暗号モジュール評価基準第0.1版

平成17年3月

独立行政法人 情報処理推進機構

独立行政法人 情報通信研究機構

本資料の利用にあたって

本資料は、運用ガイダンス第0版の訳語との統一を図るために、2003年度に作成した暗号モジュール評価基準第0版(米国NIST[1]が発行する”FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, CHANGE NOTICE (12-03-2002)”の翻訳版)の訳語の見直しを行ったものである。

別冊の暗号モジュール試験基準第0.1版及び運用ガイダンス第0版をあわせてご参照いただけると幸いである。

[1] National Institute of Standards and Technology

目次

1．概要

この標準は、コンピュータシステム及び電気通信システム(音声システムを含む)内の、”the Information Technology Management Reform Act of 1996, Public Law 104-106 ” の 5131 節に定義された重要情報を保護するセキュリティシステムで利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。

FIPS140-1 は、政府及び産業界による、運営側及びベンダ側で構成されたワーキンググループによって開発された。ワーキンググループは、データの重要度の幅広さ(例えば、低価値の管理データ、百万ドル規模の資金振替、及び生命にかかわるデータ)と使用環境の多様性(例えば、保護された設備、オフィス、及び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、4 つのセキュリティレベルの要求事項を識別した。4 つのセキュリティレベルは、それぞれ 11 に分類される複数の要求事項から規定される。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。セキュリティが漸増していくこれら 4 つのレベルは、取り扱うデータの重要度の違いや異なる使用環境に対応した、費用対効果のある解決策を提供する。FIPS140-2 は、ベンダ、試験機関、及びユーザ団体から寄せられたコメントに基づいた変更だけでなく、FIPS140-1 が開発された以降に利用可能となった標準及び技術の変更も取り入れている。

この標準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、この標準へ適合することは、ある暗号モジュールがセキュアであることを保証するのに十分ではない。暗号モジュールのオペレータは、その暗号モジュールによって提供されるセキュリティが、保護される情報の所有者にとって十分かつ容認できること、及び保護される情報の所有者に、あらゆる残存リスクが認知されかつ受け入れられていることを保証する責任がある。

同様に、認証された暗号モジュールをコンピュータシステム又は通信システムで使用することは、そのシステム全体のセキュリティを保証するのに十分ではない。暗号モジュールの全体的なセキュリティレベルは、暗号モジュールが利用されるアプリケーション及び環境のセキュリティ要求事項、並びに暗号モジュールが提供するセキュリティサービスに対して適切なレベルで選択されなければならない。それぞれの組織の責任者は、暗号モジュールを利用しているコンピュータシステム及び通信システムが、与えられたアプリケーション及び環境に対して容認できるセキュリティレベルを提供することを保証すべきである。

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的優先事項にすることの重要性は、全てのユーザに周知させるべきである。情報セキュリティの要求事項は、異なるアプリケーションによって様々であるため、組織は、組織の情報資源を識別し、かつ損失を被る可能性と損失による潜在的な影響を決定すべきである。管理手段は、潜在的なリスクに基づいて行うべきであり、管理のためのポリシ及び手続き、物理的及び環境的な管理手段、情報及びデータの管理手段、ソフトウエアの開発及び調達の管理手段、並びにバックアップ及び緊急時対応計画を含む、利用可能な管理手段から選択されるべきである。

次の節は、4 つのセキュリティレベルの概要について述べる。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、制限を加え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。

Annex A, B, C, D がどこから入手できるかは, Appendix D：参考文献に掲載している。

1.1 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 1 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、製品レベル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汎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エアコンポーネント及びファームウエアコンポーネントを許可している。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、管理手続き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を必要とする何らかのアプリケーションに適している。ソフトウエアの暗号の実装は、ハードウエアベースのメカニズムを同じ狙いで実装するよりも費用対効果がよいため、低いレベルのセキュリティ要求事項を満たすための、ハードウエ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。

1.2 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、又は暗号モジュールが持つ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 の暗号モジュール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、暗号モジュールに付設され、暗号モジュール内の平文の暗号鍵及びクリティカルセキュリティパラメータ(以下 CSP 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､許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エアコンポーネント及びファームウエアコンポーネントが、次の 2 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汎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：

・Annex B に記載されたコモンクライテリア(CC)のプロテクションプロファイル(PP)で規定されている機能要件を満たし

・かつ、EAL2(またはそれ以上)の CC 評価保証レベルの評価を得たもの。

上記の条件と同等の評価を受けた信頼できるオペレーティングシステムを使用してもよい。信頼できるオペレーティングシステムは、汎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を、専用のハードウエアシステム上に実装された暗号モジュールと、信頼レベルの点で匹敵するものにする。

1.3 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、侵入者の暗号モジュール内の CSP に対するアクセス

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、頑丈な囲いの使用及び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、平文の CSP を全てゼロ化するタンパー証跡/タンパー応答をもつ回路を含んでもよい。

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さらに強化する。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、平文の CSP の入出力（知識分散手続きを利用した平文の 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、平文の 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移動してもよい)。

セキュリティレベル 3 では、暗号モジュールのソフトウエアコンポーネント及びファームウエアコンポーネントが、次の 2 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汎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：

・Annex B に記載された PP で規定される機能要件に追加して、高信頼パスの機能要件(FTP_TRP.1)をも満たし、

・かつ、EAL3（またはそれ以上）の評価保証レベルの評価を得て、さらに、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)を満たす評価を得たもの。

上記条件と同等の評価を受けた信頼できるオペレーティングシステムを使用してもよい。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エア又はファームウエアから、平文の CSP 並びに暗号モジュールのソフトウエアコンポーネント及びファームウエアコンポーネントを保護する。

1.4 セキュリティレベル 4

セキュリティレベル 4 は、この標準のなか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、全ての許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で保護するエンベロープを提供する。あらゆる方向からの暗号モジュールの筐体への侵入は、非常に高い確率で検出され、その結果、即座にすべての平文の 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および温度の範囲を超えた環境条件または環境変動による、セキュリティの危殆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邪魔するために、正規の動作範囲を意図的に越す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殆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エアコンポーネント及びファームウエアコンポーネントが、次の 2 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汎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し、

・かつ、EAL4(またはそれ以上)の CC 評価保証レベルの評価を得ていること。

上記条件と同等の評価を受けた信頼できるオペレーティングシステムを使用してもよい。

2．用語および略語集

2.1 用語集

次の定義が、この標準のなかで用いられる。

承認(Approved)
承認された：FIPS 承認の、及び/又は、NIST 推奨の

承認された動作モード(Approved mode of operation)
承認された動作モード：承認されたセキュリティ機能のみを採用した暗号モジュールのモード（DES CBC モードのような、承認されたセキュリティ機能の特定のモードと混同しないこと。）

承認されたセキュリティ機能(Approved security function)
この標準では、次のいずれかのセキュリティ機能(例　暗号アルゴリズム、暗号化鍵管理技術、認証技術)を指す。
a)承認された標準の中で規定されている機能
b)承認された標準の中で採用されており、承認された標準の Appendix 又は承認された標準が参照している文書に規定されている機能
c)承認されたセキュリティ機能のリストの中に規定されている機能

認証コード(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(メッセージ認証コードとしても良く知られている。)

自動化された鍵配送(Automated key transport)
コンピュータネットワークのような電子的手段を用いた、通常は暗号化された形での、暗号鍵の配送（例えば、鍵配送/鍵共有プロトコル）

危殆化(Compromise)
重要なデータ（平文の暗号鍵やその他の保護されていない CSP を含む）の許可されて

いない開示、変更、置換、又は使用

守秘性(Confidentiality)

守秘性：重要な情報が、許可されていない個人、エンティティ、又はプロセスに公開されない特性

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

クリティカルセキュリティパラメータ(Critical security parameter (CSP))

セキュリティに関する情報（例えば、秘密鍵及びプライベート鍵、並びにパスワード及び PIN のような認証データ）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殆化しうるもの。

暗号境界(Cryptographic boundary)

暗号モジュールの物理的な領域を確立し、かつ、暗号モジュールの全てのハードウエア、ソフトウエア、及び／又はファームウエアのコンポーネントをそのなかに含む、明確に定義された連続する境界線

暗号鍵(鍵)(Cryptographic key (key))

次を決定する、暗号アルゴリズムに関連して使用されるパラメータ

- 平文データから暗号文データへの変換
- 暗号文データから平文データへの変換
- デジタル署名の作成
- 作成されたデジタル署名の検証
- 認証コードの作成
- 共有された秘密情報の交換

暗号鍵コンポーネント(鍵コンポーネント)(Cryptographic key component (key component))

平文の暗号鍵の形成又は暗号機能を実行するために、承認されたセキュリティ機能において、他の鍵コンポーネントと一緒に使用されるパラメータ。

暗号モジュール(Cryptographic module)

承認されたセキュリティ機能(暗号アルゴリズム及び鍵生成を含む)を実装した、暗号境界内のハードウエア、ソフトウエア、及び/又はファームウエアの集合。

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

暗号モジュールが動作する上でのセキュリティルールの明確な仕様。これには、この標準の要求事項から導出されたルール及びベンダによって課せられた付加的ルールも含まれる。(Appendix C を参照のこと)

クリプトオフィサ(Crypto officer)

暗号の初期化又は管理機能を実行するオペレータ、又はそのオペレータのために働くプロセス（サブジェクト）

データパス(Data path)

データが通過する物理的または論理的な経路。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。

差分電力解析(DPA)(Differential power analysis(DPA))

暗号アルゴリズムで使用される暗号鍵に関連した情報を抽出するための、高度な統計的手法及び／又はその他の技術を用いた、暗号モジュールの消費電力の変動の解析。

デジタル署名(Digital signature)

デジタル署名：適切な実装がされた場合に次のサービスを提供する、データの暗号化変換の結果。

1. 署名者の特定
2. データの完全性、
3. 及び、署名者の否認防止

電磁両立性(EMC)(Electromagnetic compatibility(EMC)**)**

ある電磁環境における電子デバイスの、他のデバイスに対して電磁的な誤動作をその電磁環境下で引き起こすことなく、十分に機能する能力

電磁妨害(EMI)(Electromagnetic interference(EMI)**)**

他のデバイス、装置、又はシステムの正規の動作を妨害する、デバイス、装置、又はシステムからの電磁放射

電子的鍵入力(Electronic key entry)

