# 暗号モジュール試験基準第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、米国NIST[1]が発行する“Derived Test Requirements for FIPS PUB 140-2, Security Requirement for Cryptographic Modules (March 24, 2004 Draft)”を翻訳し、さらに、運用ガイダンス第0版の訳語との統一を図るために、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評価基準第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

# 文書構成

この文書は、11 節から構成されている。それぞれの節は、FIPS PUB 140-2 の 11 分野に対応している。

それぞれの節の中で、FIPS PUB 140-2 に対応するセキュリティ要求事項は、アサーションのセット(すなわち、設定されたセキュリティレベルで、設定された分野のセキュリティ要求事項を暗号モジュールが満足するために、適用しなければならない宣言)に分けられる。全てのアサーションは FIPS PUB 140-2 から直接引用されている。

アサーションは次の形式で示される。

AS<requirement_number> <assertion_sequence_number>

<requirement_number>は FIPS140-2 で規定されている分野(1～11)に対応した番号であり、<assertion_sequence_number >はそのアサーションに対応した要求事項のシーケンス番号である。それぞれのアサーションの記述の最後には、そのアサーションが適用されるセキュリティレベル(レベル 1～4)が括弧の中に書かれている。

それぞれのアサーションの次には、ベンダに課せられる要求事項のセットが書かれている。これらの要求事項には、試験者が対応するアサーションに適合しているかどうかを決定するために、ベンダが提供しなければならない文書の種類又は明確な情報の種類が記述されている。これらの要求事項は次の形式で示される。

VE<requirement_number> <assertion_sequence_number> <sequence_number>

<requirement_number> 及び <assertion_sequence_number> は、対応する AS の <requirement_number>及び<assertion_sequence_number>と同一であり、<sequence_number> は、<assertion_sequence _number>に対応した「ベンダに課せられる要求事項」のシーケンス番号である。

また、それぞれのアサーション及びベンダに課せられる要求事項の次には、暗号モジュールの試験者に課せられる要求事項のセットが書かれている。これらの要求事項は、それぞれのアサーションに対する暗号モジュールの試験を行うためには何をしなければならないかについて、試験者に指示するものである。これらの要求事項は次の形式で示される。

TE<requirement_number> <assertion_sequence_number> <sequence_number>

<requirement_number> 及び <assertion_sequence_number> は、対応する AS の <requirement_number>及び<assertion_sequence_number>と同一であり、<sequence_number> は、<assertion_sequence _number>に対応した「試験者に課せられる要求事項」のシーケンス番号である。

# 目次

# 1．暗号モジュールの仕様

**AS01.01：(レベル 1，2，3，及び 4)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。**
注：このアサーションは、個別には試験されない。

**AS01.02：(レベル 1，2，3，及び 4)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。**
注：このアサーションは、AS01.12の一部として試験される。

**AS01.03：(レベル1，2，3，及び4)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。**

**VE01.03.01：**ベンダが提供する公開用セキュリティポリシは、承認された動作モードについて記述しなければならない。

**VE01.03.02：**ベンダが提供する公開用セキュリティポリシは、承認された動作モードを呼出すための方法を記述しなければならない。

**TE01.03.01**：試験者は、ベンダが提供する公開用セキュリティポリシに、承認された動作モードについての記述があることを検証しなければならない。

**TE01.03.02：**試験者は、ベンダが提供する公開用セキュリティポリシに記載されている方法を用いて、承認された動作モードを発起しなければならない。

**AS01.04：(レベル3及び4)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。**
[解説]
レベル1，2では、表示の必要はない。

**VE01.04.01：**ベンダが提供する公開用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にあることの表示法を記述しなければならない。

**VE01.04.02：**ベンダが提供する公開用セキュリティポリシは、承認された動作モードにあることを表示させるための方法を記述しなければならない。

**TE01.04.01：**試験者は、ベンダが提供する公開用セキュリティポリシが、暗号モジュールが承認された動作モードにあることを表示する方法についての記述を含んでいることを検証しなければならない。

**TE01.04.02：**試験者は、ベンダが提供する公開用セキュリティポリシに記述されている方法を用いて、承認された動作モードを表示させなければならない。

**AS01.05：(レベル 1，2，3，及び 4)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。**
注：このアサーションは、AS01.08の一部として試験される。

**AS01.06：(レベル1，2，3，及び4)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。**

**VE01.06.01：**ベンダは、暗号モジュール内のそれぞれのプロセッサに対して、主なサービスごとに、そのプロセッサで実行されるソフトウエア又はファームウエア、及び、その実行コード及びデータを格納するメモリデバイスを特定しなければならない。
[解説]
例えば、設計文書に記述すること。

**VE01.06.02：**ベンダは、それぞれのプロセッサに対して、プロセッサがインタフェースを持つ全てのハードウエアを特定しなければならない。
[解説]
例えば、設計文書に記述すること。

**TE01.06.01:**試験者は、このアサーションに基づいて特定されたそれぞれのプロセッサが、アサーションAS01.08に基づくマスターコンポーネントリスト、及びアサーションAS01.08に基づいて定義された暗号境界の中に含まれていることを検証しなければならない。

**TE01.06.02：**試験者は、ベンダが、それぞれのプロセッサに対し、プロセッサによって実行されるソフトウエア又はファームウエアコードモジュール、プロセッサ及び対応するコードによって実行されるサービス、並びに実行可能なコード及びデータを含むメモリデバイスを特定していることを検証しなければならない。

**TE01.06.03：**試験者は、ベンダが、それぞれのプロセッサに対し、プロセッサがインタフェースを持つ全てのハードウエアについて特定していることを検証しなければならない。これは、該当する場合には、プロセッサ及び関連するソフトウエア/ファームウエアに入力

データ、制御データ又は状態データを提供する全てのハードウエアコンポーネント、並びにプロセッサ及び関連するソフトウエア/ファームウエアから出力データ、制御データ又は状態データを受け取る全てのハードウエアコンポーネントを含まなければならない。このようなハードウエアコンポーネントは、暗号モジュールの中にあってもよく、又は入出力デバイスのようなモジュールの外側にあるユーザ装置であってもよい。

[解説]

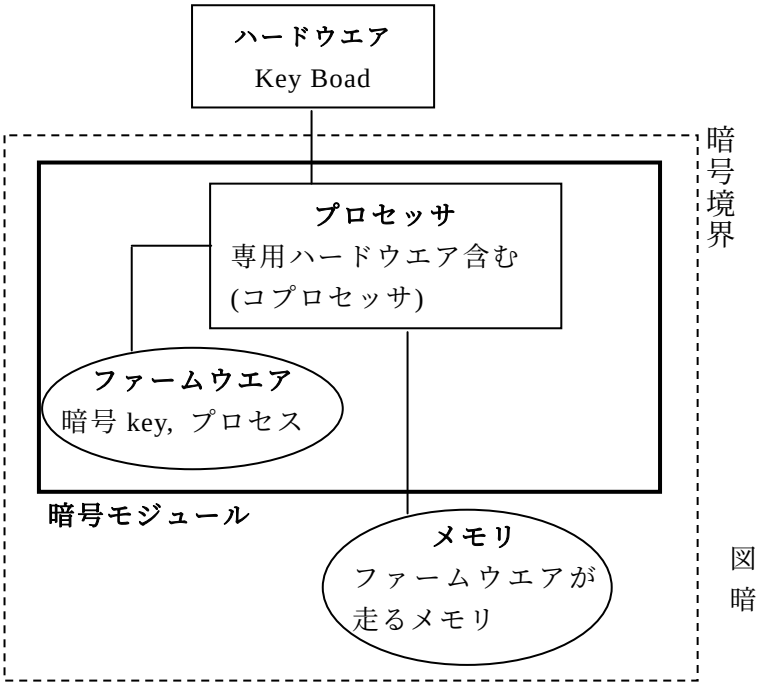



図　AS01.06 で規定する暗号境界の概念例

**AS01.07：(レベル 1，2，3，及び 4)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。**

注：このアサーションは、個別には試験されない。

**AS01.08：(レベル1，2，3，及び4)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。**

**VE01.08.01：**ベンダが提供する文書は、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全てのコンポーネントが規定されていなければならない。リスト化すべきコンポーネントには、次に掲げる項目に該当するすべてが含まれなければならない：

1. プロセッサ、メモリ、（セミ）カスタム IC を含む集積回路
2. 他の能動的電子回路部品
3. 電源入力、電源出力及び内部電源又はコンバータ
4. 回路ボード又はその他の搭載板、囲い、及びコネクタを含む物理構造
5. ソフトウエア及びファームウエアモジュール

6. 上記に記載されていない他のコンポーネント

**VE01.08.02：**上記コンポーネントのリストは、この節の他のアサーションで提示された情報と一貫した内容でなければならない。

**VE01.08.03：**ベンダが提供する文書は、暗号モジュールの暗号境界を規定しなければならない。暗号境界は、明確に定義され、暗号モジュールの物理的境界を確定する途切れのない境界でなければならない。境界の定義は、暗号モジュールのコンポーネント及びコネクション(ポート)を規定しなければならない。また、暗号モジュールの情報の流れ、処理、及び入出力データも規定しなければならない。

**VE01.08.04：**暗号境界は、それを適切に制御しなければ重要情報に危殆化をもたらすことになる重要なセキュリティパラメータを入力、処理、又は出力する、全てのハードウエア又はソフトウエアを含まなければならない。

**VE01.08.05：**ベンダが提供する文書は、その暗号モジュールの物理的形態、すなわち、FIPS PUB 140-2の4.5節で定義された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、又はマルチチップスタンドアロン型暗号モジュールのどれであるかを規定しなければならない。

**VE01.08.06：**ベンダが提供する文書は、暗号モジュールの内部のレイアウト及び組立て方法(例えば、留め金具及び接続金具)を、少なくとも縮小あるいは拡大図面を添えて示さなければならない。集積回路の内部を示す必要はない。

**VE01.08.07：**ベンダが提供する文書は、囲い、アクセスポイント、回路ボード、電源の位置、内部接続配線、冷却装置、及びその他の重要なパラメータを含む、モジュールの主な物理的パラメータを記述しなければならない。

**TE01.08.01：**試験者は、文書が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全てのコンポーネントを記載したマスターコンポーネントリストを含んでいることを検証しなければならない。

**TE01.08.02：**試験者は、マスターコンポーネントリストに、その暗号モジュール内で使用しないコンポーネントを除いて、次に掲げるコンポーネントに該当するものがあれば全て含まれていることを検証しなければならない：

1. マイクロプロセッサ、ディジタルシグナルプロセッサ、カスタムプロセッサ、マイクロコントローラ、又は他のタイプのプロセッサを含むプロセッサ
2. プログラムの実行コード及びデータための読取り専用メモリ(ROM)集積回路(マスクプログラム ROM、紫外線消去可能な PROM［EPROM］、電子的に消去可能な PROM［EEPROM］のようなプログラマブル ROM、又はフラッシュを含む)

3. 一時データ保存用のランダムアクセスメモリ(RAM)集積回路
4. ゲートアレイ、プログラムロジックアレイ、FPGA、又は他のプログラムロジックデバイスのような、セミカスタム、アプリケーションスペシフィック集積回路
5. 暗号モジュールのあらゆるカスタムな集積回路を含む、フルカスタム、アプリケーション特有の集積回路
6. 他のアクティブな電子回路の要素(ベンダは、回路部品が、暗号モジュールのセキュリティ上重要な役割に就かず、暗号モジュールの境界内に無い場合には、プルアップ/プルダウン・レジスタ又はバイパスキャパシタ等の受動回路部品を記載する必要はない)
7. 電源、電圧変換モジュール(例えば、AC-DC、又は DC-DC 変換モジュール)、トランス、入力電源コネクタ、出力電源コネクタを含む、電源コンポーネント
8. 回路ボード、又は他の覆い板を搭載したコンポーネント
9. あらゆる除去可能なアクセスドア又はカバーを含む囲い
10. 暗号モジュールの外側、又は暗号モジュールのあらゆる独立したサブモジュール間のデバイスのための物理的なコネクタ
11. 変更可能なソフトウエアモジュール/ファームウエアモジュール
12. 変更される可能性がなさそうなソフトウエアモジュール/ファームウエアモジュール
13. 上記に記載されていない他のコンポーネントタイプ

**TE01.08.03：**試験者は、マスターコンポーネントリストが、次に定義するようなこの節の他のアサーションで提示された情報と一致した内容であることを検証しなければならない：

1. アサーション AS01.08 に基づく暗号境界の仕様。暗号境界の内側にある全てのコンポーネントがマスターコンポーネントリストに含まれていること、及び暗号境界の外側にある全てのコンポーネントが暗号モジュールのコンポーネントとして記載されていないことを検証する。
2. プロセッサと AS01.06 に基づくソフトウエア/ファームウエアの仕様。マスターコンポーネントリスト内のプロセッサ、ソフトウエアモジュール、ハードウエアモジュールのリストが、アサーション AS01.06 に基づいた仕様と同じであることを検証する。
3. アサーション AS01.08 に基づく物理的構成の仕様。マスターコンポーネントリストにおける物理的構造の記載(回路ボード又はその他の搭載板及び囲いとコネクタを搭載したもの)が、アサーション AS01.08 に基いた仕様と同じであることを検証する。
4. アサーション AS01.13 に基づいたブロック図の仕様。ブロック図に引き出された個々のコンポーネント(例えば、プロセッサ、アプリケーション特有の集積回路)の全てが、マスターコンポーネントリストに記載されていることを検証する。
5. アサーション AS01.09 に基づいた FIPS PUB 140-2 の要求事項から除かれるべき全てのコンポーネント。マスターコンポーネントリストには、そのような除かれるべ

きコンポーネントも記載されていることを検証する。

**TE01.08.04：**試験者は、文書が、暗号境界の物理的な境界線がどこにあるのかを明確に示していることを検証しなければならない。これは、暗号境界の内部にある全ての重要なコンポーネント、及び、それに加えて、暗号境界の外側にある装置に接続された全てのポートをリスト化することで代えることができる。また文書は、全ての重要な情報の流れ及び暗号境界の内側で実行されるべきプロセスのリスト、それに加えて、暗号境界の外側から入力し、外側へ出力するすべての情報がリスト化されていなければならない。

**TE01.08.05：**試験者は、ベンダが提供する文書が、暗号境界にあるコンポーネントが暗号境界を正確に定義するために十分詳細な情報を含むことを検証しなければならない。

**TE01.08.06：**試験者は、暗号境界が物理的に隣接していること、すなわち制御されていない入力、出力、又は暗号モジュールへの他のアクセスを許すような隙間がないことを検証しなければならない(物理的保護とタンパー保護は、FIPS140-2の4.5節に基づく要求事項で別に取り扱われている)。また、暗号モジュールの設計では、重要なセキュリティパラメータ(CSP)、平文データ、又は誤使用により危殆化をもたらすその他の情報が通る経路に、暗号モジュールへの又は暗号モジュールからの制御されていないインタフェースが存在してはならない。

**TE01.08.07：**試験者は、暗号境界が、CSP、平文データ、又は誤使用により危殆化をもたらすその他の情報の入力、出力、又は処理において、この節のアサーションAS01.13に基づくブロック図で識別された全てのコンポーネントを包含していることを検証しなければならない。

**TE01.08.08：**上記の要求事項の部分的な例外として、ベンダは、この節のアサーションAS01.09に基づく要求事項を満たす場合は、特定のコンポーネントにFIPS140-2の要求事項を適用しないことが許される。そのときベンダは、適用除外としたコンポーネントを、実質的にその暗号モジュールの暗号境界の外部にあるように扱ってもよい。この場合、試験者は、適用除外のコンポーネントとそれ以外のコンポーネントとの間の全てのインタフェース又は物理的接続に対し、CSP、平文データ、又は誤使用により危殆化をもたらすその他の情報が、安全でない状態では漏洩されないことを検証しなければならない。

**TE01.08.09：**試験者は、ベンダが提供する文書が、その暗号モジュールがFIPS140-2の4.5節で定義されている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、又はマルチチップスタンドアロン型暗号モジュールのいずれかであることを規定していることを検証しなければならない。

**TE01.08.10：**試験者は、ベンダが提供する文書が、暗号モジュールの重要で識別可能なコンポーネントに関する配置及び寸法を含む暗号モジュールの内部レイアウトを示している

ことを検証しなければならない。これには、少なくとも縮小あるいは拡大図面を含まな　ければならない。

**TE01.08.11：**試験者は、ベンダが提供する文書が、暗号モジュールの主要な物理的部品、及びそれらの組付け方法又は暗号モジュールへの挿入方法を記述していることを検証しなければならない。

**TE01.08.12：**試験者は、ベンダが提供する文書が、暗号モジュールの主要な物理的パラメータを記述していることを検証しなければならない。これは、少なくとも次の項目を含まなければならい：

1. あらゆるアクセスドア又はカバーを含む、囲いの形及び寸法
2. （1つ又は複数の）回路ボードの寸法、レイアウト、及び接続
3. 電源、電力変換器、並びに入力電源及び出力電源の場所
4. 配線ひき回し: 配線経路及び端子配置
5. 暗号モジュールから熱を取り去るための伝導プレート、空気冷却、熱交換、冷却フィン、ファンなどの冷却手段、又はその他の手段
6. 上記に記載されていない他のコンポーネントタイプ

**AS01.09：(レベル1，2，3，及び4)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。**

**VE01.09.01：**ベンダが提供する文書は、セキュリティ要求事項の適用から除外される全てのコンポーネントが明確にリスト化されていなければならない。

**VE01.09.02：**VE01.09.01の要求事項に対応してリスト化されたそれぞれのコンポーネントの適用除外理由は、ベンダが提供する文書に記述されなければならない。ベンダは、たとえ誤動作又は誤使用であっても、それぞれのコンポーネントが、いかなる合理的な条件のもとでも危殆化を引き起こさないことを示さなければならない。

**TE01.09.01：**試験者は、ベンダが適用除外とする暗号モジュールのコンポーネントをリスト化しているかどうかを判定しなければならない。何もリスト化されていない場合には、全てのコンポーネントは、FIPS140-2の要求事項を満たさなければならない。

**TE01.09.02：**ベンダが、暗号モジュールのあるコンポーネントを FIPS140-2 の要求事項の適用除外として示している場合には、試験者はその適用除外に対する合理的な理由が規定されているかを判定しなければならない。その理由では、そのコンポーネントが誤作動しても、CSP、平文データ、又は誤使用により危殆化をもたらすその他の情報を公開する可能性がないことを示さなければならない。文書によって十分に確認される根拠として、次のものがある：

1. コンポーネントは、CSP、平文データ、又は誤使用により危殆化をもたらすその他の情報を処理しない。
2. コンポーネントは、CSP、平文データ、又は誤使用により危殆化をもたらすその他の情報の不適切な転送を許すモジュールのセキュリティに関連したコンポーネントと接続していない。
3. コンポーネントが処理する全ての情報は、完全に暗号モジュール内部での使用に限られており、決して暗号モジュールが接続されている装置に影響を与えない。

試験者は、ベンダによって提供された適用除外の根拠の正当性を判定しなければならない。証明の義務はベンダが負う；何らかの不確実性やあいまいさがある場合には、試験者は必要に応じてベンダに追加情報の作成を要求しなければならない。

**AS01.10：(レベル 1，2，3，及び 4)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、並びに暗号モジュールのすべての定義された入出力パスを規定しなければならない。**

注：このアサーションは、AS02.01の一部として試験される。

**AS01.11：(レベル 1，2，3，及び 4)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。**

注：このアサーションは、AS02.01の一部として試験される。

**AS01.12：(レベル1，2，3，及び4)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。**

**VE01.12.01：**ベンダは、全ての承認暗号アルゴリズムに対して、認証証明書を提供しなければならない。

[コメント]

日本での認定のしくみについての検討が必要。

**VE01.12.02：**ベンダは、承認されていないセキュリティ機能のリストを提供しなければならない。

**TE01.12.01：**試験者は、ベンダが上記に示した(1つ又は複数の)認証証明書を提供していることを検証しなければならない。

**TE01.12.02：**試験者は、ベンダが上記に示した承認されていないセキュリティ機能のリストを提供していることを検証しなければならない。

**AS01.13：(レベル1，2，3，及び4)文書は、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しなければならない。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。**

**VE01.13.01：**ベンダが提供する文書は、ハードウエアコンポーネント及びそれらの接続関係を示すブロック図を含まなければならない。ブロック図に含まれるべきコンポーネントは、該当するものとして、次のものがある：

1. マイクロプロセッサ
2. 入出力バッファ
3. 平文バッファ又は暗号文バッファ
4. 制御バッファ
5. 鍵格納メモリ
6. 作業メモリ
7. プログラムメモリ
8. 上記に記載されないその他のコンポーネント

**VE01.13.02:**ブロック図は、あらゆる(セミ)カスタム集積回路(例えば、ゲートアレイ、FPGA、又は他のプログラム可能なロジックデバイス)も含まなければならない。

**VE01.13.03:**ブロック図は、暗号モジュールの主要なコンポーネント間の接続関係、及び暗号モジュールと暗号境界の外部の装置間又はコンポーネントとの間の接続関係を示さなければならない。

**VE01.13.04:**ブロック図は、暗号モジュールの暗号境界を示さなければならない。

**TE01.13.01：**試験者は、ベンダが、暗号モジュールの中の主要なサブモジュールを示す 1 つ又はそれ以上のブロック図を提供していることを検証しなければならない。これらは、ベンダの設計に該当するものがあれば、少なくとも次のものを含まなければならない：

1. この節のアサーション AS01.08 に基づいたマスターコンポーネントリストに記載されたマイクロプロセッサ又はその他のプロセッサ
2. 平文/暗号文メッセージデータ又は制御情報以外の一般的な入出力データを格納又は処理する入出力バッファメモリ
3. 暗号化又は復号されるメッセージデータを格納又は処理する平文/暗号文バッファメモリ
4. 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制御情報及び状態情報を格納又は処理する制御バッファメモリ
5. 鍵格納メモリ
6. 情報を処理するための作業メモリ
7. 実行可能ソフトウエア又はファームウエアコードを含むプログラムメモリ
8. (セミ)カスタム集積回路(例えば、ASIC、ゲートアレイ、FPGA、PLA、又は他の PLD)

9. 上記に記載されないその他のコンポーネント

**TE01.13.02：**試験者は、ブロック図が、暗号モジュールの重要なコンポーネント間、及び暗号モジュールと外部装置間の全ての重要な接続関係やデータフローを示していることを検証しなければならない。特に、接続関係を示すブロック図のそれぞれの配線は、送信される情報のタイプを付記しなければならない。

**TE01.13.03：**試験者は、この節のAS01.08で要求されているように、ブロック図が暗号モジュールのための暗号境界を示していることを検証しなければならない。

**AS01.14：(レベル1，2，3，及び4)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の設計を規定しなければならない。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仕様言語を使用し、ハードウエアは回路図を使用しなければならない。**

**VE01.14.01：**ベンダは、暗号モジュールに含まれるハードウエア、ソフトウエア、ファームウエアのコンポーネントの詳細な設計仕様を提供しなければならない。この文書は、有限状態モデルとFIPS140-2の4.4節「セキュリティ要件」で言及されている記述を含まなければならない。有限状態モデルと設計仕様の関係が明らかでない場合には、ベンダはこの関係を記述した追加文書を提供しなければならない。

**TE01.14.01：**試験者は、有限状態モデルと設計仕様の関係が特定できることを検証するために、VE10.07.01で文書化されたハードウエア、ソフトウエア、及びファームウエアの全コンポーネントの名称リストと設計仕様とを比較しなければならない。

**AS01.15：(レベル1，2，3，及び4)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。**

**VE01.15.01：**ベンダは、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た文書を提供しなければならない。

**TE01.15.01：**試験者は、文書が、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ていることを検証しなければならない。

**AS01.16：(レベル1，2，3，及び4)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。**

**VE01.16.01：**ベンダは、別の公開用セキュリティポリシを提供しなければならない。セキュリティポリシはFIPS140-2のAppendix Cで定義される。

**TE01.16.01：**試験者は、ベンダによって提供された公開用セキュリティポリシをレビューしなければならない。試験者は、この公開用セキュリティポリシが FIPS140-2 の Appendix C で規定された要求事項を満たしていることを判定しなければならない。

# 2．暗号モジュールのポートとインタフェース

**AS02.01：(レベル1，2，3，及び4)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。**

**VE02.01.01：**ベンダが提供する文書は、次の項目を含む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それぞれ規定しなければならない。

1. 物理的ポート及びピンアサイン
2. 物理的なカバー、ドア又は開口部
3. 論理的インタフェース(例えば、API 及び全ての他のデータ/制御/状態信号との関係等)及び信号名及び機能
4. 適切な制御入力を物理的に行うための手動制御機器(例えば、ボタン又はスイッチ等)
5. 適切な状態出力を物理的に確認するための状態インジケータ(例えば、ライト又はディスプレイ)
6. 暗号モジュールの物理的ポート、手動制御機器、及び状態インジケータと論理的インタフェースとのマッピング
7. 上記のポート及びインタフェースのうち、該当するものの物理的特性、論理的特性、及び電気的特性

**VE02.01.02：**ベンダが提供する文書は、1節及び10節に記載されているブロック図、設計仕様、及び/又はソースコード、及び回路図において、強調したり、又は注釈をつけたりすることによって、暗号モジュールの情報の流れ及び物理的アクセスポイントを規定しなければならない。ベンダは、物理的ポート及び論理的インタフェースに対する情報の流れ並びに物理的アクセスポイントの関係を明確に規定するために必要なその他のいかなる文書も提供しなければならない。

**VE02.01.03：**ベンダが提供する文書は、暗号モジュールの物理的又は論理的な入出力ごとに、物理的な入出力が属する論理的インタフェース及び物理的な入出力ポートを規定しなければならない。ベンダが提供する文書に記載されている仕様は、1節及び10節に記載されている暗号モジュールコンポーネント仕様と、本節のアサーションAS02.03からAS02.09に記載されている論理的インタフェース仕様とで一致していなければならない。

**TE02.01.01：**試験者は、ベンダが提供する文書が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それぞれを規定していることを検証しなければならない。必須の仕様として、次の記述を含まなければならない：

1. 全ての物理的入出力ポートに関する記述。その記述には、暗号モジュール内におけるピンアサイン、物理的な配置、それぞれのポートを流れる論理信号の概要、及び 2 つ又はそれ以上の信号が同じ物理的なピンを共有している場合における信号の流れのタイミングシーケンスに関する記述を含めること。
2. 全ての物理的なカバー、ドア、又は開口部に関する記述。その記述には、暗号モジュール内におけるそれらの物理的な配置、及びそれぞれのカバー/ドア/開口部を介してアクセス及び/又は変更できるコンポーネント又は機能を含めること。
3. 全ての論理的入出力インタフェース(例えば、API 及び全ての他のデータ/制御/状態信号)に関する記述。その記述には、暗号モジュール内における全ての論理データ、及び制御入力、及びデータ、及び状態出力のリスト又はそれらの注釈を入れたブロック図、並びに、信号名及び機能のリスト並びにそれらの説明を含めること。
4. スイッチ又はボタンのように物理的な制御信号の入力に用いられる全ての手動制御手段に関する記述。その記述には、暗号モジュール内における物理的な配置、並びに手動で入力することが可能な制御信号のリスト及び説明を含めること。
5. 全ての物理的な状態インジケータに関する記述。その記述には、暗号モジュール内における物理的な配置、並びに物理的に出力される状態表示信号のリスト及び説明を含めること。
6. 論理的な入出力インタフェースと、暗号モジュールにおける物理的な入出力ポート、手動制御機器、及び物理的な状態インジケータとのマッピングに関する記述。
7. 物理的特性、論理的特性、及び電気的特性(上記の物理的ポート及びインタフェースの内、該当するもの)に関する記述。その記述には、ピン名称、それぞれのポートに入出力される論理的信号、電圧レベル及びその論理的意味(例えば、電圧の高低が論理的な”0”か”1”か、又は”その他の意味”のどれを意味するのか)、並びに信号のタイミングの概要を含めること。

**TE02.01.02：**試験者は、1 節及び 10 節に記載されているブロック図、設計仕様、及び/又はソースコード、及び回路図、及びベンダが提供するその他のすべての文書を調べることによって、ベンダが提供する文書が暗号モジュールにおける全ての情報の流れ及び物理的アクセスポイントを規定していることを検証しなければならない。文書は、暗号モジュールにおける物理的ポート及び論理的インタフェースに対する情報の流れ並びに物理的アクセスポイントの関係について規定しなければならない。試験者は、AS01.08、AS01.10、及び AS01.13 に基づく情報と上記の情報とを比較し、並びにコンポーネントの記述と入出力ポートの物理的なレイアウトの記述との間に矛盾が無いことを検証しなければならない。

**TE02.01.03：**試験者は、ベンダが提供する文書が、暗号モジュールの物理的又は論理的な入出力ごとに、物理的な入出力が属する論理的インタフェース及び物理的な入出力ポートを規定していることを検証しなければならない。ベンダが提供する文書に記載される仕様は、1節及び10節に記載されている暗号モジュールコンポーネントの仕様と、本節のAS02.03から AS02.09のアサーションに記載されている論理的インタフェースの仕様とで一致していなければならない。

TE02.01.04：試験者は、暗号モジュールを検査することによって、ベンダが提供する文書に記載されている上記の全ての仕様が、暗号モジュールの実際の設計と一致していることを検証しなければならない。

[コメント]

検証方法の具体化を含め、今後の検討が必要。

**AS02.02：(レベル1，2，3，及び4)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。**

**VE02.02.01：**ベンダの設計は、本節のAS02.03、及びAS02.09(該当する場合)に記載されたインタフェースのカテゴリに従い、暗号モジュールインタフェースを論理的に明確な及び分離されたカテゴリに分類しなければならない。この設計内容は、本節の AS02.01に記載されている論理的インタフェースと物理的ポートの仕様とで一致していなければならない。

**VE02.02.02：**ベンダが提供する文書は、論理的インタフェースのそれぞれのカテゴリと暗号モジュールの物理的ポートとのマッピングを記述しなければならない。論理的インタフェースは2つ以上の物理的ポートにわたって物理的に分散されていてもよい。また、2つ以上の論理的インタフェースは、情報の流れが論理的に分離されている限り、1つの物理的ポートを共有してもよい。2つ以上の論理的インタフェースが同一の物理的ポートを共有している場合には、ベンダが提供する文書は、異なるインタフェースのカテゴリからの情報がどのように論理的に分離されているかについて規定しなければならない。

