリティの基準をどこまで区切るか ● 電子政府システムの運用寿命とセキュリティ強度要件の関係をどのように整理するか ● セキュリティ強度要件をどのように設定するか ● セキュリティ強度要件に付与するラベリング名を何にするか ● 情報の機微度、あるいはインパクトレベルによって要件に差をつけるか

設定基準の位置づけ

CRYPTREC暗号リストに掲載されている暗号技術を利用する際に、適切なセキュリティ強度を実現するためのアルゴリズム及び鍵長の選択方法を規定したものであり、CRYPTREC暗号リストとの関係を図3.2-1に示す。

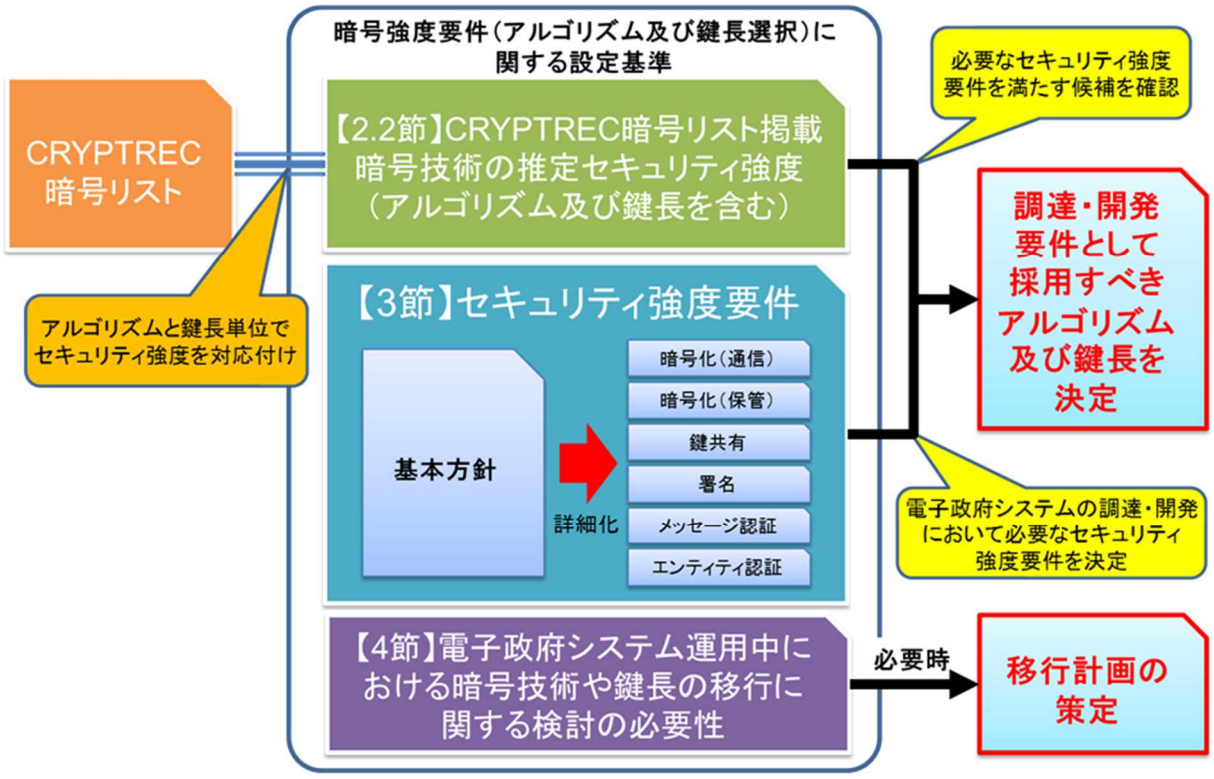


図3.2-1 「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の位置づけ

セキュリティ強度要件の基本設定方針概要

電子政府システムを調達又は開発する際は、そのシステムの運用寿命全体と、その期間に実現するセキュリティ強度の関係を考慮してセキュリティ強度要件を設定し、その強度要件を満たすアルゴリズムと鍵長の組合せを調達・開発要件としなければならない。