スマートカードまたはキーローディングデバイス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。(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。）

暗号化された鍵(Encrypted key)

鍵を暗号化するための鍵、PIN、又はパスワード付きの承認されたセキュリティ機能を用いて、元になる平文の鍵の値を隠蔽するために暗号化した、暗号鍵

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殆化することを防止する特性。

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また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殆化しないという合理的保証を得るための試験。

エラー検出コード(EDC)(Error detection code (EDC)**)**

データから計算されたコードであって、データの意図しない変更を検出する（訂正はしない）ために設計された情報の、冗長ビットで構成されているもの。

有限状態モデル(FSM)(Finite state model**)**

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。

ファームウエア(Firmware)

暗号境界のなかにあるハードウエア（例えば、POM、PROM、EPROM、EEPROM 又は FLASH）に保存され、実行している間は動的な書き込み又は変更が出来ない暗号モジュールのプログラム及びデータコンポーネント。

ハードウエア(Hardware)

暗号モジュールのプログラム及びデータを処理するために使用される、暗号境界のなかにある物理的な装置。

ハッシュ関数を用いたメッセージ認証コード(HMAC)(Hash-based message authentication code (HMAC)**)**

鍵付きハッシュを用いたメッセージ認証コード。

初期ベクトル(IV)(Initialization vector(IV)**)**

暗号アルゴリズムにおける暗号処理の出発点を定義するベクトル。

入力データ(Input data)

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、暗号モジュールに入力される情報。

完全性(Integrity)

権限が無い状態で、検出されずに重要なデータの変更又は消去が出来ない特性。

インタフェース(Interface)

物理的な信号を表現する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。

鍵を暗号化するための鍵(Key encrypting key)

他の鍵を暗号化又は復号するために用いられる暗号鍵

鍵確立(Key establishment)

手動の配送方法（例えば、キーローダー)、自動化された方法（例えば、鍵配送及び/又は鍵共有プロトコル)、又は自動化された方法及び手動の方法の組合せ（例えば、鍵配送に鍵共有を合わせたもの）を用いて、暗号鍵が暗号モジュール間をセキュアに配送されるプロセス。

キーローダ(Key loader)

少なくとも一つの暗号化されていない暗号鍵又は暗号化された暗号鍵若しくは鍵コンポーネントを格納できる独立した機構であって、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。

鍵管理(Key management)

鍵の生成、保存、確立、入力及び配送、並びにゼロ化を含む鍵のライフサイクル全体の間での、暗号鍵及び関連するセキュリティパラメータ（例えば、初期ベクトル及びパスワード）の取り扱いに関わる動作。

鍵配送(Key transport)

ある暗号モジュールから他のモジュールへの、鍵のセキュアな配送。

手動鍵配送(Manual key transport)
非電子的方法による暗号鍵の配送。

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。

マイクロコード(Microcode)
実行可能なプログラム命令に対応する基本的なプロセッサの命令。

オペレータ(Operator)
暗号モジュールにアクセスする人、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（サブジェクト)。この場合、担う役割とは関係しない。

出力データ(Output data)
暗号モジュールから生成される情報。

パスワード(Password)
本人認証を行ったり、又はアクセス権を検証したりするための文字列(文字、数字、及びその他の記号)

個人識別番号(PIN)(Personal identification number (PIN)**)**
ID 認証を行い、又はアクセス権を検証するための文字列（文字、数字、及びその他の記号）

物理的保護(Physical protection)
物理的手段を用いた、暗号モジュール、暗号鍵、又はその他の CSP の安全防護策

平文の鍵(Plaintext key)
暗号化されていない暗号鍵

ポート(Port)
論理的な情報フローによって表現された物理的な信号に対して暗号モジュールへのアクセスを提供する、暗号モジュールの物理的な入出力点。(物理的に分離されているポートは、同じ物理的なピン又は線を共有しない。)

プライベート鍵(Private key)

公開鍵暗号アルゴリズムにおいて用いられる暗号鍵。一つのエンティティに対して一意に対応し、公開されない。

プロテクションプロファイル(Protection Profile)

ある評価対象（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。

公開鍵(Public key)

公開鍵暗号アルゴリズムにおいて用いられる暗号鍵。一つのエンティティに対して一意に対応し、公開される。（公開鍵は CSP とは見なされない。）

公開鍵証明書(Public key certificate)

エンティティを一意に識別するデータの集合。その中には、エンティティの公開鍵が含まれており、信頼できる機関によってデジタル署名され、その結果、公開鍵とエンティティとが結びつけられている。

公開鍵（非対称）暗号アルゴリズム(Public key (asymmetric) cryptographic algorithm)

公開鍵及びプライベート鍵という二つの関連した鍵を用いる暗号アルゴリズム。二つの鍵には、公開鍵からプライベート鍵を導出することは計算量的に不可能であるという性質がある。

乱数生成器(Random Number Generator)

暗号アプリケーションに使用される乱数生成器（RNG）は、一般的には、組み合わされて乱数の部分列又はブロックになった、0 及び 1 のビット列を生成する。乱数生成器には、決定論的及び非決定論的の二つの基本クラスがある。決定論的 RNG は、シードと呼ばれる初期値からビット列を生成するアルゴリズムから成る。非決定論的 RNG は、人間が制御することのできない、なんらかの予測不可能な物理源に依存した出力を生成する。

除去可能なカバー(Removable cover)

暗号モジュール内部への物理的アクセスを許可するように設計されたカバー

秘密鍵(Secret key)

秘密鍵暗号アルゴリズムにおいて使用される暗号鍵。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（対称）暗号アルゴリズム（共通鍵暗号アルゴリズム）(Secret key (symmetric) cryptographic algorithm)

一つの秘密鍵を用いて、暗号化と復号の両方を行う暗号アルゴリズム。

セキュリティポリシ(Security policy)

「暗号モジュールのセキュリティポリシ」を参照のこと。

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

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、これから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。

ソフトウエア(Software)

暗号境界のなかにあるプログラム及びデータコンポーネントであって、通常、消去可能なメディア（ディスク等）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。

知識分散(Split knowledge)

暗号鍵を､元の暗号鍵の知識をもたない複数の鍵コンポーネントに分割するプロセス。個々の鍵コンポーネントは、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される。

ステータス情報(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。

システムソフトウエア(System software)

暗号境界のなかにある特別なソフトウエア（例えば、オペレーティングシステム、コンパイラ、又はユーティリティプログラム）であって、コンピュータシステム並びにその関連したプログラム及びデータの操作とメンテナンスがしやすいように、特定のコンピュータシステム又はコンピュータシステム群のために設計されたもの。

タンパー検出(Tamper detection)

暗号モジュールの物理的なセキュリティを危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。

タンパー証跡(Tamper evidence)

暗号モジュールの物理的セキュリティを危殆化する試みがなされたことを示す、外観上の表示。(試みの証跡は、試みの直後にオペレータが観察できることが望ましい。)

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に取る自動的な動作。(最低の応答動作は、平文の鍵及びその他の保護されていない CSP のゼロ化である。)

評価対象(TOE)(Target of Evaluation (TOE)**)**

評価の対象となる、情報技術(IT)の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。

テンペスト(TEMPEST)

通信装置及び自動化情報システム装置から発生する、意図していないが危殆化を及ぼす電磁波輻射に関する調査・研究、及びそれを抑制する技術の総称。

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 TOE のすべてのハードウエア、ソフトウエア、及びファームウエアからなる集合。CC で使われる用語である。

TOE セキュリティ方針(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。CC で使われる用語である。

高信頼パス(Trusted path)

オペレータと TOE セキュリティ機能とが、TOE セキュリティ方針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。

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)。

認証機関(Validation authorities)

評価結果の認証を行う機関。NIST 及び CSE。

ゼロ化(Zeroization)

データ復元を防止するために、データストレージの内容を変更又は消去することによって、保存されていたデータ、暗号鍵、及びその他の CSP を電子的に消去する方法。

2.2 略語

次の略語及び簡略名は、この標準で使用されている。

ANSI	American National Standards Institute
API	Application Program Interface
CAPP	Controlled Access Protection Profile
CBC	Cipher Block Chaining
CC	Common Criteria
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment of the Government of Canada
CSP	Critical Security Parameter
DES	Data Encryption Standard
DOD	Department of Defense
DPA	Differential Power Analysis
DTR	Derived Test Requirements
EAL	Common Criteria Evaluation Assurance Level
EDC	Error Detection Code
EEPROM	Electronically-Erasable Programmable Read-Only Memory

EFP	Environmental Failure Protection
EFT	Environmental Failure Testing
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EPROM	Erasable Programmable Read-Only Memory
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FIPS PUB	FIPS Publication
HDL	Hardware Description Language
HMAC	Hash-Based Message Authentication Code
IC	Integrated Circuit
IG	Implementation Guidance
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria
IV	Initialization Vector
NIST	National Institute of Standards and Technology
NTIS	National Technical Information Service
PIN	Personal Identification Number

PROM	Programmable Read-Only Memory
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read-Only Memory
SPA	Simple Power Analysis
TOE	Target of Evaluation
TSF	Target of Evaluation Security Functions
TSP	Target of Evaluation Security Policy
URL	Uniform Resource Locator

3．機能的セキュリティ目標

この標準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、暗号モジュールに対する高位な機能的セキュリティ目標を実現するものである。

・重要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。

・暗号モジュールを、許可されない操作又は許可されない利用から保護する。

・暗号モジュールの内容(平文の暗号鍵及びその他の保護されていない CSP を含む)の許可されない開示を防ぐ。

・暗号モジュール及び暗号アルゴリズムに対する、許可されない変更及び検出不能な変更(暗号鍵及びその他の CSP に対する、許可されない変更、置換、挿入、及び消去を含む)を防ぐ。

・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時に、暗号モジュールが適切に実行することを保証する。

・暗号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重要データ及びその他の CSP の危殆化を防ぐ。

4. セキュリティ要求事項

この章では、この標準に従う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、電磁妨害/電磁両立性(EMI/EMC)、自己テスト、及び設計保証。その他の攻撃(例えば、差分電力解析及びテンペスト)の対処に関連した付加的な分野は現在試験されていないが、ベンダは、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。