**TE02.02.01：**試験者は、ベンダが提供する文書の内容及び暗号モジュールの検査によって、暗号モジュールインタフェースが、本節の AS02.03 、及び AS02.09(該当する場合)に記載されているインタフェースのカテゴリに対して、論理的に明確に分離していることを検証しなければならない。暗号モジュールインタフェースの仕様は、本節の AS02.01 に記載されている論理的インタフェース及び物理的ポートの仕様並びに設計と一致しなければならない。

**TE02.02.02：**試験者は、ベンダが提供する文書には、論理的インタフェースのそれぞれのカテゴリと暗号モジュールの物理的ポートとのマッピングが記載されていることを検証しなければならない。論理的インタフェースは 2 つ以上の物理的ポートにわたって分散されていてもよいし、又は、2 つ以上の論理的インタフェースが 1 つの物理的ポートを共有していてもよい。2 つ以上のインタフェースが同一の物理的ポートを共有している場合には、試験者は、ベンダが提供する文書が、入力、出力、制御、及び状態のインタフェースに対する情報の流れについてどのように論理的に分離しているのかを規定していることを検証し

なければならない。

**AS02.03：(レベル 1，2，3，及び 4)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**
**・データ出力インタフェース**
**・制御入力インタフェース**
**・状態出力インタフェース**

**VE02.03.01：**ベンダが提供する文書は、暗号モジュール内に設計されている次の 4 つの論理的インタフェースを規定しなければならない。(”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(AS02.04 に規定されているデータの入力用)
・データ出力インタフェース(AS02.05 に規定されているデータの出力用)
・制御入力インタフェース(AS02.07 に規定されている命令の入力用)
・状態出力インタフェース(AS02.08に規定される状態情報の出力用)

**TE02.03.01：**試験者は、ベンダが提供する文書が、VE02.03.01に挙げられた、暗号モジュール内に設計されている4つの論理的インタフェースを規定していることを検証しなければならない。規定されている場合には、暗号モジュール内の論理的インタフェースが、AS02.04、AS02.05、AS02.07、及びAS02.08のアサーションで規定された機能で実行することを検証しなければならない。

**AS02.04：(レベル1，2，3，及び4)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。**

**VE02.04.01：**暗号モジュールはデータ入力インタフェースを持たなければならない。
暗号モジュールに入力され及び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しなければならない。全てのデータには、次のものが含まれる。

1. 平文データ
2. 暗号文又は署名データ
3. 暗号鍵及び他の鍵管理データ(平文又は暗号化されたもの)
4. 認証データ(平文又は暗号化されたもの)
5. 外部ソースからの状態情報
6. 他の全ての入力データ

**VE02.04.02：**該当する場合には、ベンダが提供する文書は、スマートカード、トークン、キーパッド、キーローダ、及び/又はバイオメトリックスデバイスのような、データ入力インタフェースへのデータ入力のために暗号モジュールで使用される全ての外部入力デバイスを規定しなければならない。

**TE02.04.01：**試験者は、検査によって、暗号モジュールがデータ入力インタフェースを含み、かつデータ入力インタフェースが規定された通りに機能することを検証しなければならない。試験者は、次を含め、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から入力されることを検証しなければならない。

1. 暗号モジュールによって暗号化又は署名される平文データ
2. 暗号モジュールによって復号される暗号文データ又は検証される署名データ
3. 初期データ及び初期ベクトル、分散鍵情報、及び/又は鍵アカウント情報を含め(他の鍵管理要求事項は 7 節で記述されている)、暗号モジュールに入力され、及び使用される平文又は暗号化された暗号鍵及び他の鍵管理データ
4. パスワード、PIN、及び/又は生体情報を含め、暗号モジュールに入力される平文又は暗号化された認証データ
5. 外部ソース(例えば、他の暗号モジュール又はデバイス)からの状態情報
6. 別に AS02.07 に記述されている制御情報を除いた、処理又は保存のために暗号モジュールに入力される他の全ての情報

注：セキュリティレベル1、2においては、平文の暗号鍵、平文の認証データ、その他の平文のCSPの入力に用いられる物理的ポートは、暗号モジュールの他の物理的ポートと共有してもよい(セキュリティレベル3、4に対応する要求事項は、別に本節のAS02.16に記述されている。)。

**TE02.04.02：**試験者は、ベンダが提供する文書に、スマートカード、トークン、キーパッド、キーローダ、及び/又はバイオメトリクスデバイスのような、データ入力インタフェースへのデータ入力のために暗号モジュールで使用される全ての外部入力デバイスが規定されているかどうかを検証しなければならない。試験者は、識別された(1つ又は複数の)外部入力デバイスを用いて、データ入力インタフェースにデータを入力して、外部入力デバイスを用いたデータ入力が規定された通りに機能することを検証しなければならない。

**AS02.05：(レベル1，2，3，及び4)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。**

**VE02.05.01：**暗号モジュールは、データ出力インタフェースを持たなければならない。
暗号モジュールによって処理され及び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は除く)は、データ出力インタフェースを介して出力しなけ

ればならない。全てのデータには、次のものが含まれる。

1. 平文データ
2. 暗号文データ及びデジタル署名
3. 暗号鍵及び他の鍵管理データ(平文又は暗号化されたもの)
4. 外部対象に対する制御情報
5. 他の全ての出力データ

**VE02.05.02：**該当する場合には、ベンダが提供する文書は、スマートカード、トークン、ディスプレイ、及び/又は他の記憶デバイスのような、データ出力インタフェースからのデータ出力のために暗号モジュールで使用される全ての外部出力デバイスを規定しなければならない。

**TE02.05.01：**試験者は、検査によって、暗号モジュールがデータ出力インタフェースを含み、かつデータ出力インタフェースが規定された通りに機能することを検証しなければならない。試験者は、次を含め、暗号モジュールによって処理され、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を介して出力されることを検証しなければならない。

1. 暗号モジュールによって復号された平文データ
2. 暗号化された暗号文データ、及び暗号モジュールによって生成されたデジタル署名
3. 初期データ及び初期ベクトル、分散鍵情報、及び/又は鍵アカウント情報を含め(他の鍵管理要求事項は7節で記述されている)、内部で生成され、及び暗号モジュールから出力される平文又は暗号化された暗号鍵及び他の鍵管理データ
4. 外部の対象(例えば、他の暗号モジュール又はデバイス)に対して、暗号モジュールの外部へ送信される制御情報
5. 別にAS02.08に記述されている状態情報を除いた、処理又は保存後に暗号モジュールから出力される他の全ての情報

注：セキュリティレベル1、2においては、平文の暗号鍵及びその他の平文のCSPを出力するための物理的ポートは、暗号モジュールのその他の物理的ポートと共有してもよい。(セキュリティレベル3、4に対応する要求事項は、別に本節のAS02.16に記述されている。)

**TE02.05.02：**試験者は、ベンダが提供する文書に、スマートカード、トークン、ディスプレイ、及び/又は他の記憶デバイスのような、データ出力インタフェースからのデータ出力のために暗号モジュールで使用される全ての外部出力デバイスが規定されているかどうかを検証しなければならない。試験者は、識別された(1つ又は複数の)外部出力デバイスを用いて、データ出力インタフェースからデータを出力して、外部出力デバイスを用いたデータ出力が規定された通りに機能することを検証しなければならない。

**AS02.06：(レベル1，2，3，及び4)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。**

**VE02.06.01：**ベンダが提供する文書は、暗号モジュールがエラー状態(エラー状態は4節に記述されている。)にある時は常に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ていることを暗号モジュールの設計の中でどのように保証しているかについて規定しなければならない。CSP、平文データ、又は誤使用された場合に危殆化を引き起こす可能性のある他の情報が状態情報の中にない場合には、エラータイプを識別するために、状態出力インタフェースから出力される状態情報を用いてもよい。

**VE02.06.02：**ベンダが提供する文書は、暗号モジュールが自己テスト状態(自己テスト状態は9節に記述されている。)にある時は常に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ていることを暗号モジュールの設計の中でどのように保証しているかについて規定しなければならない。CSP、平文データ、又は誤使用された場合に危殆化を引き起こす可能性のある他の情報が状態情報の中にない場合には、自己テストの結果を表示するために、状態出力インタフェースから出力される状態情報を用いてもよい。

**TE02.06.01：**試験者は、ベンダが提供する文書が、暗号モジュールがエラー状態にある時は常にデータ出力インタフェースからの全てのデータ出力が禁止されていることを規定していることを検証しなければならない。試験者は、ベンダが提供する文書から、一旦エラー条件が検出され及びエラー状態になると、エラーが復旧するまでデータ出力インタフェースからの全てのデータ出力が禁止されることを検証しなければならない。CSP、平文データ、又は誤使用された場合に危殆化を引き起こす可能性のある他の情報が状態情報の中にない場合には、エラータイプを識別するために、状態出力インタフェースから出力される状態情報を用いてもよい。試験者は、本アサーションに対応して規定されたエラー状態が、AS04.05で規定されたエラー状態と一致していることも検証しなければならない。

[解説]

本TEは、「試験者は、ベンダが提供する文書が、暗号モジュールがエラー状態にある時は常にデータ出力インタフェースからの全てのデータ出力が禁止されていることを規定していることを検証しなければならない。試験者は、ベンダが提供する文書から、一旦エラー条件が検出され及びエラー状態になると、エラーが復旧するまでデータ出力インタフェースからの全てのデータ出力が禁止されることを検証しなければならない。状態出力インタフェースから出力される状態情報をエラータイプを識別するために用いている場合には、試験者は、ベンダが提供する文書によって、CSP、平文データ、又は誤使用された場合に危殆化を引き起こす可能性のある他の情報が状態情報の中にないことを検証しなければならない。試験者は、本アサーションに対応して規定されたエラー状態が、AS04.05で規定されたエラー状態と一致していることも検証しなければならない。」と解釈する。

**TE02.06.02：**試験者は、暗号モジュールの設計及び操作手順が許す範囲で、暗号モジュールに対してそれぞれ規定されたエラー状態を発生させ、及びデータ出力インタフェースからの全てのデータ出力が禁止されていることを検証しなければならない。エラータイプを識別するために、状態情報が状態出力インタフェースから出力される場合には、試験者は、

出力された情報が重要情報でないことを検証しなければならない。暗号モジュールに対しエラー状態を発生させるために、次の動作を行ってもよい。「タンパー検出付きのカバー又はドアを開ける。」、「不正な形式のコマンド、鍵、又はパラメータを入力する。」、「入力電圧を下げる。」、及び/又は「エラーを発生させるための他のあらゆる動作を行う。」

**TE02.06.03：**試験者は、ベンダが提供する文書が、暗号モジュールが自己テスト状態にある時は常に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ていることを規定していることを検証しなければならない。試験者は、ベンダが提供する文書から、一旦自己テストが実行されると完了するまで、データ出力インタフェースからの全てのデータ出力が禁止されていることを検証しなければならない。CSP、平文データ、又は誤使用された場合に危殆化を引き起こす可能性のある他の情報が状態情報の中にない場合には、自己テストの結果を表示するために、状態出力インタフェースから出力される状態情報を用いてもよい。試験者は、本アサーションに対応して規定された自己テスト状態とAS09.08に規定された自己テストとが一致していることも検証しなければならない。

[解説]

本TEは、「試験者は、ベンダが提供する文書が、暗号モジュールが自己テスト状態にある時は常に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ていることを規定していることを検証しなければならない。試験者は、ベンダが提供する文書から、一旦自己テストが実行されると完了するまで、データ出力インタフェースからの全てのデータ出力が禁止されていることを検証しなければならない。状態出力インタフェースから出力される状態情報を自己テストの結果を表示するために用いている場合には、試験者は、ベンダが提供する文書によって、CSP、平文データ、又は誤使用された場合に危殆化を引き起こす可能性のある他の情報が状態情報の中にないことを検証しなければならない。試験者は、本アサーションに対応して規定された自己テスト状態とAS09.08に規定された自己テストとが一致していることも検証しなければならない。」と解釈する。

**TE02.06.04：**試験者は、暗号モジュールの設計及び操作手順が許す範囲で、暗号モジュールに対し自己テストを実行するよう命令し、及びデータ出力インタフェースからの全てのデータ出力が禁止されていることを検証しなければならない。自己テストの結果を表示するために、状態情報が状態出力インタフェースから出力されている場合には、試験者は、CSP、平文データ、又は誤使用によって危殆化を引き起こす可能性のある他の情報が状態情報の中にないことを検証しなければならない。

**TE02.06.05：**試験者は、ベンダが提供する文書が、エラー状態又は自己テストの間、データ出力インタフェースからの全てのデータ出力を禁止している方法を規定していることを検証しなければならない。試験者は、暗号モジュールの設計を検査することによって、これらの状態において、データ出力インタフェースからのデータ出力が論理的又は物理的に禁止されていることも実際に検証しなければならない。

[解説]

「これらの状態」は、「エラー状態又は自己テスト状態」を指している。

**AS02.07：(レベル1，2，3，及び4)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、及び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。**

**VE02.07.01：**暗号モジュールは、制御入力インタフェースを持たなければならない。暗号モジュールの動作の制御に使用される全てのコマンド、信号、及び制御データ(データ入力インタフェースから入力されるデータを除く)は、制御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。全てのコマンド、信号、制御データには、次のものを含む。:

1. API から論理的に入力されるコマンド(例えば、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用)
2. 1 つ以上の物理的ポートから論理的又は物理的に入力される信号(例えば、暗号モジュールのハードウエアコンポーネント用)
3. 手動制御入力(例えば、スイッチ、ボタン、又はキーボード)
4. 他の全ての入力制御データ

**VE02.07.02：**該当する場合には、ベンダが提供する文書は、コマンド、信号、及び制御データを制御入力インタフェースを通して入力するためのスマートカード、トークン、又はキーバッドのような暗号モジュールで使用される全ての外部入力デバイスを規定しなければならない。

[解説]

本VEは、「該当する場合には、ベンダが提供する文書は、コマンド、信号、及び制御データを制御入力インタフェースを通して入力するために、スマートカード、トークン、又はキーバッドのような暗号モジュールで使用される外部入力デバイスを用いる場合、ベンダが提供する文書には、全ての外部入力デバイスが規定されていなければならない。」と解釈する。

**TE02.07.01：**試験者は、検査によって、暗号モジュールが制御入力インタフェースを含んでいること、及び制御入力インタフェースが規定されたように機能することを検証しなければならない。試験者は、次を含め、暗号モジュールの動作の制御に使用される全てのコマンド、信号、又は制御データ(データ入力インタフェースから入力されるデータを除く)が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ことを検証しなければならない。:

1. ソフトウエアライブラリ又はスマートカードに対する関数呼び出しのような、API から論理的に入力されるコマンド
2. シリアルポート又は PC カードを通して送信されるコマンド及び信号のような、1 つ以上の物理的ポートから論理的又は物理的に入力される信号
3. 手動制御入力(例えば、スイッチ、ボタン、又はキーボードの利用)
4. 他の全ての入力制御データ

**TE02.07.02：**試験者は、ベンダが提供する文書が、コマンド、信号、及び制御データを制御入力インタフェースを通して入力するためのスマートカード、トークン、又はキーパッドのような暗号モジュールで使用される全ての外部入力デバイスを規定しているかどうかを検証しなければならない。試験者は、その規定された(1つ又は複数の)外部入力デバイスを用いて、制御入力インタフェースからコマンドを入力して、外部入力デバイスを用いたコマンド入力が規定された通りに機能することを検証しなければならない。

**AS02.08：(レベル1，2，3，及び4)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、及び発光ダイオード並びに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。**

**VE02.08.01：**暗号モジュールは，状態出力インタフェースを持たなければならない。暗号モジュールの状態を表示するために用いられる全ての状態情報、信号、論理的なインジケータ、及び物理的なインジケータは、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。全ての状態情報、信号、論理的なインジケータ、及び物理的なインジケータは、次のものを含む。:

1. API から論理的に出力される状態情報
2. 1つ以上の物理的ポートから論理的又は物理的に出力される信号
3. 手動の状態出力(例えば、LED、ブザー、又はディスプレイの利用)
4. 他の全ての出力状態情報

**VE02.08.02：**該当する場合には、ベンダが提供する文書は、状態情報、信号、論理的なインジケータ、及び物理的なインジケータを状態出力インタフェースを通して出力するために、スマートカード、トークン、ディスプレイ、及び/又は他の記憶デバイスのような暗号モジュールで使用される全ての外部出力デバイスを規定しなければならない。

[解説]

本VEは、「該当する場合には、ベンダが提供する文書は、状態情報、信号、論理的なインジケータ、及び物理的なインジケータを状態出力インタフェースを通して出力するために、スマートカード、トークン、ディスプレイ、及び/又は他の記憶デバイスのような暗号モジュールで使用される外部出力デバイスを用いる場合、ベンダが提供する文書には、全ての外部出力デバイスが規定されていなければならない。」と解釈する。

**TE02.08.01：**試験者は、検査によって、暗号モジュールは状態出力インタフェースを含んでいること、及び状態出力インタフェースは規定された通りに機能することを検証しなければならない。試験者は、次を含め、暗号モジュールの状態を表示するために用いられる全ての状態情報、論理的なインジケータ、及び物理的なインジケータが、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ことを検証しなければならない。:

1. ソフトウエアライブラリ又はスマートカードからの戻り値のような、API から論理的に出力される状態情報
2. シリアルポート又は PC カードコネクタを通して送信される状態情報のような、1つ以上の物理的ポートから論理的又は物理的に出力される信号
3. 手動の状態出力(例えば、LED、ブザー、又はディスプレイの利用)
4. 他の全ての出力状態情報

**AS02.09：(レベル1，2，3，及び4)暗号モジュールに入力される全ての外電力(外部電源又はバッテリからの電力を含む)は、電源ポートから入力されなければならない。**

**VE02.09.01：**暗号モジュールが、暗号境界外にある他のデバイス(例えば、電源又は外部電池)との間で電力の授受を行っている場合には、ベンダが提供する文書は、電源インタフェース及び対応する物理的ポートを規定しなければならない。暗号モジュールと暗号境界外にある他のデバイスとの間の全ての電力授受は、規定された電源インタフェースを介さなければならない。

**TE02.09.01：**試験者は、ベンダが提供する文書が、暗号モジュールと暗号境界外にある他のデバイス(例えば、電源、電源コード、電源の入出力口、又は外部バッテリ)との間で電力の授受があるかどうかを規定しているかどうかを検証しなければならない。試験者は、ベンダが提供する文書が、電源インタフェース及び対応する物理的ポートを規定していることも検証しなければならない。

**TE02.09.02：**試験者は、暗号モジュールの検査によって、暗号モジュールと暗号境界外にある他のデバイスとの間で授受される全ての電力が、規定された電源インタフェースを介していることを検証しなければならない。全ての電力が暗号モジュール内部で供給又は維持されている場合には、電源インタフェースはなくてもよいことに注意すること。また、内部バッテリの交換は物理的なメンテナンス活動としてみなされ、5節のアサーションで規定されている要求事項の対象となることに注意すること。

**AS02.10：(レベル1，2，3，及び4)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。**

**VE02.10.01：**ベンダが提供する文書は、暗号モジュールが「入力のデータ及び制御」と「出力のデータ及び状態」とをどのように分離しているかを規定しなければならない。また、ベンダが提供する文書は、該当する入力インタフェースから暗号モジュールへ入力される入力データ及び制御情報が流れる物理的・論理的パスと、該当する出力インタフェースを介してモジュールから出力される出力データ及び状態情報が流れる物理的・論理的パスとが、どのように論理的又は物理的に分離されているかを規定しなければならない。

**TE02.10.01：**試験者は、ベンダが提供する文書が、暗号モジュールが「入力のデータ及び

制御」と「出力のデータ及び状態」とをどのように分離しているかを規定していることを検証しなければならない。また、試験者は、ベンダが提供する文書が、データ入力インタフェースから入力される入力データ及び制御入力インタフェースから入力される制御情報と、出力データインタフェースから出力される出力データ及び状態出力インタフェースから出力される状態情報とが、論理的又は物理的に区別されていることを規定していることを検証しなければならない。

**TE02.10.02：**試験者は、ベンダが提供する文書が、入力データ及び制御情報によって使用される物理的・論理的パスと、出力データ及び状態情報によって使用される物理的・論理的パスとが、論理的又は物理的にどのように分離しているかを規定していることを検証しなければならない。入力データ及び制御情報、出力データ及び状態情報によって使用される物理的・論理的パスが物理的に共有されている場合には、試験者は、ベンダが提供する文書が、論理的な分離が暗号モジュール内でどのように行われているかを規定していることを検証しなければならない。

**TE02.10.03：**試験者は、検査によって、ベンダが提供する文書の一貫性を検証しなければならない。また、試験者は、暗号モジュールが「入力のデータ及び制御」と「出力のデータ及び状態」とを区別していることを検証しなければならない。また、試験者は、該当する入力インタフェースから暗号モジュールへ入力される入力データ及び制御情報が流れる物理的・論理的パスと、該当する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出力データ及び状態情報が流れる物理的・論理的パスとが、論理的又は物理的に分離されていることを検証しなければならない。

**AS02.11：(レベル1，2，3，及び4)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。**

**VE02.11.01：**ベンダが提供する文書は、データ入力インタフェース及び該当する物理的ポートから暗号モジュールへ入力される入力データの全ての主要なカテゴリによって使用される物理的・論理的パスを規定しなければならない。ベンダが提供する文書は、該当するパスの仕様(例えば、AS01.08、AS01.09、及びAS01.13に基づいて提供される回路図、ブロック図、又は他の情報に、強調又は注釈をつけた写し)が含まれていなければならない。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、暗号モジュールの物理的又は論理的サブセクションのそれぞれによって、そのデータが処理又は保存されている間は、規定されたパスのみを使用しなければならない。

**TE02.11.01：**試験者は、ベンダが提供する文書が、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入力データの全ての主要なカテゴリによって使用される物理的・論理的パスを規定していることを検証しなければならない。試験者は、パスが仕様(例えば、AS01.08、AS01.09、及びAS01.13に基づいて提供される回路図、ブロック図、又は他の情報に、強調又は注釈をつけた写し)の中に文書化されていることも検証しなければならない。

入力データパスは、どのデータタイプが該当する物理的ポートを通るのかを試験者によって判定できるほど十分詳細に規定されなければならない。

[解説]

本TEは、「試験者は、ベンダが提供する文書が、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入力データの全ての主要なカテゴリによって使用される物理的・論理的パスを規定していることを検証しなければならない。試験者は、パスが仕様(例えば、AS01.08、AS01.09、及びAS01.13に基づいて提供される回路図、ブロック図、又は他の情報に、強調又は注釈をつけた写し)の中に文書化されていることも検証しなければならない。試験者は、ベンダが提供する文書に、どのデータタイプが該当する物理的ポートを通るのかを判定できるほど十分詳細に入力データパスが規定されていることを検証しなければならない。」と解釈する。

**TE02.11.02：**試験者は、ベンダが提供する文書及び暗号モジュールの検査から、データ入力インタフェース及び該当する物理的ポートから暗号モジュールへ入力される全ての入力データが、規定されたパスのみを使用していることを検証しなければならない。試験者は、全ての論理的又は物理的情報の流れを調べて、入力データによって使用されるパスの仕様が暗号モジュールの設計及び動作と一致していることを検証しなければならない。試験者は、CSP、平文データ、又は他の情報の危殆化を引き起こす可能性のあるパス間で衝突がないことを検証しなければならない。

**AS02.12：(レベル1，2，3，及び4)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。**

**VE02.12.01：**ベンダが提供する文書は、データ出力インタフェース及び該当する物理的ポートを介して暗号モジュールから出力される出力データの主要なカテゴリ全てによって使用される物理的・論理的パスが規定されなければならない。ベンダが提供する文書は、該当するパスの仕様を含まなければならない(例えば、AS01.08、AS01.09、及びAS01.13に基づいて提供される回路図、ブロック図、又は他の情報に、強調又は注釈をつけた写し)。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、規定されたパスのみを使用しなければならない。

**TE02.12.01：**試験者は、ベンダが提供する文書が、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出力データの主要なカテゴリ全てによって使用される物理的・論理的パスが規定されていることを検証しなければならない。試験者は、それらパスが仕様の中に文書化されていること(例えば、AS01.08、AS01.09、及びAS01.13に基づいて提供される回路図、ブロック図、又は他の情報に、強調又は注釈をつけた写し)も確認しなければならない。出力データパスは、どのタイプのデータがそれぞれ該当する物理的ポートを通るのか、試験者が判定できるほど十分詳細に、規定されなければならない。

**TE02.12.02：**試験者は、ベンダが提供する文書及び暗号モジュールの検査から、データ出

力インタフェース及び該当する物理的ポート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が、規定されたパスのみを使用していることを検証しなければならない。試験者は、全ての論理的又は物理的情報の流れを調べて、出力データによって使用されるパスの仕様が暗号モジュールの設計及び動作と一致していることを検証しなければならない。試験者は、CSP、平文データ、又は他の情報の危殆化を引き起こす可能性のある、該当するパス間の衝突が存在しないことを検証しなければならない。

**AS02.13：(レベル1，2，3，及び4)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。**

**VE02.13.01：**ベンダが提供する文書は、暗号モジュールから出力される出力データの主要なカテゴリ全てによって使用される物理的・論理的パスが、鍵生成、手動鍵入力、並びに暗号鍵及び CSP のゼロ化を実行する処理から、論理的又は物理的にどのように分離されるかを規定しなければならない。暗号モジュールは、上記に規定された鍵処理が、鍵及び/又はその他の CSP の情報を出力データパスに渡すことを認めてはならない。また、暗号モジュールは、暗号モジュールから出力される出力データが、その鍵処理を妨げることを認めてはならない。

**TE02.13.01：**試験者は、ベンダが提供する文書が、暗号モジュールから出力される出力データの主要なカテゴリ全てによって使用される物理的・論理的パスが、鍵生成、手動鍵入力、並びに暗号鍵及びその他のCSPのゼロ化を実行する処理から、どのように論理的又は物理的に分離されるかについて規定していることを検証しなければならない。

**TE02.13.02:**出力データと鍵及び/又はその他のCSP情報とが流れる物理的･論理的パスが、物理的に共有されている場合には、試験者は、ベンダが提供する文書が、どのように暗号モジュールが出力データと鍵及び/又はその他のCSP情報との論理的な分離を実現しているかについて規定していることを検証しなければならない。

**TE02.13.03：**試験者は、出力データインタフェース及び該当する物理的ポートを記録又は監視すること、並びに鍵及びその他のCSP情報が漏洩されていないことを検証することによって、出力データパスが、鍵生成、手動鍵入力、並びに暗号鍵及びその他のCSPのゼロ化を実行する処理から、論理的又は物理的に分離されていることを検証しなければならない。

**AS02.14：(レベル1，2，3，及び4)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エ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つのハードウエ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。**

[解説]

例えば、

・ソフトウエアでは、データ出力コマンドが入力されると確認画面が表示され(1回目の独立した内部動作)、次にユーザがパスワードを入力しOKとなると(2回目の独立した内部動作)、初めて出力される。

・ハードウエアでは、以下のようなゲート回路を構成し、データ出力の際に、ユーザがA、Bのスイッチを両方ONすることで、初めて出力が許可される。

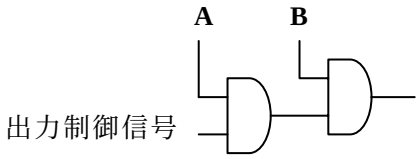



図　ハードウエアゲートの構成例

**VE02.14.01：**暗号モジュールの設計上、平文の暗号鍵コンポーネント又はその他の保護されていないCSPが1つ以上の物理的ポートに出力されることを認めている場合には、平文の暗号鍵コンポーネント又はその他の保護されていないCSPが出力される前に、2つの独立した内部動作が暗号モジュールによって実行されなければならない。ベンダが提供する文書は、実行される2つの独立した内部動作を規定して、2つの独立した内部動作が、平文の暗号鍵コンポーネント又はその他の保護されていないCSPを誤って漏洩してしまうことに対して、どのように保護しているかについて規定しなければならない。

**TE02.14.01：**試験者は、暗号モジュールが、1つ以上の物理的ポートに平文の暗号鍵コンポーネント又はその他の保護されていないCSPが出力されることを認めているかどうかを判定しなければならない。試験者は、ベンダが提供する文書が、平文の暗号鍵コンポーネント又はその他の保護されていないCSPが出力される前に暗号モジュールによって実行される、2つの独立した内部動作について規定していることを検証しなければならない。試験者はまた、ベンダが提供する文書が、平文の暗号鍵コンポーネント又はその他の保護されていないCSPを誤って漏洩することに対して、どのように2つの独立した内部動作が保護するかについて規定していることを検証しなければならない。

**TE02.14.02：**試験者は、暗号鍵コンポーネント又はその他の保護されていないCSPを1つ以上の物理的ポートに出力させて、2つの独立した内部動作が規定された通りに機能することを検証しなければならない。何らか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が、平文の暗号鍵コンポーネント又はその他の保護されていないCSPを出力している処理中に実行される場合には、試験者は、そ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が、平文の暗号鍵コンポーネント又はその他の保護されていないCSPを出力する前の2つの独立した内部動作に関する要求事項を満たしていることを確実にするために、該当するソースコードを調べなければならない。

[解説]

本TEは、「試験者は、暗号鍵コンポーネント又はその他の保護されていないCSPを1つ

以上の物理的ポートに出力させて、2つの独立した内部動作が規定された通りに機能することを検証しなければならない。何らか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が、平文の暗号鍵コンポーネント又はその他の保護されていないCSPを出力している処理中に実行される場合には、試験者は、該当するソースコードを検査して、全ての平文の暗号鍵コンポーネント又はその他の保護されていないCSPが出力される前に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が2つの独立した内部動作を要求することを確かにサポートしていることを確認しなければならない。」と解釈する。

**AS02.15：(レベル1，2，3，及び4)ベンダが提供する文書は、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しなければならない。**
**注：このアサーションは、個別に試験されない。ベンダが提供する文書の検証は、AS02.01～AS02.14、及びAS02.16～AS02.18に基づいて行われる。**

[解説]