必要なセキュリティ強度要件は表3.2-3をベースとして、電子政府システムの想定運用終了・廃棄年又は利用期間の終了年を基準に設定する。例えば、電子政府システムの運用終了・廃棄年が2057年予定であれば「2051～2060」の列を参照し、192ビット以上のセキュリティ強度要件を設定する。

表3.2-3 セキュリティ強度要件の基本設定基準

<table>
<tr><th colspan="2">想定運用終了・廃棄年
／利用期間</th><th>2022～2030</th><th>2031～2040</th><th>2041～2050</th><th>2051～2060</th><th>2061～2070</th></tr>
<tr><td rowspan="2">112ビット
セキュリティ</td><td>新規生成*1)</td><td rowspan="2">移行完遂期間
*4)</td><td>利用不可</td><td rowspan="2">利用不可</td><td rowspan="2">利用不可</td><td rowspan="2">利用不可</td></tr>
<tr><td>処理*2)</td><td>許容*3)</td></tr>
<tr><td rowspan="2">128ビット
セキュリティ</td><td>新規生成*1)</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">移行完遂期間
*4)</td><td>利用不可</td><td rowspan="2">利用不可</td></tr>
<tr><td>処理*2)</td><td>許容*3)</td></tr>
<tr><td rowspan="2">192ビット
セキュリティ</td><td>新規生成*1)</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td></tr>
<tr><td>処理*2)</td></tr>
<tr><td rowspan="2">256ビット
セキュリティ</td><td>新規生成*1)</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td></tr>
<tr><td>処理*2)</td></tr>
</table>

*1) 新規に暗号処理を実行する場合（例：暗号化、署名生成）

*2) 処理済みのデータに対して処理を実行する場合（例：復号、署名検証）

*3) 処理済みのデータに対する正当性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合

*4) よりセキュリティ強度の高い暗号技術又は鍵長への移行を完遂させなければならない期間。利用する暗号処理が短期間で完結する場合（例：エンティティ認証）、又は既存の電子政府システムの継続利用やそれらとの互換性・相互接続性維持のための利用に限定

なお、本設定基準では量子コンピュータによる暗号技術の危殆化は将来的なリスク要因として位置づけ、推定セキュリティ強度の評価に量子コンピュータの影響は考慮していない。また、将来的なアルゴリズム及び鍵長の選択要件においてもその影響を考慮しないものとしている。

アルゴリズム及び鍵長の選択・実装要件及び利用要件の基本方針

- 設定されたセキュリティ強度要件と同じかそれ以上のセキュリティ強度を満たすアルゴリズム及び鍵長の組合せを推定セキュリティ強度の表から選択してサポート（実装）しなければならない。
- 設定したセキュリティ強度要件以下の安全性のアルゴリズム及び鍵長をサポート（実装）すること自体は妨げない。ただし、サポート（実装）されたアルゴリズム及び鍵長のすべてが常に利用されてよいわけではなく、その利用期間については、そのセキュリティ強度に応じて、セキュリティ強度要件に従って定めなければならない。
- データのセキュリティ寿命は利用するアルゴリズムのセキュリティ寿命に包含されなければならない。

CRYPTREC暗号リスト上の暗号技術とセキュリティ強度との対応

本設定基準の中では、2021年末時点でのCRYPTREC暗号リストに記載の暗号アルゴリズムごとの安全性評価の現状等を踏まえた推定セキュリティ強度を示している。これらは、今後、暗号解読手法の進展や大規模量子コンピュータの実現等により、推定セキュリティ強度が見直される可能性がある（少なくとも5年ごとに再確認される）。

運用中における暗号技術及び鍵長移行に関する検討の必要性

外部要因により、利用しているアルゴリズムや鍵長の移行に関する検討を行う必要が出てくるケースとして、以下のようなものがある。これらに該当する事象が発生した場合には、直ちに内容の確認を行い、必要に応じて移行計画を策定しなければならない。本設定基準では、これらに応じて移行計画を策定する際に考慮しなければならないポイントを示している。

