

## 目 次

|                               | ページ |
|-------------------------------|-----|
| 1 適用範囲.....                   | 1   |
| 2 引用規格.....                   | 1   |
| 3 用語及び定義.....                 | 1   |
| 4 略語.....                     | 1   |
| 5 文書構成.....                   | 1   |
| 6 セキュリティ要求事項 .....            | 2   |
| 6.1 暗号モジュールの仕様 .....          | 2   |
| 6.2 暗号モジュールのポート及びインタフェース..... | 11  |
| 6.3 役割, サービス, 及び認証.....       | 25  |
| 6.4 有限状態モデル.....              | 35  |
| 6.5 物理的セキュリティ.....            | 38  |
| 6.6 動作環境 .....                | 60  |
| 6.7 暗号鍵管理 .....               | 70  |
| 6.8 自己テスト .....               | 81  |
| 6.9 設計保証 .....                | 96  |
| 6.10 その他の攻撃への対処 .....         | 106 |
| 6.11 文書化要求事項.....             | 106 |
| 6.12 暗号モジュールのセキュリティポリシ .....  | 109 |

## まえがき

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

この規格は、著作権法で保護対象となっている著作物である。

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

# セキュリティ技術—暗号モジュールのセキュリティ 試験要件

Information technology — Security technique — Security test requirements  
for cryptographic modules

## 1 適用範囲

この規格は、暗号モジュールが **JIS X 19790**（セキュリティ技術—暗号モジュールのセキュリティ要求事項）に適合しているかどうかを試験機関で試験する方法を規定する。その中で、試験者が従うべき手順、検査及び試験の詳細、並びに暗号モジュールが **JIS X 19790** の要求事項を満たすときには達成するはずの結果も示す。これらの詳細な試験方法は、試験過程での高度な客観性を提供し、試験機関すべてにわたっての一貫性を保証することを意図している。

この規格は、更に、**JIS X 19790** に対する適合性の補足材料としてベンダが提供しなければならない情報に対する要求事項も規定する。ベンダは、試験機関へ試験を申し込む前に、暗号モジュールが **JIS X 19790** の要求事項を満たすかどうか判断しようとする場合の手引としてこの規格を使用してもよい。

## 2 引用規格

次に掲げる規格は、この規格に引用されることによって、この規格の規定の一部を構成する。これらの引用規格のうちで、西暦年を付記してあるものは、記載の年の版を適用し、その後の改正版（追補を含む。）には適用しない。

**JIS X 19790:2007** セキュリティ技術—暗号モジュールのセキュリティ要求事項

注記 対応国際規格： **ISO/IEC 19790:2006** (IDT) Information technology — Security techniques — Security requirements for cryptographic modules

## 3 用語及び定義

この規格で用いる主な用語及び定義は、**JIS X 19790** による。

## 4 略語

この規格で用いる主な略語は、**JIS X 19790** による。

## 5 文書構成

この規格は、暗号モジュールのセキュリティ試験に関する要求事項を箇条 6 に規定する。箇条 6 は、**JIS X 19790** の箇条 7（セキュリティ要求事項）の 10 個の細分箇条、**JIS X 19790** の附属書 A（文書化要求事項）、及び **JIS X 19790** の附属書 B（暗号モジュールのセキュリティポリシー）に対応する 12 個の細分箇条から成

る。

簡条 6 の各細分簡条には、その細分簡条に対応する JIS X 19790 の要求事項を列挙する。列挙した個々の要求事項を、個別要件(assertion)と呼ぶ。個別要件は、分野及びセキュリティレベルに対応して、JIS X 19790 からの直接の引用である。

個別要件には、次の形の識別番号をつける。

AS 細分簡条番号 . 個別要件番号

“細分簡条番号”は、その個別要件が書いてある細分簡条(6.  $n$ )の番号( $n$ )を 2 けたの数字で表示する。この番号  $n$  が 1~10 であれば JIS X 19790 の 7.1~7.10 に対応し、11 であれば JIS X 19790 の 附属書 A に対応し、12 であれば JIS X 19790 の附属書 B に対応する。“個別要件番号”は、同じ細分簡条の個別要件につけた通し番号を 2 けたの数字で表示する。識別番号に続けて、その個別要件が適用されるセキュリティレベル(複数の場合もある。)を括弧にくくって表示する。

それぞれの個別要件に対しては、まず、ベンダに対する要求事項を“ベンダ情報要件”として列挙する。ベンダ情報要件ではその個別要件に対する適合性を試験者が判定するためにベンダが提供しなければならない情報を規定する。具体的には、情報内容を明示するか、その情報を記載すべき文書の種類を示すかする。ベンダ情報要件には、次の形の識別番号をつける。

VE 細分簡条番号 . 個別要件番号 . 一連番号

“細分簡条番号”及び“個別要件番号”は、対応する個別要件に対する識別番号の“細分簡条番号”及び“個別要件番号”と同一であり、“一連番号”は、同じ個別要件に関する“ベンダ情報要件”につけた通し番号を 2 けたの数字で表示する。

また、それぞれの個別要件に対しては、ベンダ情報要件に続けて、暗号モジュールの試験者に対する要求事項を“試験手順要件”として列挙する。試験手順要件は、その個別要件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を試験者に指示する。試験手順要件には、次の形の識別番号を付ける。

TE 細分簡条番号 . 個別要件番号 . 一連番号

“細分簡条番号”及び“個別要件番号”は、対応する個別要件に対する識別番号の“細分簡条番号”及び“個別要件番号”と同一であり、“一連番号”は、同じ個別要件に関する“試験手順要件”につけた通し番号を 2 けたの数字で表示する。

## 6 セキュリティ要求事項

**注記** 暗号モジュールは、簡条 6 で記述された各分野の要求事項に対して試験される。暗号モジュールは、分野ごとに独立に格付けされる。

### 6.1 暗号モジュールの仕様

#### AS01.01 : (レベル 1・2・3・4)

暗号モジュールは、ハードウェア、ソフトウェア、ファームウェア、又はそれらの組合せの集合でなければならない。これらハードウェア、ソフトウェア、ファームウェアは、定義された暗号境界内に含まれ、暗号機能又は暗号プロセスを実装している。

**注記** この個別要件は、単独では試験されない。

**AS01.02 : (レベル 1・2・3・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一つ実装しなければならない。

**注** 承認されたセキュリティ機能は、JIS X 19790 の**附属書 D**に記載されている。

**注記** この個別要件は、AS01.12の一部として試験される。

**AS01.03 : (レベル 1・2・3・4)**

オペレータが、承認された動作モードにあるかどうかを判定できるようになっていなければならない。

**ベンダ情報要件**

**VE01.03.01 :** ベンダが提供する公開用セキュリティポリシーは、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ーは、承認された動作モードを呼び出すための方法を記述しなければならない。

**試験手順要件**

**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ーに、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ー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呼び出さなければならない。

**AS01.04 : (レベル 3・4)**

セキュリティレベル 3 及びセキュリティレベル 4 では、暗号モジュールが承認された動作モードにあるとき、そのことを表示しなければならない。

**ベンダ情報要件**

**VE01.04.01 :** ベンダが提供する公開用セキュリティポリシーは、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ーは、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。

**試験手順要件**

**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ーが、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ー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・4)**

暗号境界は、暗号モジュールの物理的範囲及び／又は論理的範囲を確立する明確に定義された境界線で構成されなければならない。

**注記** この個別要件は、AS01.08の一部として試験される。

**AS01.06 : (レベル 1・2・3・4)**

暗号モジュールがソフトウェア又はファームウェアの構成要素から構成されている場合には、暗号境界は、一つ以上のプロセッサ及び（ソフトウェア及びファームウェアの構成要素を格納及び保護する。）その他のハードウェア構成要素を含まなければならない。

**注** 暗号モジュールのハードウェア、ソフトウェア及びファームウェアの構成要素は、これらの構成要素が暗号モジュールのセキュリティに影響を与えないことが示される場合には、**JIS X 19790** の要求事項から除外することができる。

**ベンダ情報要件**

**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ェア又はファームウェア、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。

**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もつすべてのハードウェアを特定しなければならない。

**試験手順要件**

**TE01.06.01 :** 試験者は、この個別要件に基づいて特定されたそれぞれのプロセッサが、個別要件 **AS01.08** に基づくマスター構成要素リスト、及び個別要件 **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ェア又はファームウェ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もつすべてのハードウェ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ェア・ファームウェアに入力データ、制御データ又は状態データを提供するすべてのハードウェア構成要素、並びにプロセッサ及び関連するソフトウェア/ファームウェアから出力データ、制御データ又は状態データを受け取るすべてのハードウェア構成要素を含まなければならない。このようなハードウェア構成要素は、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。

**AS01.07 : (レベル 1・2・3・4)**

次の文書化要求事項は、暗号モジュール内にあるすべてのセキュリティに関係するハードウェア、ソフトウェア及びファームウェアに適用しなければならない。

**注記** この個別要件は、単独では試験されない。

**AS01.08 : (レベル 1・2・3・4)**

文書には、暗号モジュールのハードウェア、ソフトウェア及びファームウェアの構成要素を示し、これらの構成要素を囲む暗号境界を示し、また、暗号モジュールの物理的な構成を記述しなければならない (**JIS X 19790** の 7.5 参照)。

## ベンダ情報要件

**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ェア、ソフトウェア、及びファームウェアのすべての構成要素を示さなければならない。リスト化すべき構成要素には、次の項目に該当するすべてを含まなければならない。

- 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) 回路基板又はその他の実装基板、囲い、及びコネクタを含む物理構造。
- 5) ソフトウェア及びファームウェアモジュール。
- 6) 上記に記載されていない他の構成要素。

**VE01.08.02:** 上記の構成要素のリストは、6.1 の他の個別要件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示さなければならない。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連続する境界でなければならない。境界の定義は、暗号モジュールの構成要素及びコネクション（ポート）を示さなければならない。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示さなければならない。

**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たい化をもたらすことになる重要なセキュリティパラメタを入力、処理、又は出力する、すべてのハードウェア又はソフトウェ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、JIS X 19790 の 7.5 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ことを示さなければならない。

**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、少なくとも縮小又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、回路基板、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タを含むモジュールの主な物理的パラメタを記述しなければならない。

## 試験手順要件

**TE01.08.01:** 試験者は、文書が暗号モジュールのハードウェア、ソフトウェア、及びファームウェアのすべての構成要素を記載したマスター構成要素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、マスター構成要素リストに、その暗号モジュール内で使用しない構成要素を除いて、次の構成要素に該当するものがあればすべ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のための読取り専用メモリ(ROM)[マスク 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、又はフラッシュメモリを含む。]。
- 3) 一時データ保存用のランダムアクセスメモリ(RAM)。
- 4) ゲートアレイ、プログラム可能なロジックアレイ、FPGA、又は他のプログラム可能なロジック

クデバイスのような、セミカスタム特定用途向け集積回路 (ASSP)。

- 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、フルカスタム特定用途向け集積回路 (ASCP)。
- 6) 他の能動回路部品（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ない場合には、プルアップ抵抗、プルダウン抵抗、バイパスコンデンサなど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 コンバータ、DC-DC コンバータ）、トランス、入力電源コネクタ、出力電源コネクタを含む、電源構成要素。
- 8) 回路基板、又は他の部品を搭載する基板構成要素。
- 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部にあるデバイス、又は暗号モジュール内の主要な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ェアモジュール・ファームウェアモジュール。
- 12) 変更される可能性が低いソフトウェアモジュール・ファームウェアモジュール。
- 13) 上記に記載されていない他の構成要素タイプ。

**TE01.08.03：**試験者は、マスター構成要素リストが、次に定義するような **6.1** の他の個別要件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) 個別要件 **AS01.08** に基づく暗号境界の仕様。暗号境界の内側にあるすべての構成要素がマスター構成要素リストに含まれていること、及び暗号境界の外側にあるすべての構成要素が暗号モジュールの構成要素として記載されていないことを検証する。
- 2) **AS01.06** に規定されたプロセッサ及びソフトウェア・ファームウェアの仕様。マスター構成要素リスト内のプロセッサ、ソフトウェアモジュール、ハードウェアモジュールのリストが、個別要件 **AS01.06** に基づいた仕様と同じであることを検証する。
- 3) 個別要件 **AS01.08** に基づく物理的構成の仕様。マスター構成要素リストにおける物理的構造の記載（回路基板又はその他の搭載基板、囲い、及びコネクタを搭載したもの）が、個別要件 **AS01.08** に基づいた仕様と同じであることを検証する。
- 4) 個別要件 **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構成要素[例えば、プロセッサ、特定用途向け集積回路 (ASIC)] のすべてが、マスター構成要素リストに記載されていることを検証する。
- 5) 個別要件 **AS01.09** に基づいた **JIS X 19790** の要求事項から除かれるべきすべての構成要素。マスター構成要素リストには、除かれるべき構成要素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すべての重要な構成要素、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すべ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、すべ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、暗号境界にある構成要素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すき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とは、JIS X 19790 の 7.5 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タ(CSP)、平文データ、又は誤使用によって危たい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、又は誤使用によって危たい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、6.1 の個別要件 **AS01.13** に基づくブロック図で識別されたすべての構成要素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、6.1 の個別要件 **AS01.09** に基づく要求事項を満たす場合は、特定の構成要素に JIS X 19790 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、適用除外とした構成要素を、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、適用除外の構成要素とそれ以外の構成要素との間のすべ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、又は誤使用によって危たい化をもたらすその他の情報が、安全でない状態では漏えいし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 JIS X 19790 の 7.5 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ダードアロン型暗号モジュールのいずれかであることを示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構成要素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、少なくとも縮小又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ない。

- 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) 回路基板の寸法、レイアウト、及び接続。
- 3) 電源、電圧変換器、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放熱板、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構成要素タイプ。

#### **AS01.09：（レベル 1・2・3・4）**

文書には、JIS X 19790 のセキュリティ要求事項の適用を除外する暗号モジュールのハードウェア、ソフトウェア及びファームウェアの構成要素を示し、また、適用除外とする根拠を説明しなければならない。

#### **ベンダ情報要件**

**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すべての構成要素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構成要素の適用除外理由は、

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、例えば誤動作又は誤使用であっても、それぞれの構成要素が、いかなる合理的な条件のもとでも危たい化を引き起こさないことを示さなければならない。

#### 試験手順要件

**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構成要素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、すべての構成要素は、**JIS X 19790**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構成要素を **JIS X 19790** 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示されているかを判定しなければならない。その理由では、その構成要素が誤作動しても、CSP、平文データ、又は誤使用によって危たい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) 構成要素は、CSP、平文データ、又は誤使用によって危たい化をもたらすその他の情報を処理しない。
- 2) 構成要素は、CSP、平文データ、又は誤使用によって危たい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構成要素と接続していない。
- 3) 構成要素が処理するすべての情報は、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。何らかの不確実性又は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・4）**

文書には、暗号モジュールの、物理的ポート、論理的インタフェース及び定義された入出力データパスのすべてを示さなければならない。

**注記** この個別要件は、**AS02.01**の一部として試験される。

#### **AS01.11：（レベル 1・2・3・4）**

文書には、暗号モジュールの手動の又は論理的な制御、物理的又は論理的な状態表示、並びに関連するそれらの物理的、論理的及び電気的な特徴を示さなければならない。

**注記** この個別要件は、**AS02.01**の一部として試験される。

#### **AS01.12：（レベル 1・2・3・4）**

文書には、承認されているかどうかにかかわらず、暗号モジュールに採用されるすべてのセキュリティ機能をリスト化して、承認されているかどうかにかかわらず、すべての動作モードを示さなければならない。

#### ベンダ情報要件

**VE01.12.01**：ベンダは、すべての承認された暗号アルゴリズムに対して、アルゴリズム確認書を提供しなければならない。

**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。

#### 試験手順要件

**TE01.12.01**：試験者は、ベンダが上記に示した一つ以上のアルゴリズム確認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・4）**

文書には、次を示さなければならない。

- ・ 暗号モジュールの主要なハードウェア構成要素のすべて及びそれらの接続関係を示すブロック図。これには、マイクロプロセッサ、入出力バッファ、平文・暗号文データ用バッファ、制御バッファ、鍵格納メモリ、作業メモリ及びプログラムメモリを含む。

**ベンダ情報要件**

**VE01.13.01**：ベンダが提供する文書は、ハードウェア構成要素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構成要素は、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構成要素

**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構成要素間の接続関係、及び暗号モジュールと暗号境界の外部の装置間又は構成要素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。

**試験手順要件**

**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一つ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) 6.1 の個別要件 **AS01.08** に基づいたマスター構成要素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) 実行可能ソフトウェア又はファームウェ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, プログラム可能なロジックアレイ (PLA), 又は他のプログラム可能なロジックアレイ (PLD) ]。
- 9) 上記に記載されないその他の構成要素。

**TE01.13.02:** 試験者は, ブロック図が, 暗号モジュールの主要な構成要素間, 及び暗号モジュールと外部装置との間の, すべての重要な接続関係及び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, 6.1 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・4)**

文書には, 次を示さなければならない。

- ・ 暗号モジュールのハードウェア, ソフトウェア及びファームウェアの構成要素の設計。この設計を文書化するためには, ソフトウェア・ファームウェアは高級言語を使用し, ハードウェアは回路図を使用しなければならない。

#### **ベンダ情報要件**

**VE01.14.01:** ベンダは, 暗号モジュールに含まれるハードウェア, ソフトウェア, ファームウェアの構成要素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, 有限状態モデル及び **JIS X 19790** の 7.4 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と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。

#### **試験手順要件**

**TE01.14.01:** 試験者は, 有限状態モデルと設計仕様との関係が特定できることを検証するために, **AS09.12** 及び **AS09.13** で文書化されたハードウェア, ソフトウェア, 及びファームウェアの全構成要素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・4)**

文書には, CSP, PSP, 及び開示又は変更されると暗号モジュールのセキュリティに危たい化をもたらすその他の保護された情報 (例えば, 監査イベント, 監査データ) を含む, すべてのセキュリティに関係する情報を示さなければならない。

#### **ベンダ情報要件**

**VE01.15.01:** ベンダは, CSP, PSP, 及び開示又は変更されると暗号モジュールのセキュリティに危たい化をもたらすその他の保護された情報 (例えば, 監査イベント, 監査データ) を含む, すべてのセキュリティに関係する情報を示した文書を提供しなければならない。

#### **試験手順要件**

**TE01.15.01:** 試験者は, 文書が, CSP, PSP, 及び開示又は変更されると暗号モジュールのセキュリティに危たい化をもたらすその他の保護された情報 (例えば, 監査イベント, 監査データ) を含む, すべてのセキュリティに関係する情報を示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・4)**

文書には, 暗号モジュールのセキュリティポリシーを示さなければならない。

**注記** この個別要件は、AS01.17の一部として試験される。

**AS01.17：（レベル 1・2・3・4）**

このセキュリティポリシーは、JIS X 19790 の要求事項から導かれる規則、及びモジュール開発を通じて課せられたあらゆる追加の要求事項から導かれる規則を含まなければならない（JIS X 19790 の**附属書 B** 参照）。

**ベンダ情報要件**

**VE01.17.01：**ベンダは、JIS X 19790 の**附属書 B** に規定された最小限の要求事項を満たした公開用暗号モジュールセキュリティポリシーを提供しなければならない。

**試験手順要件**

**TE01.17.01：**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ー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ーが JIS X 19790 の**附属書 B** に規定された要求事項を満たしていることを検証しなければならない。

**6.2 暗号モジュールのポート及びインタフェース**

**AS02.01：（レベル 1・2・3・4）**

暗号モジュールは、すべての情報の流れ及び物理的アクセスポイントを、暗号モジュールへのすべての入出力点を定義している物理的ポート及び論理的インタフェースに限定しなければならない。

**ベンダ情報要件**

**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示さなければならない。

- 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、すべての他のデータ信号・制御信号・状態信号）並びに信号の名称及び機能。
- 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、スイッチ）。
- 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、6.1 及び 6.9 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示さなければならない。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示す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。

ベンダは、個別要件 **AS01.08**、**AS01.10** 及び **AS01.13** に基づいて提供される情報との関係において、入出力ポートの構成要素及び物理的レイアウトの記述との不一致がないように、上記情報を提示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示さなければならない。ベンダが提

供する文書に記載されている仕様は、**6.1** 及び **6.9** に記載されている暗号モジュール構成要素仕様と、**6.2** の個別要件 **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。