	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。全てのハードウエア、ソフトウエア、ファームウエアのコンポーネント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の宣言.			
暗号モジュールのポート及びインタフェース	必須のインタフェース及び選択可能なインタフェース。全てのインタフェースの仕様及び全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又は物理的に分離された、保護されていない CSP のためのデータポート。	
役割,サービス,及び認証	必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	製品レベルの装置。	錠又はタンパー証跡。	カバー及びドアに対するタンパー検出及びタンパー応答。	囲いのタンパー検出及びタンパー応答。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。			
	手動の方法を用いて確立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。		手動の方法を用いて確立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。	
EMI/EMC	47 CFR FCC Part 15。Subpart B, Class A(ビジネス向け)。適切な FCC 要件(無線向け)。		47 CFR FCC Part 15。Subpart B, Class B(家庭向け)。	
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、ソフトウエア/ファームウエア完全性テスト、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。設計とポリシとの対応。ガイダンス文書。	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)。事前条件と事後条件。
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。			

表 1：セキュリティ要求事項の要約

暗号モジュールは、この章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。いくつかの分野では、上位のセキュリティ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全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関わらず、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。

この文書のセキュリティ要求事項の多くは、Appendix A、C 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全ての文書は、ベンダによって試験機関へ提供されなければならない。

4.1 暗号モジュールの仕様

暗号モジュールは、ハードウエア、ソフトウエア、ファームウエアの集合又はそれらの組合せでなければならない。これらハードウエア、ソフトウエア、ファームウエアは、定義された暗号境界に含まれ、暗号アルゴリズム及び場合によっては鍵生成を含む暗号機能又は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 1 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に含まれてもよい。オペレータは、承認された動作モードが選択されていることを判定できなければならない。セキュリティレベル 1 及びセキュリティレベル 2 において、暗号モジュールのセキュリティポリシは、暗号モジュールが承認された動作モードでいつ実行されるかを規定してもよい。セキュリティレベル 3 及びセキュリティレベル 4 の場合、暗号モジュールは、承認された動作モードが選択されている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この標準の Annex A に記載されている。)

暗号境界は、暗号モジュールの物理的な境界を明確に定義しなければならない。暗号モジュールがソフトウエア又はファームウエアのコンポーネントから構成されている場合には、暗号境界は、(1 つ又は複数の)プロセッサ及びその他のハードウエアコンポーネント(その他のハードウエアコンポーネントとは、ソフトウエア及びファームウエアのコンポーネントを格納及び保護するものである)を含まなければならない。暗号モジュールのハードウエア、ソフトウエア、及びファームウエアのコンポーネントは、これらのコンポーネント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、この標準の要求事項から除外することができる。

次の文書化された要求事項は、暗号モジュール内にある全てのセキュリティに関係するハードウエア、ソフトウエア、及びファームウエアに適用しなければならない。これらの要求事項は、ソースコードがベンダ向けに用意されていないマイクロコード及びシステムソフトウエア、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エア、ソフトウエア、又はファームウエアのコンポーネントには適用されない。

- 文書は、暗号モジュールのハードウエア、ソフトウエア、及びファームウエアのコンポーネントを規定し、これらのコンポーネントを囲む暗号境界を規定して、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。(4.5節参照)

・文書は、この標準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エア、ソフトウエア及びファームウエアのコンポーネントを規定して、適用除外とする根拠を説明しなければならない。

・文書は、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、並びに定義された入出力データパスの全てを規定しなければならない。

・文書は、暗号モジュールのマニュアル又は論理的な制御、物理的又は論理的な状態表示、及びそれらの物理的、論理的、及び電気的な特徴を規定しなければならない。

・文書は、承認されているかどうかに関わらず、暗号モジュールに採用される全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関わらず、全ての動作モードを規定しなければならない。

・文書は次を規定しなければならない。

□暗号モジュールの主要なハードウエアコンポーネントの全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、平文データ用のバッファ/暗号化されたデータ用のバッファ、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。

□及び、暗号モジュールのハードウエア、ソフトウエア、及びファームウエアのコンポーネントの設計。この設計を文書化するためには、ソフトウエア/ファームウエアは高級言語を使用し、ハードウエアは回路図を使用しなければならない。

・文書は、秘密鍵及びプライベート鍵(平文の状態、及び暗号化された状態の両方)、認証データ(例えば、パスワード、PIN)、その他のCSP、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殆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、全てのセキュリティに関係する情報を規定しなければならない。

・文書は、暗号モジュールのセキュリティポリシを規定しなければならない。このセキュリティポリシは、この標準の要求事項から導かれる規則、及びベンダから提示された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。(APPENDIX C参照)

4.2 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、全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全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。暗号モジュールインタフェースは、1つの物理的ポートを共有していたり(例えば、同一のポートを介して、データが入出力されてもよい)、1つ又はそれ以上の物理的ポートに分散していたりしてもよいが(例えば、シリアルポートとパラレルポートの両方を介して、入力データが入力されてもよい)、論理的には互いに分離されていなければならない。暗号モジュールのソフトウエアコンポーネントのアプリケーションプログラムインタフェース(API)は、1つ又はそれ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 4 つの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。)：

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全てのデータ(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。全てのデータには、他の暗号モジュールからの平文データ、暗号文データ、暗号鍵及びその他のCSP、認証データ、及び状態情報を含む。

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全てのデータ(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。全てのデータには、平文データ、暗号文データ、暗号鍵及びその他のCSP、認証データ、及びその他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全てのデータ出力は禁止されなければならない。(4.9節参照)

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全ての入力コマンド、信号、及び制御データ(関数呼び出し及びスイッチ、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。

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全ての出力信号、インジケータ、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全ての外部電源(外部電源又はバッテリからの電源を含む)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全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)には、電源ポートは必要とされない。

暗号モジュールは、「入力のデータ及び制御」と「出力のデータ及び状態」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全ての入力データは、入力データパスのみ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全ての出力データは、出力データパスのみ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。誤って重要情報を出力してしまうことを防止するために、2つの独立した内部動作(例えば、その1つがユーザによって開始される2つの異なるソフトウェアフラグがセットされること。又は、2つの別々の動作によって2つのハードウェアゲートが順次にセットされること)が平文の暗号鍵又はその他の保護されていないCSP又は重要データが出力される出力インタフェースから、データを出力することに対して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

セキュリティレベル1及び2において、平文の暗号鍵、暗号鍵コンポーネント、認証データ及びその他の保護されていないCSPの入出力に使用する(1つ又は複数の)物理的ポート及び(1つ又は複数の)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

セキュリティレベル3及び4において、

・平文の暗号鍵コンポーネント、認証データ、及びその他の保護されていないCSPの

入出力のために使用される(1つ又は複数の)物理的ポートは、暗号モジュールの他の全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。

又は

・平文の暗号鍵コンポーネント、認証データ、及びその他の保護されていないCSPの入出力に使用される論理的インタフェースは、高信頼パスを使用する他の全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。

及び

・平文の暗号鍵コンポーネント、認証データ、及びその他の保護されていないCSPは、暗号モジュールに直接入力されなければならない。(例えば、高信頼パスを介するか又は直接接続されたケーブルを介する)(4.7.4節参照)

4.3 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許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。複数の役割は、単一のオペレータによって担われてもよい。暗号モジュールが、同時に複数オペレータによる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及びそれに対応するサービスによって担われる役割の区分けを、内部的に管理しなければならない。オペレータは、暗号鍵及びその他のCSPが変更、開示、又は置換されないサービスを実行するために許可された役割を担うことを要求されない(例えば、状態の表示、自己テスト、又は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)。

認証メカニズムは、暗号モジュールにアクセスしているオペレータを認証するために、及びオペレータが要求された役割を担い、かつ、役割の中のサービスの実行が許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必要とされてもよい。

4.3.1 役割

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

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。

クリプトオフィサ役割
暗号関連の初期化又は管理機能を行うことを担う役割(例えば、暗号モジュールの初期化、暗号鍵及びその他のCSPの入力/出力、及び監査機能)。

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、次の許可された役割をサポートしなければならない：

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を行うことを担う役割(例えば、ハードウエア/ソフトウエアの診断)。メンテナンス役割へ入る、又はメンテナンス役割から出る場合は、全ての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はゼロ化されなければならない。

暗号モジュールは、上記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。

文書は､暗号モジュールがサポートする全ての許可された役割を規定しなければならない。

4.3.2 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、又は機能の全てを言及しなければならない。サービス入力は、特定のサービス、動作、若しくは機能を開始又は獲得させる暗号モジュールへの全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全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：

状態の表示

暗号モジュールの現在の状態を出力する。

自己テストの実行

4.9 節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。

承認されたセキュリティ機能の実行

4.1節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1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、承認された及び承認されていない両方の他のサービス、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能力を実装している場合には、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、

・たった1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能力を動作させるために、2つの独立した内部動作が要求されなければならない(例えば、2つの異なるソフトウエア又はハードウエアのフラグがセットされ、そのうち1つのフラグはユーザ操作によるものでもよい)。

・暗号モジュールは次の状態を表示しなければならない。

1) バイパス能力が動作せず、かつ、暗号モジュールが排他的に暗号処理を行うサービス(例えば、暗号化されていないデータが暗号化される)を提供している。

2) バイパス能力が動作し、かつ、暗号モジュールが排他的に暗号処理を行わないサービス(例えば、暗号化されていないデータが暗号化されない)を提供している。

3) バイパス能力は選択的に動作及び非動作となり、並びに暗号モジュールは複数の暗号処理を行うサービス及び複数の暗号処理を行わないサービス(例えば、多重通信チャネルを持つ暗号モジュールの場合、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)を複数提供している。

文書は、次を規定しなければならない：

・暗号モジュールによって提供される、承認されている及び承認されていない両方の、サービス、動作、又は機能

・及び、暗号モジュールによって提供される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許可された(1つ又は複数の)役割

・オペレータが許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、並びにそれらのサービスが暗号鍵及びその他のCSPを変更、開示、若しくは置換しない理由、又は暗号モジュールのその他のセキュリティに影響しない理由

4.3.3 オペレータ認証

認証メカニズムは、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、及びオペレータが要求された役割を担い、かつ、役割の中のサービスの実行が許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必要とされてもよい。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。

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、一つ又はそれ以上の役割をオペレータに暗黙的又は明示的に選択させて、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認証をしなければならない。

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、オペレータにより暗黙的又は明示的に一つ又はそれ以上の役割が選択されることを要求し、及びオペレータのID及びオペレータが選択された役割(又は役割の集合)を担うことの許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許可は、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許可されていないいかなる役割を担うための許可を検証しなければならない。

