CRYPTREC LS-0003-2022r1

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. 1.0）

デジタル庁

総務省

経済産業省

目次

【修正履歴】

修正日	修正内容
2022.07.01	初版発行
2023.03.30	発行月の誤り訂正 CRYPTREC 暗号リストのリンク先を修正

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、**利用する鍵長について、本書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。

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.html

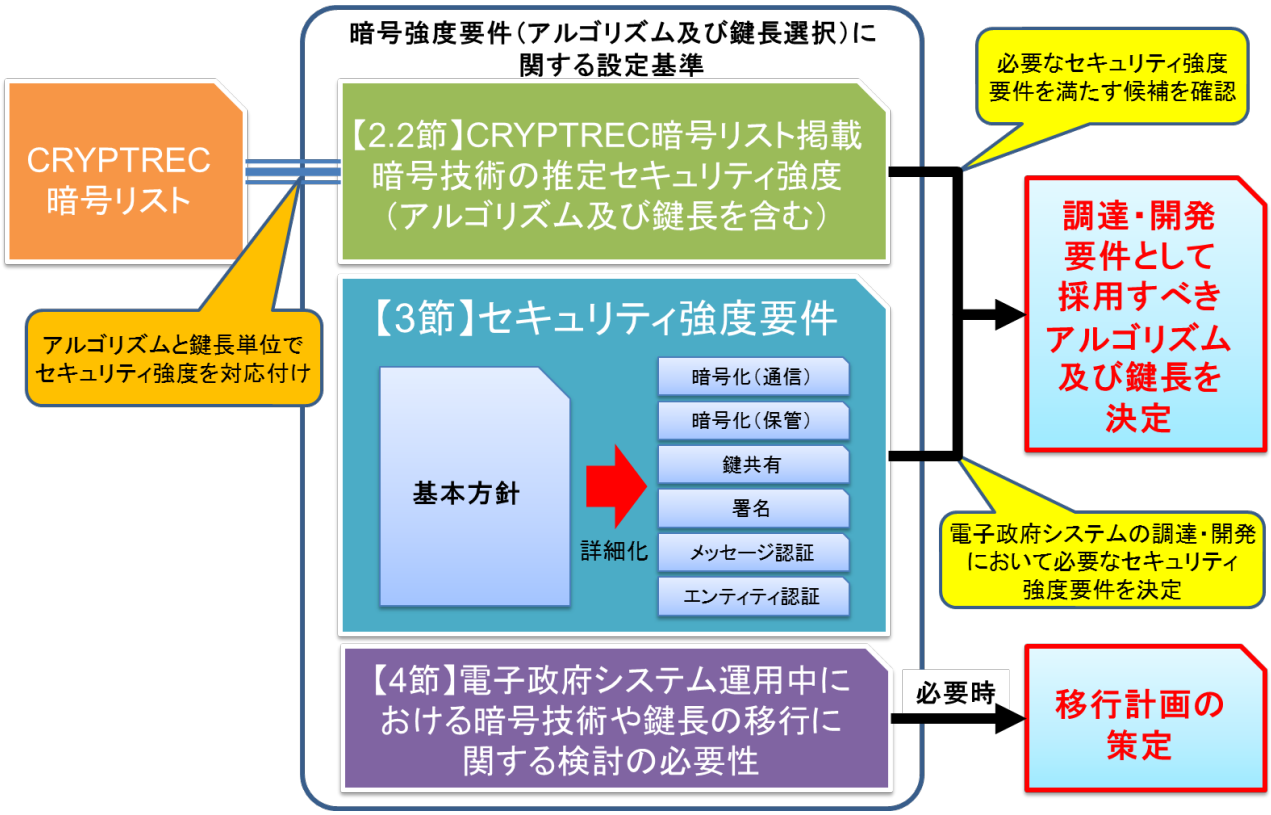

図 1　CRYPTREC 暗号リストと本書の関係

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** [2]**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　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/pdf/policy/general/kijyunr3.pdf

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（2022 年 6 月）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 6 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

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。

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[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）。