### 試験手順要件

**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示していることを検証しなければならない。要求される仕様として、次の記述を含まなければならない。

- 1) すべ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、及び二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。
- 2) すべ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／又は変更できる構成要素又は機能を含める。
- 3) すべての論理の入出力インタフェース（例えば、API、すべての他のデータ信号・制御信号・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すべての論理データ、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。
- 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すべ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。
- 5) すべ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。
- 6) 論理の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。

**TE02.01.02**：試験者は、**6.1** 及び **6.9** 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すべての情報の流れ及び物理的アクセスポイントを示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示さなければならない。試験者は、上記の情報を **AS01.08**、**AS01.10**、及び **AS01.13** に基づく情報と比較して、入出力ポートの構成要素及び物理的レイアウトの記述のなかに不一致のな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示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、**6.1** 及び **6.9** に記載されている暗号モジュール構成要素の仕様と、**6.2** の **AS02.03** から **AS02.09** の個別要件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すべての仕様が、暗号モジュールの実際的设计と一致していることを検証しなければならない。

**AS02.02：（レベル 1・2・3・4）**

暗号モジュールの論理的インタフェースは、一つの物理的ポートを共有（例えば、データの入力と出力とが、同一のポートを介して行われる。）しても、又は一つ以上の物理的ポートに分散（例えば、シリアルポートとパラレルポートとの両方を介して、入力データが入力される。）されてもよいが、互いに明確に区別して定義されていなければならない。

**ベンダ情報要件**

**VE02.02.01**：ベンダの設計は、6.2 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って、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、6.2 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二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、二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、一つの物理的ポートを共有してもよい。二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示さなければならない。

**試験手順要件**

**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、6.2 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、6.2 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二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、二つ以上の論理的インタフェースが一つの物理的ポートを共有していてもよい。二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示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・4)**

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

- ・ 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

**ベンダ情報要件**

**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四つの論理的インタフェースを明確に区別して示さなければならない（“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** 及び **AS02.06** 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）

**試験手順要件**

**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四つの論理的インタフェースを明確に区別して示していることを検証しなければならない。この場合、暗号モジュール内の論理的インタフェースが、**AS02.04** から **AS02.08** の個別要件で規定された機能で動作することを検証しなければならない。

**データ入力インタフェース****AS02.04 : (レベル 1・2・3・4)**

暗号モジュールに入力され処理されるすべてのデータ（制御入力インタフェースを介して入力される制御データを除く。）は、データ入力インタフェースを介して入力されなければならない。これらのデータには、平文データ、暗号文データ、CSP、PSP 及び別の暗号モジュールからの状態情報を含む。

**ベンダ情報要件**

**VE02.04.01 :** 暗号モジュールはデータ入力インタフェースをも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すべてのデータ（制御入力インタフェースを介して入力される制御データを除く）は、データ入力インタフェースを介して入力しなければならない。すべてのデータには、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) CSP（平文又は暗号化されたもの）
- 4) PSP（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) 他のすべての入力データ

**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／又は生体認証装置のような、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すべての外部入力デバイスを示さなければならない。

#### 試験手順要件

**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とお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すべてのデータ（制御入力インタフェースを介して入力される制御データを除く。）は、データ入力インタフェース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) CSP（平文又は暗号化されたもの）。
- 4) 暗号モジュールに入力される平文又は暗号化された PSP（平文又は暗号化されたもの）。
- 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すべての情報。

**注記** セキュリティレベル 1 及び 2 においては、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 及び 4 に対応する要求事項は、別に **6.2** 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／又は生体認証装置のような、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すべての外部入力デバイスが示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、識別された一つ以上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 that 示されたとおりに機能することを検証しなければならない。

#### データ出力インタフェース

##### **AS02.05: (レベル 1・2・3・4)**

暗号モジュールから出力されるすべてのデータ（状態出力インタフェースを介して出力される状態データを除く）は、データ出力インタフェースから出力されなければならない。これらのデータには、平文データ、暗号文データ、CSP、PSP 及び別の暗号モジュールのための制御情報を含む。

#### ベンダ情報要件

**VE02.05.01:** 暗号モジュールは、データ出力インタフェースをも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すべてのデータ（状態出力インタフェースを介して出力される状態データは除く）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。すべてのデータには、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) 他のすべての出力データ

**注記** セキュリティレベル 1 及び 2 の場合、平文暗号鍵及び他の平文 CSP の出力の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兼用してもよい（セキュリティレベル 3 及び 4

の場合に、対応する要求事項は 6.2 の AS02.16 のもとで別途取り扱われる。))。

**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すべての外部出力デバイスを示さなければならない。

#### 試験手順要件

**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示されたとお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、出力されるすべてのデータ（状態出力インタフェースを介して出力される状態データを除く）は、データ出力インタフェース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) 初期化データ及び初期化ベクトル、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 6.7 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すべての情報。

**注記** セキュリティレベル 1 及び 2 においては、平文の暗号鍵及びその他の平文 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 及び 4 に対応する要求事項は、別に 6.2 の AS02.15 又は 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すべての外部出力デバイスが示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、識別された一つ以上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示されたとお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・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すべてのデータ出力は禁止されなければならない（JIS X 19790 の 7.8 参照）。

#### ベンダ情報要件

**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 JIS X 19790 の 7.4 に記述されている。）にあるときは常に、データ出力インタフェースからのすべてのデータ出力が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示さなければならない。CSP、平文データ、又は誤使用された場合に危たい化をもたらす可能性のある他の情報が状態情報の中にある場合には、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 JIS X 19790 の 7.8 に記述されている。）にあるときは常に、データ出力インタフェースからのすべてのデータ出力が

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示さなければならない。CSP、平文データ、又は誤使用された場合に危たい化をもたらす可能性のある他の情報が状態情報の中にある場合には、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。

#### 試験手順要件

**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ときは常にデータ出力インタフェースからのすべてのデータ出力が禁止されていることを示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、いったん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すべ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たい化をもたらす可能性のある他の情報が状態情報の中にある場合には、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、この個別要件に対して示されたエラー状態のすべてが、**AS04.02** で規定されたエラー状態とすべて一致していることも検証しなければならない。

**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、データ出力インタフェースからのすべ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ときは常にデータ出力インタフェースからのすべてのデータ出力が禁止されていることを示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、いったん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すべ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たい化をもたらす可能性のある他の情報が状態情報の中にある場合には、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、この個別要件に対して示された自己テスト状態すべてと**AS08.07** に規定された自己テストとがすべて一致していることも検証しなければならない。

**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、データ出力インタフェースからのすべ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たい化をもたらす可能性のある他の情報が状態情報の中にある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すべてのデータ出力を禁止している方法を示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。

#### 制御入力インタフェース

**AS02.07 : (レベル 1・2・3・4)**

暗号モジュールの動作を制御するために使用されるすべての入力コマンド、信号及び制御データ（関数呼出し及びスイッチ、ボタン、並びにキーボードのような手動制御を含む。）は、制御入力インタフェースから入力されなければならない。

**ベンダ情報要件**

**VE02.07.01 :** 暗号モジュールは、制御入力インタフェースをも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すべてのコマンド、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。すべてのコマンド、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ェア構成要素及びファームウェア構成要素用）。
- 2) 一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ェア構成要素用）。
- 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) 他のすべ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、暗号モジュールで使用されるすべての外部入力デバイス（例えば、スマートカード、トークン、又はキーパッド）を示さなければならない。

**試験手順要件**

**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すべてのコマンド、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) ソフトウェアライブラリ又はスマートカードに対する関数呼出しのような、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、一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) 他のすべ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、暗号モジュールで使用されるすべての外部入力デバイス（例えば、スマートカード、トークン、又はキーパッド）を示しているかどうかを検証しなければならない。試験者は、その示された一つ以上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規定されたとおりに機能することを検証しなければならない。

## ステータス出力インタフェース

### AS02.08 : (レベル 1・2・3・4)

暗号モジュールの状態を示すために使用されるすべての出力信号、インジケータ及び状態データ（戻り値、並びに発光ダイオード（LED）及びディスプレイのような物理的なインジケータを含む。）は、状態出力インタフェースから出力されなければならない。

### ベンダ情報要件

**VE02.08.01 :** 暗号モジュールは、状態出力インタフェースをも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すべての状態情報、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。すべての状態情報、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) 一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) 他のすべての出力状態情報。

**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の、暗号モジュールで 사용되는すべての外部出力デバイス（例えば、スマートカード、トークン、ディスプレイ、その他の記憶デバイス）を示さなければならない。

### 試験手順要件

**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とお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すべての状態情報、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) ソフトウェ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、一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) 他のすべての出力状態情報。

**TE02.08.02 :** 試験者は、ベンダが提供する文書が、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の、暗号モジュールで 사용되는すべての外部出力デバイス（例えば、スマートカード、トークン、ディスプレイ、その他の記憶デバイス）を示しているかどうかを検証しなければならない。

### AS02.09 : (レベル 1・2・3・4)

暗号モジュールに入力されるすべての外部電力（外部電源又はバッテリーからの電力を含む。）は、電源ポートから入力されなければならない。

### ベンダ情報要件

**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、電源又は外部バッテリー）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示さなければならない。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すべての電力授受は、示された電源インタフェースを介さなければならない。

**VE02.09.02：**暗号モジュールと暗号境界外の他のデバイス間でやり取りされるすべての電力は示された電力インタフェースを通さなければならない。

#### 試験手順要件

**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、又は外部バッテリー）との間で電力の授受があるかどうかを示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示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すべての電力が、示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。すべ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。また、内部バッテリーの交換は物理的なメンテナンス活動としてみなされ、6.5の個別要件で規定されている要求事項の対象である。

#### AS02.10：（レベル 1・2・3・4）

暗号モジュールは、入力するデータと制御データとを区別し、また、他方で、出力するデータと状態データとを区別しなければならない。

#### ベンダ情報要件

**VE02.10.01：**ベンダが提供する文書は、暗号モジュールが入力するデータと制御データとをどのように分離し、出力するデータと状態データとをどのように分離しているかを示さなければならない。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示さなければならない。

**VE02.10.02：**ベンダが提供する文書は、入力データ及び制御情報によって使用される物理的・論理的パスが、出力データ及び状態情報によって使用される物理的・論理的パスとどのように分離されているかを示さなければならない。もし入力データ、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、ベンダが提供する文書は、論理的な分離が暗号モジュールによって、どのように実施されているかを示さなければならない。

**VE02.10.03：**ベンダが提供する文書は、記述の一貫性を示さなければならない。また、暗号モジュールが、入力するデータと制御データとを区別し、出力するデータと状態データとを区別すること、及び該当する入力インタフェースを経由して暗号モジュールに入力される入力データ及び制御情報の流れる物理的・論理的パスが、該当する出力インタフェースを経由して暗号モジュールから出力される出力データと状態情報の流れる物理的・論理的パス及び物理的又は論理的に分離されていることを示さなければならない。

#### 試験手順要件

**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“入力するデータ及び制御データ”と“出力するデータ及び状態データ”とをどのように分離しているかを示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示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示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示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“入力するデータ及び制御データ”と“出力するデータ及び状態データ”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・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すべての入力データは、入力データパスだけを通らなければならない。

#### **ベンダ情報要件**

**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すべての主要なカテゴリによって使用される物理的・論理的パスを示さなければならない。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すべての入力データは、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、指定されたパスだけを使用しなければならない。

**VE02.11.02：**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すべてが指定されたパスを使用することを示さなければならない。ベンダが提供する文書は、入力データによって使用されるすべての論理的・物理的情報フローは暗号モジュールの設計及び動作と一致していることを示さなければならない。ベンダが提供する文書は、該当するパス間に CSP、平文データ、又は他の情報の危たい化をもたらすことになる競合がないことを提示しなければならない。

#### **試験手順要件**

**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すべての主要なカテゴリによって使用される物理的・論理的パスを示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示されなければならない。

**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すべての入力データが、指定されたパスだけ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、すべ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、該当するパス間に、CSP、平文データ、又は他の情報の危たい化をもたらすことになる競合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・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すべての出力データは、出力データパスだけを通らなければならない。

**ベンダ情報要件**

**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すべてによって使用される物理的・論理的パスを示さなければならない。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。）。

**VE02.12.02：**データ出力インタフェースを介して暗号モジュールから出力されるすべての出力データは、指定されたパスだけを使用しなければならない。

**試験手順要件**

**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すべてによって使用される物理的・論理的パスが示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、示されてなければならない。

**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すべての出力データが、指定されたパスだけ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、すべ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、該当するパス間に、CSP、平文データ、又は他の情報の危たい化をもたらすことになる競合がないことを検証しなければならない。

**AS02.13：（レベル 1・2・3・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。

**ベンダ情報要件**

**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すべ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、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示さなければならない。

**VE02.13.02:** 出力データと CSP 情報とが物理的・論理的パスを物理的に共有している場合、暗号モジュールは出力データと CSP 情報との論理的な分離を実施しなければならない。

**VE02.13.03:** 暗号モジュールは、上記に示された鍵処理が、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。

#### 試験手順要件

**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すべ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、及び 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示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 CSP 情報とが物理的・論理的パスを、物理的に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、暗号モジュールが、出力データと CSP 情報との論理的な分離をどのように実現しているかについて示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、及び CSP 情報が漏えい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、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・4)

誤って取扱いに慎重さを要する情報を出力してしまうことを防止するために、平文の CSP 又は取扱いに慎重さを要するデータを出力インタフェースから出力することに対して、二つの独立した内部動作 [例えば、二つの異なるソフトウェアフラグがセットされるという二つの独立した内部動作 (その一つはユーザが起動するものでもよい。)、二つのハードウェアゲートが別々の動作によって順次にセットされるという二つの独立した内部動作。] が要求されなければならない。

#### ベンダ情報要件

**VE02.14.01:** 暗号モジュールの設計上、平文の CSP が一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 CSP が出力される前に、二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、実行される二つの独立した内部動作を示して、二つの独立した内部動作が、平文の CSP を誤って漏えい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示さなければならない。

**VE02.14.02:** 平文の CSP の出力処理において、ソフトウェア又はファームウェア要素が実行される場合、暗号モジュールはソフトウェア又はファームウェア要素が平文の CSP の出力の前に二つの独立した内部動作の要件を満足していることを確実にしなければならない。

#### 試験手順要件

**TE02.14.01:** 試験者は、暗号モジュールが、一つ以上の物理的ポートに平文の 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 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、二つの独立した内部動作について示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 CSP を誤って漏えいすることに対して、どのように二つの独立した内部動作が保護するかについて示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、CSP を一つ以上の物理的ポートに出力させて、二つの独立した内部動作が示されたとおりに機能することを確認しなければならない。何らかのソフトウェア構成要素又はファームウェア構成要素が、平文の 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、そのソフトウェア構成要素又はファームウェア構成要素が、平文の CSP を出力する前の二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。

**AS02.15：（レベル 3・4）**

レベル 1 及び 2 の要求事項に加えて、次のいずれかの要求事項を満たさなければならない。

- ・ 平文の CSP の入出力のために使用される一つ以上の物理的ポートは、暗号モジュールの他のすべてのポートから物理的に分離されていなければならない。
- ・ **AS02.16**

**ベンダ情報要件**

**VE02.15.01**：ベンダが提供する文書は、暗号モジュールが、平文の CSP を入力又は出力するかどうかを示さなければならない。平文の CSP の入出力に使用される一つ以上の物理的ポートは、暗号モジュールの他のすべての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。

**VE02.15.02**：暗号モジュールが平文の CSP を入出力する場合、暗号モジュールは CSP だけが該当する物理ポートを経由して入出力すること及びその他のデータが該当する物理ポートを経由して入出力しないことを確実にしなければならない。

**試験手順要件**

**TE02.15.01**：試験者は、ベンダが提供する文書が、平文の 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示しているかどうかを確認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 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すべての物理的ポートから物理的に分離されていることを確認しなければならない。

**TE02.15.02**：暗号モジュールが平文の CSP を入出力する場合には、試験者は、平文の CSP だけが、該当する物理的ポートを介して入出力されることを確認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かかわらず、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確認しなければならない。

**AS02.16：（レベル 3・4）**

レベル 1 及び 2 の要求事項に加えて、次のいずれかの要求事項を満たさなければならない。

- ・ **AS02.15**
- ・ 平文の CSP の入出力に使用される論理的インタフェースは、高信頼パスを使用して他のすべてのインタフェースから論理的に分離されていなければならない。

**ベンダ情報要件**

**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 CSP を入出力するかどうかを示さなければならない。平文の CSP の入出力に使用される論理的インタフェースは、高信頼パスを使用する他のすべてのインタフェースから論理的に分離されていなければならない。

**VE02.16.02**：暗号モジュールが CSP を入出力する場合、暗号モジュールは CSP だけが高信頼パスを使用し、該当する論理インタフェースを経由して入出力されることを確実にしなければならない。また、その他のデータは暗号化されているかいないかにかかわらず、高信頼パスを使用し、該当する論理インタ

フェースを経由して入出力されないことを確実にしなければならない。

#### 試験手順要件

**TE02.16.01**：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 CSP を入力又は出力するかどうかについて示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 CSP の入出力に使用される該当する論理的ポートが、高信頼パスを使用して暗号モジュールの他のすべ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。

**TE02.16.02**：暗号モジュールが、平文の CSP を入出力する場合には、試験者は、平文の CSP だけが、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。

#### AS02.17：（レベル 3・4）

レベル 1 及び 2 の要求事項に加えて、次の要求事項を満たさなければならない。

- ・ 平文の CSP は、高信頼パスを経由して暗号モジュールに入力されるか、又は、その鍵要素が不注意に格納、結合、若しくはその他の方法で処理される可能性のある、暗号モジュールを取り囲むシステム若しくは仲介するシステムを経由せずに、直接に暗号モジュールに入力されなければならない（JIS X 19790 の 7.7.4 参照）。

#### ベンダ情報要件

**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 CSP を入力するかどうかを示さなければならない。これらのパラメ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。）。

#### 試験手順要件

**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 CSP を入力するかどうかについて示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。

### 6.3 役割、サービス、及び認証

#### AS03.01：（レベル 1・2・3・4）

暗号モジュールは、オペレータに対して認可された役割及びそれぞれの役割に対応するサービスをサポートしなければならない。

**注記** この個別要件は、単独では試験されない。

**AS03.02 : (レベル 1・2・3・4)**

暗号モジュールが、複数のオペレータによる同時利用をサポートする場合には、その暗号モジュールは、それぞれのオペレータによって担われる役割及びそれに対応するサービスの区分けを、内部的に維持しなければならない。

**ベンダ情報要件**

**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示さなければならない。ベンダは、認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、メンテナンス役割のあるオペレータ及びユーザ役割のあるオペレータは同時には許可されない。）。

**試験手順要件**

**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及びサービスをオペレータごとに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、オペレータ 1 とオペレータ 2 という二人の独立したオペレータとして振る舞わなければならない。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。また、試験者は、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及びサービスのオペレータごと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示している場合には、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。

**6.3.1 役割****AS03.03 : (レベル 1・2・3・4)**

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

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

**ベンダ情報要件**

**VE03.03.01 :** ベンダが提供する文書は、少なくとも一つのユーザ役割及び少なくとも一つのクリプトオフィサ役割を含めなければならない。

**試験手順要件**

**TE03.03.01 :** 試験者は、ベンダが提供する文書をレビューして、少なくとも一つのユーザ役割と少なくとも一つのクリプトオフィサ役割とが定義されていることを検証しなければならない。試験者は、これらの役割が名称及び許可されたサービスによって指定されることを、検証しなければならない。

**注記** 役割を担うことに関しては、**TE11.02.02** によって試験される。

**AS03.04 : (レベル 1・2・3・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、次の認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（例えば、ハードウェア・ソフトウェアの診断）を行うことを担う役割。

**ベンダ情報要件**

**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もつ場合には、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、その役割を完全に示さなければならない。

**試験手順要件**

**TE03.04.01:**試験者は、メンテナンスインタフェースが示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仕様をレビューしなければならない(**AS05.08** 参照)。この場合、試験者は、認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示されていることを検証しなければならない。

**注記** 役割を担うことに関しては、**TE011.02.02** で試験される。

**AS03.05 : (レベル 1・2・3・4)**

暗号モジュールは、それがサポートするメンテナンス役割へ入る場合、又はメンテナンス役割から出る場合には、すべての CSP をゼロ化しなければならない。

**ベンダ情報要件**

**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、**JIS X 19790** の **3.13** で定義される暗号モジュールのすべての CSP が、どのようにして能動的にゼロ化されるかを示さなければならない。

**試験手順要件**

**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、すべての CSP をゼロ化する方法を示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、すべての 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。