暗号モジュールは、許可された役割の中で許可されたサービス全てを実行することを認証されたオペレータに許可するか、若しくは、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してもよい。暗号モジュールが電源OFFされ、及び続いて電源ON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、並びに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。

いろいろなタイプの認証データは、サポートされた認証メカニズムを実行するために暗号モジュールによって要求されてもよい。認証データの例には次がある。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；又は、個人の特徴の照合(例えば、バイオメトリクス)。暗号モジュール内の認証データは、許可されていない開示、変更、及び置換に対して保護されなければならない。

認証メカニズムの初期化は特別な扱いをしてもよい。暗号モジュールが、最初に暗号モジュールがアクセスされるときに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､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、他の認証方法(例えば、手続きによる制御、又は工場設定値、又はデフォルトの認証データの使用)が使用されなければならない。

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。

・1回の認証メカニズムの試行において、ランダムな試みが成功する確率又は誤受入率(例えば、パスワード若しくはPINの推定、バイオメトリクスデバイス、又は認証方法のいくつかの組合せの誤受入率)は、1,000,000分の1未満でなければならない。

・複数回の認証メカニズムを1分間の間に試行する場合、ランダムな試みが成功する確率又は誤受入率は100,000分の1未満でなければならない。

・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、曖昧化されなければならない(例えば、パスワード入力の時に文字列の表示が見えない)。

・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、認証メカニズムの強度を弱めてはならない。

ベンダが提供する文書は、次を規定しなければならない。

・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許可された方法

・及び、暗号モジュールによってサポートされた認証メカニズムの強度

セキュリティレベル1

セキュリティレベル1において､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須ではない。認証メカニズムが暗号モジュールによってサポートされない場合には､暗号モジュールは､1つ又はそれ以上の役割がオペレータによって暗黙的又は明示的に選択されることを要求しなければならない。

セキュリティレベル2

セキュリティレベル2において､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

セキュリティレベル3及び4において、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。

4.4 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)を用いて規定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全て

・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

・並びに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。

電源 on/off 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。

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、暗号の初期化及び鍵管理)

鍵/CSP 入力状態
暗号鍵及びその他の CSP を暗号モジュールへ入力している状態。

ユーザ状態
許可されたユーザがセキュリティサービスを受けたり、暗号操作を実行した

り、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。

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。

エラー状態

暗号モジュールがエラーとなった時の状態(例えば、自己テストに失敗した状態、又は、操作のための鍵若しくはその他のCSPがない時に暗号化を試みた状態)。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。

バイパス状態

バイパス能力が作動し、暗号化処理されないサービス(例えば、暗号モジュールを通して平文を転送する)が提供される状態。

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。

文書は、状態遷移図及び/又は状態遷移表を用いた有限状態(又は同等のもの)の表現を含まなければならない。また、その状態遷移図及び/又は状態遷移表は、次のものを規定しなければならない。

・暗号モジュールの動作状態及びエラー状態の全て。

・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。その入力イベントには、データ入力及び制御入力を含めること。

・及び、出力イベント。その出力イベントには、暗号モジュールの内部状態、データ出力、及びある状態から別の状態への遷移の結果起こる状態出力を含めること。

4.5 物理的セキュリティ

暗号モジュールは、暗号モジュールの内容への許可されていない物理的なアクセスを制限するために、及び暗号モジュールが設置されている場合、暗号モジュールの許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)を防ぐために、物理的セキュリティのメカニズムを用いなければならない。暗号境界内の全てのハードウエア、ソフトウエア、ファームウエア、及びデータコンポーネントは保護されなければならない。

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のみ提供されるようなソフトウエアによって全て実装されている暗号モジュールは、この標準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､3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。

・**シングルチップ暗号モジュール**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。

・**マルチチップ組込型暗号モジュール**は、2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、アダプター及び拡張ボードが含まれる。

・**マルチチップスタンドアロン型暗号モジュール**は、2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、許可されていない物理的なアクセス、使用、又は変更の試みは、以下のようにして高い確率で検出される。

・視覚的な形跡を残すことによって試みの後に検出する。(すなわち、タンパー証跡)

及び/又は

・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を保護するために、暗号モジュールによって適切な動作がとれるように試みの間に検出する。(すなわち、タンパー応答)

表2は、4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(一般的要求事項と形態特有の要求事項の両方)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一般的な物理的セキュリティの要求事項は、3つの識別された暗号モジュールの形態全てに適用される。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。

	全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	製品グレードコンポーネント(標準的な(皮膜)保護付)	追加要求事項なし	該当する場合、製品グレードの囲い又は除去可能なカバー	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、又はツール)	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ツ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ツール、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	メンテナンスインタフェースにアクセスするときの自動的ゼロ化。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エンベロープ	タンパー応答及びゼロ化回路の付いたタンパー検出/応答エンベロープ

表 2：物理的セキュリティ要求事項の要約

一般に、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、又はその他の許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、セキュリティ要求事項はメンテナンスアクセスインタフェースが規定されている。

4.5.1 共通の物理的セキュリティの要求事項

次の要求事項は、全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規定しなければならない。

・文書は、暗号モジュールの物理的セキュリティのメカニズムを規定しなければならない。

・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(例えば、暗号モジュールのベンダによる、又は他の許可された個人による)物理的アクセスを許す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が定義されなければならない。

□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全ての物理アクセス経路を含んでいなければならない。

□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。

□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、平文の秘密鍵及びプライベート鍵の全て、並びにその他の保護されていない CSP の全てはゼロ化されなければならない。

□及び、文書は、メンテナンスアクセスインタフェースを規定して、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、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がどのようにゼロ

化されるかを規定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 の全ての暗号モジュールに適用しなければならない。

・暗号モジュールは、標準的な保護技術(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コンポーネントで構成されなければならない。

・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平文の秘密鍵及びプライベート鍵の全て、並びにその他の保護されていない CSP の全てはゼロ化されなければならない。ゼロ化は、オペレータによって手続き的に行われるか、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の全ての暗号モジュールに適用しなければならない。

・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 の全ての暗号モジュールに適用しなければならない。

・暗号モジュールがあらゆる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、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、平文の秘密鍵及びプライベート鍵の全て、並びにその他の保護されていない CSP の全てをただちにゼロ化しなければならない。タンパー応答及びゼロ化回路は、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。

・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1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、次の要求事項はセキュリティレベル 4 の全ての暗号モジュールに適用しなければならない。

・暗号モジュールは、4.5.5 節で規定されるように、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。

4.5.2 シングルチップ暗号モジュール

4.5.1節に規定された共通のセキュリティ要求事項に加え、次の要求事項はシングルチップ暗号モジュールに対しては特有である。

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。

・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、又は不正操作を防ぎ、かつ暗号モジュールへのタンパー又は除去に対する試みの証跡を提供するために、タンパー証跡を残すコーティング(例えば、タンパー証跡を残す保護膜材料、又は保護膜を覆ったタンパー証跡を残す材料)で覆われているか、又はタンパー証跡を残す囲い内に含まれていなければならない。

・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、次の要求事項は、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。

・暗号モジュールは、堅く不透明なタンパー証跡を残すコーティング(例えば、保護膜を覆った堅く不透明なエポキシ樹脂)で覆われているか、

又は

・囲いは、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るか

のいずれか

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。

・暗号モジュールは、暗号モジュールからコーティングを剥がしたり、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)ように、硬度の特性及び接合性を持ち、堅く不透明で除去耐性のあるコーティングで覆われなければならない。

・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、モジュールが機能しなくなる)ような溶解特性を持たなければならない。

4.5.3 マルチチップ組込型暗号モジュール

4.5.1節に規定された共通のセキュリティ要求事項に加え、次の要求事項はマルチチップ組込型暗号モジュールに対しては特有である。

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。

・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、次の要求事項は、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。

・暗号モジュールコンポーネントは、暗号モジュールコンポーネントへの直接的な観察、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コンポーネントの除去の証拠を提供するために、タンパー証跡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)で覆われているか、又はタンパー証跡を残す囲いで覆われていなければならない。

・かつ、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。

又は、

・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。

・囲いは、可視領域内において不透明でなければならない。

・かつ、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、又はそれらは、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。

のいずれか。

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、次の要求事項は、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。

・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。

又は

・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。(4.5.4節)

のいずれか。

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。

・暗号モジュールコンポーネントは、封止材によって覆われ、さらにタンパー検出エンベロープによってカプセル化されているか、又は、タンパー検出エンベロープ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。これらタンパー検出エンベロープは、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に対するアクセスを可能にする程度に、封止材又は囲いを切削、掘削、粉砕、研削、又は溶解のような方法によるタンパーを検出しなければならない。

(備考)

タンパー検出エンベロープ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持つ柔軟なマイラプリント回路、又は巻き線型パッケージ、又は柔軟性がなく壊れやすい回路、又は堅固な囲いがある。

・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、タンパー検出エンベロープ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、タンパー応答及びゼロ化回路は、ただちに平文の秘密鍵及びプライベート鍵の全て、並びにその他の保護されていない CSP の全てをゼロ化しなければならない。タンパー応答及びゼロ化回路は、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。

4.5.4 マルチチップスタンドアロン型暗号モジュール

4.5.1節に規定された共通のセキュリティ要求事項に加え、次の要求事項はマルチチップスタンドアロン型暗号モジュールに対しては特有である。

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。

・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。

・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。

・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、又はそれらは、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、次の要求事項は、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。

・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。

又は、

・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。

のいずれか。

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。

・暗号モジュールの封止材又は囲いは、タンパー検出エンベロープによって、すなわち、カバースイッチ、モーション検出器、又は前述のマルチチップ組込み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。

(備考)

□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。

□モーション検出器の例には、超音波、赤外線、又は電磁波がある。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ほどのタンパー(封止材又は囲いの切削、掘削、粉砕、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。

・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、タンパー検出エンベロープを継続的に監視して、タンパーを検出したとき、ただちに、平文の秘密鍵及びプライベート鍵の全て、並びにその他の保護されていない CSP の全てをゼロ化しなければならない。タンパー応答及びゼロ化回路は、平文の暗号鍵及び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。

4.5.5 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殆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殆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される。

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)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。