本内容は、FIPS140-2のAppendix Aに記載されている。

**AS02.16：(レベル3及び4)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るか、又はAS02.17が満足される必要がある。**

**VE02.16.01：**ベンダが提供する文書は、暗号モジュールが、平文の暗号鍵コンポーネント、平文の認証データ、又はその他の保護されていないCSPを入力又は出力するかどうかを規定しなければならない。平文の暗号鍵コンポーネント、平文の認証データ、又はその他の保護されていないCSPの入出力に使用される(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物理的ポートから物理的に分離されていなければならない。

**TE02.16.01：**試験者は、ベンダが提供する文書が、平文の暗号鍵コンポーネント、平文の認証データ、又はその他の保護されていないCSPを、暗号モジュールが入力又は出力するかどうかについて規定しているかどうかを検証しなければならない。試験者は、ベンダが提供する文書から及び暗号モジュールの物理的ポートの検査によって、平文の暗号鍵コンポーネント、平文の認証データ、又はその他の保護されていないCSPの入出力に使用される該当する物理的ポートが、暗号モジュールの他の全ての物理的ポートから物理的に分離されていることを検証しなければならない。

**TE02.16.02：**暗号モジュールが平文の暗号鍵コンポーネント、平文の認証データ、又はその他の保護されていないCSPを入出力する場合には、試験者は、平文の暗号鍵、平文の認証データ、又はその他の保護されていないCSPのみが、該当する物理的ポートを介して入出力されることを検証しなければならない。また試験者は、平文であるか暗号化されたものかに関わらず、他のデータが、該当する物理的ポートを介して暗号モジュールに入出力されることがないことも検証しなければならない。

**AS02.17：(レベル3及び4)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るか、又はAS02.16が満足される必要がある。**

**VE02.17.01：**ベンダが提供する文書は、暗号モジュールが、平文の暗号鍵コンポーネント、平文の認証データ、又はその他の保護されていないCSPを入出力するかどうかを規定しなければならない。平文の暗号鍵コンポーネント、平文の認証データ、又は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。

**TE02.17.01：**試験者は、ベンダが提供する文書が、暗号モジュールが、平文の暗号鍵コンポーネント、平文の認証データ、又はその他の保護されていないCSPを入力又は出力するかどうかについて規定していることを検証しなければならない。試験者は、ベンダが提供する文書から及び暗号モジュールの検査によっても、平文の暗号鍵コンポーネント、平文の認証データ、又はその他の保護されていないCSPの入出力に使用される該当する論理的ポートが、高信頼パスを使用する暗号モジュールの他の全ての論理的なインタフェースから分離されていることを検証しなければならない。

**TE02.17.02：**暗号モジュールが、平文の暗号鍵コンポーネント、平文の認証データ、又はその他の保護されていないCSPを入出力する場合には、試験者は、平文の暗号鍵、平文の認証データ、又はその他の保護されていないCSPのみが、高信頼パスを使用する該当する論理的インタフェースを介して暗号モジュールに入出力することを検証しなければならない。また試験者は、平文であるか暗号化されたものかに関わらず、他のデータが、高信頼パスを使用する該当する論理的インタフェースを介して暗号モジュールに入出力することがないことも検証しなければならない。

**AS02.18：(レベル3及び4)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)。**

**VE02.18.01：**ベンダが提供する文書は、暗号モジュールが、平文の暗号鍵コンポーネント、平文の認証データ、又はその他の保護されていないCSPを入力するかどうかを規定しなければならない。これらのパラメータの入力に使用される物理的ポートは、暗号境界外に介在するシステム、プロセッサ、回路、他の領域を通ることなく、暗号モジュールの暗号境界に直接接続されなければならない(例えば、高信頼パスを介する、又は直接接続されたケーブルを介する)。

**TE02.18.01：**試験者は、ベンダが提供する文書が、暗号モジュールが平文の暗号鍵コンポーネント、平文の認証データ、又はその他の保護されていない CSP を入力するかどうかに

ついて規定していることを検証しなければならない。試験者は、ベンダが提供する文書から並びに物理的ポート及び暗号境界を検査することによっても、これらのパラメータの入力に使用される物理的ポートが、暗号境界外に介在するシステム、プロセッサ、回路、他の領域を通ることなく、暗号モジュールの暗号境界に直接接続されている(例えば、高信頼パスを介する、又は直接接続されたケーブルを介する)ことを検証しなければならない。

# 3．役割、サービス、及び認証

**AS03.01：(レベル1，2，3，及び4)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。**
注：このアサーションは、個別には試験されない。

**AS03.02：(レベル1，2，3，及び4)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。**

**VE03.02.01：**ベンダが提供する文書は、複数オペレータが同時に暗号モジュールを利用することを許可するかどうかを規定しなければならない。ベンダは、許可された役割及び実行されるサービスをオペレータごとに区分けする方法を記述しなければならない。ベンダが提供する文書は、同時に利用する複数のオペレータに対するいかなる制限についても記述しなければならない(例えば、メンテナンスの役割のあるオペレータ及びユーザの役割のあるオペレータは同時には許可されない)。

**TE03.02.01：**試験者は、ベンダが提供する文書をレビューして、その暗号モジュールが複数オペレータに実行される役割とサービスを区分けする方法が記述されていることを検証しなければならない。

**TE03.02.02：**試験者は、2つの独立したオペレータのIDに就かなければならない：オペレータ1とオペレータ2。これらのオペレータは、異なる役割を担わなければならない。試験者は、それぞれの役割に割り当てられたサービスだけが、その役割で実行できることを検証しなければならない。試験者は、また、同時の複数オペレータが許可されている場合において役割とサービスの区分けが行われていることを検証するために、それぞれのオペレータとして、他のオペレータだけが担っている役割に対応したサービスにアクセスを試みなければならない。

**TE03.02.03：**ベンダが提供する文書が、複数オペレータに対する何らかの制限について規定している場合には、試験者は、複数の独立したオペレータとして制限された役割を同時に担うことを試みることによって、その制限に違反することを試みて、第二のオペレータが役割を担うことを防ぐ制限を暗号モジュールが実施していることを検証しなければならない。

[解説]

本TEは、「ベンダの文書が複数オペレータに対する何らかの制限について規定している場合には、試験者は、独立した第二のオペレータとしてその制限された役割を担うことを試み、第二のオペレータがその役割を担うことができないことを検証しなけれ

ばならない。」と解釈する。

## 3.1 役割

**AS03.03：(レベル 1，2，3，及び 4)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)。**

**VE03.03.01：**VE03.06.01を満たすために要求される文書の中で、ベンダは少なくとも1つのユーザ役割及び少なくとも1つのクリプトオフィサ役割を含めなければならない。

**TE03.03.01：**試験者は、ベンダが提供する文書をレビューして、少なくとも1つのユーザ役割と少なくとも1つのクリプトオフィサ役割が定義されていることを検証しなければならない。これらの役割は、名称及び許可されたサービスによって規定されなければならない。これらの役割は、AS03.03で規定されているように記述されなければならない(役割を担うことに関しては、TE03.06.02によって試験される)。

**AS03.04：(レベル 1，2，3，及び 4)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)。**

**VE03.04.01：**暗号モジュールがメンテナンスインタフェースを持つ場合には、ベンダが提供する文書は、メンテナンス役割がサポートされていることを明確に記述しなければならない。文書は、名称及び許可されたサービスによって、その役割を完全に規定しなければならない。

**TE03.04.01：**試験者は、メンテナンスインタフェースが規定されているかどうかを判定するために、暗号モジュールインタフェースの規定をレビューしなければならない(AS05.07参照)。そうである場合には、試験者は、許可された役割に関係するベンダが提供する文書をチェックして、メンテナンス役割が、名称、目的、及び許可されたサービスによって規定されていることを検証しなければならない(役割を担うことに関しては、TE03.06.02で試験

される)。

**AS03.05：(レベル1，2，3，及び4)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。**

**VE03.05.01：**ベンダが提供する文書は、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、FIPS PUB 140-2の2.1節で定義される暗号モジュール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が、どのようにして積極的にゼロ化されるかを規定しなければならない。

[解説]

「積極的に」は、「暗号モジュールが能動的に動作することによって」と解釈する。

**TE03.05.01：**ベンダが提供する文書が、暗号モジュールの中でメンテナンス役割が実装されることを記載している場合には、試験者は、ベンダが提供する文書が、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、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をゼロ化する方法を規定していることを検証しなければならない。

**TE03.05.02：**試験者は、メンテナンス役割でない間に、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にゼロでない値をロードしなければならない。試験者は、メンテナンス役割を担うときに、ゼロ化が行われることを検証しなければならない。

[解説]

「ゼロ化が行われる」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がゼロ化される。」と解釈する。

**TE03.05.03：**試験者は、メンテナンス役割の間に、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にゼロでない値をロードしなければならない。試験者は、メンテナンス役割から出るときに、ゼロ化が行われることを検証しなければならない。

[解説]

「ゼロ化が行われる」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がゼロ化される。」と解釈する。

**AS03.06：(レベル1，2，3，及び4)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。**

**VE03.06.01：**ベンダが提供する文書は、役割の名称及びその役割で実行されるサービスを含め、それぞれ識別可能な許可された役割を規定しなければならない。

[解説]

本VEは、「ベンダが提供する文書は、それぞれ識別可能な許可された役割を規定しなければならない。規定には、役割の名称及びその役割で実行されるサービスを含めなければならない」と解釈する。

**TE03.06.01：**試験者は、ベンダが提供する文書をレビューして、定義されたそれぞれの役割に対して、名称及びこの役割で利用可能なサービスが規定されていることを検証しなければならない。記述すべき役割は、次の通り：

1. クリプトオフィサ役割(1つ以上)
2. ユーザ役割(必須)(1つ以上)
3. メンテナンス役割(暗号モジュールがメンテナンスインタフェースを含む場合のみ)
4. その他の役割

**TE03.06.02：**試験者は、ベンダが提供する文書に記述されているそれぞれの許可された役割を担うことを試みて、実際にそれぞれの役割を担うことがきることを検証しなければならない。それぞれの役割で指定されたサービスの検証は、AS03.14に基づいて実行される。

## 3.2 サービス

**AS03.07：(レベル1，2，3，及び4)サービスは、暗号モジュールが実行できるサービス、動作は機能の全てを言及しなければならない。**

注：このアサーションは、個別には試験されない。

**AS03.08：(レベル1，2，3，及び4)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。**

注：このアサーションは、個別には試験されない。

[解説]

本ASは、「サービス入力は、規定されたサービス、操作、機能を開始又は獲得する全てのデータ、又は暗号モジュールへの制御入力から構成されなければならない。」と解釈する。

**AS03.09：(レベル1，2，3，及び4)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。**

注：このアサーションは、個別には試験されない。

**AS03.10：(レベル1，2，3，及び4)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。**
注：このアサーションは、個別には試験されない。

**AS03.11：(レベル1，2，3，及び4)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。**

**VE03.11.01：**ベンダが提供する文書は、VE03.14.01及びVE03.15.01によって規定される他のサービスと共に、暗号モジュールの現在状態の出力、及びユーザが呼び出せる自己テストの開始及び実行について記述しなければならない。

**TE03.11.01：**試験者は、“状態の表示”サービス、及びユーザが呼び出せる自己テストの開始サービスが、それぞれ少なくとも1つの許可された役割に割り当てられていることを検証するために、ベンダが提供する文書をチェックしなければならない。試験者は、これらのサービスがAS03.14で規定されているように記述されていることを検証しなければならない。

**TE03.11.02：**試験者は、“状態の表示”インジケータが、ベンダが提供する文書の記述と一致していることを検証しなければならない。

**TE03.11.03：**暗号モジュールが、4.9節で規定されているパワーアップ自己テストの実行開始を行うことの検証は、TE03.14.02のもとで実施される。

**AS03.12：(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、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)。**

[解説]
バイパス能力：暗号処理を行なわずに暗号モジュール内に平文を通過させるようなサービスを提供すること。

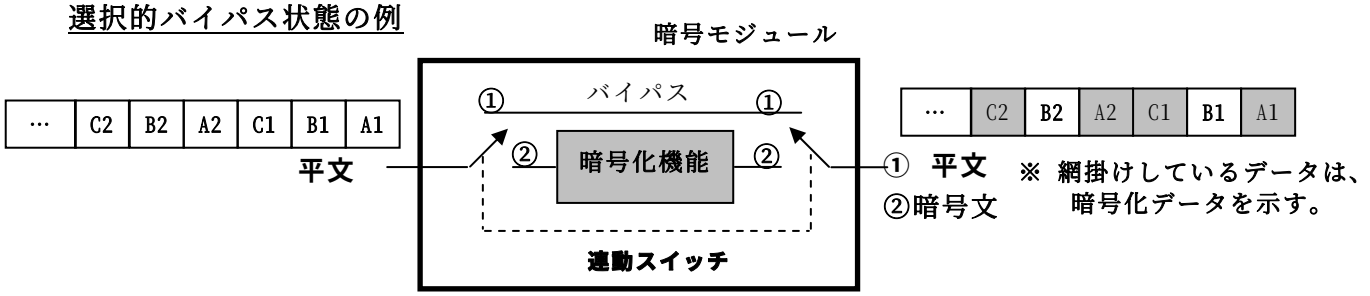
**VE03.12.01：**暗号モジュールがバイパス能力を実装している場合には、ベンダが提供する文書は、AS03.12で規定されているようにバイパスのサービスを記述しなければならない。

**VE03.12.02：**有限状態モデル及びその他に関するベンダが提供する文書は、排他的、又は交互に遷移するバイパス状態への全ての遷移について、2つの独立した内部動作がそれぞれのバイパス状態へ遷移するために必要とされることを示さなければならない。

[解説]

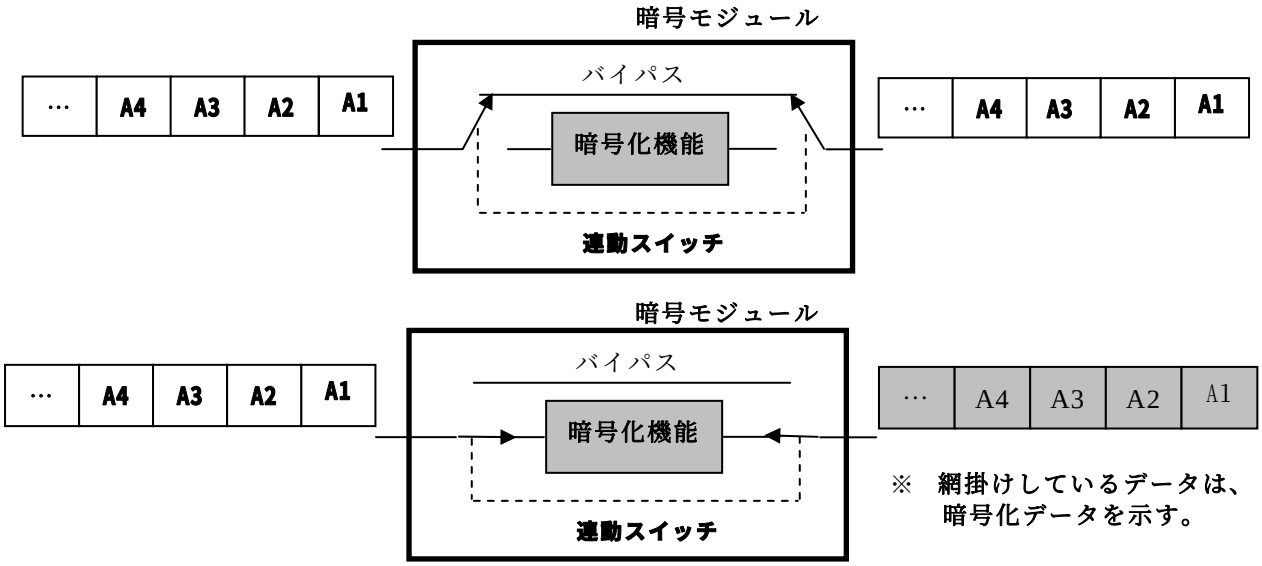
本VEは、「有限状態モデルに関する文書及びその他ベンダが提供する文書には、排他的なバイパス状態の全ての遷移について、又は選択的バイパス状態の全ての遷移について、それぞれのバイパス状態へ遷移するために必要とされる2つの独立した内部動作が示されなければならない。」と解釈する。

**選択的バイパス状態の例**




スイッチが時分割で①②の経路を切り替え、多重チャネルのデータを選択的にバイパスする。
上図は、入力された平文データの中で、チャネルBのデータのみバイパスしている例を示す。

**排他的バイパス状態の例**




スイッチは、固定的に切り替わる。従って、全ての入力データがバイパスされるか、又は全ての入力データが暗号化されて出力される。

**TE03.12.01：**試験者は、バイパス能力が暗号モジュールに実装されているかどうかを判定しなければならない。試験者は、バイパス能力が少なくとも1つの許可された役割に割り当てられることを検証するために、ベンダが提供する文書をチェックしなければならない。

**TE03.12.02：**試験者は、排他的又は交互に遷移するバイパス状態へのそれぞれの遷移が、暗号モジュールに対して排他的、又は交互に遷移するバイパス状態のどちらか一方へ遷移するために起こらなければならない2つの独立した内部動作を示しているかどうかを判断するために、状態遷移モデル及びその他に関するベンダが提供する文書をレビューしなければならない。

**TE03.12.03：**試験者は、そのような遷移を示すそれぞれの状態からそれぞれのバイパス状態まで遷移することを試みて、そのようなそれぞれの遷移を実行するために2つの内部動作が行なわれることを判定しなければならない。

**AS03.13：(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、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、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、平文が暗号化される)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。**

**VE03.13.01：**“状態の表示”サービスについてのベンダが提供する文書は、バイパス状態を示していなければならない。

[解説]

本VEは、「“状態の表示”サービスが記述されているベンダが提供する文書には、バイパス状態が記述されていなければならない。」と解釈する。

**TE03.13.01：**試験者は、“状態の表示”サービスについてのベンダが提供する文書についてレビューして、バイパスサービスの表示を検証しなければならない。

[解説]

本VEは、「試験者は、“状態の表示”サービスについてのベンダが提供する文書についてレビューして、バイパスサービスの表示について記述されていることを検証しなければならない。」と解釈する。

**TE03.13.02：**試験者は、それぞれのバイパス状態の遷移を行って、“状態の表示”が適切

なバイパス状態を表示することを検証しなければならない。

**AS03.14：(レベル 1，2，3，及び 4)文書は、次の項目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**

**VE03.14.01：**ベンダが提供する文書は、目的と機能を含むそれぞれのサービスについて説明しなければならない。

**VE03.14.02：**ベンダが提供する文書は、それぞれのサービスに対して、サービス入力、それに対応するサービス出力、及び許可された役割又はサービスが実行できる役割を規定しなければならない。サービス入力は、規定されたサービス、操作、若しくは機能を開始又は獲得するための暗号モジュールへの全てのデータ入力、又は制御入力で構成しなければならない。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、操作、若しく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しなければならない。

**TE03.14.01：**試験者は、ベンダが提供する文書をチェックして、それぞれのサービスの目的と機能が記述されていることを検証しなければならない。試験者は、次の情報がそれぞれのサービスに規定されていることもチェックしなければならない。：
サービス入力、対応するサービス出力、及び許可された役割又はそのサービスを実行できる役割。

**TE03.14.02：**試験者は、それぞれの役割について次の項目を実行しなければならない：

1. サービスがその役割のために実装されているかを検証するために、その役割のために規定されたそれぞれのサービスを実行する。
2. 規定されたそれぞれのサービス入力を入力して、規定されたサービス出力を観察する。
3. 役割に対して規定されていないサービスが実装されていないことを検証するために、役割に対して規定されていないサービスの実行を試みる。

**AS03.15：(レベル1，2，3，及び4)文書は、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について規定して、それらのサービスが、どのようにして、暗号鍵及びその他のCSPを変更、開示若しくは置換することがないか、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かを規定しなければならない。**

[解説]

「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」は、例えば、認証前のパスワードを最初に受け付けるサービス、役割を決定する前の入

力受付等がある。

**VE03.15.01：**ベンダが提供する文書は、目的及び機能を含め、それぞれのサービスを記述しなければならない。

**VE03.15.02：**ベンダが提供する文書は、それぞれのサービスに対して、サービス入力及びそれに対応するサービス出力を規定しなければならない。サービス入力は、規定されたサービス、操作、若しくは機能を開始又は獲得するための暗号モジュールの全てのデータ入力、又は制御入力で構成しなければならない。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、操作、若しく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しなければならない。

**TE03.15.01：**試験者は、ベンダが提供する文書をチェックして、それぞれのサービスの目的及び機能が記述され、並びにサービスの入力及びそれに対応するサービスの出力が記述されていることを検証しなければならない。

**TE03.15.02：**試験者は、次の試験を実行しなければならない：

1. 規定されたそれぞれのサービス入力を入力して、規定されたサービス出力が結果として得られることの観察。
2. 役割が必要なサービスが実行されないことを検証するために、役割が必要なサービスを実行することを試みる。

## 3.3 オペレータ認証

**AS03.16：(レベル 2，3，及び 4)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。**

**-役割ベース認証**

**-IDベース認証**

注：このアサーションは、個別には試験されない。

**役割ベースの認証**

**AS03.17:(レベル 2)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。**

**VE03.17.01:** ベンダは、暗号モジュールによって行われる認証方法について文書化しなければならない。ベンダは、役割又は役割の集合を暗黙的又は明示的に選択するメカニズム、及び (一つ若しくは複数の)役割を担うオペレータの認証方法を文書化しなければならない。

**TE 03.17.01:** 試験者は、ベンダが提供する文書が、一つ又はそれ以上の役割を選択するメカニズム、及び役割を担うオペレータの認証方法を規定していることを検証しなければならない。

**TE03.17.02:**試験者は、それぞれの役割を担って、認証手順の途中にエラーを発生させなければならない。試験者は、暗号モジュールがそれぞれの役割へのアクセスを拒否することを観察しなければならない。

**AS03.18:(レベル 2)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。**

**VE03.18.01:** ベンダが提供する文書は、オペレータが役割を変更するために必要な権限を記述して、オペレータが新しい役割を担うための検証が必要であることを明示しなければならない。

**TE03.18.01:**試験者は、オペレータが役割を変更するための方法が、新しい役割を担うオペレータの検証を含んでいるかを検証するために、ベンダが提供する文書をチェックしなければならない。

**TE03.18.02:**試験者は、次の試験を行わなければならない：

1. それぞれの役割を担い、オペレータが担うことが許可された他の役割への変更を試みて、暗号モジュールが新しい役割に割り当てられたサービスの要求をオペレータに対し許可することを検証する。
2. それぞれの役割を担い、オペレータが担うことが許可されない他の役割への変更を試みて、暗号モジュールが新しい役割だけに割り当てられたサービスの要求をオペレータに対し許可しないことを検証する。

### IDベースの認証

**AS03.19:(レベル 3及び4)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て、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。**

**VE03.19.01:** ベンダは、暗号モジュール内部に実装されている認証のタイプについて文書化しなければならない。ベンダは、オペレータの識別、オペレータのIDの認証、暗黙的若しくは明示的な役割又は役割の集合の選択、及び(一つ若しくは複数の)役割を担うオペレータの検証に用いられる(一つ若しくは複数の)メカニズムを文書化しなければならない。

**TE03.19.01:**試験者は、ベンダが提供する文書が、どのようにしてオペレータがユニークに識別されるか、どのようにしてオペレータのIDが認証されるか、どのようにしてオペレータが役割を選択するか、及び役割を担うためのオペレータの許可が認証されたIDに基づいてどのように実行されるかについて規定していることを検証しなければならない。

**TE03.19.02:**試験者は、認証手順の途中にエラーを発生させて、試験者が認証手順より先に処理が進むことについて暗号モジュールが許可しないことを観察しなければならない。

**TE03.19.03:**試験者は、暗号モジュールに対して、自分のIDの認証に成功しなければならない。一つ又はそれ以上の役割の選択が要求された場合、試験者は、認証されたIDとは両立しない役割を選択して、役割を担う許可が拒否されることを観察しなければならない。

**AS03.20:(レベル 3及び4)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。**

[解説]

本ASは、「オペレータが役割を変更する場合には、暗号モジュールは、変更する役割を担うことができるか否かを検証しなければならない。」と解釈する。

**VE03.20.01:** ベンダが提供する文書は、役割を変更するためのオペレータの権限について記述して、新しい役割に対するオペレータの認証の検証が要求されることを明示しなければならない。

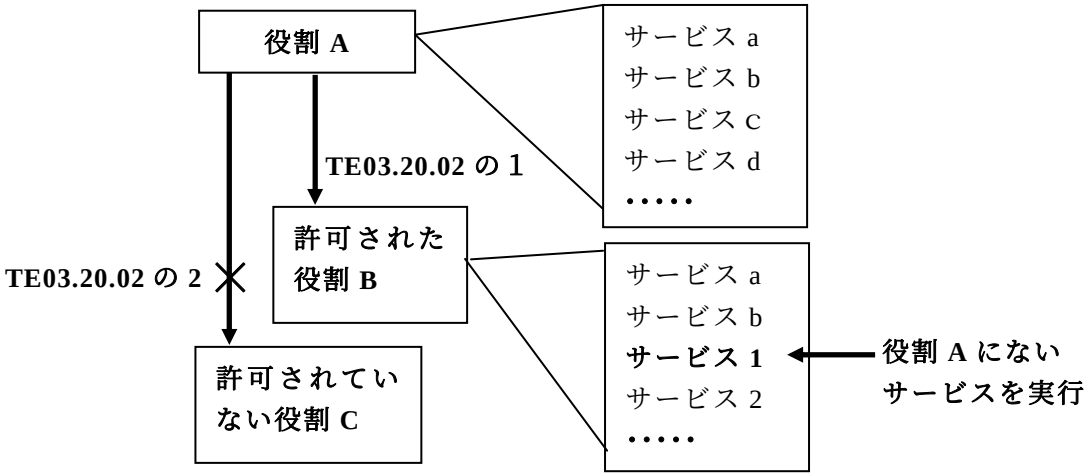
**TE03.20.01:**試験者は、ベンダの提供する文書が、オペレータのIDの再認証を行わずに役割を変更できる方法は、以前に認証されていない役割に対するオペレータの許可の検証を含んでいることを検証するために、レビューしなければならない。

**TE03.20.02：**試験者は、次の試験を行わなければならない。

1. それぞれの役割を担い、試験者が許可された他の役割への変更を試み、試験者 ID が再度の認証を必要としないことを検証して、試験者が新しい役割に関連したサービスにアクセスできることを検証しなければならない。試験者は、試験者が異なる役割を担っていることを検証するために、変更前の役割に関連していなかった新しい役割でのサービスを行わなければならない。

2.それぞれの役割を担い、試験者が許可されていない他の役割への変更を試みて、暗号モジュールがオペレータIDに基づいた役割へのアクセスを拒否することを検証しなければならない。

[解説]




**AS03.21:(レベル 1,2,3,及び4)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。**

**VE03.21.01:** ベンダが提供する文書は、暗号モジュールが電源OFFされる時に、以前の認証の結果がどのように消去されるかについて記述しなければならない。

**TE03.21.01:**試験者はベンダが提供する文書をレビューして、暗号モジュールの電源OFFによる以前の認証の消去が記述されていることを検証しなければならない。

**TE03.21.02:**試験者は、暗号モジュールに自分自身を認証させて、1つ又はそれ以上の役割を担い、暗号モジュールを電源OFFし、暗号モジュールを電源ONして、これらの役割におけるサービスを実行することを試みなければならない。暗号モジュールは、これらのサービスへのアクセスを拒否して、試験者が再認証されることを要求しなければならない。

**AS03.22:(レベル 2,3,及び4)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。**

**VE03.22.01:** ベンダが提供する文書は、暗号モジュールに対する全ての認証データの保護について記述しなければならない。その保護は、不正な開示、変更、及び置換に対して保護するメカニズムの実装方法を含まなければならない。

**TE03.22.01:**試験者は、認証データの保護について記述しているベンダが提供する文書をレ

ビューしなければならない。試験者は、ベンダが提供する文書が、不正な開示、変更、及び置換に対して、どのようにデータが保護されているかについて記述していることを検証しなければならない。

**TE03.22.02:**試験者は、次の試験を行わなければならない。

1.試験者は、試験者がアクセス権を持つことを許可されていない認証データに(文書化された保護メカニズムを回避することによって)アクセスすることを試みなさい。暗号モジュールがアクセスを拒否するか、又は、暗号モジュールが暗号化されたデータ又は他の保護されたタイプのデータのみのアクセスを認める場合には、その要求事項は満たされる。

2.試験者は、ベンダが提供する文書によって規定されていない何らかの方法を用いて、認証データを変更して、変更されたデータの入力を試みなさい。暗号モジュールは、試験者が変更されたデータを用いて認証されることを認めてはならない。

**AS03.23:(レベル 1,2,3,及び4)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、手続きによる制御若しくは工場設定値、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。**

[解説]

本ASの内容については、例えば、ICカード発行時のような状況の想定が考えられる。その際の認証メカニズムの初期化とは、オペレータの認証データのICカードへの書き込み等が考えられる。

**VE03.23.01:** ベンダが提供する文書は、初期化される前の暗号モジュールへのアクセスを制御する方法を規定しなければならない。

**TE03.23.01:**試験者は、ベンダが提供する文書が、最初に暗号モジュールにアクセスする時にオペレータが認証される手続きについて記述していることを検証しなければならない。

**TE03.23.02：**初期化前の暗号モジュールへのアクセスが制御される場合には、試験者は、初期化されていない暗号モジュールにエラーを起こさせて、暗号モジュールがアクセスを拒否することを検証しなければならない。試験者は、許可された役割を担い、要求された認証が文書化された手続に従っていることを検証しなければならない。試験者は、暗号モジュールが初期化される前に、他の役割を担うことを試みて、暗号モジュールがこれらの役割へのアクセスを拒否することを検証しなければならない。

[解説]

「エラーを起こさせ」とは、AS03.23に記述されている「他の認証方法でのアクセス」の試み等が考えられる。

**AS03.24:(レベル 2,3,及び4)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。**
注：このアサーションは、個別には試験されない。
[解説]
「次の仕様」は、AS03.25 ～ AS03.28を指す。

**AS03.25:(レベル 2,3,及び4)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、パスワード又は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。**

**VE03.25.01：**ベンダが提供する文書は、それぞれの認証方法、及びその関連の誤受入率又はランダムなアクセスが成功する確率を規定しなければならない。

**TE03.25.01:**試験者は、ベンダが提供する文書をレビューして、認証方法ごとに、その関連の誤受入率又はランダムアクセスが成功する確率が1,000,000分の1未満であることを検証しなければならない。
[解説]
本TEの内容は、文書のレビューによって検証することを求めている。