**TE03.05.03:**試験者は、メンテナンス役割の間に、すべての 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。

**6.3.2 サービス****AS03.06 : (レベル 1・2・3・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、又は機能のすべてを意味しなければならない。

**注記** この個別要件は、単独では試験されない。

**AS03.07 : (レベル 1・2・3・4)**

サービス入力、特定のサービス、動作、又は機能を開始又は獲得させる暗号モジュールへのすべてのデータ入力又は制御入力から構成されなければならない。

**注記** この個別要件は、単独では試験されない。

**AS03.08 : (レベル 1・2・3・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。

**注記** この個別要件は、単独では試験されない。

**AS03.09 : (レベル 1・2・3・4)**

それぞれのサービス入力、サービス出力をもたらさなければならない。

**注記** この個別要件は、単独では試験されない。

**AS03.10 : (レベル 1・2・3・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。

- a) 状態の表示。暗号モジュールの現在の状態を出力する。
- b) 自己テストの実行。JIS X 19790 の 7.8 で規定されているように、自己テストを開始及び実行する。
- c) 承認されたセキュリティ機能の実行。JIS X 19790 の 7.1 で規定されているように、承認された動作モードで使用される少なくとも一つの承認されたセキュリティ機能を実行する。

**ベンダ情報要件**

**VE03.10.01 :** ベンダが提供する文書は、VE11.02.01 に規定されたように、暗号モジュールの現在状態の出力、ユーザが呼び出せる自己テストの開始及び実行、並びにその他のサービスについて記述しなければならない。

**試験手順要件**

**TE03.10.01 :** 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一つの認可された役割に割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 AS11.02 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。

**TE03.10.02 :** 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。

**TE03.10.03 :** 暗号モジュールが、JIS X 19790 の 7.8 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、TE11.02.02 で実施される。

**AS03.11 : (レベル 1・2・3・4)**

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

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

**ベンダ情報要件**

**VE03.11.01 :** 暗号モジュールがバイパス機能を実装している場合には、ベンダが提供する文書は、**AS03.11**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。

**VE03.11.02 :** 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すべての遷移について、二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。

**試験手順要件**

**TE03.11.01 :** 試験者は、バイパス機能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、バイパス機能が少なくとも一つの認可された役割に割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。

**TE03.11.02 :** 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二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。

**TE03.11.03 :** 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二つの内部動作が行われることを判定しなければならない。

**6.3.3 オペレータ認証**

**注記** 暗号モジュールは、セキュリティレベル 1 の場合、暗号モジュールのアクセス管理のための認証メカニズムを採用することは要求されない。

**AS03.12 : (レベル 2・3・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。

- ・ 役割ベースの認証 (AS03.13 から AS03.15 まで)
- ・ ID ベースの認証 (AS03.16 から AS03.17 まで)

**注記** この個別要件は、単独では試験されない。

**役割ベースの認証****AS03.13 : (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、オペレータが一つ以上の役割を選択することを要求しなければならない。

**注記** この個別要件は、AS03.14 の一部として試験される。

**AS03.14 : (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、オペレータが選択された役割を担っていることを認証しなければならない。

**ベンダ情報要件**

**VE03.14.01:**ベンダは、暗号モジュールのために行われ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、役割又は役割の集合の暗黙的又は明示的な選択、及びその役割を担うオペレータの認証に用いられるメカニズムを文書化しなければならない。

**試験手順要件**

**TE 03.14.01:** 試験者は、ベンダが提供する文書が、一つ以上の役割の選択、及びその役割を担うオペレータの認証に用いられるメカニズムを示していることを検証しなければならない。

**TE03.14.02:**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。

**AS03.15 : (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ときで、暗号モジュールがオペレータの役割変更を許可する場合には、暗号モジュールは、オペレータが以前に認証されていないいかなる役割を担うことに対しても認証をしなければならない。

**ベンダ情報要件**

**VE03.15.01:** 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記しなければならない。

**試験手順要件**

**TE03.15.01:**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。

**TE03.15.02:**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認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認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

##### AS03.16 : (レベル 3・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、オペレータによって暗黙的又は明示的に一つ以上の役割が選択されることを要求し、並びにオペレータの ID 及びオペレータが選択された役割（又は役割の集合）を担うことの認可を認証しなければならない。

#### ベンダ情報要件

**VE03.16.01:** ベンダは、暗号モジュール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、役割又は役割の集合の暗黙的又は明示的な選択、及びその役割を担うオペレータの検証に用いられるメカニズムを文書化しなければならない。

#### 試験手順要件

**TE03.16.01:** 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一意に識別されるか、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認可が認証された ID に基づいてどのように実行されるかについて示していることを検証しなければならない。

**TE03.16.02:** 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。

**TE03.16.03:** 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、役割を担う認可が拒否されることを観察しなければならない。

##### AS03.17 : (レベル 3・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ときで、暗号モジュールがオペレータに役割を変更することを許可する場合には、暗号モジュールは、識別されたオペレータが以前に認可されていないいかなる役割を担うための認可を検証しなければならない。

#### ベンダ情報要件

**VE03.17.01:** 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記しなければならない。

#### 試験手順要件

**TE03.17.01:** 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認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。

**TE03.17.02:** 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、試験者が認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、試験者が認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。

**AS03.18 : (レベル 1・2・3・4)**

暗号モジュールが電源オフに続いて電源オンされた場合には、以前の認証の結果は維持されてはならず、暗号モジュールはオペレータに再認証されるように要求しなければならない。

**ベンダ情報要件**

**VE03.18.01:** ベンダが提供する文書は、暗号モジュールが電源オフされるときに、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。

**試験手順要件**

**TE03.18.01:** 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オフ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。

**TE03.18.02:** 試験者は、暗号モジュールに自分自身を認証させて、一つ以上の役割を担い、暗号モジュールを電源オフし、暗号モジュールを電源オンして、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。

**AS03.19 : (レベル 2・3・4)**

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

**ベンダ情報要件**

**VE03.19.01:** ベンダが提供する文書は、暗号モジュールに対するすべ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、認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方法を含まなければならない。

**試験手順要件**

**TE03.19.01:** 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、認可されていない開示、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。

**TE03.19.02:** 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もつことを認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だけ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示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。

**AS03.20 : (レベル 2・3・4)**

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

**ベンダ情報要件**

**VE03.20.01 :** 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示さなければならない。

**試験手順要件**

**TE03.20.01 :** 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ときにオペレータが認証される手続について記述していることを検証しなければならない。

**TE03.20.02 :** 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、認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。

**AS03.21 : (レベル 2・3・4)**

認証メカニズムの強度は、次の仕様（**AS3.22** から **AS3.25** まで）に適合しなければならない。

**注記** この個別要件は、単独では試験されない。

**AS03.22 : (レベル 2・3・4)**

1 回の認証メカニズムの試行において、ランダムな試行が成功する確率（例えば、パスワード又は PIN の推定の成功率、生体認証デバイスの誤受入率、それらの幾つかの組合せ。）は、目標認証強度を満たさなければならない。この確率は、例えば、1 000 000 分の 1 未満である。

**ベンダ情報要件**

**VE03.22.01 :** ベンダが提供する文書は、それぞれの認証方法、及びそれに関係する誤受入率又はランダムな試行が成功する確率を示さなければならない。

**試験手順要件**

**TE03.22.01 :** 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 未満であるといった、目標認証強度を満たしていることを検証しなければならない。

**AS03.23 : (レベル 2・3・4)**

複数回の認証メカニズムを 1 分間に試行する場合、確率は、定められた目標認証強度を満たさなければならない。ランダムな試行が成功する確率は、例えば、100 000 分の 1 未満である。

**ベンダ情報要件**

**VE03.23.01 :** ベンダが提供する文書は、すべての認証方法及びそれに対応する 1 分間のランダムな試行における成功の確率を示さなければならない。

**試験手順要件**

**TE03.23.01:** 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 未満又は、示された値未満であることを検証しなければならない。

**AS03.24: (レベル 2・3・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、あいまいにしなければならない（例えば、パスワード入力の際に文字列の表示が見えない。）。

**ベンダ情報要件**

**VE03.24.01:** 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あいまい化するために使用される方法を示さなければならない。

**試験手順要件**

**TE03.24.01:** 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、認証データがあいまい化されていることを検証しなければならない。

**TE03.24.02:** 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。

**AS03.25: (レベル 2・3・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、認証の成功又は失敗の事実以上の情報を提供することで、認証メカニズムの強度を弱めてはならない。

**ベンダ情報要件**

**VE03.25.01:** 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ときに使用されるフィードバックメカニズムを示さなければならない。

**試験手順要件**

**TE03.25.01:** 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。

**TE03.25.02:** 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。

**AS03.26: (レベル 1)**

暗号モジュールが、認証メカニズムをサポートしない場合には、暗号モジュールは、オペレータが一つ以上の役割を暗黙的又は明示的に選択すること要求しなければならない。

**ベンダ情報要件**

**VE03.26.01:** ベンダは、暗号モジュールのために行われ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、役割又は役割の集合の暗黙的又は明示的な選択、及びその役割を担うオペレータの認証に用いられるメカニズムを文書化しなければならない。

**VE03.26.02:** ベンダが提供する公開用セキュリティポリシーは、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。

**VE03.26.03:** ベンダが提供する公開用セキュリティポリシーは、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。

**試験手順要件**

**TE03.26.01:** 試験者は、ベンダが提供した公開用セキュリティポリシーが、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。

**TE03.26.02:** 試験者は、ベンダが提供した公開用セキュリティポリシー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。

**AS03.27: (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。

**注記** この個別要件は、**AS03.13**の一部として試験される。

**AS03.28: (レベル 3・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。

**注記** この個別要件は、**AS03.16** 及び **AS3.17** の一部として試験される。

#### 6.4 有限状態モデル

**AS04.01: (レベル 1・2・3・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）を用いて示されなければならない。

状態遷移図及び／又は状態遷移表は、次を含む。

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

#### ベンダ情報要件

**VE04.01.01:** ベンダは、有限状態モデル記述を提供しなければならない。この記述はモジュールのすべての状態とその遷移の記述及び識別を含まなければならない。状態遷移記述は、モジュール内部状態、ある状態から別の状態に遷移する原因となるデータ入力、制御入力、ある状態から別の状態に遷移した結果のデータ出力、ステータス出力を含まなければならない。

**VE04.01.02:** ベンダが提供する文書は、次の完全な記述を提示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) クリプトオフィサー役割
- 6) ユーザ役割
- 7) その他の役割（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) その他の認可されたサービス、オペレーション、機能（該当する場合）

- 12) エラーステータス
- 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 (該当する場合)
- 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) 未初期化状態 (該当する場合)

#### 試験手順要件

**TE04.01.01:** 試験者は、ベンダが有限状態モデルの説明を提供していることを検証しなければならない。この説明はモジュールのすべての状態の識別及び記述、及びすべての対応する状態遷移の記述を含まなければならない。試験者は状態遷移記述が、暗号モジュール内部状態、ある状態から別の状態に遷移する要因となるデータ入力、制御入力、及びある状態から別の状態に遷移した結果のステータス出力を含むことを検証しなければならない。

**TE04.01.02:** 試験者は、有限状態図とその記述が次の各項を記述しなければならないベンダが提供する文書と整合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) クリプトオフィサー役割
- 6) ユーザ役割
- 7) その他の役割 (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) その他の認可されたサービス、オペレーション、機能 (該当する場合)
- 12) エラーステータス
- 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 (該当する場合)
- 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) 未初期化状態 (該当する場合)

**TE04.01.03:** 試験者は、有限状態図で識別されたすべての状態がその説明書の中でも識別され記述されていることを検証しなければならない。

**TE04.01.04:** 試験者は、説明書で識別され記述されているすべての状態が、有限状態図でも識別されていることを検証しなければならない。

**TE04.01.05:** 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書と一致していることを検証し

なければならない。

**TE04.01.06:** 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、試験者は有限状態モデルが少なくとも一つのメンテナンス状態を定義していることを検証しなければならない。すべてのメンテナンス状態が有限状態図に含まれ、かつ、有限状態モデルの説明書に記述される必要がある。

**TE04.01.07:** 試験者は、その記述が明確に状態の分離を定義しているかどうか判定するために暗号モジュールの状態の記述を調査しなければならない。試験者はすべての可能なデータ入力と制御入力との組合せが状態を分けることを検証しなければならない。

**TE04.01.08:** 試験者は、暗号モジュールを動作させて主要な各状態に遷移させなければならない。別個の状態表示をもつ各状態につき、試験者は暗号モジュールがその状態にある間に状態表示の観察を試みなければならない。期待される状態表示が観察されない場合、又は二つ以上の状態表示が同時に観察される（暗号モジュールが同時に二つ以上の状態にいることを示している）場合、この試験は失敗である。

**TE04.01.09:** 試験者は電源投入初期状態から、それ以外の各状態への一連の状態遷移があることを検証しなければならない。

**TE04.01.10:** 試験者は電源オフ状態でない各状態から電源オフ状態への一連の状態遷移があることを検証しなければならない。

**TE04.01.11:** 試験者は、すべての可能なデータ入力及び制御入力の結果として、有限状態モデルの振る舞いが定義されていることを検証しなければならない。許容範囲内の説明の一例は、“他のすべてのデータ、制御入力の組み合わせの結果、有限状態モデルの振る舞いは ERROR3 状態になることである。”

#### AS04.02 : (レベル 1・2・3・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。

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

**注記** この個別要件は、AS04.01 の一部として試験される。

#### AS04.03 : (レベル 1・2・3・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。

#### 試験手順要件

**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。

ない。この試みは、次の二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確認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確認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・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。

**注記** この個別要件は、AS04.01の一部として試験される。

**6.5 物理的セキュリティ****AS05.01 : (レベル 1・2・3・4)**

暗号モジュールは、物理的セキュリティのメカニズムを用いて、実装後の暗号モジュールの内容への認可されていない物理的なアクセスを制限し、実装後の暗号モジュールの認可されていない使用又は変更（暗号モジュール全体の置き換えを含む。）を防がなければならない。

**ベンダ情報要件**

**VE05.01.01:** ベンダが提供する文書は、暗号モジュールに採用された該当する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。暗号モジュールの内容はすべてのハードウェア、ファームウェア、ソフトウェア及び（CSPを含む。）データを含めて保護されなければならない。

**試験手順要件**

**TE05.01.01:** 試験者は、ベンダが提供する文書が暗号モジュールに採用された該当する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。

**AS05.02 : (レベル 1・2・3・4)**

暗号境界内のすべてのハードウェア、ソフトウェア、ファームウェア及びデータ構成要素は保護されなければならない。

**注記** この個別要件は、単独では試験されない。

**AS05.03 : (レベル 1・2・3・4)**

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

- ・ 攻撃後。ただし視覚的な形跡（すなわち、タンパー証跡）を残す仕組みが設けてある場合。
- ・ **AS05.04**

**注記** この個別要件は、単独では試験されない。

**AS05.04 : (レベル 1・2・3・4)**

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

- **AS05.03**
- 攻撃の最中。ただし、CSP 及び PSP を保護するために、暗号モジュールによって適切な即座の動作（すなわち、タンパー応答）がとれる場合。

**注記** この個別要件は、単独では試験されない。

**AS05.05 : (レベル 1・2・3・4)**

その即座の動作（**AS05.04** の場合）は、CSP 及び PSP の読出しが不可能であることを意味しなければならない。

**注記** この個別要件は、単独では試験されない。

**6.5.1 共通の物理的セキュリティ要求事項****AS05.06 : (レベル 1・2・3・4)**

**AS05.07** から **AS05.23** までの要求事項は、すべての物理的な形態に対して適用しなければならない。

**注記** この個別要件は、単独では試験されない。

**AS05.07 : (レベル 1・2・3・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示さなければならない。

**ベンダ情報要件**

**VE05.07.01:**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[JIS X 19790 の 7.5（**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]を示さなければならない。示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、更に暗号モジュールがどのセキュリティレベル（1～4）を満たそうとしているのかを述べなければならない。

**試験手順要件**

**TE05.07.01:**試験者は、ベンダが、暗号モジュールが **JIS X 19790** の 7.5（**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、次に規定する三つの基準のうちの一つを満足することを独立に判定しなければならない。三つの物理的な形態を決定する基本的な特徴、及び幾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単体の集積回路、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み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 チップをもつスマートカード, 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: 二つ又はそれ以上の IC チップが相互接続されて, 物理的に保護されていない可能性のある他の製品又は囲い内に物理的に組み込まれている。

3) マルチチップスタンドアロン型暗号モジュール

特徴: 二つ又はそれ以上の IC チップが相互接続されて, 物理的に完全に保護されている囲い内に物理的に組み込まれている。

**TE05.07.02:** 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。

**AS05.08: (レベル 1・2・3・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物理的アクセス (例えば, 暗号モジュールのベンダ又は他の認可された個人によるもの。) を許すように設計されている場合には, 次の事項を適用する。

- ・ 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。
- ・ **AS05.09**
- ・ **AS05.10**
- ・ **AS05.11**

**ベンダ情報要件**

**VE05.08.01:** ベンダが提供する文書は, 暗号モジュールが採用す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。

**試験手順要件**

**TE05.08.01:** 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。

**TE05.08.02:** 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。

**AS05.09: (レベル 1・2・3・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物理的アクセス (例えば, 暗号モジュールのベンダ又は他の認可された個人によるもの。) を許すように設計されている場合には, 次の事項を適用する。

- ・ **AS05.08**
- ・ メンテナンスアクセスインタフェースは, あらゆる除去可能なカバー又はドアを含む, 暗号モジュールの内容へのすべての物理アクセス経路を含んでいなければならない。
- ・ **AS05.10**
- ・ **AS05.11**

**ベンダ情報要件**

**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, 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示さなければならない。

**試験手順要件**

**TE05.09.01**：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。

**AS05.10：（レベル 1・2・3・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物理的アクセス（例えば、暗号モジュールのベンダ又は他の認可された個人によるもの。）を許すように設計されている場合には、次の事項を適用する。

- ・ **AS05.08**
- ・ **AS05.09**
- ・ メンテナンスアクセスインタフェース内に含まれるあらゆる除去可能なカバー又はドアは、適切な物理的セキュリティメカニズムを用いて保護されなければならない。
- ・ **AS05.11**

**ベンダ情報要件**

**VE05.10.01**：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内に含まれるあらゆる除去可能なカバー若しくはドアが、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るように、物理的な保護を示さなければならない。

**試験手順要件**

**TE05.10.01**：試験者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が、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ていることを検証しなければならない。

**AS05.11：（レベル 1・2・3・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物理的アクセス（例えば、暗号モジュールのベンダ又は他の認可された個人によるもの。）を許すように設計されている場合には、次の事項を適用する。

- ・ **AS05.08**
- ・ **AS05.09**
- ・ **AS05.10**
- ・ メンテナンスアクセスインタフェースがアクセスされたとき、すべての CSP はゼロ化されなければならない。

**ベンダ情報要件**

**VE05.11.01**：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 CSP がどのようにゼロ化されるかを示さなければならない。

**試験手順要件**

**TE05.11.01**：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 CSP がどのようにゼロ化されるかを示していることについて検証しなければならない。

**TE05.11.02**：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、すべての CSP 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。

**AS05.12 : (レベル 1)**

AS05.13 から AS05.15 までの要求事項は、セキュリティレベル 1 のすべての暗号モジュールに適用しなければならない。

**注記** この個別要件は、単独では試験されない。

**AS05.13 : (レベル 1・2・3・4)**

暗号モジュールは、表面安定化処理（例えば、環境又はその他の物理的損害から保護するために、暗号モジュールの回路に施されている絶縁保護コーティング又はシーリングコート。）を含んだ製品グレードの構成要素で構成されなければならない。

**ベンダ情報要件**

**VE05.13.01 :** 暗号モジュールは、電力、温度、信頼性、衝撃、振動などにおいて商用グレードの仕様に満たすように設計された標準的な製品品質の 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。

**試験手順要件**

**TE05.13.01 :** 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。

**TE05.13.02 :** 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ことを示すための情報を提供しなければならない。

**AS05.14 : (レベル 1・2・3・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すべての CSP はゼロ化されなければならない。

**注記** この個別要件は、AS05.11 の一部として試験される。

**AS05.15 : (レベル 1・2・3・4)**

そのゼロ化は、オペレータによって手続的に行われるか、又は暗号モジュールによって自動的行われなければならない。

**注記** この個別要件は、単独では試験されない。

**AS05.16 : (レベル 2・3・4)**

セキュリティレベル 1 の共通の要求事項に加え、AS05.17 の要求事項はセキュリティレベル 2 のすべての暗号モジュールに適用しなければならない。

**注記** この個別要件は、単独では試験されない。

**AS05.17 : (レベル 2・3・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。

**注記** この個別要件は、シングルチップ形態については **AS05.25** の一部として、マルチチップ組込型形態については **AS05.35** 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 **AS05.54** の一部として試験される。

