

目 次

	ページ
0 序文.....	1
0.1 一般.....	1
0.2 暗号モジュールのセキュリティ.....	1
1 適用範囲.....	2
2 引用規格.....	2
3 用語及び定義.....	2
4 略語.....	10
5 暗号モジュールのセキュリティレベル.....	11
5.1 セキュリティレベル 1.....	11
5.2 セキュリティレベル 2.....	11
5.3 セキュリティレベル 3.....	12
5.4 セキュリティレベル 4.....	12
6 機能的セキュリティ目標.....	13
7 セキュリティ要求事項.....	13
7.1 暗号モジュールの仕様.....	15
7.2 暗号モジュールのポート及びインタフェース.....	16
7.3 役割, サービス及び認証.....	17
7.4 有限状態モデル.....	20
7.5 物理的セキュリティ.....	21
7.6 動作環境.....	27
7.7 暗号鍵管理.....	30
7.8 自己テスト.....	33
7.9 設計保証.....	35
7.10 その他の攻撃への対処.....	38
附属書 A (規定) 文書化要求事項.....	39
附属書 B (規定) 暗号モジュールのセキュリティポリシ.....	43
附属書 C (規定) 承認されたプロテクションプロファイル.....	45
附属書 D (参考) 承認されたセキュリティ機能.....	46
附属書 E (参考) 承認された鍵確立方法.....	48
附属書 F (参考) 推奨ソフトウェア開発要領.....	49
附属書 G (参考) その他の攻撃への対処の例.....	51

まえがき

この規格は、工業標準化法に基づき、日本工業標準調査会の審議を経て、経済産業大臣が制定した日本工業規格である。

この規格は、著作権法で保護対象となっている著作物である。

この規格の一部が、技術的性質をもつ特許権、出願公開後の特許出願、実用新案権、又は出願公開後の実用新案登録出願に抵触する可能性があることに注意を喚起する。経済産業大臣及び日本工業標準調査会は、このような技術的性質をもつ特許権、出願公開後の特許出願、実用新案権、又は出願公開後の実用新案登録出願にかかわる確認について、責任をもたない。

セキュリティ技術—暗号モジュールのセキュリティ 要求事項

Information technology — Security techniques — Security requirements for cryptographic modules

0 序文

0.1 一般

この規格は、2006 年に第 1 版として発行された ISO/IEC 19790:2006, Information technology—Security techniques—Security requirements for cryptographic modules を基に、技術的内容及び対応国際規格の構成を変更することなく作成した日本工業規格である。

0.2 暗号モジュールのセキュリティ

情報技術分野において、エンティティ認証のため及び否認防止のために、また、認可されていない開示又は操作からのデータ保護の仕組みとして、暗号メカニズムを利用する必要性は益々高くなってきている。このメカニズムのセキュリティ及び信頼性は、そこに実装されている暗号モジュールに依存している。

この規格は、内容が段階的に深まる四つのレベルのセキュリティ要求事項を規定しているが、これは、様々なものが考えられる応用業務及び環境に広く対応できるように考慮したからである。このセキュリティ要求事項は、暗号モジュールの設計及び実装に関係した分野を取り上げている。

その分野には、次のものがある。

- ・暗号モジュールの仕様
- ・暗号モジュールのポート及びインタフェース
- ・役割、サービス及び認証
- ・有限状態モデル
- ・物理的セキュリティ
- ・動作環境
- ・暗号鍵管理
- ・自己テスト
- ・設計保証
- ・その他の攻撃への対処

暗号モジュールの全体的なセキュリティレベルは、暗号モジュールを利用する応用業務及び環境からのセキュリティ要求事項、並びに暗号モジュールの提供するセキュリティサービスに応じた適切なレベルになるように選ぶ必要がある。それぞれの組織の責任者は、暗号モジュールを利用するコンピュータシステム及び通信システムが、所与の応用業務及び環境からみて受容し得るセキュリティレベルを提供することを確実にすることが望ましい。それぞれの組織の責任者は、承認されたセキュリティ機能のどれが所与の

応用業務に対して適切であるか選択することに責任があるのであり、この規格に適合していることが、適合製品の完全な相互運用性及び相互受容可能性のいずれをも意味しない。セキュリティ意識の重要性、及び情報セキュリティを経営の優先課題とすることの重要性を、関係するすべての人々に周知させることが望ましい。

情報セキュリティに対する要求事項は、応用業務が異なれば違ったものになる。組織は、組織の情報資産を識別し、適切な管理策を実施することによって、その損失の可能性及び損失による影響を判断することが望ましい。管理策には次のようなものがあるが、これに限らない。

- a) 物理的・環境的管理策
- b) ソフトウェアの開発策
- c) バックアップ計画及び緊急時対応計画
- d) 情報及びデータについての管理策

これらの管理策は、運用環境内で、適切なセキュリティポリシー及び手順による運営が効果的に行われているときに効果的となる。

1 適用範囲

この規格は、コンピュータの中の取扱いに慎重さを要する情報を保護するセキュリティシステム及び通信システムの中で使用される暗号モジュールに対するセキュリティ要求事項を規定する。この規格は、データの重要度の幅広さ（例えば、低価値の管理データ、一億円規模の資金振替、生命にかかわるデータ）及び使用環境の多様性（例えば、保護された設備、オフィス、全く保護されていない場所）に応じて暗号モジュールを提供するために、四つのセキュリティレベルを定義している。10種の要件分野のそれぞれに対して四つのセキュリティレベルの内容を規定する。各セキュリティレベルは、下位のレベルにセキュリティを上乗せする形で提供されている。

この規格で規定されているセキュリティ要求事項は、暗号モジュールによって提供されるセキュリティの確保を目的とするが、この規格に適合していることだけでは、ある暗号モジュールがセキュアであることは保証されないし、保護しようとする情報の所有者にとって、その暗号モジュールが提供するセキュリティが十分かつ満足できることも保証されない。

注記 この規格の対応国際規格及びその対応の程度を表す記号を、次に示す。

ISO/IEC 19790:2006, Information technology — Security techniques — Security requirements for cryptographic modules (IDT)

なお、対応の程度を表す記号 (IDT)は、**ISO/IEC Guide 21** に基づき、一致していることを示す。

2 引用規格

次に掲げる規格は、この規格に引用されることによって、この規格の規定の一部を構成する。これらの引用規格は、その最新版（追補を含む。）を適用する。

ISO/IEC 15408 (all parts) Information technology — Security techniques — Evaluation criteria for IT security

ISO/IEC 18031 Information technology — Security techniques — Random bit generation

3 用語及び定義

この規格で用いる主な用語及び定義は、次による。

3.1

承認機関 (approval authority)

セキュリティ機能を承認、及び／又は評価する国内又は国際の組織・機関。

3.2

承認 (approved)

ISO/IEC 承認又は承認機関による承認。

3.3

承認された動作モード (approved mode of operation)

承認されたセキュリティ機能だけを採用した暗号モジュールの動作形態。

注記 Cipher Block Chaining (CBC)モードのような、特定のセキュリティ機能の動作モードとは異なる。

3.4

承認されたオペレーティングシステム (approved operating system)

承認機関によって評価され承認されたオペレーティングシステム。

3.5

承認されたプロテクションプロファイル (approved protection profile)

承認機関によって承認されたプロテクションプロファイル。

3.6

ISO/IEC 承認 (ISO/IEC approved)

次のいずれかのセキュリティ機能。

- ・ ISO/IEC 規格の中で規定されているもの。
- ・ ISO/IEC 規格の中で採用・推奨されており、その ISO/IEC 規格の附属書又は ISO/IEC 規格が参照している文書に規定されているもの。

3.7

非対称鍵暗号技術 (asymmetric cryptographic technique)

二つの関連する変換[公開変換(公開鍵によって定義される。)及びプライベート変換(プライベート鍵によって定義される。)]を使う暗号技術であって、公開変換が与えられたとしても、与えられた限られた時間及び計算能力内でプライベート変換を導出するのが計算的に不可能な特性をもつもの。

3.8

認証符号 (authentication code)

承認されたセキュリティ機能に基づく暗号チェックサム。

注記 メッセージ認証符号 (MAC) としても良く知られている。

3.9

証明書 (certificate)

認証局のプライベート鍵又は秘密鍵で、偽造できないようにされたエンティティのデータ。

3.10

危たい(殆)化 (compromise)

CSP が認可なく開示、変更、置換、若しくは使用されること、又は PSP が認可なく変更、若しくは置換されること。

3.11

機密性 (confidentiality)

重要な情報が、認可されていないエンティティに利用又は公開されない特性。

3.12

制御情報 (control information)

暗号モジュールの動作を指示するために暗号モジュールに入力される情報。

3.13

クリティカルセキュリティパラメタ, CSP (critical security parameter, CSP)

秘密又はプライベートセキュリティに関する情報であって、その開示又は変更が、暗号モジュールのセキュリティを危たい（殆）化し得るもの。

例 秘密鍵、プライベート鍵、認証データ（例えば、パスワード、PIN）

3.14

暗号境界 (cryptographic boundary)

暗号モジュールの物理的及び／又は論理的な領域を確立し、かつ、暗号モジュールのすべてのハードウェア、ソフトウェア、及び／又はファームウェアの構成要素をその内側に含む、明確に定義された連続する境界線。

3.15

暗号鍵, 鍵 (cryptographic key, key)

暗号変換の操作を制御する一連の記号。

注記 暗号変換は、暗号化、復号、ハッシュ値生成、署名生成、又は署名検証を含むが、これに限定しない。

3.16

暗号鍵要素, 鍵要素 (cryptographic key component, key component)

暗号機能を実行するために、セキュリティ機能において使用されるパラメタ。

3.17

暗号モジュール, モジュール (cryptographic module, module)

セキュリティ機能を実装した、暗号境界内のハードウェア、ソフトウェア、及び／又はファームウェアの集合。

3.18

暗号モジュールのセキュリティポリシ, セキュリティポリシ (cryptographic module security policy, security policy)

暗号モジュールが動作するうえでのセキュリティルールの明確な仕様。これには、この規格の要求事項から導出されたルール及びモジュールによって課せられた付加的ルールも含まれる。

注記 附属書 B を参照。

3.19

クリプトオフィサ (crypto officer)

暗号モジュールが機能するように、暗号関連の初期化又は管理機能を実行する個人又はその個人のために働くプロセス（すなわち、サブジェクト）によって担われる役割。

3.20

データパス (data path)

データが通過する物理的又は論理的な経路。

注記 物理的データパスは、複数の論理的データパスによって共有されてもよい。

3.21**差分電力解析, DPA (differential power analysis, DPA)**

暗号操作に関連した情報を抽出するための、暗号モジュールの消費電力変動の解析手法の一つで、統計処理に基づく差分解析によって当該情報を推定するもの。

3.22**デジタル署名 (digital signature)**

データユニットの受信者が、データユニットの出所及び完全性の証明、並びに（例えば、受信者による）偽造防止を可能にする、データ列に付加された又は暗号化変換されたデータ。

3.23**電子的鍵入力 (electronic key entry)**

鍵ローダ又はオンラインのような電子的手法を用いた、暗号モジュールへの暗号鍵入力。

注記 鍵のオペレータは入力しようとする鍵の値について知らなくてもよい。

3.24**電子的鍵配送 (electronic key transport)**

暗号鍵の移動であって、通常、暗号化された形で、コンピュータネットワークのような電子的手法を用いるもの。

3.25**暗号化された鍵 (encrypted key)**

承認されたセキュリティ機能を用いて、鍵を暗号化するための鍵で暗号化された暗号鍵。

3.26**エンティティ (entity)**

人、グループ、デバイス又はプロセス。

3.27**環境故障保護, EFP (environmental failure protection, EFP)**

暗号モジュールの正規の動作範囲外の環境条件又は環境変動によって、暗号モジュールのセキュリティが危たい（殆）化することを防止する特性を使用すること。

3.28**環境故障試験, EFT (environmental failure testing, EFT)**

暗号モジュールの正規の動作範囲外の環境条件又は環境変動によっても、暗号モジュールのセキュリティが危たい（殆）化しないという合理的保証を得るために特定の方法を使用すること。

3.29**誤り検出符号, EDC (error detection code, EDC)**

データから計算され、冗長ビットで表現される値で、データの意図しない改変を検出するためのもの。データの訂正は行わない。

3.30**有限状態モデル, FSM (finite state model, FSM)**

入力イベントの有限集合、出力イベントの有限集合、状態の有限集合、状態及び入力を出力に写像する関数、状態及び入力を状態に写像する関数（状態遷移関数）、並びに初期状態について記述する仕様からなる、シーケンシャルマシンの数学的モデル。

3.31

ファームウェア (firmware)

暗号境界内のハードウェアに保存され、実行している間は動的な書込みも変更もできない暗号モジュールのプログラム及びデータ構成要素。

例 ファームウェアの保存用ハードウェアには ROM, PROM, EPROM, EEPROM 又はフラッシュメモリを含むがそれに限定しない。

3.32**ハードウェア (hardware)**

プログラム及びデータを処理するために使用される、暗号境界内の物理的な装置・コンポーネント。

3.33**入力データ (input data)**

暗号モジュールに入力され、承認されたセキュリティ機能を用いて変換又は計算を行うために使用される情報。

3.34**完全性 (integrity)**

取扱いに慎重さを要するデータが、権限がなくかつ検出されない方法で、変更も消去もされなかったという特性。

3.35**インタフェース (interface)**

論理的な情報フローに対して暗号モジュールへのアクセスを提供する、暗号モジュールの論理的な入出力点。

3.36**鍵を暗号化するための鍵, KEK (key encrypting key, KEK)**

他の鍵を暗号化又は復号するために用いられる暗号鍵。

3.37**鍵確立 (key establishment)**

一つ以上のエンティティに共有された秘密鍵を利用可能にするプロセス。

注記 鍵確立は、鍵共有及び鍵配送を含む。

3.38**鍵ローダ (key loader)**

平文のまま又は暗号化された、暗号鍵又は鍵要素の少なくとも一つを格納できる独立のデバイスであって、要求があったときは、それらを暗号モジュール内に転送できるもの。

3.39**鍵管理 (key management)**

セキュリティポリシーに従った鍵及び鍵関連情報の生成、登録、証明、登録抹消、配送、インストール、保存、保管、廃止、導出及び破壊の管理及び使用。

3.40**鍵配送 (key transport)**

あるエンティティから他のエンティティへ鍵を配送するプロセス。

3.41**メンテナンス役割 (maintenance role)**

物理的メンテナンス及び／又は論理的メンテナンスのサービスを実行することを担う役割。

例 メンテナンスサービスは、ハードウェア及び／又はソフトウェアの診断を含むが、それに限定されない。

3.42

手動鍵入力 (manual key entry)

キーボードのようなデバイスを使用した、暗号モジュールへの暗号鍵の入力。

3.43

手動鍵配送 (manual key transport)

例えば鍵ローダのような、コンピュータネットワークによらない方法での暗号鍵の配送。

3.44

マイクロコード (microcode)

ある実行可能なプログラム命令に対応するプロセッサの一連の命令。

例 アセンブラコード

3.45

オペレータ (operator)

一つ以上の役割を担うことを認可された人、又はその人のために暗号モジュールを操作するプロセス。

3.46

出力データ (output data)

暗号モジュールから生成される情報。

3.47

表面安定化処理 (passivation)

回路の振る舞いを変えるかもしれないものからの保護手段を、接点、コンポーネントの表面及び集積回路に与える、半導体デバイスの製造におけるプロセス。

注記 二酸化けい素ガラス又はりん（燐）けい（珪）酸ガラスは、この目的に使用可能である。

3.48

パスワード (password)

本人認証を行うため又はアクセス権を検証したりするために用いる文字（例：英字、数字、記号）の列。

3.49

個人識別番号, PIN (personal identification number, PIN)

本人認証を行うために使用される数字コード。

3.50

物理的保護 (physical protection)

物理的手段を用いた、暗号モジュール、CSP 及び PSP の安全防護策。

3.51

平文の鍵 (plaintext key)

暗号化されていない暗号鍵。

3.52

ポート (port)

暗号モジュールへのアクセスを提供する、暗号モジュールの物理的・論理的な入出力点。

3.53

プライベート鍵 (private key)

エンティティが所有する非対称鍵ペアの鍵で、そのエンティティしか使えないもの。

注記 非対称署名システムの場合、プライベート鍵は署名変換を定義する。非対称暗号化システムの場合、プライベート鍵は復号変換を定義する。

3.54**製品グレード (production-grade)**

操作仕様に合致することが試験によって確認されている製品、コンポーネント又はソフトウェア。

3.55**プロテクションプロファイル, PP (protection profile, PP)**

TOE の分野に関して特定の利用者の要求を満たす、実装に依存しないセキュリティ要求事項の集合。

3.56**公開鍵 (public key)**

エンティティが所有する非対称鍵ペアの鍵で、公開できるもの。

注記 非対称署名システムの場合、公開鍵は検証変換を定義する。非対称暗号化システムの場合、公開鍵は暗号化変換を定義する。“公知”の鍵は、全世界的に利用可能である必要はない。鍵は、既定のグループの全メンバーに利用可能であるだけでもよい。

3.57**公開鍵証明書 (public key certificate)**

適切な認証局によって署名され、それゆえ偽造できないようにされた、エンティティの公開鍵情報。

3.58**公開セキュリティパラメタ, PSP (public security parameter, PSP)**

セキュリティに関連する公開情報であって、その変更が、暗号モジュールのセキュリティを危たい（殆）化し得るもの。

例 公開暗号鍵、公開鍵証明書、自己署名証明書、トラストアンカ、及びカウンタに関連付けられたワンタイムパスワード。

3.59**乱数生成器, RBG (random bit generator, RBG)**

統計的に独立し、不偏であるように出現するビット列を出力するデバイス又はアルゴリズム。

3.60**除去可能なカバー (removable cover)**

暗号モジュールの中にある物理的な物へのアクセスを許す物理的な手段。

3.61**役割 (role)**

ユーザのアクセス権限又は暗号モジュールのサービスへの制限を定義している、ユーザと関連付けられているセキュリティ属性。

注記 一つ以上のサービスが一つの役割に関連付けられてもよい。一つの役割が一つ以上のユーザに関連付けられてもよいし、一つのユーザが一つ以上の役割を担ってもよい。

3.62**秘密鍵 (secret key)**

一つ以上のエンティティに対して一意に対応し、公開されてはならない、秘密鍵暗号アルゴリズムにお

いて使用される暗号鍵。

3.63

セキュリティ機能 (security function)