**AS03.26:(レベル 2,3,及び4)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。**

**VE03.26.01：**ベンダが提供する文書は、それぞれの認証方法及び1分間のランダム試行におけるその関連の成功の確率を規定しなければならない。

**TE03.26.01：**試験者はベンダが提供する文書をレビューして、認証方法ごとに、1分間のランダム試行におけるその関連の成功の確率が100,000分の1未満であることを検証しなければならない。

**AS03.27:(レベル 2,3,及び4)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)。**

**VE03.27.01：**ベンダが提供する文書は、認証データの入力の間、オペレータへの認証データのフィードバックを曖昧化するために使用される方法を規定しなければならない。

**TE03.27.01:**試験者は、ベンダが提供する文書をレビューして、データ入力の間、認証データが曖昧化されていることを検証しなければならない。

**TE03.27.02:**試験者は、認証データを入力して、データ入力の間、認証データの表示が見えないことを検証しなければならない。

**AS03.28:(レベル 2,3,及び4)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。**

**VE03.28.01:** ベンダが提供する文書は、オペレータが認証データを入力している時に使用されるフィードバックメカニズムを規定しなければならない。

**TE03.28.01:**試験者は、ベンダが提供する文書をレビューして、フィードバックメカニズムが、認証データを推定又は決定するために用いることのできる情報を提供していないことを検証しなければならない。

**TE03.28.02:**試験者は、フィードバックメカニズムが有益な情報を提供していないことを確実にするために、それぞれの役割を担うための認証データを入力しなければならない。

**AS03.29:(レベル 1,2,3,及び 4)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**

注：このアサーションは、個別には試験されない。

**AS03.30:(レベル 1)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。**

[解説]

レベル１は、認証メカニズムはなくてもよいと理解できる。例えば、メンテナンス時に認証を省略することも考えられる。

**VE03.30.01:** ベンダは、暗号モジュールに対して行われる認証のタイプを文書化しなければならない。ベンダは、1つの役割又は役割の集合を暗黙的又は明示的に選択するために使用されるメカニズム及びその(1つ又は複数の)役割を担うオペレータの認証を文書化しなければならない。

**VE03.30.02:**ベンダが提供する公開用セキュリティポリシは、オペレータが担うことができる暗黙的又は明示的な役割の記述を提供しなければならない。

**VE03.30.03:**ベンダが提供する公開用セキュリティポリシは、オペレータが暗黙的又は明示的な役割を担うための方法を提供しなければならない。

**TE03.30.01:**試験者は、ベンダが提供した公開用セキュリティポリシが、オペレータが担うことができる暗黙的又は明示的な役割及びそれぞれの役割を担うための方法を提供することを検証しなければならない。

**TE03.30.02:**試験者は、ベンダが提供した公開用セキュリティポリシに記述された方法を用いて、それぞれの役割が暗黙的又は明示的に担われることを検証しなければならない。

**AS03.31:(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。**
注：このアサーションは、AS03.17の一部として試験される。

**AS03.32:(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。**
注：このアサーションは、AS03.19の一部として試験される。

# 4．有限状態モデル

**AS04.01:(レベル 1,2,3,及び 4)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、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を含む)。**
注：このアサーションは、AS04.05の一部として試験される。

**AS04.02：(レベル 1,2,3,及び 4)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。**

注：このアサーションは、AS04.05の一部として試験される。

**AS04.03：(レベル 1,2,3,及び 4) 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。**

**TE04.03.01:**試験者は、暗号モジュールが、メンテナンス、サービス、又は修理を必要としないそれぞれのエラー状態から、適切な動作状態又は初期化状態へ遷移することができることを検証しなければならない。この試みは次の 2 つの項目から構成される。第一に、試験者は、暗号モジュールがエラー状態にあるとき、それを表示することを検証しなければならない。また、第二に、試験者は、暗号モジュールがこの対象の状態において正しく動作することを検証しなければならない。試験者は、この要求事項がどのように検証された

か(例えば、コード試験によって、又は暗号モジュールの実行によって)について報告しなければならない。

**AS04.04：(レベル 1,2,3,及び 4)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。**
注：このアサーションは、AS04.05の一部として試験される。

**AS04.05：(レベル 1,2,3,及び 4) 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。**

**VE04.05.01:**ベンダは、有限状態モデルの説明を提供しなければならない。この説明は、暗号モジュールの全ての状態の識別及び説明、並びに対応する状態遷移の全てを含まなければならない。状態遷移の説明は、暗号モジュールの内部状態、ある状態から別の状態への遷移を引き起こすデータ入力及び制御入力、ある状態から別の状態への遷移の結果起こるデータ出力及び状態出力を含まなければならない。

**TE04.05.01:**試験者は、ベンダが有限状態モデルの説明を提供したことを検証しなければならない。この説明は、暗号モジュールの全ての状態の識別及び説明、並びに対応する状態遷移の全ての説明を含まなければならない。試験者は、状態遷移の説明が、暗号モジュールの内部状態、ある状態から別の状態への遷移を引き起こすデータ入力及び制御入力、ある状態から別の状態への遷移の結果起こるデータ出力及び状態出力を含むことを検証しなければならない。

**TE04.05.02:**試験者は、有限状態図及びその説明が、次を記述しているベンダが提供する文書と一致していることを検証しなければならない。

1. データ入力インタフェース
2. データ出力インタフェース
3. 制御入力インタフェース
4. 状態出力インタフェース
5. クリプトオフィサ役割
6. ユーザ役割
7. 他の役割(該当する場合)
8. 鍵入力サービス(該当する場合)

9. 状態表示サービス
10. 自己テスト
11. 許可されたサービス、操作、機能(該当する場合)
12. エラー状態
13. バイパスサービス(該当する場合)
14. メンテナンスインタフェース(該当する場合)
15. メンテナンス役割(メンテナンスインタフェースが提供される場合)
16. 鍵生成サービス(該当する場合)
17. 鍵出力サービス(該当する場合)
18. アイドル状態(該当する場合)
19. 初期化されていない状態(該当する場合)

**TE04.05.03:**試験者は、(1つ又は複数の)有限状態図の中で識別された状態が、さらに、その説明の中でも識別及び記述されていることを検証しなければならない。

[解説]

「その説明」とは、VE04.05.01に基づいてベンダが提供し、TE04.05.01に基づいて試験者が検証した「有限状態モデルの説明」を指す。TE04.05.04、TE04.05.05、TE04.05.06においても同じである。

**TE04.05.04:**試験者は、その説明の中で識別及び記述されている全ての状態が、さらに、(1つ又は複数の)有限状態図においても識別されていることを検証しなければならない。

**TE04.05.05:**試験者は、暗号モジュールの動作が有限状態図及びその説明と一致していることを検証しなければならない。

**TE04.05.06:**暗号モジュールがメンテナンスインタフェースを含む場合には、試験者は、有限状態モデルが少なくとも1つのメンテナンス状態の定義を有していることを検証しなければならない。全てのメンテナンス状態は(1つ又は複数の)有限状態図に含まれなければならず、また有限状態モデルの説明に記述されなければならない。

**TE04.05.07:**試験者は、その説明が交わりのない状態を明確に定義するかどうかを決定するために、暗号モジュールの状態の説明をレビューしなければならない。試験者は、データ入力及び制御入力の可能な組合せの全てを交わりのないセットに分割できることを検証しなければならない。

**TE04.05.08:**試験者は、暗号モジュールが主要な状態のそれぞれになるように、暗号モジュールを操作しなければならない。試験者は、明確なインジケータを有するそれぞれの状態に対して、暗号モジュールがその状態にある間、インジケータを観察することを試みなければならない。期待されるインジケータが観察されない場合か、又は、2つ若しくはそれ以上のインジケータが同時に観察される場合には(暗号モジュールが同時に2つ以上の状態に

あることを示す)、この試験は不合格である。

[解説]

「主要な状態」には次の状態があり、主要な状態の他には、“メンテナンス状態”及び“バイパス状態”がある(DTRには記載がないが、FIPS140-2には記載あり)。

(1) 電源ON/OFF状態(Power on/off states)
(2) クリプトオフィサ状態(Crypto officer states)
(3) 鍵/CSP入力状態(Key/CSP entry states)
(4) ユーザ状態(User states)
(5) 自己テスト状態(Self-test states)
(6) エラー状態(Error states)

**TE04.05.09:**試験者は、初期電源ON状態から、有限状態モデルの初期電源ON状態ではない他のそれぞれの状態への遷移の連鎖が存在することを検証しなければならない。

[解説]

本TEは、「試験者は、初期電源ON状態から、直接又は他の状態を経由して、初期電源ON状態ではない全ての状態に遷移できることを確認しなければならない。」と解釈する。

**TE04.05.10:**試験者は、電源OFF状態ではないそれぞれの状態から、有限状態モデルの電源OFF状態への遷移の連鎖が存在することを検証しなければならない。

[解説]

本TEは、「試験者は、電源OFF状態ではない全ての状態から、直接又は他の状態を経由して、電源OFF状態に遷移できることを確認しなければならない。」と解釈する。

**TE04.05.11:**試験者は、データ入力及び制御入力の可能な組合せの全ての結果によって生じる有限状態モデルの動作が、定義されていることを検証しなければならない。包括的な記述で受け入れられるものの例は、次の通りである。

「データ入力及び制御入力の組合せ以外の全ての結果によって生じる有限状態モデルの動作は、有限状態モデルをエラー3状態にする。」

# 5．物理的セキュリティ

**AS05.01：(レベル1,2,3,及び4)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。**
注：このアサーションは、個別には試験されない。

**AS05.02：(レベル1,2,3,及び4)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。**
注：このアサーションは、個別に試験されない。

## 5.1 共通の物理的セキュリティ要求事項

**AS05.03：(レベル 1,2,3,及び 4)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。**
注：このアサーションは、個別には試験されない。
[解説]
「次の要求事項」は、AS05.04～AS05.10を指す。

**AS05.04：(レベル 1,2,3,及び 4)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。**

**VE05.04.01:**ベンダが提供する文書は、暗号モジュールの物理的な形態(FIPS PUB140-2の4.5節(VE01.08.05も参照)において定義される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、又はマルチチップスタンドアロン型暗号モジュール)を規定しなければならない。規定された物理的な形態は、暗号モジュールの物理的設計に整合していなければならない。ベンダが提供する文書は、さらに暗号モジュールがどのセキュリティレベル(1から4)を満たそうとしているのかを宣言しなければならない。

**TE05.04.01:**試験者は、ベンダが、暗号モジュールが FIPS PUB140-2 の 4.5 節(VE01.08.09も参照)において定義される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、又はマルチチップスタンドアロン型暗号モジュールのいずれかであることを識別していることについて検証しなければならない。試験者は、物理的な形態が、次に規定された 3 つ又はマルチチップスタンドアロン型暗号モジュールのいずれかであることを識別の基準のうちの 1 つを満足することを独立に判定しなければならない。3 つの物理的な形態

の基本的な決定的特徴、及びいくつかの典型例は次のようにまとめられる。

1. シングルチップ暗号モジュール

特徴:スタンドアロンデバイスとして使用されるシングル集積回路(IC)チップ、又は、物理的に保護されていない可能性のある他の暗号モジュール若しくは囲い内に物理的に組込まれているシングル集積回路(IC)チップ。シングルチップは、プラスチック又はセラミックのような均一な外部素材に覆われている単一ダイ、及び外部入出力コネクタから構成される。

例：シングル IC チップ、シングル IC チップを持つスマートカード、又は暗号機能を実装するためにシングル IC チップが用いられているその他のシステム。

2. マルチチップ組込型暗号モジュール

特徴：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可能性のある他の製品又は囲い内に物理的に組込まれている。

3. マルチチップスタンドアロン型暗号モジュール

特徴：2 つ又はそれ以上の IC チップが相互接続されて、物理的に完全に保護されている囲い内に物理的に組込まれている。

**TE05.04.02：**試験者は、ベンダが提供する文書が、暗号モジュールがどのセキュリティレベルを満たそうと宣言しているかを検証しなければならない。試験者は、暗号モジュールが実際に満たしているセキュリティレベルを独立に判定しなければならない。

**AS05.05：(レベル1,2,3,及び4)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。**

**VE05.05.01：**ベンダが提供する文書は、暗号モジュールによって用いられている適切な物理的セキュリティメカニズムを記述しなければならない。全てのハードウエア、ファームウエア、ソフトウエア、及びデータ(平文の暗号鍵、及びその他の保護されていないCSPを含む)を含む暗号モジュールの内容は、保護されなければならない。

**TE05.05.01：**試験者は、ベンダが提供する文書が暗号モジュールによって用いられている適切な物理的セキュリティメカニズムを記述していることを検証しなければならない。

**AS05.06：(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が定義されなければならない。**

**VE05.06.01：**ベンダが提供する文書は、暗号モジュールによって用いられるメンテナンスアクセスインタフェースを記述しなければならない。

**TE05.06.01：**試験者は、ベンダが提供する文書が、メンテナンスアクセスインタフェース

を記述していることを検証しなければならない。

**TE05.06.02：**試験者は、ベンダが提供している文書に記載されている内容及び実装が整合していることを検証しなければならない。

**AS05.07：(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。**

**VE05.07.01：**ベンダが提供する文書は、メンテナンスアクセスインタフェース、及び除去可能なカバー又はドアが提供されていることを規定しなければならない。

**TE05.07.01：**試験者は、メンテナンスアクセスインタフェース、及び除去可能なカバー又はドアが提供されていることを検証するために、ベンダが提供する文書をレビューしなければならない。

**AS05.08：(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内に含まれるあらゆる除去可能なカバー若しくはドアは、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。**
注：このアサーションは、AS05.07の一部として試験される。

**AS05.09：(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。**

**VE05.09.01：**ベンダが提供する文書は、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、暗号モジュールの平文の鍵、及び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。

**TE05.09.01：**ベンダが提供する文書が、メンテナンスアクセスインタフェースが提供されていると宣言している場合には、試験者は、ベンダが提供する文書が、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、暗号モジュール内に含まれる平文の鍵、及び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ていることについて

検証しなければならない。

**TE05.09.02：**暗号モジュール設計及び操作手順が許容する場合には、試験者は、ユニットの電源が入っている間、メンテナンスアクセスインタフェースにアクセスして、全ての操作鍵がゼロ化されることを検証しなければならない。メモリへの電力供給を無くして、徐々に電荷を放電させていく方法では十分ではない。

**AS05.10：(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、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。**

**VE05.10.01：**ベンダが提供する文書は、暗号モジュールへの許可されたメンテナンス動作が行われる手順を定義しなければならない。

**TE05.10.01：**ベンダが提供する文書が、メンテナンスアクセスインタフェースが提供されていると宣言している場合には、試験者は、ベンダが提供する文書が暗号モジュールへの許可されたメンテナンス動作を規定していることを検証しなければならない。

**AS05.11：(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。**

注：このアサーションは、個別には試験されない。

[解説]

「次の要求事項」は、AS05.12～AS05.14を指す。

**AS05.12：(レベル1,2,3,及び4)暗号モジュールは、標準的な皮膜保護技術(例えば、環境若しく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。**

**VE05.12.01：**暗号モジュールは、電力、温度、信頼性、衝撃、及び振動等において商用グレードの仕様を満たすように設計された標準品、製品品質のICでなければならない。暗号モジュールは、チップ全体に対して標準的な保護技術を使わなければならない。ベンダが提供する文書は、ICの品質について記述しなければならない。標準デバイスでないICが使われる場合には、その保護設計についても記述されなければならない。

**TE05.12.01：**試験者は、検査によって又はベンダが提供する文書から、暗号モジュールが、均一な外側素材及び標準的なコネクタからなる標準的な集積回路を含んでいることを検証

しなければならない。試験者は、ベンダが提供する文書から、暗号モジュール内のチップが、電力及び電圧の範囲、温度、信頼性、並びに衝撃及び振動に対して、商用グレードであることを検証しなければならない。

[解説]

「均一な外側素材」とは、例えば、一般的なICで使われているモールド樹脂のようなもの、又は外傷保護素材のようなものである。

**TE05.12.02：**試験者は、ベンダが提供する文書から、暗号モジュールに標準的な保護が施されていることを検証しなければならない。その保護は、環境又はその他の物理的損害から暗号モジュールを保護するために、チップの回路全体に施されるシーリングコートでなければならない。標準的な保護が使われない場合には、ベンダが提供する文書は、それがなぜ標準的な保護方法と同等であるかを示すための情報を提供しなければならない。

**AS05.13：(レベル 1,2,3,及び 4)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。**

注：このアサーションは、AS05.09の一部として試験される。

**AS05.14：(レベル 1,2,3,及び 4)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。**

注：このアサーションは、個別には試験されない。

**AS05.15：(レベル 2,3,及び 4)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。**

注：このアサーションは、個別には試験されない。

[解説]

「次の要求事項」は、AS05.16を指す。

**AS05.16：(レベル 2,3,及び 4)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。**

注：このアサーションは、シングルチップ形態についてはAS05.25の一部として、及びマルチチップ組込型形態についてはAS05.36及びAS05.37の一部として、及びマルチチップスタンドアロン型形態についてはAS05.50の一部として試験される。

**AS05.17：(レベル 3 及び 4)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。**

注：このアサーションは、個別には試験されない。

[解説]

「次の要求事項」は、AS05.18～AS05.21を指す。

**AS05.18：(レベル 3 及び 4)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。**
注：このアサーションは、シングルチップ形態についてはAS05.29の一部として、マルチチップ組込型形態及びマルチチップスタンドアロン型形態についてはAS05.53の一部として試験される。

**AS05.19：(レベル 3 及び 4)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。**
注：このアサーションは、シングルチップ形態についてはAS05.29の一部として、マルチチップ組込型形態についてはAS05.39の一部として、及びマルチチップスタンドアロン型形態についてはAS05.53の一部として試験される。

**AS05.20:(レベル3及び4)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。**
注：このアサーションは、シングルチップ形態についてはAS05.29の一部として、マルチチップ組込型形態についてはAS05.39の一部として、及びマルチチップスタンドアロン型形態についてはAS05.53の一部として試験される。

**AS05.21：(レベル3及び4)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)。**

**VE05.21.01：**暗号モジュールが、あらゆる通気孔又はスリットを含むカバー若しくは囲い内に入っている場合には、通気孔又はスリットは、囲い内部に対して、検出されない物理的なプロービングを防ぐような構造でなければならない。ベンダが提供する文書は、通気の物理的な設計方法を記述しなければならない。

**TE05.21.01：**試験者は、検査によって、及びベンダが提供する文書から、暗号モジュールが通気孔、スリット又は他の開口のあるカバー若しくは囲いを有しているかどうかを検証して、そうである場合には、それらがカバー又は囲い内部に対して検出されないプロービングを防ぐような構造であるかどうかを検証しなければならない。

**AS05.22：(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。**

注：このアサーションは、個別には試験されない。
[解説]
「次の要求事項」は、AS05.23を指す。

**AS05.23：(レベル 4)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。**
注：このアサーションは、AS05.60－AS05.69 の一部として試験される。

## 5.2 シングルチップ暗号モジュール

注：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。

**AS05.24：(シングルチップ－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、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。**
注：このアサーションは、個別には試験されない。
[解説]
「次の要求事項」は、AS05.25、05.26を指す。

**AS05.25：(シングルチップ－レベル 2,3,及び 4)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。**
注：この要求事項は、AS05.16 と関連している。

**VE05.25.01：**ベンダが提供する文書は、タンパー証跡を残すコーティング及びその特性を識別しなければならない。

**TE05.25.01：**試験者は、検査によって及びベンダが提供する文書から、暗号モジュールが、タンパー証跡を残すコーティングで覆われていることを検証しなければならない。検査は、タンパー証跡を残すコーティングが暗号モジュールを完全に覆っていること、及びシングルチップの直接観察、プロービング、又は不正操作を防ぐことを検証しなければならない。

**AS05.26：(シングルチップ－レベル 2,3,及び 4)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。**

**VE05.26.01：**ベンダが提供する文書は、材料が可視光領域内において不透明でなければな

らないことを規定しなければならない。
[解説]
「材料」は、「タンパー証跡を残すためのコーティング又は囲いの材料」と解釈する。

**TE05.26.01：**試験者は、検査によって及びベンダが提供する文書から、シングルチップ暗号モジュールが、可視光領域内において不透明なコーティングで覆われていることを検証しなければならない。

**AS05.27：(シングルチップ－レベル 3 及び 4) 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。**
注：このアサーションは、個別には試験されない。
[解説]
「次の要求事項」は、AS05.28、AS05.29を指す。

**AS05.28：(シングルチップ－レベル 3 及び 4)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、AS05.29 が満足されなければならない。**

**VE05.28.01：**ベンダが提供する文書は、AS05.28 で規定されている 2 つの方法のうちどちらが要求事項を満たすために使われているかを宣言して、サポートしている詳細な設計情報を提供しなければならない。
オプション 1：試験者は TE05.28.01 の手順に従わなければならない。
オプション2：試験者はTE05.29.01で規定された手順に従わなければならない。

**TE05.28.01：**試験者は、検査によって及びベンダが提供する文書から、暗号モジュールが堅く不透明なタンパー証跡を残すコーティングで覆われていることを検証しなければならない。ベンダが提供する文書は、使用されているコーティングの種類及びその特性について規定しなければならない。

**TE05.28.02：**試験者は、コーティングが容易に回路層の深さまで貫かれることがなく、かつコーティングがタンパー証跡を残すことを検証しなければならない。検査は、コーティングが完全に暗号モジュールを覆い、明らかに不透明であること、及びコーティングが直接的な観察、プロービング、又は不正操作を防ぐことを検証しなければならない(この検証の一部は、TE05.25.01 の中のセキュリティレベル 2 ですでに行われているかもしれない)。

**AS05.29：(シングルチップ－レベル 3 及び 4)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、又は AS05.28 が満足されなければならない。**
注：これらの要求事項は、AS05.18、AS05.19、AS05.20と関連している。

**VE05.29.01：**暗号モジュールが囲い内に含まれている場合には、ベンダが提供する文書は、囲いに関する設計情報を提供しなければならない。囲いは、囲いの除去の試みが高い確率で暗号モジュール内の回路に重大な損害を与えるように設計されていなければならない。

**VE05.29.02：**囲いがあらゆる除去可能なカバー若しくはドアを含むか、又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。回路は、継続的にカバー及びドアを監視し、並びに回路はカバーの除去又はドア開放がなされたときは、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。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が暗号モジュール内に含まれているときはいつでも、回路は、作動していなければならない。

[解説]

「回路」は、「タンパー応答及びゼロ化回路」と解釈する。

**TE05.29.01：**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を持つ場合には、ベンダが提供する文書は、暗号モジュールがタンパー応答及びゼロ化回路を含まれるべきことを規定しなければならない。

**TE05.29.02：**囲いが除去可能なカバー若しくはドアを有するか、又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場合には、試験者は、ベンダが提供する文書から、カバー若しくはドアが除去される際、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る際に、暗号モジュールが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ことを検証しなければならない。

**TE05.29.03：**試験者は、検査によって及びベンダが提供する文書から、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が暗号モジュール内に含まれるとき、タンパー応答及びゼロ化回路が作動していることを検証しなければならない。

**TE05.29.04：**試験者は、検査によって及びベンダが提供する文書から、高い確率で暗号モジュールに重大な損害を与えることなく、囲いが除去又は貫かれないことを検証しなければならない。

**TE05.29.05：**囲いが除去可能なカバー若しくはドアを有するか、又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場合には、試験者は、カバー若しくはドアが除去されるとき、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る場合、暗号モジュールが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ことを試験しなければならない。

注：この試験は、次の一つ又はそれ以上の方法で行われる。

1．試験者は、試験者の設備において試験を行う。

2．試験者は、ベンダの設備において試験を行う。
3．試験者は、ベンダの設備において、ベンダが行う試験を監督する。
・試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
・試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
・試験者は、行われている試験を直接観察しなければならない。

**TE05.29.06：**試験者は、囲いが、高い確率で暗号モジュールに重大な損害を与えることなく、除去又は貫かれないことを試験しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。
1．試験者は、試験者の設備において試験を行う。
2．試験者は、ベンダの設備において試験を行う。
3．試験者は、ベンダの設備において、ベンダが行う試験を監督する。
・試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
・試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
・試験者は、行われている試験を直接観察しなければならない。

**AS05.30：(シングルチップ-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。**
注：このアサーションは、個別には試験されない。
[解説]
「次の要求事項」は、AS05.31、AS05.32を指す。

**AS05.31：(シングルチップ-レベル 4)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。**

**VE05.31.01：**暗号モジュールは、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。材料の硬度の特性及び接合性は、暗号モジュールから材料を剥がしたり、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(例えば、暗号モジュールが機能しなくなる)ものでなければならない。材料は、可視光領域内において不透明でなければならない。ベンダが提供する文書は、使用されるコーティングの種類及びその特性を識別しなければならない。

**TE05.31.01：**試験者は、検査によって及びベンダが提供する文書から、暗号モジュールが堅く不透明な除去耐性のあるコーティングで覆われていることを検証しなければならない。ベンダが提供する文書は、使用されるコーティングを規定して、その硬度及び除去耐性に

関するデータを提供しなければならない。

**TE05.31.02：**試験者は、暗号モジュールのコーティングの除去耐性に関する特性について検証しなければならない。試験者は、暗号モジュールから材料を剥がしたり、又はこじ開けたりしようと試みて、このような試みは想定される力の範囲では不可能であり、暗号モジュールが機能を停止する、又は暗号モジュールの回路が明らかに物理的に破壊されることを検証しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。

1. 試験者は、試験者の設備において試験を行う。
2. 試験者は、ベンダの設備において試験を行う。
3. 試験者は、ベンダの設備において、ベンダが行う試験を監督する。
   - ・試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
   - ・試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
   - ・試験者は、行われている試験を直接観察しなければならない。

**AS05.32:(シングルチップ-レベル4)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。**

**VE05.32.01：**ベンダが提供する文書は、除去耐性のあるコーティングの溶解特性について記述しなければならない。材料の溶解特性は、材料を除去するための溶解が、高い確率で暗号モジュールを溶解する、又は重大な損害を与えるような特性でなければならない。

**TE05.32.01：**試験者は、暗号モジュールの除去耐性のあるコーティングの溶解特性を判定するために、ベンダが提供する文書をレビューしなければならない。

**TE05.32.02：**試験者は、暗号モジュールの除去耐性のあるコーティングの溶解特性を試験しなければならない。試験者は、VE05.32.01で提供された文書に基づき、どのタイプの溶剤が除去耐性のあるコーティングを危殆化するために必要かを判定しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。

1. 試験者は、試験者の設備において試験を行う。
2. 試験者は、ベンダの設備において試験を行う。
3. 試験者は、ベンダの設備において、ベンダが行う試験を監督する。
   - ・試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
   - ・ 試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
   - ・試験者は、行われている試験を直接観察しなければならない。

## 5.3 マルチチップ組込型暗号モジュール

**AS05.33：(マルチチップ組込型-レベル 1,2,3,及び 4)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。**

注：このアサーションは、個別には試験されない。

[解説]

「次の要求事項」は、AS05.34を指す。

**AS05.34：(マルチチップ組込型-レベル 1,2,3,及び 4)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。**

**VE05.34.01：**暗号モジュールは、製品グレードの囲い又は除去可能なカバー内に完全に含まれなければならない。ベンダが提供する文書は、カバー又は囲いについて記述しなければならない。

**TE05.34.01：**試験者は、検査によって及びベンダが提供する文書から、暗号モジュールが、製品グレードの囲い又は除去可能なカバー内に含まれていることを検証しなければならない。

**AS05.35:(マルチチップ組込型-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、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。**

注：このアサーションは、個別には試験されない

[解説]

「次の要求事項」は、AS05.36、AS05.37を指す。

**AS05.36：(マルチチップ組込型-レベル2,3,及び4)**

- **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、又は封止材(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)、若しく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、AS05.37が満たされなければならない。**

注：この要求事項は、AS05.16と関連している。

**VE05.36.01：**暗号モジュールは、エッチング耐性のあるコーティング又は厚い塗装のよう

な、不透明でタンパー証跡を残すコーティングでカプセル化されていなければならない。その材料は、可視光領域で不透明でなければならない。ベンダが提供する文書は、不透明でタンパー証跡を残すコーティングの種類及びその特性を識別しなければならない。

**TE05.36.01：**試験者は、検査によって及びベンダが提供する文書から、暗号モジュールが、不透明でタンパー証跡を残す材料でカプセル化されていることを検証しなければならない。検査は、タンパー証跡を残す材料が暗号モジュールを完全に覆い、及びタンパー証跡を残す材料が視覚的に不透明であることを検証しなければならない。

**TE05.36.02：**試験者は、試験によって、暗号モジュールが、暗号モジュールコンポーネントへのタンパー又は除去の試みの証拠を提供することを検証しなければならない。

**AS05.37：(マルチチップ組込型-レベル2,3,及び4)**

- **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。**

**又は**

- **AS05.36が満足されなければならない。**

注：この要求事項は、AS05.16と関連している。

**VE05.37.01：**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、除去可能なカバー又はドアを含んでもよい。ベンダが提供する文書は、囲い及びその硬度の特性について記述しなければならない。

**VE05.37.02：**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。ベンダが提供する文書は、囲いの不透明度の特性を記述しなければならない。

**VE05.37.03：**囲いが、除去可能なカバー又はドアを含む場合には、除去可能なカバー又はドアは、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によって保護されていなければならない。ベンダが提供する文書は、そのタンパー証跡を残すシールについて記述しなければならない。

**TE05.37.01：**試験者は、検査によって及びベンダが提供する文書から、暗号モジュールが次の要求事項を満たす囲いに含まれていることを検証しなければならない。

1. 囲いは、暗号モジュール全体を完全に囲まなければならない。
2. 囲いの材料は、ベンダが提供する文書で定義された組成でなければならない。
3. 囲いは、製品グレードでなければならない。ベンダが提供する印刷物は、同じ材料の囲いが商用に用いられていたことを示すか、又はその囲いが商用の製品と同等であることを示すためのデータを提供しなければならない。

