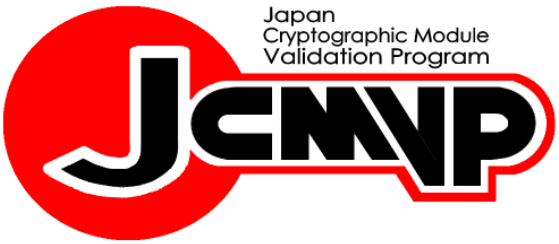

JCMVP
運用ガイダンス

平成 30 年 7 月 1 日

IPA

JIG-01

JCMVP Implementation Guidance

独立行政法人　情報処理推進機構

新しいガイダンス

追加日	内　容
2008/1/28	新規発行
2008/2/20	3.2.3　NIST SP800-90 のベンダ自己確認要求事項
2008/8/7	2.5　エミュレータとシミュレータを使用した試験
2008/8/7	2.6　認証後の問い合わせ
2008/8/7	3.2.4　暗号アルゴリズム確認書に基づく実装の制約事項
2008/8/7	3.2.5　SHS アルゴリズム及び SHS アルゴリズムを用いた上位の暗号アルゴリズムの試験
2008/8/7	3.2.6　複数の承認された動作モード
2008/8/7	3.4.1　許可された役割
2008/8/7	3.6.1　レベル 2 におけるファン、通気孔又はスリットを有する暗号モジュールの不透明性及びプロービング
2008/8/7	3.6.2　タンパー証跡シールのテスト
2009/3/18	2.7　ソフトウェア暗号モジュール又はファームウェア暗号モジュールの認証適合状態の維持
2009/3/18	2.8　再認証の要求事項
2009/3/18	3.7.1　単一オペレータモード及び複数同時オペレータ
2009/3/18	3.7.2　動作環境要求事項の JAVA スマートカードに対する適用
2009/3/18	3.7.3　承認された完全性技術
2009/3/18	3.8.2　パワーアップ自己テストで使用する鍵のゼロ化
2009/3/18	3.8.3　鍵確立、鍵入力、及び鍵出力
2009/3/18	3.9.1　下位の暗号アルゴリズムに対する既知解テスト
2009/3/18	3.9.2　完全性テストで使用される暗号アルゴリズムに対する既知解テスト
2009/3/18	3.9.3　SHS アルゴリズムと SHS アルゴリズムを用いた上位の暗号アルゴリズムの暗号アルゴリズムテスト
2009/8/7	2.9　FIPS140-2 認証済み暗号モジュールの JCMVP 認証取得
2012/2/29	3.2.7　XTS 利用モードを用いた大容量データの暗号化
2012/2/29	3.7.4　承認されたプロテクションプロファイル
2013/2/13	3.16.1　承認された鍵導出関数
2013/6/21	3.1.3　CAVP で認証された Algorithm Certificate
2014/1/17	2.10　暗号アルゴリズム及び鍵長の移行に伴う認証への影響

改正されたガイダンス

改正日	内　容
2008/2/20	2.2　暗号モジュール試験報告書の完成（認証機関に提出すべき情報）の一部修正
2008/2/20	3.8.1　個別要件、試験手順要件、ベンダ情報要件の追加
2008/8/7	3.8.1　擬似乱数生成器の仕様
2009/3/18	2.2　暗号モジュール試験報告書の完成（認証機関に提出すべき情報）の一部修正
2009/3/18	3.2.1　セキュリティ機能のベンダ自己確認

2009/11/10	2.8　　再認証の要求事項の記述を 保証継続を含める形に一部修正
2012/02/29	JIS X 5091 から JIS X 24759 への変更に対応して、次の運用ガイダンスを修正。 2.8, 3.1.1, 3.1.2, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5, 3.2.6, 3.4.1, 3.6.1, 3.6.2, 3.7.1, 3.7.2, 3.7.3 3.8.1, 3.8.2, 3.8.3 3.9.1, 3.9.2, 3.9.3 3.13.1
2013/6/21	FIPS140-2 の適用を許可したことにより、暗号モジュール試験要件の類別を MTR-01 から FIPS140-2 DTR に変更。 3.15.1　擬似乱数生成器の仕様
2018/6/28	3.7.4 URL 更新

目次

JCMVP 運用ガイダンス

制定　平成 20 年 1 月 28 日
最終改正　平成 30 年 6 月 28 日 2018 情セ第 234 号

1. 概要

この文書は、暗号モジュール試験及び認証制度(JCMVP[1])の説明、特に、暗号モジュール試験及び認証制度の基本規程(JCM-01)附属書 A に掲げる暗号モジュールセキュリティ要件への適合を試験するために暗号モジュール試験機関（以下、「試験機関」という。）が使用する、暗号モジュール試験要件に関係する質問への回答及び補足説明（以下、「ガイダンス」という。）を提供することを意図しています。この文書が提示するガイダンスは、試験機関、ベンダ及び他の関心がある団体から寄せられた質問に対して、暗号モジュール認証機関（以下、「認証機関」という。）が行った回答などに基づいています。

この文書の 2 章には、本制度に関するガイダンスを、3 章には暗号モジュール試験要件に関するガイダンスを載せています。3 章のガイダンスはテーマに沿って掲げられています。テーマには複数の要求事項の細分箇条にあてはまるものもありますが、その場合には、最適な細分箇条に掲げています。各テーマの下には、そのガイダンスの発行日を含んだリストがあり、試験手順要件に記載されている関連する個別要件、試験者に課せられる試験手順要件及びベンダに課せられるベンダ情報要件を列記しています。次に、質問又は問題の説明と、関連情報を添えた回答及び補足説明を記載しています。その回答及び補足説明が、列記された項目についての運用ガイダンスです。

[1] Japan Cryptographic Module Validation Program

2. 本制度に関するガイダンス

2.1. JCMVP への問い合わせ

暗号モジュール試験要件	
適用レベル：	全て
発効日：	2008 年 1 月 28 日
最終修正日：	
個別要件：	全般
試験手順要件：	
ベンダ情報要件：	

質問

JCMVPに関する質問は誰にしたらよいですか？また、質問をする場合、所定の書式がありますか？

回答

JCMVPでは、JCMVPのウェブサイトで公開されているお知らせや資料を、最初の回答として参照可能です。JCMVPのウェブサイト上で公開した情報は、JCMVPとしての公式な立場を示しています。

JCMVPの制度に関する質問事項は、下記の認証機関の連絡先まで連絡して下さい。

暗号モジュール試験について試験機関と契約を交わしているベンダは、試験要件についての質問及びその試験要件が、どのように実装の試験に影響を及ぼすか、試験機関と相談して下さい。

試験機関は、試験機関で解決できない試験要件や規格に関する質問事項について、下記の項目内容を認証機関の連絡先に提出して下さい。

試験機関との契約を交わしていないベンダが、暗号モジュール試験の試験要件などに具体的な疑問が生じた場合には、下記の認証機関の連絡先まで連絡して下さい。

質問事項は、電子メールで提出して下さい。

記

質問事項項目：

質問事項として、以下の該当する項目が含まれるようにして下さい。

1. 質問事項が非公開か公開可能かの指定

2. 件名

3. JIS X 19790又はFIPS140-2の選択

4. **個別要件番号**

5. **ベンダ情報要件番号**

6. **試験手順要件番号**

7. **JCMVP運用ガイダンスの記述箇所**

8. **暗号アルゴリズム規格文書の記述箇所**

9. **背景情報**

10. **質問事項を含む問題点の記述**

11. **回答についての提案**

認証機関連絡先：

独立行政法人 情報処理推進機構
セキュリティセンター セキュリティ技術評価部(JCMVP 担当)
E-mail： jcmvp-info@ipa.go.jp

補足説明

2.2. 暗号モジュール試験報告書の完成（認証機関に提出すべき情報）

暗号モジュール 試験要件	
適用レベル：	全て
発効日：	2008 年 1 月 28 日
最終修正日：	2009 年 3 月 18 日
個別要件：	全般
試験手順要件：	
ベンダ情報要件：	

質問

認証機関が認証作業を行うために、試験機関の暗号モジュール試験が完了したとき、どのような情報を認証機関に提出したらいいですか？

回答

試験機関は、次の情報を認証機関に提出して下さい。

1. 公開用セキュリティポリシ＜PDF＞
   要求事項については暗号モジュールセキュリティ要件及び JCMVP 運用ガイダンス 3.13 を参照して下さい。公開用セキュリティポリシは、複写又は配布可能でなければなりません。著作権表示する場合は、複写又は配布可能であることを明記して下さい。

2. 暗号モジュール試験報告書
   暗号モジュール試験報告書内の詳細報告書は認証機関提供の暗号モジュール試験報告書作成支援ツール(以下、「CRYPTIPA」という。)から出力して下さい。

   a. 一般情報＜PDF＞
      様式については付録１を参照。
   b. 所見を含めた詳細報告書＜PDF:CRYPTIPA からの出力＞
   c. 定義／参考文書＜PDF：オプション＞
   d. 物理的セキュリティ試験報告書＜PDF:セキュリティレベル 2,3,4 では必須。ただし、ソフトウェア暗号モジュールを除く＞
      試験機関の物理的セキュリティ試験報告書。必要に応じて写真や図面などを添付。

3. 有限状態モデル＜PDF＞
   状態遷移図及び状態遷移表

4. 再認証のための変更の要約＜PDF：該当する場合＞

試験機関は所見を含めた詳細報告書と共に、注記及び非公開の結果を追加提供することも可能です。PDF ファイルはロックしないで下さい。物理的セキュリティ試験報告書を含む、CRYPTIPA による PDF ファイルでのすべての提出文書は、一つの PDF ファイルに統合して下さい。

補足説明

2.3. 暗号モジュールの設計及び試験

暗号モジュール 試験要件	
適用レベル：	全て
発効日：	2008 年 1 月 28 日
最終修正日：	
個別要件：	全般
試験手順要件：	
ベンダ情報要件：	

質問

暗号モジュールの設計及び試験に関して、試験機関はどのような活動をすることができますか？

回答

以下の情報は独立行政法人 製品評価技術基盤機構が公表している「ASNITE 試験事業者 IT 認定の一般要求事項」を補足するものです。
試験機関の設計、コンサルティング及び試験役割の分離について規定します。
本制度の方針は次の通りです。

1. 試験機関は、次の場合には、暗号モジュールの試験をしてはいけません。
   a. その試験機関が暗号モジュールの一部でも設計した場合
   b. その試験機関が暗号モジュールの一部でもオリジナル文書を作成した場合
   c. その試験機関が暗号モジュールの一部でも組立て、コーディング又は実装をした場合
   d. その試験機関が暗号モジュールの所有権又は利害関係を持っている場合

2. 上記要求事項を満たす場合には、試験機関は以下のベンダの製品を試験することができます。
   a. ベンダ会社が試験機関のオーナーでない場合
   b. 試験機関とベンダの経営陣が全く異なる場合
   c. 試験機関及びベンダ間のビジネスが他のベンダと同様に契約書に基づいて実施される場合

3. 試験機関は、暗号モジュールのライフサイクルの全過程において暗号モジュールセキュリティ要件、暗号モジュール試験要件及びその他の関連する文書の説明をする業務は可能です。

補足説明

上記回答の 3 項のその他の関連する文書には次のものがあります。

- 認証機関により作成された暗号モジュール試験に関する文書（例えば、JCMVP 運用ガイダンス）

また有限状態モデル及びセキュリティポリシの統合又は再編成に関しては JCMVP 運用ガイダンス 2.4 を参照して下さい。

2.4. 有限状態モデル、セキュリティポリシ、ユーザガイダンス及びクリプトオフィサガイダンスの文書

暗号モジュール試験要件	
適用レベル：	全て
発効日：	2008 年 1 月 28 日
最終修正日：	
個別要件：	全般
試験手順要件：	
ベンダ情報要件：	

質問

試験機関は暗号モジュールセキュリティ要件で規定された設計文書を作成することができますか？この設計文書とは、有限状態モデル、セキュリティポリシ、ユーザガイダンス及びクリプトオフィサガイダンスです。

回答

有限状態モデル及びセキュリティポリシ

試験機関は既に開発され設計された暗号モジュールのベンダ作成文書を手に入れ、既存の情報を統合又は再編成可能です。この場合には、暗号モジュール試験報告書を提出するときに、認証機関にそのことを通知して下さい。個々の文書に関する詳細を次に示します。

有限状態モデル：

ベンダから提供された文書には、状態の有限集合、入力の有限集合、出力の有限集合、入力及び状態の集合から状態の集合への写像(すなわち、状態遷移)、並びに、入力及び状態の集合から出力の集合への写像(すなわち、出力機能)に関して記述しなければなりません。

セキュリティポリシ：

ベンダから提供された文書には、暗号モジュールセキュリティ要件のセキュリティ要求事項から得られたセキュリティルール及びベンダによって課された付加的なセキュリティルールを含む、暗号モジュールが動作する上でのセキュリティルールの明確な仕様を記述しなければなりません。