ブロック暗号、ストリーム暗号、非対称鍵暗号、メッセージ認証コード、ハッシュ関数又は他のセキュリティ機能、乱数生成器、エンティティ認証及び鍵確立のような、ISO/IEC 又は承認機関によって承認されたすべての、動作モードを伴う暗号アルゴリズム。

注記 附属書 D を参照。

3.64

シード鍵 (seed key)

暗号機能又は暗号操作を初期化するために使用される秘密値。

3.65

単純電力解析, SPA (simple power analysis, SPA)

暗号アルゴリズムの特徴及びその実装内容を暴露し、その結果暗号鍵の値を暴露することを目的とした、暗号モジュールの消費電力の変動を観察することによって得られる命令実行（又は個別命令の実行）のパターンの、直接的な（主に視覚的な）解析。

3.66

ソフトウェア (software)

暗号境界内のプログラム及びデータ構成要素であって、通常、消去可能なメディアに格納され、実行中に動的に書き込み及び変更が可能であるもの。

例 消去可能なメディアには、ハードディスクを含むがそれに限定されない。

3.67

知識分散 (split knowledge)

暗号鍵を、元の暗号鍵の知識を単独ではもたない複数の鍵要素に分割するプロセス。個々の鍵要素は、別々のエンティティによって暗号モジュールに入出力され、元の暗号鍵を再構成するために組み合わせられる。

3.68

状態情報 (status information)

暗号モジュールのある動作の特徴又は状態を示すために、暗号モジュールから出力される情報。

3.69

対称暗号技術 (symmetric cryptographic technique)

暗号化変換及び復号変換の両方に同じ秘密鍵を使用する暗号技術。

3.70

システムソフトウェア (system software)

暗号モジュールの操作を容易にするように設計された暗号境界内のはん用ソフトウェア。

例 オペレーティングシステム、コンパイラ及びユーティリティプログラム。

3.71

タンパー検出 (tamper detection)

暗号モジュールのセキュリティを危たい（殆）化する試みがなされたことの、暗号モジュールによる自動的な判定。

3.72

タンパー証跡 (tamper evidence)

暗号モジュールのセキュリティを危たい（殆）化する試みがなされたことを示す、外観上の表示。

注記 タンパーの試みの証跡を、観察できるようにすべきである。

3.73**タンパー応答 (tamper response)**

暗号モジュールがタンパーを検出したとき取る自動的な動作。

3.74**評価対象, TOE (target of evaluation, TOE)**

ISO/IEC15408 に基づく評価の対象となる、情報技術 (IT) 製品又はシステム、並びに、それに関連する管理者及びユーザのガイダンス文書。

3.75**TOE セキュリティ機能, TSF (TOE security functions, TSF)**

TOE セキュリティ方針(TSP)を正しく実現するために必要となるすべてのハードウェア、ソフトウェア、及びファームウェアからなる TOE の部分集合。

3.76**TOE セキュリティ方針, TSP (TOE security policy, TSP)**

TOE 内での資産の管理方法、保護方法、及び配付方法を規定する規則の集合。

3.77**トラストアンカ (trust anchor)**

公開鍵暗号アルゴリズム、公開鍵の値、発行者の名前、及び場合によって他のパラメタを含む、信頼される情報。

注記 1 他のパラメタには、有効期間を含むがそれに限定されない。

注記 2 トラストアンカは、自己署名証明書の形で提供されてもよい。

3.78**高信頼パス (trusted path)**

ユーザと TSF とが、TSP を実現するのに必要な信頼度を確保するための通信手段。

3.79**ユーザ (user)**

暗号サービスを受けるために暗号モジュールにアクセスする人、又はその人のために働くプロセス（サブジェクト）。

3.80**ゼロ化 (zeroisation)**

データ復元及び再使用を防止するために、CSP を無効化する方法。

4 略語

このドキュメントのために、次の略語を適用する。

API: 応用プログラムインタフェース (Application Program Interface)

CAPP: Controlled Access Protection Profile (附属書 C 参照)

CBC: 暗号ブロック連鎖 (Cipher Block Chaining) 暗号利用モードの一つ

EAL: 評価保証レベル(Evaluation Assurance Level)

EDC: 誤り検出符号(Error Detection Code)

HDL: ハードウェア記述言語(Hardware Description Language)

IC: 集積回路(Integrated Circuit)

PROM: プログラム可能な読出し専用メモリ(Programmable Read-Only Memory)

RAM: ランダムアクセスメモリ(Random Access Memory)

ROM: 読出し専用メモリ(Read-Only Memory)

5 暗号モジュールのセキュリティレベル

四つのセキュリティレベルの概要については、次による。どのように要求事項が満たされるかを示すために掲げた例示は、そこに掲げたものだけに限ることを意図したものでなく、すべてを網羅したものでもない。

なお、この規格において、“モジュール”という用語は“暗号モジュール”を意味する。

5.1 セキュリティレベル1

セキュリティレベル1は、セキュリティの最も低いレベルである。暗号モジュールとしての基本的なセキュリティ要求事項（例えば、少なくとも一つの承認されたアルゴリズム、又は承認されたセキュリティ機能が使用されていなければならないこと。）がここで規定されている。セキュリティレベル1では、製品グレードとしての基本的な要求事項を超える特別な物理的セキュリティのメカニズムは要求されない。セキュリティレベル1の暗号モジュールの例として、パーソナルコンピュータ（PC）の暗号ボードがある。

セキュリティレベル1では、評価されていないオペレーティングシステムを使用しているはん用コンピュータシステム上で実行される暗号モジュールのソフトウェア構成要素及びファームウェア構成要素を許可している。このような暗号モジュールの実装は、例えば、物理的セキュリティ、ネットワークセキュリティ、管理手段のような他の管理手段が限られているか又は存在しないときの、低いレベルのセキュリティのアプリケーションに適している。暗号のソフトウェア実装は、ハードウェア実装よりも費用対効果が高いため、低いレベルのセキュリティ要求事項を満たすための、ハードウェアメカニズムに代わる暗号での解決策として選択できる。

5.2 セキュリティレベル2

セキュリティレベル2は、タンパー証跡をもつコーティング若しくはシール、又は除去可能なカバー若しくはドアに対してこじ開け耐性のある錠を含むタンパー証跡に関する要求事項を追加することで、セキュリティレベル1の物理的セキュリティのメカニズムを強化したものである。

タンパー証跡をもつコーティング又はシールは、モジュールに付設され、暗号モジュール内のクリティカルセキュリティパラメタ（以下、CSPと記す。）及び／又は公開セキュリティパラメタ（以下、PSPと記す。）への物理的なアクセスがあった場合、そのコーティング又はシールは必ず破壊されなければならない。タンパー証跡をもつシール又はこじ開け耐性のある錠は、認可されていない物理的なアクセスから保護するために、カバー又はドアに付設される。

セキュリティレベル2は、役割ベースの認証を最低限必要とする。この認証では、オペレータが特定の役割を担い、その役割に対応したサービスを実行する権限があることを、暗号モジュールが認証する。

セキュリティレベル2では、暗号モジュールのソフトウェア構成要素及びファームウェア構成要素が、次の二つの条件を満たすオペレーティングシステムを使用しているはん用コンピュータシステムで実行されることを許可している。

- ・ 附属書Cに記載する承認されたプロテクションプロファイル（以下、PPと記す。）で規定する機能

要件を満たす。

- ・ EAL2（又はそれ以上）の ISO/IEC 15408 評価保証レベルの評価を得ている。

この条件を満たすオペレーティングシステムはある信頼レベルを提供するので、はん用コンピュータプラットフォーム上で実行される暗号モジュールは、専用のハードウェアシステム上に実装された暗号モジュールに匹敵する。

5.3 セキュリティレベル3

セキュリティレベル2で要求されるタンパー証跡をもつ物理的セキュリティのメカニズムに加えて、セキュリティレベル3は、侵入者がモジュール内の CSP 及び／又は PSP に対してアクセスすることを防止することを意図している。セキュリティレベル3で要求される物理的セキュリティのメカニズムは、物理的アクセスの試み、暗号モジュールの利用又は変更に対して、高い確率で検出及び応答することを目的としている。この物理的セキュリティのメカニズムには、暗号モジュールの除去可能なカバー・ドアが開かれたときに、CSP をすべてゼロ化するタンパー証跡・タンパー応答をもつ回路、及び頑丈な囲いの使用を含んでもよい。

セキュリティレベル3は、ID ベースの認証メカニズムを要求する。これは、セキュリティレベル2で規定される役割ベースの認証メカニズムが提供するセキュリティを更に強化する。暗号モジュールは、オペレータの ID を認証し、かつ、識別されたオペレータが特定の役割を担って、その役割に応じたサービスを実行する権限が与えられていることを検証する。

セキュリティレベル3は、CSP の入出力（知識分散の技術を利用した CSP の入出力を含む。）が、他のポートから物理的に分離されたポートを使用して、又は他のインタフェースから論理的に分離された、高信頼パスを使用するインタフェースを使用して実行されることを要求する。また、CSP が、暗号化された形式で暗号モジュールへ入出力されることでもよい（このときは、CSP が暗号モジュールを取り囲むシステム又は仲介するシステムを経由してもよい。）。

セキュリティレベル3では、暗号モジュールのソフトウェア構成要素及びファームウェア構成要素が、次の二つの条件を満たすオペレーティングシステムを使用しているはん用のコンピュータシステムで実行されることを許可している。

- ・ （附属書 C に記載する）承認された P P で規定する機能要件に追加して、高信頼パスの機能要件 (FTP_TRP.1) を満たす。
- ・ EAL3（又はそれ以上）の ISO/IEC 15408 評価保証レベルの評価を得て、更に、非形式的な TOE セキュリティ方針モデルの保証要件 (ADV_SPM.1) を満たす評価を得ている。

高信頼パスの実装は、このシステム上で実行される他の信頼できないソフトウェア又はファームウェアから、CSP 並びに暗号モジュールのソフトウェア構成要素及びファームウェア構成要素を保護する。

5.4 セキュリティレベル4

セキュリティレベル4は、この規格の中で定義される最も高いレベルのセキュリティを提供する。このセキュリティレベルでの物理的セキュリティのメカニズムは、外部電源を用いるかどうかにかかわらず、CSP 及び／又は PSP がモジュールに含まれる場合、すべての認可されていない物理的なアクセスに対して検出及び応答するための、暗号モジュールの周りを完全に囲んだ包被での保護を提供する。あらゆる方向からの暗号モジュールの囲いへの侵入は、非常に高い確率で検出され、その結果、即座にすべての CSP がゼロ化される。セキュリティレベル4の暗号モジュールは、物理的に保護されていない環境下での使用に役立つ。

また、セキュリティレベル4では、暗号モジュールが正常に動作する電圧及び温度の範囲を超えた環境

条件又は環境変動による、セキュリティの危たい化に対して暗号モジュールを保護する。攻撃に対する暗号モジュールの防御を妨害するために、正規の動作範囲を意図的に逸脱する方法が攻撃者に用いられることがある。暗号モジュールは、周囲の環境変動を検出し CSP をゼロ化するように設計された特別な環境保護特性を含むか、又は暗号モジュールのセキュリティを危たい化しようとする攻撃による、暗号モジュールの正規の動作範囲外での変動に影響されない合理的な保証をもたらすために、厳しい環境故障試験を受けることが要求される。

セキュリティレベル 4 では、暗号モジュールのソフトウェア構成要素及びファームウェア構成要素が、次の二つの条件を満たすオペレーティングシステムを使用しているはん用のコンピュータシステムで実行されることを許可している。

- ・ セキュリティレベル 3 で規定された機能要件を満たす。
- ・ EAL4（又はそれ以上）の ISO/IEC 15408 評価保証レベルの評価を得ている。

6 機能的セキュリティ目標

この規格で規定されているセキュリティ要求事項は、暗号モジュールのセキュアな設計及び実装に関するものである。これらの要求事項は、次のことを暗号モジュールに実現するという、高位の機能的セキュリティ目標から導き出されている。

- ・ 取扱いに慎重さを要する情報を保護するために、承認されたセキュリティ機能を採用し、正しく実装する。
- ・ 認可されていない操作又は認可されていない利用から暗号モジュールを保護する。
- ・ その暗号モジュールの内容（CSP を含む。）の認可されていない開示を防ぐ。
- ・ その暗号モジュール及び暗号アルゴリズムに対する、認可されていない変更及び検出不能な変更（CSP 及び／又は PSP に対する、認可されていない変更、置換、挿入、及び消去を含む。）を防ぐ。
- ・ その暗号モジュールの動作状態を表示する。
- ・ 承認された動作モードで動作するとき、その暗号モジュールが適切に実行することを保証する。
- ・ モジュールの動作においてエラーを検出し、かつ、これらのエラーによる CSP 及び／又は PSP の危たい化を防ぐ。

7 セキュリティ要求事項

ここでは、この規格に適合する暗号モジュールが満たすべきセキュリティ要求事項を規定している。これらのセキュリティ要求事項は、暗号モジュールの設計及び実装に関連した分野を網羅している。これらの分野には、次のものがある。

- ・ 暗号モジュールの仕様
- ・ 暗号モジュールのポート及びインタフェース
- ・ 役割、サービス及び認証
- ・ 有限状態モデル
- ・ 物理的セキュリティ
- ・ 動作環境
- ・ 暗号鍵管理
- ・ 自己テスト
- ・ 設計保証

その他の攻撃（例えば、DPA）の対処に関連した付加的な分野は、セキュリティレベル 4 を除いては、現在試験されていないが、ペンダは、実装された抑制手段を文書化することが要求される。表 1 は、それぞれの分野におけるセキュリティ要求事項をまとめたものである。

表 1—セキュリティ要求事項の要約

	セキュリティ レベル 1	セキュリティ レベル 2	セキュリティ レベル 3	セキュリティ レベル 4
暗号モジュールの仕様	暗号モジュール、暗号境界、承認されたアルゴリズム、承認された動作モードの仕様。すべてのハードウェア、ソフトウェア、ファームウェアの構成要素を含む暗号モジュールの記述。暗号モジュールのセキュリティポリシーの宣言。			
暗号モジュールのポート及びインタフェース	必ず（須）のインタフェース及び選択可能なインタフェース。すべてのインタフェースの仕様及びすべての入出力データパスの仕様。		他のデータポートから論理的に分離された、CSP のためのデータポート。	
役割、サービス、及び認証	必ず（須）の役割及びサービスと選択可能な役割及びサービスとの論理的な分離。	役割ベースのオペレータ認証又は ID ベースのオペレータ認証。	ID ベースのオペレータ認証。	
有限状態モデル	有限状態モデルの仕様。必ず（須）の状態及び選択可能な状態。状態遷移図及び状態遷移の仕様。			
物理的セキュリティ	製品グレードの装置。	錠又はタンパー証拠。	カバー及びドアに対してのタンパー検出及びタンパー応答。	タンパー検出及びタンパー応答が可能な包被。EFP 又は EFT。
動作環境	単一のオペレータ。実行可能なコード。承認された完全性技術。	参照 PP に適合し、EAL2 の条件で評価を受けた環境。EAL2 の条件で評価を受け、任意アクセス制御機構及び監査機構をもつ環境。	参照 PP に加え、高信頼パスに適合し、EAL3 に加え、セキュリティポリシーのモデル化の条件で評価を受けた環境。	参照 PP に加え、高信頼パスに適合し、EAL4 の条件で評価を受けた環境。
暗号鍵管理	鍵管理機構：乱数生成及び鍵生成、鍵確立、鍵配送、鍵入出力、鍵の保管、並びに鍵のゼロ化。			
	手動の転送方法を用いて転送された秘密鍵及びプライベート鍵は、平文の形式で入力又は出力してもよい。		手動の転送方法を用いて転送された秘密鍵及びプライベート鍵は、暗号化又は知識分散処理を用いて、入力又は出力されなければならない。	
自己テスト	パワーアップ自己テスト：暗号アルゴリズムテスト、ソフトウェア/ファームウェア完全性テスト及び重要機能テスト。 条件自己テスト。			
設計保証	構成管理(CM)。セキュアな設置及び生成。設計とポリシーとの対応。ガイドダンス文書。	構成管理システム。セキュアな配送。機能仕様。	高級言語による実装。	形式的モデル。詳細な説明（非形式的証明）。事前条件及び事後条件。
その他の攻撃への対処	攻撃への対処の仕様。 現在は、試験可能な要求事項は用意されていない。			試験可能な要求事項を備えた、攻撃への対処の仕様。

暗号モジュールは、箇条 7 で記述された各分野の要求事項に対して、試験されなければならない。暗号モジュールは分野ごとに独立に格付けされなければならない。幾つかの分野では、上位のセキュリティレ

レベルの要求事項が下位のセキュリティレベルの要求事項を包含する。これらの分野では、暗号モジュールは、その項目の要求事項すべてを満足する最大のセキュリティレベルに照らして格付けされる。セキュリティレベルの区別がない項目においては、暗号モジュールは、セキュリティレベルにかかわらず、同一の規定が適用される。

セキュリティ分野ごとの独立したセキュリティレベルの格付けに加え、暗号モジュールは総合的なセキュリティレベルも格付けされる。総合的なセキュリティレベルの格付けは、各項目で独立に格付けしたセキュリティレベルのうち、最小のセキュリティレベルを示す。