**AS05.18 : (レベル 3・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、**AS05.19** から **AS05.22** までの要求事項はセキュリティレベル 3 のすべての暗号モジュールに適用しなければならない。

**注記** この個別要件は、単独では試験されない。

**AS05.19 : (レベル 3・4)**

暗号モジュールがドア若しくは除去可能なカバーを含むか、又はメンテナンスアクセスインタフェースが定義されている場合には、暗号モジュールはタンパー応答及びゼロ化機能を含まなければならない。

**注記** この個別要件は、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 **AS05.42** 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 **AS05.57** の一部として試験される。

**AS05.20 : (レベル 3・4)**

そのタンパー応答及びゼロ化機能は、ドアを開けられたとき、カバーが取り外されたとき、又はメンテナンスアクセスインタフェースがアクセスされたとき、すべての CSP を速やかにゼロ化しなければならない。

**注記** この個別要件は、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 **AS05.41** 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 **AS05.55** の一部として試験される。

**AS05.21 : (レベル 3・4)**

そのタンパー応答及びゼロ化機能は、CSP が暗号モジュール内に含まれているときは、作動していなければならない。

**注記** この個別要件は、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。

**AS05.22 : (レベル 3・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、少なくとも一つ以上の 90 度の曲げ、又は堅固な保護素材による障害物を必要とする。）。

**ベンダ情報要件**

**VE05.22.01 :** 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。

#### 試験手順要件

**TE05.22.01**：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もっ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。

#### AS05.23：（レベル 4）

セキュリティレベル 1, 2 及び 3 の共通の要求事項に加え、暗号モジュールは、セキュリティレベル 4 のために JIS X 19790 の 7.5.2 で規定された、環境故障保護(EFP)特性を含むか、又は環境故障試験(EFT)を受けなければならない。

**注記 1** この個別要件は、AS05.60～AS05.63 の一部として試験される。

#### 6.5.1.1 シングルチップ暗号モジュール

**注記** JIS X 19790 の 7.5.1 で規定される一般的セキュリティ要件に加えて、AS05.24 から AS05.32 がシングルチップ暗号モジュールに特有の要件である。

**注記** 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・4）

セキュリティレベル 1 の要求事項に加え、AS05.25 から AS05.26 までの要求事項は、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。

**注記** この個別要件は、単独では試験されない。

#### AS05.25：（シングルチップ—レベル 2・3・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、又は不正操作を防ぐために、及びタンパーの試みの証拠又は暗号モジュールの除去証拠を提供するために、タンパー証跡を残すコーティング（例えば、タンパー証跡を残す表面安定化処理の材料、又は表面安定化処理を覆うタンパー証跡を残す材料）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。

**注記** この要求事項は、AS05.17 と関連している。

#### ベンダ情報要件

**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。

#### 試験手順要件

**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・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（すなわち、波長が 400 nm～750 nm の範囲の光）においては不透明でなければならない。

**ベンダ情報要件**

**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。

**試験手順要件**

**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・4）**

セキュリティレベル 1 及び 2 の要求事項に加え、**AS05.28** 又は **AS05.29** のいずれかの要求事項を、セキュリティレベル 3 のシングルチップ暗号モジュールに適用しなければならない。

**ベンダ情報要件**

**VE05.27.01**：ベンダが提供する文書は、**AS05.28** 及び **AS05.29** で規定されている二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明記しなければならない。

**試験手順要件**

**TE05.27.01**：試験者は、検査によって及びベンダが提供する文書から、**AS05.28** 及び **AS05.29** で規定されている二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検証しなければならない。

**TE05.27.02**：**AS05.28** が適用される場合、試験者は **TE05.29** ではなく **TE05.28** に示される手続に従わなければならない。また、**AS05.29** が適用される場合、試験者は **TE05.28** ではなく **TE05.29** に規定される手続に従わなければならない。

**AS05.28：（シングルチップ—レベル 3・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、表面安定化処理を覆った堅く不透明なエポキシ樹脂）で覆われていなければならない（**AS05.29** を満足させることでもよい）。

**ベンダ情報要件**

**VE05.28.01**：ベンダが提供する文書は、**AS05.28** で規定されている方法が要求事項を満たすために使われていることを明記しなければならない。

**VE05.28.02**：ベンダが提供する文書は、詳細な設計情報（特に使用されているコーティング材の種類とその特性）を示さなければならない。

**試験手順要件**

**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。

**TE05.28.02**：試験者は、ベンダが提供する文書が、詳細な設計情報（特に使用されているコーティングの種類及びその特性）を示していることを検証しなければならない。

**TE05.28.03**：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。

**AS05.29 : (シングルチップレベル 3・4)**

暗号モジュールの囲いは、その除去又は貫通の攻撃が高い確率で暗号モジュールに重大な損害を与える（すなわち、暗号モジュールが機能しなくなる。）ように設計されていなければならない（**AS05.28** を満足させることでもよい）。

**注記** これらの要求事項は、**AS05.19**、**AS05.20**、**AS05.21** と関連している。

**ベンダ情報要件**

**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示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、すべての CSP をゼロ化しなければならない。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。

**試験手順要件**

**TE05.29.01** : 試験者は、文書が、囲いが容易に取り外せないこと、及び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もつかどうかを示していることを検証しなければならない。その囲い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もつ場合には、試験者はベンダが提供する文書が、暗号モジュールがタンパー応答及びゼロ化回路を含まれるべきことを示していることを検証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もつか、又はメンテナンスアクセスインタフェースが示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時、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時に、暗号モジュールがすべての CSP 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、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もつか、又はメンテナンスアクセスインタフェースが示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時、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、暗号モジュールがすべての CSP をゼロ化することを試験しなければならない。

**注記** この試験は、次の一つ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でき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、除去又は貫かれなことを試験しなければならない。

**注記** TE05.29.05 の注記に同じ。

**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、**AS05.31** から **AS05.32** まで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。

**注記** この個別要件は、単独では試験されない。

**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はがそうとする試み、又はこじ開けようとする試みが、高い確率で暗号モジュールに重大な損害を与える（すなわち、暗号モジュールが機能しなくなる。）ような硬度及び接着特性をもった、堅く不透明で除去耐性のあるコーティングで覆われているなければならない。

**ベンダ情報要件**

**VE05.31.01：**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を識別すると共にその特性、特に硬度及び除去耐性の詳細情報を提供しなければならない。

**VE05.31.02：**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はがそうとする試み、又はこじ開けようとする試みが、高い確率で暗号モジュールに重大な損害を与える（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。

**試験手順要件**

**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示して、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はがすこと、又はこじ開けることを試みて、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。

**注記** TE05.29.05 の注記に同じ。

**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、暗号モジュールが機能しなくなる。）ような溶解特性をもたなければならない。

**ベンダ情報要件**

**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。

**試験手順要件**

**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、**VE05.33.01** 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たい化するために必要かを判定しなければならない。

**注記 TE05.29.05 の注記**に同じ。

**6.5.1.2 マルチチップ組込型暗号モジュール**

**注記 JIS X 19790 の 7.5.1 の一般的セキュリティ要件に加えて、AS05.33 から AS05.49 がマルチチップ組込型に特有の要件である。**

**AS05.33：（マルチチップ組込型－レベル 1・2・3・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。

**ベンダ情報要件**

**VE05.33.01**：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。

**試験手順要件**

**TE05.33.01**：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。

**AS05.34：（マルチチップ組込型－レベル 2・3・4）**

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

- a) AS05.35 及び AS05.36
- b) AS05.37, AS05.38, 及び AS05.39
- c) AS05.37, AS05.38, 及び AS05.40

**ベンダ情報要件**

**VE05.34.01**：ベンダが提供する文書は、次のいずれかの要件の組合せが満足されるかを示さなければならない。

- a) AS05.35 及び AS05.36
- b) AS05.37, AS05.38 及び AS05.39
- c) AS05.37, AS05.38 及び AS05.40

**試験手順要件**

**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、次のいずれかの要件の組合せが満足されていることを検証しなければならない。

- a) AS05.35 及び AS05.36
- b) AS05.37, AS05.38 及び AS05.39
- c) AS05.37, AS05.38 及び AS05.40

**AS05.35：（マルチチップ組込型－レベル 2・3・4）**

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

**ベンダ情報要件**

**VE05.35.01：**ベンダが提供する文書は、暗号モジュールが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することを示さなければならない。

**試験手順要件**

**TE05.35.01：**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。

**TE05.35.02：**試験者は、試験によって、暗号モジュールが、暗号モジュール構成要素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。

**AS05.36：（マルチチップ組込型－レベル 2・3・4）**

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

**注記** この要求事項は、AS05.17 と関連している。

**ベンダ情報要件**

**VE05.36.01：**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。

**試験手順要件**

**TE05.36.01：**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。

**AS05.37：（マルチチップ組込型－レベル 2・3・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。

**ベンダ情報要件**

**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。ベンダ作成文書は、囲いとその堅さ特性を記述しなければならない。

**試験手順要件**

**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。

**AS05.38 : (マルチチップ組込型－レベル 2・3・4)**

その囲いは、可視領域内において不透明でなければならない。

**ベンダ情報要件**

**VE05.38.01 :** 囲いは可視光領域内で不透明でなければならない。ベンダ提供文書は、囲いの不透明特性を記述しなければならない。

**試験手順要件**

**TE05.38.01 :** 試験者は、検査によって及びベンダが提供する文書から、囲いが可視光領域内で不透明であることを検証しなければならない。

**AS05.39 : (マルチチップ組込型－レベル 2・3・4)**

その囲いが、ドア又は除去可能なカバーを含む場合には、ドア又はカバーは、物理的若しくは論理的鍵を用いたこじ開け耐性のある機械的錠が掛けられていなければならない。

**ベンダ情報要件**

**VE05.39.01 :** 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。

**試験手順要件**

**TE05.39.01 :** 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、次の二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) または、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、シールを破る又はは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。

**AS05.40 : (マルチチップ組込型－レベル 2・3・4)**

その囲いが、ドア又は除去可能なカバーを含む場合には、ドア又はカバーは、タンパー証跡を残すシール（例えば、証跡性テープ、ホログラフシール）で保護されていないなければならない。

**注記** この要求事項は、AS05.17 と関連している。

**ベンダ情報要件**

**VE05.40.01 :** 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。

**試験手順要件**

**TE05.40.01 :** 試験者は、カバー又はドアが、シールを破る又はは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。

**AS05.41 : (マルチチップ組込型－レベル 3・4)**

セキュリティレベル 1 及び 2 の要求事項に加え、**AS05.42** 又は **AS05.43** のいずれかの要求事項を、セキュリティレベル 3 のマルチチップ組込型暗号モジュールに適用しなければならない。

**注記 1** この個別要件は、単独では試験されない。

**注記 2** **TE05.42.01**, **TE05.42.02**, **TE05.43.04**, **TE05.42.05**, **TE05.42.09**, 及び **TE05.42.10** は, **AS05.19**, **AS05.20**, 及び **AS05.21** と関連している。

**AS05.42 : (マルチチップ組込型－レベル 3・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。

**ベンダ情報要件**

**VE05.42.01** : ベンダが提供する文書は、**AS05.42** 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を明記し、また、その方法をサポートしている設計文書を提供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、すべての保護されない CSP をゼロ化しなければならない。回路は、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。

**試験手順要件**

**TE05.42.01** : 試験者は、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もつ場合には、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、ベンダが提供する文書が示していることを検証しなければならない。

**TE05.42.02** : 囲いが除去可能なカバー若しくはドアをもつか、又はメンテナンスアクセスインタフェースが示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時、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、すべての CSP をゼロ化することを検証しなければならない。

**TE05.42.03** : 試験者は、ベンダが提供する文書が、**VE05.42.01** のどの選択要求事項が実装されているかを示して、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。

**TE05.42.04** : 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 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。

**TE05.42.05** : 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、又は貫かれなことを検証しなければならない。

**TE05.42.06** : (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示さなければならない。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。

**注記 TE05.29.05** の注記に同じ。

**TE05.42.07:** (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。

**注記 TE05.29.05** の注記に同じ。

**TE05.42.08:** (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もつ場合には、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、暗号モジュールがすべての CSP をゼロ化することを検証しなければならない。

**注記 TE05.29.05** の注記に同じ。

**TE05.42.09:** 囲いが、ドア若しくは除去可能なカバーをもつか、又はメンテナンスアクセスインタフェースが示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、暗号モジュールがすべての CSP をゼロ化することを試験しなければならない。

**注記 TE05.29.05** の注記に同じ。

**TE05.42.10:** 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。

**注記 TE05.29.05** の注記に同じ。

#### **AS05.43: (マルチチップ組込型—レベル 3・4)**

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 (AS05.57) が、適用されなければならない (JIS X 19790 の 7.5.1.3)。

**注記** この個別要件は、単独では試験されない。

#### **AS05.44: (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、AS05.45 から AS05.49 までの要求事項は、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。

**注記** この個別要件は、単独では試験されない。

#### **AS05.45: (マルチチップ組込型—レベル 4)**

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

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

**ベンダ情報要件**

**VE05.45.01**：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包被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、タンパー検出包被の設計について記述しなければならない。

#### 試験手順要件

**TE05.45.01**：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、暗号モジュール構成要素を覆っているタンパー検出包被を含んでいることを検証しなければならない。この包被バリアは、暗号モジュール構成要素へアクセスするための掘削、粉碎、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構成要素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。

#### AS05.46：（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。タンパー応答及びゼロ化回路は、タンパー検出包被を継続的に監視しなければならない。

#### ベンダ情報要件

**VE05.46.01**：暗号モジュールは、タンパー応答及びゼロ化回路を含み、タンパー検出包被を継続的に監視しなければならない。タンパー検出時には、すべての CSP をゼロ化しなければならない。タンパー応答及びゼロ化回路は CSP が暗号モジュール内に含まれる場合は継続的に動作しなければならない。ベンダ提出文書はタンパー応答及びゼロ化回路の設計について記述しなければならない。

#### 試験手順要件

**TE05.46.01**：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応答及びゼロ化回路を含み、それがタンパー検出包被を継続的に監視し、掘削、粉碎、研削、又は溶解のような方法によるあらゆる破損を検出し、すべての CSP をゼロ化することを検証しなければならない。

#### AS05.47：（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、そのタンパー応答及びゼロ化回路は、速やかにすべての CSP をゼロ化しなければならない。

#### ベンダ情報要件

**VE05.47.01**：暗号モジュールは、タンパーの有無をタンパー検出包被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、すべての CSP をゼロ化しなければならない。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。

#### 試験手順要件

**TE05.47.01**：試験者は、タンパー検出包被を壊し、及びその結果、試験者は暗号モジュールがすべての CSP をゼロ化することを検証しなければならない。

**注記** TE05.29.05 の注記に同じ。

#### AS05.48：（マルチチップ組込型－レベル 4）

そのタンパー応答回路は、平文の秘密鍵及びプライベート鍵、又はその他の保護されていない CSP が暗号モジュール内に含まれているときは、作動していなければならない。

**注記** この個別要件は、単独では試験されない。

#### AS05.49：（マルチチップ組込型－レベル 4）

そのゼロ化機能は、CSP が暗号モジュール内に含まれているときは、作動していなければならない。

**注記** この個別要件は、単独では試験されない。

### 6.5.1.3 マルチチップスタンドアロン型暗号モジュール

**注記** JIS X 19790 の 7.5.1 の共通のセキュリティ要件に加えて、AS05.50 から AS05.63 がマルチチップスタンドアロン型に特有の要件である。

#### AS05.50：（マルチチップスタンドアロン型－レベル 1・2・3・4）

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

#### ベンダ情報要件

**VE05.50.01**：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。

#### 試験手順要件

**TE05.50.01**：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。

#### AS05.51：（マルチチップスタンドアロン型－レベル 2・3・4）

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

- a) AS05.52 及び AS05.53
- b) AS05.52 及び AS05.54

**注記** この個別要件は、単独では試験されない。

#### AS05.52：（マルチチップスタンドアロン型－レベル 2・3・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。

#### ベンダ情報要件

**VE05.52.01**：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。

#### 試験手順要件

**TE05.52.01**：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。

**注記** AS05.53 又は AS05.54 のいずれかが満足されなければならない。

#### AS05.53：（マルチチップスタンドアロン型－レベル 2・3・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なければならない。

#### ベンダ情報要件

**VE05.53.01**：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に、物理的又は論理的な鍵を用いる、こじ開け耐性のある機械的錠が掛けられていなければならない。ベンダが提供する文書は、物理的又は論理的な鍵を用いる、こじ開け耐性のある機械的錠について記述しなければならない。

#### 試験手順要件

**TE05.53.01**：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、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ことを検証しなければならない。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。

#### AS05.54：（マルチチップスタンドアロン型－レベル 2・3・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、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。

#### ベンダ情報要件

**VE05.54.01**：囲いが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る場合には、ベンダが提供する文書は、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。

#### 試験手順要件

**TE05.54.01**：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。

#### AS05.55：（マルチチップスタンドアロン型－レベル 3・4）

セキュリティレベル 1 及び 2 の要求事項に加え、**AS05.56** 又は **AS05.57** のいずれかの要求事項を、セキュリティレベル 3 のマルチチップスタンドアロン型暗号モジュールに適用しなければならない。

**注記** この個別要件は、単独では試験されない。

#### AS05.56：（マルチチップスタンドアロン型－レベル 3・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。

#### ベンダ情報要件

**VE05.56.01**：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。

#### 試験手順要件

**TE05.56.01**：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不透明な堅い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示さなければならない。

**TE05.56.02**：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。

**AS05.57：（マルチチップスタンドアロン型－レベル 3・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。

**注記** TE05.57.01, TE05.57.02, TE05.57.04, TE05.57.05, TE05.57.08, 及び TE05.57.09 は, AS05.19, AS05.20 及び AS05.21 と関連している。

**ベンダ情報要件**

**VE05.57.01：**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、平文のすべて、CSP のすべてをゼロ化しなければならない。その回路は、平文の 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。

**試験手順要件**

**TE05.57.01：**試験者は、検査によって及びベンダが提供する文書から、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、除去又は貫かれなことを検証しなければならない。

**TE05.57.02：**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。

**注記** TE05.29.05 の注記に同じ。

**TE05.57.03：**強固な囲いが、除去可能なカバー又はドアをもつ場合には、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すべて、CSP のすべてをゼロ化することを検証しなければならない。

**注記** TE05.29.05 の注記に同じ。

**TE05.57.04：**囲いが、除去可能なカバー又はドアをもつか、又はメンテナンスアクセスインタフェースが示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すべて、CSP のすべてをゼロ化することを試験しなければならない。

**注記** TE05.29.05 の注記に同じ。

**TE05.57.05：**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。

**注記** TE05.29.05 の注記に同じ。

**AS05.58：（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, AS05.59 から AS05.63 までの要求事項は, 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。

**注記** この個別要件は、単独では試験されない。

**AS05.59 : (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、タンパー検出包被によって、すなわち、カバースイッチ（カバースイッチの例には、マイクロスイッチ、磁気ホール効果スイッチ、永久磁石アクチュエータなどがある。）、モーション検出器（モーション検出器の例には、超音波、赤外線、又は電磁波がある。）、又は前述のマルチチップ組込型暗号モジュールで記述されたその他のタンパー検出メカニズムのようなタンパー検出メカニズムの使用によって、カプセル化されなければならない。

**ベンダ情報要件**

**VE05.59.01 :** 囲い又は封止材は、タンパー検出包被によって、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、タンパー検出包被の設計について記述しなければならない。

**試験手順要件**

**TE05.59.01 :** 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、暗号モジュール構成要素を保護する、タンパー検出包被を形成しなければならない。そのメカニズムは、暗号モジュール構成要素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。

**AS05.60 : (マルチチップスタンドアロン型—レベル 4)**

そのタンパー検出メカニズムは、平文の秘密鍵及びプライベート鍵、並びにその他の保護されていない CSP にアクセスするのに十分なタンパー（封止材又は囲いの切削、掘削、粉碎、研削、又は溶解のような方法による。）を検出しなければならない。