4.5.5.1 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殆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。特に、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回路又は電子デバイスを持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、保護回路は、(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)平文の秘密鍵及びプライベート鍵の全て、並びにその他の保護されていない CSP の全てを、ただち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規定しなければならない。

4.5.5.2 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殆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、暗号モジュール内の電子デバイス又は電子回路の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殆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、摂氏－100 ° ～＋200 ° (華氏－150 ° ～＋400 °)でなければならない。試験する電圧範囲は、電圧の極性反転を含め、電子デバイス又は電子回路のゼロ化を引き起こす(基準電圧での)最小の負電圧から、電子デバイス又は電子回路のゼロ化を引き起こす(基準電圧での)最小の正電圧までででなければならない。

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規定しなければならない。

4.6 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エアコンポーネント、ファームウエアコンポーネント、及び/又はハードウエアコンポーネントの管理を指す。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エア、又は入出力デバイスの機能を無効にしたコンピュータに収められたソフトウエア)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エア、又は汎用コンピュータで実行されるソフトウエア)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。

汎用動作環境とは、暗号境界内のソフトウエアコンポーネント及びファームウエアコンポーネントを管理し、並びにワードプロセッサのような汎用アプリケーションソフトウエアを含むシステム及びオペレータプロセス/スレッドも管理する商業利用可能な汎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)を利用することを指す。

限定動作環境とは、汎用オペレーティングシステムを持たず、その上に動作環境がただひと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。

変更可能な動作環境とは、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、汎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、又はプログラミング可能なファームウエアの使用)を含んでもよい動作環境を指す。ソフトウエアコンポーネント/ファームウエアコンポーネントがオペレータによって変更できる場合、及び/又はオペレータが暗号モジュールの認証機関から認証される部分として含まれていないソフトウエア又はファームウエア(例えば、ワードプロセッサ)をロード及び実行することが出来る場合には、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、4.6.1 節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。動作環境が限定動作環境である場合には、4.6.1 節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規定しなければならない。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、PP 及び CC 保証レベルも含めて規定しなければならない。

4.6.1 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。

- セキュリティレベル 1 のみにおいて、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)。

- セキュリティレベル 1 のみにおいて、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平文のプライベート鍵及び秘密鍵、鍵生成の中間値、並びにその他の保護されていない CSP 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処理は、暗号モジュールによって所有され、外部の処理/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り込み処理を行えてはならない。

・全ての暗号ソフトウエア及び暗号ファームウエアは、ソフトウエア及びファームウエアのソースコード及び実行可能コードが許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設置されなければならない。

・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又は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全ての暗号ソフトウエアコンポーネント及び暗号ファームウエアコンポーネント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エア/ファームウエア完全性テスト(4.9.1 節参照)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。

・全ての暗号ソフトウエア及び暗号ファームウエア、暗号鍵及びその他の CSP、並びに制御情報及び状態情報は、次の制御下におかれなければならない。

□Annex B のリストに記載された PP に規定された機能要件を満たし、かつ、CC 評価保証レベル EAL2 において評価されたオペレーティングシステム

□又は、同等の評価がなされた高信頼オペレーティングシステム

・平文データ、暗号ソフトウエア及び暗号ファームウエア、暗号鍵及びその他の CSP、並びに認証データを保護するため、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、次のように構成されなければならない。

□格納されている暗号ソフトウエア及び暗号ファームウエアを実行できる役割の集合を規定すること。

□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エアコンポーネ

ント又はファームウエアコンポーネントを変更(すなわち、書き込み、置換、及び削除)できる役割の集合を規定すること。：暗号プログラム、暗号データ(例えば、暗号鍵及び監査データ)、平文データ、及びその他の CSP。

□暗号境界内に格納されている次の暗号ソフトウエアコンポーネントの読み取りを行うことができる役割の集合を規定すること。：暗号データ(例えば、暗号鍵及び監査データ)、平文データ、及びその他のCSP。

□暗号鍵及びその他のCSPの入力を行うことができる役割の集合を規定すること。

・オペレーティングシステムは、全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形)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関わらず、全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。

・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エアの読み出しを行うことを防がなければならない。

・オペレーティングシステムは、暗号データ及びその他の CSP 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。

□次のイベントは、監査メカニズムによって記録されなければならない。

- クリプトオフィサ機能に対する無効な入力の試み、
- 及び、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

□監査メカニズムは、次のイベントの監査が出来なければならない。

- 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係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係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
- 及び、クリプトオフィサ役割への機能の割り当て

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。

・全ての暗号ソフトウエア及び暗号ファームウエア、暗号鍵及びその他の CSP、並びに制御情報及び状態情報は、次の制御下におかれなければならない。

□Annex B のリストに記載された 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。そのオペレーティングシステムは、CC 評価保証レベル EAL3 及び次の追加要件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)、

□又は、同等の評価がなされた高信頼オペレーティングシステム。

・全ての暗号鍵及びその他の CSP、認証データ、制御入力、並びに状態出力は、高信頼メカニズム(例えば、専用の入出力物理ポート又は高信頼パス)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 により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。

・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り記録されなければならない：

□高信頼パス機能の利用の試み、

□及び、高信頼パスの起動者及び対象の識別

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。

・全ての暗号ソフトウェア、暗号鍵及びその他のCSP、並びに制御情報及び状態情報は、次の制御下におかれなければならない。

□Annex Bのリストに掲載された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。そのオペレーティングシステムは、CC評価保証レベルEAL4において評価されなければならない。

□又は、同等の評価がなされた高信頼オペレーティングシステム

4.7 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暗号鍵、暗号鍵コンポーネント、その他のCSPのライフサイクル全体を包含している。鍵管理は、乱数生成及び鍵生成、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。暗号化された暗号鍵及びその他の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暗号鍵及びその他のCSPを指す。承認されていない暗号アルゴリズム又は、独自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暗号鍵及びその他のCSPは、この標準の適用範囲内では、平文形式とみなされる。

秘密鍵及びプライベート鍵、並びにその他の CSP は、暗号モジュール内において、許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。公開鍵は、暗号モジュール内において、許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。

文書は、暗号モジュールに用いられる全ての暗号鍵、暗号鍵コンポーネント、及びその他の CSP を規定しなければならない。

4.7.1 乱数生成器(RNG)

暗号モジュールは乱数生成器(RNG)を採用してもよい。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RNG又は承認されていないRNGを用いる場合には、RNGからのデータ出力は、4.9.2節で規定されたような連続乱数生成器テストに合格しなければならない。承認されたRNGは、4.9.1節の暗号アルゴリズムテストの対象とされなければならない。承認されたRNGは、この標準のAnnex Cに記載されている。

承認された非決定論的RNGの標準が存在するような時までは、機密のアプリケーションにおける使用が承認された非決定論的RNGは、鍵生成に使われるか、又は鍵生成に使用される承認された決定論的RNGのシードとして使われてもよい。商用的に利用可能な非決定論的RNGは、承認された決定論的RNGのシードを生成するために用いられてもよい。非決定論的RNGは、この標準の適用可能なRNG要求事項の全てを満たさなければならない。

承認された RNG は、承認されたセキュリティ機能に用いられる暗号鍵の生成に用いられなければならない。承認されていない RNG からの出力は、1)承認された決定論的 RNG への入力(例えば、シード及びシード鍵)、又は 2)承認されたセキュリティ機能に対する初期ベクトル(IVs)を生成するために、使用されてもよい。シード及びシード鍵は、同じ値をもってはならない。

文書は、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)RNG のそれぞれを規定しなければならない。

4.7.2 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、承認された鍵生成方法を用いて、生成されなければならない。承認された鍵生成方法は、この標準のAnnex Cに記載されている。承認された鍵生成方法がRNGからの入力を必要とする場合には、4.7.1節で規定された要求事項を満たす承認されたRNGが用いられなければならない。

鍵生成方法のセキュリティの危殆化(例えば、決定論的 RNG を初期化するためのシード値を推定すること)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、4.7.4 節に規定された鍵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、鍵生成処理の完了時に、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)知識分散の手順のもとで、出力されなければならない。

文書は、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を規定しなければならない。

4.7.3 鍵確立

鍵確立は、自動化された方法(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)、又は自動化された方法と手動の方法の組合せによって行われてもよい。鍵確立の方法が暗号モジュールに用いられている場合には、承認された鍵確立の技術だけが使用されなければならない。承認された鍵確立方法は、この標準のAnnex Dに記載されている。

承認された鍵確立の技術の代わりに、無線通信暗号モジュールが、OTAR(Over-The-Air-Rekeying)を実装する場合には、“The TIA/EIA Telecommunications Systems Bulletin, APCO Project 25, Over-The-Air-Rekeying (OTAR) Protocol, New Technology Standards Project, Digital Radio Technical Standards, TSB102.AACA, January, 1996, Telecommunications Industry Association”に規定されているように実装されなければならない。

鍵確立の方法のセキュリティを危殆化すること(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を危殆化すること)は、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くらい多く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、4.7.4 節の鍵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)には、共有された値は 4.7.4 節の鍵入出力の要求事項を満たす必要はない。

文書は、暗号モジュールに用いられる鍵確立の方法を規定しなければならない。

4.7.4 鍵の入力及び出力

暗号鍵は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。暗号鍵が暗号モジュールに入力又は暗号モジュールから出力される場合には、鍵の入力又は出力は、手動(例えば、キーボードを介して)、又は電子的方法(例えば、スマートカード/トークン、PCカード、又は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、全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されるか、又は暗号モジュールから出力されてもよい。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、鍵が割り当てられている正しいエンティティ(例えば、人、グループ、又はプロセス)に関係づけなければならない。

手動で入力される暗号鍵(手動の方法を用いて入力された鍵)は、暗号モジュールへの入力の間に、正確を期して 4.9.2 節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コンポーネントが暗号モジュールに手動で入力される場合には、暗号鍵又は鍵コンポーネントの平文の値は、表示されてはならない。

文書は、暗号モジュールに用いられる鍵入力の方法及び鍵出力の方法を規定しなければならない。

セキュリティレベル1及び2

セキュリティレベル 1 及び 2 において、自動化された方法を用いて確立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。手動の方法を用いて確立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

セキュリティレベル3及び4において、

・自動化された方法を用いて確立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。

・手動の方法を用いて確立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)知識分散の手順(すなわち、2 つ又はそれ以上の平文の暗号鍵コンポーネントのように)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。