この規格のセキュリティ要求事項の多くは、**附属書 A** で要約されている特定の文書化要求事項を含んでいる。ユーザマニュアル及び設置マニュアルを含むすべての文書は、評価のためにベンダによって試験機関へ提供されなければならない。

7.1 暗号モジュールの仕様

暗号モジュールは、ハードウェア、ソフトウェア、ファームウェア、又はそれらの組合せの集合でなければならない。これらハードウェア、ソフトウェア、ファームウェアは、定義された暗号境界内に含まれ、暗号機能又は暗号プロセスを実装している。暗号モジュールは、承認された動作モードで使用される承認されたセキュリティ機能を少なくとも一つ実装しなければならない。承認されていないセキュリティ機能は、承認されていない動作モードでの使用のために含まれてもよい（すなわち、暗号モジュールの範囲内ではセキュリティと無関係である。）。オペレータが承認された動作モードにあるかどうかを判定できるようになっていなければならない。セキュリティレベル 1 及びセキュリティレベル 2 では、いつ暗号モジュールが承認された動作モードにあるのかをセキュリティポリシーで示してもよい。セキュリティレベル 3 及びセキュリティレベル 4 では、暗号モジュールが承認された動作モードにあるとき、そのことを表示しなければならない。承認されたセキュリティ機能は**附属書 D** に記載している。

暗号境界は、暗号モジュールの物理的範囲及び／又は論理的範囲を確立する明確に定義された境界線で構成されなければならない。暗号モジュールがソフトウェア又はファームウェアの構成要素から構成されている場合には、暗号境界は、一つ以上のプロセッサ及び（ソフトウェア及びファームウェアの構成要素を格納及び保護する）その他のハードウェア構成要素を含まなければならない。暗号モジュールのハードウェア、ソフトウェア及びファームウェアの構成要素は、これらの構成要素が暗号モジュールのセキュリティに影響を与えないことが示される場合には、この規格の要求事項から除外することができる。

次の文書化要求事項は、暗号モジュール内にあるすべてのセキュリティに関係するハードウェア、ソフトウェア及びファームウェアに適用しなければならない。これらの要求事項は、ソースコードが利用できないマイクロコード又はシステムソフトウェア、若しくは暗号モジュールのセキュリティに影響しないことを示すことができるハードウェア、ソフトウェア、又はファームウェアの構成要素には適用しない。

- a) 文書には、暗号モジュールのハードウェア、ソフトウェア及びファームウェアの構成要素を示し、これらの構成要素を囲む暗号境界を示し、また、暗号モジュールの物理的な構成を記述しなければならない（7.5 参照）。
- b) 文書には、この規格のセキュリティ要求事項の適用を除外する暗号モジュールのハードウェア、ソフトウェア及びファームウェアの構成要素を示し、また、適用除外とする根拠を説明しなければならない。
- c) 文書には、暗号モジュールの、物理的ポート、論理的インタフェース及び定義された入出力データパスのすべてを示さなければならない。
- d) 文書には、暗号モジュールの手動の又は論理的な制御、物理的又は論理的な状態表示、並びに関連す

るそれらの物理的、論理的及び電氣的な特徴を示さなければならない。

- e) 文書には、承認されているかどうかにかかわらず、暗号モジュールに採用されるすべてのセキュリティ機能をリスト化して、承認されているかどうかにかかわらず、すべての動作モードを示さなければならない。
- f) 文書には、次を示さなければならない。
 - 1) 暗号モジュールの主要なハードウェア構成要素のすべて及びそれらの接続関係を示すブロック図。これには、マイクロプロセッサ、入出力バッファ、平文・暗号文データ用バッファ、制御バッファ、鍵格納メモリ、作業メモリ及びプログラムメモリを含む。
 - 2) 暗号モジュールのハードウェア、ソフトウェア及びファームウェアの構成要素の設計。この設計を文書化するためには、ソフトウェア・ファームウェアは高級言語を使用し、ハードウェアは回路図を使用しなければならない。
- g) 文書には、CSP、PSP 及び、開示又は変更されると暗号モジュールのセキュリティに危たい化をもたらすその他の保護された情報（例えば、監査イベント、監査データ）を含む、すべてのセキュリティに関係する情報を示さなければならない。
- h) 文書には、暗号モジュールのセキュリティポリシーを示さなければならない。このセキュリティポリシーは、この規格の要求事項から導かれる規則及び製品開発を通じて課せられたあらゆる追加要求事項から導かれる規則を含まなければならない（**附属書 B** 参照）。

7.2 暗号モジュールのポート及びインタフェース

暗号モジュールは、すべての情報の流れ及び物理的アクセスポイントを、暗号モジュールへのすべての入出力点を定義している物理的ポート及び論理的インタフェースに限定しなければならない。暗号モジュールの論理的インタフェースは、一つの物理的ポートを共有（例えば、データの入力と出力とが、同一のポートを介して行われる。）しても、又は一つ以上の物理的ポートに分散（例えば、シリアルポートとパラレルポートとの両方を介して、入力データが入力される）されてもよいが、互いに明確に区別して定義されていなければならない。暗号モジュールのソフトウェア構成要素のアプリケーションプログラムインタフェース(API)は、一つ以上の論理的インタフェースとして定義されてもよい。

暗号モジュールは、次の四つの明確に区別して定義された論理的インタフェースをもたなければならない（“入力”及び“出力”とは、暗号モジュールから見たときの“入力”及び“出力”である。）。

- a) **データ入力インタフェース** 暗号モジュールに入力され処理されるすべてのデータ（制御入力インタフェースを介して入力される制御データを除く）は、データ入力インタフェースを介して入力されなければならない。これらのデータには、平文データ、暗号文データ、CSP、PSP 及び別の暗号モジュールからの状態情報を含む。
- b) **データ出力インタフェース** 暗号モジュールから出力されるすべてのデータ（状態出力インタフェースを介して出力される状態データを除く）は、データ出力インタフェースから出力されなければならない。これらのデータには、平文データ、暗号文データ、CSP、PSP 及び別の暗号モジュールのための制御情報を含む。エラー状態にある場合及び自己テスト中の場合には、データ出力インタフェースからのすべてのデータ出力は禁止されなければならない（7.8 参照）。
- c) **制御入力インタフェース** 暗号モジュールの動作を制御するために使用されるすべての入力コマンド、信号及び制御データ（関数呼出し及びスイッチ、ボタン、並びにキーボードのような手動制御を含む。）は、制御入力インタフェースから入力されなければならない。
- d) **状態出力インタフェース** 暗号モジュールの状態を示すために使用されるすべての出力信号、インジ

データ及び状態データ（戻り値、並びに発光ダイオード及びディスプレイのような物理的なインジケータを含む。）は、状態出力インタフェースから出力されなければならない。

暗号モジュールに入力されるすべての外部電力（外部電源又はバッテリーからの電力を含む。）は、電源ポートから入力されなければならない。暗号モジュールの暗号境界にすべての電力が内部的に供給又は維持されているとき（例えば、内部バッテリー）には、電源ポートは必要とされない。

暗号モジュールは、入力するデータと制御データとを区別し、また、他方で、出力するデータと状態データとを区別しなければならない。データ入力インタフェースから暗号モジュールへ入力されるすべての入力データは、入力データパスだけを通らなければならない。データ出力インタフェースを介して暗号モジュールから出力されるすべての出力データは、出力データパスだけを通らなければならない。出力データパスは、鍵生成、手動鍵入力、又は鍵のゼロ化が実行されている間は、回路及び処理から論理的に分離されていなければならない。誤って取扱いに慎重さを要する情報を出力してしまうことを防止するために、平文の CSP 又は取扱いに慎重さを要するデータを出力インタフェースから出力することに対して、二つの独立した内部動作[例えば、二つの異なるソフトウェアフラグがセットされるという二つの独立した内部動作(その一つはユーザが起動するものでもよい。)、二つのハードウェアゲートが別々の動作によって順次にセットされるという二つの独立した内部動作。]が要求されなければならない。

セキュリティレベル 1 及び 2

データの入出力に使用する一つ以上の物理的ポート及び一つ以上の論理的インタフェースは、暗号モジュールの他のポート及び他のインタフェースと物理的及び論理的に共有されてもよい。

セキュリティレベル 3 及び 4

レベル 1 及び 2 の要求事項に加えて、レベル 3 及び 4 に対する追加的要求事項は、次の 3 条件のうち、第 1 条件又は第 2 条件と第 3 条件とを満たすこととする。

- ・ 平文の CSP の入出力のために使用される一つ以上の物理的ポートは、暗号モジュールの他のすべてのポートから物理的に分離されていなければならない。
- ・ 平文の CSP の入出力に使用される論理的インタフェースは、高信頼パスを使用して他のすべてのインタフェースから論理的に分離されていなければならない。
- ・ 平文の CSP は、高信頼パスを経由して暗号モジュールに入力されるか、又は、その鍵要素が不注意に格納、結合、若しくはその他の方法で処理される可能性のある、暗号モジュールを取り囲むシステム若しくは仲介するシステムを経由せずに、直接に暗号モジュールに入力されなければならない（7.7.4 参照）。

7.3 役割、サービス及び認証

暗号モジュールは、オペレータに対して認可された役割及びそれぞれの役割に対応するサービスをサポートしなければならない。単一のオペレータは、複数の役割を担ってもよい。暗号モジュールが、複数のオペレータによる同時利用をサポートする場合には、その暗号モジュールは、それぞれのオペレータによって担われる役割及びそれに対応するサービスの区分けを、内部的に維持しなければならない。オペレータは、CSP 及び PSP が変更、開示、又は置換されないサービス（例えば、状態の表示、自己テスト、暗号モジュールのセキュリティに影響を与えない他のサービス）を実行するために、認可された役割を担うことを要求されない。

暗号モジュールにアクセスするオペレータを認証するために、並びにオペレータが要求された役割を担うことが認可されていること及び役割の中のサービスを実行することが認可されていることを検証するために、認証メカニズムを暗号モジュール内に組み込んでよい。

7.3.1 役割

暗号モジュールは、オペレータに対し次の認可された役割をサポートしなければならない。

- a) **ユーザ役割** 暗号操作及びその他の承認されたセキュリティ機能を含む、一般的なセキュリティサービスを行うことを担う役割。
- b) **クリプトオフィサ役割** 暗号関連の初期化又は管理機能（例えば、暗号モジュールの初期化、CSP・PSPの入出力、監査機能）を行うことを担う役割。

暗号モジュールが、オペレータにメンテナンスサービスの実施を許可する場合には、暗号モジュールは、次の認可された役割をサポートしなければならない。

- a) **メンテナンス役割** 物理的なメンテナンス及び／又は論理的なメンテナンスサービス（例えば、ハードウェア・ソフトウェアの診断）を行うことを担う役割。暗号モジュールは、それがサポートするメンテナンス役割へ入る場合、又はメンテナンス役割から出る場合には、すべてのCSPをゼロ化しなければならない。

暗号モジュールは、7.3.1に規定した役割に加え、他の役割又は付随する役割をサポートしてもよい。

7.3.2 サービス

サービスは、暗号モジュールが実行できるサービス、動作、又は機能のすべてを意味しなければならない。サービス入力、特定のサービス、動作、又は機能を開始又は獲得させる暗号モジュールへのすべてのデータ入力又は制御入力から構成されなければならない。サービス出力は、サービス入力によって開始又は獲得されるサービス、動作、又は機能から生じるすべてのデータ出力及び状態出力から構成されなければならない。それぞれのサービス入力は、サービス出力をもたらさなければならない。

暗号モジュールは、オペレータに次のサービスを提供しなければならない。

- a) **状態の表示** 暗号モジュールの現在の状態を出力する。
- b) **自己テストの実行** 7.8で規定されているように、自己テストを開始及び実行する。
- c) **承認されたセキュリティ機能の実行** 7.1で規定されているように、承認された動作モードで使用される少なくとも一つの承認されたセキュリティ機能を実行する。

暗号モジュールは、上記に規定したサービスに加え、承認済み及び未承認のその他のサービス、動作、又は機能を提供してもよい。特定のサービスは、複数の役割に提供されてもよい（例えば、鍵入力サービスは、ユーザ役割及びクリプトオフィサ役割に提供されてもよい）。

暗号モジュールがバイパス機能を実装している場合、つまり暗号的処理が行われない（例えば、暗号モジュールの中で暗号化せずに平文を転送する）サービスが提供される場合には、次の二つが要求される。

- ・ たった一つのエラーによって暗号化されていないデータが不注意にバイパスされることを防ぐための機能を起動させるために、二つの独立した内部動作（例えば、二つの異なるソフトウェア又はハードウェアのフラグがセットされる。そのうち一つのフラグのセットは、ユーザ操作によるものでよい。）が要求されなければならない。
- ・ 暗号モジュールは、バイパス機能が次のいずれの状態にあるかを表示しなければならない。
 - 1) バイパス機能が動作せず、暗号モジュールが暗号処理を行うサービス（例えば、平文データを暗号化するサービス）だけを提供している状態。
 - 2) バイパス機能が動作し、暗号モジュールが暗号処理を行わないサービス（例えば、平文データを暗号化しないサービス）だけを提供している状態。
 - 3) バイパス機能の動作と非動作とが交互に起こり、暗号モジュールが、暗号処理を行うサービスと暗号処理を行わないサービスの双方を提供している状態（例えば、多重通信チャンネルをもつ暗号モジ

ジュールの場合、それぞれのチャネル構成によって、平文データを暗号化したり暗号化しなかったりする状態。))。

7.3.3 オペレータ認証

暗号モジュールにアクセスするオペレータを認証するため、そしてオペレータが要求された役割を担って、その役割の中のサービスを実行することが認可されていることを検証するために、暗号モジュール内で認証メカニズムが必要となることがある。暗号モジュールは、セキュリティレベルに応じて暗号モジュールへのアクセスを制御するために、少なくとも次のメカニズムのうち一つを備えなければならない。

a) 役割ベースの認証

暗号モジュールに役割ベースの認証メカニズムがサポートされている場合には、暗号モジュールは、オペレータが一つ以上の役割を選択することを要求しなければならない。暗号モジュールは、オペレータが選択された役割（又は役割の集合）を担っていることを認証しなければならない。暗号モジュールは、オペレータ個人の ID を認証することは要求されない。役割の選択及び選択された役割を担うことの認証は、同時に行われてもよい。暗号モジュールが、オペレータの役割変更を許可する場合には、暗号モジュールは、オペレータが以前に認証されていないいかなる役割を担うことに対しても認証をしなければならない。

b) ID ベースの認証

暗号モジュールにおいて ID ベースの認証メカニズムがサポートされている場合には、暗号モジュールはオペレータが個別に識別されることを要求し、オペレータによって暗黙的又は明示的に一つ以上の役割が選択されることを要求し、並びにオペレータの ID 及びオペレータが選択された役割（又は役割の集合）を担うことの認可を認証しなければならない。オペレータの ID、役割の選択及び選択された役割を担うことの認可は、同時に行われてもよい。暗号モジュールがオペレータに役割を変更することを許可する場合には、暗号モジュールは、識別されたオペレータが以前に認可されていないいかなる役割を担うための認可を検証しなければならない。

暗号モジュールは、認証されたオペレータに対して、認可された役割の中で許容されるサービスすべてを実行することを許す方式としてもよいし、それぞれのサービス又は異なるサービスの集合に対して個々の認証を要求する方式としてもよい。暗号モジュールが電源オフに続いて電源オンされた場合には、以前の認証の結果は維持されてはならず、暗号モジュールはオペレータに再認証されるように要求しなければならない。

暗号モジュールは、サポートする認証メカニズムを実行するため、いろいろなタイプの認証データを必要とすることがある。認証データの例を次に示す（ただし、これらに限定するものではない）。

- ・ パスワード、PIN、暗号鍵、又は同等のデータの知識又は所有。
- ・ 物理鍵、トークン、又は同等のものの所有。
- ・ 個人の特徴の照合。

暗号モジュール内の認証データは、認可されていない開示、変更及び置換から保護されなければならない。

認証メカニズムの初期化では、特別な扱いが必要になることがある。暗号モジュールが、最初にアクセスされるとき、オペレータを認証するために必要な認証データを含まない場合には、他の認可された方法（例えば、手続による制御、又は工場設定値、又はデフォルトの認証データの使用）を用いて、暗号モジュールへのアクセスを制御し、認証メカニズムを初期化しなければならない。

認証メカニズムの強度は、次の仕様に適合しなければならない。

- a) 1 回の認証メカニズムの試行において、ランダムな試行が成功する確率（例えば、パスワード又は PIN

の推定の成功率、生体認証デバイスの誤受入率、それらの幾つかの組合せ。)は、目標認証強度を満たさなければならない。この確率は、例えば、1 000 000 分の 1 未満である。

- b) 複数回の認証メカニズムを 1 分間に試行する場合、確立は、定められた目標認証強度を満たさなければならない。ランダムな試行が成功する確率は、例えば、100 000 分の 1 未満である。
- c) オペレータへの認証データのフィードバックは、認証の間、あいまいにしなければならない(例えば、パスワード入力の際に文字列の表示が見えない)。
- d) 認証の試行の間、オペレータに提供されるフィードバックは、認証の成功又は失敗の事実以上の情報を提供することで、認証メカニズムの強度を弱めてはならない。

各セキュリティレベルに適用されるオペレータ認証への要求事項は、次のとおりである。

セキュリティレベル 1

暗号モジュールは、暗号モジュールへのアクセスを制御するための認証メカニズムの採用が必ず(須)ではない。暗号モジュールが、認証メカニズムをサポートしない場合には、暗号モジュールは、オペレータが一つ以上の役割を暗黙的又は明示的に選択すること要求しなければならない。