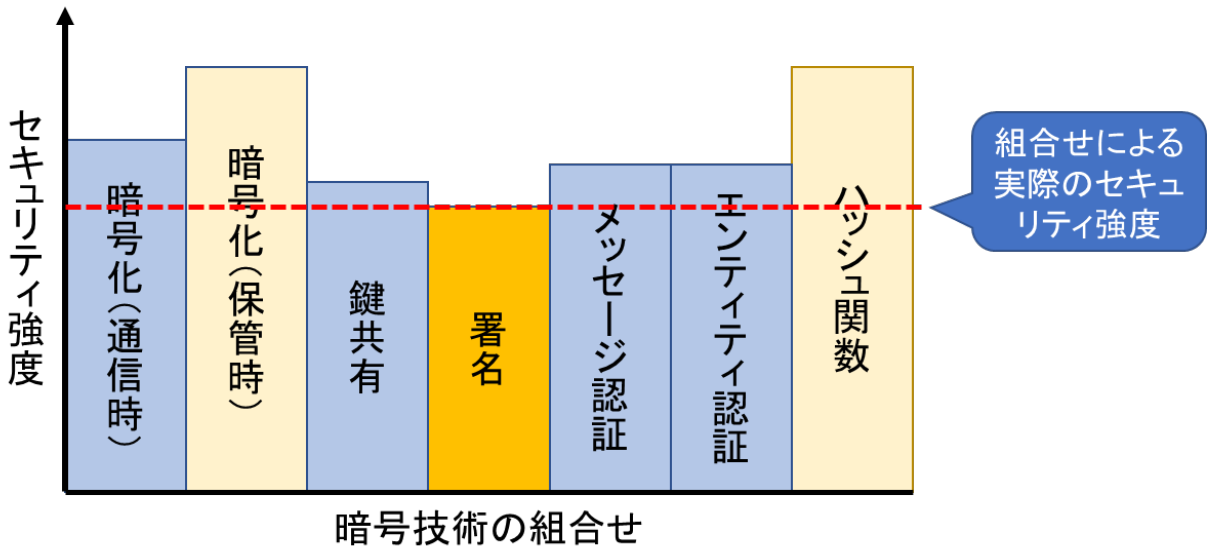

図 2　暗号技術の組合せによるセキュリティ強度（イメージ図）

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。

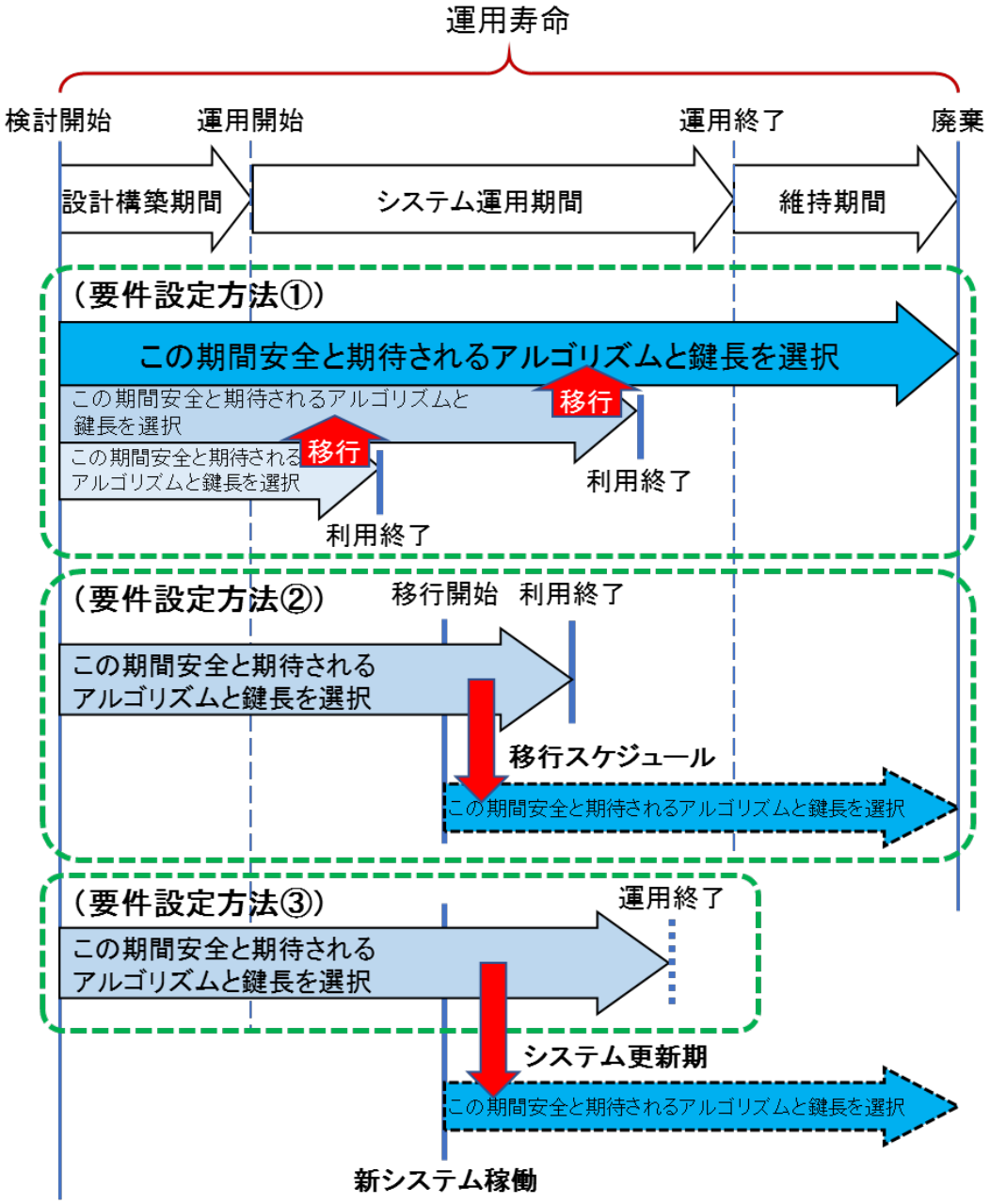

図 3　システムの運用寿命と求められるセキュリティ強度要件