更に、試験機関は統合又は再編成された有限状態モデル及びセキュリティポリシから元のベンダ作成文書に戻れることを示さなければなりません。この対応付けは試験機関により試験記録の一環として維持されなければなりません。

統合及び再編成は次のように定義されます。

- 元の文書はベンダにより準備され、暗号モジュールとともに試験機関に提出されます。

- 試験機関は、元の文書より有限状態モデル及び/又はセキュリティポリシで用いるための技術表現を抽出します。この技術表現は有限状態モデル及び/又はセキュリティポリシを読みやすくするためだけに再編成することができます。技術表現の内容を変更することはでき

ません。

- **試験機関は、読み易くするために有限状態モデル及び/又はセキュリティポリシの記述を変更可能です。これらの記述の変更は試験機関により実施されたことを示すようにして下さい。**

<u>ユーザガイダンス及びクリプトオフィサガイダンス</u>

試験機関はユーザガイダンス、クリプトオフィサガイダンス及び既存の暗号モジュールの設計に関係しないその他の文書を作成可能です。この場合には、暗号モジュール試験報告書提出時に認証機関に通知して下さい。

補足説明

2.5. エミュレータとシミュレータを使用した試験

暗号モジュール 試験要件	
適用レベル：	全て
発効日：	2008 年 8 月 7 日
最終修正日：	
個別要件：	全般
試験手順要件：	
ベンダ情報要件：	

質問

試験機関の試験者は、暗号モジュール試験を実施する場合、暗号モジュールのエミュレーション及び/又はシミュレーションによる方法を使用することができますか？

回答

暗号モジュールの機能試験は、大きく3つに分けられます。暗号モジュールで定義された暗号境界で実施される暗号モジュールの動作試験、操作上のエラー確認試験及び暗号アルゴリズム実装試験です。

1.動作試験

暗号モジュールの動作試験では、エミュレータやシミュレータは禁止されます。暗号モジュールの実際の試験は、暗号モジュールに備わっている、定められたポート、インタフェース及びサービスを用いて実施されなければなりません。

2.エラー確認試験

エミュレータ又はシミュレータは、ソースコードレビューを補完するものとして、暗号モジュールがエラー状態に遷移することを試験するために利用されても問題ありません。どうして試験において実際のモジュールをエラー状態に導く方法が存在しないのかという根拠を、該当する試験手順要件に対して示さなければなりません。

3.暗号アルゴリズム実装試験

暗号モジュールに備わっている、定められたポート、インタフェース及びサービスを用いた暗号アルゴリズム実装試験が望ましい方法です。暗号モジュールで定められたポート、インタフェース及びサービスが、内蔵されている暗号アルゴリズムエンジンへのアクセスを許可しないために、暗号アルゴリズム実装試験が不可能な場合には、以下の2通りの代替的な方法を用いることができます。

a.暗号モジュールの暗号アルゴリズムエンジンへのアクセスを許可し、試験を実施するために、試験機関は試験治具、試験API等を用いて修正してもかまいません。

b.暗号モジュールのシミュレータを用います。

暗号アルゴリズム実装試験の結果を認証機関に提出する場合には、試験が実施された実際の操作環境について具体的な記述がされなければなりません（すなわち、修正されたモジュールの識別又はシミュレーション環境）。暗号モジュール試験報告書を認証機関に提出

する場合には、AS01.12には、なぜ、暗号アルゴリズム実装試験が実際の暗号モジュール上で試験されなかったかを説明する根拠が記載されていなければなりません。

エミュレータは、暗号アルゴリズム実装試験に用いることはできません。

補足コメント

定義：

エミュレータは、暗号モジュールによる振舞いを模擬します。エミュレータの動作の正確さは、エミュレータに入力された情報と、エミュレータがどのように設計されたかによるところが大きくなります。大半の動作が正確に又は確実に模擬されていない場合には、暗号モジュールの実際の動作が、エミュレータのそれと同一であるかどうかは保証できません。

シミュレータは、暗号モジュールの中（すなわち、FPGA 又は、カスタム ASIC）に物理的な情報を組み込む前に、実際の暗号モジュールのソースコード（すなわち、VHDL コード）を実行します。動作という観点から、シミュレータにおけるソースコードの動作は、暗号モジュールに実装された場合又は論理ゲートで実現化されている場合、論理的には同一です。しかしながら、これ以外に実際の動作を変える多くの変数（すなわち、配線遅延、伝送時のエラー、雑音、環境的な原因によるものなど）があります。多くの変数が確実か、否かが識別できない場合には、暗号モジュールの実際の動作が同一であることは保証されません。

2.6. 認証後の問い合わせ

暗号モジュール試験要件	
適用レベル：	全て
発効日：	2008年8月7日
最終修正日：	
個別要件：	
試験手順要件：	
ベンダ情報要件：	

背景

試験機関によって実施された暗号モジュールセキュリティ要件に対する適合性試験及び認証機関による試験結果に対する認証は、その暗号モジュールが暗号モジュールセキュリティ要件に適合している、という保証を提供します。

認証を取得した暗号モジュールのレビューを実施する関係機関は、暗号モジュールセキュリティ要件に適合していない懸念がある場合又は試験においては適合性が判断されていない懸念がある場合、確認のために認証機関に問い合わせをすることがあります。

質問

確認の問い合わせをする手続きはどうすればよいですか？確認の作業はどのように実施されますか？確認することによって、暗号モジュールセキュリティ要件に適合していないと判断された場合、暗号モジュールの認証状態に関して、どのような処理がされますか？

回答

確認の問い合わせは、JCMVP運用ガイダンス 2.1のガイダンスに従って、認証機関に提出されなければなりません。暗号モジュールは、認証番号を参照して識別できなければなりません。技術面で詳細に述べられている箇所は暗号モジュール試験要件の具体的な個別要件が識別されて関係付けられていなければなりません。その要求は公開可能で、認証機関による配布を妨げてはなりません。

認証機関は、識別された暗号モジュールの適合性試験を実施した試験機関に対して公式な要求を修正しないで送付します。試験機関は、問い合わせの価値を判断する間、暗号モジュールのベンダを参加させることもできます。一旦、試験機関によるレビューが終了すると、試験機関は、認証機関に確認の問い合わせに関する技術的な検証の根拠を提供します。試験機関は、暗号モジュールに関する確認の問い合わせに関して次のどちらかの立場を記述します。

1. 確認の問い合わせに価値がなく、その暗号モジュールの認証に変更はない。

2. 確認の問い合わせに価値があり、暗号モジュールの認証に影響がある。試験機関は、認証を継続することについて推奨するかどうか明らかにしなければなりません。

認証機関は、試験機関の立場や試験機関による結論を裏付ける根拠をレビューします。
認証機関がその公式な要求は価値がないと判断した場合、更なる処置は取りません。
認証機関がその公式な要求は価値があると判断した場合、サーベイランスを実施します。

補足説明

2.7. ソフトウェア暗号モジュール又はファームウェア暗号モジュールの認証適合状態の維持

暗号モジュール 試験要件	
適用レベル：	全て
発効日：	2009 年 3 月 18 日
最終修正日：	
個別要件：	全般
試験手順要件：	
ベンダ情報要件：	

質問

認証されたソフトウェア暗号モジュール又はファームウェア暗号モジュールをどのようにすれば認証適合状態を維持して実装できますか？

回答

認証された暗号モジュールのバージョン、それを試験した動作環境及び開発したベンダが暗号モジュール認証製品リストに記述されています。暗号モジュール認証製品リストに記述された情報は、暗号モジュールの認証適合を検討する際の基準として役立ちます。

このガイダンスは次の 3 つの場合を扱います。

・ベンダが暗号モジュールの認証適合を維持していると主張する場合
・ベンダが暗号モジュールの認証適合を維持して変更できると主張する場合
・ユーザが暗号モジュールの認証適合を維持していると主張する場合

このガイダンスは物理的セキュリティがレベル 2 以上で認証されている暗号モジュールには適用されません。

1. ベンダが暗号モジュールの認証適合を維持していると主張する場合

(1)次の項目が維持される場合、ベンダは、認証済みソフトウェア暗号モジュール又はファームウェア暗号モジュールの再コンパイルを実施して、認証適合を維持していると主張できます。

a. 再コンパイルして別の動作環境に移植するためにソースコードの修正(例えばコードの変更、追加、削除）を必要としないソフトウェア暗号モジュールは、以下の条件を満たさなければなりません。

i) レベル 1 の動作環境に対して、ソフトウェア暗号モジュールが汎用コンピュータ上で動作する場合、その汎用コンピュータが、暗号モジュール認証製品リストで特定されている単一ユーザオペレーティングシステム/モードを使用しているか、又は別の互換性のある単一ユーザオペレーティングシステムを使用しているときは、認証適合状態が維持されます。

ii) レベル 2 の動作環境に対して、ソフトウェア暗号モジュールが汎用コンピュータ上で動作する場合、その汎用コンピュータが、特定された CC 評価保証レベル EAL2 のオペレーティングシステム/モード/動作設定を組込んでいるときは、認証適合状態が維持されます。

b. **再コンパイルするのにソースコードの修正（例えば、コードの変更、追加、削除）を必要としないファームウェア暗号モジュール（すなわち、動作環境が適用除外）をある汎用コンピュータ又はプラットフォームから他の汎用コンピュータ又はプラットフォームに移植する場合は、暗号モジュールの認証適合状態が維持されます。**

本制度は、ベンダが認証されたソフトウェア暗号モジュール及びファームウェア暗号モジュールを暗号モジュール認証製品リストで特定されている OS 及び/又は汎用コンピュータから、暗号モジュール試験の一部として含まれていなかった OS 及び/又は汎用コンピュータへ移植すること及び再コンパイルすることを許可しています。認証適合状態は、新しい OS 及び/又は汎用コンピュータ上で暗号モジュールを再試験することなく、新しい OS 及び/又は汎用コンピュータ上で維持されます。しかしながら、本制度は、暗号モジュール認証製品リストに記載されていない OS 及び/又は汎用コンピュータ上に移植されたときに、その暗号モジュールの動作の正当性については保証していません。

2. ベンダが暗号モジュールの認証適合状態を維持して変更できると主張する場合

(1)ソフトウェア又はファームウェア暗号モジュールで、再コンパイルして別のハードウェア又は動作環境に移植するために、セキュリティに関係しないソースコードの修正（例えばコードの変更、追加、削除）を必要とする場合、暗号モジュールが特定の動作環境への、又は特定のハードウェア環境へのコード依存性を持っていないことを確認するために、ベンダは試験機関にレビューの実施及び再認証のための試験報告書作成を依頼し、JCMVP 運用ガイダンス 2.8「再認証の要求事項」の変更シナリオ 1 による確認を受けなければなりません。

(2)暗号モジュール認証製品リスト上の動作環境及び/又はプラットフォームを新しいものに更新することが要求された場合、試験機関は JCMVP 運用ガイダンス 2.8 の変更シナリオ 1 のセキュリティに関係しない変更の要求事項に従うものとし、さらに、JCMVP 運用ガイダンス 2.8 の表 2.8.1 または表 2.8.2 に示されたリグレッションテストを実行しなければなりません。基礎となる暗号アルゴリズム確認は、JCMVP 運用ガイダンス 3.2.5「暗号アルゴリズム確認書に基づく実装の制約事項」の中で規定された要求事項を満たさなければなりません。

再認証により、新しく追加された OS 及び/又はプラットフォームの動作環境に移植されたときの暗号モジュールの正しい動作に関して、本制度は当初の動作環境及びプラットフォームにおける場合と同様の保証を提供します。なお、新しく追加された OS 及び/又はプラットフォームは、暗号モジュール認証製品リスト上で追記されます。

ベンダは「設計保証」の中で適用可能な要求事項をすべて満たさなければなりません。

このガイダンスは、ソフトウェア暗号モジュール又はファームウェア暗号モジュールが実行される動作環境についてのみ述べたもので、その他の暗号モジュールセキュリティ要件には影響を与えません。暗号モジュールは申請しているセキュリティレベルのすべてのセキュリティ要件を満たさなければなりません。

JCMVP 運用ガイダンス 3.2.4「ファームウェア指定」は、ソフトウェア暗号モジュールとファームウェア暗号モジュールの定義を記述しています。

3. ユーザが暗号モジュールは認証適合状態を維持していると主張する場合：

ユーザは認証された暗号モジュールを改変してはいけません。ユーザによるいかなる改変は暗号モジュールの認証を無効にします。

次の項目が維持される場合、ユーザは認証済みソフトウェア暗号モジュール又はファームウェア暗号モジュールの再コンパイルを実施して、認証適合状態を維持していると主張できます。

(1)レベル 1 の動作環境に対して、ソフトウェア暗号モジュールが汎用コンピュータ上で動作する場合で、その汎用コンピュータが暗号モジュール認証製品リストで規特定されている単一ユーザオペレーティングシステム/モードを使用しているか、又は別の互換性のある単一ユーザオペレーティングシステムを使用しているときは、認証適合状態が維持されます。