セキュリティレベル 2

暗号モジュールは、暗号モジュールへのアクセスを制御するために、役割ベースの認証を採用しなければならない。

セキュリティレベル 3 及び 4

暗号モジュールは、暗号モジュールへのアクセスを制御するために、ID ベースの認証メカニズムを採用しなければならない。

7.4 有限状態モデル

暗号モジュールの動作は、状態遷移図及び／又は状態遷移表によって表現される有限状態モデル(又は同等のもの)を用いて示されなければならない。

状態遷移図及び／又は状態遷移表は、次を含む。

- ・ 暗号モジュールの動作状態及びエラー状態のすべて。
- ・ 対応するある状態から別の状態への遷移。
- ・ ある状態から別の状態への遷移を引き起こす入力イベント。
- ・ ある状態から別の状態への遷移の結果起きる出力イベント。

暗号モジュールは、次の動作状態及びエラー状態を含まなければならない。

- a) **電源オン・オフ状態** 主電源、副電源、又はバックアップ電源の状態。これらの状態は、暗号モジュールに適用されている電源間を区別してもよい。
- b) **クリプトオフィサ状態** クリプトオフィサのサービスが実行されている状態(例えば、暗号関連の初期化及び鍵管理)。
- c) **CSP/PSP 入力状態** CSP 及び PSP を暗号モジュールへ入力している状態。
- d) **ユーザ状態** 認可されたユーザがセキュリティサービスを受け、暗号操作を実行し、又はその他の承認された機能若しくは承認されていない機能を実行している状態。
- e) **自己テスト状態** 暗号モジュールが自己テストを実行している状態。
- f) **エラー状態** 暗号モジュールがエラーとなったときの状態 エラー状態は、装置故障を指し示し、かつ、暗号モジュールのメンテナンス、サービス、若しくは修理を必要とするかもしれない“ハード”エラー又は暗号モジュールの初期化若しくはリセットを必要とするかもしれない復旧可能な“ソフト”エラーを含んでもよい。エラー状態からの復旧は、暗号モジュールのメンテナンス、サービス、又は

修理を必要とするハードエラーによって引き起こされたものを除いて、可能でなければならない。

暗号モジュールは、次のような他の状態を含んでもよい。ただし、これらに限定するものではない。

- a) **バイパス状態** バイパス能力が作動し、暗号化処理がされない（例えば、暗号モジュールを通して平文を転送する）サービスが提供される状態。
- b) **メンテナンス状態** 物理的及び論理的メンテナンステストを含む暗号モジュールのメンテナンス及びサービスを行う状態。暗号モジュールがメンテナンス役割を含む場合には、メンテナンス状態が含まれていなければならない。

7.5 物理的セキュリティ

暗号モジュールは、物理的セキュリティのメカニズムを用いて、実装後の暗号モジュールの内容への認可されていない物理的なアクセスを制限し、実装後の暗号モジュールの認可されていない使用又は変更（暗号モジュール全体の置き換えを含む。）を防がなければならない。暗号境界内のすべてのハードウェア、ソフトウェア、ファームウェア及びデータ構成要素は保護されなければならない。

ソフトウェアによってすべて実装されている暗号モジュール（例えば、物理的セキュリティがホストのプラットフォームによってだけ提供される暗号モジュール）は、この規格の物理的セキュリティの要求事項の対象ではない。

物理的セキュリティの要求事項は、次の三つの定義された暗号モジュールの物理形態に対して規定されている。

- a) **シングルチップ暗号モジュール** これは、単一の集積回路(IC)チップがスタンドアロンのデバイスとして用いられているか、又は物理的に保護されていない囲い若しくは製品内に組込まれている物理形態である。シングルチップ暗号モジュールの例には、単一 IC チップ又は単一 IC チップの付いたスマートカードが含まれる。
- b) **マルチチップ組込型暗号モジュール** これは、二つ又はそれ以上の IC チップが相互接続されて、物理的に保護されていない囲い又は製品内に組込まれている物理形態である。マルチチップ組込型暗号モジュールの例には、アダプタ及び拡張ボードが含まれる。
- c) **マルチチップスタンドアロン型暗号モジュール** これは、二つ又はそれ以上の IC チップが相互接続されて、囲い全体が物理的に保護されている物理形態である。マルチチップスタンドアロン型暗号モジュールの例には、暗号化ルータ又はセキュア無線が含まれる。

暗号モジュールの物理的セキュリティのメカニズムに依存して、認可されていない物理的なアクセス、使用、又は変更の攻撃は、次の二つの時点のいずれか一方又は双方で高い確率で検出されなければならない。

- ・ 攻撃後。ただし視覚的な形跡（すなわち、タンパー証跡）を残す仕組みが設けてある場合。
- ・ 攻撃の最中。ただし、CSP 及び PSP を保護するために、暗号モジュールによって適切な即座の動作（すなわち、タンパー応答）がとれる場合。その即座の動作は、CSP 及び PSP の読出しが不可能であることを意味しなければならない。

表 2 は、四つのセキュリティレベルそれぞれの物理的セキュリティの要求事項（一般的な要求事項及び三つの形態に特有の要求事項）を要約している。それぞれのセキュリティレベルにおける形態特有の物理的セキュリティの要求事項は、同じセキュリティレベルの一般的な要求事項を強化し、かつ、それよりも低いセキュリティレベルにおける形態特有の要求事項を包含している。

表 2—物理的セキュリティ要求事項の要約

	すべての形態に対する一般的要求事項	シングルチップ暗号モジュール	マルチチップ組込型暗号モジュール	マルチチップスタンドアロン型暗号モジュール
セキュリティレベル 1	製品グレードの構成要素(標準的な表面安定化処理)。メンテナンスアクセスインタフェースへのアクセス時の自動ゼロ化。	追加要求事項なし	囲い又は除去可能なカバーを用いる場合は、製品グレードのもの。	製品グレードの囲い
セキュリティレベル 2	タンパー証跡(例えば、カバー、囲い、又はシール)	不透明でタンパー証跡を残す、チップ上のコーティング又は囲い	不透明でタンパー証跡を残すカプセル化した材料又はドア若しくは除去可能なカバーにタンパー証跡を残すシール若しくはこじ開け耐性のある錠の付いた囲い	ドア又は除去可能なカバーにタンパー証跡を残すシール、又はこじ開け耐性のある錠の付いた不透明な囲い
セキュリティレベル 3	タンパー応答及びゼロ化回路。保護された通気孔。	堅く不透明なタンパー証跡を残すチップ上のコーティング又は強固で除去耐性及び貫き耐性のある囲い	堅く不透明な封止材でカプセル化されたマルチチップ回路形態又はマルチチップスタンドアロン型のセキュリティレベル 3 の要求事項相当	堅く不透明な封止材でカプセル化されたマルチチップ回路形態又は除去若しくは貫くことの試みが重大な損害を与える強固な囲い
セキュリティレベル 4	温度及び電圧に関する EFP 又は EFT	堅く不透明で除去耐性のあるチップ上のコーティング	タンパー応答及びゼロ化回路の付いたタンパー検出包被	タンパー応答及びゼロ化回路の付いたタンパー検出/応答包被

通常、セキュリティレベル 1 は、最小限の物理的保護を要求している。セキュリティレベル 2 では、タンパー証跡メカニズムの追加を要求している。セキュリティレベル 3 では、除去可能なカバー及びドアに対して、タンパー検出及びタンパー応答メカニズム付きの強固な囲いの使用の要求事項を追加している。セキュリティレベル 4 では、囲い全体に対して、タンパー検出及びタンパー応答メカニズム付きの強固な囲いの使用の要求事項を追加している。環境故障保護 (EFP) 又は環境故障試験 (EFT) はセキュリティレベル 4 で要求されている。タンパー検出及びタンパー応答は、タンパー証跡の代わりにはならない。

暗号モジュールが(例えば、暗号モジュールベンダによる、又はその他の認可された個人による)物理的なアクセスを許容するように設計されている場合には、メンテナンスアクセスインタフェースに対してセキュリティ要求事項が規定されている。

7.5.1 共通の物理的セキュリティの要求事項

次の要求事項は、すべての物理的な形態に対して適用しなければならない。

- 文書は、物理的な形態及び暗号モジュールの物理的セキュリティのメカニズムが実装されるセキュリティレベルを示さなければならない。
- 暗号モジュールが、暗号モジュールの内容への物理的アクセスを必要とするメンテナンス役割を含むか、又は暗号モジュールが物理的アクセス(例えば、暗号モジュールのベンダ又は他の認可された個人によるもの)を許すように設計されている場合には、次の事項を適用する。

- 1) メンテナンスアクセスインタフェースが定義されなければならない。

- 2) メンテナンスアクセスインタフェースは、あらゆる除去可能なカバー又はドアを含む、暗号モジュールの内容へのすべての物理アクセス経路を含んでいなければならない。
- 3) メンテナンスアクセスインタフェース内に含まれるあらゆる除去可能なカバー又はドアは、適切な物理的セキュリティメカニズムを用いて保護されなければならない。
- 4) メンテナンスアクセスインタフェースがアクセスされたとき、すべての CSP はゼロ化されなければならない。

セキュリティレベル 1

次の要求事項は、セキュリティレベル 1 のすべての暗号モジュールに適用しなければならない。

- a) 暗号モジュールは、表面安定化処理（例えば、環境又はその他の物理的損害から保護するために、暗号モジュールの回路に施されている絶縁保護コーティング又はシーリングコート。）を含んだ製品グレードの構成要素で構成されなければならない。
- b) 物理メンテナンスを行うとき、暗号モジュール内に含まれるすべての CSP はゼロ化されなければならない。そのゼロ化は、オペレータによって手続的に行われるか、又は暗号モジュールによって自動的に行われなければならない。

セキュリティレベル 2

セキュリティレベル 1 の共通の要求事項に加え、次の要求事項はセキュリティレベル 2 のすべての暗号モジュールに適用しなければならない。

- a) 物理的なアクセスが暗号モジュールに試みられたとき、暗号モジュールは（例えば、カバー、囲い及びシールに）タンパーされた証跡を提供しなければならない。

セキュリティレベル 3

セキュリティレベル 1 及び 2 の共通の要求事項に加え、次の要求事項はセキュリティレベル 3 のすべての暗号モジュールに適用しなければならない。

- a) 暗号モジュールがドア若しくは除去可能なカバーを含むか、又はメンテナンスアクセスインタフェースが定義されている場合には、暗号モジュールはタンパー応答及びゼロ化機能を含まなければならない。そのタンパー応答及びゼロ化機能は、ドアを開けられたとき、カバーが取り外されたとき、又はメンテナンスアクセスインタフェースがアクセスされたとき、すべての CSP を速やかにゼロ化しなければならない。そのタンパー応答及びゼロ化機能は、CSP が暗号モジュール内に含まれているときは、作動していなければならない。
- b) 暗号モジュールが通気孔又はスリットを含む場合には、通気孔又はスリットは、囲いの内部に対する、検出されない物理的なプロービングを妨げるような構造でなければならない（例えば、少なくとも一つ以上の 90 度の曲げ、又は堅固な保護素材による障害物を必要とする。）。

セキュリティレベル 4

セキュリティレベル 1, 2 及び 3 の共通の要求事項に加え、暗号モジュールは、セキュリティレベル 4 のために 7.5.2 で規定された、環境故障保護(EFP)特性を含むか、又は環境故障試験(EFT)を受けなければならない。

7.5.1.1 シングルチップ暗号モジュール

7.5.1 に規定された一般的なセキュリティ要求事項に加え、シングルチップ暗号モジュールに特有の要求事項を次に示す。

セキュリティレベル 1

シングルチップ暗号モジュールに対するセキュリティレベル 1 の追加要求事項はない。

セキュリティレベル 2

セキュリティレベル 1 の要求事項に加え、次の要求事項は、セキュリティレベル 2 のシングルチップ暗号モジュールに適用しなければならない。

- a) 暗号モジュールは、暗号モジュールへの直接的な観察、プロービング、又は不正操作を防ぐために、及びタンパーの試みの証拠又は暗号モジュールの除去証拠を提供するために、タンパー証拠を残すコーティング（例えば、タンパー証拠を残す表面安定化処理の材料、又は表面安定化処理を覆うタンパー証拠を残す材料）で覆われているか、又はタンパー証拠を残す囲い内に含まれていなければならない。
- b) タンパー証拠を残すコーティング、又はタンパー証拠を残す囲いは、可視光領域内（すなわち、波長が 400 nm～750 nm の範囲の光）においては不透明でなければならない。

セキュリティレベル 3

セキュリティレベル 1 及び 2 の要求事項に加え、次のいずれかの要求事項を、セキュリティレベル 3 のシングルチップ暗号モジュールに適用しなければならない。

- a) 暗号モジュールは、堅く不透明なタンパー証拠を残すコーティング（例えば、表面安定化処理を覆った堅く不透明なエポキシ樹脂）で覆われていなければならない。
- b) 暗号モジュールの囲いは、その除去又は貫通の攻撃が高い確率で暗号モジュールに重大な損害を与える（すなわち、暗号モジュールが機能しなくなる。）ように設計されていなければならない。

セキュリティレベル 4

セキュリティレベル 1, 2 及び 3 の要求事項に加え、次の要求事項はセキュリティレベル 4 のシングルチップ暗号モジュールに適用しなければならない。

- a) 暗号モジュールは、暗号モジュールからコーティングをはがそうとする試み、又はこじ開けようとする試みが、高い確率で暗号モジュールに重大な損害を与える（すなわち、暗号モジュールが機能しなくなる。）ような硬度及び接着特性をもった、堅く不透明で除去耐性のあるコーティングで覆われていなければならない。
- b) 除去耐性のあるコーティングは、コーティングの溶解が、高い確率で暗号モジュールを溶解する、又は暗号モジュールに重大な損害を与える（すなわち、暗号モジュールが機能しなくなる。）ような溶解特性をもたなければならない。

7.5.1.2 マルチチップ組込型暗号モジュール

7.5.1 に規定された一般的なセキュリティ要求事項に加え、マルチチップ組込型暗号モジュールに特有の要求事項を次に示す。

セキュリティレベル 1

暗号モジュールが、囲い又は除去可能なカバー内に含まれる場合には、製品グレードの囲い又は除去可能なカバーが使用されなければならない。

セキュリティレベル 2

セキュリティレベル 1 の要求事項に加え、次のいずれかの要求事項を、セキュリティレベル 2 のマルチチップ組込型暗号モジュールに適用しなければならない。

- a) 暗号モジュール構成要素は、暗号モジュール構成要素への直接的な観察、プロービング、又は不正操作を防ぐために、及びタンパーの試みの証拠、又は暗号モジュール構成要素の除去の証拠を提供するために、タンパー証拠を残すコーティング若しくは封止材（例えば、エッチング耐性のあるコーティング又は厚い塗装）で覆われていなければならない。

そのタンパー証跡を残すコーティング又はタンパー証跡を残す囲いは、可視光領域内において不透明でなければならない。

- b) 暗号モジュールは、金属製又は堅いプラスチック製の製品グレードの囲い内に完全に含まれていなければならない。これらは、ドア又は除去可能なカバーを含んでもよい。

その囲いは、可視領域内において不透明でなければならない。また、その囲いが、ドア又は除去可能なカバーを含む場合には、ドア又はカバーは、物理的若しくは論理的鍵を用いたこじ開け耐性のある機械的錠が掛けられているか、又はそのドア若しくはカバーは、タンパー証跡を残すシール（例えば、証跡性テープ又はホログラフシール）で保護されていなければならない。

セキュリティレベル 3

セキュリティレベル 1 及び 2 の要求事項に加え、次のいずれかの要求事項を、セキュリティレベル 3 のマルチチップ組込型暗号モジュールに適用しなければならない。

- a) 暗号モジュール内の回路のマルチチップ形態は、可視光領域内において不透明な堅いコーティング又は封止材（例えば、堅いエポキシ樹脂材料）で覆われていなければならない。
- b) マルチチップスタンドアロン型暗号モジュールに適用可能なセキュリティレベル 3 の要求事項が、適用されなければならない（7.5.1.3 参照）。

セキュリティレベル 4

セキュリティレベル 1, 2 及び 3 の要求事項に加え、次の要求事項は、セキュリティレベル 4 のマルチチップ組込型暗号モジュールに適用しなければならない。

- a) 暗号モジュール構成要素は、封止材によって覆われているか、又はタンパー検出包被によってカプセル化された囲い内に含まれていなければならない。タンパー検出包被は、CSP 及び／又は PSP へのアクセスを可能にする程度のタンパー（例えば、封止材又は囲いの切削、掘削、粉碎、研削、溶解）を検出しなければならない。

タンパー検出包被によるカプセル化の例には、曲がりくねった幾何学パタンの導電体をもつ柔軟なマイラプリント回路、巻き線型パッケージ、柔軟性がなく壊れやすい回路、又は堅固な囲いがある。

- b) 暗号モジュールは、タンパー応答及びゼロ化回路を含まなければならない。タンパー応答及びゼロ化回路は、タンパー検出包被を継続的に監視しなければならない。タンパーが検出されたときは、そのタンパー応答及びゼロ化回路は、速やかにすべての CSP をゼロ化しなければならない。そのタンパー応答回路は、平文の秘密鍵及びプライベート鍵、又はその他の保護されていない CSP が暗号モジュール内に含まれているときは、作動していなければならない。そのゼロ化機能は、CSP が暗号モジュール内に含まれているときは、作動していなければならない。

7.5.1.3 マルチチップスタンドアロン型暗号モジュール

7.5.1 に規定された一般的なセキュリティ要求事項に加え、マルチチップスタンドアロン型暗号モジュールに特有の要求事項を次に示す。

セキュリティレベル 1

セキュリティレベル 1 に対して、暗号モジュールは、金属製又は堅いプラスチック製の製品グレードの囲い内に完全に含まれていなければならない。これらは、ドア又は除去可能なカバーを含んでもよい。