知識分散の手順が用いられる場合には、

□暗号モジュールは、それぞれの鍵コンポーネント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。

□平文の暗号鍵コンポーネントが不注意に格納、結合、又はその他の手段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通ることなしに、平文の暗号鍵コンポーネントが、直接、(例えば、高信頼パス又は直接接続されたケーブルを介して)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。(4.2 節参照)

□元の暗号鍵を再組立てするために、少なくとも 2 つの鍵コンポーネントが要求されなければならない。

□文書は、n 個の鍵コンポーネント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 個の鍵コンポーネントの知識も長さ以外に元の鍵の情報を提供しないことを証明しなければならない。

□文書は、暗号モジュールに用いられる手順を規定しなければならない。

4.7.5 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、許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、鍵が割り当てられている正しいエンティティ(例えば、人、グループ、又はプロセス)とを関係づけなければならない。

文書は、暗号モジュールに用いられる鍵の格納方法を規定しなければならない。

4.7.6 鍵のゼロ化

暗号モジュールは、暗号モジュール内における平文の秘密鍵及びプライベート鍵の全て、並びにその他の保護されていない CSP の全てをゼロ化するための方法を提供しなければならない。暗号化された暗号鍵及び CSP のゼロ化又は暗号化とは違う方法として付加的に組込まれ認定された暗号モジュール(この標準の要求事項を満たすもの)内で物理的若しくは論理的に保護されている鍵のゼロ化は要求されない。

文書は、暗号モジュールに用いられる鍵のゼロ化方法を規定しなければならない。

4.8 電磁妨害/電磁両立性(EMI/EMC)

暗号モジュールは、EMI/EMC について、次の要求事項を満たさなければならない。無線は、これらの要求事項から明白に除外されるが、全ての該当する FCC 要求事項を満たさなければならない。

文書は、EMI/EMC要求事項に適合していることの証明を含まなければならない。

セキュリティレベル1及び2

セキュリティレベル1及び2において、暗号モジュールは、47 Code of Federal Regulation, part15, Subpart B, Unintentional Radiators, Digital Devices, Class A(すなわち、

商用)に規定されたEMI/EMC要求事項に(最低限)適合していなければならない。

セキュリティレベル3及び4

セキュリティレベル3及び4において、暗号モジュールは、47 Code of Federal Regulation, part15, Subpart B, Unintentional Radiators, Digital Devices, Class B(すなわち、家庭用)に規定されたEMI/EMC要求事項に(最低限)適合していなければならない。

4.9 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、この標準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、状態出力インタフェースを通じてエラーインジケータを出力しなければならない。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全てのデータ出力は、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、次を規定しなければならない：

- 電源投入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

- 及び、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、これは、暗号モジュールのメンテナンス、又は修理のために暗号モジュールをベンダに返却することを含んでもよい。)

4.9.1 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、リブート等の後で)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､オペレータの介在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(すなわち、成功又は失敗の表示)は“ 状態出力 ” インタフェースを通じて出力されなければならない。出力インタフェースを通る全てのデータ出力は、パワーアップ自己テストが実行される時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：
暗号アルゴリズムテスト、ソフトウエア/ファームウエア完全性テスト、重要機能テスト

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、及び乱数生成)の全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でなければならない。

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(例えば､デジタル署名アルゴリズム)は、既知解テストを用いてテストされるか、又は(次に規定された)鍵ペア整合性テスト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が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(例えば、デジタル署名標準)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２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。

・その2つの実装の出力は連続的に比較されなければならない。

・及び、2つの実装の出力が等しくない際は、暗号アルゴリズムテストは失敗としなければならない。

ソフトウエア/ファームウエア完全性テスト

エラー検出コード(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)を用いるソフトウエア/ファームウエア完全性テストは、暗号モジュール内の、全ての認証されたソフトウエア及びファームウエアコンポーネントに対して、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。ソフトウエア/ファームウエア完全性テストは、この標準(4.1章参照)のセキュリティ要求事項から除外されたソフトウエアコンポーネント及びファームウエアコンポーネントには要求されない。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、ソフトウエア/ファームウエア完全性テストは失敗でなければならない。

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。

重要機能テスト

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は、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。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全てを規定し、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。

4.9.2 条件自己テスト

条件自己テストは、次のテストで規定される条件が発生するときに、暗号モジュールによって実行されなければならない。
鍵ペア整合性テスト、ソフトウエア/ファームウエアロードテスト、手動鍵入力テスト、連続乱数生成器テスト、及びバイパステスト。

(公開鍵及びプライベート鍵の)鍵ペア整合性テスト

暗号モジュールが公開鍵又はプライベート鍵を生成する場合には、公開鍵及びプライベート鍵に対して、次の鍵ペア整合性テストが実行されなければならない。

1. 公開鍵及びプライベート鍵が承認された鍵配送方法を行うために用いられる場合には、公開鍵は平文の値を暗号化しなければならない。その結果の暗号文の値は、元の平文の値と比較されなければならない。2つの値が等しい場合には、そのテストは失敗としなければならない。2つの値が異なる場合には、プライベート鍵は暗号文を復号するために用いられ、かつ、その結果の値は元の平文の値と比較されなければならない。2つの値が等しくない場合には、そのテストは失敗としなければならない。

2. 公開鍵及びプライベート鍵がデジタル署名の計算及び検証を行うために用いられる場合には、２つの鍵の整合性は、デジタル署名の計算及び検証によってテストされなければならない。デジタル署名を検証できない場合には、そのテストを失敗としなければならない。

ソフトウエア/ファームウエアロードテスト

ソフトウエアコンポーネント又はファームウエアコンポーネントを外部から暗号モジュール内にロードできる場合には、次のソフトウエア/ファームウエアロードテストが実行されなければならない。

1. 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、デジタル署名アルゴリズム、又はHMAC)は、認証されたソフトウエアコンポーネント及びファームウエアコンポーネントが外部から暗号モジュール内にロードされるときに、それらのコンポーネントの全てに適用されなければ

ならない。ソフトウエア/ファームウエアロードテストは本標準のセキュリティ要求事項から除外された任意のソフトウエア及びファームウエアコンポーネントについては要求されない。(4.1節参照)

2.計算された結果は、あらかじめ生成された結果と比較されなければならない。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、ソフトウエア/ファームウエア完全性テストは失敗としなければならない。

手動鍵入力テスト

暗号鍵又は暗号鍵コンポーネント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。

1.暗号鍵又は暗号鍵コンポーネントはEDCがつけられているか、又は繰り返し入力を用いて入力されなければならない。

2.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。

3.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。

連続乱数生成器テスト

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RNG又は承認されていないRNGを用いる場合には、暗号モジュールは、それぞれのRNG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生成器テストを実行しなければならない。

1.RNG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。その後に続いて生成される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。2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。

2.RNG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。その後に続いて生成される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。2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する。

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って平文を転送すること)バイパス能力を実装している場合には、暗号モジュールコンポーネント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は実行されなければならない。

1. 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。

2. 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際(例えば、IPアドレスのソース/ディスティネーション表)、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。

文書は、切替え手順を管理する、メカニズム又は論理を規定しなければならない。

4.10 設計保証

設計保証は、暗号モジュールの設計、配置、及び運用において、暗号モジュールが適切にテスト、構成、配付、設置、及び開発される保証の提供、並びに適切なオペレータガイダンス文書が提供される保証を提供することについて暗号モジュールのベンダによる最善の実行手順を指す。セキュリティ要求事項は、構成管理、配付及び運用、開発、並びにガイダンス文書について規定される。

4.10.1 構成管理

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ために、暗号モジュールベンダによって実施される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コンポーネントに対して、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要素(例えば、暗号モジュール、暗号モジュールコンポーネント、ユーザガイダンス、セキュリティポリシ、及び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。

4.10.2 配付及び運用

配付及び運用は、暗号モジュールが、許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、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

セキュリティレベル1において、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規定しなければならない。

セキュリティレベル2、3**及び**4

セキュリティレベル2、3及び4において、セキュリティレベル1の要求事項に加えて、文書は、許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規定しなければならない。

4.10.3 開発

開発は、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

ュールの振舞いの高位記述を指す。

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。

・文書は、暗号モジュールのハードウエアコンポーネント、ソフトウエアコンポーネント、及びファームウエアコンポーネントの設計と暗号モジュールのセキュリティポリシとの対応を規定しなければならない。(4.1 節参照)

・暗号モジュールがソフトウエアコンポーネント又はファームウエアコンポーネントを含む場合には、文書は、コンポーネント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注釈をつけた、ソフトウエアコンポーネント及びファームウエアコンポーネントのソースコードを規定しなければならない。

・暗号モジュールがハードウエアコンポーネントを含む場合には、文書は、ハードウエアコンポーネントの回路図及び/又はハードウエア記述言語(HDL)のソースコードを規定しなければならない。

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規定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全てのソフトウエアコンポーネント及びファームウエアコンポ

ーネントは、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、アセンブラ言語又はマイクロコード)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全てのハードウエアコンポーネントは、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。

・文書は、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的モデルを規定しなければならない。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規定されなければならない。

・文書は、暗号モジュールのセキュリティポリシについて、形式的モデルの一致及び完全性を実証する根拠を規定しなければならない。

・文書は、形式的モデルと機能仕様との対応に関する、非形式的な証明を規定しなければならない。

・暗号モジュールのそれぞれのハードウエアコンポーネント、ソフトウエアコンポーネント、及びファームウエアコンポーネントに対して、ソースコードは、(1)正しく実行するために暗号モジュール、関数、又は手続きへの入力に必要な事前条件、及び(2)暗号モジュールコンポーネント、関数、又は手続き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規定するコメントを用いて注釈がつけられなければならない。事前条件及び事後条件は、暗号モジュールコンポーネント、関数、又は手続きの振舞いを完全、かつ、明快に、説明するのに十分詳細な注釈を用いて規定されてもよい。

・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、非形式的な証明を規定しなければならない。

全てのセキュリティレベルにおける推奨ソフトウエア開発手順

APPENDIX B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エアコンポーネント及びファームウエアコンポーネントの実装は、そのコンポーネントのこの標準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であろう。

4.10.4 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、方法、ガイドライン、及び警告とともに、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は、次を規定しなければならない。

- 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、セキュリティパラメータ(及び、必要ならば、パラメータ値)、物理ポート、及び論理インタフェース。