(2)レベル 2 の動作環境に対して、ソフトウェア暗号モジュールが汎用コンピュータ上で動作する場合で、その汎用コンピュータが、規特定された CC 評価保証レベル EAL2 のオペレーティングシステム/モード/動作設定を組込んでいるか、又は類似のモード及び動作設定を有する、CC 評価保証レベル EAL2 と互換性のある別のオペレーティングシステムを組込んでいるときは、認証適合状態が維持されます。

本制度では、認証書暗号モジュール認証製品リストで特定されている OS 及び/又は汎用コンピュータから試験の一部として含まれていなかった OS 及び/又は汎用コンピュータへの、認証されたソフトウェア暗号モジュールの移植を許可しています。認証適合状態は、新しい OS 及び/又は汎用コンピュータ上の暗号モジュールを再認証に伴う試験をすることなく維持されます。しかしながら、本制度では、認証書暗号モジュール認証製品リストに記載されていない OS 及び/又は汎用コンピュータ上に移植された際に、暗号モジュールが正しい動作をするかどうかについては保証していません。

補足説明

ユーザには、認証書暗号モジュール認証製品リストに特定された開発元ベンダを除く、第三者のインテグレータを含んだあらゆる組織、個人が含まれます。

(注)修正されていないソースコードが利用可能であり、暗号モジュールのセキュリティポリシが、本ガイダンスに対する具体的な例外事項として、受容可能な再コンパイル法について提供されている場合、ユーザは認証後に暗号モジュールを再コンパイルできます。セキュリティポリシで述べられている方法は、本ガイダンスにおける認証適合状態を維持するために、修正されていない状態が保たれていなければなりません。

2.8. 再認証の要求事項

暗号モジュール 試験要件	
適用レベル：	全て
発効日：	2009 年 3 月 18 日
最終修正日：	2012 年 2 月 29 日
個別要件：	全般
試験手順要件：	
ベンダ情報要件：	

質問

既に認証された暗号モジュールの多くの部分を元にした新しい暗号モジュールの認証に関して、認証機関の方針はどのようになっていますか？

回答

既に認証された暗号モジュールの改訂版は、変更部分の割合によって、新たな認証又は再認証となります。

変更シナリオには次の 4 通りがあります。

1. 変更が暗号モジュールセキュリティ要件に関連した事項に影響を与えないハードウェア、ソフトウェア、又はファームウェアに対して行われるとき

   ベンダは、まず、変更が暗号モジュールセキュリティ要件に関連した事項に影響を与えないことを証明するものとして、暗号モジュール認証申請手続等に関する規程の様式 11 に従って「暗号モジュール影響分析報告書」を作成してください。
   次に、ベンダは、作成した「暗号モジュール影響分析報告書」をもとに、再認証の一部である保証継続の妥当性を確認するための事前検討を認証機関に依頼することができます。
   認証機関は、ベンダから提出された「暗号モジュール影響分析報告書」をレビューして、変更が暗号モジュールセキュリティ要件の関連項目に与える影響の有無を検査します。変更箇所が明らかにセキュリティ要件とは無関係と認められ、認証機関が暗号モジュールセキュリティ要件の関連項目への影響がないと判断した場合は、保証継続の手続きを適用することができます。これにより当該暗号モジュール認証の効果を維持することができます。

   認証機関が、暗号モジュールセキュリティ要件の関連項目への影響があると判断した場合、保証継続を適用することはできません。

2. セキュリティの関連項目に関する、ハードウェア、ソフトウェア、又はファームウェアコンポーネントの変更を行ったとき

セキュリティポリシ及び有限状態モデルにおける変更が軽微なもので、その暗号モジュールのセキュリティに関する変更が30%以内の場合、変更された暗号モジュールは、元の暗号モジュールと類似していると考えられ、再認証の手続きを適用することができます。
試験機関は、再認証が十分であるか否かを判断する際に必要な提出文書を特定する責任があり、ベンダは、試験機関が必要な文書を提出する責任があります。提出文書には、以前の試験報告書、設計文書、及びソースコードなどを含めることができます。

試験機関は、修正が影響する個別要件を特定し、その個別要件に関する試験を実施しなければなりません。試験機関は次のことを実施する必要があります。

a. 暗号モジュールの実装形態、及びセキュリティレベルに関する全ての個別要件を見直します。

b. 以前の試験報告書から変更が影響する個別要件を特定します。

c. 以前は試験されなかったが、今回、変更を加えることによって試験が必要になった追加的な個別要件を特定します。

影響する個別要件に対して実施された試験に加え、試験機関は、表2.8.1、表2.8.2のリグレッションテストに含まれる、オペレーション試験に関するリグレッションテストも実施しなければなりません。

試験機関は、変更点の概要とガイドラインの30%未満の変更であることの根拠を提出しなければなりません。認証機関のレビュー時にその変更が30%以上であると判断することがあり、その場合には、全ての試験報告書を提出しなければなりません。
試験機関は、影響を受けたTEに「再試験」と注記した上で、そのTEを文書化し、試験結果に対する所見を記述して、試験報告書として提出して下さい。ベンダは再認証を申請して下さい。
認証機関によるレビューが問題なく行われた場合には、更新バージョンが再認証され、新たな認証書が交付されます。

3. 上述の条件には適合しない、ハードウェア、ソフトウェア、又はファームウェアコンポーネントに変更が行われた場合、暗号モジュールは、新たな暗号モジュールとして、試験機関で全面的に試験が実施されなければなりません。試験機関は、JCMVP運用ガイダンス2.2「暗号モジュール試験報告書の完成」で詳述されている暗号モジュール試験報告書を提出しなければなりません。

暗号モジュールのセキュリティレベルが全面的に変更された場合、又は物理的な変更がされた場合、すなわち、マルチチップスタンドアロンからマルチチップ組込みに変更された場合、暗号モジュールは、新たな暗号モジュールとして、試験機関で全面的に試験が実施されなければなりません。

4. 暗号モジュールのハードウェア、ソフトウェア、又はファームウェアコンポーネントのいずれも変更しないで、ベンダ自己確認のセキュリティ機能が、暗号アルゴリズム実装試験されたとき

試験機関は、暗号アルゴリズム実装試験報告書と以前の試験報告書を認証機関へ提出して下さ

い。暗号モジュール自体に変更箇所がないため、試験機関は動作試験についてリグレッションテストを実施する必要はありません。

認証機関での確認が終了後、セキュリティポリシ、及び承認されたセキュリティ機能の情報は、元の暗号モジュールが登録されている暗号モジュール認証製品リストで更新されます。新たに暗号アルゴリズム実装試験されたセキュリティ機能は、暗号アルゴリズム確認登録簿に追加されます。再認証の申請は必要ありません。

表 2.8.1 リグレッションテスト項目(JIS X 24759)

リグレッションテスト					
AS	TE	セキュリティレベル			
		1	2	3	4
暗号モジュールの仕様					
AS01.03	TE01.03.02	x	x	x	x
暗号モジュールのポート及びインタフェース					
AS02.06	TE02.06.02	x	x	x	x
	TE02.06.04	x	x	x	x
AS02.13	TE02.13.03	x	x	x	x
AS02.14	TE02.14.02	x	x	x	x
AS02.15	TE02.15.02			x	x
AS02.16	TE02.16.02			x	x
役割、サービス及び認証					
AS03.02	TE03.02.02	x	x	x	x
	TE03.02.03	x	x	x	x
AS03.11	TE03.11.03	x	x	x	x
AS03.14	TE03.14.02		x		
AS03.15	TE03.15.02		x		
AS03.16	TE03.16.02			x	x
	TE03.16.03			x	x
AS03.18	TE03.18.02	x	x	x	x
AS03.19	TE03.19.02		x	x	x
AS03.20	TE03.20.02	x	x	x	x
有限状態モデル					
AS04.01	TE04.01.08	x	x	x	x
AS04.03	TE04.03.01	x	x	x	x
物理的セキュリティ					
	なし。				
動作環境					
AS06.05	TE06.05.02	x			
AS06.06	TE06.06.01	x			
AS06.07	TE06.07.01	x	x	x	x
AS06.08	TE06.08.02	x	x	x	x
AS06.11	TE06.11.02		x	x	x

	TE06.11.03		x	x	x
AS06.12	TE06.12.02		x	x	x
	TE06.12.03		x	x	x
AS06.13	TE06.13.02		x	x	x
	TE06.13.03		x	x	x
AS06.14	TE06.14.02		x	x	x
	TE06.14.03		x	x	x
AS06.15	TE06.15.02		x	x	x
AS06.16	TE06.16.02		x	x	x
AS06.17	TE06.17.02		x	x	x
	TE06.17.03		x	x	x
AS06.24	TE06.24.02			x	x
	TE06.24.03			x	x
AS06.26	TE06.26.02			x	x
	TE06.26.03			x	x
AS06.27	TE06.27.02			x	x
暗号鍵管理					
AS07.01	TE07.01.02	x	x	x	x
AS07.02	TE07.02.02	x	x	x	x
AS07.12	TE07.12.02	x	x	x	x
	TE07.12.03	x	x	x	x
	TE07.12.04	x	x	x	x
AS07.19	TE07.19.02	x	x	x	x
	TE07.19.03	x	x	x	x
AS07.21	TE07.21.02	x	x	x	x
AS07.22	TE07.22.02	x	x	x	x
AS07.24	TE07.24.04			x	x
AS07.32	TE07.32.02	x	x	x	x
AS07.33	TE07.33.02	x	x	x	x
自己テスト					
AS08.04	TE08.04.03	x	x	x	x
AS08.05	TE08.05.03	x	x	x	x
AS08.09	TE08.09.02	x	x	x	x
AS08.10	TE08.10.02	x	x	x	x
AS08.12	TE08.12.02	x	x	x	x
AS08.21	TE08.21.07	x	x	x	x
AS08.32	TE08.32.03	x	x	x	x
	TE08.32.04	x	x	x	x
AS08.37	TE08.37.03	x	x	x	x
AS08.38	TE08.38.03	x	x	x	x
設計保証					
AS09.11	TE09.11.02	x	x	x	x
その他の攻撃への対処					
	なし。				
文書化要求事項					

	なし。				
暗号モジュールのセキュリティポリシ					
	なし。				

注）xは試験を実施することを意味します。

表 2.8.2 リグレッションテスト項目(FIPS140-2 DTR)

リグレッションテスト					
AS	TE	セキュリティレベル			
		1	2	3	4
暗号モジュールの仕様					
AS01.03	TE01.03.02	x	x	x	x
暗号モジュールのポート及びインタフェース					
AS02.06	TE02.06.02	x	x	x	x
	TE02.06.04	x	x	x	x
AS02.13	TE02.13.03	x	x	x	x
AS02.14	TE02.14.02	x	x	x	x
AS02.16	TE02.16.02			x	x
AS02.17	TE02.17.02			x	x
役割、サービス及び認証					
AS03.02	TE03.02.02	x	x	x	x
	TE03.02.03	x	x	x	x
AS03.12	TE03.12.03	x	x	x	x
AS03.13	TE03.13.02	x	x	x	x
AS03.14	TE03.14.02	x	x	x	x
AS03.15	TE03.15.02	x	x	x	x
AS03.17	TE03.17.02		x		
AS03.18	TE03.18.02		x		
AS03.19	TE03.19.02			x	x
	TE03.19.03			x	x
AS03.21	TE03.21.02	x	x	x	x
AS03.22	TE03.22.02		x	x	x
AS03.23	TE03.23.02	x	x	x	x
有限状態モデル					
AS04.03	TE04.03.01	x	x	x	x
AS04.05	TE04.05.08	x	x	x	x
物理的セキュリティ					
	なし。				
動作環境					
AS06.05	TE06.05.01	x			
AS06.06	TE06.06.01	x			
AS06.07	TE06.07.01	x	x	x	x
AS06.08	TE06.08.02	x	x	x	x
AS06.11	TE06.11.02		x	x	x
	TE06.11.03		x	x	x
AS06.12	TE06.12.02		x	x	x
	TE06.12.03		x	x	x
AS06.13	TE06.13.02		x	x	x
	TE06.13.03		x	x	x

AS06.14	TE06.14.02		x	x	x
	TE06.14.03		x	x	x
AS06.15	TE06.15.02		x	x	x
AS06.16	TE06.16.02		x	x	x
AS06.17	TE06.17.02		x	x	x
AS06.22	TE06.22.02			x	x
	TE06.22.03			x	x
AS06.24	TE06.24.02			x	x
	TE06.24.03			x	x
AS06.25	TE06.25.02			x	x
暗号鍵管理					
AS07.01	TE07.01.02	x	x	x	x
AS07.02	TE07.02.02	x	x	x	x
AS07.15	TE07.15.02	x	x	x	x
	TE07.15.03	x	x	x	x
	TE07.15.04	x	x	x	x
AS07.25	TE07.25.02	x	x	x	x
AS07.27	TE07.27.02	x	x	x	x
AS07.28	TE07.28.02	x	x	x	x
AS07.29	TE07.29.02	x	x	x	x
AS07.31	TE07.31.04			x	x
AS07.39	TE07.39.02	x	x	x	x
AS07.41	TE07.41.02	x	x	x	x
電磁妨害／電磁両立性					
	なし。				
自己テスト					
AS09.04	TE09.04.03	x	x	x	x
AS09.05	TE09.05.03	x	x	x	x
AS09.09	TE09.09.02	x	x	x	x
AS09.10	TE09.10.02	x	x	x	x
AS09.12	TE09.12.02	x	x	x	x
AS09.22	TE09.22.07	x	x	x	x
AS09.35	TE09.35.05	x	x	x	x
AS09.40	TE09.40.03	x	x	x	x
	TE09.40.04	x	x	x	x
AS09.45	TE09.45.03	x	x	x	x
AS09.46	TE09.46.03	x	x	x	x
設計保証					
AS10.03	TE10.03.02	x	x	x	x
その他の攻撃への対処					
	なし。				
暗号モジュールセキュリティポリシ					
	なし。				