セキュリティレベル 2

セキュリティレベル 1 の要求事項に加え、次の要求事項は、セキュリティレベル 2 のマルチチップスタンドアロン型暗号モジュールに適用しなければならない。

- a) 暗号モジュールの囲いは、可視光領域内において不透明でなければならない。

- b) 暗号モジュールの囲いが、ドア又は除去可能なカバーを含む場合には、ドア又はカバーは、物理的若しくは論理的な鍵を用いたこじ開け耐性のある機械的錠が掛けられているか、そのドア又はカバーは、タンパー証跡を残すシール（例えば、証跡性テープ又はホログラフシール）で保護されていなければならない。

セキュリティレベル 3

セキュリティレベル 1 及び 2 の要求事項に加え、次のいずれかの要求事項を、セキュリティレベル 3 のマルチチップスタンドアロン型暗号モジュールに適用しなければならない。

- a) 暗号モジュール内の回路のマルチチップ形態は、可視光領域内において、不透明な堅い封止材（例えば、堅いエポキシ樹脂材料）で覆われていなければならない。
- b) 暗号モジュールは、囲いの除去又は貫くことの試みが、高い確率で、暗号モジュールに対し重大な損害を与える（すなわち、暗号モジュールが機能しなくなる）ような強固な囲い内に含まれていなければならない。

セキュリティレベル 4

セキュリティレベル 1, 2 及び 3 の要求事項に加え、次の要求事項は、セキュリティレベル 4 のマルチチップスタンドアロン型暗号モジュールに適用しなければならない。

- a) 暗号モジュールは、タンパー検出包被によって、すなわち、カバースイッチ（カバースイッチの例には、マイクロスイッチ、磁気ホール効果スイッチ、永久磁石アクチュエータなどがある。）、モーション検出器（モーション検出器の例には、超音波、赤外線、又は電磁波がある。）、又は前述のマルチチップ組込型暗号モジュールで記述されたその他のタンパー検出メカニズムのようなタンパー検出メカニズムの使用によって、カプセル化されなければならない。そのタンパー検出メカニズムは、平文の秘密鍵及びプライベート鍵、並びにその他の保護されていない CSP にアクセスするのに十分なタンパー（封止材又は囲いの切削、掘削、粉碎、研削、又は溶解のような方法による）を検出しなければならない。
- b) 暗号モジュールはタンパー応答及びゼロ化機能を含まなければならない。タンパー応答及びゼロ化回路は、タンパー検出包被を継続的に監視して、タンパーを検出したとき、速やかに、すべての CSP をゼロ化しなければならない。そのタンパー応答機能は、CSP 及び／又は PSP が暗号モジュール内に含まれているときは、作動していなければならない。そのゼロ化機能は、CSP が暗号モジュール内に含まれているときは、作動していなければならない。

7.5.2 環境故障保護・環境故障試験

電子デバイス及び電子回路は、特定の環境条件の範囲内において動作するように設計されている。電圧及び温度が規定された正規の動作範囲外に故意又は偶然に外れることは、電子デバイス又は電子回路の異常な動作又は故障を引き起こし、暗号モジュールのセキュリティを危たい化させる可能性がある。暗号モジュールのセキュリティが極度の環境条件によって危たい化されないという合理的保証は、暗号モジュールが環境故障保護 (EFP) をもつか、又は環境故障試験 (EFT) を受けることによって提供することができる。

セキュリティレベル 1, 2 及び 3 において、暗号モジュールは、環境故障保護 (EFP) 特性をもつこと、又は環境故障試験 (EFT) を受けることを要求されない。セキュリティレベル 4 において、暗号モジュールは、環境故障保護 (EFP) 特性を用いるか、又は環境故障試験 (EFT) を受けなければならない。

7.5.2.1 環境故障保護特性 (選択 1)

環境故障保護 (EFP) 特性は、暗号モジュールのセキュリティを危たい化させる可能性がある異常な環境

条件又は暗号モジュールの正規の動作範囲外の（偶然又は故意の）環境変動に対して、暗号モジュールを保護しなければならない。

暗号モジュールは監視を行って、規定された正規の動作範囲外の動作温度及び動作電圧における変動に対し、正しく応答しなければならない。

EFP 特性は、暗号モジュールの動作温度及び動作電圧を継続的に測定する電子的な機能又はデバイスをもたなければならない。温度又は電圧が、暗号モジュールの正規の動作範囲外になる場合には、保護機能は、(1) それ以上動作しないように暗号モジュールをシャットダウンするか、又は (2) すべての CSP を、即座にゼロ化しなければならない。

ベンダが提供する文書は、暗号モジュールの正規の動作範囲及び暗号モジュールによって用いられる環境故障保護特性を示さなければならない。

7.5.2.2 環境故障試験手順（選択 2）

温度及び電圧に関して暗号モジュールの正規の動作範囲外の（偶然又は故意の）環境条件又は環境変動が、暗号モジュールのセキュリティを危たい化しないという合理的保証を提供するために、環境故障試験 (EFT) は、暗号モジュールの解析、シミュレーション及び試験の組合せを含まなければならない。

動作温度又は動作電圧が暗号モジュールの正規の動作範囲外となり、その結果、故障が発生する場合には、EFT は、暗号モジュールのセキュリティが決して危たい化されないことを実証しなければならない。

試験する温度範囲は、通常動作温度範囲から始めて温度を下げていったとき、(1) さらなる操作を阻止するようにシャットダウンする、又は、(2) 即座にすべての CSP をゼロ化する、のいずれかが起こる温度までとしなければならない。また、通常動作温度範囲から始めて温度を上げていったとき、(1) さらなる操作を阻止するようにシャットダウンする、又は、(2) 即座にすべての CSP をゼロ化する、のいずれかが起こる温度までとしなければならない。試験する温度範囲は、摂氏 $-100^{\circ}\sim+200^{\circ}$ （華氏 $-150^{\circ}\sim+400^{\circ}$ ）でなければならないが、しかしながら、(1) 暗号モジュールがさらなる操作を阻止するようにシャットダウンする、(2) すべての CSP が即座にゼロ化される、(3) 暗号モジュールが故障状態になる、のいずれかが起こると速やかに試験を中断しなければならない。

試験する電圧範囲は、さらなる操作を阻止するようにシャットダウン、又はすべての CSP の即座の無効化のいずれかが起こる、最小電圧から最大電圧までとしなければならない。また、正規の動作電圧範囲内で電圧の極性反転も行わなければならない。

ベンダが提供する文書は、暗号モジュールの正規の動作範囲及び行われる環境故障試験を示さなければならない。

7.6 動作環境

暗号モジュールの動作環境とは、暗号モジュールが動作するために必要なソフトウェア構成要素、ファームウェア構成要素及び／又はハードウェア構成要素の管理を指す。動作環境は、変更不可能（例えば、ROM に収められたファームウェア、入出力デバイスの機能が無効にしたコンピュータに収められたソフトウェア）であるか、又は変更可能（例えば、RAM に収められたファームウェア、はん用コンピュータで実行されるソフトウェア）である。オペレーティングシステムは、暗号モジュールの動作環境の重要なコンポーネントである。

はん用動作環境とは、次の機能をもつ市販のはん用オペレーティングシステム（すなわち、リソースマネジャー）を利用していることを指す。

- ・ 暗号境界内のソフトウェア構成要素及びファームウェア構成要素の管理。
- ・ ワードプロセッサのようなはん用アプリケーションソフトウェアを含むシステム及びオペレータプロ

セス・スレッドの管理。

この箇条では、次に示す二つの操作環境を規定している。それらは互いに明確に区別され、一方に対しては 7.6.1 への適合が要求され、もう一方に対しては要求されない。

- a) **限定動作環境** これは、はん用オペレーティングシステムをもたず、その上に動作環境がただ一つ存在する静的で変更不可能な仮想動作環境（例えば、プログラミング不可能な PC カード上での JAVA 仮想マシン）を指す。
- b) **変更可能な動作環境** これは、機能を追加、削除、変更するために再構成されてもよい動作環境及び／又ははん用オペレーティングシステムの能力（例えば、コンピュータの OS の使用、コンフィグレーション可能なスマートカードの OS の使用、プログラミング可能なファームウェアの使用）を含んでもよい動作環境を指す。ソフトウェア構成要素・ファームウェア構成要素がオペレータによって変更できる場合及び／又は暗号モジュールに、その暗号モジュールが認証機関によって認証される時点では含まれていなかったソフトウェア又はファームウェア（例えば、ワードプロセッサ）をオペレータがロード及び実行することができる場合には、オペレーティングシステムは、変更可能な動作環境であるとみなされる。

動作環境が変更可能な動作環境である場合には、7.6.1 のオペレーティングシステム要求事項を適用しなければならない。

動作環境が変更不可能な場合又は限定動作環境である場合には、7.6.1 のオペレーティングシステム要求事項は適用しない。

文書は、暗号モジュールに対する動作環境を示さなければならない。該当する場合には、暗号モジュールに採用されるオペレーティングシステム、並びにセキュリティレベル 2, 3 及び 4 については、**附属書 C** に記載する承認された PP も含めて示さなければならない。

7.6.1 オペレーティングシステム要求事項

セキュリティレベル 1

次の要求事項は、セキュリティレベル 1 のオペレーティングシステムに対して適用しなければならない。

- a) セキュリティレベル 1 だけに適用される要求事項として、オペレーティングシステムは、単一オペレータ動作モードに限定されなければならない（すなわち、複数同時オペレータは明示的に除外される。）。
- b) セキュリティレベル 1 だけに適用される要求事項として、暗号モジュールは、暗号モジュールが実行中又は作動している間、他のプロセスからの CSP 及び／又は PSP へのアクセスを防止しなければならない。暗号モジュールによって引き起こされるプロセスは、暗号モジュールによって所有され、外部のプロセス・オペレータによっては所有されない。非暗号プロセスは、実行中の暗号モジュールへの割込み処理を行ってはならない。
- c) すべての暗号ソフトウェア及び暗号ファームウェアは、ソフトウェア及びファームウェアのソースコード及び実行可能コードが認可されていない開示及び変更から保護されるような形態でインストールされなければならない。
- d) 承認された完全性の技術（例えば、承認されたメッセージ認証コード、デジタル署名アルゴリズム）を用いた暗号メカニズムは、暗号モジュール内のすべての暗号ソフトウェア構成要素及び暗号ファームウェア構成要素に対して適用されなければならない。承認された認証技術がソフトウェア・ファームウェア完全性テスト（7.8.1 参照）に採用される場合には、この暗号メカニズムの要求事項は、そのテストの一部として組込まれてもよい。

セキュリティレベル 2

セキュリティレベル 1 に適用される要求事項で他のレベルにも適用可能なもの（すなわち上記のセキュリティレベル 1 における c 及び d）に加え、次の要求事項もまたセキュリティレベル 2 に適用しなければならない。

- a) すべての暗号ソフトウェア及び暗号ファームウェア、CSP、PSP、並びに制御情報及び状態情報は、**附属書 C** に記載する PP に規定された機能要件を満たし、かつ、**ISO/IEC 15408** の評価保証レベル EAL2 で評価されたオペレーティングシステムの制御下に置かれなければならない。
- b) 平文データ、暗号ソフトウェア及び暗号ファームウェア、CSP、並びに PSP を保護するため、オペレーティングシステムの任意アクセス制御メカニズムは、次の役割が果たせるように構成されていなければならない。
 - 1) 格納されている暗号ソフトウェア及び暗号ファームウェアの実行。
 - 2) 暗号境界内に格納されている、次の暗号モジュールのソフトウェア構成要素又はファームウェア構成要素の変更（書き込み、置換及び削除）。
 - ・ 暗号プログラム
 - ・ 暗号データ（例えば、監査データ）
 - ・ CSP
 - ・ PSP
 - ・ 平文データ
 - 3) 暗号境界内に格納されている次の暗号ソフトウェア構成要素の読み取り。
 - ・ 暗号データ（例えば、監査データ）
 - ・ CSP
 - ・ 平文データ
 - 4) CSP 及び／又は PSP の入力。
- c) オペレーティングシステムは、すべてのオペレータ及び実行中のプロセスが、実行中の暗号プロセス（すなわち、ロードされて、実行中の暗号プログラムのコピー。）の変更を行うことを防がなければならない。この場合、実行中のプロセスとは、暗号プロセス又は非暗号プロセスにかかわらず、すべての非オペレーティングシステムのプロセス（すなわち、オペレータに開始されたプロセス）を指す。
- d) オペレーティングシステムは、オペレータ及び実行中のプロセスが、暗号境界内に格納されている暗号ソフトウェアの読み出しを行うことを防がなければならない。
- e) オペレーティングシステムは、暗号データ、CSP 及び PSP の変更、アクセス、削除及び追加を記録する監査メカニズムを提供しなければならない。
 - 1) 監査メカニズムは、次のイベントを記録しなければならない。
 - ・ クリプトオフィサ機能に対する無効な入力の試み。
 - ・ クリプトオフィサ役割へのオペレータの追加、又はクリプトオフィサ役割からのオペレータの削除。
 - 2) 監査メカニズムは、次のイベントの監査ができなければならない。
 - ・ 監査証跡に格納された監査データを処理する操作。
 - ・ 認証データ管理メカニズムの使用要求。
 - ・ セキュリティに関係するクリプトオフィサ機能の使用。
 - ・ 暗号モジュールに関するユーザ認証データへのアクセス要求。
 - ・ 暗号モジュールに関する認証メカニズム（例えば、ログイン）の使用。

- ・ クリプトオフィサ役割を担う明示的な要求。
- ・ クリプトオフィサ役割への機能の割当て。

3) 保存された監査データは認可されてないアクセスから保護されなければならない。

セキュリティレベル 3

セキュリティレベル 1 及び 2 の適用可能な要求事項に加え、次の要求事項は、セキュリティレベル 3 に適用しなければならない。

- a) すべての暗号ソフトウェア及び暗号ファームウェア、CSP、PSP、並びに制御情報及び状態情報は、**附属書 C** に記載する PP に規定された機能要件を満たすオペレーティングシステムの制御下に置かれなければならない。そのオペレーティングシステムは、**ISO/IEC 15408** の評価保証レベル EAL3 及び次の追加要求事項を含めて評価されなければならない。
- ・ 高信頼パス(FTP_TRP.1)及び非形式的な TOE セキュリティ方針モデル(ADV_SPM.1)
- b) すべての CSP、制御入力及び状態出力は、高信頼メカニズム（例えば、専用の入出力物理ポート、高信頼パス）を介して通信されなければならない。高信頼パスが使用される場合には、TOE セキュリティ機能(TSF)は、TSF からオペレータへの明確な接続が要求されたとき、TSF とオペレータとの間の高信頼パスをサポートしなければならない。この高信頼パスを介する通信は、オペレータ又は TSF によって排他的に活性化されて、他のパスから論理的に分離されなければならない。
- c) セキュリティレベル 2 の監査要求事項に加え、次のイベントが、監査メカニズムによって記録されなければならない。
- 1) 高信頼パス機能の利用の試み
 - 2) 高信頼パスの起動者及び対象の識別
 - 3) 自己テストの失敗
 - 4) タンパー検出の通知

セキュリティレベル 4

セキュリティレベル 1, 2 及び 3 の適用可能な要求事項に加え、更に次の要求事項もセキュリティレベル 4 のオペレーティングシステムに適用しなければならない。

- a) すべての暗号ソフトウェア、CSP、PSP、並びに制御情報及び状態情報は、**附属書 C** に記載する PP に規定された機能要件を満たすオペレーティングシステムの制御下に置かれなければならない。そのオペレーティングシステムは、**ISO/IEC 15408** の評価保証レベル EAL4 において評価されなければならない。

7.7 暗号鍵管理

暗号鍵管理に対するセキュリティ要求事項は、暗号モジュールによって採用される CSP、PSP のライフサイクル全体を包含している。鍵管理は、乱数ビット列生成及び鍵生成、鍵確立、鍵配送、鍵入出力、鍵の格納、並びに鍵のゼロ化を含んでいる。ある暗号モジュールはまた、他の暗号モジュールの鍵管理機能を採用してもよい。暗号化された CSP は、承認された暗号アルゴリズム又は承認されたセキュリティ機能を用いて暗号化された CSP を指す。

注記 承認されていない暗号アルゴリズム又は非公開の暗号アルゴリズム若しくは方法を用いて暗号化された CSP は、この規格の適用範囲内では、平文形式とみなされる。

CSP は、暗号モジュール内において、認可されていない開示、変更及び置換から保護されなければならない。PSP は、暗号モジュール内において、認可されていない変更及び置換に対し保護されなければならない。

ない。

文書は、暗号モジュールに用いられるすべての CSP, PSP を示さなければならない。

7.7.1 乱数ビット列生成器(RBG)

暗号モジュールは乱数ビット列生成器(RBG)を、複数の RBG の連鎖、又は単体で採用してもよい。すべての RBG 及びその使用方法が定義されなければならない。暗号モジュールが、承認された動作モードにおいて、承認された RBG 又は複数の RBG の連鎖を用いる場合には、次を満たさなければならない。

- RBG のエントロピーソースは 7.8.1 で規定された RBG エントロピー試験を受けなければならない。
- RBG の決定論的構成要素は 7.8.1 の暗号アルゴリズム試験を受けなければならない。
- RBG からのデータ出力は、7.8.2 で規定されたような連続乱数ビット列生成器試験に合格しなければならない。

RBG 及びその動作モードは、ISO/IEC 18031 に適合しなければならない。

7.7.2 鍵生成

暗号モジュールは内部で暗号鍵を生成してもよい。承認された暗号アルゴリズム又は承認されたセキュリティ機能に使用するために、暗号モジュールによって生成される暗号鍵は、承認された RBG を用いて、生成されなければならない。

鍵生成方法のセキュリティの危たい化（例えば、決定論的 RBG を初期化するためのシード値の推定）は、少なくとも、生成された鍵の値を決定するのと同じだけの操作を必要としなければならない。

シード鍵が鍵生成処理中に入力される場合には、鍵の入力は、7.7.4 に規定された鍵の入力の要求事項を満たさなければならない。中間の鍵生成値が、暗号モジュールから出力される場合には、その値は、(1) 暗号化された形式、又は (2) 知識分散の技術のもとで、出力されなければならない。