**TE05.37.02：**試験者は、検査によって、囲いが可視光領域内において不透明であることを検証しなければならない。

**TE05.37.03：**試験者は、囲いが除去可能なカバー又はドアを含んでいるかどうかを判定しなければならない。試験者は、それぞれのカバー及びドアが、次の 2 つの要求事項のうち一方を満たすことを検証しなければならない。

1. カバー又はドアは、物理的鍵又は論理的鍵を必要とする、こじ開け耐性のある錠が掛けられている。試験者は、鍵を使用せずに、錠が掛けられたカバー又はドアを開けることを試みて、そのカバー又はドアが、損傷の痕跡なしには開かないことを判定しなければならない。
2. 又は、カバー又はドアは、証跡性テープ又はホログラフシールのようなシールで保護されている。試験者は、カバー又はドアが、シールを破る又は剥がすことなしに開けられないこと、並びにそのシールが剥がされ、及び後で置き換えられないことを検証しなければならない。

**AS05.38：(マルチチップ組込型-レベル 3,及び 4)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。**

注：このアサーションは、個別には試験されない。

[解説]

「次の要求事項」は、AS05.39を指す。

**AS05.39：(マルチチップ組込型-レベル 3,及び 4)**

- **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)。**

注：次の要求事項(TE05.39.01、TE05.39.02、TE05.39.04、TE05.39.05、TE05.39.09、及びTE05.39.10)は、AS05.18、AS05.19、及びAS05.20と関連している。

**VE05.39.01：**ベンダが提供する文書は、AS05.39で規定されている方法のどちらが暗号モジュールに実装されているか、及びその方法がサポートしている設計文書(VE05.28.01)を提供することを宣言しなければならない。この選択に依存して、それぞれに対応するベンダ

の要求事項(次に示す項目それぞれ)が満たされなければならない。

1. 暗号モジュールのマルチチップ回路は、堅く不透明な封止材で完全に覆われていなければならない。材料は可視光領域内において不透明でなければならない。
2. 暗号モジュールは、強固な囲い内に完全に含まれていなければならない。囲いは、それを除去しようとする試みが、高い確率で暗号モジュール内に重大な損害を与える(例えば、暗号モジュールが機能しなくなる)ように設計されなければならない。囲いが、あらゆる除去可能なカバー又はドアを含む場合には、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。その回路は、継続的にカバー及びドアを監視して、カバーの除去又はドアの開放時に、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。回路は、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が暗号モジュール内に含まれているときはいつでも作動していなければならない。

**TE05.39.01：**ベンダが提供する文書は、暗号モジュールが、ドア又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を有する場合には、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ことを規定しなければならない。

**TE05.39.02：**囲いが除去可能なカバー若しくはドアを有するか、又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場合には、試験者は、ベンダが提供する文書から、カバー若しくはドアが除去されるとき、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る場合、暗号モジュールが、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ことを検証しなければならない。

**TE05.39.03：**試験者は、ベンダが提供する文書が、VE05.39.01の中のどの選択要求事項が実装されているかを規定して、設計文書を提供していることを検証しなければならない。

**TE05.39.04：**試験者は、検査によって及びベンダが提供する文書から、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が暗号モジュール内に含まれているときは、タンパー応答及びゼロ化回路が作動していることを検証しなければならない。

**TE05.39.05：**試験者は、検査によって及びベンダが提供する文書から、囲いが、高い確率で暗号モジュールに重大な損害を与えることなしに除去、又は貫かれないことを検証しなければならない。

**TE05.39.06：**(選択 1-堅く不透明な材料の利用)試験者は、検査によって及びベンダが提供する文書から、暗号モジュールが堅く不透明な材料で覆われていることを検証しなければならない。ベンダが提供する文書は、使用している材料を規定しなければならない。試験者は、その材料が、容易に回路層の深さまで貫かれないことを検証しなければならない。試験者は、材料が暗号モジュールを完全に覆っていること、及び材料が可視光領域内にお

いて不透明であることを検証しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。
1．試験者は、試験者の設備において試験を行う。
2．試験者は、ベンダの設備において試験を行う。
3．試験者は、ベンダの設備において、ベンダが行う試験を監督する。
・試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
・試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
・試験者は、行われている試験を直接観察しなければならない。

**TE05.39.07：**(選択 2-強固な囲いの使用)試験者は、その下の回路へのアクセスを試みることによって、及び囲いが容易に破壊されないことを検証することによって、囲いの強度を判定しなければならない。試験者は、検査によって及びベンダが提供する文書から、囲いを除去できないことを検証しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。
1．試験者は、試験者の設備において試験を行う。
2．試験者は、ベンダの設備において試験を行う。
3．試験者は、ベンダの設備において、ベンダが行う試験を監督する。
・試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
・試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
・試験者は、行われている試験を直接観察しなければならない。

**TE05.39.08：**(選択 2-強固な囲いの使用)強固な囲いが、除去可能なカバー又はドアを有する場合には、試験者は、ベンダが提供する文書から、カバー又はドアが除去されるときに、暗号モジュールが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ことを検証しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。
1．試験者は、試験者の設備において試験を行う。
2．試験者は、ベンダの設備において試験を行う。
3．試験者は、ベンダの設備において、ベンダが行う試験を監督する。
・試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
・試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
・試験者は、行われている試験を直接観察しなければならない。

**TE05.39.09：**囲いが、ドア若しくは除去可能なカバーを有するか、又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場合には、試験者は、カバー若しくはドアが除去されるとき、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る場合、暗号モジュールが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

全てをゼロ化することを試験しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。
1．試験者は、試験者の設備において試験を行う。
2．試験者は、ベンダの設備において試験を行う。
3．試験者は、ベンダの設備において、ベンダが行う試験を監督する。
・試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
・試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
・試験者は、行われている試験を直接観察しなければならない。

**TE05.39.10：**試験者は、囲いが、高い確率で暗号モジュールに重大な損害を与えることなしに、除去又は貫かれないことを試験しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。
1．試験者は、試験者の設備において試験を行う。
2．試験者は、ベンダの設備において試験を行う。
3．試験者は、ベンダの設備において、ベンダが行う試験を監督する。
・試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
・試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
・試験者は、行われている試験を直接観察しなければならない。

**AS05.40：(マルチチップ組込型-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。**
注：このアサーションは、個別には試験されない。
[解説]
「次の要求事項」は、AS05.41～AS05.45を指す。

**AS05.41：(マルチチップ組込型-レベル4)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、若しく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配線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。**

**VE05.41.01：**暗号モジュールは、封止材又は囲いに対するタンパー攻撃を検出するタンパ

ー検出エンベロープ内に含まれていなければならない。ベンダが提供する文書は、タンパー検出エンベロープの設計について記述しなければならない。

[解説]

「暗号モジュール」(The module)は、「暗号モジュールコンポーネント」(The module component)と解釈する。

**TE05.41.01：**試験者は、ベンダが提供する文書から及び検査によって、暗号モジュールが、暗号モジュールコンポーネントを覆っているタンパー検出エンベロープを含んでいることを検証しなければならない。このバリアは、暗号モジュールコンポーネントへアクセスするための掘削、粉砕、研削、又は溶解のような方法によるあらゆる破損が、暗号モジュール内のコンポーネントを監視することによって検出できるよう設計されていなければならない。

[コメント]

暗号モジュールとタンパー検出エンベロープ及び封止材との包含関係が混乱している。VE05.41.01では、暗号モジュール内に、タンパー検出エンベロープ、封止材が含まれていない表現をしているのに対し、TE05.41.01では、暗号モジュール内に、タンパー検出エンベロープ、封止材が含まれている表現をしている。

**AS05.42：(マルチチップ組込型-レベル 4)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。**

注：このアサーションは、AS05.43 及び AS05.44 の一部として試験される。

**AS05.43：(マルチチップ組込型-レベル 4)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。**

注：このアサーションは、AS05.44 にて試験される。

**AS05.44：(マルチチップ組込型-レベル4)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。**

**VE05.44.01：**暗号モジュールは、タンパーの有無をタンパー検出エンベロープで継続的に監視しているタンパー応答及びゼロ化回路を含み、かつタンパーが検出されるとき、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の全てをゼロ化しなければならない。回路は、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が暗号モジュール内に含まれているときはいつでも作動していなければならない。ベンダが提供する文書は、タンパー応答及びゼロ化の設計について記述しなければならない。

**TE05.44.01：**試験者は、ベンダが提供する文書から、暗号モジュールが、タンパー検出の有無をタンパー検出エンベロープで継続的に監視し、エンベロープのあらゆる部分の掘削、

粉砕、研削、又は溶解のような方法によるあらゆる破損をも検出し、及びその結果、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タンパー応答及びゼロ化回路を含んでいることを検証しなければならない。

**TE05.44.02：**試験者は、タンパー検出エンベロープのバリアを壊し、及びその結果、試験者は暗号モジュールが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ことを検証しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。

1. 試験者は、試験者の設備において試験を行う。
2. 試験者は、ベンダの設備において試験を行う。
3. 試験者は、ベンダの設備において、ベンダが行う試験を監督する。
   - 試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
   - 試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
   - 試験者は、行われている試験を直接観察しなければならない。

**AS05.45：(マルチチップ組込型-レベル 4)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。**
注：このアサーションは、AS05.44の一部として試験される。

## 5.4 マルチチップスタンドアロン型暗号モジュール

**AS05.46：(マルチチップスタンドアロン型-レベル 1, 2, 3，及び 4)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。**
注：このアサーションは、個別には試験されない。
[解説]
「次の要求事項」は、AS05.47を指す。

**AS05.47：(マルチチップスタンドアロン型-レベル1，2，3，及び4)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。**

**VE05.47.01：**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、除去可能なカバー又はドアを含んでもよい。ベンダが提供する文書は、囲い及びその硬度の特性を記述しなければならない。

**TE05.47.01：**試験者は、検査によって及びベンダが提供する文書から、暗号モジュールが

次の要求事項を満たす囲い内に含まれていることを検証しなければならない。

1. 囲いは、暗号モジュール全体を完全に囲まなければならない。
2. 囲いの材料は、ベンダが提供する文書で定義された組成でなければならない。
3. 囲いは、製品グレードでなければならない。ベンダが提供する印刷物は、同じ材料の囲いが商用に用いられていたことを示すか、又はその囲いが商用の製品と同等であることを示すためのデータを提供しなければならない。

**AS05.48：(マルチチップスタンドアロン型-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、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。**

注：このアサーションは、個別には試験されない。

[解説]

「次の要求事項」は、AS05.49、AS05.50を指す。

**AS05.49：(マルチチップスタンドアロン型-レベル2，3，及び4)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。**

**VE05.49.01：**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。ベンダが提供する文書は、囲いの不透明度の特性を記述しなければならない。

**TE05.49.01：**試験者は、検査によって、囲いが可視光領域内において不透明であることを検証しなければならない。

**AS05.50：(マルチチップスタンドアロン型-レベル2，3，及び4)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。**

**VE05.50.01：**囲いが除去可能なカバー又はドアを含む場合には、除去可能なカバー又はドアは、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、証跡性テープ若しくはホログラフシールのようなタンパー証跡を残すシールによって保護されていなければならない。ベンダが提供する文書は、実装されたタンパー保護方法について記述しなければならない。

**TE05.50.01：**試験者は、囲いが除去可能なカバー又はドアを含んでいるかどうかを判定しなければならない。試験者は、それぞれのカバー及びドアが、次の２つの要求事項のうち一方を満たすことを検証しなければならない。

1. カバー又はドアは、物理的鍵又は論理的鍵を必要とする、こじ開け耐性のある錠が掛けられている。試験者は、鍵を使用せずに、錠が掛けられたカバー又はドアを開けることを試みて、そのカバー又はドアが、損傷の痕跡なしには開かないことを判

定しなければならない。

2.又は、カバー又はドアは、証跡性テープ又はホログラフシールのようなシールで保護されている。試験者は、カバー又はドアが、シールを破る又はシールを剥がすことなしに開けられないこと、並びにそのシールが剥がされ、及び後で置き換えられないことを検証しなければならない。

**AS05.51：(マルチチップスタンドアロン型-レベル 3 及び 4)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。**

注：このアサーションは、個別には試験されない。

[解説]

「次の要求事項」は、AS05.52、AS05.53を指す。

**AS05.52：(マルチチップスタンドアロン型-レベル 3 及び 4)**

**・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**

**・ AS05.53が満たされなければならない。**

**VE05.52.01：**ベンダが提供する文書は、AS05.52で規定された2つの方法のうちのどちらが実装されているかについて宣言して、設計情報を提供しなければならない。

**VE05.52.02：**(選択1)回路のマルチチップ形態は、堅い不透明な封止材で覆われていなければならない。その材料は、可視光領域内において、不透明でなければならない。

**TE05.52.01：**試験者は、ベンダが提供する文書が、VE05.52.01における要求事項の選択のどちらが実装されているかについて規定していて、設計文書を含むことを検証しなければならない。

**TE05.52.02：**(選択1-堅い不透明な封止材による覆い)堅い不透明な封止材内にカプセル化しなさい。内部アクセスが可能な場合には、試験者は、ベンダが提供する文書から及び検査によって、暗号モジュール内の回路が堅い不透明な封止材で覆われていることを検証しなければならない。ベンダが提供する文書は、どのような封止材が使用されているか、及びその封止材の硬度の特性について規定しなければならない。

**TE05.52.03：**(選択1-堅い不透明な封止材による覆い)アクセスが可能な場合には、試験者は、カバーがその下の回路層の深さまで容易に貫かれないことを検証しなければならない。アクセスが可能な場合には、試験者は、封止材が暗号モジュール内の回路を覆い、及びその封止材が可視光領域内において不透明であることを検証しなければならない。

**AS05.53：(マルチチップスタンドアロン型-レベル 3 及び 4)**

**・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。**

**又は、**

**・AS05.52が満たされなければならない。**

注：次の要求事項(TE05.53.01、TE05.53.02、TE05.53.04、TE05.53.05、TE05.53.08、及びTE05.53.09)は、AS05.18、AS05.19、及びAS05.20と関連している。

**VE05.53.01：**ベンダが提供する文書は、AS05.53で規定された方法のどちらが暗号モジュールに実装されているのかについて宣言して、サポートしている設計文書を提供しなければならない。

**VE05.53.02：**（選択1）暗号モジュールは強固な囲い内に完全に含まれていなければならない。その囲いは、囲いを除去する試みが、高い確率で、暗号モジュール内の回路に重大な損害を与えるように設計されていなければならない。その囲いが除去可能なカバー又はドアを含む場合には、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。その回路は、カバー及びドアを継続的に監視して、カバーの除去又はドアの開放時に、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。その回路は、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が暗号モジュール内に含まれている時はいつでも作動していなければならない。

**TE05.53.01：**ベンダが提供する文書は、暗号モジュールがドア又は除去可能なカバーを含んでいるか、又はメンテナンスアクセスインタフェースを有している場合には、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ことを規定しなければならない。

**TE05.53.02：**囲いが除去可能なカバー又はドアを有するか、又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場合には、試験者は、ベンダが提供する文書から、カバー又はドアが除去されるときに、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る場合、暗号モジュールが、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ことを検証しなければならない。

**TE05.53.03：**試験者は、ベンダが提供する文書がVE05.53.01における要求事項の選択のどちらが実装されているかについて規定して、設計文書を含むことを検証しなければならない。

**TE05.53.04：**試験者は、検査によって及びベンダが提供する文書から、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が暗号モジュール内に含まれている

ときに、タンパー応答及びゼロ化回路が作動していることを検証しなければならない。

**TE05.53.05：**試験者は、検査によって及びベンダが提供する文書から、囲いが高い確率で暗号モジュールに重大な損害を与えることなしに、除去又は貫かれないことを検証しなければならない。

**TE05.53.06：**（選択 1-強固な囲いの使用）試験者は、囲いに内在する回路へのアクセスを試みることによって、及び囲いが容易に破損されないことを検証することによって、囲いの強度を判定しなければならない。試験者は、検査によって及びベンダが提供する文書から、囲いが除去されないことを検証しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。

1. 試験者は、試験者の設備において試験を行う。
2. 試験者は、ベンダの設備において試験を行う。
3. 試験者は、ベンダの設備において、ベンダが行う試験を監督する。
   - 試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
   - 試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
   - 試験者は、行われている試験を直接観察しなければならない。

**TE05.53.07：**（選択 1-強固な囲いの使用）強固な囲いが、除去可能なカバー又はドアを有する場合には、試験者は、ベンダが提供する文書から、カバー又はドアが除去されるときに、暗号モジュールが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ことを検証しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。

1. 試験者は、試験者の設備において試験を行う。
2. 試験者は、ベンダの設備において試験を行う。
3. 試験者は、ベンダの設備において、ベンダが行う試験を監督する。
   - 試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
   - 試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
   - 試験者は、行われている試験を直接観察しなければならない。

**TE05.53.08：**囲いが、除去可能なカバー又はドアを有するか、又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場合には、試験者は、カバー又はドアが除去されるときに、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るときに、暗号モジュールが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ことを試験しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。

1. 試験者は、試験者の設備において試験を行う。
2. 試験者は、ベンダの設備において試験を行う。

3．試験者は、ベンダの設備において、ベンダが行う試験を監督する。
・試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
・試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
・試験者は、行われている試験を直接観察しなければならない。

**TE05.53.09：**試験者は、高い確率で暗号モジュールに重大な損害を与えることなく、囲いを除去できないこと、又は囲いに侵入できないことを試験しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。
1．試験者は、試験者の設備において試験を行う。
2．試験者は、ベンダの設備において試験を行う。
3．試験者は、ベンダの設備において、ベンダが行う試験を監督する。
・試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
・試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
・試験者は、行われている試験を直接観察しなければならない。

**AS05.54：(マルチチップスタンドアロン型-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。**
注：このアサーションは、個別には試験されない。
[解説]
「次の要求事項」は、AS05.55～AS05.59を指す。

**AS05.55：(マルチチップスタンドアロン型-レベル4)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。**

**VE05.55.01：**囲い又は封止材は、タンパー検出エンベロープによって、すなわち、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。ベンダが提供する文書は、タンパー検出エンベロープの設計について記述しなければならない。

**TE05.55.01：**試験者は、ベンダが提供する文書から及び検査によって、暗号モジュールの囲い又は封止材がタンパー検出メカニズムを含んでいることを検証しなければならない。そのタンパー検出メカニズムは、暗号モジュールコンポーネントを保護する、タンパー検

出エンベロープを形成しなければならない。そのメカニズムは、暗号モジュールコンポーネントへアクセスするための、囲い又は封止材のあらゆる破損が検出できるように設計されなければならない。

**AS05.56：(マルチチップスタンドアロン型-レベル 4)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。**
注：このアサーションは、AS05.58の一部として試験される。

**AS05.57：(マルチチップスタンドアロン型-レベル 4) 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。**
注：このアサーションは、AS05.58の一部として試験される。

**AS05.58：(マルチチップスタンドアロン型-レベル4)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。**

**VE05.58.01：**暗号モジュールは、タンパーの有無をタンパー検出エンベロープで継続的に監視しているタンパー応答及びゼロ化回路を含み、かつタンパーが検出されるとき、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の全てをゼロ化しなければならない。回路は、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が暗号モジュール内に含まれているときはいつでも、作動していなければならない。ベンダが提供する文書は、タンパー応答及びゼロ化の設計について記述しなければならない。

**TE05.58.01：**試験者は、ベンダが提供する文書から、タンパーの有無をタンパー検出エンベロープで継続的に監視し、エンベロープのいかなる部分の切削、掘削、粉砕、研削、又は溶解のような方法によるいかなる破損をも検出し、及びその結果、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タンパー応答及びゼロ化回路を、暗号モジュールが含んでいることを検証しなければならない。

**TE05.58.02：**試験者は、タンパー検出エンベロープのバリアを壊し、及びその結果、試験者は暗号モジュールが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ことを検証しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。
1．試験者は、試験者の設備において試験を行う。
2．試験者は、ベンダの設備において試験を行う。
3．試験者は、ベンダの設備において、ベンダが行う試験を監督する。

・試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
・試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
・試験者は、行われている試験を直接観察しなければならない。

**AS05.59：(マルチチップスタンドアロン型-レベル 4)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。**
注：このアサーションは、AS05.58の一部として試験される。

## 5.5 環境故障保護/環境故障試験

**AS05.60：(レベル4)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。**

**VE05.60.01：**ベンダは、4.5.5 節に規定されたように、次のいずれかを使用しなければならない。
1. EFP 特性
2. 又は、EFT

ベンダは、次の 4 つの異常な環境条件又は正規の動作範囲外の(偶然又は故意の)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ことを確実にするために､上記の 1. 又は 2.を使用しなければならない。
A. 低温度
B. 高温度
C. 負の高電圧
D. 正の高電圧

ベンダは、それぞれの条件に対して、EFP又はEFTの使用を選択しなければならないが、それぞれの選択は、他の条件に対する選択とは独立である。ベンダは、それぞれの条件に対応した、サポートしているEFP/EFTの文書を提供しなければならない。その文書は、選択された方法がどのように使用されているかについて規定しなければならない。

### 5．5．1　環境故障保護特性(選択1)

**AS05.61：(レベル 4)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。**

注：このアサーションは、AS05.64の一部として試験される。

**AS05.62：(レベル 4)特に、暗号モジュールは、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を監視し、その変動に対して正しく対処しなければならない。**
注：このアサーションは、AS05.64の一部として試験される。

**AS05.63：(レベル 4)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。**
注：このアサーションは、AS05.64 の一部として試験される。

**AS05.64：(レベル4)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。**

**VE05.64.01：** EFP が特定の条件に対して選択される場合には、暗号モジュールは、監視を行って、その条件で暗号モジュールが正規の動作範囲外となる動作温度又は動作電圧における変動に対して正しく応答しなければならない。保護特性は、これらの環境条件を継続的に測定しなければならない。条件が暗号モジュールの正規の動作範囲外であると判定された場合には、保護回路は次のいずれかを実施しなければならない。

1. 暗号モジュールをシャットダウンする。
2. 又は、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。

ベンダが提供する文書は、これらの方法のどちらが選択されたかについて宣言して、暗号モジュール内に実装された EFP 特性の詳細記述を提供しなければならない。

**TE05.64.01：**試験者は、暗号モジュールに対して規定された正規の動作範囲の限界付近の環境条件(周囲温度及び電圧)を設定して、暗号モジュールが正規の動作パラメータ内で実行し続けることを検証しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。

1. 試験者は、試験者の設備において試験を行う。
2. 試験者は、ベンダの設備において試験を行う。
3. 試験者は、ベンダの設備において、ベンダが行う試験を監督する。
   - ・試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
   - ・試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
   - ・試験者は、行われている試験を直接観察しなければならない。

**TE05.64.02：**試験者は、温度及び電圧を規定された正規の範囲外に広げて、暗号モジュールがそれ以上動作しないようにシャットダウンするか、又は暗号モジュールが平文の秘密

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ことを判定しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。
1．試験者は、試験者の設備において試験を行う。
2．試験者は、ベンダの設備において試験を行う。
3．試験者は、ベンダの設備において、ベンダが行う試験を監督する。
・試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
・試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
・試験者は、行われている試験を直接観察しなければならない。

**TE05.64.03：**暗号モジュールが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ように設計されており、かつ暗号モジュールが正規の環境範囲に戻った後もまだ作動していた場合には、試験者は、鍵を必要とするサービスを実行して、暗号モジュールがこれらのサービスを実行しないことを検証しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。
1．試験者は、試験者の設備において試験を行う。
2．試験者は、ベンダの設備において試験を行う。
3．試験者は、ベンダの設備において、ベンダが行う試験を監督する。
・試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
・試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
・試験者は、行われている試験を直接観察しなければならない。

**AS05.65：(レベル 4)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。**
注：このアサーションは、AS05.60及びAS05.64の一部として試験される。

## 5．5．2　環境故障試験手順(選択2)

**AS05.66：(レベル 4)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。**
注：このアサーションは、AS05.68の一部として試験される。

**AS05.67：(レベル 4)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。**
注：このアサーションは、AS05.68の一部として試験される。

**AS05.68：(レベル4)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)最小の正電圧までなければならない。**

**VE05.68.01：**EFT が特定の条件に対して選択される場合には、暗号モジュールは AS05.68 で規定された温度及び電圧の範囲内で試験されなければならない。暗号モジュールは、次のいずれかでなければならない。

1. 正常に動作を続ける。
2. 又は、シャットダウンする。
3. 又は、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。

ベンダが提供する文書は、これらの方法のどれが選択されたかについて宣言して、EFTの詳細記述を提供しなければならない。

**TE05.68.01：**試験者は、AS05.68で規定されているような環境条件(周囲温度及び電圧)を設定して、暗号モジュールが正常に動作し続けるか、又は暗号モジュールが以後の動作を中止するためにシャットダウンするか、若しくは暗号モジュールが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かのいずれかであることを検証しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。

1. 試験者は、試験者の設備において試験を行う。
2. 試験者は、ベンダの設備において試験を行う。
3. 試験者は、ベンダの設備において、ベンダが行う試験を監督する。
   - 試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
   - 試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
   - 試験者は、行われている試験を直接観察しなければならない。

**TE05.68.02：**暗号モジュールが、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設計がされており、かつ暗号モジュールが正規の環境範囲に戻った後もまだ作動していた場合には、試験者は鍵を必要とするサービスを実行して、暗号モジュールがこれらのサービスを実行しないことを検証しなければならない。
注：この試験は、次の一つ又はそれ以上の方法で行われる。

1. 試験者は、試験者の設備において試験を行う。

2．試験者は、ベンダの設備において試験を行う。
3．試験者は、ベンダの設備において、ベンダが行う試験を監督する。
・試験者による報告書の根拠資料には、試験者がなぜ試験を行うことが出来なかったかの説明が含まれなければならない。
・試験者は、必要とされる試験計画、及び試験内容を作成しなければならない。
・試験者は、行われている試験を直接観察しなければならない。

**AS05.69：(レベル 4)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。**

注：このアサーションは、AS05.68の一部として試験される。

# 6．動作環境

**AS06.01：(レベル 1，2，3，及び 4)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。**

注：このアサーションは、個別に試験されない。

[解説]

FIPS140-2は、変更可能な動作環境について、次のように記述している。

「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の部分に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。」

**AS06.02：(レベル 1，2，3，及び 4)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。**

**VE06.02.01：**ベンダが提供する文書は、暗号モジュールが動作する動作環境を記述しなければならない。

**TE06.02.01：**試験者は、VE06.02.01で規定された情報が含まれていることを検証しなければならない。この情報が含まれていない場合には、本アサーションは不合格とする。

## 6．1　オペレーティングシステム要求事項

**AS06.03：(レベル 1，2，3，及び 4)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。**

注：このアサーションは、AS06.04からAS06.08までの一部として試験される。

[解説]

「次の要求事項」は、AS06.04～AS06.08を指す。

**AS06.04：(レベル 1 のみ)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)。**
注：この要求事項は、管理者に対する文書及び手順によって実現されるのではなく、暗号モジュールそのものによって実現されなければならない。

**VE06.04.01：**ベンダは、同時にただ一人のユーザが暗号モジュールを使用できることを確実にするために用いているメカニズムについて説明しなければならない。

**TE06.04.01：**試験者は、クリプトオフィサ向けガイダンス文書及びユーザ向けガイダンス文書で説明される通りに暗号モジュールを操作しなければならない。暗号モジュールが規定されたように動作している間に、同一又はもう一人の試験者は、単一ユーザ強制メカニズムを回避することを試みなければならない。

**AS06.05：(レベル 1 のみ) 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生じるプロセスは、その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所有されない。**
注：この要求事項は、管理者に対する文書及び手順によって実現されるのではなく、暗号モジュールそのものによって実現されなければならない。

**VE06.05.01：**ベンダは、暗号プロセスが行われている間、他のいかなるプロセスも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にアクセスすることはできないことを確実にするメカニズムについて説明しなければならない。

**TE06.05.01：**試験者は、クリプトオフィサ向けガイダンス文書及びユーザ向けガイダンス文書で説明される通りに暗号機能を操作しなければならない。暗号機能が実行している間に、同一又はもう一人の試験者は、秘密鍵及びプライベート鍵、鍵生成の中間値、並びにその他のCSPへのアクセスを試みなければならない。

**AS06.06：(レベル 1 のみ)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。**

**VE06.06.01：**ベンダは、他のいかなるプロセスも実行中の暗号モジュールへの割り込み処理を行えないことを確実にするために用いているメカニズムについて説明しなければならない。

**TE06.06.01：**試験者は、クリプトオフィサ向けガイダンス文書及びユーザ向けガイダンス文書で説明される通りに暗号機能を操作しなければならない。暗号機能が動作している間に、同一又はもう一人の試験者は、他のプロセスの実行を試みなければならない。

**AS06.07：(レベル 1，2，3，及び 4)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。**

**VE06.07.01：**ベンダは、暗号モジュールに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のリストを提供して、許可されていない開示や変更を防止する保護メカニズムについて説明しなければならない。

**TE06.07.01：**試験者は、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に許可されていないアクセス及び許可されていない変更を試みなければならない。

**AS06.08：(レベル 1，2，3，及び 4)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。**

**VE06.08.01：**ベンダは、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の完全性を維持するために用いている技術を識別する文書を提供しなければならない。

**TE06.08.01：**試験者は、VE06.08.01で規定された情報が含まれていることを検証しなければならない。この情報が含まれていない場合には、このアサーションは不合格とする。

**TE06.08.02：**試験者は、暗号ソフトウエア及び暗号ファームウエアを改ざんすることを試みなければならない。完全性が維持される場合には、このTE(試験)は不合格とする。

[解説]

「完全性が維持される場合には」は、「改ざんしたにも関わらず、改ざんを検出できず、完全性が維持される場合には」を意味する。

**AS06.09：(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。**

注：このアサーションは、AS06.10からAS06.19までのアサーションの一部として試験される。

[解説]

「次の要求事項」は、AS06.10 ～AS06.19を指す。

「キュリティレベル2にも適用されるセキュリティレベル1の要求事項」は、AS06.07 ～AS06.08を指す。

**AS06.10：(レベル 2)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**

**VE06.10.01：**ベンダは、暗号モジュールの制御をおこなうオペレーティングシステムが、Annex Bのリストに記載されたPPに規定されている機能要件に対してEAL2の評価に見事合格したことことを示す文書を提供しなければならない。

**TE06.10.01：**試験者は、オペレーティングシステムが、情報技術セキュリティの分野におけるコモンクライテリア認証書の承認に関するアレンジメントに従い相互承認された証明書をもつことを検証しなければならない。

**AS06.11：(レベル 2，3，及び 4)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、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ように構成されなければならない。**