注）xは試験を実施することを意味します。

補足説明

2.9. FIPS140-2 認証済み暗号モジュールの JCMVP 認証取得

暗号モジュール試験要件	
適用レベル：	全て
発効日：	2009年8月7日
最終修正日：	
個別要件：	
試験手順要件：	
ベンダ情報要件：	

質問

既にFIPS140-2認証を取得している暗号モジュールについて、JCMVP制度の要求事項を満足していることを示すためにJCMVP認証を受けようと思います。その場合に、暗号モジュール試験を再度受ける必要がありますか。それとも試験が免除される可能性はありますか？

回答

JCMVP認証制度では2007年4月の正式運用よりセキュリティ要件としてJIS X 19790を採用していますが、それ以前の試行運用で採用しておりましたFIPS140-2ベースの認証も経過措置として認めています。

従ってこの間にFIPS140-2認証を取得した暗号モジュールで、かつFIPS140-2で承認された動作モードにおいて、JCMVPで承認されたセキュリティ機能のみを使用している場合、上記経過措置適用条件を満足することが期待されます。

この条件を満足する場合、既にFIPS140-2認証を取得したベンダはJCMVP制度の試験を再度受ける必要はありません。ベンダはFIPS140-2認証に提出した試験報告書をIPAに提出して下さい。試験報告書の内容を確認して問題がなければ、規程に従って認証書を発行します。

しかしFIPS140-2認証取得後に実装変更した場合は、認証機関がその内容をレビューして再認証または新規認証の判断をし、ベンダはそれに従って試験を受ける必要があります。

補足説明

このガイダンスは2009年12月31日までにFIPS140-2認証を取得した暗号モジュールを対象にします。また、認証費用については再認証として取り扱います。

2.10. 暗号アルゴリズム及び鍵長の移行に伴う認証への影響

暗号モジュール 試験要件	
適用レベル：	**全て**
発効日：	**2014年1月17日**
最終修正日：	
個別要件：	**AS01.12**
試験手順要件：	**TE01.12.01-02**
ベンダ情報要件：	**VE01.12.01-02**

背景

近年、電子計算機の能力向上などの理由により、一部の暗号アルゴリズム及び鍵長における安全性低下が懸念されている。そのため、より安全性の高い暗号アルゴリズム及び鍵長への移行が課題となっている。

米国では、2011年1月に移行計画をまとめた文書であるNIST SP800-131Aが発行された。CMVPにおいては、基本的にSP800-131Aに沿った移行計画を実行する方針を表明している。

日本では、情報セキュリティ対策推進会議により、「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行方針」が発行されている。これは、ハッシュ関数SHA-1及び1024ビット鍵を使用したRSA暗号に関する移行方針を記述した文書である。

このようにJCMVPの一部の承認されたセキュリティ機能ついても影響があることを踏まえた上で、CMVPと足並みを揃えて運用する立場から、JCMVPにおける暗号アルゴリズム及び鍵長の移行は、基本的にCMVPの方針、すなわちSP800-131Aの方針を踏襲する。

JCMVPの「承認されたセキュリティ機能一覧 ASF-01」は、この方針に基づいて、2014年4月に改正される。

質問

2014年4月に施行される、承認されたセキュリティ機能の移行では、暗号アルゴリズム確認と暗号モジュール認証はどのような影響を受けますか?

回答

1. **用語**

1.1 **暗号モジュール認証と暗号アルゴリズム確認に関わる用語**

JCMVPは、認証済みモジュールの実装に変更が加えられるか新たな動作環境が追加されるたびに認証済みモジュール実装の再認証を実行する。これらの変更は新たな実装の認証、及び/又は確認済みの暗号アルゴリズム確認の再確認を要求することがある。

- 新規実装とは、JCMVPによって認証されていない暗号アルゴリズム実装あるいは暗号モジュールのことを言う。

  暗号アルゴリズム実装に対しては、新規実装はこれから試験されるかあるいは認定された試験機関によって試験中であり、その試験報告書が認証機関に提出されるものである。

  暗号モジュールに対しては、新規実装は新しいモジュールであるか、JCMVP運用ガイダンス2.8のシナリオ2と3の下で再認証されるモジュールのことである。これらのモジュールはまだ試験されていないか、認定された試験機関によって試験中であり、その試験報告書が認証機関に提出されるものである。

- 認証済み実装とは、認定された試験機関によって既に試験され、JCMVPによって既に認証されたものをいう。

  暗号モジュール認証は少なくとも1個の承認されたセキュリティ機能の実装を参照する。この参照は暗号アルゴリズム確認された暗号アルゴリズム実装、暗号モジュール認証時には標準が存在しなかった暗号アルゴリズム、あるいは暗号モジュール認証時には暗号アルゴリズム実装試験が利用可能でなかった暗号アルゴリズムを指している。

1.2 暗号アルゴリズムと鍵長の使用分類に関する用語

「使用可」「当面使用可」「制限付き使用可」「互換性維持用」の使用分類の用語を使用して承認されたセキュリティ機能の使用を以下のように分類する。

- 「使用可」は、暗号アルゴリズムと鍵長の使用が安全である、すなわち、セキュリティリスクが現状では知られていないことを意味する。
- 「当面使用可」は、暗号アルゴリズムと鍵長の使用は許可されているが、ユーザがある程度のリスクを受け入れなければならないことを意味する。
- 「制限付き使用可」は、暗号アルゴリズムと鍵長の使用は推奨されず、このアルゴリズムと鍵長の仕様に関して、データの暗号的保護に適用するにあたって追加の制限が要求されることを意味する(例: 暗号化)。
- 「互換性維持用」は、暗号アルゴリズムと鍵長を、暗号的な保護を施すためには当面使用可、制限付き使用可、あるいはかつて承認されていたが現在は非承認となっている暗号アルゴリズムあるいは鍵長を使用して既に保護された情報を処理する(例: 暗号化されたデータの復号、あるいはデジタル署名の検証)ために使用してもよいことを意味する。

暗号アルゴリズムあるいは鍵長は、使用可、当面使用可、制限付き使用可、互換性維持用のいずれにも分類されない場合､その目的に対してはその使用が許可されない(もはや承認されない)。

2.一般的な認証の方針

新規及び認証済み実装に対するJCMVPで採用する一般的な認証の方針は以下の通りである。

- 新規の実装:
  暗号アルゴリズム確認に適用する場合、暗号アルゴリズム実装試験報告書が提出された日に有効なASF-01に従って暗号アルゴリズム確認が行われる。

  暗号モジュール認証に適用する場合、暗号モジュール試験報告書が最初に提出された日に

有効なASF-01に従って暗号モジュール認証が行われる。

新規の暗号モジュール実装に対するセキュリティポリシに関しては4. 文書化要求事項で議論する。

- 認証済みの実装:
  人的資源が許す限り、JCMVPはこれらの実装とその認証の、2014年4月に施行される新しいセキュリティ要求事項への適合性を、移行日を迎えた時点で見直す。

  認証機関は暗号アルゴリズム確認を、確認された暗号アルゴリズムあるいは鍵長が、移行後における承認されたセキュリティ機能であるかどうかを決定するために見直す。完全に暗号アルゴリズム確認が非承認となった場合、認証機関は暗号アルゴリズム確認を取り消す。取り消された暗号アルゴリズム確認への参照は記録目的のために維持される。暗号アルゴリズム確認の一部のみが取り消された場合(例えば、確認された鍵長の1つが承認されていない場合)、取り消された部分について、暗号アルゴリズム確認の一覧上に注記を付す。

  認証機関は暗号モジュール認証の一覧を見直し、暗号モジュールが実装している暗号アルゴリズム確認への参照に基づいて適切な処置を行う。

  - Ø 暗号アルゴリズム確認が取り消された場合、暗号モジュール認証からの参照は「承認されたセキュリティ機能」から削除され、「非承認セキュリティ機能」に移動する。
  - Ø 修正された暗号アルゴリズム確認に対する参照は変更されることなく保持される。すなわち、もし一部の暗号アルゴリズム確認のみが非承認になった場合、認証からの参照は変更されない。
  - Ø その他の暗号アルゴリズムへの参照は、修正を許すような十分な情報が供給された場合に限って変更される。暗号モジュール認証と認証製品リストに掲載された時点で提供された情報は、暗号モジュールが依然として全ての新しいセキュリティ要求事項を満たしているかどうか、すなわち暗号モジュール認証が依然として有効かどうかを判定するために十分ではない可能性がある。したがって、JCMVPは部分的に取消にされた認証にフラグを付す。このフラグは、移行に関する問題を記述するよう適切に更新されたセキュリティポリシがモジュールベンダから自発的に提出されることによって除去されることがある。
  - Ø 暗号モジュールの全ての暗号アルゴリズム確認が取り消された場合、暗号モジュール認証は取り消され、認証リストは認証取消になったことを示す注記が付せられる。記録目的のため、注記が付せられた認証リストの項目は保持される。
  - Ø ユーザのシステムで使用される暗号アルゴリズムと鍵長が移行後の要求事項に適合しているかどうかを確認することはユーザの責任である。JCMVP認証リストに存在する暗号モジュールの実装及び/又は使用に関する全ての疑問はまずベンダの問い合わせ先(各項目にリストされている)に向けられるべきである。
  - Ø 必要に応じて、JCMVPは暗号モジュール認証の項目の情報のみを修正する。しかしながら、暗号モジュール認証のために提供されたセキュリティポリシは、ベンダの要請以外では修正されない。JCMVPはベンダに、適切な版の更新されたセキュリティポリシを提出することを推奨する。更新されたセキュリティポリシは認証機関に直接提出してもよい。更新されたセキュリティポリシはJCMVPのウェブサイトに置かれ、更新されたセキュリティポリシと認証製品リスト上の対応する暗号モジュールは更新されたことを示す注記が付せられる。
  - Ø JCMVP運用ガイダンス 2.8のシナリオ1, 4に沿って再認証された暗号モジュールは、

認証済み実装として取り扱われる。

3. 分類ごとの、暗号アルゴリズム及び暗号モジュールの認証の対応

3.1 使用可

新規の暗号アルゴリズム実装試験報告書あるいは暗号モジュール試験報告書の提出は、承認されたセキュリティ機能として認められる期間内であれば、認証機関に受理される。

JCMVP運用ガイダンス2.8のシナリオ1, 4の下で再認証される暗号モジュールに対して新たな要求事項は付されない。

3.2 当面使用可

一般的に、新規の暗号アルゴリズム実装試験報告書あるいは暗号モジュール試験報告書の提出は、承認されたセキュリティ機能として認められる期間内であれば、認証機関に受理される。

既に認証された暗号モジュール認証は、承認されたセキュリティ機能として認められる期間内は有効である。

当面使用可の乱数生成器の場合、2014年3月末までに限って、新規のモジュール認証の提出は認証機関に受理される。しかしながら、JCMVP運用ガイダンス 2.8のシナリオ1, 2, 4の下でのJCMVPの再認証のために提出され、当面使用可の乱数生成器を含む暗号モジュールは、その乱数生成器が非承認になる2015年12月31日まで受理される。

3.3 制限付き使用可

現在JCMVPで承認された暗号アルゴリズムには、制限付き使用可に分類されるものはない。

3.4 互換性維持用

互換性維持用の分類は、過去に、その時点では使用可、制限付き使用可、あるいは当面使用可であった暗号アルゴリズムか鍵長を適用して保護された情報を処理することを許可することを目的としている。

新規の暗号アルゴリズム実装試験報告書あるいは暗号モジュール試験報告書の提出は、それが非承認になるまでは受理される。

既に認証された暗号アルゴリズム確認及び暗号モジュール認証は、過去に保護された情報を処理する目的に対しては有効であり続ける。

3.5 非承認の暗号アルゴリズムと鍵長

新規の暗号アルゴリズム実装試験報告書又は暗号モジュール試験報告書の提出はJCMVPに受理されない。少なくとも1個の暗号アルゴリズム、及び/又は鍵長で使用可、当面使用可、制限付き使用可、互換性維持用のいずれかに分類されているものを含む暗号モジュールの認証申請は引き続き受理される。