- 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。

- 及び、暗号モジュールのセキュアな動作に関係するユーザの振る舞いについての前提条件。

ユーザガイダンスは、次を規定しなければならない。

- 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。

- 暗号モジュールのセキュアな運用のために必要な全てのユーザ責任。

4.11 その他の攻撃への対処

暗号モジュールは、本標準のこのバージョンが発行された時点で試験可能なセキュリティ

要求事項を用意できなかったその他の攻撃(例えば、電力解析、タイミング解析、故障利用)、又は標準の適用範囲外であった攻撃(例えば、テンペスト)に対して、影響を受けやすい場合がある。そのような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許可されたオペレータになるかも知れない環境)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。全ての場合において、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は次の通りである。

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考えられる。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係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持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１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。

テンペスト

テンペスト攻撃は、暗号モジュール及び関連の装置が処理中に放射する電磁信号を遠隔又は外部で検知し、収集することをいう。そのような攻撃は、キーストローク情報、ビデオ画面に表示されるメッセージ、その他のフォームの重要なセキュリティ情報(例えば、暗号鍵)を得るために使用される。ネットワークケーブルを含む全てのコンポーネントの特殊なシールドは、そのような攻撃のリスクを減らすために使用されるメカニズムである。シールドは、電磁信号の放射を減らし、場合によっては電磁信号の放射を防止する。

暗号モジュールが 1 つ又はそれ以上の特定の攻撃に対処するように設計される場合には、暗号モジュールのセキュリティポリシは、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規定しなければならない。要求事項及び関係した試験が開発されるとき、そのセキュリティメカニズムの存在及び適切に機能していることが認証されるであろう。

APPENDIX A：文書要求事項のまとめ

次のチェックリストは、この標準の文書の要求事項を要約している。全ての文書は、暗号モジュールのベンダによって認証機関に提出されなければならない。

暗号モジュールの仕様

・暗号モジュールのハードウエア、ソフトウエア、及びファームウエアのコンポーネントを規定すること。これらのコンポーネントを囲む暗号境界を規定し、並びに暗号モジュールの物理的な構成を記述すること。(セキュリティレベル1、2、3、及び4)

・この標準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エア、ソフトウエア及びファームウエアのコンポーネントを規定して、適用除外とする根拠を説明すること。(セキュリティレベル1、2、3、及び4)

・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を規定すること。(セキュリティレベル1、2、3、及び4)

・暗号モジュールのマニュアル又は論理的な制御、物理的又は論理的な状態表示、及びそれらの物理的、論理的、及び電気的な特徴を規定すること。(セキュリティレベル1、2、3、及び4)

・承認されているかどうかに関わらず、暗号モジュールに採用される全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関わらず、全ての動作モードを規定すること。

・暗号モジュールの主要なハードウエアコンポーネントの全て及びそれらの接続関係を示すブロック図を規定すること。これには、マイクロプロセッサ、入出力バッファ、平文データ用のバッファ/暗号化されたデータ用のバッファ、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、及び4)

・暗号モジュールのハードウエア、ソフトウエア、及びファームウエアのコンポーネントの設計を規定すること。(セキュリティレベル1、2、3、及び4)

・秘密鍵及びプライベート鍵(平文の状態、及び暗号化された状態の両方)、認証データ(例えば、パスワード、PIN)、その他のCSP、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殆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、全てのセキュリティに関係する情報を規定すること。

・暗号モジュールのセキュリティポリシを規定すること。このセキュリティポリシは、この文書の要求事項から導かれる規則、及びベンダから提示された追加要求事項から導かれる規則を含むこと。

暗号モジュールのポート及びインタフェース

・物理的ポート及び論理的インタフェース及び定義された全ての入出力データパスを規定すること。(セキュリティレベル1、2、3、及び4)

役割,サービス,及び認証

・暗号モジュールがサポートする全ての許可された役割を規定すること。(セキュリティレベル1、2、3、及び4)

・暗号モジュールによって提供される、承認されている及び承認されていない両方の、サービス、動作、又は機能を規定すること。暗号モジュールによって提供される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許可された(1つ又は複数の)役割を規定すること。

・オペレータが許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、並びにそれらのサービスが、暗号鍵及びその他のCSPを変更、開示、若しくは置換する方法、又は暗号モジュールのその他のセキュリティへの影響を規定すること。

・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許可された方法及び暗号モジュールによってサポートされた認証メ

カニズムの強度を規定すること。(セキュリティレベル2、3、及び4)

有限状態モデル

・状態遷移図及び/又は状態遷移表を用いて有限状態(又は同等のもの)を表現すること。また、その状態遷移図及び/又は状態遷移表は、暗号モジュールの動作状態及びエラー状態の全て、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)を規定すること。(セキュリティレベル 1、2、3、及び 4)

物理的セキュリティ

・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規定すること。暗号モジュールの物理的セキュリティのメカニズムを規定すること。(セキュリティレベル1、2、3、及び4)

・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(例えば、暗号モジュールのベンダによる、又は他の許可された個人による)物理的アクセスを許す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を規定して、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、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 がどのようにゼロ化されるかを規定すること。(セキュリティレベル 1、2、3、及び 4)

・暗号モジュールの正規の動作範囲を規定すること。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規定するか、又は行われる環境故障試験を規定しなければならない。(セキュリティレベル 4)

動作環境

・暗号モジュールに対する動作環境を規定しなければならない。(セキュリティレベル 1、2、3、及び 4)

・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 PP 及び CC 保証レベルを規定すること。(セキュリティレベル 2、3、及び 4)

暗号鍵管理

・暗号モジュールに用いられる全ての暗号鍵、暗号鍵コンポーネント、及びその他の CSP を規定すること。

・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)RNG のそれぞれを規定すること。(セキュリティレベル 1、2、3、及び 4)

・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を規定すること。(セキュリティレベル1、2、3、及び4)

・暗号モジュールに用いられる鍵確立の方法を規定すること。(セキュリティレベル1、2、3、及び4)

・暗号モジュールに用いられる鍵入力の方法及び鍵出力の方法を規定すること。

・知識分散の手順が用いられる場合には、n 個の鍵コンポーネント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 個の鍵コンポーネントの知識も長さ以外に元の鍵の情報を提供しないことを証明し、暗号モジュールに用いられる手順を規定すること。(セキュリティレベル 3 及び 4)

・暗号モジュールに用いられる鍵の格納方法を規定すること。(セキュリティレベル1、2、3、及び4)

・暗号モジュールに用いられる鍵のゼロ化方法を規定すること。(セキュリティレベル 1、2、3、及び 4)

電磁妨害/電磁両立性

・EMI/EMC 要求事項に適合していることを証明すること。(セキュリティレベル 1、2、3、及び 4)

自己テスト

・電源投入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を規定すること。(セキュリティレベル 1、2、3、及び 4)

・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を規定すること。(セキュリティレベル 1、2、3、及び 4)

・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全てを規定し、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すること。(セキュリティレベル 1、2、3、及び 4)

・暗号モジュールがバイパス能力を実装している場合には、切替え手順を管理する、メカニズム又は論理を規定すること。(セキュリティレベル 1、2、3、及び 4)

設計保証

・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規定すること。(セキュリティレベル 1、2、3、及び 4)

・許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規定すること。(セキュリティレベル 2、3、及び 4)

・暗号モジュールのハードウエアコンポーネント、ソフトウエアコンポーネント、及びファームウエアコンポーネントの設計と暗号モジュールのセキュリティポリシとの対応を規定すること。(セキュリティレベル 1、2、3、及び 4)

・暗号モジュールがソフトウエアコンポーネント又はファームウエアコンポーネントを含む場合には、コンポーネント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注釈をつけた、ソフトウエアコンポーネント及びファームウエアコンポーネントのソースコードを規定すること。(セキュリティレベル1、2、3、及び4)

・暗号モジュールがハードウエアコンポーネントを含む場合には、ハードウエアコンポーネントの回路図及び/又はハードウエア記述言語(HDL)のソースコードを規定す

ること。(セキュリティレベル1、2、3、及び4)

・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規定すること。(セキュリティレベル2、3、及び4)

・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て、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を規定しなければならない。(セキュリティレベル4)

・暗号モジュールのセキュリティポリシについて、形式モデルの一致及び完全性を実証する根拠を規定すること。(セキュリティレベル4)

・形式モデルと機能仕様との対応に関する、非形式的な証明を規定すること。(セキュリティレベル4)

・暗号モジュールのそれぞれのハードウエアコンポーネント、ソフトウエアコンポーネント、及びファームウエアコンポーネントに対して、(1)正しく実行するために暗号モジュール、関数、又は手続きへの入力に必要な事前条件、及び(2)暗号モジュールコンポーネント、関数、又は手続き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規定するコメントを用いて注釈がつけられたソースコードを規定すること。(セキュリティレベル4)

・(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、非形式的な証明を規定すること。(セキュリティレベル4)

・クリプトオフィサガイダンスは、次を規定すること。

□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、セキュリティパラメータ(及び、必要ならば、パラメータ値)、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、及び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、及び4)

□及び、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、及び 4)

・ユーザガイダンスは、次を規定すること。

□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、及び 4)

□暗号モジュールのセキュアな運用のために必要な全てのユーザ責任。(セキュリティレベル 1、2、3、及び 4)

その他の攻撃への対処

・暗号モジュールが1つ又はそれ以上の特定の攻撃に対処するように設計される場合には、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を規定すること。(セキュリティレベル1、2、3、及び4)

セキュリティポリシ

・Appendix C参照。(セキュリティレベル1、2、3、及び4)

APPENDIX B：推奨ソフトウエア開発手順

この Appendix は、情報提供のみを目的としており、この標準の範囲にある暗号モジュールに適用するセキュリティ要求事項を含まない。

ライフサイクルソフトウエアエンジニアリング(ソフトウエアの仕様、構造、検証、試験、メンテナンス、及び文書の扱い)の推奨は、次のようでなければならない。ソフトウエ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エア開発プロセスを含んでもよい。

大規模、小規模に関わらず、全てのソフトウエア開発において、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エアコンポーネント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なければならない。

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エ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エアモジュールは、明確で容易に理解される論理的インターフェースをもたなければならない。

・ソフトウエアコンポーネントは、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なければならない。

・ソフトウエアは、一連の階層構造として構造化されなければならない。

ソフトウエアモジュール/プロシージャインタフェース

・ソフトウエアモジュール又は手続きへのエントリは、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なければならない。