- 電子政府システムの運用寿命の延長に伴う対応
- セキュリティ強度要件の設定変更に伴う対応
- 暗号技術の推定セキュリティ強度の変更に伴う対応
- 運用監視暗号リストに掲載されたアルゴリズムの継続利用にあたっての対応
- 突発的な理由に伴う緊急移行にあたっての対応
- 量子コンピュータの実現リスクへの対応

３．２．２．３．「暗号鍵設定ガイダンス」の作成

2020年度活用委員会での議論を踏まえ、2021年度の活用委員会では表3.2-4の通りに作成方針を定め、「暗号鍵設定ガイダンス」を作成した。作成にあたっては、以下の論点について主に検討を行い、検討結果を設定基準に反映させた。

詳細は、暗号鍵設定ガイダンス[10]を参照されたい。

表3.2-4 「暗号鍵設定ガイダンス」の作成方針

文書体系	運用ガイドラインの一つと位置付け。GLを附番
利用目的	暗号技術に用いられる暗号鍵に対して適切に鍵長を設定し、さらに適切に鍵管理を行って安全に運用していくための技術的ガイダンスを提供する
想定読者	暗号技術を組込んだシステム又はアプリケーションの設計・開発・運用・提供にあたって、安全な暗号技術の選定、及び暗号技術の安全な運用方針・対策の作成や決定などに携わる管理者、設計者、開発者など
備考	SP800-57 Part 1に記載がある「アルゴリズムや鍵長の設定以外の鍵管理に関する事項（保護手段など）」は「暗号鍵管理ガイダンス」に分ける
主な論点	● 「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」との位置づけの違いの明確化 ● ビットセキュリティの基準をどこまで区切るか ● システムやアプリケーションの運用寿命とセキュリティ強度要件の関係をどのように整理するか ● 求められるセキュリティ強度要件の考え方 ● 「暗号鍵のライフサイクル」「暗号鍵の（タイプごとの）利用期間」「鍵の保護」についての記載内容 ● 移行に関する検討の必要性についての記載内容

本書では、まず安全な暗号技術の導入の観点から、暗号技術を利用する際の鍵長の選択方法に関する一般的な考え方を解説する。また、暗号技術の安全な運用の観点から、適切に暗号鍵の管理を行うために必要となる項目についての技術的概要を示す。具体的には、暗号鍵を安全に設定し、運用していくために考慮すべき項目として以下の項目を解説している。

- 暗号鍵の鍵長
- 暗号鍵の鍵タイプ
- 暗号鍵のライフサイクル
- 運用中における鍵長移行に関する検討の必要性

なお、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」との最大の違いは求められるセキュリティ強度要件の考え方が違うことである。「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」では電子政府システムにおいて十分なセキュリティ強度を持たせるために必要な要件として予め規定しているのに対して、本ガイダンスでは実際の利用用途や利用期間、環

[10] CRYPTREC, 暗号鍵設定ガイダンス, https://www.cryptrec.go.jp/op_guidelines.html

境、コスト、その他様々な制約条件を踏まえて、読者が必要なセキュリティ強度を決めるように勧めている。

３．２．２．４．暗号鍵管理の参照プロファイルの作成に向けた検討結果について

情報を安全に取り扱うためには、通信情報や保管情報の暗号化に使う暗号アルゴリズムのみに注意を払うだけでは不十分であり、その暗号アルゴリズムに用いられる暗号鍵の管理が適切に行われる必要がある。そこで、2020年度に鍵管理のフレームワークとなる「暗号鍵管理システム設計指針（基本編）」を公開したことに引き続き、暗号鍵管理ガイドラインの拡充を目的として暗号鍵管理ガイダンスを作成するため、暗号鍵管理ガイダンスWGを設置した。