4. 文書化要求事項

新規の認証のために提出されたモジュールセキュリティポリシと認証済みモジュールに提供された(任意提出の)更新されたセキュリティポリシは、JCMVPのウェブサイトの移行表を含むか参照を設けるかをしなければならない。表のデータはユーザに、特定のアルゴリズムと与えられた鍵長を使用することによるリスクを周知する。

この文書化要求事項はこのJCMVP運用ガイダンス2.10の発行の3か月後以降に提出された全ての新規モジュール認証に適用される。この要求事項はJCMVP運用ガイダンス2.8のシナリオ2と3の再認証に対しても適用される。

補足説明

3. 暗号モジュール試験要件に関するガイダンス

3.1. 細分箇条共通のガイダンス

3.1.1. 細分箇条の適用除外条件

暗号モジュール試験要件	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2008 年 1 月 28 日	2013 年 6 月 21 日
最終修正日：	2012 年 2 月 29 日	
個別要件：	全般	全般
試験手順要件：		
ベンダ情報要件：		

質問

暗号モジュールセキュリティ要件の選択された細分箇条に対してのみ認証されることは可能ですか？
暗号モジュールセキュリティ要件のどの細分箇条を適用除外とすることが可能ですか？

回答

認証機関は暗号モジュールが、次に示すように適用除外と指定することのできる細分箇条を除いた、すべての細分箇条に対して少なくともレベル 1 のセキュリティ要求事項を満たさなければ認証書を交付しません。

- **細分箇条の「物理的セキュリティ」は、暗号モジュールがソフトウェアのみのモジュールで物理的保護メカニズムを持たない場合には適用除外と指定可能です。**
- **細分箇条の「動作環境」は暗号モジュールの実装によっては（例えば、暗号モジュールの動作環境が限定動作環境の場合には）適用除外と指定可能です。**
- **細分箇条の「その他の攻撃への対処」は、ベンダが暗号モジュールがそのような保護手段を備えていることを主張しない場合には、適用除外と指定可能です。**

試験機関は暗号モジュール試験報告書で適用除外と記入した細分箇条の根拠を提供しなければなりません。

補足説明

ある細分箇条が適用除外である場合には、その暗号モジュール認証書に N/A と記入されます。
細分箇条の「動作環境」が適用除外である場合でも、暗号モジュール実装によっては、暗号モジュールの構成情報を暗号モジュール認証書に要求されることがあります。（例えば、ファームウェア暗号モジュールは、試験された構成を提示しなければなりません。）

3.1.2. 承認された動作モード及び承認されていない動作モードを持つ暗号モジュール

（承認されたセキュリティ機能及び承認されていないセキュリティ機能を搭載した暗号モジュール）

暗号モジュール試験要件	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2008 年 1 月 28 日	2013 年 6 月 21 日
最終修正日：	2012 年 2 月 29 日	
個別要件：	全般	全般
試験手順要件：		
ベンダ情報要件：		

質問

暗号モジュールが承認されたセキュリティ機能及び承認されていないセキュリティ機能の両方を搭載しているとき、その暗号モジュールはどのように定義することができますか？

回答

承認されたセキュリティ機能及び承認されていないセキュリティ機能の両方を搭載した暗号モジュールは、少なくとも一つの承認された動作モードを持たなければなりません。その動作モードは承認されたセキュリティ機能の動作のみを許可します。このことは暗号モジュールが承認された動作モードにあるとき、承認されていないセキュリティ機能は、承認されたセキュリティ機能の代わりに使用されてはならない（例えば、暗号モジュールが MD5 **と** SHA-1 **を持っている場合には、承認された動作モードでハッシュ機能が要求されたとき、**SHA-1 **が使用されなければなりません。）ことを意味します。オペレータがどのサービスが暗号モジュールセキュリティ要件に適合しているか分かるようにしなければなりません。**
暗号モジュール認証書は暗号モジュールの“承認された動作モード”を識別します。

“承認された動作モード”の選択は特定の暗号モジュールオペレータに限定させる必要はありません。しかし、いずれのオペレータも承認された動作モードが選択されるかどうかを判定できなければなりません。
承認された動作モードが常時選択されている必要はありません。

補足説明

承認された動作モード変更時の CSP **の取扱いについては** JCMVP **運用ガイダンスの** 3.2.2 **を参照して下さい。**

3.1.3. CAVP で認証された Algorithm Certificate

暗号モジュール試験要件	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2013 年 6 月 21 日	2013 年 6 月 21 日
最終修正日：		
個別要件：	AS01.12	AS01.12
試験手順要件：	TE01.12.01	TE01.12.01
ベンダ情報要件：	VE01.12.01	VE01.12.01

背景

JIS X 24759 の VE01.12.01、FIPS140-2 の VE01.12.01 によれば、ベンダはすべての承認されたセキュリティ機能に対して暗号アルゴリズム確認書を提供しなければならないと規定されています。

質問

CAVPで認証されたAlgorithm Certificateを以て、承認されたセキュリティ機能に対する暗号アルゴリズム確認書として提供することはできますか?

回答

JCMVP認証制度では、JCMVPの暗号アルゴリズム確認だけでなく、CAVPで認証された Algorithm Certificateも、JCMVPで承認されたセキュリティ機能であれば、VE01.12.01で提供することを要求するアルゴリズム確認書として受け入れています。

3.2. 暗号モジュールの仕様

3.2.1. セキュリティ機能のベンダ自己確認

暗号モジュール試験要件	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2008年1月28日	2008年1月28日
最終修正日：	2012年2月29日	2009年3月18日
個別要件：	AS01.12	AS01.12
試験手順要件：	TE01.12.01-01	TE01.12.01-01
ベンダ情報要件：	VE01.12.01-02	VE01.12.01-02

背景

暗号モジュールは、承認された動作モードにおいて少なくとも 1 つの承認されたセキュリティ機能を実装しなければならない。承認されていないセキュリティ機能は、承認されていない動作モードにおける利用に含まれる。試験用提供物件には、暗号モジュールで採用した承認された動作モード及び承認されていない動作モードの全てのセキュリティ機能をリスト化し具体的に記載しなければならない。ベンダは、全ての承認されたセキュリティ機能に関する暗号アルゴリズム確認書を提供しなければならない。試験者は、ベンダから提供された暗号アルゴリズム確認書について検証しなければならない。

質問

承認されたセキュリティ機能について暗号アルゴリズム実装試験が利用できない場合でも、承認された動作モードの中で承認されたセキュリティ機能として用いることができますか？その場合、どのように試験され、暗号モジュール認証書及びセキュリティポリシでは、どのような説明がされますか？

回答

1. **新たに承認されたセキュリティ機能が今までにない機能として追加された場合又は新たに承認されたセキュリティ機能が、既存のセキュリティ機能（すなわち新たな共通鍵暗号アルゴリズム、RBG、ハッシュ、電子署名、など）に相当する、新たなセキュリティ機能として追加された場合、暗号アルゴリズム実装試験ツール（以下「JCATT」という。）でそのセキュリティ機能を試験できるようになるまで本制度では次の対応をします。**

   ベンダが新たに承認されたセキュリティ機能（暗号アルゴリズム実装試験はされていないが、「ベンダ自己確認」の注記と共に暗号モジュール認証製品リストにある）を利用することを許可します。

   新たに承認されたセキュリティ機能をJCATTがサポート可能になった場合、本制度では次の対応をします。

   a. **新たな暗号アルゴリズム実装試験報告書の受理猶予期間中（猶予期間は数ヶ月）**
      猶予期間中に新たに承認されたセキュリティ機能は、暗号アルゴリズム実装試験が実施されて暗号モジュール認証製品リストに掲示されるか又は試験が実施されない場合には、「ベンダ自己確認」と注記されて暗号モジュール認証製品リストに掲示されます。

b. **新たな暗号アルゴリズム実装試験報告書の受理猶予期間が終了した場合**
試験済みで暗号アルゴリズム確認書にあるセキュリティ機能のみが許可されます。それ以外のセキュリティ機能については、承認された動作モードでの使用は許可されません。

c. **新たに暗号アルゴリズム実装試験を実施した場合**
ベンダは、暗号アルゴリズム実装試験を実施していない「ベンダ自己確認」されたセキュリティ機能を任意に追加試験することができ、その場合、「ベンダ自己確認」の注記が暗号モジュール認証製品リストから削除されます。

2. **JCMVPでは、承認されているセキュリティ機能を遡及的に承認されていないセキュリティ機能と判断し、承認された動作モードでの使用を許可されないセキュリティ機能に移行させることがあります。その場合、認証機関は承認されているセキュリティ機能から承認されていないセキュリティ機能への移行期間を公表します。**

3. **承認された全てのセキュリティ機能に対して、該当する全てのセキュリティ要件は適合しなければなりません。（すなわち、鍵管理、セルフテスト、など。）**

補足説明

ベンダ自己確認：JCATTによる試験がされておらず、JCMVPが適切な実装又は動作に関する保証を提供していないが、暗号モジュールのベンダがその暗号アルゴリズムが適切に実装されていると確認すること。

「ベンダ自己確認」のセキュリティ機能を暗号モジュールに実装するユーザは、試験がされていないセキュリティ機能の利用に関するリスクを考慮しなければなりません。

試験要件

暗号モジュール試験要件及びCRYPTIPAツールが更新され、公開されるまでは、ベンダ情報要件及び試験手順要件に関して以下の情報を提供して下さい。

ベンダ情報要件

VE01.12.03：ベンダは、「ベンダ自己確認」された全てのセキュリティ機能のリストを提供しなければなりません。

VE01.12.04：ベンダが提供する公開用セキュリティポリシには、「ベンダ自己確認」された全てのセキュリティ機能の情報を含まなければなりません。

試験手順要件

TE01.12.03：試験者は、ベンダが上で述べたような「ベンダ自己確認」された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りません。

TE01.12.04：試験者は、ベンダが提供する文書において、「ベンダ自己確認」されたセキュリティ機能が、どのように関連する規格に適合しているかが具体的に述べられていることを検証しなければなりません。

「ベンダ自己確認」の注記の使用に関する要求事項

「ベンダ自己確認」された承認されたセキュリティ機能は、暗号モジュール認証書及びセキュリティポリシの中で具体的に記載し、適宜、要求される他の注記に加え、暗号アルゴリズム名と本注記（ベンダ自己確認）と共に記載します。

注記の例
承認された＜セキュリティ機能名称＞の実装はベンダ自己確認です。
＜セキュリティ機能名称＞（ベンダ自己確認）

3.2.2. 承認された動作モード

暗号モジュール試験要件	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2008 年 1 月 28 日	2013 年 6 月 21 日
最終修正日：	2012 年 2 月 29 日	
個別要件：	AS01.02,AS01.03,AS01.04	AS01.02,AS01.03,AS01.04
試験手順要件：	TE01.03.01-02,TE01.04.01-02	TE01.03.01-02,TE01.04.01-02
ベンダ情報要件：	VE01.03.01-02,VE01.04.01-02	VE01.03.01-02,VE01.04.01-02

定義

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

質問

承認された動作モードから承認されていない動作モードへ又はその逆に動作モードを変更するときに何か動作上の要求事項がありますか？

回答

AS01.02、AS01.03 及び AS01.04 で規定された要求事項に加えて、暗号モジュールは承認された動作モードと承認されていない動作モード間で CSP を共有しないで下さい。

補足説明

この分離により、承認された動作モードで生成された CSP が、信頼できない取り扱いを受けるリスクを低減できます。

例:

- 暗号モジュールは、承認されていない動作モードで鍵を生成し、その後承認された動作モードに変更して、承認されたサービスにその生成された鍵を使用しないで下さい。
  鍵は承認されていない方法で生成されたかもしれないので、その完全性及び保護は保証することができません。
- 暗号モジュールは、承認されていない動作モードで平文の鍵を電子的に取り込み、その後承認された動作モードに変更して、承認されたサービスにそれらの鍵を使用しないで下さい。
- 暗号モジュールは、承認された動作モードで鍵を生成させ、その後承認されていない動作モードに変更して、承認されていないサービスに生成された鍵を使用しないで下さい。 承認されていない動作モードで承認された鍵の完全性及び保護を保証することができません。

3.2.3. NIST SP800-90 のベンダ自己確認要求事項

	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2008年2月20日	2013年6月21日
最終修正日：	2012年2月29日	
個別要件：	AS01.12	AS01.12
試験手順要件：	TE01.12.01	TE01.12.01
ベンダ情報要件：	VE01.12.01	VE01.12.01

質問／問題

NISTのSP800-90に関して、ベンダ自己確認を主張するためにはNIST SP800-90のどの章を参考にしたらいいですか？

回答

ベンダ自己確認を主張するためには、ベンダはNIST　SP800-90「Recommendation for Random Number Generation Using Deterministic Random Bit Generators(Revised)」の、次の3つの章に適合していることを確認してください。

9章	DRBG Mechanism Functions
10章	DRBG Algorithm Specifications
11章	Assurance

ベンダは、8.6節のエントロピー要件を含めて、8章の要件に適合する必要はありません。エントロピー要件はJIS X 5091のAS.07.10又はFIPS140-2 DTRのAS.07.13で扱われています。