【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。

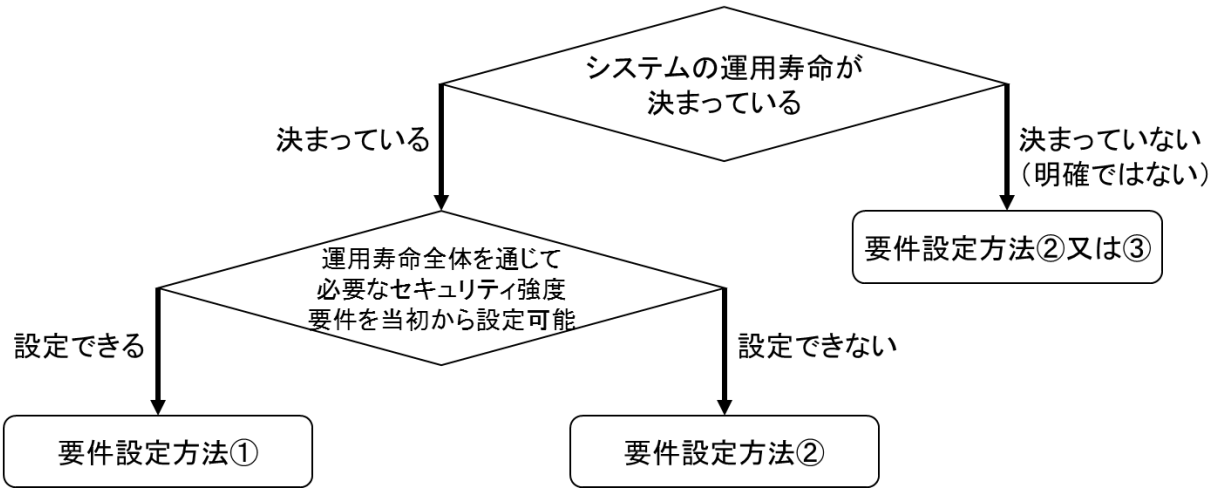

図 4　要件設定方法の選択フロー

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