**VE06.11.01：**このVEは、VE06.14.01の一部として試験される。

**TE06.11.01：**このTEは、TE06.14.01の一部として試験される。

**TE06.11.02：**試験者は、格納された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を実行する特権をもつ役割を担わなければならない。試験者は、オペレーティングシステムのアクセス制御メカニズムが正しく構成されていることを検証するために格納された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を実行しなければならない。

**TE06.11.03：**試験者は、格納された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を実行する特権をもたない役割を担わなければならない。試験者は、オペレーティングシステムのアクセス制御メカニズムが正しく構成されていることを検証するために、格納された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を実行することを試みなければならない。試験者が格納された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を実行できる場合には、このアサーションは不合格とする。

**AS06.12：(レベル 2，3，及び 4)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、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できるように構成されなければならない：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。**

**VE06.12.01：**このVEは、VE06.14.01の一部として試験される。

**TE06.12.01：**このTEは、TE06.14.01の一部として試験される。

**TE06.12.02：**試験者は、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及びファームウエアコンポーネントを変更する特権をもつ役割を担わなければならない：

1. 暗号プログラム
2. 暗号データ(例えば、暗号鍵、監査データ)
3. その他の CSP
4. 平文データ

試験者は、暗号境界内に格納されてい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変更しなければならない。

**TE06.12.03：**試験者は、格納されている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を変更する特権をもたない役割を担わなければならない。試験者は、格納されている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を変更することを試みなければならない。

**AS06.13：(レベル 2，3，及び 4)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、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とりを行うことができる役割の集合を規定できるように構成されなければならない：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。**

**VE06.13.01：**このVEは、VE06.14.01の一部として試験される。

**TE06.13.01：**このTEは、TE06.14.01の一部として試験される。

**TE06.13.02：**試験者は、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の読み出しを行う特権をもつ役割を担わなければならない：

1. 暗号データ(例えば、暗号鍵及び監査データ)
2. CSP
3. 平文データ

試験者は、暗号境界内に格納され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読み出しを行わなければならない。

**TE06.13.03：**試験者は、格納されている暗号ソフトウエアコンポーネントの読み出しを行う特権をもたない役割を担わなければならない。試験者は、格納されている暗号ソフトウ

エアコンポーネントの読み出しを行うことを試みなければならない。

**AS06.14：(レベル 2，3，及び 4)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、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ように構成されなければならない。**

**VE06.14.01：**ベンダは、AS06.11、AS06.12、AS06.13、及びAS06.14の要求事項を満足するために、任意アクセス制御(DAC)メカニズムがどのように構成されているかを規定する文書を提供しなければならない。

**TE06.14.01：**試験者は、ベンダがVE06.14.01において必要とされる情報を提供していることを検証しなければならない。

**TE06.14.02：**試験者は、暗号鍵及びその他のCSPを入力する特権をもつ役割を担わなければならない。試験者は、暗号鍵及びその他のCSPを入力しなければならない。

**TE06.14.03：**試験者は、暗号鍵及びその他のCSPを入力する特権をもたない役割を担わなければならない。試験者は、暗号鍵及びその他のCSPの入力を試みなければならない。

**AS06.15：(レベル 2，3，及び 4)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。**

**VE06.15.01：**ベンダは、オペレーティングシステムが、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の変更を行うことを、どのように防ぐかを規定する文書を提供しなければならない。

**TE06.15.01：**試験者は、ベンダがVE06.15.01において必要とされる情報を提供していることを検証しなければならない。

**TE06.15.02：**試験者は、実行中の暗号プロセスの変更を試みなければならない。オペレータ又は実行中のプロセスが、実行中の暗号プロセスを変更できる場合には、この試験は不合格とする。

**AS06.16：(レベル 2，3，及び 4)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。**

**VE06.16.01：**ベンダは、オペレーティングシステムが、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、どのように防ぐかを説明する文書を提供しなければならない。

**TE06.16.01：**試験者は、ベンダがVE06.16.01において必要とされる情報を提供していることを検証しなければならない。

**TE06.16.02：**試験者は、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試みなければならない。試験者は、いかなるオペレータ又は実行中のプロセスも、暗号境界内に格納された暗号ソフトウエアの読み出しができないことを検証しなければならない。

**AS06.17：(レベル 2，3，及び 4)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。注：このアサーションの前提は、識別されたイベントを監査するために、暗号モジュールが、オペレーティングシステムによって提供される監査メカニズムを使用しなければならないということである。暗号モジュールのソフトウエアが監査ログとして別のファイルを使用することは、それがどのように適切に保護されているとしても十分でない。**

**VE06.17.01：**ベンダは、暗号モジュールソフトウエアによって監査することができる全てのイベントを識別しなければならない。このリストは、AS06.18、及びAS06.19で規定されたイベントを含まなければならない
注：試験者は、オペレーティングシステムによって提供され、かつ、ベンダによって識別された監査メカニズムを試験しなくてもよい。

**TE06.17.01：**試験者は、ベンダがVE06.17.01において必要とされる情報を提供していることを検証しなければならない。

**TE06.17.02：**試験者は、監査能力が機能している状態で暗号モジュールを実行して、監査イベントを発生する操作を行わなければならない。試験者は、全てのイベントが監査されているかどうかを判定するために、システムの監査ログをレビューしなければならない。

**AS06.18：(レベル 2，3，及び 4)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**

注：このアサーションは、AS06.17の一部として試験される。

**AS06.19：(レベル 2，3，及び 4)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**

注：このアサーションは、AS06.17の一部として試験される。

**AS06.20：(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。**
**注：このアサーションは、AS06.21からAS06.25の一部として試験される。**

[解説]

「次の要求事項」は、AS06.21～AS06.25を指す。

**AS06.21：(レベル 3)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。**

**VE06.21.01：**ベンダは、暗号モジュールを制御するオペレーティングシステムが、Annex Bのリストに記載されたPPに規定されている機能要件(加えて、高信頼パス(FTP_TRP.1))に対して、評価レベルEAL3(加えて、非形式的なTOEセキュリティ方針モデル(ADV_SPM.1))に合格したことを示す文書を提供しなければならない。

**TE06.21.01：**試験者は、オペレーティングシステムが、情報技術セキュリティの分野におけるコモンクライテリア認証書の承認に関するアレンジメントに従い相互承認された証明書をもつことを検証しなければならない。

[解説]

ここでは、暗号モジュールとその動作環境である OS に対する要求事項の整合を要求している。

暗号モジュールのセキュリティレベルに対する、高信頼チャネルの使用とセキュリティポリシの文書化についての要求は以下のとおりである。

| レベル | 高信頼チャネル<br>AS02.17 | セキュリティポリシ<br>AS01.16 |
|---|---|---|

| | | |
|---|---|---|
| 1 | なし | ○ |
| 2 | なし | ○ |
| 3 | ○ | ○ |
| 4 | ○ | ○ |

AnnexB の PP が要求する機能要件，保証要件は以下である。

| PP 識別 | 保証レベル | FTP_TRP.1 | ADV_SPM.1 |
|---|---|---|---|
| CAPP | EAL3 | なし | なし |
| SLMOSPP | EAL4+ | ○ | ○ |

CAPP には FTP_TRP.1 及び ADV_SPM.1 が含まれていないため、当該 PP に AS06.21 で Argument を追加している。

**AS06.22：(レベル 3 及び 4)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。**

**VE06.22.01：**ベンダは、暗号鍵及びその他のCSP、認証データ、制御入力、並びに状態出力を通信するために暗号モジュールに使用されている高信頼パスのメカニズムを文書化しなければならない。

**TE06.22.01：**試験者は、ベンダがVE06.22.01において必要とされる情報を提供していることを検証しなければならない。

**TE06.22.02：**試験者は、全ての暗号鍵及びその他のCSP、認証データ、制御入力、及び状態出力を通信するために高信頼メカニズムを使用しなければならない。
注：高信頼メカニズムが高信頼パスであって、高信頼パスがオペレーティングシステムの一部として評価されたものである場合には、試験者は、高信頼パスを独自に試験する必要はない。高信頼メカニズムが高信頼パスでないか、又は、高信頼パスがオペレーティングシステムの一部として評価されていないものである場合には、試験者は、その高信頼メカニズムが正しく動作すること、及び高信頼メカニズムを回避できないことを試験しなければならない。

**TE06.22.03：**試験者は、AS06.22に識別されたそれぞれの入出力に対して、信頼できないあるメカニズムを介して情報を入力又は出力することを試みなければならない。

**AS06.23：(レベル 3 及び 4)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。**

**VE06.23.01：**ベンダは、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で使用されている高信頼パスを文書化しなければならない。

**TE06.23.01：**試験者は、ベンダがVE06.23.01において必要とされる情報を提供していることを検証しなければならない。

**AS06.24：(レベル 3 及び 4)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。**

**VE06.24.01：**ベンダは、どのようにして高信頼パスがオペレータ又は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るかを文書化しなければならない。

**TE06.24.01：**試験者は、ベンダがVE06.24.01において必要とされる情報を提供していることを検証しなければならない。

**TE06.24.02：**試験者は、高信頼パスを用いなければならない。TSFに高信頼パスを用いる能力がある場合には、試験者は、TSFに高信頼パスを用いさせるために暗号モジュールを操作しなければならない。

**TE06.24.03：**試験者は、高信頼パスがTSFでないソフトウエアに用いられるように試みなければならない。

**AS06.25：(レベル 3 及び 4)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**

**VE06.25.01：**ベンダが提供する監査イベントのリストは、高信頼パス機能を使用する試み、並びに高信頼パスの起動者及び対象の識別を含まなければならない。
注：試験者は、オペレーティングシステムが提供する監査メカニズム、及びベンダによって識別された監査メカニズムを試験する必要はない。

**TE06.25.01：**試験者は、ベンダがVE06.25.01において必要とされる情報を提供していることを検証しなければならない。

**TE06.25.02：**試験者は、監査能力が機能している状態で暗号モジュールを実行して、監査イベントを発生する操作を行わなければならない。試験者は、全てのイベントが監査されているかどうかを判定するために、そのシステムの監査ログをレビューしなければならない。

**AS06.26：(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。**
注：このアサーションは、AS06.27の一部として試験される。
[解説]
「次の要求事項」は、AS06.27を指す。

**AS06.27: (レベル 4)全ての暗号ソフトウエア、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**

**VE06.27.01:**ベンダは、当該暗号モジュールの制御をおこなうオペレーティングシステムが、Annex Bのリストに掲載されたPPに規定されている機能要件に対してEAL4の評価合格に成功したことを示す文書を提供しなければならない。

**TE06.27.01:**試験者は、オペレーティングシステムが、情報技術セキュリティの分野におけるコモンクライテリア認証書の承認に関するアレンジメントに従い相互承認された証明書をもつことを検証しなければならない。

# 7．暗号鍵管理

## 総　論

**AS07.01：(レベル 1，2，3，及び 4)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。**

**VE07.01.01：**ベンダが提供する文書は、暗号モジュール内部の、秘密鍵及びプライベート鍵の全て、並びにその他のCSPの全ての保護について記述しなければならない。保護は、許可されていない開示、変更、及び置換に対して保護するメカニズムの実装を含まなければならない。

**TE07.01.01：**試験者は、秘密鍵及びプライベート鍵、並びにその他のCSPの保護について記述しているベンダが提供する文書をチェックしなければならない。試験者は、ベンダが提供する文書が、これらの鍵が許可されていない開示、許可されていない変更、及び許可されていない置換からどのように保護されているかについて記述していることを検証しなければならない。

**TE07.01.02：**試験者は次の試験を行わなければならない。:

1. 試験者がアクセスを許可されていない、秘密鍵及びプライベート鍵、並びにその他の CSP に(文書化された保護メカニズムを回避して)アクセスを試みなさい。暗号モジュールがアクセスを拒否するか、又は暗号モジュールが暗号化された形式若しくは別のやり方で保護された形式の､秘密鍵及びプライベート鍵､並びにその他の CSP に対してだけアクセスを許す場合には、この要求事項は満たされる。
2. ベンダが提供する文書によって規定されていない方法を用いて、秘密鍵及びプライベート鍵の全て、並びにその他のCSPの全てを変更して、暗号モジュール内にそれらをロードすることを試みなさい。暗号モジュールは、いかなる秘密鍵及びプライベート鍵、並びにその他のCSPもロードを成功させてはならない。試験者は、秘密鍵及びプライベート鍵を用いて、暗号操作を行うことを試みなければならない。暗号モジュールは、それらの動作を行ってはならない。試験者は、その他のCSPを用いて、暗号サービスを行うことを試みなければならない。暗号モジュールは、それらの動作を行ってはならない。

**AS07.02：(レベル 1，2，3，及び 4)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。**

**VE07.02.01：**ベンダが提供する文書は、許可されていない変更及び置換に対する全ての公

開鍵の保護について記述しなければならない。

**TE07.02.01：**ベンダが提供する文書は、公開鍵が、許可されていない変更及び許可されていない置換から、どのように保護されているかについて記述しなければならない。

**TE07.02.02：**試験者は、ベンダが提供する文書によって規定されていない方法を用いて、全ての公開鍵を変更して、暗号モジュール内にそれらをロードすることを試みなければならない。暗号モジュールは、いかなる鍵もロードを成功させてはならない。試験者は、これらの鍵を用いて、暗号操作を行うことを試みなければならない。暗号モジュールは、これらの鍵がロードされなかったことを示し、これらの動作を行ってはならない。

**AS07.03：(レベル 1，2，3，及び 4)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。**

**VE07.03.01：**ベンダが提供する文書は、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 のリストを提供しなければならない。

**TE07.03.01：**試験者は、VE07.03.01 に規定された情報が含まれていることを検証するために、ベンダが提供する文書をレビューしなければならない。

## 7.1 乱数生成器(RNG)

**AS07.04：(レベル 1，2，3，及び 4)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。**
注：このアサーションはAS09.41-AS09.43で試験される。

**AS07.05:**
注：このアサーション番号に対する要求事項はない。

**AS07.06：(レベル１，２，３，及び４)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。**
注：このアサーションは、AS09.13 で試験される。

**AS07.07：(レベル 1，2，3，及び 4)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。**
注：このアサーションは、個別には試験されない。

**AS07.08：(レベル 1，2，3，及び 4)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。**

**VE07.08.01：**ベンダは、承認された RNG が鍵を生成するために用いられていることを宣言している文書を提供しなければならない。承認された RNG は、FIPS PUB 140-2 の Annex C に記載されている。

**TE07.08.01：**試験者は、ベンダが、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使用される RNG が FIPS PUB 140-2 の AnnexC に記載されている承認された RNG であると主張する文書を提供したことを検証しなければならない。

**TE07.08.02：**試験者は、実装された RNG が規定された承認された RNG と一致していることを検証するために、ベンダが提供する文書をレビューしなければならない。

**AS07.09：(レベル 1，2，3，及び 4)シード及びシード鍵は、同じ値をもってはならない。**

**VE07.09.01：**ベンダは、承認された RNG に入力されるシード及びシード鍵が同じ値をもっていないことを確実にする方法を記述している文書を提供しなければならない。

**TE07.09.01：**試験者は、ベンダが提供する文書が、シード及びシード鍵が同じ値にならないことを示していることを検証しなければならない。

**TE07.09.02：**試験者は、ベンダが提供する文書の記述が実装と一致していることを検証しなければならない。

**AS07.10：(レベル 1, 2, 3，及び 4)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。**

**VE07.10.01：**ベンダが提供する文書は、暗号モジュールに用いられている全ての(承認された及び承認されていない)RNG、それらのタイプ(承認された又は承認されていない)及びそれぞれの(承認された及び承認されていない)RNG が、暗号モジュール内において、どのように使用されているかを規定しなければならない。

**TE07.10.01：**試験者は、VE07.10.01 に規定された情報が含まれていることを検証するために、ベンダが提供する文書をレビューしなければならない。

## 7.2 鍵生成

**AS07.11:(レベル１，２，３，及び４)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。**

**VE07.11.01：**ベンダは、承認された鍵生成方法が鍵生成に使用されていることを宣言する文書を提供しなければならない。

**TE07.11.01：**試験者は、ベンダが、暗号鍵の生成に用いられる方法が承認された鍵生成方法であることを主張している文書を提供したことを検証しなければならない。

**TE07.11.02：**試験者は、実装された鍵生成方法が、規定された承認された鍵生成方法と一致していることを検証するために、ベンダが提供する文書をレビューしなければならない。

**AS07.12：(レベル 1，2，3，及び 4)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。**
注：このアサーションは、AS07.04－AS07.08及びAS07.10の一部として試験される。

**AS07.13：(レベル 1，2，3，及び 4)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。**
[解説]
「少なくとも」の部分は、原文では” as least ”であるが、”at least ”の誤りと解釈した。
【同様の箇所】VE07.13.01, TE07.13.01

**VE07.13.01：**ベンダは、どのようにして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)が、少なくとも、生成された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かを宣言している根拠を提供している文書を提供しなければならない。

**TE07.13.01:**試験者は、ベンダが提供する文書が、どのようにして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)が、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かを宣言している根拠を提供していることを検証しなければならない。

**TE07.13.02：**試験者は、ベンダによって与えられるあらゆる根拠の正確さを判定しなけれ

ばならない。証明の責任は、ベンダにある。すなわち、不確かさ又は曖昧さがある場合には、試験者は、必要とされる付加情報を提示するように、ベンダに要求しなければならない。

**AS07.14：(レベル 1，2，3，及び 4)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。**
注：このアサーションは、AS07.23の一部として試験される。

**AS07.15：(レベル 1，2，3，及び 4)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。**

**VE07.15.01：**ベンダが提供する文書は、何らかの中間の鍵生成値が、鍵生成処理の完了時に、暗号モジュールから出力されているかどうかを示さなければならない。

**VE07.15.02：**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、ベンダが提供する文書は、その値が、1)暗号化された形式、又は 2)知識分散の手順のもとで、出力されていることを規定しなければならない。

**TE07.15.01：**試験者は、ベンダが提供する文書が、何らかの中間の鍵生成値が、鍵生成処理の完了時に、暗号モジュールから出力されているかどうかを示していることを検証しなければならない。

**TE07.15.02：**試験者は、いかなる中間の鍵生成値も、鍵生成処理中に、暗号モジュールから出力されないことを検証しなければならない。

**TE07.15.03：**試験者は、出力インタフェースを観察して、全ての出力が文書化された出力と一致していること、及びいかなる平文の中間の鍵生成値も出力されないことを検証しなければならない。

**TE07.15.04：**試験者は、処理完了時に、中間の鍵生成値が、1)暗号化された形式、又は 2)知識分散の手順のもとで、出力されていることを検証しなければならない。

**AS07.16：(レベル 1, 2, 3，及び 4)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。**

**VE07.16.01：**ベンダは、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)鍵生成方法を宣言している文書を提供しなければならない。

**TE07.16.01：**試験者は、ベンダが、(承認された及び承認されていない)鍵生成方法につい

て記述している文書を提供したことを検証しなければならない。

**TE07.16.02：**試験者は、実装された鍵生成方法が規定された(承認された及び承認されていない)鍵生成方法と一致していることを検証するために、ベンダが提供する文書をレビューしなければならない。

## 7.3 鍵確立

**AS07.17：(レベル 1，2，3，及び 4)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。**

**VE07.17.01：**ベンダは、承認された鍵確立の技術が使用されていることを宣言する文書を提供しなければならない。承認された鍵確立の技術は、FIPS PUB 140-2 の Annex D に記載されている。

**TE07.17.01：**試験者は、ベンダが、使用される承認された鍵確立の技術が FIPS PUB 140-2 の Annex D に記載されていることを主張する文書を提供したことを検証しなければならない。

**TE07.17.02：**試験者は、実装された鍵確立の技術が、規定されている承認された鍵確立の技術と一致していることを検証するために、ベンダが提供する文書をレビューしなければならない。

**AS07.18：(レベル 1，2，3，及び 4)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。**

[コメント]

本ASの内容は、米国の国内規制に基づく事項である。

**VE07.18.01：**ベンダが提供する文書は、暗号モジュールが無線通信用に使用されているかどうかを示さなければならない。無線通信用に私用されている場合で、かつ、暗号モジュールが OTAR プロトコルを実装している場合には、ベンダは、OTAR の実装が“ APCO Project 25, OTAR Protocol ”に適合していることを宣言する文書を提供しなければならない。

**TE07.18.01：**試験者は、ベンダが提供する文書が、“ 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”で規定されているように、無線通信暗号モジュールが､どのように OTAR(Over-The-Air-Rekeying)を実装しているかについて宣言している根拠を提供していることを検証しなければならない。

**TE07.18.02：**試験者は、ベンダによって与えられるあらゆる根拠の正確さを判定しなければならない。立証責任は、ベンダにある。すなわち、不確かさ又は曖昧さがある場合には、試験者は、必要とされる付加情報を提示するように、ベンダに要求しなければならない。

**AS07.19：(レベル 1，2，3，及び 4)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。**

**VE07.19.01：**ベンダは、どのようにして鍵確立方法のセキュリティの危殆化(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を危殆化すること)が、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かを宣言している根拠を提供している文書を提供しなければならない。

**TE07.19.01：**試験者は、ベンダが提供する文書が、どのようにして鍵確立方法のセキュリティの危殆化(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を危殆化すること)が、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かを宣言している根拠を提供していることを検証しなければならない。

**TE07.19.02：**試験者は、ベンダによって与えられるあらゆる根拠の正確さを判定しなければならない。立証責任は、ベンダにある。すなわち、不確かさ又は曖昧さがある場合には、試験者は、必要とされる付加情報を提示するように、ベンダに要求しなければならない。

**AS07.20：(レベル 1，2，3，及び 4)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。**
注：このアサーションは、AS07.23-AS07.30の一部として試験される。

**AS07.21：(レベル 1，2，3，及び 4)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。**

**VE07.21.01：**ベンダは、暗号モジュールに用いられる鍵確立の方法について宣言している文書を提供しなければならない。

**TE07.21.01：**試験者は、ベンダが、鍵確立の方法について記述している文書を提供したことを検証しなければならない。

**TE07.21.02：**試験者は、実装された鍵確立の方法が規定された鍵確立の方法と一致していることを検証するために、ベンダが提供する文書をレビューしなければならない。

## 7.4 鍵入出力

**AS07.22：(レベル 1，2，3，及び 4)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。**
注：このアサーションは、AS07.28の一部として試験される。

**AS07.23：(レベル 1，2，3，及び 4)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。**

**VE07.23.01：**鍵管理に関する文書は、シード鍵の入力について記述しなければならない。

**TE07.23.01：**試験者は、シード鍵が鍵生成に使用されているかどうか判定するために、ベンダが提供する文書をレビューしなければならない。シード鍵が鍵生成に使用されている場合には、試験者は鍵管理に関する文書をレビューして、シード鍵の入力が暗号鍵の入力と一致していることを検証しなければならない。

**TE07.23.02：**試験者はシード鍵を入力して、シード鍵を入力するのに用いられた方法が文書化された方法と一致していることを検証しなければならない。

**AS07.24:(レベル 1, 2, 3，及び 4)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。**

**VE07.24.01：**ベンダは、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秘密鍵及びプライベート鍵を暗号化するために用いられる承認された暗号アルゴリズムを規定している文書を提供しなければならない。

**TE07.24.01：**試験者は、ベンダが提供する文書が、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秘密鍵及びプライベート鍵を暗号化するために用いられる承認された暗号アルゴリズムを規定していることを検証しなければならない。

**TE07.24.02：**試験者は、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秘密鍵及びプライベート鍵を暗号化するために用いられる、実装されている承認された暗号アルゴリズムが、規定された暗号化方法と一致していることを検証するために、ベンダが提供する文書をレビューしなければならない。

**AS07.25：(レベル 1，2，3，及び 4)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。**

**VE07.25.01：**文書化された鍵入出力の手順は、それぞれの鍵が正しいエンティティに関係づけられていることを確実にするために用いられるメカニズム又は手続きを記述しなければならない。

**TE07.25.01：**試験者は文書化された鍵入出力の手順をレビューして、その手順が入力又は出力された鍵がどのように正しいエンティティに関係づけられているかについて対処していることを検証しなければならない。

**TE07.25.02：**入力又は出力される鍵のそれぞれに対して、試験者は、最初に、特定のエンティティを担っている間に鍵を出力しなければならない。次に、試験者は、次の試験を行うことによって、鍵とエンティティとの間の関係を検証しなければならない。

1. 試験者は、鍵が出力されていたときに担っていたエンティティとは異なるエンティティを担わなければならない。次に、試験者は鍵の入力を試みて、鍵の入力が失敗することを検証しなければならない。
2. 試験者は、可能な場合には、鍵が異なるエンティティに関係づけられるように鍵コンポーネントを変更しなければならない。次に、試験者は、鍵が出力されていたときのエンティティを担い、鍵の入力を試みて、鍵の入力が失敗することを検証しなければならない。

**AS07.26：(レベル 1, 2, 3，及び 4)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鍵入力テストを用いて、検証されなければならない。**
注：このアサーションは、AS09.40の一部として試験される。

**AS07.27：(レベル 1，2，3，及び 4)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。**

**VE07.27.01：**文書化された鍵入力の手順は、暗号化された鍵又は鍵コンポーネントの入力の結果として生じる平文の秘密鍵又はプライベート鍵の表示を不可能にしなければならない。

**TE07.27.01：**試験者は文書化された鍵入力の手順をレビューして、暗号化された鍵又は鍵コンポーネントの入力の結果として生じる平文の鍵の表示が、鍵入力の処理の間、許されないことを検証しなければならない。

**TE07.27.02：**試験者は全ての暗号化された暗号鍵及び鍵コンポーネントを入力して、結果として生じるいかなる平文の鍵マテリアルも表示されないことを検証するために、暗号モジュールの出力インタフェースを監視しなければならない。

**AS7.28：(レベル 1, 2, 3，及び 4)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。**

**VE07.28.01：**ベンダが提供する文書は、暗号モジュールによって用いられる鍵の入力方法及び出力方法を規定しなければならない。

**TE07.28.01：**試験者は、VE07.28.01 に規定された情報が含まれていることを検証するために、ベンダが提供する文書をレビューしなければならない。

**TE07.28.02：**試験者は、手動で入力された鍵のそれぞれを入力及び出力して、それらが文書に従って入力及び/又は出力されることを検証しなければならない。

**AS07.29：(レベル 1，2，3，及び 4)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。**

**VE07.29.01：**ベンダが提供する文書は、自動化された方法を用いて確立された鍵を規定しなければならない。ベンダが提供する文書は、これらの鍵が暗号化された形式で入力及び出力されるかどうかを宣言しなければならない。

**TE07.29.01：**試験者は、ベンダが、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が、暗号モジュールから暗号化された形式で入力及び出力されることを主張した文書を提供したことを検証しなければならない。

**TE07.29.02：**自動化された方法が秘密鍵及びプライベート鍵を確立するために用いられる場合には、試験者は、これらの鍵が暗号モジュールから暗号化された形式で入力及び出力されることを検証しなければならない。

**AS07.30：(レベル 3 及び 4)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。**

注：このアサーションは、AS07.29の一部として試験される。

**AS07.31：（レベル 3 及び 4）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。**

**VE07.31.01：**この VE は VE07.28.01 の一部として試験される。

**TE07.31.01：**ベンダが提供する文書の検証は、TE07.28.01 のもとで行われる。

**TE07.31.02：**試験者は、ベンダが、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が(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ることを主張する文書を提供したことを検証しなければならない。

**TE07.31.03：**手動の方法が秘密鍵及びプライベート鍵を確立するために用いられる場合には、試験者は、これらの鍵が(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されることを検証しなければならない。

**TE07.31.04：**手動の方法が秘密鍵及びプライベート鍵を確立するために用いられる場合には、試験者は、これらの鍵が(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、暗号モジュールから出力されることを検証しなければならない。

**AS07.32：(レベル 3 及び 4)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。**

**VE07.32.01：**ベンダが提供する文書は、暗号モジュールが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するために用いる方法を規定しなければならない。

**TE07.32.01：**試験者は、認証がそれぞれの鍵コンポーネントに対して行われること、及び認証が文書化された鍵の入力及び出力の手順と合致していることをチェックしなければならない。

**TE07.32.02：**試験者は、知識分散の手順を用いて、それぞれの鍵コンポーネントを入力して、鍵コンポーネントを入力するオペレータのそれぞれが認証されることを検証しなければならない。

**TE07.32.03：**試験者は、知識分散の手順を用いて、それぞれの鍵コンポーネントを出力して、鍵コンポーネントを出力するオペレータのそれぞれが認証されることを検証しなければならない。

**AS07.33：(レベル 3 及び 4)知識分散の手順が用いられる場合には、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)。**
注：このアサーションは，AS02.18の一部として試験される。

**AS07.34：(レベル 3 及び 4)知識分散の手順が用いられる場合には、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。**

**VE07.34.01：**手動で確立された秘密鍵又はプライベート鍵が、知識分散の手順のもとで、入力又は出力される場合には、ベンダが提供する文書は、元の鍵を組立てるために必要な鍵コンポーネントの数を規定しなければならない。

**TE07.34.01：**試験者は、知識分散の手順のもとで、手動で確立された秘密鍵又はプライベート鍵を入力するには、元の鍵を組立てるのに少なくとも 2 つの鍵コンポーネントを必要とすることを検証するために、ベンダが提供する文書をレビューしなければならない。

**TE07.34.02：**試験者は、知識分散の手順のもとで、手動で確立された秘密鍵又はプライベート鍵の出力が、結果として、元の鍵を組立てることができる単一の鍵コンポーネントの出力にならないことを検証するために、ベンダが提供する文書をレビューしなければならない。

**AS07.35：(レベル 3 及び 4)知識分散の手順が用いられる場合には、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。**

**VE07.35.01：**ベンダは、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は元の鍵のどんな情報も提供しないようにする方式についての根拠を提供している文書を提供しなければならない。

**TE07.35.01：**試験者は、ベンダが提供する文書が、ｎ個の鍵コンポーネントが元の鍵を組立てるのに必要とされる場合には、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宣言する根拠を提供していることを検証しなければならない。

**TE07.35.02：**試験者は、ベンダによって与えられるあらゆる根拠の正確さを判定しなければならない。立証責任は、ベンダにある。すなわち、不確かさ又は曖昧さがある場合には、試験者は、必要とされる付加情報を提示するように、ベンダに要求しなければならない。