補足説明

NIST SP800-90に記載されている要件は、例えば、SHA、AES及び3-key Triple DESなどの承認されたセキュリティ機能に依存します。NIST SP800-90のベンダ自己確認の前提条件として、使用されている承認されたセキュリティ機能については暗号アルゴリズム確認がなされている必要があります。

NIST SP800-90に関して、ベンダ自己確認を主張するには、次のセキュリティ機能が使用されている場合は、暗号アルゴリズム実装試験がなされ、かつ暗号アルゴリズム確認がされていなければなりません。

- 適用しているハッシュアルゴリズム(SHA-1、SHA-224、SHA-256、SHA-384及び/又はSHA-512)
- 適用しているメッセージ認証コードアルゴリズム(HMAC)
- AES
- 3-key Triple DES

試験要件

ベンダ情報要件

ベンダは、実装が上述の各章の内容を完全かつ正確に実装しているかについて、その証拠を提供して下さい。これは文書及びソースコードレビューによって行われる必要があります。

試験手順要件

試験者は、ベンダの実装が上述で特定した仕様に適合することをベンダの証拠が示していることをレビューしなければなりません。これは文書及びソースコードレビューによって行われる必要があります。試験者は、ベンダが提供した根拠を検証しなければなりません。

3.2.4. 暗号アルゴリズム確認書に基づく実装の制約事項

暗号モジュール試験要件	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2008年8月7日	2013年6月21日
最終修正日：	2012年2月29日	
個別要件：	AS01.12	AS01.12
試験手順要件：	TE01.12.01	TE01.12.01
ベンダ情報要件：	VE01.12.01	VE01.12.01

背景

暗号アルゴリズムの実装確認は暗号アルゴリズム実装試験で行われます。暗号アルゴリズム確認書には試験された実装の名称、バージョン番号及び試験の動作環境が記載されています。

暗号モジュール認証書にも認証された暗号モジュールの名称、バージョン番号及び試験の動作環境が記載されています。

暗号アルゴリズム確認書及び暗号モジュール認証書は、試験中に使われた構成及び動作環境の基準として役立ちます。

質問

暗号モジュールセキュリティ要件の適合性試験が実施されるとき、暗号モジュール内に組込まれている暗号アルゴリズム実装の構成管理及び動作環境に対する要求事項は何ですか？

回答

暗号モジュールセキュリティ要件の適合性試験を実施したソフトウェア暗号モジュール、ファームウェア暗号モジュール又はハードウェア暗号モジュール内に組込まれている承認された暗号アルゴリズムの実装に関して、次の要求事項を満足しなければなりません。

1.暗号アルゴリズム確認された実装が、暗号モジュールへの組込み時に修正されていないこと。
2.JCATT により暗号アルゴリズム実装試験実行時の動作環境と、試験機関により試験されている暗号モジュールの動作環境とが同一であること。

補足説明

3.2.5. SHS[2]アルゴリズム及び SHS アルゴリズムを用いた上位の暗号アルゴリズムの試験

暗号モジュール試験要件	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2008年8月7日	2013年6月21日
最終修正日：	2012年2月29日	
個別要件：	AS01.12	AS01.12
試験手順要件：	TE01.12.01	TE01.12.01
ベンダ情報要件：	VE01.12.01	VE01.12.01

背景

本制度では、実装されたSHSアルゴリズム（SHA-1、SHA-224、SHA-256、 SHA-384 及び SHA-512）ごとに暗号アルゴリズム実装試験を実施します。いくつかの上位の暗号アルゴリズムは、動作の中で、これらのSHSハッシュアルゴリズムを使用しています。

質問

承認された動作モードで使用するための、SHSアルゴリズム及びSHSアルゴリズムを実装している上位の暗号アルゴリズムに対する試験要求事項は何ですか？

回答

承認された動作モードで使用するためには、次のことを実施する必要があります。

- 実装されたSHSアルゴリズムごとに試験されなければなりません。
- DSA、RSA、ECDSA、HMAC、Hash_DRBG、HMAC_DRBG、DH、ECDH及びPSEC-KEMに対しては、実装の組合せごとに試験されなければなりません。

暗号モジュール認証書には、承認された動作モードで使用できるすべての暗号アルゴリズムが記載されます。

補足説明

[2] Secure Hash Standard

3.2.6. 複数の承認された動作モード

	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2008 年 8 月 7 日	2013 年 6 月 21 日
最終修正日：	2012 年 2 月 29 日	
個別要件：	AS.01.03, AS.01.04	AS.01.03, AS.01.04
試験手順要件：	TE.01.03.01-02, TE.01.04.01-02	TE.01.03.01-02, TE.01.04.01-02
ベンダ情報要件：	VE.01.03.01-02, VE.01.04.01-02	VE.01.03.01-02, VE.01.04.01-02

背景

暗号モジュールにおいて、ベンダが複数の承認された動作モードを実装することを許可されています。複数の承認された動作モードを持つ暗号モジュールの例としては、モード毎に異なるサービスの集合を持った暗号モジュールです。

質問

暗号モジュールが複数の承認された動作モードを実装することはできますか？　暗号モジュールが複数の承認された動作モードを実装するための要求事項とは何ですか？

回答

複数の承認された動作モードをサポートするように暗号モジュールを設計してもかまいません。

複数の承認された動作モードを実装する暗号モジュールには、次のことを適用します。

- 異なる承認された動作モードが設定されている場合、全体的なセキュリティレベルを変更することはできません。
- セキュリティポリシは、暗号モジュールに実装された、それぞれの承認された動作モードについてと、それぞれがどのように設定されるかについて記載しなければなりません。
- 承認された動作モードから別の承認された動作モードに再設定した場合、暗号モジュールは動作モード変更に伴う初期化を実行し、パワーアップ自己テストを実施しなければなりません。
- パワーアップ自己テストは、選択された承認された動作モードにおける、承認された全てのセキュリティ機能について実施しなければなりません。
- 再設定することによって、モジュールの物理的なセキュリティレベルが変更される場合、暗号モジュールを再設定する際に、モジュール内の全ての CSP をゼロ化しなければなりません。

複数の動作モードが正しく運用されていることを確認するために、試験者は次のことを実施しなければなりません。

- 承認された動作モードのそれぞれを記載している文書を検証します。
- 公開用のセキュリティポリシに記載されている、ベンダが提供した方法に従って、承認された動作モードをそれぞれ起動します。
- それぞれの承認された動作モード用に実装された、セキュリティ機能のみがアクセス可能で

あり、実装されていないセキュリティ機能にはアクセス不可であることを検証します。

- **上で述べた要件が、承認された全ての動作モードで適合していることを検証します。**
- **AS01.03 及び AS01.04 要件が、承認された全ての動作モードで適合していることを検証します。**
- **CSP が、複数の承認された動作モード間で共有されていないことを検証します。**

補足説明

3.2.7. XTS 利用モードを用いた大容量データの暗号化

	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2012 年 2 月 29 日	2013 年 6 月 21 日
最終修正日：		
個別要件：	AS01.12,AS09.19,AS09.34, AS09.35,AS09.36,AS09.38,	AS01.12, AS10.06, AS10.21, AS10.22, AS10.23, AS10.25
試験手順要件：	TE01.12.01, TE09.19.01, TE09.36.01, TE09.38.01	TE01.12.01, TE10.06.01, TE10.23.01, TE10.25.01
ベンダ情報要件：	VE01.12.01, VE09.19.01, VE09.36.01, VE09.38.01	VE01.12.01, VE10.06.01, VE10.23.01, VE10.25.01

背景

XTS 利用モードの仕様である NIST SP800-38E は、IEEE Std 1619 を参照していますが、その Annex D.4.2 には、一つの鍵で XTS 利用モードを用いて暗号化するデータ容量に関して、ブロック長 n ビットで q ブロックを暗号化している場合の攻撃成功確率は、およそ

$4.5q^2/2^n$

であると記述されています。例えば、1 つの鍵で 1TB のデータを暗号化しようとすると、およそ $q=2^{36}$ なので、攻撃成功確率は $1/2^{53}$ 程度あることになります。

質問／問題

XTS 利用モードを用いる場合、一つの鍵で大容量データを暗号化する際に、どのような注意を払えばよいですか？

回答

XTS 利用モードを用いた暗号モジュールを提供するベンダは、一つの暗号鍵で暗号化可能な最大データ容量を、セキュリティポリシを通じて、利用者に示すことが必要です。

複数の暗号鍵でデータ暗号化を行う場合も、同様の情報をセキュリティポリシに記載する必要があります。

補足説明

3.3. 暗号モジュールのポート及びインタフェース

現在、ガイダンスは発行されていません。

3.4. 役割、サービス及び認証

3.4.1. 認可された役割

	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2008 年 8 月 7 日	2013 年 6 月 21 日
最終修正日：	2012 年 2 月 29 日	
個別要件：		
試験手順要件：		
ベンダ情報要件：		

背景

オペレータは、暗号鍵及びその他の CSP が変更、開示又は置換されないサービス（例えばステータスの表示、自己テスト又は暗号モジュールのセキュリティに影響を与えないその他のサービス）を実行するために役割を担う必要はありません。

暗号モジュールにアクセスするオペレータを認証し、そのオペレータが要求する役割を担うこと及び、その役割に含まれているサービスを実行することが認可されていることを確認するために認証メカニズムが、要求されることがあります。

質問

オペレータが役割を担うことなく実行することが許される、承認されたセキュリティ機能にはどのようなものがありますか?

回答

CSP を生成、修正、公開又は変更もしない次の場合を除き、オペレータは承認されたセキュリティ機能を用いた全てのサービスに対して認可された役割を担います。

・2004 年 2 月 25 日付、FIPS180-2 Change Notice1 の「Secure Hash Standard」で示されたハッシュ関数(SHA-1,SHA-224,SHA-256,SHA-384 及び SHA-512)

・2008 年 3 月付けの NIST の SP800-90「Recommendation for Random Number Generation Using Deterministic Random Bit Generators(Revised)」で示されている決定論的乱数生成器。RBG サービスが、認可された役割として与えられていないオペレータに提供される場合、RBG のエントロピー源とシード入力は、完全に暗号モジュールの境界内に含まれなければならず、オペレータによる操作の対象又は暗号モジュールのサービスによって操作される対象であってはなりません。

・認証用のプロセス（例えば、秘密鍵共有の対称暗号アルゴリズム、認証用の非対称暗号アルゴリズム）。認証メカニズムによるオペレータ認証が完了するまでは、認可された役割が利用を許可されている承認されたセキュリティ機能を使うサービスを使用できてはなりません（例えば、本回答に示すサービスを例外として、オペレータ認証が完了するまでは、電源投入直後であっても承認されたセキュリティ機能を用いたサービスの機能を停止しなけれ

ばなりません)。

・ステータス表示、自己テスト、ゼロ化又はこれ以外の暗号モジュールのセキュリティに影響を及ぼさないサービス

補足説明

3.5. 有限状態モデル

現在、ガイダンスは発行されていません。

3.6. 物理的セキュリティ

3.6.1. レベル 2 におけるファン、通気孔又はスリットを有する暗号モジュールの不透明性及びプロービング

	JIS X 24759	FIPS140-2 DTR
適用レベル：	レベル 2,3,4	レベル 2,3,4
発効日：	2008 年 8 月 7 日	2013 年 6 月 21 日
最終修正日：	2012 年 2 月 29 日	
個別要件：	AS05.52	AS05.49
試験手順要件：	TE05.52.01	TE05.49.01
ベンダ情報要件：	VE05.52.01	VE05.49.01

背景

暗号モジュールは、通常、ファン、通気孔又はスリットの使用を含めた放熱技術の使用を必要とします。暗号モジュールの囲いの中のこれらの開口部又はファンの羽根の隙間が、暗号モジュール内の内部コンポーネント及び構成の観察又はプロービングを可能にするかもしれません。

質問

不透明性の要求事項がセキュリティレベル 2 の暗号モジュールにおける放熱設計にどのように影響しますか？セキュリティレベル 2 の暗号モジュールは通気孔又はスリットからのプロービングを阻止すべきですか？

回答

次のものは不透明性及びプロービングに関連する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の物理的セキュリティの要求事項です。

- 金属製又は堅いプラスティック製の製品グレードの囲いの中に完全に収められ、その囲いにはドア又は除去可能なカバーを含んでもよい形態（セキュリティレベル 1 の要求事項）
- 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。

プロービングの要求事項

プロービングはセキュリティレベル 2 では扱われていません。通気孔又はスリットからのプロービングはセキュリティレベル 3 で取り扱われます。

不透明性の要求事項

不透明性の要求事項の目的は暗号モジュールの内部コンポーネント及び設計情報の直接観察を阻止し、暗号モジュールの構成又は実装を特定不能とすることです。

可視光光源を用いて、囲いの開口部又は半透明な表面から照らす、可視光領域内の目視検査によって、内部コンポーネント（例えば、特定の IC の型名）のベンダ名称及び/又はモデル番号及び/又は設計情報及び構成情報（例えば、PCB の部品配置と配線パターン）を判断できない場合にのみ、暗号モジュールは「不透明」としてみなされます。