**注記** この個別要件は、単独では試験されない。

**AS05.61 : (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機能を含まなければならない。タンパー応答及びゼロ化回路は、タンパー検出包被を継続的に監視して、タンパーを検出したとき、速やかに、すべての CSP をゼロ化しなければならない。

**ベンダ情報要件**

**VE05.61.01 :** 暗号モジュールは、タンパーの有無をタンパー検出包被で継続的に監視しているタンパー応答及びゼロ化機能を含み、かつ、タンパーが検出されるとき、すべての保護されない CSP をゼロ化しなければならない。タンパー応答ゼロ化機能は、保護されない 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。ゼロ化機能は、CSP が暗号モジュール内に含まれているときは、作動していなければならない。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。

**試験手順要件**

**TE05.61.01 :** 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の有無をタンパー検出包被で継続的に監視し、包被のいかなる部分の切削、掘削、粉碎、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、その結果、すべての保護されない CSP をゼロ化するタンパー応答及びゼロ化機能を含んでいることを検証しなければならない。

**TE05.61.02 :** 試験者は、タンパー検出包被のバリアを壊し、その結果、試験者は暗号モジュールがすべ

ての CSP をゼロ化することを検証しなければならない。

**注記** TE05.29.05 の注記に同じ。

**AS05.62 : (マルチチップスタンドアロン型—レベル 4)**

そのタンパー応答機能は、CSP 及び／又は PSP が暗号モジュール内に含まれているときは、作動していなければならない。

**注記** この個別要件は、単独では試験されない。

**AS05.63 : (マルチチップスタンドアロン型—レベル 4)**

そのゼロ化機能は、CSP が暗号モジュール内に含まれているときは、作動していなければならない。

**注記** この個別要件は、単独では試験されない。

**6.5.2 環境故障保護・環境故障試験**

**AS05.64 : (レベル 4)**

暗号モジュールは、環境故障保護(EFP)特性 (AS05.65 から AS05.69 まで) を用いるか、又は環境故障試験(EFT) (AS05.70 から AS05.74 まで) を受けなければならない。

**注記** この個別要件は、単独では試験されない。

**6.5.2.1 環境故障保護特性 (選択 1)**

**AS05.65 : (レベル 4)**

環境故障保護(EFP)特性 (AS05.66 から AS05.69 まで) は、暗号モジュールのセキュリティを危たい化させる可能性がある異常な環境条件又は暗号モジュールの正規の動作範囲外の (偶然又は故意の) 環境変動に対して、暗号モジュールを保護しなければならない。

**注記** この個別要件は、AS05.64 の一部として試験される。

**AS05.66 : (レベル 4)**

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

**注記** この個別要件は、AS05.64 の一部として試験される。

**AS05.67 : (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的な機能又はデバイスをもたなければならない。

**注記** この個別要件は、AS05.64 の一部として試験される。

**AS05.68 : (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、保護機能は、(1) それ以上動作しないように暗号モジュールをシャットダウンするか、又は、(2) すべての CSP を、即座にゼロ化しなければならない。

**ベンダ情報要件**

**VE05.68.01 :** 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。保護機能は、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、保護機能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) すべての平文の秘密鍵、プライベート鍵、及びその他の保護されていない CSP 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を明記し、また、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。

#### 試験手順要件

**TE05.68.01**：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タ内で実行し続けることを検証しなければならない。

**注記 TE05.29.05 の注記**に同じ。

**TE05.68.02**：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すべての CSP をゼロ化することを判定しなければならない。

**注記 TE05.29.05 の注記**に同じ。

**TE05.68.03**：暗号モジュールがすべての CSP 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。

**注記 TE05.29.05 の注記**に同じ。

#### 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暗号モジュールによって用いられる環境故障保護特性を示さなければならない。

**注記** この個別要件は、**AS05.60** 及び **AS05.64** の一部として試験される。

#### 6.5.2.2 環境故障試験手順（選択 2）

#### AS05.70：（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たい化しないという合理的保証を提供するために、環境故障試験(EFT)は、暗号モジュールの解析、シミュレーション及び試験の組合せを含まなければならない。

**注記** この個別要件は、**AS05.64** の一部として試験される。

#### AS05.71：（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、故障が発生する場合には、EFT は、暗号モジュールのセキュリティが決して危たい化されないことを実証しなければならない。

**注記** この個別要件は、**AS05.64** の一部として試験される。

**AS05.72 : (レベル 4)**

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

**ベンダ情報要件**

**VE05.72.01:** 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) シャットダウンする。
- 3) すべての CSP 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を明記し、また、EFT の詳細記述を提供しなければならない。

**試験手順要件**

**TE05.72.01:** 試験者は、**AS05.68** で規定された環境条件（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すべての CSP 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。

**注記 TE05.29.05 の注記に同じ。**

**TE05.72.02:** 暗号モジュールが、すべての CSP 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。

**注記 TE05.29.05 の注記に同じ。**

**AS05.73 : (レベル 4)**

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

**注記** この個別要件は、**AS05.72** の一部として試験される。

**AS05.74 : (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示さなければならない。

**注記** この個別要件は、**AS05.72** の一部として試験される。

**6.6 動作環境**

**AS06.01 : (レベル 1・2・3・4)**

動作環境が変更可能な動作環境である場合には、**JIS X 19790** の **7.6.1** のオペレーティングシステム要求事項を適用しなければならない。

**注** 動作環境が変更不可能な場合又は限定動作環境である場合には、**JIS X 19790** の **7.6.1** のオペレーティングシステム要求事項は適用しない。

**注記** この個別要件は、単独では試験されない。

**AS06.02 : (レベル 1・2・3・4)**

文書は、暗号モジュールに対する動作環境を示さなければならない。該当する場合には、暗号モジュールに採用されるオペレーティングシステム、並びにセキュリティレベル 2, 3 及び 4 については、**JIS X 19790** の**附属書 C**に記載する承認されたプロテクションプロファイル (PP) も含めて示さなければならない。

**ベンダ情報要件**

**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。

**試験手順要件**

**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、この個別要件は不合格とする。

**AS06.03 : (レベル 1・2・3・4)**

**AS06.04** から **AS06.08** までの要求事項は、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。

**注記** この個別要件は、**AS06.04** から **AS06.08** までの一部として試験される。

**AS06.04 : (レベル 1)**

セキュリティレベル 1 だけに適用される要件として、オペレーティングシステムは、単一オペレータ動作モードに限定されなければならない（すなわち、複数同時オペレータは明示的に除外される。）。

**注記** 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。

**ベンダ情報要件**

**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。

**試験手順要件**

**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とお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)**

セキュリティレベル 1 だけに適用される要件として、暗号モジュールは、暗号モジュールが実行中又は作動している間、他のプロセスからの CSP 及び／又は PSP へのアクセスを防止しなければならない。

**注** 暗号モジュールによって引き起こされるプロセスは、暗号モジュールによって所有され、外部のプロセス・オペレータによっては所有されない。

**注記** 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。

**ベンダ情報要件**

**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 CSP 及び／又は PSP 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。

**試験手順要件**

**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とおりに暗号機能进行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、CSP 及び／又は PSP へのアクセスを試みなければならない。

**AS06.06 : (レベル 1)**

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ってはならない。

**ベンダ情報要件**

**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。

**試験手順要件**

**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とおりに暗号機能进行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・4)**

すべての暗号ソフトウェア及び暗号ファームウェアは、ソフトウェア及びファームウェアのソースコード及び実行可能コードが認可されていない開示及び変更から保護されるような形態でインストールされなければならない。

**ベンダ情報要件**

**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ェア及び暗号ファームウェアのリストを提供して、認可されていない開示及び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。

**試験手順要件**

**TE06.07.01 :** 試験者は、ソフトウェア及びファームウェアのソースコード及び実行可能コードに認可されていないアクセス及び認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・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、デジタル署名アルゴリズム）を用いた暗号メカニズムは、暗号モジュール内のすべての暗号ソフトウェア構成要素及び暗号ファームウェア構成要素に対して適用されなければならない。

**注** 承認された認証技術がソフトウェア・ファームウェア完全性テスト（JIS X 19790 の 7.8.1 参照）に採用される場合には、この暗号メカニズムの要求事項は、そのテストの一部として組込まれてもよい。

**ベンダ情報要件**

**VE06.08.01 :** ベンダは、暗号ソフトウェア構成要素及び暗号ファームウェア構成要素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。

**試験手順要件**

**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、この個別要件は不合格とする。

**TE06.08.02 :** 試験者は、暗号ソフトウェア及び暗号ファームウェアを改ざんすることを試みなければならない。完全性が維持されていると示されるならば、この TE（試験）は不合格とする。

**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で他のレベルにも適用可能なもの（すなわち上記のセキュリティレベル 1 における AS06.07 及び AS06.08 の要求事項に加え、AS06.10 から AS06.20 までの要求事項もセキュリティレベル 2 に適用しなければならない。）。

**注記** この個別要件は、AS06.10 から AS06.19 までの個別要件の一部として試験される。

**AS06.10 : (レベル 2)**

すべての暗号ソフトウェア及び暗号ファームウェア、CSP、PSP、並びに制御情報及び状態情報は、JIS X 19790 の附属書 C に記載する PP に規定された機能要件を満たし、かつ、ISO/IEC 15408 の評価保証レベル EAL2 で評価されたオペレーティングシステムの制御下に置かれなければならない。

**ベンダ情報要件**

**VE06.10.01 :** ベンダは、当該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、JIS X 19790 の附属書 C に記載する PP に規定された機能要件に対して ISO/IEC 15408 の評価保証レベル EAL2 の評価に合格したことを示す文書を提供しなければならない。

**試験手順要件**

**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って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・4)**

平文データ、暗号ソフトウェア及び暗号ファームウェア、CSP、並びに PSP を保護するため、オペレーティングシステムの任意アクセス制御メカニズムは、次の役割が果たせるように構成されていなければならない。

- 1) 格納されている暗号ソフトウェア及び暗号ファームウェアの実行。

**ベンダ情報要件**

**VE06.11.01**：ベンダ情報要件は、**VE06.14.01** で規定する。

#### 試験手順要件

**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ェア構成要素及び暗号ファームウェア構成要素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ェア構成要素及び暗号ファームウェア構成要素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ェア構成要素及び暗号ファームウェア構成要素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ェア構成要素及び暗号ファームウェア構成要素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ェア構成要素及び暗号ファームウェア構成要素を実行できる場合には、この個別要件は不合格とする。

#### **AS06.12**：（レベル 2・3・4）

平文データ、暗号ソフトウェア及び暗号ファームウェア、CSP、並びに PSP を保護するため、オペレーティングシステムの任意アクセス制御メカニズムは、次の役割が果たせるように構成されていなければならない。

- 2) 暗号境界内に格納されている、次の暗号モジュールのソフトウェア構成要素又はファームウェア構成要素の変更（書き込み、置換及び削除）。
  - ・ 暗号プログラム
  - ・ 暗号データ（例えば、監査データ）
  - ・ CSP
  - ・ PSP
  - ・ 平文データ

#### ベンダ情報要件

**VE06.12.01**：ベンダ情報要件は、**VE06.14.01** で規定する。

#### 試験手順要件

**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ェア構成要素及びファームウェア構成要素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、監査データ）
- 3) CSP
- 4) PSP
- 5) 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ェア構成要素及びファームウェア構成要素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ェア構成要素及び暗号ファームウェア構成要素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ェア構

成要素及び暗号ファームウェア構成要素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・4)**

平文データ, 暗号ソフトウェア及び暗号ファームウェア, CSP, 並びに PSP を保護するため, オペレーティングシステムの任意アクセス制御メカニズムは, 次の役割が果たせるように構成されていなければならない。

- 3) 暗号境界内に格納されている次の暗号ソフトウェア構成要素の読み取り。
  - ・ 暗号データ (例えば, 監査データ)
  - ・ CSP
  - ・ 平文データ

**ベンダ情報要件**

**VE06.13.01 :** ベンダ情報要件は, **VE06.14.01** で規定する。

**試験手順要件**

**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ェア構成要素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, 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ェア構成要素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ェア構成要素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ェア構成要素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・4)**

平文データ, 暗号ソフトウェア及び暗号ファームウェア, CSP, 並びに PSP を保護するため, オペレーティングシステムの任意アクセス制御メカニズムは, 次の役割が果たせるように構成されていなければならない。

- 4) CSP 及び／又は PSP の入力。

**ベンダ情報要件**

**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, 任意アクセス制御メカニズムがどのように構成されているかを示文書を提供しなければならない。

**試験手順要件**

**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, CSP 及び／又は PSP 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, CSP 及び／又は PSP を入力しなければならない。

**TE06.14.03 :** 試験者は, CSP 及び／又は PSP 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, CSP 及び／又は PSP の入力を試みなければならない。

**AS06.15 : (レベル 2・3・4)**

オペレーティングシステムは、すべてのオペレータ及び実行中のプロセスが、実行中の暗号プロセス（すなわち、ロードされて、実行中の暗号プログラムのコピー。）の変更を行うことを防がなければならない。

**ベンダ情報要件**

**VE06.15.01 :** ベンダは、すべてのオペレータ及び実行中のプロセスが、実行中の暗号プロセスの変更を行うことを、オペレーティングシステムがどのように防ぐかを示す文書を提供しなければならない。

**試験手順要件**

**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・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ェアの読み出しを行うことを防がなければならない。

**ベンダ情報要件**

**VE06.16.01 :** ベンダは、オペレータ及び実行中のプロセスが、暗号境界内に格納されている暗号ソフトウェアの読み出しを行うことを、オペレーティングシステムが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。

**試験手順要件**

**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ェ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ェ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・4)**

オペレーティングシステムは、暗号データ、CSP 及び PSP の変更、アクセス、削除及び追加を記録する監査メカニズムを提供しなければならない。

**注記** この個別要件の前提は、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ェ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。

**ベンダ情報要件**

**VE06.17.01 :** ベンダは、暗号モジュールソフトウェアによって監査することができるすべ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。

**試験手順要件**

**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。

**注記** 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。

**TE06.17.02**：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、すべ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・4）**

その監査メカニズムは、次のイベントを記録しなければならない。

- ・ クリプトオフィサ機能に対する無効な入力を試み。
- ・ クリプトオフィサ役割へのオペレータの追加，又はクリプトオフィサ役割からのオペレータの削除

**注記** この個別要件は、**AS06.17**の一部として試験される。

**AS06.19：（レベル 2・3・4）**

その監査メカニズムは、次のイベントの監査ができなければならない。

- ・ 監査証跡に格納された監査データを処理する操作
- ・ 認証データ管理メカニズムの使用要求
- ・ セキュリティに関係するクリプトオフィサ機能の使用
- ・ 暗号モジュールに関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
- ・ クリプトオフィサ役割への機能の割当て

**注記** この個別要件は、**AS06.17**の一部として試験される。

**AS06.20：（レベル 2・3・4）**

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

**ベンダ情報要件**

**VE06.20.01**：ベンダはどのようにして保存された監査データが認可されていないアクセスから保護されるかを示す文書を提供しなければならない。

**試験手順要件**

**TE06.20.01**：試験者は **VE06.20.01** で要求される情報が提供されていることを検証しなければならない。

**TE06.20.02**：試験者は暗号境界内に保存された監査データの読み出しを試みなければならない。試験者は、ユーザが認可を得なければ暗号境界内に保存された監査データにアクセスできないことを検証しなければならない。

**AS06.21：（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、**AS06.22** から **AS06.26** までの要求事項は、セキュリティレベル 3 に適用しなければならない。

**注記** この個別要件は、**AS06.22** から **AS06.26** の一部として試験される。

**AS06.22 : (レベル 3)**

すべての暗号ソフトウェア及び暗号ファームウェア、CSP、PSP、並びに制御情報及び状態情報は、**JIS X 19790 の附属書 C**に記載する PP に規定された機能要件を満たすオペレーティングシステムの制御下に置かれなければならない。そのオペレーティングシステムは、**ISO/IEC 15408** の評価保証レベル EAL3 及び次の追加要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)

**ベンダ情報要件**

**VE06.22.01** : ベンダは、当該暗号モジュールの制御を行うオペレーティングシステムが、**JIS X 19790 の附属書 C**に記載する PP に規定された機能要件[加えて、“高信頼パス” (FTP\_TRP.1)]に対して、**ISO/IEC 15408** の評価保障レベル 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。

**試験手順要件**

**TE06.22.01** : 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って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。

**AS06.23 : (レベル 3・4)**

すべての CSP、制御入力及び状態出力は、高信頼メカニズム（例えば、専用の入出力物理ポート、高信頼パス）を介して通信されなければならない。

**ベンダ情報要件**

**VE06.23.01** : ベンダは、CSP、制御入力及び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。

**試験手順要件**

**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。

**TE06.23.02** : 試験者は、すべての CSP、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。

**注記** 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。

**TE06.23.03** : 試験者は、**AS06.23** 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。

**AS06.24 : (レベル 3・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。

**ベンダ情報要件**

**VE06.24.01** : 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。

#### 試験手順要件

**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。

#### AS06.25：（レベル 3・4）

この高信頼パスを介する通信は、オペレータ又は TSF によって排他的に活性化されて、他のパスから論理的に分離されなければならない。

#### ベンダ情報要件

**VE06.25.01**：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 によって排他的に活性化されて、他のパスから論理的に分離されるかを文書化しなければならない。

#### 試験手順要件

**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、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。

**TE06.25.03**：試験者は、高信頼パスが TSF でないソフトウェアに用いられるように試みなければならない。

#### AS06.26：（レベル 3・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って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
- ・ 高信頼パスの起動者及び対象の識別
- ・ 自己テストの失敗
- ・ タンパー検出の通知

#### ベンダ情報要件

**VE06.26.01**：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、高信頼パスの起動者及び対象の識別、自己テストの失敗、並びにタンパー検出の通知を含まなければならない。

#### 試験手順要件

**TE06.26.01**：試験者は、ベンダが **VE06.26.01** 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。

**注記** 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。

**TE06.26.02**：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、すべ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。

**AS06.27 : (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, **AS06.28** 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。

**注記** この個別要件は, **AS06.28** の一部として試験される。

**AS06.28 : (レベル 4)**

すべての暗号ソフトウェア, CSP, PSP, 並びに制御情報及び状態情報は, **JIS X 19790** の**附属書 C**に記載する PP に規定された機能要件を満たすオペレーティングシステムの制御下に置かれなければならない。そのオペレーティングシステムは, **ISO/IEC 15408** の評価保証レベル EAL4 において評価されなければならない。

**ベンダ情報要件**

**VE06.28.01:**ベンダは, 当該暗号モジュールの制御を行うオペレーティングシステムが, **JIS X 19790** の**附属書 C**に記載する PP に規定された機能要件に対して **ISO/IEC 15408** の評価保障レベル EAL4 に合格したことを示す文書を提供しなければならない。

**試験手順要件**

**TE06.28.01:**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って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。

**6.7 暗号鍵管理**

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

**総 論****AS07.01 : (レベル 1・2・3・4)**

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

**ベンダ情報要件**

**VE07.01.01:**ベンダが提供する文書は, 暗号モジュール内部の, CSP のすべての保護について記述しなければならない。保護は, 認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。

**試験手順要件**

**TE07.01.01:**試験者は, 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, CSP が認可されていない開示, 認可されていない変更及び認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) 試験者によるアクセスが認可されていない CSP に対してアクセスを(文書化された保護メカニズムを回避して)を試みる。暗号モジュールがそのアクセスを拒否するか, 又は暗号化された形式若しくは別の方法で保護された形式の 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ている。

- 2) ベンダが提供する文書が示していない方法を用いて CSP のすべてを変更し、暗号モジュールのなかにそれらをロードすることを試みる。暗号モジュールは、いかなる CSP もロードも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 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・4)**

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

**ベンダ情報要件**

**VE07.02.01 :** ベンダが提供する文書は、認可されていない変更及び置換に対するすべての PSP の保護について記述しなければならない。

**試験手順要件**

**TE07.02.01 :** 試験者は、PSP が、認可されていない変更及び認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ベンダが提供する文書が記述していることを検証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が示していない方法を用いて、すべての PSP を変更し、暗号モジュールのなか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 PSP のロードも成功させてはならない。試験者は、その PSP 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、その PSP がロードされなかったことを示して、それらの動作を行ってはならない。