7.7.3 鍵確立

鍵確立は、承認された方法（例えば、公開鍵暗号アルゴリズムの使用）、手動の配送方法（手動で配送された鍵ローディングデバイスの使用）、又は電子化された方法と手動の配送方法との組合せによって行われてもよい。暗号モジュールが鍵確立の方法を用いている場合には、承認された鍵確立の技術だけが使用及び定義されなければならない。承認された鍵確立方法の例は、この規格の**附属書 E**に記載されている。

鍵確立の方法のセキュリティの危たい化（例えば、鍵確立に使用されるアルゴリズムのセキュリティの危たい化。）は、少なくとも、鍵配送又は鍵共有された暗号鍵の値を決定するのと同じだけの操作を必要としなければならない。

鍵配送の方法が用いられる場合には、鍵配送される暗号鍵は、7.7.4 の鍵の入出力の要求事項を満たさなければならない。鍵共有の方法が用いられる場合（例えば、暗号鍵が共有された中間値から導出される場合）には、共有された値は 7.7.4 の鍵入力・出力の要求事項を満たす必要はない。

7.7.4 鍵の入力及び出力

暗号モジュールは、外部から暗号鍵を入手してもよい（鍵の入力）。また、暗号モジュールは、暗号鍵を外部に出力してもよい。鍵の入力又は出力は、手動（例えば、キーボードを介して）又は電子化された方法（例えば、スマートカード、トークン、PC カード、他の電子鍵ローディングデバイス）のいずれかを用いて行われ、定義されなければならない。

シード鍵は、鍵生成中に入力される場合には、暗号鍵と同じ方法で入力されなければならない。

暗号モジュールへ入力又は暗号モジュールから出力され、かつ、承認された動作モードで使用される、すべての暗号化された秘密鍵及びプライベート鍵は、承認された暗号アルゴリズム（**附属書 D**に記載）を用いて、暗号化されなければならない。公開鍵は、平文の形式で、暗号モジュ

ールへ入力,又は暗号モジュールから出力されてもよく,完全性を保護されてもよい。暗号モジュールは,暗号モジュールへ入力又は暗号モジュールから出力される鍵(秘密鍵,プライベート鍵,又は公開鍵)を,鍵が割当てられている正しいエンティティの名称(例えば,人,グループ,プロセス)に関係づけなければならない。

手動で入力される暗号鍵は,暗号モジュールへの入力の間に,正確を期して 7.8.2 で規定された手動の鍵入力試験を用いて,検証されなければならない。鍵入力の間,手動で入力される値は,目視による確認を許すために及び正確さを向上させるために,一時的に表示されてもよい。暗号化された暗号鍵又は鍵要素が暗号モジュールに手動で入力される場合には,暗号鍵又は鍵要素の平文の値は,表示されてはならない。

セキュリティレベル 1 及び 2

電子化された方法を用いて配送された秘密鍵及びプライベート鍵は,暗号化された形式で,暗号モジュールへ入力及び暗号モジュールから出力されなければならない。手動の配送方法を用いて配送された秘密鍵及びプライベート鍵は,平文の形式で,暗号モジュールへ入力されるか,又は暗号モジュールから出力されてもよい。

セキュリティレベル 3 及び 4

次の要求事項は,セキュリティレベル 3 及び 4 における鍵の入出力の要求事項である。

- a) 電子化された方法を用いて配送された秘密鍵及びプライベート鍵は,暗号化された形式で,暗号モジュールへ入力及び暗号モジュールから出力されなければならない。
- b) 手動の配送方法を用いて配送された秘密鍵及びプライベート鍵は,(1)暗号化された形式又は(2)知識分散の技術(すなわち,二つ以上の平文の暗号鍵要素を用いる技術)を用いて,暗号モジュールへ入力又は暗号モジュールから出力されなければならない。
- c) 知識分散の手順が用いられる場合には,次の要求事項を満たさなければならない。
 - 1) 暗号モジュールは,それぞれの鍵要素を入力又は出力するオペレータを別々に認証しなければならない。
 - 2) 平文の暗号鍵要素の暗号モジュール入出力は,高信頼パス経由又は直接入出力のいずれかでなければならない。直接入出力とは,その鍵要素が不注意に格納,結合,又はその他の方法で処理される可能性のある,暗号モジュールを取り囲むシステム又は仲介するシステムを経由しないことを指す(7.2 参照)。
 - 3) 元の暗号鍵を再組立するために,少なくとも二つの鍵要素が要求されなければならない。
 - 4) 文書は, n 個の鍵要素の知識が元の鍵を再組立するのに必要とされる場合,いかなる $n-1$ 個の鍵要素の知識も長さ以外に元の鍵の情報を提供しないことを検証しなければならない。
 - 5) 文書は,暗号モジュールに用いられる手順を示さなければならない。

7.7.5 鍵の格納

暗号モジュール内に格納されている暗号鍵は,平文の形式又は暗号化された形式のいずれかで格納されなければならない。平文の秘密鍵及びプライベート鍵は,認可されていないオペレータに対して,暗号モジュールの外側からアクセス可能であってはならない。

暗号モジュールは,暗号モジュール内に格納されている暗号鍵(秘密鍵,プライベート鍵,又は公開鍵)と,鍵が割当てられている正しいエンティティの名称(例えば,人,グループ,プロセス)とを関係づけなければならない。

7.7.6 鍵のゼロ化

暗号モジュールは,CSP のすべてをゼロ化するための方法を提供しなければならない。

次の CSP にはゼロ化は要求されない。

- ・ 暗号化された CSP。
- ・ 暗号化されていないが、物理的又は論理的に保護された CSP であって、付加的に組込まれる、認証された暗号モジュール（この規格の要求事項を満たすもの）の中のもの。

認証プロキシであるプロセスに対して排他的に平文データを渡すために CSP が使用される場合、これらのゼロ化の要求事項を満たす必要はない。

注記 このような CSP の一例は、暗号モジュール初期化鍵である。

7.8 自己テスト

暗号モジュールが適切に機能することを確実にするため、暗号モジュールは、パワーアップ自己テスト及び条件自己テストを実行しなければならない。パワーアップ自己テストは、暗号モジュールが電源投入されたときに実行されなければならない。条件自己テストは、該当するセキュリティ機能又は動作（すなわち、自己テストを必要とするセキュリティ機能）が呼び出されるときに実行されなければならない。暗号モジュールは、この規格に規定されているテストに加え、その他のパワーアップ自己テスト又はその他の条件自己テストを実行してもよい。

暗号モジュールが自己テストを失敗した場合には、その暗号モジュールはエラー状態になり、かつ、エラーインジケータを出力しなければならない。エラーインジケータは状態出力インタフェースを通じて明示的に、又はその他のメカニズムを通じて暗黙のうちに出力されてもよい。暗号モジュールは、エラー状態の間は、いかなる暗号動作も実行してはならない。データ出力インタフェースを通るすべてのデータ出力は、エラー状態のときには抑止されなければならない。

文書は、次を示さなければならない。

- ・ パワーアップ自己テスト及び条件自己テストを含む、暗号モジュールによって実行される自己テスト。
- ・ 自己テスト失敗時に暗号モジュールが進み得るエラー状態。
- ・ 暗号モジュールがエラー状態から抜け出して、正規の動作を再開するために必要な条件及びアクション（すなわち、暗号モジュールのメンテナンス、又は修理を含んでもよい。）。

7.8.1 パワーアップ自己テスト

パワーアップ自己テストは、暗号モジュールが（電源オフ、リセット、リブートなどの後で）電源投入されたときに、その暗号モジュールによって実行されなければならない。パワーアップ自己テストは自動的に開始され、かつ、オペレータの介入を必要としてはならない。パワーアップ自己テストが完了したとき、その結果は“状態出力”インタフェースを通じて明示的に又は暗黙のうちに出力されなければならない。出力インタフェースを通るすべてのデータ出力は、パワーアップ自己テストが実行されるときには抑止されなければならない。

電源投入時にパワーアップ自己テストを実行することに加え、暗号モジュールは、暗号モジュールの定期的なテストのため、オペレータがオンデマンドでテストを開始することを許可しなければならない。リセット、リブート及び電源切断・投入は、パワーアップ自己テストをオンデマンドで開始することができる方法である。

暗号モジュールは次のパワーアップ自己テストを実行しなければならない。

- a) **暗号アルゴリズムテスト** 既知解を用いた暗号アルゴリズムテストは、暗号モジュールによって実装された、それぞれの承認された暗号アルゴリズムの暗号機能（例えば、暗号化、復号、認証）のすべてについて実行されなければならない。既知解テストは、正しい出力が既に知られているデータ上での暗号アルゴリズムを操作することを意味し、かつ、計算された出力と既に生成されている（既知解

の) 出力とを比較することを意味する。計算された出力が既知解と異なる場合には、既知解テストは失敗としなければならない。

与えられる入力値の集合に対して出力値が変化する暗号アルゴリズムは、既知解テストを用いてテストされるか、又は鍵ペア整合性テスト (7.8.2.1 参照) を用いてテストされなければならない。メッセージダイジェストアルゴリズムは独立した既知解テストをもつか、又は既知解テストが関係づけられた暗号アルゴリズムテストに含まれていなければならない。

暗号モジュールが同じ暗号アルゴリズムの二つの独立した実装を含んでいる場合には、既知解テストは省略されてもよいが、その二つの実装の出力を連続的に比較することで代替しなければならない。二つの実装の出力が等しくない場合は、暗号アルゴリズムテストは失敗としなければならない。

- b) **RBG エントロピーテスト** 暗号モジュールが承認された動作モードにおいて承認された RBG を用いる場合、暗号モジュールは、ISO/IEC 18031 に記載されている RBG エントロピーソースについての暗号ヘルステストを実行しなければならない。
- c) **ソフトウェア・ファームウェア完全性テスト** 誤り検出符号 (EDC) 又は承認された認証技術 (例えば、承認されたメッセージ認証コード、又はデジタル署名アルゴリズム) を用いるソフトウェア・ファームウェア完全性テストは、暗号モジュール内の、すべての認証されたソフトウェア及びファームウェア構成要素に対して、暗号モジュールが電源投入時に、適用されなければならない。ソフトウェア・ファームウェア完全性テストは、この規格のセキュリティ要求事項から除外されたあらゆるソフトウェア構成要素及びファームウェア構成要素には要求されない (7.1 参照)。計算された結果があらかじめ生成された結果と等しくない場合には、ソフトウェア・ファームウェア完全性テストは失敗としなければならない。

誤り検出符号 (EDC) が用いられる場合には、EDC は少なくとも 16 ビットの長さでなければならない。

注記 ソフトウェア・ファームウェア完全性テストは ROM に格納されたデータには適用しない。

- d) **重要機能テスト** 暗号モジュールが電源投入されたときに、パワーアップ自己テストの一部としてテストされなければならない、暗号モジュールのセキュアな動作にとって重要な、その他のセキュリティ機能があるかもしれない。特定の条件のもとで実行されるその他の重要なセキュリティ機能は、条件自己テストとしてテストされなければならない。

文書は暗号モジュールのセキュアな動作にとって重要なセキュリティ機能のすべてを示し、かつ、暗号モジュールによって実行される該当するパワーアップ自己テスト及び条件自己テストを識別しなければならない。

7.8.2 条件自己テスト

条件自己テストは、次に規定するとおりに実行されなければならない。

7.8.2.1 鍵ペア整合性テスト

承認された機能である鍵配送又はデジタル署名の生成及び検証に使用するために、暗号モジュールが非対称鍵を生成する場合には、既知解テストを利用してそれらの鍵の鍵ペア整合性が検証されなければならない。

7.8.2.2 手動鍵入力テスト

暗号鍵又は暗号鍵要素が暗号モジュール内に手動で入力される場合には、次の手動鍵入力テストが実行されなければならない。

- a) 暗号鍵又は暗号鍵要素は EDC が付けられているか、又は繰り返し入力を用いて入力されなければならない

ない。

- b) EDC が用いられる場合には、EDC は少なくとも 16 ビットの長さでなければならない。
- c) EDC を検証できない場合か、又は繰り返し入力が一致しない場合には、そのテストは失敗としなければならない。

7.8.2.3 連続乱数ビット列生成器テスト

暗号モジュールが、承認された動作モードにおいて承認された RBG を用いる場合には、暗号モジュールは、それぞれの RBG に対し、定常値にならないかどうかのテストをする次の連続乱数ビット列生成器テストを実行しなければならない。

- a) RBG へのそれぞれの呼出しが n ビット ($n > 15$) のブロックを生成する場合には、電源投入後、初期化後、又はリセット後に生成される最初の n ビットのブロックは使用されてはならないが、生成される次の n ビットのブロックと比較するために保存されなければならない。その後が続いて生成される n ビットのブロックのそれぞれは、前に生成されたブロックと比較されなければならない。二つの比較した n ビットのブロックが等しい場合には、そのテストは失敗としなければならない。
- b) RBG への呼出しのそれぞれが 16 ビット未満のビット列を生成する場合には、電源投入後、初期化後、又はリセット後に生成される（ある $n > 15$ に対して）最初の n ビットは使用されてはならないが、次に生成される n ビットとの比較のために保存されなければならない。その後が続いて生成される n ビットのそれぞれは、前に生成された n ビットと比較されなければならない。二つの比較された n ビット列が等しい場合には、そのテストは失敗としなければならない。

本テストは RBG の最小限のヘルステストだけを目的としており、乱数生成の品質にかかわるものではない。

RBG についての他のすべてのテストは、ISO/IEC 18031 に従って実行される。

7.8.2.4 バイパステスト

暗号モジュールが、暗号処理なしにサービスが提供される（例えば、暗号モジュールを通して平文を転送すること）バイパス機能を実装している場合には、暗号モジュール構成要素の単一の誤動作が意図しない平文の出力につながらないことを確実にするために、次のバイパステストを実行しなければならない。

暗号モジュールは、排他的なバイパスサービスと排他的な暗号サービスとの間で切替えが発生するとき、暗号処理を提供するサービスの正しい動作をテストしなければならない。

暗号モジュールがバイパスサービスと暗号サービスとを自動的に切替えることができ、暗号処理を伴う何らかのサービス及び暗号処理を伴わない何らかのサービスを提供する場合には、暗号モジュールは、切替え手順を管理するメカニズムが変更される時点（例えば、IP アドレスのソース・ディスティネーション表が変更される時点）で、暗号処理を提供するサービスの正しい動作をテストしなければならない。

切替え手順を管理するメカニズム又は論理を定め、文書化しなければならない。

7.9 設計保証

設計保証とは、暗号モジュールの設計、配置及び運用における最善の慣行（best practice）の使用を指し、次の二つを保証する。

- ・ 暗号モジュールの適切なテスト、構成、配付、設置及び開発。
- ・ 適切な操作ガイダンス文書の提供。

この箇条では、構成管理、配付及び運用、開発、並びに文書についてセキュリティ要求事項を規定する。

7.9.1 構成管理

この細分箇条では、構成管理システムに対するセキュリティ要求事項を規定する。構成管理は、機能要

求事項及び機能仕様が暗号モジュールの実装において実現されることの保証を提供する。

構成管理システムは、暗号境界内の暗号モジュール及び暗号モジュール構成要素に対して、並びに関係した暗号モジュールの文書に対して、実施されなければならない。暗号モジュール及び関係した文書を構成するそれぞれの構成アイテム（例えば、暗号モジュール、暗号モジュール構成要素、ユーザガイダンス、セキュリティポリシ、オペレーティングシステム）のそれぞれのバージョンは、一意の ID 番号が割当てられ、かつ、ラベル付けされなければならない。

構成管理システムは認可された変更だけが構成アイテムに対して行われる手段を提供しなければならない。

構成管理システムは、暗号モジュールの生成をサポートしなければならない。

構成管理システムは、認可された変更だけが暗号モジュールの実装表現に対して行われるように自動化された手段を提供しなければならない。

構成管理システムは暗号モジュールの生成をサポートする、自動化された手段を提供しなければならない。

構成管理システムは、すべての構成アイテムを一意に識別しなければならない。

構成リストは、暗号モジュールを形成するすべての構成アイテムを一意に識別しなければならない。

構成管理システムが構成管理計画に従って運用されていること、及び構成管理システムの下で効果的にすべての構成アイテムが継続的に維持されていることを証拠は示さなければならない。

構成アイテムのリストは、以前のセキュリティ欠陥とそれらの解決に関する情報を含まなければならない。

7.9.2 配付及び運用

この細分箇条では、暗号モジュールが、認可されたオペレータにセキュアに配付され、正確かつセキュアな方法で設置及び初期化されることの保証を提供するために、暗号モジュールのセキュアな配付、設置及び立上げに関するセキュリティ要求事項を規定する。

セキュリティレベル 1

文書は、暗号モジュールのセキュアな設置、初期化及び立上げに関する手順を示さなければならない。

セキュリティレベル 2, 3 及び 4

セキュリティレベル 1 の要求事項に加えて、文書は、認可されたオペレータに対して暗号モジュールのバージョンを配送及び配付している間、セキュリティを維持するために必要な手順を示さなければならない。

7.9.3 開発

この細分箇条では、機能的インタフェースから実装表現までのいろいろな抽象レベルにおいて、暗号モジュールのセキュリティ機能の表現についてのセキュリティ要求事項を規定する。開発は、暗号モジュールの実装が、暗号モジュールのセキュリティポリシ及び機能仕様に対応していることの保証を提供する。

機能仕様は、オペレータに見えるポート及びインタフェースの高位記述、並びに暗号モジュールの振る舞いの高位記述を指す。

開発セキュリティ文書は、その開発環境において暗号モジュール設計及び実装の機密性及び完全性を保護するために必要な、すべての物理的、手続的、人的及びその他のセキュリティ手段を記述しなければならない。