コンポーネントのベンダ名称及び/又はモデル番号、及び/又は構成及び暗号モジュールの設

計についての情報を判断できない限り、コンポーネントの形状は、囲いの開口部又は半透明な表面から見えても問題ありません。

暗号モジュール内のすべてのコンポーネントは、セキュリティ要件で規定された不透明性の要求事項を満たさなければなりません。除外された、セキュリティに関係ないコンポーネントは、これらの要求事項を満たす必要はありません。

補足説明

可視光は、400nm から 750nm までの波長帯域内の光として定義されています。

3.6.2. タンパー証跡シールのテスト

	JIS X 24759	FIPS140-2 DTR
適用レベル：	レベル 2、3 及び 4	レベル 2、3 及び 4
発効日：	2008 年 8 月 7 日	2013 年 6 月 21 日
最終修正日：	2012 年 2 月 29 日	
個別要件：	AS05.17,AS05.35,AS05.36,AS05.37, AS05.38,AS05.39,AS05.40,AS05.51, AS05.52, AS05.53, AS05.54	AS05.16,AS05.35,AS05.36,AS05.37, AS05.48, AS05.50
試験手順要件：		
ベンダ情報要件：		

質問

タンパー証跡シールをテストする場合、どのような攻撃手順と攻撃手段が適用されますか？

回答

暗号モジュールにタンパー証跡シールを使用する場合には、タンパー証跡を残さずにシールを剥がして、シールを再利用できてはなりません。例えば、タンパー証跡を残さずに暗号モジュールのシールを剥がすことができ、同じシールを再利用することができるならば、要件を満足していません。

それとは逆に、シールを剥がす試みがタンパー証跡を残し、剥がすことや再利用がタンパー証跡を残す場合や剥がす途中でシールが破損する場合、要件を満足します。タンパー証跡を残さず、オリジナルのシールを破損することもなく剥がし、タンパー証跡を残さずに剥がしたシールを再利用することができるように試験機関は、化学的、機械的、熱的などあらゆる手段を用いなければなりません。

補足説明

攻撃者が攻撃の証拠を覆い隠すために、新しいシールを貼ることは、試験の範囲外です。

3.7. 動作環境

3.7.1. 単一オペレータモード及び複数同時オペレータ

暗号モジュール試験要件	JIS X 24759	FIPS140-2 DTR
適用レベル：	レベル 1	レベル 1
発効日：	2009 年 3 月 18 日	2013 年 6 月 21 日
最終修正日：	2012 年 2 月 29 日	
個別要件：	AS06.04	AS06.04
試験手順要件：	TE06.04.01, TE06.04.02	TE06.04.01
ベンダ情報要件：	VE06.04.01	VE06.04.01

質問

AS06.04 では「（レベル 1 のみ）オペレーティングシステムは単一オペレータ動作モードに限定されなければならない。（即ち複数同時オペレータは明示的に除外されている）」と記述されています。この文脈で複数同時オペレータの定義はどのようになっていますか？特に、レベル 1 のソフトウェア暗号モジュールはサーバに実装して本制度の認証を受けられますか？

回答

クライアント／サーバアーキテクチャに実装されたソフトウェア暗号モジュールはクライアント及びサーバの両方で使用されることが意図されています。暗号モジュールは暗号機能をクライアント及びサーバアプリケーションに提供するために使用されます。暗号モジュールがサーバ環境で実装されている場合には、サーバアプリケーションが暗号モジュールのユーザです。サーバアプリケーションは暗号モジュールを呼び出します。そのため、サーバアプリケーションが、複数のクライアントに対応していても、サーバアプリケーションは、暗号モジュールにとっての単一ユーザになります。

AS06.04は、暗号モジュールの動作環境において、暗号モジュールが使用するメモリが、(暗号、非暗号を問わず)他のプロセスから分離されていることを要求する個別要件です。本ASの注記では、次のように述べられています。
「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。」

従って、本ASは、オペレーティングシステムだけではなく、暗号モジュールの実装に対する個別要件でもあることに注意してください。

本ASに不適合となる例としては、最新のオペレーティングシステムを使用していても、共有メモリを使用して他のプロセスとデータを共有するような暗号モジュールの実装が挙げられます。

補足説明

この情報は公開セキュリティポリシに含まれなければなりません。

3.7.2. 動作環境要求事項の JAVA スマートカードに対する適用

	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2009 年 3 月 18 日	2013 年 6 月 21 日
最終修正日：	2012 年 2 月 29 日	
個別要件：	AS06.01	AS06.01
試験手順要件：		
ベンダ情報要件：		

質問

スマートカードが、JAVA アプレット(それが暗号モジュール認証を取得しているかに関わらず)を受け付けて走らせているような変更不可能なオペレーティングシステムを実装している場合、限定動作環境であると言えますか?

回答

全ての JAVA カード暗号モジュールに適用できる一般的な説明をすることはできません。なぜなら、暗号モジュールごとに機能及び設計が非常に異なる可能性があるからです。判断は試験のために利用可能な（ベンダから提供された）暗号モジュールの完全な文書を持っている試験機関に委ねられます。しかしながら、一般的に、認証後に認証されていないアプレットをロードできる JAVA カード暗号モジュールは、ある種の変更可能な動作環境であると見なされ、「動作環境」の要求事項が適用されます。

次のいずれかの変更可能な動作環境を持つ JAVA カード暗号モジュールは、限定動作環境を持つと考えられます。そして、暗号モジュール試験報告書の「動作環境」の要求事項の節は、“ 適用除外 ” と記載できます。

a)アプレットのローディングができないように構成されている。
b)JCMVP で認証されたアプレットのみをロードしている。

認証された JAVA カード暗号モジュールは、ロードされたすべてのアプレットに対して承認された認証技術を用いなければなりません。また、この暗号モジュールは、少なくとも、その他の適用可能な個別要件と同様に、AS09.11,AS09.12（FIPS140-2 DTR では AS09.34,AS09.35, AS10.03 及び AS10.04）の要求事項を満たさなければなりません。暗号モジュールの認証状態は、スマートカード自身の認証過程で試験及び認証されたか又は独立して認証された（すなわち、アプレット自身も自分の認証番号を持っている）アプレットをロードすることにより維持されます。

認証されたスマートカード暗号モジュールのセキュリティポリシは次のことを記述しなければなりません。

- 認証されたスマートカード暗号モジュールのセキュリティポリシは、暗号モジュールが、(アプレットが認証済みかどうかにかかわらず)、認証後にアプレットをロードすることができるか否かを記述しなければなりません。(注：ただし、暗号モジュールが認証後に認証されていないアプレットをロードできる場合には、セキュリティポリシは、もし、認証されていないアプレットがロードされれば、暗号モジュールの認証適合状態が無効であることを

明確に示さなければなりません。）

・認証された暗号モジュール内に格納される全てのアプレットについて、その名前とバージョン番号が登録されていなければなりません。

補足説明

認証された暗号モジュール内に含まれる全てのアプレットの名前及びバージョン番号は、暗号モジュールの認証書及び暗号モジュール認証製品リストに記載されます。

3.7.3. 承認された完全性技術

	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2009 年 3 月 18 日	2013 年 6 月 21 日
最終修正日：	2012 年 2 月 29 日	
個別要件：	AS06.08	AS06.08
試験手順要件：	TE06.08.01、TE06.08.02	TE06.08.01、TE06.08.02
ベンダ情報要件：	VE06.08.01	VE06.08.01

背景

「承認された完全性技術(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)を使用する暗号メカニズムは暗号モジュールの中ですべての暗号ソフトウェア及びファームウェアコンポーネントに適用されなければならない。」とセキュリティ要件にあります。

質問／問題

AS06.08 で規定される、承認された完全性技術とは何ですか、そして、それはいつ実行されなければなりませんか？

回答

承認された完全性技術とは、承認された暗号セキュリティ機能を使用している鍵付き暗号メカニズムです。 それにはデジタル署名、HMAC 及び CMAC が含まれています。 承認されたセキュリティ機能の一覧は http://www.ipa.go.jp/security/jcmvp/algorithm.html に記載されています。

承認された完全性技術は、パワーアップ自己テストに用いられ、すべてのパワーアップ自己テストの要求事項を満たさなければなりません。

補足説明

3.7.4. 承認されたプロテクションプロファイル

	JIS X 24759	FIPS140-2 DTR
適用レベル：	2	2
発効日：	2012 年 2 月 29 日	2013 年 6 月 21 日
最終修正日：		
個別要件：	AS06.10	AS06.10
試験手順要件：	TE06.10.01	TE06.10.01
ベンダ情報要件：	VE06.10.01	VE06.10.01

背景

JIS X 19790 では、セキュリティレベル 2 の暗号モジュールに対する動作環境に関して「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」を要求しています。

質問／問題

JIS X 19790 のセキュリティレベル 2 を満たすために、使用可能なオペレーティングシステムはありますか？

回答

JIS X 19790 は、ISO/IEC 15408 の最新版を参照しているため、CC Ver.3.1 に基づいて評価されたオペレーティングシステムが必要になります。
JIS X 19790 の附属書 C に記載されている Controlled Access Protection Profile (CAPP), Version 1.d は、CC Ver.2.x に基づいて評価されたプロテクションプロファイル(PP)であり、CAPP に基づいて評価・認証されたオペレーティングシステムは、JIS X 19790 と組み合わせて使用することは出来ません。

JIS X 19790 の附属書 C に記載された PP の代わりに、CC Ver.3.1 で評価された次の PP に基づいて評価されたオペレーティングシステムをセキュリティレベル 2 の暗号モジュールに対する動作環境として使用可能です。

U.S. Government Approved Protection Profile - U.S. Government Protection Profile for General-Purpose Operating Systems in a Networked Environment, CC Version 3.1, 30 August 2010
https://www.niap-ccevs.org/MMO/PP/pp_gpospp_v1.0.pdf

補足説明

3.8. 暗号鍵管理

3.8.1. 3.15.1 に移動

3.8.2. パワーアップ自己テストで使用する鍵のゼロ化

暗号モジュール試験要件	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2009年3月18日	2013年6月21日
最終修正日：	2012年2月29日	
個別要件：	AS07.33	AS07.41
試験手順要件：	TE07.33.01-04	TE07.41.01-04
ベンダ情報要件：	VE07.33.01	VE07.41.01

背景

暗号モジュールセキュリティ要件の暗号鍵管理に関する個別要件には、保護されていない CSP の全てをゼロ化するための方法を暗号モジュールが提供しなければならないことが規定されています。

質問

パワーアップ自己テストを実行するためだけに暗号モジュールによって使用される暗号鍵は、CSP とみなされ、ゼロ化が要求されますか？

回答

パワーアップ自己テストを実行するためだけに暗号モジュールによって使用される暗号鍵は、CSP とはみなされません。従って、これらは個別要件 AS07.33（FIPS140-2 DTR では AS07.41）で要求されるゼロ化の対象ではありません。

補足説明

3.8.3. 鍵確立、鍵入力及び鍵出力

暗号モジュール試験要件	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2009年3月18日	2013年6月21日
最終修正日：	2012年2月29日	
個別要件：	全般	全般
試験手順要件：		
ベンダ情報要件：		

質問

鍵確立の方法及び鍵の入出力の方法の組み合わせにおいて様々な暗号モジュールの実装形態がありますが、「暗号モジュールのポート及びインタフェース」、「鍵確立」、及び「鍵入出力」の要求事項をそれぞれの組み合わせにどのように当てはめればよいですか？

回答

次のガイドラインを利用して、最初に鍵がどのようにして暗号モジュールで確立されるかを決定します。一旦、確立方法が決定すれば、鍵入力フォーマットの表3.8.3.1によって、鍵がどのように入力、又は出力されるべきかの要求事項が示されます。

- **用語及び定義**
  - **CM: 認証済みの暗号モジュール**
  - **CM ソフトウェア: 認証済みのソフトウェア暗号モジュール。**
  - **CM ハードウェア: 認証済みのハードウェア暗号モジュール。**
  - **GPC: 汎用コンピュータ又は汎用コンピュータで利用できることを表す。**
  - **EXT: CMソフトウェアの物理的境界の外部にあることを表す。**
  - **EXT CMハードウェア: 当該暗号モジュールの物理的暗号境界外にある暗号モジュール。スタンドアロン型の暗号モジュールも含まれる。**
  - **EXTポート: CMの物理的暗号境界上にある入出力ポート。**
  - **INT: CMソフトウェアの物理的暗号境界の内部にあることを表す。**
  - **INT CM ハードウェア: CMソフトウェアの物理的境界の内部にある暗号モジュール。具体例としては、PCIカードに実装された暗号アクセラレータなどが挙げられる。**
  - **INTパス： CMソフトウェアの物理的暗号境界内部にある物理的パス。具体例としてはPCIバスなどが挙げられる。**
  - **INTポート: CMソフトウェアの物理的暗号境界内部にあるポート。具体例としては、PCIスロットなどが挙げられる。**
  - **App ソフトウェア: CMソフトウェアの物理的暗号境界の内側で動作する、暗号機能をもたない、又は非承認のアプリケーションソフトウェア。**