**AS07.03 : (レベル 1・2・3・4)**

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

**ベンダ情報要件**

**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すべての CSP、PSP のリストを提供しなければならない。

**試験手順要件**

**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。

**6.7.1 乱数生成器(RBG)**

**注記** 暗号モジュールは複数の乱数生成器、一連の乱数生成器、又は単独の乱数生成器を搭載してもよい。

**AS07.04 : (レベル 1・2・3・4)**

すべての RBG 及びその使用方法が定義されなければならない。

**注記** この個別要件は、単独では試験されない。

**AS07.05 : (レベル 1・2・3・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 RBG 又は複数の RBG の連鎖を用いる場合には、次を満たさなければならない。

- ・ RBG のエントロピーソースは **JIS X 19790** の **7.8.1** で規定された RBG エントロピー試験を受けなければならない。

**注記** この個別要件に対する要求事項はない。

**AS07.06 : (レベル 1・2・3・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 RBG 又は複数の RBG の連鎖を用いる場合には、次を満たさなければならない。

- ・ RBG の決定論的構成要素は JIS X 19790 の 7. 8.1 の暗号アルゴリズム試験を受けなければならない。

**注記** この個別要件は、AS08.13 で試験される。

**AS07.07 : (レベル 1・2・3・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 RBG 又は複数の RBG の連鎖を用いる場合には、次を満たさなければならない。

- ・ RBG からのデータ出力は、JIS X 19790 の 7. 8. 2 で規定されたような連続乱数ビット列生成器試験に合格しなければならない。

**注記** この個別要件は、単独では試験されない。

**AS07.08 : (レベル 1・2・3・4)**

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

**ベンダ情報要件**

**VE07.08.01 :**ベンダは承認された RBG が鍵生成に使用されていることを明記した文書を提供しなければならない。

**試験手順要件**

**TE07.08.01 :**試験者は、承認されたセキュリティ機能で、暗号鍵生成に使われる RBG が JIS X 19790 の 附属書 D に示されるものであることをベンダが主張した文書を提供していることを検証しなければならない。

**TE07.08.02 :**試験者は、ベンダが提供する文書を調査して、実装された RBG が、指定の承認された RBG に一致することを検証しなければならない。

**6.7.2 鍵生成**

**AS07.09 : (レベル 1・2・3・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 RBG を用いて、生成されなければならない。

**ベンダ情報要件**

**VE07.09.01 :**ベンダは、承認された RBG が鍵生成に使用されていることを明記した文書を提供しなければならない。

**試験手順要件**

**TE07.09.01 :**試験者は、ベンダが、承認された RBG を暗号鍵の生成に用いていることを示した文書を提供していることを検証しなければならない。

**TE07.9.02 :**試験者は、ベンダが提供する文書をレビューして、実装された鍵生成方法が、示されたとおりの承認された RBG 方式に合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・4)**

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

**ベンダ情報要件**

**VE07.10.01 :** 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たい化（例えば、決定論的 RBG を初期化するためのシード値を推定すること）に、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の、多くの操作が必要となるかを明らかにする根拠を掲げた文書を提供しなければならない。

**試験手順要件**

**TE07.10.01 :** 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たい化（例えば、決定論的 RBG を初期化するためのシード値を推定すること）に、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の、多くの操作が必要となるかを明らかにした根拠を提供していることを検証しなければならない。

**TE07.10.02 :** 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、不確かさ又はあいまいさがある場合には、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。

**AS07.11 : (レベル 1・2・3・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、 **JIS X 19790** の **7.7.4** に規定された鍵の入力の要求事項を満たさなければならない。

**注記** この個別要件は、単独では試験されない。

**AS07.12 : (レベル 1・2・3・4)**

中間の鍵生成値が、暗号モジュールから出力される場合には、その値は、(1) 暗号化された形式、又は (2) 知識分散の技術のもとで、出力されなければならない。

**ベンダ情報要件**

**VE07.12.01 :** ベンダが提供する文書は、何らかの中間の鍵生成値が、鍵生成過程の終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。

**VE07.12.02 :** 中間の鍵生成値が、鍵生成の終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) 知識分散の技術のもとで、出力されていることを示さなければならない。

**試験手順要件**

**TE07.12.01 :** 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の終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。

**TE07.12.02 :** 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。

**TE07.12.03 :** 試験者は、出力インタフェースを観察して、すべ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。

**TE07.12.04 :** 試験者は、鍵生成過程の終了時に中間の鍵生成値が、1) 暗号化された形式、又は 2) 知識分散の技術のもとで、出力されていることを検証しなければならない。

**6.7.3 鍵確立**

**注記** 鍵確立は承認された方式(例えば公開鍵暗号アルゴリズムの使用), マニュアルの鍵配送手法(人手で運ばれる鍵格納デバイス), 又は電子的及び人手による配送手段の組合せによって実行されてもよい。

**AS07.13 : (レベル 1・2・3・4)**

暗号モジュールが鍵確立の方法を用いている場合には, 承認された鍵確立の技術だけが使用及び定義されなければならない。

**注** 承認された鍵確立方法の例は, JIS X 19790 の**附属書 E**に記載されている。

**ベンダ情報要件**

**VE07.13.01 :** 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記載する文書を提供しなければならない。

**試験手順要件**

**TE07.13.01 :** 試験者は, ベンダが, 使用している承認された鍵確立の技術が JIS X 19790 の**附属書 E**に記載されていることを主張する文書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, ベンダが提供する文書をレビューして, 実装された鍵確立の技術が, 示されている承認された鍵確立の技術と合致していることを検証しなければならない。

**AS07.14 : (レベル 1・2・3・4)**

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

**ベンダ情報要件**

**VE07.14.01 :** 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たい化(例えば, 鍵確立に使用されるアルゴリズムのセキュリティを危たい化すること)に, 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の, 多くの操作が必要となるかを明らかにする根拠を掲げた文書を提供しなければならない。

**試験手順要件**

**TE07.14.01 :** 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たい化(例えば, 鍵確立に使用されるアルゴリズムのセキュリティを危たい化すること)に, 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の, 多くの操作が必要となるかを明らかにした根拠を提供していることを検証しなければならない。

**TE07.14.02 :** 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, 不確かさ又はあいまいさがある場合には, 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。

**AS07.15 : (レベル 1・2・3・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, JIS X 19790 の 7.7.4 の鍵の入出力の要求事項を満たさなければならない。

**注記 1** この個別要件は, AS07.23~AS07.30 の一部として試験される。

**注記 2** 鍵共有方式が用いられる場合(例えば, 暗号鍵が共有された中間値から導出される場合)には, 共有される値は JIS X 19790 の 7.7.4 の入出力要件を満足することは要求されない。

#### 6.7.4 鍵入出力

**注記** 暗号鍵は暗号モジュールに入力されるか、出力されてもよい。

##### AS07.16 : (レベル 1・2・3・4)

鍵の入力又は出力は、手動（例えば、キーボードを介して）又は電子化された方法（例えば、スマートカード、トークン、PC カード、他の電子鍵ローディングデバイス）のいずれかを用いて行われ、定義されなければならない。

**注記** この個別要件は、AS07.25 の一部として試験される。

##### AS07.17 : (レベル 1・2・3・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。

#### ベンダ情報要件

**VE07.17.01** : 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。

#### 試験手順要件

**TE07.17.01** : 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。

**TE07.17.02** : 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。

##### AS07.18 : (レベル 1・2・3・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、すべての暗号化された秘密鍵及びプライベート鍵は、承認された暗号アルゴリズム（JIS X 19790 の**附属書 D**に記載）を用いて、暗号化されなければならない、完全性を保護されてもよい。

**注** 公開鍵は、平文の形式で、暗号モジュールへ入力、又は暗号モジュールから出力されてもよく、完全性を保護されてもよい。

#### ベンダ情報要件

**VE07.18.01** : 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示している文書を提供しなければならない。

#### 試験手順要件

**TE07.18.01** : 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示規定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、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、示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。

**AS07.19 : (レベル 1・2・3・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、鍵が割当てられている正しいエンティティの名称（例えば、人、グループ、プロセス）に関係づけなければならない。

**ベンダ情報要件**

**VE07.19.01 :** 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の名称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を記述しなければならない。

**試験手順要件**

**TE07.19.01 :** 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の名称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。

**TE07.19.02 :** 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、鍵とエンティティの名称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の名称に関係づけられるように鍵要素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。

**AS07.20 : (レベル 1・2・3・4)**

手動で入力される暗号鍵は、暗号モジュールへの入力の間に、正確を期して **JIS X 19790** の **7.8.2** で規定された手動の鍵入力試験を用いて、検証されなければならない。

**注** 鍵入力の間、手動で入力される値は、目視による確認を許すために及び正確さを向上させるために、一時的に表示されてもよい。

**注記** この個別要件は、単独では試験されない。

**AS07.21 : (レベル 1・2・3・4)**

暗号化された暗号鍵又は鍵要素が暗号モジュールに手動で入力される場合には、暗号鍵又は鍵要素の平文の値は、表示されてはならない。

**ベンダ情報要件**

**VE07.21.01 :** 文書化された鍵入力の手順は、暗号化された鍵又は鍵要素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。

**試験手順要件**

**TE07.21.01 :** 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要素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。

**TE07.21.02 :** 試験者はすべての暗号化された暗号鍵及び鍵要素を入力して、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。

**AS07.22 : (レベル 1・2・3・4)**

電子化された方法を用いて配送された秘密鍵及びプライベート鍵は、暗号化された形式で、暗号モジュールへ入力及び暗号モジュールから出力されなければならない。

**注** 手動の配送方法を用いて配送された秘密鍵及びプライベート鍵は、平文の形式で、暗号モジュールへ入力されるか、又は暗号モジュールから出力されてもよい。

**ベンダ情報要件**

**VE07.22.01 :** ベンダが提供する文書は、電子化された方法を用いて配送される鍵を示さなければならない。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明記しなければならない。

**試験手順要件**

**TE07.22.01 :** 試験者は、ベンダが、電子化された方法を用いて配送される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ていることを検証しなければならない。

**TE07.22.02 :** 電子化された方法が秘密鍵及びプライベート鍵を配送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。

**AS07.23 : (レベル 3・4)**

電子化された方法を用いて配送された秘密鍵及びプライベート鍵は、暗号化された形式で、暗号モジュールへ入力及び暗号モジュールから出力されなければならない。

**注記** この個別要件は、AS07.29の一部として試験される。

**AS07.24 : (レベル 3・4)**

手動の配送方法を用いて配送された秘密鍵及びプライベート鍵は、(1) 暗号化された形式又は (2) 知識分散の技術（すなわち、二つ以上の平文の暗号鍵要素を用いる技術。）を用いて、暗号モジュールへ入力又は暗号モジュールから出力されなければならない。

**ベンダ情報要件**

**VE07.24.01 :** ベンダ情報要件は、VE07.28.01 で規定する。

**試験手順要件**

**TE07.24.01 :** ベンダが提供する文書の検証は、TE07.27.01 のもとで行われる。

**TE07.24.02 :** 試験者は、ベンダが、手動の方法を用いて配送された秘密鍵及びプライベート鍵が (1) 暗号化された形式で、又は (2) 知識分散の技術を用いて（すなわち、二つ又はそれ以上の平文の暗号鍵要素のように）、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した文書を提供していることを検証しなければならない。

**TE07.24.03 :** 手動の方法が秘密鍵及びプライベート鍵を配送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) 暗号化された形式で、又は (2) 知識分散の技術を用いて、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。

**TE07.24.04 :** 手動の方法が秘密鍵及びプライベート鍵を配送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) 知識分散の技術を用いて、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。

**AS07.25 : (レベル 3・4)**

知識分散の手順が用いられる場合には、次の要求事項を満たさなければならない。

- ・ 暗号モジュールは、それぞれの鍵要素を入力又は出力するオペレータを別々に認証しなければならない。
- ・ **AS07.26**
- ・ **AS07.27**
- ・ **AS07.28**
- ・ **AS07.29**

**ベンダ情報要件**

**VE07.25.01** : 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要素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示さなければならない。

**試験手順要件**

**TE07.25.01** : 試験者は、認証がそれぞれの鍵要素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。

**TE07.25.02** : 試験者は、知識分散の技術を用いて、それぞれの鍵要素を入力して、鍵要素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。

**TE07.25.03** : 試験者は、知識分散の技術を用いて、それぞれの鍵要素を出力して、鍵要素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。

**AS07.26 : (レベル 3・4)**

知識分散の手順が用いられる場合には、次の要求事項を満たさなければならない。

- ・ **AS07.25**
- ・ 平文の暗号鍵要素の暗号モジュール入出力は、高信頼パス経由又は直接入出力のいずれかでなければならない。直接入出力とは、その鍵要素が不注意に格納、結合、又はその他の方法で処理される可能性のある、暗号モジュールを取り囲むシステム又は仲介するシステムを経由しないことを指す（**JIS X 19790** の 7.2 参照）。
- ・ **AS07.27**
- ・ **AS07.28**
- ・ **AS07.29**

**注記** この個別要件は、単独では試験されない。

**AS07.27 : (レベル 3・4)**

知識分散の手順が用いられる場合には、次の要求事項を満たさなければならない。

- ・ **AS07.25**
- ・ **AS07.26**
- ・ 元の暗号鍵を再組立てするために、少なくとも二つの鍵要素が要求されなければならない。
- ・ **AS07.28**
- ・ **AS07.29**

**ベンダ情報要件**

**VE07.27.01** : 手動で確立された秘密鍵又はプライベート鍵が、知識分散の技術のもとで、入力又は出力

される場合には、ベンダが提供する文書は、元の鍵を組み立てるために必要な鍵要素の数を示さなければならない。

#### 試験手順要件

**TE07.27.01**：試験者は、知識分散の技術のもとで、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、元の鍵を組み立てるのに少なくとも二つの鍵要素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。

**TE07.27.02**：試験者は、知識分散の技術のもとで、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、元の鍵を組み立てることができる単一の鍵要素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。

#### AS07.28：（レベル 3・4）

知識分散の手順が用いられる場合には、次の要求事項を満たさなければならない。

- ・ **AS07.25**
- ・ **AS07.26**
- ・ **AS07.27**
- ・ 文書は、 $n$  個の鍵要素の知識が元の鍵を再組立てするのに必要とされる場合、いかなる  $n-1$  個の鍵要素の知識も長さ以外に元の鍵の情報を提供しないことを検証しなければならない。
- ・ **AS07.29**

#### ベンダ情報要件

**VE07.28.01**：ベンダは、どのようにして、いかなる  $n-1$  個の鍵要素の知識も、長さ以外には元の鍵に関する情報を提供しないかを明らかにする根拠を掲げた文書を提供しなければならない。

#### 試験手順要件

**TE07.28.01**：試験者は、 $n$  個の鍵要素が元の鍵を組み立てるのに必要とされる場合に、ベンダが提供する文書が、いかなる  $n-1$  個の鍵要素の知識も、長さ以外には元の鍵に関する情報を提供しないかを明らかにした根拠を提供していることを検証しなければならない。

**TE07.28.02**：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、不確かさ又はあいまいさがある場合には、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。

#### AS07.29：（レベル 3・4）

知識分散の手順が用いられる場合には、次の要求事項を満たさなければならない。

- ・ **AS07.25**
- ・ **AS07.26**
- ・ **AS07.27**
- ・ **AS07.28**
- ・ 文書は、暗号モジュールに用いられる手順を示さなければならない。

#### ベンダ情報要件

**VE07.29.01**：ベンダは、暗号モジュールに用いられる知識分散の技術について示している文書を提供しなければならない。

### 試験手順要件

**TE07.29.01**：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。

#### 6.7.5 鍵の格納

##### AS07.30：（レベル 1・2・3・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。

**注記** この個別要件は、**AS11.06** のもとで試験される。

##### AS07.31：（レベル 1・2・3・4）

平文の秘密鍵及びプライベート鍵は、認可されていないオペレータに対して、暗号モジュールの外側からアクセス可能であってはならない。

**注記** この個別要件は、**AS07.01** のもとで試験される。

##### AS07.32：（レベル 1・2・3・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、鍵が割当てられている正しいエンティティの名称（例えば、人、グループ、プロセス）とを関係づけなければならない。

### ベンダ情報要件

**VE07.32.01**：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の名称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。

### 試験手順要件

**TE07.32.01**：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の名称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。

**TE07.32.02**：試験者は、鍵とエンティティの名称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一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。

#### 6.7.6 鍵のゼロ化

##### AS07.33：（レベル 1・2・3・4）

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

**注** 次の CSP には、ゼロ化は要求されない。

- ・ 暗号化された CSP。
- ・ 暗号化されてはいないが、物理的又は論理的に保護された CSP であって、付加的に組込まれる、認証された暗号モジュール（**JIS X 19790** の要求事項を満たすもの）の中のもの。

### ベンダ情報要件

**VE07.33.01**：ベンダが提供する文書は、次の CSP のゼロ化の情報を示さなければならない。

- a. ゼロ化技術
- b. CSP をゼロ化するときの制限
- c. ゼロ化される CSP
- d. ゼロ化されない CSP 及びゼロ化されない根拠

- e. CSP を危たい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

#### 試験手順要件

**TE07.33.01**：試験者は、**VE07.33.01** 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、不確かさ又はあいまいさがある場合には、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。

**TE07.33.02**：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 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、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。

**TE07.33.03**：試験者はゼロ化を実行して、CSP が危たい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。

**TE07.33.04**：試験者は、ゼロ化のコマンドによってゼロ化されない CSP のすべてが、(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) 組み込まれた認証された暗号モジュール(**JIS X 19790** 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。

#### 6.8 自己テスト

##### **AS08.01**：(レベル 1・2・3・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。

**注記** この個別要件は、**AS08.07** の一部として試験される。

##### **AS08.02**：(レベル 1・2・3・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。

**注記** この個別要件は、**AS08.07** の一部として試験される。

##### **AS08.03**：(レベル 1・2・3・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** 暗号モジュールは、**JIS X 19790** に規定されているテストに加え、その他のパワーアップ自己テスト又はその他の条件自己テストを実行してもよい。

**注記** この個別要件は、**AS08.07** の一部として試験される。

##### **AS08.04**：(レベル 1・2・3・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、エラーインジケータを出力しなければならない。

#### ベンダ情報要件

**VE08.04.01**：ベンダは、それぞれの自己テストに関係するすべてのエラー状態を文書化し、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。

**試験手順要件**

**TE08.04.01** : 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すべ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。

**TE08.04.02** : それぞれの自己テストがエラーをどのように扱うかを示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。

**TE08.04.03** : 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示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、この個別要件は不合格とする。

**AS08.05 : (レベル 1・2・3・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。

**ベンダ情報要件**

**VE08.05.01** : ベンダの設計要求事項に関しては **VE02.06.01** を参照する。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。

**試験手順要件**

**TE08.05.01** : 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、暗号モジュールがすべ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。

**TE08.05.02** : 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示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

**TE08.05.03** : 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。

**AS08.06 : (レベル 1・2・3・4)**

データ出力インタフェースを通るすべてのデータ出力は、エラー状態のときには抑止されなければならない。

**ベンダ情報要件**

**VE08.06.01** : ベンダの設計要求事項に関しては **VE02.06.01** を参照する。ベンダの設計は、データ出力インタフェースを通るすべてのデータ出力は抑止されることを確実にしなければならない。

### 試験手順要件

**TE08.06.01**：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すべ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。

**TE08.06.02**：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すべ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。

#### AS08.07：（レベル 1・2・3・4）

文書は、次を示さなければならない。

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

### ベンダ情報要件

**VE08.07.01**：ベンダは、暗号モジュールが実行できるすべ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。

**VE08.07.02**：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。

### 試験手順要件

**TE08.07.01**：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
  - － RBG エントロピーテスト
  - － ソフトウェア・ファームウェア完全性テスト
  - － 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）
  - － ソフトウェア・ファームウェアロードテスト
  - － 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

**TE08.07.02**：試験者は、上記の情報が、それぞれのエラー条件に対して示されていることをチェックしなければならない。

**TE08.07.03**：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。

#### 6.8.1 パワーアップ自己テスト

##### AS08.08 : (レベル 1・2・3・4)

パワーアップ自己テストは、暗号モジュールが（電源オフ、リセット、リブートなどの後で）電源投入されたときに、その暗号モジュールによって実行されなければならない。

**注記** この個別要件は、AS08.09の一部として試験される。

##### AS08.09 : (レベル 1・2・3・4)

パワーアップ自己テストは自動的に開始され、かつ、オペレータの介入を必要としてはならない。

#### ベンダ情報要件

**VE08.09.01 :** 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。

#### 試験手順要件

**TE08.09.01 :** 試験者は、ベンダが提供する文書が **VE08.09.01** 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。

**TE08.09.02 :** 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入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。