・それぞれのプロシージャは、1 つのエントリポイント及び多くとも 2 つのエグジットポイント(1 つは正常エグジットで、1 つはエラーエグジット)を持たなければならない。

・データは、引数リスト及び/又は明示的な戻り値を用いて、ソフトウエアモジュール間及びプロシージャ間で通信されなければならない。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てはならない。入力値は、アサーション文を用いて(使用するプログラミング言語によって提供される場合)、範囲エラーチェックがされなければならない。

内部構造

・それぞれのプロシージャは、単一で、明確な関数のみを実行しなければならない。

・単一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なければならない。

・(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、ソフトウエアコンポーネントは、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しなければならない。

・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られてはならない。

・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、範囲外のパラメータ、及び入出力バッファーオーバーフローに対して保護するために実装されなければならない。

インライン文書

・それぞれのソフトウエアモジュール、プロシージャ、及び主要なプログラミング構文は、実行される関数を規定するために、(形式的な又は非形式的な)事前条件及び事後条件の規定と共に文書化されなければならない。

・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)が記述されなければならない。

・変数名は、同じプロシージャの中で 1 つの意味にのみ使用されなければならない。

・それぞれの変数は、変数の目的を識別する関連のコメント及び範囲が制限されていない場合を含め、許容値の範囲を注記する関連のコメントを持たなくてはならない。

・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規定しなければならない。

アセンブラ言語

次の付加的なプログラミング手順は、実装がアセンブラ言語のときに使用されなければならない。

・全てのコードは、特定のセキュリティ上の目的、効率、又はハードウエア制限が位置に依存することを要求する場合を除いて、位置に依存されてはならない。

・全てのレジスタ参照はシンボリックレジスタ名を使用しなければならない。

・自己変更コードは使用してはならない。

・全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たなければならない。

・制御遷移命令は、数値リテラルを使用してはならない。

・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まなければならない。

APPENDIX C：暗号モジュールのセキュリティポリシ

暗号モジュールのセキュリティポリシは、ベンダが提供する文書に含まれていなければならない。次のパラグラフは、セキュリティポリシの要求内容の概略を述べる。

C.1 暗号モジュールのセキュリティポリシの定義

暗号モジュールのセキュリティポリシは、次から構成されなければならない：

・本標準の要求事項に基づくセキュリティルール及びベンダによって課された付加的なセキュリティルールを含む、暗号モジュールが動作中に従うべきセキュリティルールの規定。

その規定は、次の質問に答えるほど十分詳細でなければならない。

・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があるか。

・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。

・本標準で試験可能な要求事項が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。

C.2 暗号モジュールのセキュリティポリシの目的

明確な暗号モジュールのセキュリティポリシを開発し、従う目的は主に 2 つある。

・暗号モジュールが、実装時に、述べられたセキュリティポリシを満足するかどうかを個人及び組織が判定することを許可する暗号セキュリティの仕様を供給するため。

・暗号モジュールによって提供される能力、防御、及びアクセス権を個人及び組織に宣言するため。これによって、暗号モジュールが個人又は組織のセキュリティ要求事項を適切に供給するかどうかのアセスメントを許可する。

C.3 暗号モジュールのセキュリティポリシの規定

暗号モジュールのセキュリティポリシは、役割、サービス、並びに暗号鍵及び CSP に関する項目について表現されなければならない。最低限、次が規定されなければならない：

・識別と認証(I&A)ポリシ

・アクセス制御ポリシ

・物理的セキュリティポリシ

・及び、その他の攻撃への対処のためのセキュリティポリシ

C.3.1 識別と認証ポリシ

暗号モジュールのセキュリティポリシは、次を含む識別と認証ポリシを規定しなければならない：

・全ての役割(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、又は無し)

・及び、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

C.3.2 アクセス制御ポリシ

暗号モジュールのセキュリティポリシは､アクセス制御ポリシを規定しなければならない。規定は､サービス実行中に､オペレータがアクセス可能な暗号鍵及びその他のCSP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持つアクセスタイプを識別するために、十分詳細でなければならない。

セキュリティポリシは次を規定しなければならない：

・暗号モジュールにサポートされた全ての役割、

・暗号モジュールに提供される全てのサービス、

・暗号モジュールに採用される全ての暗号鍵及びその他の CSP、これらは次を含む

□(平文と暗号文の両方の)秘密鍵、プライベート鍵、及び公開鍵、

□パスワード又は PIN のような認証データ、

□及び、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許可されたサービス、

・それぞれの役割の中でのそれぞれのサービスにおいて、暗号鍵及びその他の CSP へアクセスするタイプ。

C.3.3 物理的セキュリティポリシ

暗号モジュールのセキュリティポリシは、次を含む、物理的セキュリティポリシを規定しなければならない。

・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)、

・及び、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)

C.3.4 その他の攻撃への対処ポリシ

暗号モジュールのセキュリティポリシは、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を規定しなければならない。

C.4 セキュリティポリシチェックリスト表

次のチェックリスト表は、セキュリティポリシが完全であり、かつ、適切な詳細を含んでいることを確実にするためのガイドとして使用されてもよい。

役割	認証のタイプ	認証データ
・・・	・・・	・・・
・・・	・・・	・・・

表C1. 役割、並びに必要な識別及び認証

認証メカニズム	メカニズムの強度
・・・	・・・
・・・	・・・

表C2. 認証メカニズムの強度

役割	許可されたサービス
・・・	・・・
・・・	・・・

表C3. 役割に対して許可されたサービス

サービス	暗号鍵及びその他のCSP	アクセスのタイプ (例えば、リード/ライト/実行)
...	...	...
...	...	...

表C4. サービスにおけるアクセス権

物理的セキュリティ メカニズム	推奨する検査/試験の 繰り返し数	検査/試験のガイダンス詳細
...	...	...
...	...	...

表C5. 物理的セキュリティメカニズムの検査/試験

その他の攻撃	対処メカニズム	特定の制限
...	...	...
...	...	...

表C6. その他の攻撃への対処

APPENDIX D:参考文献

American Bankers Association, *Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA),* ANSI X9.31-1998, Washington, D.C., 1998.

American Bankers Association, *Triple Data Encryption Algorithm Modes of Operation,* ANSI X9.52-1998, Washington, D.C., 1998.

American Bankers Association, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm,* American National Standard X9.62-1998, Washington, D.C., 1998.

Common Criteria Implementation Board (CCIB), *International Standard (IS) 15408, Common Criteria for Information Technology Security Evaluation,* Version 2, May 1998, ISO/IEC JTC 1 and Common Criteria Implementation Board.

Computer Security Act of 1987, 40 U.S. Code 759, (Public Law 100-235), January 8, 1988.

Department of Defense, *Department of Defense Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD, December 1985.

Information Technology Management Reform Act of 1996, U.S. Code, (Public Law 104-106), 10 February *1996.*

Information Technology Security Evaluation Criteria (ITSEC), Harmonized Criteria of France – Germany - the Netherlands - the United Kingdom, Version 1.1, January 1991.

Keller, Sharon and Smid, Miles, *Modes of Operation Validation System (MOVS): Requirements and Procedures*, Special Publication 800-17, Gaithersburg, MD, National Institute of Standards and Technology, February 1998.

Keller, Sharon, *Modes of Operation Validation System for the Triple Data Encryption*

Algorithm (TMOVS): Requirements and Procedures, Special Publication 800-20, Gaithersburg, MD, National Institute of Standards and Technology, October 1999.

Lee, Annabelle, *Guideline for Implementing Cryptography in the Federal Government*, Special Publication 800-21, Gaithersburg, MD, National Institute of Standards and Technology, November, 1999.

National Institute of Standards and Technology, *FIPS 140-2 Annex A: Approved Security Functions*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex B: Approved Protection Profiles*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex C: Approved Random Number Generators*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex D: Approved Key Establishment Techniques*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *Computer Data Authentication,* Federal Information Processing Standards Publication 113, 30 May 1985.

National Institute of Standards and Technology, *Data Encryption Standard*, Federal Information Processing Standards Publication 46-3, October 25, 1999.

National Institute of Standards and Technology and Communications Security Establishment, *Derived Test Requirements(DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules,* available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *DES Modes of Operation,* Federal Information Processing Standards Publication 81, December 2, 1980.

National Institute of Standards and Technology, *Digital Signature Standard (DSS),* Federal Information Processing Standards Publication 186-2, January 27, 2000.

National Institute of Standards and Technology, *Digital Signature Standard*

Validation System (DSSVS) User's Guide, June 20, 1997.

National Institute of Standards and Technology, *Entity Authentication Using Public Key Cryptography*, Federal Information Processing Standards Publication 196, February 18, 1997.

National Institute of Standards and Technology, *Guideline for the Use of Advanced Authentication Technology Alternatives*, Federal Information Processing Standards Publication 190, September 28, 1994.

National Institute of Standards and Technology and Communications Security Establishment, *Implementation Guidance (IG) for FIPS 140-2*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *Key Management using ANSI X9.17*, Federal Information Processing Standards Publication 171, April 27, 1992.

National Institute of Standards and Technology, *Secure Hash Standard*, Federal Information Processing Standards Publication 180-1, April 17, 1995.

National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards Publication 140-1, January 11, 1994.

Office of Management and Budget, *Security of Federal Automated Information Resources*, Appendix III to OMB Circular No. A-130, February 8, 1996.

Telecommunications Industry Association, *Over-The-Air-Rekeying (OTAR) Protocol*, New Technology Standards Project, Digital Radio Technical Standards, TIA/EIA Telecommunications Systems Bulletin, APCO Project 25, TSB102.AACA, January 1996.

APPENDIX E: 使用可能なインターネットの URL

Communications Security Establishment (CSE): http://www.cse-cst.gc.ca

Cryptographic Module Validation Program (CMVP): http://www.nist.gov/cmvp

NIST Information Technology Laboratory (NIST ITL): http://www.nist.gov/itl

NIST Security Publications including FIPS and Special Publications: http://csrc.nist.gov/publications

National Technical Information Service (NTIS): http://www.ntis.gov

National Voluntary Laboratory Accreditation Program (NVLAP): http://ts.nist.gov/nvlap

National Information Assurance Partnership® (NIAP): http://niap.nist.gov/

Validated Protection Profiles: http://niap.nist.gov/cc-scheme/PPRegistry.html