開発セキュリティ文書は、これらのセキュリティ手段が暗号モジュールの開発及びメンテナンスを通して適用される証拠を提供しなければならない。

実装に使用されるすべての開発ツールは、明確に識別されなければならない。

開発ツールの文書は、実装において用いられるすべての規定事項の意味を明確に定義しなければならない。

開発ツールの文書は、すべての実装関連任意選択事項の意味を明確に定義しなければならない。

セキュリティレベル 1

次の要求事項は、セキュリティレベル 1 の暗号モジュールに対して適用しなければならない。

- a) 文書は、暗号モジュールのハードウェア構成要素、ソフトウェア構成要素及びファームウェア構成要素の設計と暗号モジュールのセキュリティポリシーとの対応を示さなければならない (7.1 参照)。
- b) 暗号モジュールがソフトウェア構成要素又はファームウェア構成要素を含む場合には、文書は、構成要素と暗号モジュールの設計との対応を明確に表現するコメントの形で注釈をつけた、ソフトウェア構成要素及びファームウェア構成要素のソースコードを示さなければならない。
- c) 暗号モジュールがハードウェア構成要素を含む場合には、文書は、ハードウェア構成要素の回路図及び／又はハードウェア記述言語(HDL)のソースコードを示さなければならない。

セキュリティレベル 2

セキュリティレベル 1 の要求事項に加えて、次の要求事項は、セキュリティレベル 2 の暗号モジュールに適用しなければならない。

文書は、暗号モジュール、暗号モジュールの外部ポート及び外部インタフェース、並びにそのインタフェースの目的を非形式的に記述した機能仕様を示さなければならない。

セキュリティレベル 3

セキュリティレベル 1 及び 2 の要求事項に加えて、次の要求事項は、セキュリティレベル 3 の暗号モジュールに適用しなければならない。

暗号モジュール内のすべてのソフトウェア構成要素及びファームウェア構成要素は、高級言語を用いて実装されなければならない。ただし、暗号モジュールの性能に不可欠な場合か、又は高級言語が利用できない場合には、低級言語（例えば、アセンブラ言語、マイクロコード）の限定された使用が許される。

HDL が使用される場合には、暗号モジュール内のすべてのハードウェア構成要素は、高級言語を用いて実装されなければならない。

セキュリティレベル 4

セキュリティレベル 1, 2 及び 3 の要求事項に加えて、次の要求事項は、セキュリティレベル 4 の暗号モジュールに適用しなければならない。

- a) 文書は、暗号モジュールのセキュリティポリシーのルール及び特徴を記述した形式的モデルを示さなければならない。形式的モデルは、一階述語論理又は集合論のような確立された数学に基づいた厳密な表記法である形式的仕様言語を用いて示さなければならない。
- b) 文書は、暗号モジュールのセキュリティポリシーについて、形式的モデルの一致及び完全性を実証する根拠を示さなければならない。
- c) 文書は、形式的モデルと機能仕様との対応に関する、非形式的な証明を示さなければならない。
- d) 暗号モジュールのそれぞれのハードウェア構成要素、ソフトウェア構成要素及びファームウェア構成要素に対して、ソースコードは、(1) 正しく実行するためにモジュール構成要素、関数、又は手続への入力に必要な事前条件、及び (2) モジュール構成要素、関数、又は手続の実行が完了するときに正しいと期待される事後条件、の二つを示すコメントを用いて注釈が付けられなければならない。事前条件及び事後条件は、暗号モジュール構成要素、関数、又は手続の振る舞いを完全、かつ、明快に、

説明するのに十分詳細な注釈を用いて示されてもよい。

- e) 文書は、(事前条件及び事後条件の注釈に記述された) 暗号モジュールの設計と機能仕様との一致に関する、非形式的な証明を示さなければならない。

注記 附属書 F に記載された推奨開発手順を用いた暗号モジュール内のソフトウェア構成要素及びファームウェア構成要素の実装は、その構成要素のこの規格の要求事項への適合性の解析を容易にし、設計誤りの機会を減らすとされる。

7.9.4 ガイダンス文書

クリプトオフィサガイダンスは、暗号モジュールの正しい構成、メンテナンス及び管理に関係している。ユーザガイダンスは、暗号モジュールのセキュアな使用に関する指示、ガイドライン及び警告と共に、暗号モジュールのセキュリティ機能を記述する。暗号モジュールがメンテナンス役割をサポートする場合には、ユーザガイダンス・クリプトオフィサガイダンスは、メンテナンス役割を担うオペレータに対する物理的な及び／又は論理的なメンテナンスサービスを記述する。

クリプトオフィサガイダンスには、次を定めておかなければならない。

- a) クリプトオフィサが利用可能な暗号モジュールの管理機能、セキュリティイベント、セキュリティパラメタ (及び、必要ならば、パラメタ値)、物理ポート及び論理インタフェース。
- b) どのように暗号モジュールをセキュアな手段で管理するかに関する手順。
- c) 暗号モジュールのセキュアな動作に関するユーザの振る舞いについての前提条件。

ユーザガイダンスには、次を定めておかなければならない。

- a) 暗号モジュールのユーザが利用可能な承認されたセキュリティ機能、物理ポート及び論理インタフェース。
- b) 暗号モジュールのセキュアな運用のために必要なすべてのユーザ責任。

7.10 その他の攻撃への対処

その他の攻撃に対する暗号モジュールの影響の受けやすさは、暗号モジュールのタイプ、実装及び実装環境に依存する。そのような攻撃は、敵意のある環境 (例えば、攻撃者が暗号モジュールの認可されたオペレータになるかもしれない環境) で実装される暗号モジュールでは特に注意を要すると考えられる。そのようなタイプの攻撃は、一般に、物理的に暗号モジュールの外部にある情報源から得られた情報の解析に依存する。すべての場合において、攻撃は、暗号モジュール内の暗号鍵及びその他の CSP についての、ある知識を決定しようとする。現在知られている攻撃の概要を**附属書 G**に記載する。

セキュリティレベル 1, 2, 3

セキュリティメカニズムが存在すること、それが適切に機能することは、要求事項及び関連テストの開発によって検証される。

セキュリティレベル 4

セキュリティレベル 4 ではその他の攻撃にも対処すると主張する場合、文書は、その追加されたセキュリティを検証するために必要となる適切な方法及び手段の仕様を含まなければならない。使用される対処方法をテストするためにテスト方法の仕様が用いられなければならない。

附属書 A

(規定)

文書化要求事項

A.1 目的

この附属書は、独立した検証又は評価を受ける暗号モジュールに対する最小限の文書化要求事項を規定している。

A.1.1 暗号モジュールの仕様

- a) 暗号モジュールのハードウェア、ソフトウェア及びファームウェアの構成要素の仕様。これらの構成要素を囲む暗号境界の仕様、並びに暗号モジュールの物理的な構成の記述。(セキュリティレベル 1・2・3・4)
- b) この規格のセキュリティ要求事項の適用を除外する暗号モジュールのハードウェア、ソフトウェア及びファームウェアの構成要素の仕様、並びに適用除外とする根拠の説明。(セキュリティレベル 1・2・3・4)
- c) 暗号モジュールの物理的ポート及び論理的インタフェースの仕様。(セキュリティレベル 1・2・3・4)
- d) 暗号モジュールの手動制御又は論理的制御、物理的又は論理的な状態表示、並びにそれらの物理的、論理的及び電気的な特徴の仕様。(セキュリティレベル 1・2・3・4)
- e) 承認されているかどうかにかかわらず、暗号モジュールに採用されるすべてのセキュリティ機能のリスト、並びに承認されているかどうかにかかわらず、すべての動作モードの仕様。(セキュリティレベル 1・2・3・4)
- f) 暗号モジュールの主要なハードウェア構成要素のすべて及びそれらの接続関係を示すブロック図。これには、マイクロプロセッサ、入出力バッファ、テキスト(平文又は暗号文)バッファ、制御バッファ、鍵格納メモリ、作業メモリ及びプログラムメモリを含む。(セキュリティレベル 1・2・3・4)
- g) 暗号モジュールのハードウェア、ソフトウェア及びファームウェアの構成要素の設計仕様。(セキュリティレベル 1・2・3・4)
- h) CSP、PSP 及び開示又は変更されると暗号モジュールのセキュリティに危たい化をもたらすその他の保護された情報(例えば、監査イベント、監査データ)を含む、すべてのセキュリティに関する情報の仕様。(セキュリティレベル 1・2・3・4)
- i) この規格の要求事項から導かれる規則及びベンダによって課された追加要求事項から導かれる規則を含む、暗号モジュールのセキュリティポリシーの仕様。(セキュリティレベル 1・2・3・4)

A.1.2 暗号モジュールのポート及びインタフェース

暗号モジュールの物理的ポート及び論理的インタフェース、並びに定義されたすべての入出力データパスの仕様。(セキュリティレベル 1・2・3・4)

A.1.3 役割、サービス、及び認証

- a) 暗号モジュールがサポートするすべての認可された役割の仕様。(セキュリティレベル 1・2・3・4)
- b) 暗号モジュールによって提供される(承認された及び承認されていない)、サービス、動作、又は機能の仕様。それぞれのサービスにおいて、サービス入力、それに対応するサービス出力及びそれらのサービスを実行できる認可された一つ以上の役割の仕様。(セキュリティレベル 1・2・3・4)
- c) オペレータが認可された役割を担うことなく受けられる暗号モジュールのサービスの仕様、並びにそ

これらのサービスによって、どのように CSP 及び／又は PSP が変更、開示、若しくは置換されないか、又はそうでなければ、暗号モジュールのセキュリティがどのように影響されないかの仕様。(セキュリティレベル 1・2・3・4)

- d) 暗号モジュールによってサポートされる認証メカニズム、サポートされた認証メカニズムを実装するために暗号モジュールによって要求される認証データのタイプ、最初の暗号モジュールへのアクセスを制御して認証メカニズムを初期化するために使用される認可された方法及びモジュールによってサポートされた対応する認証メカニズムの強度の仕様。(セキュリティレベル 2・3・4)

A.1.4 有限状態モデル

動作状態及びエラー状態のすべて、ある状態から別の状態への対応する遷移、ある状態から別の状態への遷移を引き起こす入力イベント（データ入力及び制御入力を含む）及びある状態から別の状態への遷移の結果起こる出力イベント（暗号モジュールの内部状態、データ出力及び状態出力を含む）を示す、状態遷移図及び／又は状態遷移表を用いた有限状態モデル（又は同等のもの）の表現。(セキュリティレベル 1・2・3・4)

A.1.5 物理的セキュリティ

- a) 物理的な形態及び暗号モジュールの物理的セキュリティのメカニズムが実装されるセキュリティレベルの仕様。暗号モジュールの物理的セキュリティのメカニズムの仕様。(セキュリティレベル 1・2・3・4)
- b) 暗号モジュールが、モジュールの内容への物理的アクセスを必要とするメンテナンス役割を含む場合、又はモジュールが物理的アクセスを許すように設計されている場合、メンテナンスアクセスインタフェースの仕様及びメンテナンスアクセスインタフェースがアクセスされたとき、CSP がどのようにゼロ化されるかの仕様。(セキュリティレベル 1・2・3・4)
- c) 暗号モジュールの正規の動作範囲の仕様。暗号モジュールによって用いられる環境故障保護特性の仕様、又は行われる環境故障試験の仕様。(セキュリティレベル 4)

A.1.6 動作環境

- a) 暗号モジュールの動作環境の仕様。(セキュリティレベル 1・2・3・4)
- b) 暗号モジュールに採用されるオペレーティングシステム、並びに該当するプロテクションプロファイル及び ISO/IEC 15408 保証レベルの識別。(セキュリティレベル 2・3・4)

A.1.7 暗号鍵管理

- a) 暗号モジュールに用いられるすべての CSP 及び PSP の仕様。(セキュリティレベル 1・2・3・4)
- b) 暗号モジュールに用いられる（承認された及び承認されていない）RBG のそれぞれの仕様。(セキュリティレベル 1・2・3・4)
- c) 暗号モジュールに用いられる（承認された及び承認されていない）鍵生成方法のそれぞれの仕様。(セキュリティレベル 1・2・3・4)
- d) 暗号モジュールに用いられる鍵確立の方法の仕様。(セキュリティレベル 1・2・3・4)
- e) 暗号モジュールに用いられる鍵の入出力方法の仕様。(セキュリティレベル 1・2・3・4)
- f) 知識分散の手順が用いられる場合には、 n 個の鍵要素の知識が元の鍵を再組立てするのに必要とされる際、いかなる $n-1$ 個の鍵要素の知識も長さ以外に元の鍵の情報を提供しないことの証明及び暗号モジュールに用いられる知識分散の手順の仕様。(セキュリティレベル 3・4)
- g) 暗号モジュールに用いられる鍵の格納方法の仕様。(セキュリティレベル 1・2・3・4)
- h) 暗号モジュールに用いられる鍵のゼロ化方法の仕様。(セキュリティレベル 1・2・3・4)

A.1.8 自己テスト

- a) パワーアップ自己テスト及び条件自己テストを含む、暗号モジュールによって実行される自己テストの仕様。(セキュリティレベル 1・2・3・4)
- b) 自己テスト失敗時に暗号モジュールが進み得るエラー状態、並びに、暗号モジュールがエラー状態から抜け出して、通常の動作を再開するために必要な条件及びアクションの仕様。(セキュリティレベル 1・2・3・4)
- c) 暗号モジュールのセキュアな動作にとって重要なセキュリティ機能のすべての仕様及びモジュールによって実行される該当するパワーアップ自己テスト及び条件自己テストの識別。(セキュリティレベル 1・2・3・4)
- d) 暗号モジュールがバイパス能力を実装している場合、切替え手順を管理するメカニズム又は論理の仕様。(セキュリティレベル 1・2・3・4)

A.1.9 設計保証

- a) 暗号モジュールのセキュアな設置、初期化、及び立上げに関する手順の仕様。(セキュリティレベル 1・2・3・4)
- b) 認可されたオペレータに対して暗号モジュールのバージョンを配送及び配付している間、セキュリティを維持するために必要な手順の仕様。(セキュリティレベル 2・3・4)
- c) 暗号モジュールのハードウェア構成要素、ソフトウェア構成要素、及びファームウェア構成要素の設計と暗号モジュールのセキュリティポリシ（すなわち動作のルール）との対応の仕様。(セキュリティレベル 1・2・3・4)
- d) 暗号モジュールがソフトウェア構成要素又はファームウェア構成要素を含む場合、構成要素とモジュールの設計との対応を明確に表現するコメントの注釈をつけた、ソフトウェア構成要素及びファームウェア構成要素のソースコードの仕様。(セキュリティレベル 1・2・3・4)
- e) 暗号モジュールがハードウェア構成要素を含む場合、ハードウェア構成要素の回路図及び／又はハードウェア記述言語(HDL) のソースコードの仕様。(セキュリティレベル 1・2・3・4)
- f) 暗号モジュール、暗号モジュールの外部ポート及び外部インタフェースの機能を非形式的に記述した仕様、並びにそのインタフェースの目的。(セキュリティレベル 2・3・4)
- g) 一階述語論理又は集合論のような確立された数学に基づいた厳密な表記法である形式仕様言語を用い、暗号モジュールのセキュリティポリシのルール及び特徴を記述した形式モデルの仕様。(セキュリティレベル 4)
- h) 暗号モジュールのセキュリティポリシについて、形式モデルの一貫性及び完全性を実証する根拠の仕様。(セキュリティレベル 4)
- i) 形式モデルと機能仕様との対応に関する、非形式的な証明の仕様。(セキュリティレベル 4)
- j) 暗号モジュールのそれぞれのハードウェア構成要素、ソフトウェア構成要素及びファームウェア構成要素に対して、(1) 正しく実行するために暗号モジュール、関数又は手続への入力に必要な事前条件及び (2) 暗号モジュール構成要素、関数、又は手続の実行が完了するときに正しいと期待される事後条件を示すコメントからなるソースコードの注解。(セキュリティレベル 4)
- k) (事前条件及び事後条件の注釈に記述された) 暗号モジュールの設計と機能仕様との一致に関する、非形式的な証明の仕様。(セキュリティレベル 4)
- l) クリプトオフィサガイダンス。これには、次の内容を含む。
 - ・ クリプトオフィサ向けに用意された暗号モジュールの管理機能、セキュリティイベント、セキュリティ

ィパラメタ（及び、必要ならば、パラメタ値）、物理ポート並びに論理インタフェース。（セキュリティレベル 1・2・3・4）

- ・ どのように暗号モジュールをセキュアなやり方で管理するかに関する手順。（セキュリティレベル 1・2・3・4）
- ・ 暗号モジュールのセキュアな運用に関係するユーザの振る舞いについての前提条件。（セキュリティレベル 1・2・3・4）

m) ユーザガイダンス。これには、次の内容を含む。

- ・ 暗号モジュールのユーザ向けに用意される承認されたセキュリティ機能、物理ポート及び論理インタフェース。（セキュリティレベル 1・2・3・4）
- ・ モジュールのセキュアな運用のために必要なすべてのユーザ責任。（セキュリティレベル 1・2・3・4）

A.1.10 その他の攻撃への対処

暗号モジュールが一つ以上の特定の攻撃に対処するように設計される場合、その攻撃に対処するために暗号モジュールに採用されるセキュリティメカニズムを記述した暗号モジュールのセキュリティポリシーの仕様。（セキュリティレベル 1・2・3・4）

A.1.11 セキュリティポリシー

セキュリティポリシーは、この規格の要求事項から導かれる規則及びアプリケーションによって課されたあらゆる追加の要求事項から導かれる規則が含まれる。（セキュリティレベル 1・2・3・4）

附属書 B は、暗号モジュールセキュリティポリシーの最低限の要求事項を規定している。

附属書 B

(規定)

暗号モジュールのセキュリティポリシー

B.1 目的

この附属書は、暗号モジュールセキュリティポリシーの最低限の要求事項を規定している。セキュリティポリシーは、この規格の要求事項から導かれる規則及びアプリケーションによって課せられたあらゆる追加の要求事項から導かれる規則を含まなければならない。