##### AS08.10 : (レベル 1・2・3・4)

パワーアップ自己テストが完了したとき、その結果は“状態出力”インタフェースを通じて明示的に又は暗黙のうちに出力されなければならない。

#### ベンダ情報要件

**VE08.10.01 :** 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。

#### 試験手順要件

**TE08.10.01 :** 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示していることを検証しなければならない。

**TE08.10.02 :** 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。

##### AS08.11 : (レベル 1・2・3・4)

出力インタフェースを通るすべてのデータ出力は、パワーアップ自己テストが実行されるときには抑止されなければならない。

**注記** この個別要件は、AS02.06の一部として試験される。

**AS08.12 : (レベル 1・2・3・4)**

電源投入時にパワーアップ自己テスト (AS08.08 から AS08.11 まで) 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。

**ベンダ情報要件**

**VE08.12.01 :** 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すべてが含まれていなければならない。

**試験手順要件**

**TE08.12.01 :** 試験者は、すべ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示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。

**TE08.12.02 :** 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。

**AS08.13 : (レベル 1・2・3・4)**

暗号モジュールは次のパワーアップ自己テスト (AS08.14 から AS08. 25 まで) を実行しなければならない。

**ベンダ情報要件**

**VE08.13.01 :** ベンダ情報要件は、VE08.07.01 で規定する。

**試験手順要件**

**TE08.13.01 :** 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、TE08.07.01 のもとで行われる。

**TE08.13.02 :** 暗号モジュールが文書化された自己テストを実行することの検証は、AS08.16～AS08.28 における検証要求事項のもとで行われる。

**暗号アルゴリズムテスト****AS08.14 : (レベル 1・2・3・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) のすべてについて実行されなければならない。

**注** 既知解テストは、正しい出力が既に知られているデータ上での暗号アルゴリズムを操作することを意味し、かつ、計算された出力と既に生成されている (既知解の) 出力とを比較することを意味する。

**ベンダ情報要件**

**VE08.14.01 :** ベンダ情報要件は、VE08.07.01 で規定する。

**試験手順要件**

**TE08.14.01 :** 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すべてと関係していることを検証しなければならない。

**TE08.14.02 :** 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。

**AS08.15 : (レベル 1・2・3・4)**

計算された (AS08.14 の) 出力が既知解と異なる場合には、既知解テストは失敗としなければならない。

**ベンダ情報要件**

**VE08.15.01 :** 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示さなければならない。

**VE08.15.02 :** ベンダが提供する文書は、二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。

**試験手順要件**

**TE08.15.01 :** 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。

**TE08.15.02 :** これは **TE08.04.01**、**TE08.04.02** 及び **TE08.04.03** のもとで試験される。

**AS08.16 : (レベル 1・2・3・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 (AS08. 28 及び JIS X 19790 の 7. 8. 2.1 参照) を用いてテストされなければならない。

**ベンダ情報要件**

**VE08.16.01 :** ベンダ情報要件は、**VE08.07.01** で規定する。

**VE08.16.02 :** ベンダが提供する文書は、実装されている一つ以上のテストについて示さなければならない。

**試験手順要件**

**TE08.16.01 :** 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。

**TE08.16.02 :** 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。

**TE08.16.03 :** 鍵ペア整合性テストは **AS08.31** で試験される。

**AS08.17 : (レベル 1・2・3・4)**

メッセージダイジェストアルゴリズムは独立した既知解テストをもつか、又は既知解テストが関係づけられた暗号アルゴリズムテストに含まれていなければならない。

**ベンダ情報要件**

**VE08.17.01 :** ベンダ情報要件は、**VE08.07.01** で規定する。

**VE08.17.02 :** ベンダが提供する文書は、実装されている一つ以上のテストについて示さなければならない。

**試験手順要件**

**TE08.17.01 :** 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。

**TE08.17.02 :** 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示  
していることを検証しなければならない。

**TE08.17.03**：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。

**AS08.18：（レベル 1・2・3・4）**

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

**ベンダ情報要件**

**VE08.18.01**：ベンダ情報要件は、**VE08.07.01** で規定する。

**VE08.18.02**：ベンダは、既知解テスト又は二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示さ  
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。

**試験手順要件**

**TE08.18.01**：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) 二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) 二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

**TE08.18.02**：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。

**TE08.18.03**：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、**TE08.04.01**、**TE08.04.02** 及び **TE08.04.03** のもとで行われる。これらの試験の内、  
どれか一つでも不合格の場合には、この個別要件は不合格とする。

**AS08.19：（レベル 1・2・3・4）**

その二つの実装の出力が等しくない場合には、暗号アルゴリズムテストは失敗としなければならない。

**注記** この個別要件は、**AS08.20** の一部として試験される。

**RBG エントロピーテスト**

**AS08.20：（レベル 1・2・3・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 RBG を用いる場合、暗号モジュールは、  
**ISO/IEC 18031** に記載されている RBG エントロピーソースについての暗号ヘルステストを実行しなけ  
ればならない。

**ベンダ情報要件**

**VE08.20.01**：ベンダが提供する文書は、暗号モジュールが承認された動作モードにおいて承認された

RBG を用いる場合、暗号モジュールが、ISO/IEC 18031 に記載されている RBG エントロピーソースについての暗号ヘルステストを実行することを示さなければならない。

#### 試験手順要件

**TE08.20.01**：試験者は、ソースコード及び／又は設計文書を検査することで、暗号モジュールが RBG エントロピーソースについての暗号ヘルステストを実装していることを検証しなければならない。

**TE08.20.02**：試験者は、可能なら、強制的にエラーを起こさせてエントロピーテストを失敗させなければならない。暗号モジュールが、エラー状態に移り、エントロピーテストの失敗によるエラーインジケータを出力するかどうかを検証しなければならない。このテストが失敗すれば、この個別要件は不合格とする。

#### ソフトウェア・ファームウェア完全性テスト

##### AS08.21：（レベル 1・2・3・4）

誤り検出符号(EDC)又は承認された認証技術（例えば、承認されたメッセージ認証コード、又はデジタル署名アルゴリズム）を用いるソフトウェア・ファームウェア完全性テストは、暗号モジュール内の、すべての認証されたソフトウェア及びファームウェア構成要素に対して、暗号モジュールが電源投入時に、適用されなければならない。

**注** ソフトウェア・ファームウェア完全性テストは、JIS X 19790 のセキュリティ要求事項から除外されたあらゆるソフトウェア構成要素及びファームウェア構成要素には要求されない（JIS X 19790 の 7.1 参照）。

#### ベンダ情報要件

**VE08.21.01**：ベンダが提供する文書は、誤り検出符号(EDC)又は承認された認証技術（例えば、承認されたメッセージ認証コード又はデジタル署名アルゴリズム）が、すべてのソフトウェア及びファームウェア構成要素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示さなければならない。

**VE08.21.02**：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。

**VE08.21.03**：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確認書を提供しなければならない。
- (2) 又は、承認された暗号アルゴリズム確認書を発行する手順がない場合には、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。

#### 試験手順要件

**TE08.21.01**：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ェア・ファームウェア構成要素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。

**TE08.21.02**：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、又は承認された暗号アルゴリズム確認書を発行する手順がない場合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。

**TE08.21.03**：暗号モジュールがソフトウェア・ファームウェ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、ソフトウェア・ファームウェ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ェア及びファームウェアの識別。

- 3) ソフトウェア及びファームウェアがインストールされときの EDC 計算。
- 4) 自己テストが開始されときの 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) 二つの EDC が等しくないときの自己テストの失敗。

**TE08.21.04**：暗号モジュールが、ソフトウェア・ファームウェ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、ソフトウェア・ファームウェ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。

**TE08.21.05**：暗号モジュールが、ソフトウェア・ファームウェ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、ソフトウェア・ファームウェ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。
- 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ェア及びファームウェアの識別。
- 3) ソフトウェア及びファームウェアがインストールされ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。

**TE08.21.06**：ソースコード及び／又は設計書をチェックすることによって、試験者は、ソフトウェア・ファームウェア完全性テストの実装が **TE08.21.01**, **TE08.21.02**, **TE08.21.03** 又は **TE08.21.04** と一致していることを検証しなければならない。

**TE08.21.07**：可能な場合には、試験者は、格納されたソフトウェア、ファームウェア、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ェア・ファームウェ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、この個別要件は不合格とする。

**AS08.22：（レベル 1・2・3・4）**

（**AS08.21** で）計算された結果があらかじめ生成された結果と等しくない場合には、ソフトウェア・ファームウェア完全性テストは失敗としなければならない。

**注記** この個別要件は **AS08.21** の一部として試験される。

**AS08.23：（レベル 1・2・3・4）**

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

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

**ベンダ情報要件**

**VE08.23.01**：暗号モジュールが、ソフトウェア・ファームウェ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。

**試験手順要件**

**TE08.23.01**：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**

**AS08.24 : (レベル 1・2・3・4)**

暗号モジュールが電源投入されたときに、パワーアップ自己テストの一部としてテストされなければならない。暗号モジュールのセキュアな動作にとって重要な、その他のセキュリティ機能があるかもしれない。

**注記** この個別要件は、AS08.27の一部として試験される。

**AS08.25 : (レベル 1・2・3・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 (AS08.27) としてテストされなければならない。

**注記** この個別要件は、単独では試験されない。

**AS08.26 : (レベル 1・2・3・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すべてを示し、かつ、暗号モジュールによって実行される該当するパワーアップ自己テスト及び条件自己テストを識別しなければならない。

**注記** 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挙げられるが、これらに限るものではない。

**ベンダ情報要件**

**VE08.26.01 :** ベンダは、すべ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。

**試験手順要件**

**TE08.26.01 :** 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) すべての重要機能の識別及び記述。
- 2) すべての重要機能について、少なくとも一つの自己テストの識別。

**TE08.26.02 :** 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。

**6.8.2 条件自己テスト****AS08.27 : (レベル 1・2・3・4)**

条件自己テストは、AS08.28 から AS08.39 までに規定するとおりに実行されなければならない。

**注記** この個別要件は単独では試験されない。

**6.8.2.1 (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**

**AS08.28 : (レベル 1・2・3・4)**

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

**ベンダ情報要件**

**VE08.28.01 :** 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、ベンダが提供する文書は、鍵ペア整合性テストについて記述しなければならない。このテストでは、平文に対して公開鍵を適用する。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。

- ・ 二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。
- ・ 二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。
- ・ 暗号文を復号した結果と元の平文と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。

**VE08.28.02 :** 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、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。

**試験手順要件**

**TE08.28.01 :** 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、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。

**TE08.28.02 :** 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、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。

**手動鍵入力テスト****AS08.29 : (レベル 1・2・3・4)**

暗号鍵又は暗号鍵要素が暗号モジュール内に手動で入力される場合には、**AS08.30** から **AS08.32** までの手動鍵入力テストが実行されなければならない。

**注記** この個別要件は、単独では試験されない。

**AS08.30 : (レベル 1・2・3・4)**

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

**注記** この個別要件は単独では試験されない。

**AS08.31 : (レベル 1・2・3・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。

**注記** この個別要件は単独では試験されない。

**AS08.32 : (レベル 1・2・3・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。

**ベンダ情報要件**

**VE08.32.01 :** 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。EDC 又は繰り返し鍵入力がか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) EDC
  - 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。

**VE08.32.02 :** 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、EDC 用のフィールドを含んでいなければならない。

**試験手順要件**

**TE08.32.01 :** 試験者は、ベンダが提供する文書をレビューして鍵入力方法が含まれていることを検証しなければならない。

**TE08.32.02 :** 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 (EDC 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示している設計文書をチェックしなければならない。

- 1) EDC
  - EDC 用のフィールド (AS07.03 を参照) を含むすべ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すべて。
- 2) 繰り返し鍵入力
  - 手動で入力された鍵のすべ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すべて。

**TE08.32.03 :** 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すべてを入力して、入力され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べきインジケータの姿と実際のインジケータと

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と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。

**TE08.32.04**：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と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）の一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と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。

### 6.8.2.3 連続乱数ビット列生成器テスト

**注記** このテストは RBG の最低限のヘルステストだけを目的とし、乱数生成の品質は扱っていない。

RBG に関するその他のすべての試験は、ISO/IEC 18031 に従って実施される。

#### AS08.33：（レベル 1・2・3・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 RBG を用いる場合には、暗号モジュールは、それぞれの RBG に対し、定常値にならないかどうかのテストをする AS08.34 から AS08.35 までの連続乱数ビット列生成器テストを実行しなければならない。

**注記** この個別要件は単独では試験されない。

**AS08.34 : (レベル 1・2・3・4)**

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

**ベンダ情報要件**

**VE08.34.01** : 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。

**試験手順要件**

**TE08.34.01** : 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示している文書、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。
- 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。
- 3) 二つの比較したブロックが等しい場合には、そのテストを不合格とする。

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。
- 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。
- 3) 二つの比較した  $n$  ビット列が等しい場合には、このテストを不合格とする。

**AS08.35 : (レベル 1・2・3・4)**

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

**ベンダ情報要件**

**VE08.35.01** : 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。

**試験手順要件**

**TE08.35.01** : 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示している文書、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。

- 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。
- 3) 二つの比較したブロックが等しい場合には、そのテストを不合格とする。

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。
- 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。
- 3) 二つの比較した  $n$  ビット列が等しい場合には、このテストを不合格とする。

#### 6.8.2.4 バイパステスト

##### AS08.36 : (レベル 1・2・3・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して平文を転送すること）バイパス機能を実装している場合には、暗号モジュール構成要素の単一の誤動作が意図しない平文の出力につながらないことを確実にするために、AS08.37 から AS08.39 までのバイパステストを実行しなければならない。

**注記** この個別要件は、単独では試験されない。

##### AS08.37 : (レベル 1・2・3・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。

#### ベンダ情報要件

**VE08.37.01 :** 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。

**VE08.37.02 :** ベンダは、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り替わるとき、暗号モジュールが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。

#### 試験手順要件

**TE08.37.01 :** 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。

**TE08.37.02 :** 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。

**TE08.37.03 :** 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り替えて、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。

##### AS08.38 : (レベル 1・2・3・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時点（例えば、IP アドレスのソース・ディスタネーション表が変更される時点）で、暗号処理を提供するサービスの正しい動作をテストしなければならない。

#### ベンダ情報要件

**VE08.38.01**：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り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時点で、暗号サービスの正しい動作を検証する、バイパステストを実装しなければならない。

**VE08.38.02**：ベンダは、バイパス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時点で、次のことを実証するものでなければならない。

- 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。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) その暗号サービスの正しい動作が、暗号モジュールが、平文の情報を出力しないことの実証によって検証される。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。

#### 試験手順要件

**TE08.38.01**：試験者は、暗号モジュールに、切替え手順を管理するメカニズムが変更される時点で、暗号サービスの正しい動作を検証する、バイパステストが実装されていることを検証しなければならない。

**TE08.38.02**：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。

**TE08.38.03**：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、メカニズムは最後の変更から変更され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。試験者は、用いられる方法について文書化する。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の検証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。

#### AS08.39：（レベル 1・2・3・4）

切替え手順を管理するメカニズム又は論理を定め、文書化しなければならない。

**注記** この個別要件は、**AS08.37** 及び **AS08.38** の一部として試験される。

### 6.9 設計保証

#### 6.9.1 構成管理

#### AS09.01：（レベル 1・2・3・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構成要素に対して、並びに関係した暗号モジュールの文書に対して、実施されなければならない。

#### ベンダ情報要件

**VE09.01.01**：ベンダが提供する文書は、暗号モジュール、暗号モジュール構成要素及び関係した暗号モジュールの文書に対する構成管理システムを記述しなければならない。

#### 試験手順要件

**TE09.01.01**：試験者は、構成管理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。

**AS09.02 : (レベル 1・2・3・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アイテム（例えば、暗号モジュール、暗号モジュール構成要素、ユーザガイダンス、セキュリティポリシ、オペレーティングシステム）のそれぞれのバージョンは、一意の ID 番号が割当てられ、かつ、ラベル付けされなければならない。

**ベンダ情報要件**

**VE09.02.01 :** ベンダの構成管理文書は、すべての構成アイテムの構成リストを含まなければならない。

構成管理文書は、構成アイテム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。

**VE09.02.02 :** ベンダが提供する文書は、認証されるそれぞれの構成アイテム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。

**試験手順要件**

**TE09.02.01 :** 試験者は、構成アイテム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。

**TE09.02.02 :** 試験者は、構成管理文書がすべての構成アイテムを一意に識別するために用いられる方法を示していることを検証しなければならない。

**TE09.02.03 :** 試験者は、認証される構成アイテム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文書をレビューしなければならない。

**TE09.02.04 :** 試験者は、構成管理文書が、認証されるそれぞれの構成アイテム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。

**AS09.03 : (レベル 1・2・3・4)**

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

**ベンダ情報要件**

**VE09.03.01 :** ベンダが提供する文書は、構成アイテムに対して認可された変更だけが行われるように、構成管理システムの手段を定義しなければならない。

**試験手順要件**

**TE09.03.01 :** 試験者は、構成アイテムに対して認可された変更だけが行われるように構成管理システムの手段を定義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。

**AS09.04 : (レベル 1・2・3・4)**

構成管理システムは、暗号モジュールの生成をサポートしなければならない。

**ベンダ情報要件**

**VE09.04.01 :** ベンダが提供する文書は、暗号モジュールの生成のために構成管理システムが行うサポートを定義しなければならない。

**試験手順要件**

**TE09.04.01 :** 試験者は、暗号モジュールの生成のために構成管理システムが行うサポートが定義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。

**AS09.05 : (レベル 1・2・3・4)**

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

**ベンダ情報要件**

**VE09.05.01 :** ベンダが提供する文書は、構成管理システムにおける、認可された変更だけが暗号モジュールの実装表現に対して行われるように自動化された手段を定義しなければならない。

**試験手順要件**

**TE09.05.01 :** 試験者は、構成管理システムの自動化された手段が、暗号モジュールの実装表現に対して認可された変更だけを行っ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。

**AS09.06 : (レベル 1・2・3・4)**

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

**ベンダ情報要件**

**VE09.06.01 :** ベンダが提供する文書は、構成管理システムにおける、暗号モジュールの生成をサポートする自動化された手段を定義しなければならない。

**試験手順要件**

**TE09.06.01 :** 試験者は、構成管理システムの自動化された手段が、暗号モジュールの生成をサポート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。

**AS09.07 : (レベル 1・2・3・4)**

構成管理システムは、すべての構成アイテムを一意に識別しなければならない。

**ベンダ情報要件**

**VE09.07.01 :** ベンダが提供する文書は、構成管理システムにおける、すべての構成アイテムを一意に識別する手段を定義しなければならない。

**試験手順要件**

**TE09.07.01 :** 試験者は、構成管理システムにおいて、すべての構成アイテムが一意に識別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。

**AS09.08 : (レベル 1・2・3・4)**

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

**ベンダ情報要件**

**VE09.08.01 :** ベンダが提供する文書は、構成リストにおける、暗号モジュールを形成するすべての構成アイテムを一意に識別する手段を定義しなければならない。

**試験手順要件**

**TE09.08.01 :** 試験者は、構成リストにおいて、暗号モジュールを形成するすべての構成アイテムが一意に識別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。

**AS09.09 : (レベル 1・2・3・4)**

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

**ベンダ情報要件**

**VE09.09.01 :** ベンダが提供する文書は、構成管理システムが構成管理計画に従って運用していること、及び構成管理システムの下で効果的にすべての構成アイテムのメンテナンスが行われていることを示す証拠を示さなければならない。

**試験手順要件**

**TE09.09.01 :** 試験者は、構成管理システムが構成管理計画に従って運用していること、及び構成管理システムの下で効果的にすべての構成アイテムのメンテナンスが行われていることを示す証拠を規定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。

**AS09.10 : (レベル 1・2・3・4)**

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

**ベンダ情報要件**

**VE09.10.01 :** ベンダは、以前のセキュリティ欠陥とそれらの解決に関する情報を含む構成アイテムのリストを定義しなければならない。

**試験手順要件**

**TE09.10.01 :** 試験者は、以前のセキュリティ欠陥とそれらの解決に関する情報が構成アイテムのリストに含まれていることを検証しなければならない。

**6.9.2 配付及び運用****AS09.11 : (レベル 1・2・3・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示さなければならない。

**ベンダ情報要件**

**VE09.11.01 :** 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。

**試験手順要件**

**TE09.11.01 :** 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。

**TE09.11.02 :** 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。

**AS09.12 : (レベル 2・3・4)**

セキュリティレベル 1 の要求事項 (**AS09.03**) に加えて、文書は、認可されたオペレータに対して暗号モジュールのバージョンを配送及び配付している間、セキュリティを維持するために必要な手順を示さなければならない。