2021年度は、実際のガイダンス作成の進め方についての検討を行い、ガイダンス作成に向けた執筆方針の方向性を取りまとめることに注力した。なお、暗号鍵管理ガイダンスの位置づけと想定読者は以下の通りとする。

位置づけ

- 暗号鍵管理プロファイルを作成するためのガイダンスを作成する。ただし、特定の業界において使用する参照可能なプロファイルは含まれない点については注意されたい。
- 暗号鍵管理で必要となる項目について、シンプルなモデルを例示し説明する。
- シンプルなモデルを用いた説明においては、鍵管理における要求や思想が理解できるような記載を行う。
- 暗号鍵管理における特に注意すべきリスクや、発生しうる失敗例を説明する。

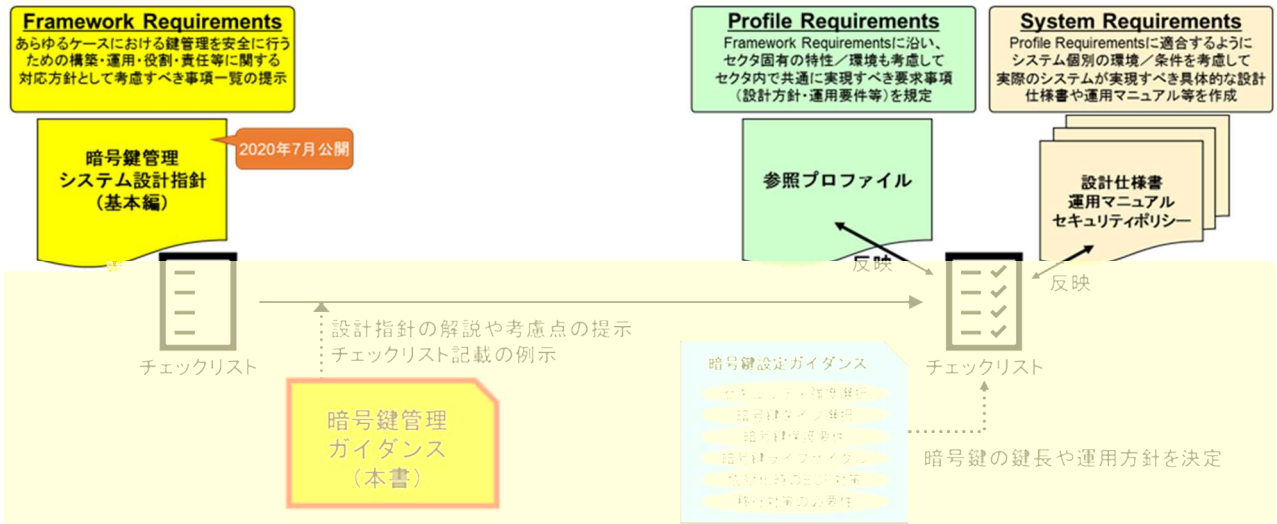


図3.2-2 「暗号鍵管理ガイダンス」作成の位置づけ

想定読者

- 暗号鍵管理機能を持つシステム設計者
- 各業界において、暗号鍵管理の参照プロファイルを作成する担当者

- 一部の内容については、暗号鍵管理プロファイルの利用者、暗号鍵管理機能を持つシステム調達者等

【ガイダンス内容のイメージ】

本ガイダンスでは、要求内容については基本的に暗号鍵管理システム設計指針（基本編）のFrame Requirementsの内容をそのまま転記し、「ガイダンスで記載する説明事項」と「チェックリストの記載例」を中心に説明を加筆する。

表3.2-4 「暗号鍵管理ガイダンス」の執筆内容

各節のフォーマット		
検討番号	*.**	ー
要求内容	暗号鍵管理システム設計指針（基本編）の説明やFrame Requirementsの内容を基本的に引用	● 目的・趣旨 ● 要求事項 ● 記載内容
ガイダンスで記載する説明事項	**1. 要求に対する判断理由に関する考え方を記載 2. 必要に応じて、要求に関する補足説明を記載**	**● 解説・考慮点**
チェックリスト [redacted]	**トイモデルを利用した判断理由の記載内容を例示**	**● トイモデルとチェックリストの記載例**