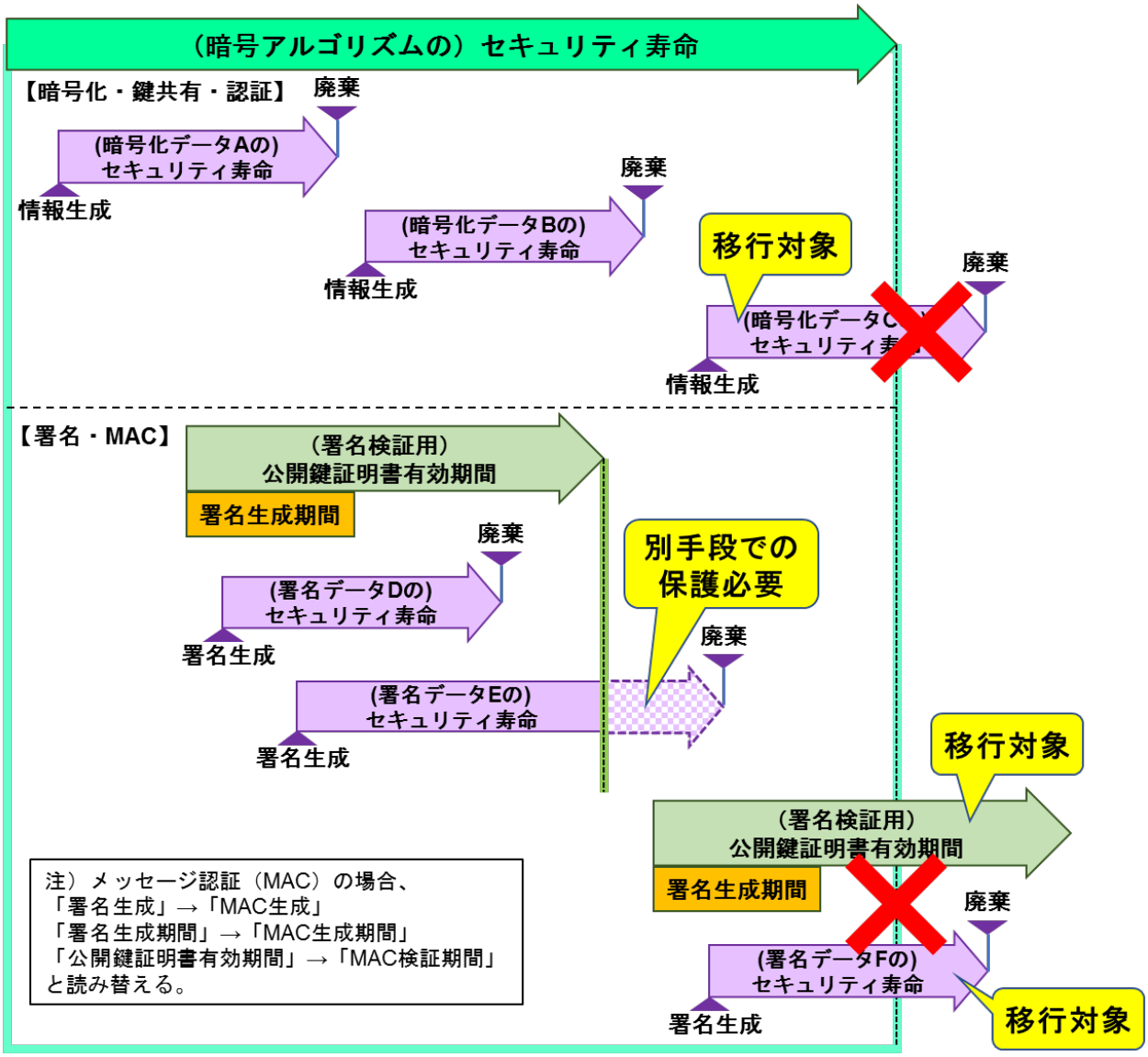

図 5　アルゴリズムのセキュリティ寿命とデータのセキュリティ寿命の関係

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**。

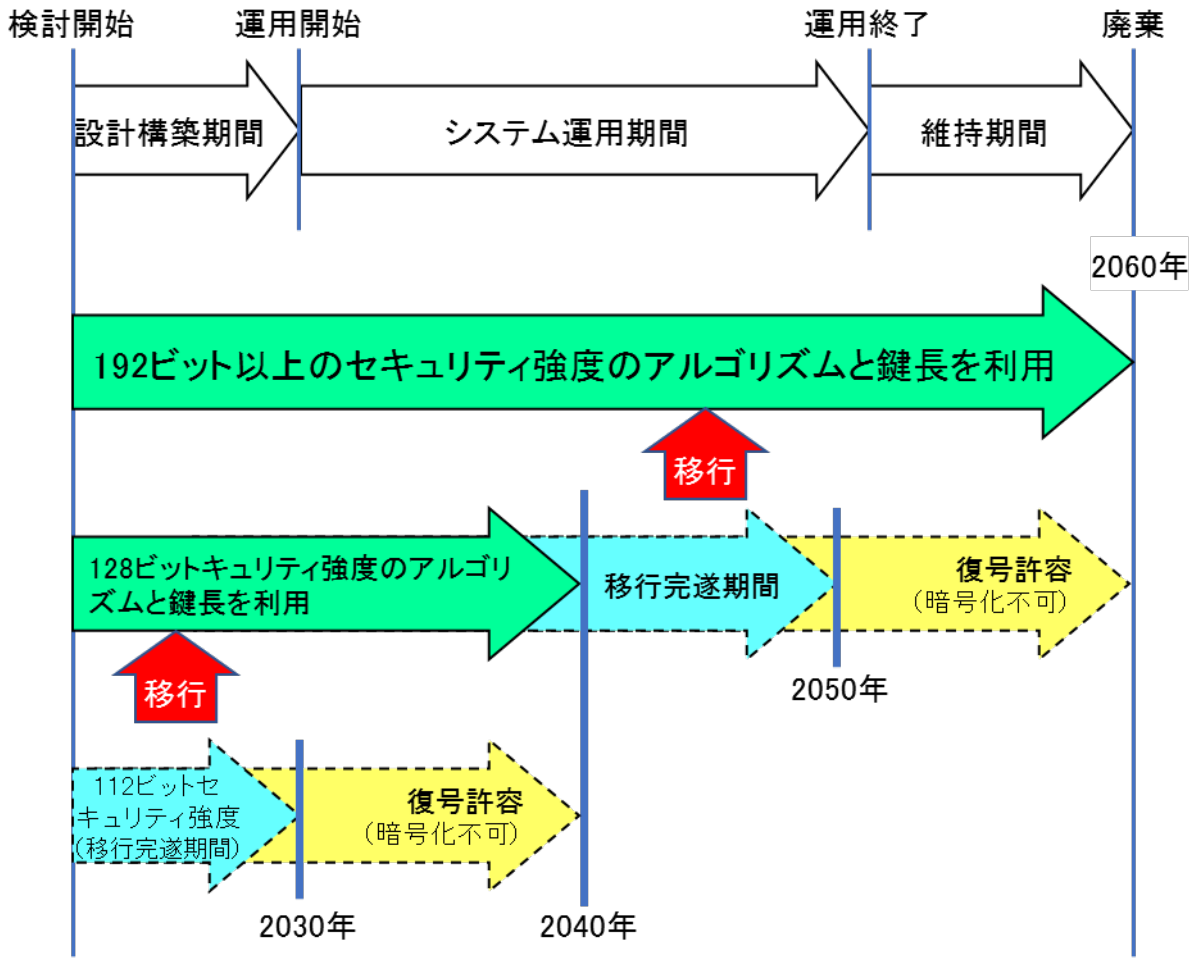

図 6　保管時の暗号化の例

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 [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] CRYPTREC、暗号鍵設定ガイダンス、https://www.cryptrec.go.jp/report/cryptrec-gl-3003-1.0.pdf