**AS07.36：(レベル 3 及び 4)知識分散の手順が用いられる場合には、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。**

**VE07.36.01：**ベンダは、暗号モジュールに用いられる知識分散の手順について規定している文書を提供しなければならない。

**TE07.36.01：**試験者は、ベンダが提供する文書の記述が実装と一致していることを検証しなければならない。

## 7.5 鍵の格納

**AS07.37：(レベル 1，2，3，及び 4)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。**
注：このアサーションは、AS07.40のもとで試験される。

**AS07.38：(レベル 1，2，3，及び 4)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。**
注：このアサーションは、AS07.40のもとで試験される。

**AS07.39：(レベル 1，2，3，及び 4)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。**

**VE07.39.01：**鍵の格納に関するベンダが提供する文書は、それぞれの鍵が正しいエンティティと関係づけられていることを確実にするために用いられるメカニズム又は手順を記述しなければならない。

**TE07.39.01：**試験者は鍵の格納に関するベンダが提供する文書をレビューして、その手順が、格納された鍵がどのように正しいエンティティに関係づけられているかについて対処していることを検証しなければならない。

**TE07.39.02：**試験者は、鍵とエンティティとの関係づけを変更しなければならない。次に、試験者はエンティティの 1 つとして暗号機能を行うことを試みて、これらの機能が働かな

いことを検証しなければならない。

**AS07.40：(レベル 1，2，3，及び 4)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。**

**VE07.40.01：**ベンダが提供する文書は、格納された鍵のそれぞれに対して、次の情報を規定しなければならない。

a. タイプ及び識別名
b. 格納場所
c. 鍵が格納される形式(平文、暗号化された形式、知識分散の手順のもと)。鍵が暗号化された形式で格納される場合には、鍵を暗号化するために用いられた承認された暗号アルゴリズムを規定しなければならない。

**TE07.40.01：**試験者は、VE07.40.01 で規定された情報が含まれていることを検証するために、ベンダが提供する文書をレビューしなければならない。

## 7.6 鍵のゼロ化

**AS07.41：(レベル 1，2，3，及び 4)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。**

[解説]

暗号化された暗号鍵及びその他のCSP、又はそうでなければ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(FIPS140-2の33ﾍﾟｰｼﾞ、4.7.6節2-4行目参照)。

**VE07.41.01：**ベンダが提供する文書は、次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 のゼロ化の情報を規定しなければならない。

a.ゼロ化技術
b.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 をゼロ化できるときの制限
c.ゼロ化される、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
d.ゼロ化されない、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、及びゼロ化されない根拠
e.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 を危殆化するのには不十分な時間内に、ゼロ化技術がどのように行われるかについて説明している根拠

**TE07.41.01：**試験者は、VE07.41.01で規定された情報が含まれていることを検証するために、ベンダが提供する文書をレビューしなければならない。試験者は、ベンダによって与えられるあらゆる根拠の正確さを判定しなければならない。立証責任は、ベンダにある。すなわち、不確かさ又は曖昧さがある場合には、試験者は、必要とされる付加情報を提示するように、ベンダに要求しなければならない。

**TE07.41.02：**試験者はどの鍵が暗号モジュール内に存在しているかについて注意して、ゼロ化のコマンドを実行しなければならない。ゼロ化のコマンドの完了に続いて、試験者は、暗号モジュール内に格納されていた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 のそれぞれを用いて、暗号操作を行うことを試みなければならない。試験者は、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 のそれぞれをアクセスできないことを検証しなければならない。

**TE07.41.03：**試験者はゼロ化を実行して、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 が危殆化するのには不十分な時間内に鍵の破壊手段が行われることを検証しなければならない。

**TE07.41.04：**試験者は、ゼロ化のコマンドによってゼロ化されない秘密鍵及びプライベート鍵の全て、並びにその他の CSP の全てが、(1)承認されたアルゴリズムを用いて暗号化されているか、又は、(2)組込まれた認証された暗号モジュール(この標準に適合しているとして認証されたもの)内において物理的若しくは論理的に保護されていることを検証しなければならない。

[解説]

暗号化された暗号鍵及びその他の CSP、又はそうでなければ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(FIPS140-2 の 33 ﾍﾟｰｼﾞ、4.7.6 節 2-4 行目参照)。

**AS07.42：(レベル 1，2，3，及び 4)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。**

注：このアサーションは、AS07.41のもとで試験される。

# 8．電磁妨害/電磁両立性(EMI/EMC)

[コメント]
本章は、米国の国内規制に基づく基準である。

**AS08.01：(レベル 1，2，3，及び 4)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。**
注：このアサーションは、個別に試験されない。
[解説]
「次の要求事項」は、AS08.02～AS08.05を指す。

**AS08.02：(レベル 1，2，3，及び 4)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。**
注：ここでの“これらの要求事項”とは、FIPS PUB 140-2に示される要求事項を指す。
[解説]
FCC は**米国連邦通信委員会(Federal Communications Commission)を指す。**

**VE08.02.01：**ベンダは FCC 要求事項の試験をした試験所名を提供しなければならない。

**VE08.02.02：**ベンダは、暗号モジュールの FCC ID 番号を提供しなければならない。
[解説]
本VEは、「ベンダは、提供する文書に、暗号モジュールが承認を受けたFCCのID番号を記述しなければならない」と解釈する。

**TE08.02.01：**試験者は、ベンダがVE08.02.01において要求されたFCC公認の試験所名を提供していることを検証しなければならない。
[解説]
本TEは、ベンダが提供する文書によって検証すると解釈する。

**TE08.02.02：**試験者は、ベンダが VE08.02.02 において要求された FCC ID 番号を提供していることを検証しなければならない。
[解説]
本TEは、ベンダが提供する文書によって検証すると解釈する。

**AS08.03：(レベル 1，2，3，及び 4)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。**
注：このアサーションは、AS08.04及びAS08.05の一部として試験される。

**AS08.04：(レベル 1 及び 2)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。**

**VE08.04.01：**ベンダは、暗号モジュールが 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 要求事項に適合していることを示す証拠及び文書を提供しなければならない。

**TE08.04.01：**試験者は、ベンダが VE08.04.01 において要求された情報を提供していることを検証しなければならない。

**TE08.04.02：**試験者は、TE08.04.01 が規定する提供情報に示された暗号モジュールのバージョンが AS10.02 で参照されていることを検証しなければならない。

**AS08.05：(レベル 3 及び 4)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。**

**VE08.05.01：**ベンダは、暗号モジュールが 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 要求事項に適合していることを示す証拠及び文書を提供しなければならない。

**TE08.05.01：**試験者は、ベンダが VE08.05.01 において要求された情報を提供していることを検証しなければならない。

**TE08.05.02：**試験者は、TE08.04.01 が規定する提供情報に示された暗号モジュールのバージョンが AS10.02 で参照されていることを検証しなければならない。

# 9．自己テスト

## 一般

**AS09.01：(レベル 1，2，3,及び 4)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。**
注：このアサーションは、AS09.07の一部として試験される。

**AS09.02：(レベル 1，2，3，及び 4)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。**
注：このアサーションは、AS09.07の一部として試験される。

**AS09.03：(レベル 1，2，3，及び 4)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。**
注：このアサーションは、AS09.07の一部として試験される。

**AS09.04：(レベル 1，2，3，及び 4)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。**

**VE09.04.01：**ベンダは、それぞれの自己テストに関係する全てのエラー状態を文書化し、及びそれぞれのエラー状態に対して期待されたエラーインジケータを示さなければならない。

**TE09.04.01：**試験者は、ベンダが提供する文書を検査し、暗号モジュールが自己テストを失敗したときの全てのエラー状態をリスト化していること、及びそれぞれのエラー状態に関係するエラーインジケータを示していることをチェックしなければならない。試験者は、エラー状態のリストと有限状態モデル(AS04.05 参照)で定義されたエラー状態とが一致していることを検証するために、それらを比較しなければならない。

**TE09.04.02：**それぞれの自己テストがエラーをどのように扱うかを規定したベンダが提供する文書を検査することによって、試験者は次を検証しなければならない：
1.暗号モジュールは、自己テストを失敗したときにエラー状態になる。
2.エラー状態は、文書及び有限状態モデルに一致する。
3.暗号モジュールは、エラーインジケータを出力する。
4.エラーインジケータは、文書化されたエラーインジケータと一致する。

**TE09.04.03：**試験者は、自己テストを実行して、暗号モジュールをそれぞれのエラー状態にしなければならない。試験者は、観察したエラーインジケータをベンダが提供する文書に規定されたインジケータと比較しなければならない。一致しない場合には、このアサーションは不合格とする。

**AS09.05：(レベル 1，2，3，及び 4)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。**

**VE09.05.01:**ベンダの設計要求事項に関しては VE02.06.01 を参照のこと。ベンダの設計は、暗号モジュールがエラー状態の間は暗号動作を実行できないことを確実にしなければならない。

**TE09.05.01：**試験者による出力の抑止の検証は、TE02.06.01 及び TE02.06.02 において行われる。検証の結果は、暗号モジュールがエラー状態にあるときに、暗号モジュールが全てのデータ出力を抑止することを示さなければならない。

**TE09.05.02：**試験者は、ベンダが提供する文書が、暗号モジュールがエラー状態の間、暗号機能が抑止されていることを規定していることを検証しなければならない。暗号機能は、次の内容を含む：

1. 暗号化
2. 復号
3. セキュアメッセージのハッシュ化
4. デジタル署名の生成及び検証
5. 暗号の使用を必要とするその他の操作

**TE09.05.03：**試験者は、暗号モジュールをエラー状態にして、試験者が開始しようと試みたいかなる暗号操作も阻止されることを検証しなければならない。

**AS09.06：(レベル1, 2, 3，及び4)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。**

**VE09.06.01:**ベンダの設計要求事項に関しては VE02.06.01 を参照のこと。ベンダの設計は、データ出力インタフェースを通る全てのデータ出力は抑止されることを確実にしなければならない。

**TE09.06.01:**試験者による出力の抑止の検証は、TE02.06.01 及び TE02.06.02 で行われる。試験者の検証の結果は、ベンダが提供する文書が、暗号モジュールがエラー状態にある限りデータ出力インタフェースを通る全てのデータ出力が抑止されることを説明していることを示さなければならない。

**TE09.06.02：**試験者は、暗号モジュールをエラー状態にして、エラー状態のときにはデータ出力インタフェースを通る全てのデータ出力が抑止されることを検証しなければならない。

**AS09.07：(レベル 1，2，3，及び 4)文書は、次を規定しなければならない：**

- **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**
- **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。）**

**VE09.07.01：**ベンダは、暗号モジュールが実行できる全ての自己テストのリストを提供しなければならない。このリストは、パワーアップ自己テスト及び条件自己テストの両方を含まなければならない。

**VE09.07.02：**それぞれのエラー条件に対して、ベンダが提供する文書は、その条件名、その条件を発生することができるイベント群、及びその条件をクリアして、通常動作を再開

するために必要なアクションを提供しなければならない。

**TE09.07.01：**自己テストのリストに次の記述があることを検証するために、試験者はリストを検査しなければならない。

1. パワーアップ自己テスト
   - 暗号アルゴリズムテスト
   - 乱数生成器テスト
   - ソフトウエア/ファームウエアテスト
   - 重要機能テスト
   - 電源投入時及びオンデマンド実行されるその他の自己テスト
2. 条件自己テスト
   - 鍵ペア整合性テスト(暗号モジュールが公開鍵及びプライベート鍵を生成する場合)
   - 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
   - バイパステスト
   - その他の条件自己テスト

**TE09.07.02：**試験者は、上記の情報が、それぞれのエラー条件に対して規定されていることをチェックしなければならない。

**TE09.07.03：**試験者は、それぞれのエラー条件を発生させて、エラー条件をクリアするよう試みなければならない。試験者は、エラー条件をクリアするために必要なアクションが、ベンダが提供する文書と一致することを検証しなければならない。試験者がそれぞれのエラー条件を発生させることができない場合には、試験者はそれぞれのエラー条件をクリアするために必要なアクションがベンダが提供する文書内の記述と一致するかどうかを判断するために、ソースコード及び/又は設計文書をレビューしなければならない。

## 9.1 パワーアップ自己テスト

[解説]

原文では、「パワーアップテスト」と「パワーアップ自己テスト」の2つの用語が使用されている。パワーアップテストは、自動的に開始、オペレータ介在不可(AS09.09)と定義している一方で、オンデマンドで試験可能(AS09.12)とされている。パワーアップ自己テストも、VE09.12.01, TE09.12.01でオンデマンドで行うことが示されている。このため、パワーアップテストとパワーアップ自己テストとの違いはない(単なる語句の不統一)と考え、用語を「パワーアップ自己テスト」に統一した。

### 一 般

**AS09.08：(レベル 1, 2, 3, 及び 4)パワーアップ自己テストは、暗号モジュールが(電源 OFF、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。**

注：このアサーションは、AS09.09の一部として試験される。

**AS09.09：(レベル 1，2，3，及び 4)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。**

**VE09.09.01：**ベンダが提供する文書は、パワーアップ自己テストの実行は、オペレータからのいかなる入力、又はオペレータによるいかなるアクションも伴わないことを要求しなければならない。

**TE09.09.01：**試験者は、ベンダが提供する文書が VE09.09.01 において必要とされる情報を含むことを検証しなければならない。

**TE09.09.02：**試験者は、暗号モジュールを電源投入して、その暗号モジュールがオペレータのいかなる介在も要求せずにパワーアップ自己テストを実行することを検証しなければならない。

**AS09.10：(レベル 1，2，3，及び 4)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。**

[解説]

本ASのVE,TEは自己テストの成功時の記述のみであるが、自己テストの失敗時については、(パワーアップ自己テストを含む)AS09.04で規定されている。

**VE09.10.01：**ベンダは、パワーアップ自己テストの成功完了時に、暗号モジュールが出力するインジケータを文書化しなければならない。

**TE09.10.01：**試験者は、ベンダが提供する文書が、パワーアップ自己テストの成功完了時に状態出力インタフェースから出力されるインジケータを規定していることを検証しなければならない。

**TE09.10.02：**試験者は、暗号モジュールを電源投入して、状態出力インタフェースを監視しなければならない。状態出力インタフェースからの期待されるインジケータは、文書化されたインジケータと一致しなければならない。

**AS09.11：(レベル 1，2，3，及び 4)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。**

注：このアサーションは、AS02.06の一部として試験される。

**AS09.12：(レベル 1，2，3，及び 4)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。**

**VE09.12.01：**ベンダは、オペレータがオンデマンドでパワーアップ自己テストを開始できる手順を記述しなければならない。パワーアップ自己テストの全てが含まれていなければならない。

**TE09.12.01：**試験者は、全てのパワーアップ自己テストに対して、オンデマンドのパワーアップ自己テストの開始が規定されていることを検証するために、ベンダが提供する文書

を検査しなければならない。

**TE09.12.02：**試験者は、オンデマンドのパワーアップ自己テストの開始がベンダが提供する文書と一致することを検証するために、オンデマンドのパワーアップ自己テストを開始しなければならない。

**AS09.13：(レベル 1，2，3，及び 4)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**

**VE09.13.01：**ベンダへの要求事項に関しては、VE09.07.01 を参照のこと。

**TE09.13.01：**パワーアップ自己テストに関する文書化されたリストの検証は、TE09.07.01 のもとで行われる。

**TE09.13.02：**暗号モジュールが文書化された内容のように自己テストを実行することの検証は、AS09.16-AS09.28 における検証要求事項のもとで行われる。

**AS09.14：**
注：このアサーション番号に関する要求事項は無い。

**AS09.15：**
注：このアサーション番号に関する要求事項は無い。

**暗号アルゴリズムテスト**

**AS09.16：(レベル 1，2，3，及び 4)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。**

**VE09.16.01：**ベンダへの要求事項に関しては、VE09.07.01 参照のこと。

**TE09.16.01：**ベンダが提供する文書を検査することによって、試験者は、既知解テストが AS01.12 で示されるような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の全てと関係していることを検証しなければならない。

**TE09.16.02：**試験者は、ベンダが提供する文書が、暗号モジュールの実装と一致していることを検証しなければならない。

**AS09.17：(レベル 1，2，3，及び 4)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。**

**VE09.17.01：**ベンダが提供する文書は、計算された出力と既知解とを比較するために用いる方法を規定しなければならない。

**VE09.17.02：**ベンダが提供する文書は、2 つの出力が等しくないときの、エラー状態への遷移、及びエラーインジケータの出力を示さなければならない。

**TE09.17.01：**試験者は、ベンダが提供する文書が暗号モジュールの実装と一致していることを検証しなければならない。

**TE09.17.02：**これは TE09.04.01、TE09.04.02、及び TE09.04.03 のもとで試験される。

**AS09.18：(レベル 1，2，3，及び 4)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。**

**VE09.18.01：**ベンダへの要求事項に関しては、VE09.07.01 参照のこと。

**VE09.18.02：**ベンダが提供する文書は、実装されている(一つ又は複数の)テストについて規定及び記述しなければならない。

**TE09.18.01：**試験者は、ベンダが提供する文書と暗号モジュールの実装とが一致していることを検証しなければならない。

**TE09.18.02：**ベンダが提供する文書を検査することによって、試験者は、既知解テスト又は鍵ペア整合性テストのいずれが暗号機能と関係しているかを検証しなければならない。

**TE09.18.03：**鍵ペア整合性は、AS09.31(暗号化)、AS09.32(鍵共有)及び AS09.33(デジタル署名生成及び検証)で試験される。

**AS09.19：(レベル 1，2，3，及び 4)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。**

[解説]

デジタル署名標準（Digital Signature Standard）は、FIPS186-2のことである。

**VE09.19.01：**ベンダへの要求事項に関しては、VE09.07.01 参照のこと。

**VE09.19.02：**ベンダが提供する文書は、実装されている(一つ又は複数の)テストについて規定及び記述しなければならない。

**TE09.19.01：**試験者は、ベンダが提供する文書と暗号モジュールの実装とが一致していることを検証しなければならない。

**TE09.19.02：**試験者は、暗号モジュールがメッセージダイジェストアルゴリズムを実装しているかどうかを判定しなければならない。メッセージダイジェストアルゴリズムが実装されている場合には、試験者は、ベンダが提供する文書が、メッセージダイジェストアルゴリズムが独自の既知解テストをもっているかどうか、又は他のアルゴリズムの既知解テストにその既知解テストが含まれているかどうかを規定していることを検証しなければならない。

**TE09.19.03：**ソースコード及び/又は設計書をチェックすることによって、試験者は、暗号モジュールがメッセージダイジェストアルゴリズムをテストするために、単独の既知解テスト、又はアルゴリズムの既知解テストのいずれかを用いていることを検証しなければならない。

**AS09.20：(レベル 1，2，3，及び 4)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、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。**

**VE09.20.01：**ベンダへの要求事項に関しては、VE09.07.01 参照のこと。

**VE09.20.02：**ベンダは、既知解テスト又は 2 つの独立した暗号アルゴリズムの実装の出力の比較(比較解テスト)が、暗号モジュールの暗号アルゴリズムをテストするために用いられているかどうかを規定しなければならない。比較解テストが用いられる場合には、ベンダはその事実を文書化しなければならない。

**TE09.20.01：**試験者は、ベンダが提供する文書から、既知解テスト又は比較解テストが暗号モジュールの暗号アルゴリズムをテストするために用いられているかどうかを判定しなければならない。比較解テストが使用される場合には、試験者は、比較解テストに関する文書が次を含んでいるかどうかを判定しなければならない：

1. 2 つの独立した暗号アルゴリズム実装の利用
2. 暗号アルゴリズム実装の出力の連続的な比較
3. 2つの出力が等しくないときの、エラー状態への遷移及びエラーインジケータの出力

**TE09.20.02：**ソースコード及び/又は設計書をチェックすることによって、試験者は、暗号モジュールが比較解テストを実行するための文書化された手順を実装していることを検証しなければならない。

**TE09.20.03：**自己テスト失敗時に、暗号モジュールがエラー状態になって、エラーインジケータを出力するかどうかの検証は、TE09.04.01、TE09.04.02、及び TE09.04.03 のもとで行われる。これらの試験の内、どれか 1 つでも不合格の場合には、このアサーションは不合格とする。

**AS09.21：(レベル 1，2，3，及び 4)暗号モジュールが暗号アルゴリズムの２つの独立した実装を含む場合には、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。**

注：このアサーションは、AS09.20の一部として試験される。

## ソフトウエア/ファームウエア完全性テスト

**AS09.22:(レベル 1，2，3，及び 4)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。**

**VE09.22.01:**ベンダが提供する文書は、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)が、全てのソフトウエア及びファームウエアコンポーネントに対する完全性テストとして実装されているかどうかを規定しなければならない。

**VE09.22.02：**ベンダが提供する文書は、実装されている完全性メカニズムを記述しなければならない。

**VE09.22.03：**暗号モジュールが、承認された認証技術を実装している場合には、
(1) ベンダは、VE01.12.01で規定されたような認定証を提供しなければならない。
(2) 又は、CMVPアルゴリズム認定証を発行する手順がない際には、ベンダの組織は、暗号モジュールに実装された認証技術が承認されていることを主張する確約書を提供しなければならない。

**TE09.22.01：**試験者は、ベンダが提供する文書から、どの技術がソフトウエア/ファームウエアコンポーネント完全性テストに使用されているかを判定しなければならない。

**TE09.22.02：**試験者は、承認された認証技術が実装されている場合には、ベンダが提供する文書が TE01.12.01 の要求事項を含むか、又は CMVP アルゴリズム認定証を発行する手順がない際にはベンダの組織が適合の確約書を提供するかのいずれかであることを検証しなければならない。

**TE09.22.03：**暗号モジュールがソフトウエア/ファームウエアの完全性のために EDC を実装している場合には、試験者は、ソフトウエア/ファームウエア完全性テストに関するベンダが提供する文書が次を含んでいることを検証しなければならない。：
1.EDC アルゴリズムの記述。
2.EDC を用いて保護されているソフトウエア及びファームウエアの識別。
3.ソフトウエア及びファームウエアが設置される時の EDC 計算。
4.自己テストが開始されるときの EDC の再計算。
5.再計算された EDC に対する格納された EDC との比較。
6．2つのEDCが等しくないときの自己テストの失敗。

**TE09.22.04：**暗号モジュールが、ソフトウエア/ファームウエアの完全性のために MAC を実装している場合には、試験者は、ソフトウエア/ファームウエア完全性テストに関するベンダが提供する文書に､MAC が計算され及び検証されるプロセスが完全に記述されていることを検証しなければならない。

**TE09.22.05：**暗号モジュールが、ソフトウエア/ファームウエアの完全性のために承認されたデジタル署名を実装している場合には、試験者は、ソフトウエア/ファームウエア完全性テストに関するベンダが提供する文書が次を含むことを検証しなければならない：
1．実装されている承認されたデジタル署名アルゴリズムの規定。
2．承認されたデジタル署名を用いて保護されているソフトウエア及びファームウエアの識別。
3．ソフトウエア及びファームウエアが設置されるときの承認されたデジタル署名の計算。
4．自己テストが開始されるときの承認されたデジタル署名の検証。
5．承認されたデジタル署名の検証の失敗による自己テストの失敗。

**TE09.22.06：**ソースコード及び/又は設計書をチェックすることにより、試験者は、ソフトウエア/ファームウエア完全性テストの実装が TE09.22.02、TE09.22.03、TE09.22.04 又は TE09.22.05 と一致していることを検証しなければならない。

**TE09.22.07：**可能な場合には、試験者は、格納されたソフトウエア、ファームウエア、又は実装された完全性メカニズムを変更し、及び自己テストを開始し、並びに状態出力インタフェースからの出力を観察することによって、暗号モジュールを試験しなければならない。どのインジケータもソフトウエア/ファームウエア自己テストが失敗したことを示す出力がない場合には、このアサーションは不合格とする。
[解説]

ソフトウエア/ファームウエア自己テスト(software/firmware self-test)は、ソフトウエア/ファームウエア完全性テスト(software/firmware integrity test)を指していると思われる。

**AS09.23：(レベル 1，2，3，及び 4)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。**
注：このアサーションは AS09.22 の一部として試験される。

**AS09.24：(レベル 1，2 ,3，及び 4)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。**

**VE09.24.01：**暗号モジュールが、ソフトウエア/ファームウエアの完全性のために、EDC を実装する場合には、ベンダが提供する文書は EDC が少なくとも 16 ビット長であることを示さなければならない。

**TE09.24.01：**試験者は、実装された EDC が少なくとも 16 ビット長であることを検証しなければならない。

## 重要機能テスト

**AS09.25：(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。**
注：このアサーションは、AS09.27 の一部として試験される。

**AS09.26：(レベル 1，2，3，及び 4)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。**
注：このアサーションは、AS09.27の一部として試験される。
[解説]
条件自己テスト(conditional tests)の定義は、FIPS140-2，4.9.2節参照。

**AS09.27：(レベル 1，2，3，及び 4)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。**
注：重要機能は、誤動作時に CSP の開示を引き起こす可能性のある機能として定義される。重要機能の例として、乱数生成、暗号アルゴリズムの動作、及び暗号化のバイパスがあげられるが、これらに限るものではない。
[解説]
パワーアップ自己テストの定義は、FIPS140-2，4.9.1 節参照。
条件自己テストの定義は、FIPS140-2，4.9.2 節参照。

**VE09.27.01：**ベンダは全ての重要機能に関する文書を提供しなければならない。それぞれの重要機能に対して、ベンダは次を示さなければならない。
1. 重要機能の目的。
2. どの重要機能がどのパワーアップ自己テストによって試験されるか。
3. どの重要機能がどの条件自己テストによって試験されるか。

**TE09.27.01：**試験者は、重要機能及びそれらを試験するために設計された自己テストに関するベンダが提供する文書をレビューしなければならない。このベンダが提供する文書は、次を含まなければならない。

1. 全ての重要機能の識別及び記述。
2. 重要機能ごとの、少なくとも 1 つの自己テストの識別。

**TE09.27.02：**ソースコード及び/又は設計文書をチェックすることによって、試験者は、暗号モジュールがそれぞれの重要機能に対して特定の自己テストを実行することを検証しなければならない。

**AS09.28：**
注：このアサーション番号に対する要求事項はない。

## 9.2 条件自己テスト

[解説]
原文では、「条件自己テスト」と「条件テスト」の 2 つの用語が使用されている。各テストが実行される条件について、条件自己テストは AS09.03 で定義され、条件テストは AS09.29 で定義されている。しかし、両 AS の記載は、同一内容であり、条件テストと条件自己テストとの違いはない(単なる語句の不統一)と考え、用語を「条件自己テスト」に統一した。

**AS09.29：(レベル 1，2，3，及び 4)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。**
注：このアサーションは個別には試験されない。

**(公開鍵及びプライベート鍵に対する)鍵ペア整合性テスト**

**AS09.30：(レベル1，2，3，及び4)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。**
注：このアサーションは、AS09.31及びAS09.33の一部として試験される。

**AS09.31：(レベル1，2，3，及び4)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。**

**VE09.31.01：**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、暗号モジュールは、公開鍵を平文の値に適用することによって、鍵ペア整合性をテストしなければならない。その結果の暗号文は、元の平文と異なることを検証するために、元の平文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、暗号モジュールはエラー状態になり、かつ、状態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。
- 2つの値が異なる場合には、プライベート鍵は暗号文に適用され、かつ、その結果は元の平文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。

**TE09.31.01：**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、試験者は、AS09.31で定義されたような鍵ペア整合性テストの実装が、ソースコード及び/又は設計文書のチェックによって、ベンダが提供する文書の記述と一致していることを検証しなければならない。

**AS09.32：**
注：このアサーション番号に対する要求事項はない。

**AS09.33：(レベル1，2，3，及び4)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。**

**VE09.33.01：**公開鍵及びプライベート鍵がデジタル署名の計算及び/又は検証にだけ用いられる場合には、暗号モジュールは、署名の計算及び検証によって鍵ペア整合性をテストしなければならない。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。

**TE09.33.01：**公開鍵及びプライベート鍵がデジタル署名の計算及び/又は検証に用いられる場合には、試験者は、AS09.33で定義されているような鍵ペア整合性テストの実装が、ソースコード及び/又は設計文書をチェックすることによって、ベンダが提供する文書の記述と一致していることを検証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

**AS09.34：(レベル 1，2，3，及び 4)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。**
注：このアサーションはAS09.34、AS09.35、及びAS09.36の一部として試験される。

**AS09.35：(レベル 1，2，3，及び 4)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。**

**VE09.35.01：**ベンダが提供する文書は、外部からロードされる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の完全性を保護するために用いられる承認された認証技術を記述しなければならない。

**VE09.35.02：**暗号モジュールが承認された認証技術を実装する場合には、
(1)ベンダはVE01.12.01で規定されたような認定証を提供しなければならない。
(2)又は、CMVPアルゴリズム認定証を発行する手順がない際には、ベンダの組織は暗号モジュールに実装された認証技術が承認されていることを主張する確約書を提供しなければならない。

**TE09.35.01：**試験者は、ベンダが提供する文書から、どの承認された認証技術がソフトウエア/ファームウエアロードテストに用いられているかを判定しなければならない。

**TE09.35.02：**試験者は、承認された認証技術が実装されている場合には、ベンダが提供する文書がTE01.12.01の要求事項を含むか、又はCMVPアルゴリズム認定証を発行する手順がない際にはベンダの組織が適合の確約書を提供するかのいずれかであることを検証しなければならない。

**TE09.35.03：**暗号モジュールがソフトウエア/ファームウエアロードテスト用に承認された認証技術を実装している場合には、試験者は、ソフトウエア/ファームウエアロードテストに関するベンダが提供する文書には次のものが含まれていることを検証しなければならない。

1. 実装されている承認された認証技術の規定。
2. 承認された認証技術を用いて保護されているソフトウエア及びファームウエアの識別。
3. ソフトウエア及びファームウエアがロードされるときの、承認された認証技術の計算。
4. ソフトウエア/ファームウエアロードテストが開始されたときの、承認された認証技術の検証。
5. 承認された認証技術の検証の失敗による自己テストの失敗。

**TE09.35.04：**ソースコード及び/又は設計文書をチェックすることによって、試験者は、ソフトウエア/ファームウエアロードテストの実装が TE09.35.01、TE09.35.02、及び TE09.35.03 と一致していることを検証しなければならない。