【ガイダンス作成の進め方】 e 口

暗号鍵管理システム設計指針（基本編）の要件（チェックリスト）の解説にあたって、参考例として「トイモデル」を使う。

- 暗号鍵管理システム設計指針（基本編）での6つの目的別分類ごとに、理解しやすいトイモデルを用意
- トイモデルを使ったガイダンスの中でCBPに該当する部分を参考
- 「ユースケースを例 ま

		● 利用実績による選定基準について ● 鍵長設定要件（仮称）について ● 鍵長設定ガイダンス（一般用）（仮称）について
第二回	2021年12月13日	● 利用実績による選定基準案について ● 鍵長設定要件（仮称）について ● 鍵長設定ガイダンス（一般用）（仮称）について
第三回	2022年3月1日	● メール審議結果及び暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準について ● 暗号鍵設定ガイダンス（仮称）について ● 利用実績による選定基準（案）について ● 暗号鍵管理ガイダンス WG 活動報告 ● 2021 年度暗号技術活用委員会活動報告案について

４．今後のCRYPTRECの活動について

CRYPTRECでは、暗号アルゴリズムの安全性確保やその利活用に係る議論のみならず、鍵管理の安全な運用に向けた取組など、暗号をとりまく環境変化に応じた新たなニーズへの対応などに取り組むこととしている。2022年度にはCRYPTREC暗号リストの10年に一度の大規模改定を予定しており、その改定に向けた検討を進めていく。

暗号技術評価委員会においては、CRYPTREC暗号リストの大規模改定に向け、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、引き続き、耐量子計算機暗号、軽量暗号及び高機能暗号に関するガイドラインの作成に向けた検討を行う。暗号技術活用委員会においては、CRYPTREC暗号リストの大規模改定に向け、IPAと協力して暗号利用実績調査を実施し、策定された選定基準に照らし合わせた実績評価を行う。また、暗号鍵管理ガイダンスWGにて検討中の暗号鍵管理ガイダンスを完成させる予定である。

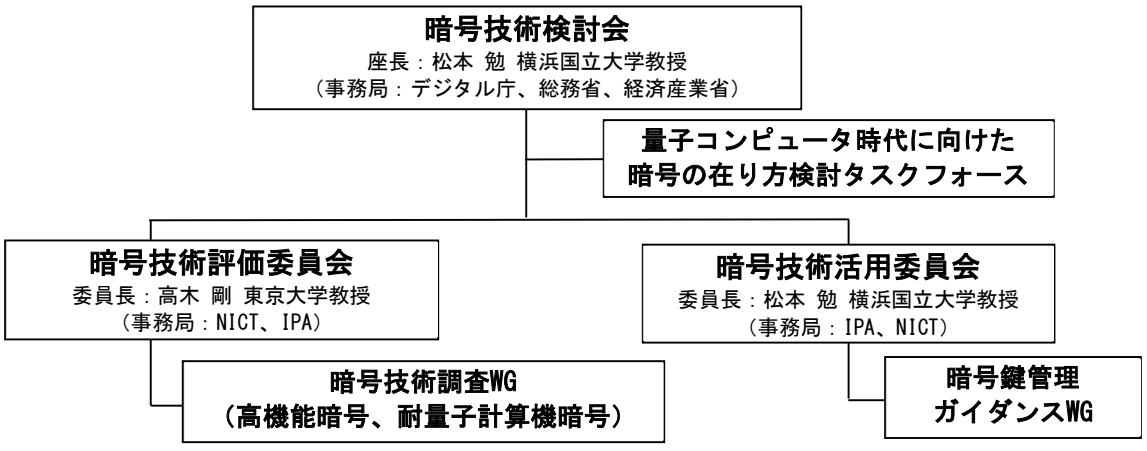


図4-1 2022年度CRYPTRECの体制図（予定）