**ベンダ情報要件**

**VE09.12.01 :** 配付に関する文書は、認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。

#### 試験手順要件

**TE09.12.01**：試験者は、認可されたオペレータに対して暗号モジュールのバージョンを配送及び配付する間、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。

#### 6.9.3 開発

##### AS09.13：（レベル 1・2・3・4）

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

**注記** この個別要件は **AS09.14** 及び **AS09.17** の一部として試験される。

##### AS09.14：（レベル 1・2・3・4）

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

#### ベンダ情報要件

**VE09.14.01**：ベンダが提供する文書は、**AS09.13** に示すセキュリティ手段が暗号モジュールの開発及びメンテナンスを通して適用される証拠を記述しなければならない。

#### 試験手順要件

**TE09.14.01**：試験者は、**AS09.13** に示すセキュリティ手段が暗号モジュールの開発及びメンテナンスを通して適用される証拠が記述されていることを確認するために、ベンダが提出する文書をレビューしなければならない。

##### AS09.15：（レベル 1・2・3・4）

実装に使用されるすべての開発ツールは、明確に識別されなければならない。

#### ベンダ情報要件

**VE09.15.01**：ベンダが提供する文書は、実装に用いるすべての開発ツールを、明確に識別しなければならない。

#### 試験手順要件

**TE09.15.01**：試験者は、実装に用いるすべての開発ツールが明確に識別されていることを確認するために、ベンダが提出する文書をレビューしなければならない。

##### AS09.16：（レベル 1・2・3・4）

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

#### ベンダ情報要件

**VE09.16.01**：ベンダが提供する文書は、実装において用いられるすべての規定事項の意味を明確に定義する開発ツールの文書を列挙しなければならない。

#### 試験手順要件

**TE09.16.01**：試験者は、実装において用いられるすべての規定事項の意味が明確に定義されていることを確認するために、ベンダが提供する開発ツールの文書をレビューしなければならない。

**AS09.17 : (レベル 1・2・3・4)**

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

**ベンダ情報要件**

**VE09.17.01 :** ベンダが提供する文書は、すべての実装依存の任意選択事項の意味を明確に定義した開発ツールの文書を列挙しなければならない。

**試験手順要件**

**TE09.17.01 :** 試験者は、すべての実装関連の任意選択事項の意味が明確に定義されている開発ツールの文書を列挙したベンダが提供する文書をレビューしなければならない。

**AS09.18 : (レベル 1・2・3・4)**

AS09.19 から AS09.21 までの要求事項は、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。

**注記** この個別要件は、単独では試験されない。

**AS09.19 : (レベル 1・2・3・4)**

文書は、暗号モジュールのハードウェア構成要素、ソフトウェア構成要素及びファームウェア構成要素の設計と暗号モジュールのセキュリティポリシとの対応を示さなければならない(JIS X 19790 の 7.1 参照)。

**ベンダ情報要件**

**VE09.19.01 :** ベンダが提供する文書は、ハードウェア設計、ソフトウェア設計及びファームウェ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。

**試験手順要件**

**TE09.19.01 :** 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。

**AS09.20 : (レベル 1・2・3・4)**

暗号モジュールがソフトウェア構成要素又はファームウェア構成要素を含む場合には、文書は、構成要素と暗号モジュールの設計との対応を明確に表現するコメントの形で注釈をつけた、ソフトウェア構成要素及びファームウェア構成要素のソースコードを示さなければならない。

**ベンダ情報要件**

**VE09.20.01 :** ベンダは、暗号モジュールに含まれるすべてのソフトウェア構成要素及びファームウェア構成要素の名称のリストを提供しなければならない。

**VE09.20.02 :** 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ェア構成要素及びファームウェア構成要素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。

**試験手順要件**

**TE09.20.01 :** 試験者は、それぞれのソフトウェア構成要素又はファームウェア構成要素の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。

**AS09.21 : (レベル 1・2・3・4)**

暗号モジュールがハードウェア構成要素を含む場合には、文書は、ハードウェア構成要素の回路図及び／又はハードウェア記述言語(HDL)のソースコードを示さなければならない。

**ベンダ情報要件**

**VE09.21.01 :** ベンダは、暗号モジュールに含まれるハードウェア構成要素のリストを提供しなければならない。

**試験手順要件**

**TE09.21.01 :** 試験者は、文書がハードウェア構成要素の回路図及び／又はハードウェア記述言語(HDL)のソースコードを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。

**AS09.22 : (レベル 2・3・4)**

セキュリティレベル 1 の要求事項に加えて、**AS09.23** 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。

**注記** この個別要件は単独では試験されない。

**AS09.23 : (レベル 2・3・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記述した機能仕様を示さなければならない。

**ベンダ情報要件**

**VE09.23.01 :** 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。

**VE09.23.02 :** 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。

**試験手順要件**

**TE09.23.01 :** 試験者は、**VE09.23.01** 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、この個別要件は不合格とする。

**TE09.23.02 :** 試験者は、**VE09.23.02** 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、この個別要件は不合格とする。

**AS09.24 : (レベル 3・4)**

セキュリティレベル 1 及び 2 の要求事項に加えて、**AS09.25** から **AS09.26** までの要求事項は、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。

**注記** この個別要件は単独では試験されない。

**AS09.25 : (レベル 3・4)**

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

**ベンダ情報要件**

**VE09.25.01**：ベンダは、高級言語で記述されていないソフトウェア構成要素及びファームウェア構成要素のそれぞれを識別して、その構成要素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、又はソフトウェア若しくはファームウェ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。

**試験手順要件**

**TE09.25.01**：試験者は、どの構成要素が低級言語で記述されているかを判定するために、ソフトウェア構成要素及びファームウェア構成要素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、**VE09.25.01** 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ェア構成要素及び／又はファームウェア構成要素はないことを検証しなければならない。

**AS09.26：（レベル 3・4）**

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

**ベンダ情報要件**

**VE09.26.01**：ベンダは、高級言語を用いて実装されたハードウェア構成要素に関する文書を提供しなければならない。

**試験手順要件**

**TE09.26.01**：試験者は、**VE09.26.01** 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、この個別要件は不合格とする。

**AS09.27：（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、**AS09. 28** から **AS09. 33** までの要求事項は、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

**注記** この個別要件は、単独では試験されない。

**AS09.28：（レベル 4）**

文書は、暗号モジュールのセキュリティポリシーのルール及び特徴を記述した形式的モデルを示さなければならない。

**ベンダ情報要件**

**VE09.28.01**：ベンダは、暗号モジュールのセキュリティポリシー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。

**試験手順要件**

**TE09.28.01**：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) 形式的モデルの記載は、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。
- 2) 形式的モデルは次を含んでいる。
  - 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

**注記** 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 にある。

**AS09.29 : (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示されなければならない。

**注記** この個別要件は、AS09.28 の一部として試験される。

**AS09.30 : (レベル 4)**

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

**ベンダ情報要件**

**VE09.30.01 :** 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ー（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。

**VE09.30.02 :** モデルは、モデル化することができるすべてのポリシーについて、セキュリティポリシーと一致し、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。

**試験手順要件**

**TE09.30.01 :** 試験者は、暗号モジュールのセキュリティポリシー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ー、形式的モデル及びセキュリティポリシー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。

**AS09.31 : (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、非形式的な証明を示さなければならない。

**ベンダ情報要件**

**VE09.31.01 :** 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。

**試験手順要件**

**TE09.31.01 :** 試験者は、VE09.31.01 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、この個別要件は不合格とする。

**AS09.32 : (レベル 4)**

暗号モジュールのそれぞれのハードウェア構成要素、ソフトウェア構成要素及びファームウェア構成要素に対して、ソースコードは、(1) 正しく実行するためにモジュール構成要素、関数、又は手続への入力に必要な事前条件、及び (2) モジュール構成要素、関数、又は手続の実行が完了するときに正しいと期待される事後条件、の二つを示すコメントを用いて注釈が付けられなければならない。

**注** 事前条件及び事後条件は、暗号モジュール構成要素、関数、又は手続の振る舞いを完全、かつ、明快に、説明するのに十分詳細な注釈を用いて示されてもよい。

**ベンダ情報要件**

**VE09.32.01 :** すべてのハードウェア構成要素、ソフトウェア構成要素及びファームウェア構成要素のソースコードは、AS09.32 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。

らない。

#### 試験手順要件

**TE09.32.01**：試験者は、**VE09.32.01** 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、この個別要件は不合格とする。

#### AS09.33：（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、非形式的な証明を示さなければならない。

#### ベンダ情報要件

**VE09.33.01**：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。

#### 試験手順要件

**TE09.33.01**：試験者は、**VE09.33.01** 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、この個別要件は不合格とする。

### 6.9.4 ガイダンス文書

#### AS09.34：（レベル 1・2・3・4）

クリプトオフィサガイダンスには、次を定めておかななければならない。

- ・ クリプトオフィサが利用可能な暗号モジュールの管理機能、セキュリティイベント、セキュリティパラメタ（及び、必要ならば、パラメタ値）、物理ポート及び論理インタフェース。

**注記** この個別要件は **AS09.36** の一部として試験される。

#### AS09.35：（レベル 1・2・3・4）

クリプトオフィサガイダンスには、次を定めておかななければならない。

- ・ どのように暗号モジュールをセキュアな手段で管理するかに関する手順。

**注記** この個別要件は、**AS09.36** の一部として試験される。

#### AS09.36：（レベル 1・2・3・4）

クリプトオフィサガイダンスには、次を定めておかななければならない。

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

#### ベンダ情報要件

**VE09.36.01**：ベンダが提供する文書は、**AS09.34**、**AS09.35** 及び **AS09.36** で記載された情報を含まなければならない。

**VE09.36.02**：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。

#### 試験手順要件

**TE09.36.01**：試験者は、**VE09.36.01** 及び **VE09.36.02** 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、この個別要件は不合格とする。

**AS09.37 : (レベル 1・2・3・4)**

ユーザガイダンスには、次を定めておかなければならない。

- ・ 暗号モジュールのユーザが利用可能な承認されたセキュリティ機能、物理ポート及び論理インタフェース。

**注記** この個別要件は、**AS09.38** の一部として試験される。

**AS09.38 : (レベル 1・2・3・4)**

ユーザガイダンスには、次を定めておかなければならない。

- ・ 暗号モジュールのセキュアな運用のために必要なすべてのユーザ責任。

**ベンダ情報要件**

**VE09.38.01** : ベンダが提供する文書は、**AS09.37** 及び **AS09.38** で記載された情報を含まなければならない。

**VE09.38.02** : 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。

**試験手順要件**

**TE09.38.01** : 試験者は、**VE09.38.01** 及び **VE09.38.02** 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、この個別要件は不合格とする。

**6.10 その他の攻撃への対処**

**注記** セキュリティレベル 1, 2, 3 の場合は、セキュリティメカニズムの搭載及びその動作の適切さは、それに対する要求事項とそれに対応した試験要件が開発された時に検証される。

**AS10.01 : (レベル 4)**

セキュリティレベル 4 ではその他の攻撃にも対処すると主張する場合、文書は、その追加されたセキュリティを検証するために必要となる適切な方法及び手段の仕様を含まなければならない。

**注記** この個別要件は、単独では試験されない。

**AS10.02 : (レベル 4)**

使用される対処方法をテストするためにテスト方法の仕様が用いられなければならない。

**ベンダ情報要件**

**VE10.02.01** : ベンダが提供する公開セキュリティポリシーは、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。ベンダは公開セキュリティポリシーで、暗号モジュールに実装された、それらの攻撃に対するセキュリティメカニズムを規定しなければならない。

**VE10.02.02** : ベンダが提供する公開用セキュリティポリシーは、どのようにして、実装されたメカニズムが攻撃に対処するかについて示さなければならない。

**試験手順要件**

**TE10.02.01** : 試験者は、ベンダが提供する公開セキュリティポリシーが、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規定していることを検証しなければならない。

**TE10.02.02** : 試験者は、ベンダが提供する公開用セキュリティポリシーが、どのようにして、実装されたメカニズムが攻撃に対処するかについて示していることを検証しなければならない。

**6.11 文書化要求事項**

**AS11.01 : (レベル 1・2・3・4)**

**JIS X 19790** のセキュリティ要求事項の多くは、**JIS X 19790** の**附属書 A** に要約されている特定の文書化要求事項を含んでいる。ユーザマニュアル及び設置マニュアルを含むすべての文書は、評価のためにベンダによって試験機関へ提供されなければならない。

**注記** **JIS X 19790** の**附属書 A** に要約されている文書化要求事項の多くは、関連する要求事項とともに **AS01**～**AS10** 及び **AS12** のもとで規定している。それらを除く文書化要求事項は、**AS11.02**～**AS11.06** で規定する。

**ベンダ情報要件**

**VE11.01.01** : ベンダは **JIS X 19790 附属書 A** の **A.1.1** から **A.1.10** に規定された最小限の文書化項目をすべて記述した、しかしそれに限定されない、暗号モジュールの文書を提供しなければならない。

**試験手順要件**

**TE11.01.01** : 試験者はベンダが **VE11.01.01** に規定された文書を提供していることを検証しなければならない。

**AS11.02 : (レベル 1・2・3・4)**

役割、サービス、及び認証に関する文書は、次の事項を示さなければならない。

- ・ 暗号モジュールが提供するサービス、操作又は機能。これらには、承認されているもの及び承認されていないものを含む。
- ・ 暗号モジュールが提供するそれぞれのサービスにおける、サービス入力、それに対応するサービス出力、及びそれらのサービスを実行できる認可された役割。

**ベンダ情報要件**

**VE11.02.01** : ベンダが提供する文書は、それぞれのサービスを、その目的及び機能を含めて記述しなければならない。

**VE11.02.02** : ベンダが提供する文書は、それぞれのサービスについて、サービス入力、それに対応するサービス出力、及び認可された役割又はサービスを実行できる役割を示さなければならない。サービス入力は、示されたサービス、操作、又は機能を開始若しくは獲得するための、暗号モジュールへのすべ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若しくは獲得されるサービス、操作、又は機能から生じるすべてのデータ出力及び状態出力で構成しなければならない。

**試験手順要件**

**TE11.02.01** : 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ていることを検証しなければならない。試験者は、それぞれのサービスについて、サービス入力、対応するサービス出力、及び認可された役割又はそのサービスを実行できる役割が示されていることもチェックしなければならない。

**TE11.02.02** : 試験者は、次の事項をそれぞれの役割について実行しなければならない。

- 1) 示されたサービスがその役割のために実装されていることを検証するために、その役割のための示されたサービスを、それぞれ実行する。
- 2) 示されたサービス入力のそれぞれを入力して、示されたサービス出力が得られることを観察する。
- 3) 示されていないサービスがその役割のために実装されていないことを検証するために、その役割に対して示されていないサービスの実行を試みる。

**AS11.03 : (レベル 1・2・3・4)**

役割, サービス, 及び認証に関する文書は, オペレータが認可された役割を担うことなく受けられる暗号モジュールのサービスを示し, また, それらのサービスが, どのようにして CSP を変更, 開示又は置換することがないかを示すか, 又はどのようにして暗号モジュールのセキュリティに影響を与えないかを示さなければならない。

**ベンダ情報要件**

**VE11.03.01 :** ベンダが提供する文書は, それぞれのサービスを, その目的及び機能を含めて記述しなければならない。

**VE11.03.02 :** ベンダが提供する文書は, それぞれのサービスについて, サービス入力, 及びそれに対応するサービス出力を示さなければならない。サービス入力は, 示されたサービス, 操作, 又は機能を開始若しくは獲得するための, 暗号モジュールへのすべ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若しく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で構成しなければならない。

**試験手順要件**

**TE11.03.01 :** 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ていることを検証しなければならない。試験者は, それぞれのサービスについて, サービス入力及び対応するサービス出力が示されていることもチェックしなければならない。

**TE11.03.02 :** 試験者は, 次の試験を実行しなければならない。

- 1) 示されたサービス入力のそれぞれを入力して, 示されたサービス出力が得られることを観察する。
- 2) 示されていないサービスがその役割のために実装されていないことを検証するために, その役割に対して示されていないサービスの実行を試みる。

**AS11.04 : (レベル 1・2・3・4)**

物理的セキュリティに関する文書は, 暗号モジュールが, 暗号モジュールの内容に対する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その他の認可された個人による) 物理的アクセスを許すように設計されている場合には, メンテナンスアクセスインタフェースを示し, また, 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に, 保護されていない CSP がどのようにゼロ化されるかを示さなければならない。

**ベンダ情報要件**

**VE11.04.01 :** ベンダが提供する文書は, 暗号モジュールに対して認可されたメンテナンス動作を行う手順を定義しなければならない。

**試験手順要件**

**TE11.04.01 :** 試験者は, ベンダが提供する文書に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述べられている場合には, その文書が暗号モジュールに対する認可されたメンテナンス動作を示していることを検証しなければならない。

**AS11.05 : (レベル 1・2・3・4)**

暗号鍵管理に関する文書は, 暗号モジュールが用いる鍵入力の方法及び鍵出力の方法を示さなければならない。

**ベンダ情報要件**

**VE11.05.01 :** ベンダが提供する文書は, 暗号モジュールが用いる鍵の入力方法及び出力方法を規定しな

なければならない。

#### 試験手順要件

**TE11.05.01**：試験者は、**VE11.05.01** 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。

**TE11.05.02**：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。

#### AS11.06：（レベル 1・2・3・4）

暗号鍵管理に関する文書は、暗号モジュールが用いる鍵の格納方法を示さなければならない。

#### ベンダ情報要件

**VE11.06.01**：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、次の情報を示さなければならない。

- a. タイプ及び識別名
- b. 格納場所
- c. 鍵の格納形式（例えば、平文形式、暗号形式、知識分散形式など）。鍵を暗号化して格納する場合には、鍵の暗号化に用いられる承認された暗号アルゴリズムを示さなければならない。

#### 試験手順要件

**TE11.06.01**：試験者は、**VE11.06.01** 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。

### 6.12 暗号モジュールのセキュリティポリシー

**注記** **JIS X 19790 の附属書 B** は、暗号モジュールセキュリティポリシーの最小限の要求事項を規定する。

#### AS12.01：（レベル 1・2・3・4）

セキュリティポリシーは、**JIS X 19790** の要求事項から導かれる規則、及びモジュール開発を通じて課せられたあらゆる追加の要求事項から導かれる規則を含まなければならない。

#### ベンダ情報要件

**VE12.01.01**：ベンダは **JIS X 19790** の **附属書 B** に規定された最小限の要求事項を満たし、それに限定されない、公開用暗号モジュールのセキュリティポリシーを提供しなければならない。

#### 試験手順要件

**TE12.01.01**：試験者は、ベンダが **JIS X 19790 附属書の B** に規定された最小限の文書化要求事項を満たし、それに限定されない、暗号モジュールのセキュリティポリシーを提供していることを検証しなければならない。

#### AS12.02：（レベル 1・2・3・4）

暗号モジュールのセキュリティポリシーは、**JIS X 19790** の要求事項に基づくセキュリティ規則、及びモジュール開発を通じて課された追加のセキュリティ規則を含む、暗号モジュールが動作中に従わなければならないセキュリティ規則の仕様から構成される。

#### ベンダ情報要件

**VE12.02.01**：（必要ならば）物理的な暗号モジュールの図面又は写真をセキュリティポリシーに含めなければならない。写真は、暗号モジュールのセキュリティ関連特性（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、電源接続など)を示すのに用いてもよい。

**VE12.02.02**：ベンダは、次を含み、**JIS X 19790** の **附属書 B** の要求事項に限定することなく、公開暗号モジュールセキュリティポリシーを提供しなければならない。

- 1) 背景
- 2) 目的
- 3) 識別及び認証ポリシー
- 4) アクセス管理ポリシー
- 5) 物理的セキュリティポリシー
- 6) その他の攻撃への対処ポリシー

#### **試験手順要件**

**TE12.02.01**：試験者は、図面又は写真が試験した暗号モジュールを表していることを検証しなければならない。

**TE12.02.02**：試験者は、ベンダが、次を含み、**JIS X 19790** の**附属書 B** の要求事項に限定することなく、公開暗号モジュールセキュリティポリシーを提供することを検証しなければならない。

- 1) 背景
- 2) 目的
- 3) 識別及び認証ポリシー
- 4) アクセス管理ポリシー
- 5) 物理的セキュリティポリシー
- 6) その他の攻撃への対処ポリシー