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/iaarchive/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 2021

https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2021.pdf

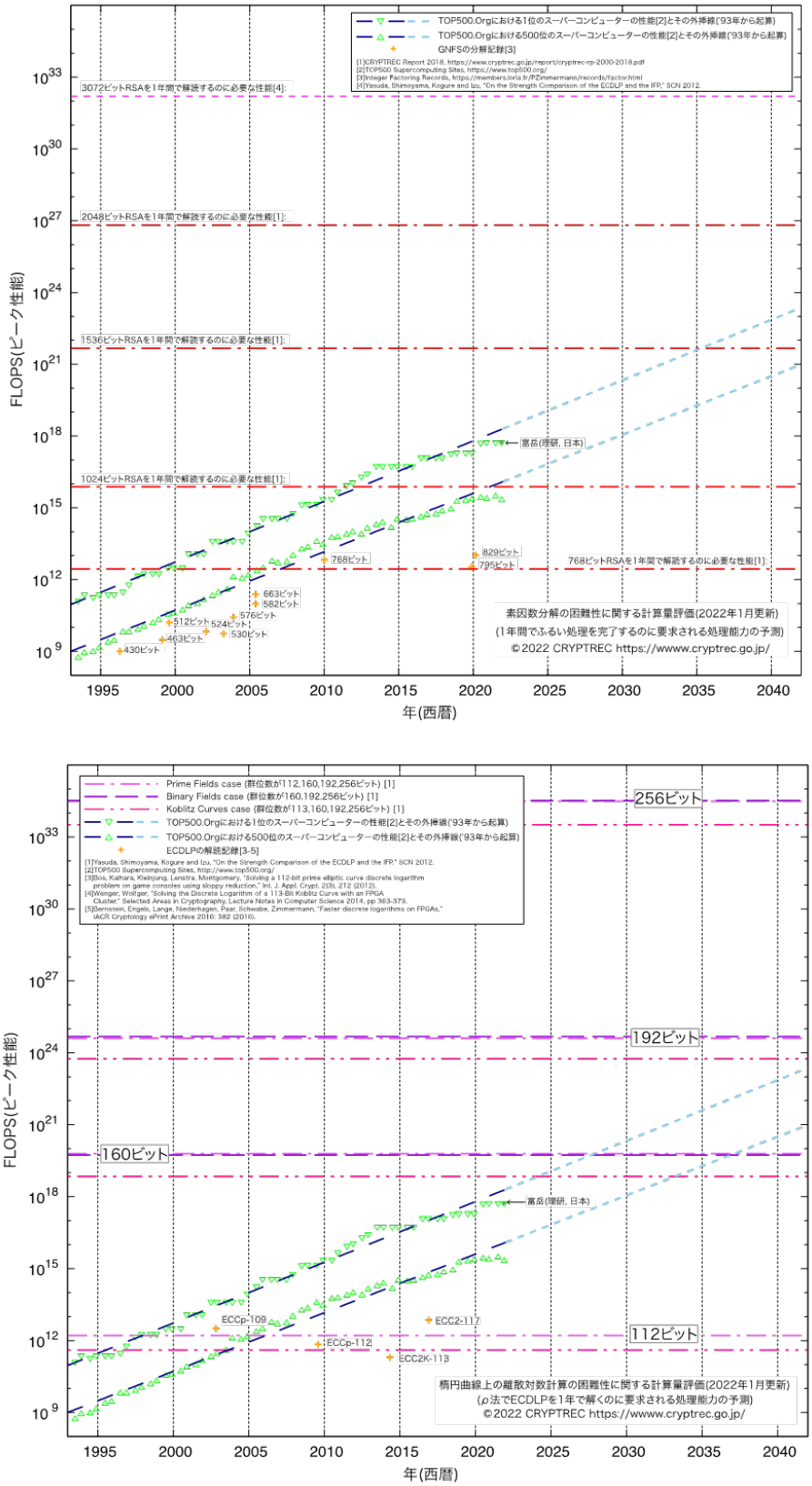

図 7　1 年で解読するのに必要な性能が達成できると見込まれる時期（図 3.2-1、図 3.2-2）