B.2 背景

暗号モジュールのセキュリティポリシーは、この規格の要求事項に基づくセキュリティルール及びモジュール開発を通じて課された付加的なセキュリティ規則を含む、暗号モジュールが動作中に従わなければならないセキュリティ規則の仕様から構成される。

その仕様は、次の質問に十分答えられるように詳述する。

- a) 暗号モジュールに含まれるすべての役割、サービス及びセキュリティに関連するデータに対して、役割 Z を担ってサービス Y を実行しているオペレータ X は、セキュリティに関連するデータ項目 W へのどのようなアクセスを行うか？
- b) 暗号モジュールを保護するためにどのようなセキュリティメカニズムが実装されているか、及び暗号モジュールの物理的セキュリティが維持されていることを確実にするためにどのような操作が必要か？
- c) 試験可能な要求事項がこの規格で定義されていない攻撃に対処するために、どのようなセキュリティメカニズムが、暗号モジュールに実装されているか？

B.3 目標

明確な暗号モジュールのセキュリティポリシーを開発し、従う目標は主に二つある。

- a) モジュールのセキュリティポリシーが提供するものは、暗号モジュールが実装されたとき、そのセキュリティポリシーを満足しているかどうかを個人及び組織が判定することができる暗号セキュリティの仕様である。
- b) モジュールのセキュリティポリシーは、暗号モジュールによって個人及び組織に提供される能力、防御、及びアクセス権を記述する。これによって、個人又は組織のセキュリティに対する要求に、モジュールが十分に役立つかどうかを判断できるようにしている。

B.3.1 識別・認証ポリシー

暗号モジュールのセキュリティポリシーは、次を含む識別・認証ポリシーを規定する。

- ・ すべての役割（例えば、ユーザ、クリプトオフィサ、及びメンテナンス）及び対応する認証のタイプ（例えば、ID ベース、役割ベース、又はなし）
- ・ それぞれの役割又はオペレータが必要な認証データ（例えば、パスワード又はバイオメトリクスデータ）及び対応する認証メカニズムの強度

B.3.2 アクセス制御ポリシー

暗号モジュールのセキュリティポリシーは、アクセス制御ポリシーを規定する。その仕様は、サービス実行

中に、オペレータがアクセス可能な CSP 及び PSP を識別するために、並びにオペレータがこれらのパラメータに対してもアクセスタイプを識別するために、十分に詳述する。

セキュリティポリシーは次を規定する。

- ・ 暗号モジュールにサポートされたすべての役割
- ・ 暗号モジュールに提供されるすべてのサービス
- ・ 暗号モジュールに採用されるすべての CSP 及び PSP, これらは次を含む
 - a) 秘密鍵, プライベート鍵及び公開鍵 (平文と暗号文の両方)
 - b) パスワード又は PIN のような認証データ
 - c) それ以外のセキュリティに関連する情報 (例えば, 監査イベント及び監査データ)
- ・ それぞれの役割において, オペレータがその役割の中で実行することを認可されたサービス。
- ・ それぞれの役割の中でのそれぞれのサービスにおいて, CSP 及び PSP へアクセスするタイプ。

B.3.3 物理的セキュリティポリシー

暗号モジュールのセキュリティポリシーは, 次を含む, 物理的セキュリティポリシーを規定する。

- ・ 暗号モジュールに実装される物理的セキュリティのメカニズム (例えば, タンパー証跡を残すシール, 錠, タンパー応答及びゼロ化スイッチ, 並びにアラーム)
- ・ 物理的セキュリティが維持されることを確実にするためにオペレータに要求されるアクション (例えば, タンパー証跡を残すシール及びゼロ化スイッチの定期検査)

B.3.4 その他の攻撃への対処ポリシー

暗号モジュールのセキュリティポリシーは, その他の攻撃に対処するために実装されたセキュリティメカニズムを含む, その他の攻撃に対処するためのセキュリティポリシーを規定する。

附属書 C

(規定)

承認されたプロテクションプロファイル

C.1 目的

この附属書は、この規格に適用可能な **ISO/IEC** が承認したプロテクションプロファイルのリストを提供する。

さらに、承認機関によって承認されたプロテクションプロファイル（P P）を使用してもよい。

- a) Controlled Access Protection Profile (CAPP), Version 1.d, Protection Profile NoPP006, October 1999.
(http://niap.bahialab.com/cc-scheme/pp/PP_CAPP_V1.d.cfm)

附属書 D

(参考)

承認されたセキュリティ機能

D.1 目的

この附属書は、この規格に適用できる承認されたセキュリティ機能を規定する、ISO/IEC が承認した規格のリストを提供する。カテゴリには、ブロック暗号、ストリーム暗号、非対称鍵、メッセージ認証コード、ハッシュ関数、エンティティ認証、鍵確立及び乱数ビット生成器が含まれる。このリストは、すべてを網羅するものではない。

このリストは承認機関が承認したセキュリティ機能の使用を排除しない。

D.1.1 ブロック暗号

- a) ISO/IEC 18033-3, Information technology—Security techniques—Encryption algorithms—Part 3: Block ciphers

D.1.2 ストリーム暗号

- a) ISO/IEC 18033-4, Information technology—Security techniques—Encryption algorithms—Part 4: Stream ciphers

D.1.3 非対称アルゴリズム及び技術

- a) ISO/IEC 9796-2, Information technology—Security techniques—Digital signature schemes giving message recovery—Part 2: Integer factorization based mechanisms
- b) ISO/IEC 9796-3, Information technology—Security techniques—Digital signature schemes giving message recovery—Part 3: Discrete logarithm based mechanisms
- c) JIS X 5061 (-1, -2, -3) セキュリティ技術—添付型デジタル署名
注記 対応国際規格：ISO/IEC 14888 (all parts), Information technology—Security techniques—Digital signatures with appendix (IDT)
- d) ISO/IEC 15946 (all parts), Information technology—Security techniques—Cryptographic techniques based on elliptic curves
- e) ISO/IEC 18033-2, Information technology—Security techniques—Encryption algorithms—Part 2: Asymmetric ciphers

D.1.4 メッセージ認証コード

- a) JIS X 5055-2 セキュリティ技術—メッセージ認証符号 (MACs) —第 2 部：専用ハッシュ関数を用いる機構
注記 対応国際規格：ISO/IEC 9797-2, Information technology—Security techniques—Message Authentication Codes (MACs)—Part 2: Mechanisms using a dedicated hash-function (IDT)

D.1.5 ハッシュ関数

- a) JIS X 5057-2 セキュリティ技術—ハッシュ関数—第 2 部：n ビットブロック暗号を用いるハッシュ関数
注記 対応国際規格：ISO/IEC 10118-2, Information technology—Security techniques—Hash-functions—Part 2: Hashfunctions using an n-bit block cipher (IDT)
- b) ISO/IEC 10118-3, Information technology—Security techniques—Hash-functions—Part 3: Dedicated

hash-functions

- c) **JIS X 5057-4** セキュリティ技術－ハッシュ関数－第4部：剰余演算を用いるハッシュ関数

注記 対応国際規格：ISO/IEC 10118-4, Information technology－Security techniques－Hash-functions－Part 4: Hash-functions using modular arithmetic (IDT)

D.1.6 エンティティ認証

- a) **JIS X 5056-2** セキュリティ技術－エンティティ認証－第2部：対称暗号アルゴリズムを用いる機構

注記 対応国際規格：ISO/IEC 9798-2, Information technology－Security techniques－Entity authentication－Part 2: Mechanisms using symmetric encipherment algorithms (IDT)

- b) **JIS X 5056-3** セキュリティ技術－エンティティ認証－第3部：デジタル署名技術を用いる機構

注記 対応国際規格：ISO/IEC 9798-3, Information technology－Security techniques－Entity authentication－Part 3: Mechanisms using digital signature techniques (IDT)

- c) **JIS X 5056-4** セキュリティ技術－エンティティ認証－第4部：暗号検出関数を用いる機構

注記 対応国際規格：ISO/IEC 9798-4, Information technology－Security techniques－Entity authentication－Part 4: Mechanisms using a cryptographic check function (IDT)

- d) **JIS X 5056-5** セキュリティ技術－エンティティ認証－第5部：ゼロ知識技術を用いる機構

注記 対応国際規格：ISO/IEC 9798-5, Information technology－Security techniques－Entity authentication－Part 5: Mechanisms using zero-knowledge techniques (IDT)

- e) **ISO/IEC 9798-6**, Information technology－Security techniques－Entity authentication－Part 6: Mechanisms using manual data transfer

- f) **JIS X 5058-2** セキュリティ技術－かぎ管理－第2部：対称暗号技術を用いるかぎ確立機構

注記 対応国際規格：ISO/IEC 11770-2, Information technology－Security techniques－Key management－Part 2: Mechanisms using symmetric techniques (IDT)

- g) **JIS X 5058-3** セキュリティ技術－かぎ管理－第3部：非対称暗号技術を用いるかぎ確立機構

注記 対応国際規格：ISO/IEC 11770-3, Information technology－Security techniques－Key management－Part 3: Mechanisms using asymmetric techniques (IDT)

- h) **ISO/IEC 11770-4**, Information technology－Security techniques－Key management－Part 4: Key establishment mechanisms based on weak secrets

D.1.7 乱数ビット生成器

- a) **ISO/IEC 18031**, Information technology－Security techniques－Random bit generation

附属書 E

(参考)

承認された鍵確立方法

E.1 目的

この附属書は、この規格に適用できる、**ISO/IEC** が承認した鍵確立方法のリストを提供する。このリストは承認機関が承認した鍵確立方法の使用を排除しない。このリストは、すべてを網羅するものではない。

E.1.1 鍵確立方法

- a) **JIS X 5058-2** セキュリティ技術—かぎ管理—第 2 部：対称暗号技術を用いるかぎ確立機構

注記 対応国際規格：**ISO/IEC 11770-2**, Information technology—Security techniques—Key management
—Part 2: Mechanisms using symmetric techniques (IDT)

- b) **JIS X 5058-3** セキュリティ技術—かぎ管理—第 3 部：非対称暗号技術を用いるかぎ確立機構

注記 対応国際規格：**ISO/IEC 11770-3**, Information technology—Security techniques—Key management
—Part 3: Mechanisms using asymmetric techniques (IDT)

- c) **ISO/IEC 15946-3**, Information technology—Security techniques—Cryptographic techniques based on elliptic curves—Part 3: Key establishment

附属書 F

(参考)

推奨ソフトウェア開発要領

F.1 目的

この附属書は、ソフトウェア開発における最良の慣行への手引きを与える。この附属書は、この規格が適用される暗号モジュールに対するセキュリティ要求事項を規定していない。

F.2 背景

ライフサイクルソフトウェアエンジニアリング(ソフトウェアの仕様、構造、検証、試験、メンテナンス、及び文書の扱い)の推奨は、次のようにするのが望ましい。ソフトウェアエンジニアリング手順は、文書化された単体試験、ソースコードレビュー、明示的な高位及び低位設計文書、明示的な要求及び機能仕様、構造チャート及びデータフロー図、ファンクションポイント解析、欠陥及び問題解決の追跡、構成管理、並びに文書化されたソフトウェア開発プロセスを含んでもよい。

大規模、小規模にかかわらず、すべてのソフトウェア開発において、次のプログラミング技術は現行の手順と一致している。暗号モジュールのソフトウェア構成要素の解析を容易にするために、及びプログラミングエラーの可能性を減らすために、これらの技術が使用されるのが望ましい。

F.3 モジュール化設計

モジュール化設計は、特に大規模ソフトウェアの開発労力を緩和するために推奨される。それぞれのソフトウェアモジュールは、明確で容易に理解される論理的インタフェースをもつのが望ましい。

ソフトウェア構成要素は、データ抽象化の原理を用いて構造化されなければならない。利用できる場合には、抽象データ型の構文をサポートするオブジェクト指向型高級言語が使用されるのが望ましい。

ソフトウェアは、一連の階層構造として構造化されるのが望ましい。

F.4 ソフトウェアモジュール・プロシージャインタフェース

ソフトウェアモジュール又は手続へのエントリは、明示的に定義されたインタフェース上で外部呼出しを通して行われるのが望ましい。

それぞれの手続は、一つの開始点及び多くとも二つの終了点(一つは正常終了で、一つはエラー終了)をもつのが望ましい。

データは、引数リスト及び／又は明示的な戻り値を用いて、ソフトウェアモジュール間及びプロシージャ間で通信されるのが望ましい。グローバル変数は、抽象データ型の実装に必要な場合を除いて、プロシージャ間で使用されないのが望ましい。使用するプログラミング言語で表明文(assertion statement)が使える場合、これを用いて、入力値及び出力値の範囲エラーチェックをすることが望ましい。

CSPが入力値として使用される場合、呼出し機能には、そのメモリアドレスによって通信されるのが望ましい。それによって取扱いに慎重さを要する情報の複製を防ぐ。

F.5 内部構造

それぞれのプロシージャは、単一で、明確な機能だけを実行するのが望ましい。

単スレッドの実行内の制御フローは、逐次構文、条件に対する構造化プログラミング構文(例えば、if-then-else 又は case)、及びループに対する構造化プログラミング構文(例えば、while-do 又は repeat-until)だけを用いて定義されるのが望ましい。

(例えば、マルチスレッド、マルチタスク、又はマルチプロセスによって)並列実行が採用される場合には、ソフトウェア構成要素は、許容される最大並列処理数に制限を設け、かつ、共有データへのアクセスを制御するために、構造化された同期化構文を使用するのが望ましい。

記憶領域共有は、目的が競合するメモリの多重使用を許すために用いないのが望ましい。

堅牢なコマンド構文解析及び範囲チェックメカニズムは、異常な要求、範囲外のパラメタ、及び入出力バッファオーバーフローに対して保護するために実装されるのが望ましい。

中間変数の使用(例えばメモリアロケーション)が、CSPを計算する手続によって要求される場合、ソフトウェア構成要素は、中間変数が使用後にゼロ化されることを保証するのが望ましい。

F.6 説明文の挿入

それぞれのソフトウェアモジュール、手続、及び主要なプログラミング構文は、実行する機能並びに(形式的な又は非形式的な)事前条件及び事後条件を記述するように文書化することが望ましい。

それぞれのループの前に、終了が保証されることが納得できる説明文(コメントとして)が記述されるのが望ましい。

変数名は、同じプロシージャの中で一つの意味にだけ使用されるのが望ましい。

すべての変数に対して、変数の目的及び許容値の範囲(制限されていない場合も含める。)を記述するコメントをもつことが望ましい。

並列処理が採用される場合には、文書は、許容される最大並列処理数がどのように制限されか、及び共有データへのアクセスが、(おそらく検出されない)実行時のエラーを避けるために、どのように同期化されるかを示すことが望ましい。

F.7 アセンブラ言語

実装がアセンブラ言語のときには、次のプログラミング慣行を用いることが望ましい。

- すべてのコードは、特定のセキュリティ上の目的、効率、又はハードウェア制限が位置に依存することを要求する場合を除いて、位置非依存が望ましい。
- すべてのレジスタ参照は、シンボリックレジスタ名を使用するのが望ましい。
- 自己変更コードは使用しないのが望ましい。
- すべてのプロシージャは、プロシージャ内で使用されるレジスタの内容を保存及び復旧する責任をもつのが望ましい。
- 制御遷移命令は、数値リテラルを使用しないのが望ましい。
- それぞれのユニットは、そのユニットにおけるレジスタの使用を記述するコメントを含むことが望ましい。

附属書 G

(参考)

その他の攻撃への対処の例

電力解析: 消費電力の解析に基づく攻撃は、一般に、単純電力解析(SPA)及び差分電力解析(DPA)の2種類に分けられる。SPAは、暗号モジュールによって暗号処理中に実行される個々の命令の実行から発生する消費電力のパターン及びタイミングの直接的な（主に目視による）解析をいう。そのパターンは、暗号アルゴリズムの特徴及び実装、並びにその後に暗号鍵の値を暴露する目的で、暗号モジュールの消費電力の変動を監視することを通して得られる。DPAは同じ目的であるが、暗号モジュールの消費電力の変動を解析するための、高度な統計的方法及び／又はその他の技術を活用する。外部の（直流）電源を利用する暗号モジュールは最も大きなリスクがあるとされる。電力解析攻撃の全体的なリスクを減らす方法には、消費電力を一定にするためのコンデンサの使用、内部電源の使用、及び暗号処理中の消費電力の割合を一定にするための暗号アルゴリズム又は暗号処理の個々の動作の調整が含まれる。

タイミング解析: タイミング解析攻撃は、暗号アルゴリズム又は暗号処理に関する特定の数学的操作を実行するために暗号モジュールに必要な時間を正確に測定することに依存する。収集されたタイミング情報は、暗号モジュールへの入力と暗号アルゴリズム又は暗号処理に使用される暗号鍵との関係を決定するために解析される。その関係の解析は、暗号鍵又はその他のCSPを暴露するためのタイミング測定を利用するために用いられる場合がある。タイミング解析攻撃は、攻撃者が暗号モジュールの設計の知識をもっていることを前提とする。暗号処理中のタイミング変動を減らすための暗号アルゴリズム又は暗号処理の個々の動作を調整することは、この攻撃のリスクを減らすための一つの方法である。

故障利用: 故障利用攻撃は、暗号モジュール内で処理エラーを引き起こすために、電磁波、温度限界、及び電圧の不正操作のような外部的な力を活用する。これらのエラー及びパターンの解析は、暗号アルゴリズムのある特徴及び実装を暴露したり、並びにその後に暗号鍵の値を暴露するために、暗号モジュールのリバースエンジニアリングの試みに使用される。限られた物理的セキュリティをもつ暗号モジュールは最大のリスクがあると考えられる。物理的セキュリティの特徴を適切に選択することは、この攻撃のリスクを減らすために使用される場合がある。