**TE09.35.05：**可能な場合には、試験者は、ロードされたソフトウエア若しくはファームウエア、又は実装された認証メカニズムを変更し、及び自己テストを開始し、並びに状態出力インタフェースからの出力を観察することによって、暗号モジュールを試験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が失敗したことを示す出力のインジケータがない場合には、このアサーションは不合格とする。

**AS09.36：(レベル 1，2，3，及び 4)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。**
注：このアサーションはAS09.35の一部として試験される。

## 手動鍵入力テスト

**AS09.37：(レベル 1，2，3，及び 4)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。**
注：このアサーションは、個別には試験されない。

**AS09.38：(レベル 1，2，3，及び 4)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。**
注：このアサーションは AS09.40 の一部として試験される。

**AS09.39：(レベル 1，2，3，及び 4)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：このアサーションは AS09.40 の一部として試験される。

**AS09.40：(レベル 1，2，3，及び 4)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。**

**VE09.40.01：**ベンダは手動鍵入力テストを文書化しなければならない。エラー検出コード又は繰り返し鍵入力が用いられているかどうかによって、手動鍵入力テストは次を含まなければならない。

1. エラー検出コード(EDCs)
   －EDC 計算アルゴリズムの記述
   －検証手順の記述
   －テストの成功又は失敗に対して期待される出力
2. 繰り返し鍵入力
   －検証手順の記述
   －テストの成功又は失敗に対して期待される出力

**VE09.40.02：**EDC が鍵に関係している場合には、暗号鍵のフォーマットを記述するベンダが提供する文書(AS07.03 を参照)は､エラー検出コード用のフィールドを含んでいなければならない。

**TE09.40.01：**ベンダが提供する文書の検証は、TE07.28.01のもとで行われる。

**TE09.40.02：**試験者は、ベンダが提供する文書から、手動鍵入力テストにどの方法(エラー検出コード又は繰り返し鍵入力)が用いられるかを判定しなければならない。試験者は、次の情報が含まれているかどうかを判定するために、用いられる方法に基づいて、ベンダが提供する文書、ソースコード、及び/又は手動鍵入力テストの実装を規定している設計文書をチェックしなければならない。

１．エラー検出コード
   －EDC用のフィールド(AS07.03を参照)を含む全ての手動で入力される鍵の鍵フォーマット
   －EDC アルゴリズムの記述

－EDC 検証手順の記述
－テストの成功又は失敗に対する期待される出力の全て

２．繰り返し鍵入力
－手動で入力された鍵の全てに対する繰り返し鍵入力
－繰り返し鍵、入力検証手順の記述
－テストの成功又は失敗に対する期待される出力の全て

**TE09.40.03：**EDC を用いた手動鍵入力テストに関して、試験者は次の試験を実行しなければならない。

1. 試験者は手動で入力される鍵の全てを入力して、入力されるときの鍵の形式を含め、それぞれの鍵を入力するために用いられる手順が文書化された手順に基づいていることを検証しなければならない。
2. 試験者はエラーを起こすことなく手動で入力される鍵のタイプのそれぞれを入力して、状態出力インタフェースを観察しなければならない。どのインジケータも検出されない場合、又は手動鍵入力テストの成功に対して文書が示すあるべきインジケータの姿と実際のインジケータが一致しない場合には、その試験は不合格とされる。
3. 試験者は、鍵が正しく入力されたことを検証するために、入力した鍵のそれぞれを用いて暗号操作を行うことを試みなければならない。
4. 試験者は、手動で入力された鍵のそれぞれと関係する EDC、又は鍵自身のいずれかを変更して、暗号モジュール内にそれらを入力しなければならない。試験者は状態出力インタフェースから出力されているインジケータを観察しなければならない。どの出力も検出されない場合、又は手動鍵入力テストの失敗に対して文書が示すあるべきインジケータの姿と実際のインジケータが一致しない場合には、その試験は不合格とされる。
5. 試験者は、入力に成功しなかった鍵のそれぞれを用いて暗号操作を行うことを試みなければならない。鍵が入力されなかったことを検証するために、それぞれの鍵を用いるそれぞれの操作は失敗しなければならない。

**TE09.40.04：**繰り返し鍵を用いた手動鍵入力テストに関して、試験者は次の試験を行わなければならない。

1. 試験者はエラーを起こすことなく手動で入力される鍵のタイプのそれぞれを入力して、状態出力インタフェースを観察しなければならない。どのインジケータも検出されない場合、又は手動鍵入力テストの成功に対して文書が示すあるべきインジケータの姿と実際のインジケータが一致しない場合には、その試験は不合格とされる。
2. 試験者は、鍵が正しく入力されたことを検証するために、入力した鍵のそれぞれを用いて暗号操作を行うことを試みなければならない。
3. 試験者は、手動で入力された鍵(1 番目又は 2 番目の繰り返し鍵のいずれか)の 1 つを正確な値から変更して、暗号モジュール内にそれらを入力しなければならない。試験者は状態出力インタフェースから出力されているインジケータを観察しなければならない。どの出力も検出されない場合、又は手動鍵入力テストの失敗に対して文書が示すあるべきインジケータの姿と実際のインジケータが一致しない場合には、その試験は不合格とされる。
4. 試験者は、入力に成功しなかった鍵のそれぞれを用いて暗号操作を行うことを試みなければならない。鍵が入力されなかったことを検証するために、それぞれの鍵を用いるそれぞれの操作は失敗しなければならない。

### 連続乱数生成器テスト

**AS09.41：(レベル 1，2，3，及び 4)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。**
注：このアサーションは AS09.42 及び AS09.43 の一部として試験される。

**AS09.42：(レベル 1，2，3，及び 4)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。**

**VE09.42.01：**暗号モジュールが乱数生成器を実装している場合には、ベンダは連続乱数生成器テストについて文書化しなければならない。

**TE09.42.01：**試験者は暗号モジュールが乱数生成器を実装しているかどうかを判定しなければならない。暗号モジュールが乱数生成器を実装している場合には、試験者は、テストの仕様を実装していることを検証するために、連続乱数生成器テストを規定している文書、ソースコード、及び/又は設計文書をチェックしなければならない。乱数生成器が n ビット(n>15)のブロックを生成する場合には、試験者はテストの実装が次を含んでいることを検証しなければならない。

1. 次のブロックに対する比較のために最初のブロックを格納すること。
2. 続いて生成されるブロックのそれぞれを、前に生成されたブロックと比較すること。
3. 2 つの比較したブロックが等しい場合には、そのテストを失敗とすること。

乱数生成器が連続的に 16 ビット未満のビット列を生成する場合には、試験者はそのテストの実装が次を含んでいることを検証しなければならない。

1. 次に生成される n ビットに対して比較するために、最初の n ビット(n>15)を格納すること。
2. 続いて生成される n ビットのそれぞれを、前に生成された n ビットと比較すること。
3. 2 つの比較した n ビット列が等しい場合には、このテストを失敗とすること。

**AS09.43：(レベル 1，2，3，及び 4)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。**

**VE09.43.01：**暗号モジュールが乱数生成器を実装する場合には、ベンダは連続乱数生成器テストについて文書化しなければならない。

**TE09.43.01：**試験者は暗号モジュールが乱数生成器を実装しているかどうかを判定しなければならない。暗号モジュールが乱数生成器を実装している場合には、試験者は、テストの仕様を実装していることを検証するために、連続乱数生成器テストを規定している文書、ソースコード、及び/又は設計文書をチェックしなければならない。乱数生成器が n ビット（n>15）のブロックを生成する場合には、試験者はテストの実装が次を含んでいることを検証しなければならない。

1. 次のブロックに対する比較のために最初のブロックを格納すること。
2. 続いて生成されるブロックのそれぞれを、前に生成されたブロックと比較するこ

と。
3. 2つの比較したブロックが等しい場合には、そのテストを失敗とすること。
乱数生成器が連続的に16ビット未満のビット列を生成する場合には、試験者はそのテストの実装が次を含んでいることを検証しなければならない。
1. 次に生成されるnビットに対して比較するために、最初のnビット(n>15)を格納すること。
2. 続いて生成されたnビットのそれぞれを、前に生成されたnビットと比較すること。
3. 2つの比較したnビット列が等しい場合には、このテストを失敗とすること。
[解説]
本TEの記載内容は、TE09.42.01と同じであるが、適用される試験は異なる。

## バイパステスト

**AS09.44：(レベル1, 2, 3, 及び4)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。**
注：このアサーションは個別に試験されない。

**AS09.45：(レベル1, 2, 3, 及び4)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。**

**VE09.45.01：**暗号モジュールがバイパスサービスを実装している場合には、ベンダは、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、暗号サービスの正しい動作を検証するために、バイパステストを実装しなければならない。

**VE09.45.02：**ベンダは、AS09.48 で定義されているように、テストの記述を提供しなければならない。バイパステストは、排他的な暗号サービスに切替わるとき、暗号モジュールが AS09.47 で定義されているように平文の情報を出力しないことを実証しなければならない。暗号モジュールが平文の情報を出力する場合には、このテストは失敗とする。

**TE09.45.01：**試験者は、暗号モジュールが、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、暗号サービスの正しい動作を検証するために、バイパステストを実装していることを検証しなければならない。

**TE09.45.02：**試験者は、ベンダが提供する文書が、ソースコード及び/又は設計文書のレビューを通して、バイパステストの実装と一致していることを検証しなければならない。

**TE09.45.03：**試験者は暗号モジュールを排他的なバイパスサービスから排他的な暗号サービスに切替えて、平文の情報が出力されないことを検証しなければならない。

**AS09.46：(レベル1, 2, 3, 及び4)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。**

**VE09.46.01：**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ように設計されている場合には、ベンダは、切替え手順を管理するメカニズムが変更される際、暗号サービスの正しい動作を検証するために、バイパステストを実装しなければならない。

**VE09.46.02：**ベンダは、AS09.48で定義されているように、テストの記述を提供しなければならない。バイパステストは、切替え手順を管理するメカニズムが変更される際、次のことを実証しなければならない。

1. そのメカニズムは、最後の変更から変更されていないことが検証されること。そのメカニズムが変更された場合には、暗号モジュールはエラー状態になり、かつ、状態インタフェースにエラーインジケータを出力しなければならない。
2. 暗号サービスの正しい動作が、暗号モジュールが、AS09.47で定義されているように、平文の情報を出力しないことを実証することによって検証されること。暗号モジュールが平文の情報を出力する場合には、そのテストは失敗とする。

**TE09.46.01：**試験者は、暗号モジュールが、切替え手順を管理するメカニズムが変更される際、暗号サービスの正しい動作を検証するために、バイパステストを実装していることを検証しなければならない。

**TE09.46.02：**試験者は、ベンダが提供する文書が、ソースコード及び/又は設計文書のレビューを通して、バイパステストの実装と一致していることを検証しなければならない。

**TE09.46.03：**試験者は、次を行うことによって、バイパステストの正しい動作を検証しなければならない。

1. 切替え手順を管理するメカニズムが、メカニズムの変更が最後の変更から発生していないことを確実にするために、チェックしていることを検証すること。試験者は、用いられる方法について文書化すること。設計が許容する場合には、試験者は、用いられる方法を試験するためにメカニズムを変更しなければならない。
2. メカニズムの正しい動作を検証し、かつ、平文の情報が出力されないことを検証することによって暗号サービスの正しい動作を検証するために、切替え手順を管理するメカニズムを変更すること。

**AS09.47：(レベル1, 2, 3，及び4)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ってはならない。**

注：このアサーションはAS09.45及びAS09.46の一部として試験される。

[解説]

本内容は、AS09.44の一部を、一般論として引き出した内容である。従って、本文章はFIPS140-2内にはない。

**AS09.48：(レベル1, 2, 3，及び4)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。**

注：このアサーションはAS09.45とAS09.46の一部として試験される。

# 10．設計保証

## 10.1 構成管理

**AS10.01：(レベル 1，2，3，及び 4)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。**

**VE10.01.01：**ベンダが提供する文書は、暗号モジュール、暗号モジュールコンポーネント、及び関係した暗号モジュールの文書に対する構成管理(CM)システムを記述しなければならない。

**TE10.01.01：**試験者は、構成管理(CM)システムが実施されていることを検証するために、ベンダが提供する文書をレビューしなければならない。

**AS10.02：(レベル 1，2，3，及び 4)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。**

**VE10.02.01：**ベンダの構成管理(CM)文書は、全ての構成要素の構成リストを含まなければならない。構成管理(CM)文書は、構成要素を一意に識別するために用いられる方法を記述しなければならない。

**VE10.02.02：**ベンダが提供する文書は、認証されるそれぞれの構成要素のバージョンを一意に識別するために用いられる方法を記述しなければならない。

**TE10.02.01：**試験者は、構成要素が含まれていることを検証するために、ベンダが提供する構成リストをレビューしなければならない。

**TE10.02.02：**試験者は、構成管理(CM)文書が全ての構成要素を一意に識別するために用いられる方法を規定していることを検証しなければならない。

**TE10.02.03：**試験者は、認証される構成要素のそれぞれのバージョンを一意に識別するために用いられる方法の記述を含むことを検証するために、ベンダが提供する構成管理(CM)文書をレビューしなければならない。

**TE10.02.04：**試験者は、構成管理(CM)文書が、認証されるそれぞれの構成要素のバージョンを一意に識別することを検証しなければならない。

## 10.2 配付及び運用

**AS10.03：(レベル 1，2，3，及び 4)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。**

**VE10.03.01：**ベンダが提供する文書は、暗号モジュールのセキュアな設置、初期化、及び立上げに必要なステップを記述しなければならない。

**TE10.03.01：**試験者は、セキュアな構成となる設置、初期化、及び立上げ手順を含むことを検証するために、ベンダが提供する文書をレビューしなければならない。

**TE10.03.02：**試験者は、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実行して、それらが正しいことを検証しなければならない。

**AS10.04：(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、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。**

[解説]

「セキュリティレベル1の要求事項」は、AS10.03を指す。

ここでいうバージョンとは、バージョン番号のことではなく、あるバージョンの暗号モジュールの構成全体を指す。

**VE10.04.01：**配付に関する文書は、許可されたオペレータに対して暗号モジュールを配送するときに、セキュリティを維持するために必要な手順を記述しなければならない。

**TE10.04.01：**試験者は、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する間、セキュリティを維持するために必要な手順が正しいことを検証するために、ベンダが提供する文書をレビューしなければならない。

## 10.3 開発

**AS10.05：(レベル 1，2，3，及び 4)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。**

注：このアサーションは AS10.06 及び AS10.07 の一部として試験される。

[解説]

「次の要求事項」は、AS10.06～AS10.08を指す。

**AS10.06：(レベル 1, 2, 3，及び 4)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。**

**VE10.06.01：**ベンダが提供する文書は、ハードウエア設計、ソフトウエア設計、及びファームウエア設計が暗号モジュールのセキュリティポリシ(動作のルール)とどのように対応しているかを記述しなければならない。

**TE10.06.01：**試験者は、暗号モジュールのセキュリティポリシ(動作のルール)が正しいことを検証するために、ベンダが提供する文書をレビューしなければならない。試験者は、それぞれのセキュリティルールが設計に反映され、かつ、その設計がそのルールを実装していることを検証しなければならない。

**AS10.07：(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、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。**

**VE10.07.01：**ベンダは、暗号モジュールに含まれる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の名称のリストを提供しなければならない。

**VE10.07.02：**ベンダは、暗号モジュールに含まれるそれぞれ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注釈のついたソースコードを提供しなければならない。

**TE10.07.01：**試験者は、それぞれ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のソースコードが暗号モジュールに含まれることを検証するために、ベンダによって提供されるリストを用いなければならない。

**AS10.08：(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、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。**

**VE10.08.01：**ベンダは、暗号モジュールに含まれるハードウエアコンポーネントのリストを提供しなければならない。

**TE10.08.01：**試験者は、文書が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)のソースコードを含むことを検証するために、ベンダによって提供されるリストを用いなければならない。

**AS10.09：(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、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。**
注：このアサーションは AS10.10 の一部として試験される。
[解説]
「セキュリティレベル1の要求事項」は、AS10.06～AS10.08を指す。
「次の要求事項」は、AS10.10を指す。

**AS10.10：(レベル 2, 3，及び 4)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機能仕様を規定しなければならない。**

**VE10.10.01：**ベンダが提供する機能仕様は、暗号モジュール、並びにそれぞれの外部インタフェース及び外部ポートを記述しなければならない。

**VE10.10.02：**ベンダが提供する機能仕様は、それぞれの外部インタフェースの目的を記述しなければならない。

**TE10.10.01：**試験者は、VE10.10.01で規定された情報が含まれることを検証するために、ベンダが提供する機能仕様をレビューしなければならない。この情報が含まれない場合には、このアサーションは不合格とする。

**TE10.10.02：**試験者は、VE10.10.02で規定された情報が含まれることを検証するために、ベンダが提供する機能仕様をレビューしなければならない。この情報が含まれない場合には、このアサーションは不合格とする。

**AS10.11：(レベル 3 及び 4)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。**
注：このアサーションは AS10.12 及び AS10.13 の一部として試験される。
[解説]
「セキュリティレベル1及び2の要求事項」は、AS10.06～AS10.08、AS10.10を指す。
「次の要求事項」は、AS10.12、AS10.13を指す。

**AS10.12：(レベル 3 及び 4)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。**

**VE10.12.01：**ベンダは、高級言語で記述されていない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それぞれを識別して、そのコンポーネントがなぜ低級言語で記述されているかの根拠又は正当性を提供しなければならない。その根拠は、高級言語が利用できないことか、又はソフトウエア若しくはファームウエアのより一層の性能を必要とすることかのいずれかを挙げなければならない。

**TE10.12.01：**試験者は、どのコンポーネントが低級言語で記述されているかを判定するために、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それぞれに対するソースコードを調べなければならない。試験者は、VE10.12.01でベンダによって識別されなかった低級言語で記述されたソフトウエアコンポーネント及び/又はファームウエアコンポーネントはないことを検証しなければならない。

**AS10.13：(レベル 3 及び 4) ハードウエア記述言語(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。**

[解説]

FIPS140-2では原文の冒頭に”If HDL is used, ”がある。このため、「HDLが使用される場合には」を本ASの冒頭に追記した。

**VE10.13.01：**ベンダは、高級仕様言語を用いて実装されたハードウエアコンポーネントに関する文書を提供しなければならない。

**TE10.13.01：**試験者は、VE10.13.01で規定された情報が含まれることを検証するために、ベンダが提供する文書をレビューしなければならない。この情報が含まれない場合には、このアサーションは不合格とする。

**AS10.14：(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。**

注：このアサーションは AS10.15 から AS10.20 の一部として試験される。

[解説]

「セキュリティレベル1、2、及び3の要求事項」は、AS10.06～AS10.08、AS10.10、AS10.12、AS10.13を指す。

「次の要求事項」は、AS10.15～AS10.20を指す。

**AS10.15：(レベル 4)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。**

**VE10.15.01：**ベンダは、暗号モジュールのセキュリティポリシの形式的仕様言語で文書化された形式的モデルを提供しなければならない。形式的モデルは、少なくとも、モデルの

要素リスト、これらの要素上で実行される操作、及びこれらの操作が従うセキュリティルールを含まなければならない。

TE10.15.01：試験者は次を検証するために形式的モデルを分析しなければならない。

1. 形式的モデルの宣言は、ベンダが選択した形式的仕様言語で正しく記述されていること。
2. 形式的モデルは次を含むこと。
   a) セキュアな状態の定義
   b) 暗号モジュールの初期状態の表現
   c) 暗号モジュールがある状態から他の状態へ進む道筋(すなわち、状態遷移)のモデル

注：セキュリティモデル提示の明快さに関する付加的なガイドラインは、NCSC-TG-10(*A Guide to Understanding Security Modeling in Trusted Systems,* National Computer Security Center, October 1992)の2.4節にある。

[解説]

”注：”に記載されたガイドラインは、米国の国内制度におけるガイドラインである。

**AS10.16：(レベル 4)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。**

注：このアサーションは AS10.15 の一部として試験される。

**AS10.17：(レベル 4)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。**

**VE10.17.01：**ベンダが提供する文書は、形式的モデルが暗号モジュールのセキュリティポリシ(動作のルール)とどのように一致しているかを記述しなければならない。

**VE10.17.02：**モデルは、モデル化することができる全てのポリシについて、セキュリティポリシと一致し、かつ、完全であることを実証する根拠を含まなければならない。

**TE10.17.01：**試験者は、暗号モジュールのセキュリティポリシに規定されたルールの表現における完全性及び正確性について、ベンダが提供する文書(セキュリティポリシ、形式的モデル、及びセキュリティポリシと形式的モデルとの対応に関する文書)をレビューしなければならない。

**AS10.18：(レベル 4)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。**

**VE10.18.01：**ベンダは、形式的モデルと機能仕様との対応に関する、非形式的な証明を提供しなければならない。

**TE10.18.01：**試験者は、VE10.18.01で規定された情報が含まれることを検証するために、非形式的な証明をレビューしなければならない。この情報が含まれない場合には、このアサーションは不合格とする。

**AS10.19：(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、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。**

[解説]

FIPS140-2では、本ASの後にさらに以下の文が記載されている。

「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、又は手続きの振る舞いを完全に、かつ、あいまいなところなく、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。」

**VE10.19.01：**全て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ソースコードは、AS10.19で要求されるように、コメントとして、事前条件及び事後条件を含まなければならない。

**TE10.19.01：**試験者は、VE10.19.01で規定された情報が含まれることを検証するために、ソースコードをレビューしなければならない。この情報が含まれない場合には、このアサーションは不合格とする。

**AS10.20：(レベル 4)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。**

**VE10.20.01：**ベンダが提供する文書は、暗号モジュールの設計と機能仕様との一致に関する、非形式的な証明を含まなければならない。

**TE10.20.01：**試験者は、VE10.20.01で規定された情報が含まれることを検証するために、非形式的な証明をレビューしなければならない。この情報が含まれない場合には、このアサーションは不合格とする。

## 10.4　ガイダンス文書

**AS10.21：(レベル 1，2，3，及び 4)クリプトオフィサガイダンスは、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を規定しなければならない。**
注：このアサーションは AS10.23 の一部として試験される。

**AS10.22：(レベル 1，2，3，及び 4)クリプトオフィサガイダンスは、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を規定しなければならない。**
注：このアサーションは AS10.23 の一部として試験される。

**AS10.23：(レベル 1，2，3，及び 4)クリプトオフィサガイダンスは、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を規定しなければならない。**

**VE10.23.01：**ベンダが提供する文書は、AS10.21、AS10.22、及びAS10.23で記載された情報を含まなければならない。

**VE10.23.02：**公開されるクリプトオフィサガイダンスは、クリプトオフィサ向けに用意されなければならない。

**TE10.23.01：**試験者は、VE10.23.01及びVE10.23.02で規定された情報が含まれることを検証しなければならない。この情報が含まれない場合には、このアサーションは不合格とする。

**AS10.24：(レベル 1，2，3，及び 4)ユーザガイダンスは、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を規定しなければならない。**
注：このアサーションは AS10.25 の一部として試験される。

**AS10.25：(レベル 1，2，3，及び 4)ユーザガイダンスは、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を規定しなければならない。**

**VE10.25.01：**ベンダが提供する文書は、AS10.24及びAS10.25で記載された情報を含まなければならない。

**VE10.25.02：**公開されるユーザガイダンスは、ユーザ向けに用意されなければならない。

**TE10.25.01：**試験者は、VE10.25.01及びVE10.25.02で規定された情報が含まれることを検証しなければならない。この情報が含まれない場合には、このアサーションは不合格とする。

# 11．その他の攻撃への対処

**AS11.01：(レベル 1，2，3，及び 4)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。**

**VE11.01.01：**ベンダが提供する公開されるセキュリティポリシは、暗号モジュールが特定の攻撃に対処するように設計されているかどうかを規定しなければならない。ベンダは、その攻撃に対処するために暗号モジュールに実装されているセキュリティメカニズムを、公開されるセキュリティポリシの中で規定しなければならない。

**VE11.01.02：**ベンダが提供する公開されるセキュリティポリシは、規定された実装メカニズムがどのように攻撃に対処するかを示さなければならない。

**TE11.01.01：**試験者は、ベンダが提供する公開されるセキュリティポリシが、攻撃に対処するために実装されたメカニズムを規定していることを検証しなければならない。

**TE11.01.02：**試験者は、ベンダが提供する公開されるセキュリティポリシが、規定された実装メカニズムがどのように攻撃に対処するかを示していることを検証しなければならない。

# Appendix A：文書要求事項のまとめ

**AS12.01：(レベル1, 2, 3，及び4)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。**

注：このアサーションは個別に試験されない。

# Appendix B：推奨ソフトウエア開発手順

注：この節に要求事項はない。

# Appendix C：暗号モジュールのセキュリティポリシ

**AS14.01：(レベル 1，2，3，及び 4)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。**

**VE14.01.01：**物理的暗号モジュールの図面又は画像(それが含まれることが適切な場合には)が、セキュリティポリシに含まれていなければならない。その画像は、暗号モジュールのセキュリティに関係する機能を示すために使用されてもよい(例えば、タンパー証跡、状態インジケータ、ユーザインタフェース、電源接続、等)。

**TE14.01.01：**試験者は、図面又は画像が試験される暗号モジュールを表現していることを検証しなければならない。

## C.1　暗号モジュールのセキュリティポリシの定義

**AS14.02：(レベル 1，2，3，及び 4)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。**
注：このアサーションは、AS14.05-AS14.09の一部として試験される。

**AS14.03：(レベル1，2，3，及び4)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。**

注：このアサーションは、AS14.05-AS14.09の一部として試験される。

## C.2　暗号モジュールのセキュリティポリシの目的

注：この節に要求事項はない。

## C.3　暗号モジュールのセキュリティポリシの規定

**AS14.04：(レベル 1，2，3，及び 4)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**

注：このアサーションは、AS14.05-AS14.09の一部として試験される。

### C．3．1　識別と認証ポリシ

**AS14.05：(レベル 1，2，3，及び 4)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**

**VE14.05.01：**ベンダは、暗号モジュールのオペレータによって担われる全ての役割を規定しなければならない。このリストは、ユーザ役割、及びクリプトオフィサ役割(AS03.03参照)を含まなければならない。暗号モジュールがメンテナンスを許可する場合には、リストはメンテナンス役割を含まなければならない(AS03.04参照)。それ以外の全ての許可された役割が規定されなければならない(AS03.06参照)。

**VE14.05.02：**セキュリティレベル2、3、及び4については、ベンダは、VE14.05.01で記載されているそれぞれの役割に対して、認証のタイプがIDベースか、又は役割ベースかを規定しなければならない。ベンダは、それぞれの役割に対して要求される認証データ(AS03.17、AS03.19、及びAS03.23参照)を規定しなければならない。ベンダは、対応する認証メカニズムの強度を規定しなければならない(AS03.24、AS03.25、及びAS03.28参照)。

**VE14.05.03：**ベンダは、FIPS PUB 140-2のAppendixCに規定された表書式を利用しなければならない。

**TE14.05.01：**試験者は、全ての許可された役割が規定されること、及びそれらがアサーションAS03.03、AS03.04、及びAS03.06によって要求された情報と一致することを確実にするために、セキュリティポリシをチェックしなければならない。

**TE14.05.02：**試験者は、認証のタイプがそれぞれの役割に対して規定されること、要求される認証データがそれぞれの役割に対して規定されること、及び暗号モジュールに実装されている全ての対応する認証メカニズムの強度が規定されることを検証しなければならない。試験者は、この情報が、アサーションAS03.17、AS03.19、AS03.23、AS03.24、AS03.25、及びAS03.28によって要求された情報と一致することを確実にしなければならない。

## C．3．2　アクセス制御ポリシ

**AS14.06：(レベル1，2，3，及び4)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。**
注：このアサーションは個別には試験されない。

**AS14.07：(レベル 1，2，3，及び 4)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。**

**VE14.07.01：**ベンダは、許可された役割に提供される全てのサービスを規定しなければならない。このリストは、状態表示サービス及び全ての自己テストサービスを含まなければならない(AS03.11参照)。その他全ての許可された役割が規定されなければならない

(AS03.06参照)。

**VE14.07.02：**それぞれの許可された役割の中のそれぞれの提供されたサービスにおいて、ベンダは、(平文と暗号文の両方の)秘密鍵及びプライベート鍵、認証データ、その他のCSP、及びその他の保護された情報を含む、セキュリティに関連する情報への許可されたアクセスのタイプを規定しなければならない(AS01.15参照)。

**VE14.07.03：**ベンダは、FIPS PUB 140-2の附属書Cに規定された表書式を用いなければならない。

**TE14.07.01：**試験者は、それぞれの役割に提供されるサービスが規定され(VE14.07.01)、アサーションAS03.14において要求された情報と一致することを確実にするために、セキュリティポリシを検証しなければならない。

**TE14.07.02：**試験者は、役割の中のサービスによって許可された、全てのセキュリティ関連情報への許可されたアクセスのタイプを規定していることを確実にするために、セキュリティポリシを検証しなければならない(VE14.07.02)。試験者は、その情報がアサーションAS03.14の要求事項と一致していることを検証しなければならない。

## C．3．3　物理的セキュリティポリシ

**AS14.08：(レベル 1，2，3，及び 4)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)**

**VE14.08.01：**ベンダは、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を規定しなければならない。

**VE14.08.02：**ベンダは、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を規定しなければならない。

**TE14.08.01：**試験者は、実装されるセキュリティメカニズムがアサーションAS05.01で要求される情報と一致することを確実にするために、セキュリティポリシを検証しなければならない。

## C．3．4　その他の攻撃への対処ポリシ

**AS14.09：(レベル 1，2，3，及び 4)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。**

**VE14.09.01：**ベンダは、特定の攻撃による被害を軽減するために設計される暗号モジュールのセキュリティメカニズムを規定しなければならない。この規定は、実装されたメカニズムがどのようにして攻撃による被害を軽減するかを示し、かつ、これらのメカニズムの限界を記述しなければならない(すなわち、メカニズムが有効でなくなることが分かっている特定の条件又は環境)。

**VE14.09.02：**ベンダは、FIPS PUB 140-2のAppendixCに規定された表書式を用いなければならない。

**TE14.09.01：**試験者は、セキュリティポリシは、特定の攻撃に対して採用されるメカニズ

ムを規定し、その実装されたメカニズムが攻撃による被害をどのように軽減するかを記述し、かつ、既知の限界を記載していることを検証しなければならない。

[解説]

「既知の限界」は、「メカニズムが有効でなくなることが分かっている特定の条件又は環境」と解釈する。