表3.8.3.1 － 鍵確立		
MD: 手動配送	ME: 手動入出力	
ED: 電子的配送	EE: 電子的入出力	
GPCキーボードからCMソフトウェア*		MD/ME
CMソフトウェア*へ／からGPCキーローダ（例：フロッピーディスク、USBトー		MD/EE

クン、その他）	
CMソフトウェア*へ／からGPC　EXTポート（例：ネットワークポート）	ED/EE
INTパス経由でCMソフトウェア*からCMソフトウェア*へ	適用除外
INTパス経由でCMソフトウェア*へ／からGPC App ソフトウェア	適用除外
INTパス経由でCMソフトウェア*へ／からGPC INT CMハードウェア	適用除外
CMソフトウェア*へ／からネットワークに接続していないGPCで動作中のEXT CMハードウェア（キーローダ）	MD/EE
CMソフトウェア*へ／からネットワークに接続しているGPCで動作中のEXT CM ハードウェア	ED/EE
INTパス経由でINT CMハードウェアへ／からGPC App ソフトウェア	ED/EE
INTパス経由でINT CMハードウェアへ／からGPC EXTポート	ED/EE
INTパス経由でGPC キーボードからINT CMハードウェア	ED/EE
INT CMハードウェアへ／からそれが直接接続されているキーローダ	MD/EE
キーボードからそれが直接接続されている CMハードウェアへ	MD/ME
EXT CMハードウェアへ／からネットワーク接続されたGPC	ED/EE
EXT CMハードウェアへ／からそれが直接接続されたキーローダ（ネットワーク接続されていないGPCは、キーローダと見なすことができる。）	MD/EE
＊CMソフトウェアは、AS.06.04、AS06.05、AS.06.06に適合しなければなりません。	

次の図は、上述の鍵確立の表の具体例を示したものです。

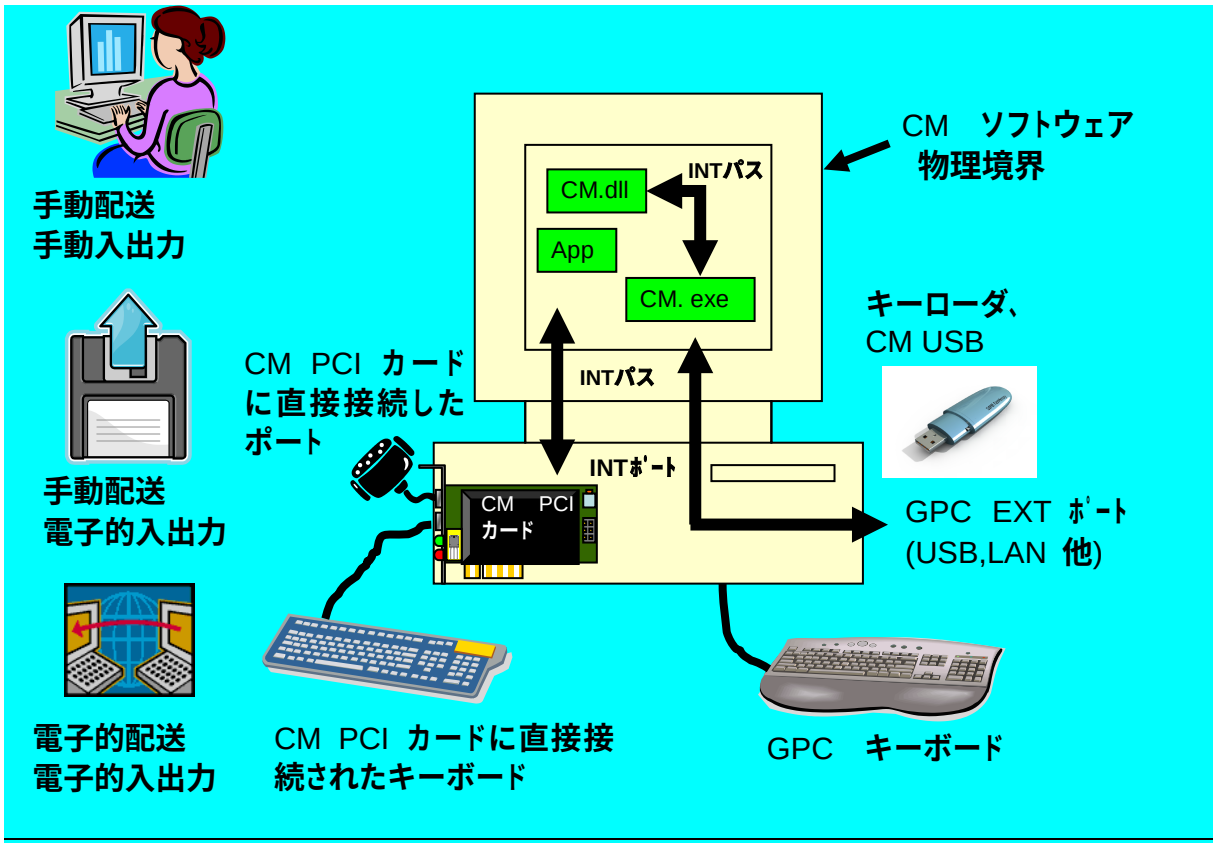

表3.8.3.2 － 鍵の入出力形式

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="8">配送（確立）</td></tr>
<tr><td colspan="4">手動</td><td colspan="4">自動</td></tr>
<tr><td rowspan="5">入力／出力</td><td rowspan="2">手動</td><td colspan="4">キーボード、サムホイール、スイッチ、ダイヤル</td><td colspan="4" rowspan="3"></td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td>P/E</td><td>P/E</td><td>E/SK</td><td>E/SK</td></tr>
<tr><td rowspan="3">電子的</td><td colspan="4">スマートカード、トークン、ディスク、及びキーローダ</td><td colspan="4">鍵配送、又は鍵共有</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td>P/E</td><td>P/E</td><td>E/SK</td><td>E/SK</td><td>E</td><td>E</td><td>E</td><td>E</td></tr>
</table>

解説

P/E: 平文、または暗号化。
E: 暗号化。
E/SK: 暗号化、又は平文による知識分散方法（分離された物理的なポート、又は高信頼パス経由による）

レベル3、及びレベル4では、平文の鍵コンポーネントは、物理的に分離されたポート、又は高信頼性パスを使った論理的に分離されたポートを経由して入力することができます。マニュアルで入力する平文の鍵は、知識分散方法を用いて入力しなければなりません。鍵は、暗号化して手動で入力することもできます。自動的な手段を用いる場合には、必ず暗号化しなければなりません。

補足説明

本ガイダンスでは、手動による配送方法や暗号モジュールへの電子的入力、又は出力を用いて確立される鍵は、レベル1、及びレベル2においては平文で入力、又は出力が可能であることを再確認しています。

3.9. 自己テスト

3.9.1. 下位の暗号アルゴリズムに対する既知解テスト

暗号モジュール試験要件	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2009年3月18日	2013年6月21日
最終修正日：	2012年2月29日	
個別要件：	AS08.17	AS09.19
試験手順要件：	TE08.17.01-03	TE09.19.01-03
ベンダ情報要件：	VE08.17.01-02	VE09.19.01-02

背景

下位の暗号アルゴリズムは承認された動作モードでの動作のために、しばしば、上位の暗号アルゴリズムに組み込まれます（例えば、HMAC-SHA-256 及び RSA に組み込まれた SHA-256 アルゴリズム、RBG に組込まれた AES 又は 3-key Triple　DES アルゴリズム）。承認された動作モードで使用される承認された暗号アルゴリズムを実装する暗号モジュールは、パワーアップ時に自己テストの一部として既知解テストを実行することを要求されています。この要求事項は、下位の暗号アルゴリズム実装においても有効です。しかしながら、暗号モジュールが上位の暗号アルゴリズムにおいて既知解テストを実行する場合には、下位の暗号アルゴリズムもまた、自己テストが実施されたことになる場合もあります。

質問

下位の暗号アルゴリズムが、その組み込まれている上位の暗号アルゴリズムの既知解テストの中で自己テストされる場合、暗号モジュールは下位の暗号アルゴリズムの既知解テストを別途、実装する必要がありますか？

回答

次の全ての条件が満たされれば、暗号モジュールは下位の暗号アルゴリズムの既知解テストを実施する必要はありません。

1. **上位の暗号アルゴリズムがその実装を用いている。**
2. **上位の暗号アルゴリズムがパワーアップ時に既知解テストを実施している。**
3. **下位の暗号アルゴリズム内のすべての暗号機能がテストされている（例えば、AES に対する暗号化及び復号）。**

補足説明

暗号モジュールが下位の暗号アルゴリズムのいくつかの実装を含み（例えば、**SHA-256** アルゴリズムの異なるいくつかの実装）、その暗号アルゴリズムに、他の上位の承認された暗号アルゴリズムで使用されない実装がある場合には（それゆえ、自己テストが実施されない）、その暗号モジュールは、それぞれの実装に対して、電源投入時の既知解テストを実行しなければなりません。

ANSI X9.31 に記載されているような RNG 内の AES 又は 3-key Triple DES の実装はすべての AES 又は 3-key Triple　DES の暗号機能がテストされていないため（例えば、暗号化は RNG 生成で実行されますが、復号は実行されていません）、上記の第 3 項を満たしません。

3.9.2. 完全性テストで使用される暗号アルゴリズムに対する既知解テスト

暗号モジュール試験要件	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2009年3月18日	2013年6月21日
最終修正日：	2012年2月29日	
個別要件：	AS06.08, AS08.14	AS06.08, AS09.16
試験手順要件：	TE06.08.01-02, TE08.14.01-02	TE06.08.01-02, TE09.16.01-02
ベンダ情報要件：	VE06.08.01, VE08.14.01	VE06.08.01, VE09.16.01

背景

AS06.08 は、承認された完全性の技術を用いた暗号メカニズムが暗号モジュール内のすべての暗号ソフトウェアコンポーネント及び暗号ファームウェアコンポーネントに対して適用されなければならないことを要求しています。また、既知解テストを用いた暗号アルゴリズムテストは暗号モジュールに実装され、承認された動作モードで使用されている、それぞれの承認された暗号アルゴリズムのすべての暗号機能について実施されなければならないことを要求しています。

質問

暗号モジュールは、承認された完全性の技術で使われている下位の暗号アルゴリズムに対して既知解テストを別途、実装する必要がありますか？

回答

承認された完全性の技術で使われている下位の暗号アルゴリズムのすべての暗号機能（例えば、AES の暗号化及び復号）がテストされている場合には、暗号モジュールは、その下位の暗号アルゴリズムに対して既知解テストを別途、実装する必要はありません。

根拠

暗号モジュールはソフトウェア/ファームウェア自身を暗号アルゴリズムへの入力として使用し、既知解を期待される出力として使用するため、承認された完全性の技術を用いたソフトウェア/ファームウェアの完全性テストは既知解テストと考えられます。

例：HMAC-SHA-256 が、ソフトウェアコンポーネント又はファームウェアコンポーネントを検証するために承認された完全性の技術として使用される場合には、既知解テストは HMAC-SHA-256 又は下位の SHA-256 アルゴリズムに対して要求されません。

例：RSA が、ソフトウェアコンポーネント又はファームウェアコンポーネントの署名を検証するために使用される場合には､完全性テストは RSA の署名生成機能を使用しないため､RSA の既知解テストは要求されます。しかしながら、下位のハッシュ関数の既知解テストは要求されません。

補足説明

3.9.3. SHS アルゴリズムと SHS アルゴリズムを用いた上位の暗号アルゴリズムの暗号アルゴリズムテスト

暗号モジュール試験要件	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2009年3月18日	2013年6月21日
最終修正日：	2012年2月29日	
個別要件：	AS08.14	AS09.16
試験手順要件：	TE08.14.01	TE09.16.01
ベンダ情報要件：	VE08.14.01	VE09.16.01

背景

暗号アルゴリズムテスト

既知解を用いた暗号アルゴリズムテストは、暗号モジュールによって実装された、それぞれの承認された暗号アルゴリズムの暗号機能（例えば、暗号化、復号、認証、及び乱数生成）のすべてについて実行されなければなりません。既知解テストは、正しい出力が既に分かっている入力データを使って暗号アルゴリズムを動作させ、計算された出力と過去に生成された出力（既知解）とを比較します。計算された出力が既知解と異なる場合には、既知解テストは失敗でなければなりません。

与えられた一組の入力値に対して出力値が変化する暗号アルゴリズム（乱数生成などが実装に含まれているために出力値が固定ではない暗号アルゴリズム、例えば、デジタル署名アルゴリズム）は、既知解テスト又は鍵ペア整合性テストを用いてテストされなければなりません。

承認された動作モードで使用される各暗号アルゴリズムの実装は暗号アルゴリズムテストを実行しなければなりません。暗号アルゴリズムテストは、パワーアップ時又はオンデマンドで実行される暗号アルゴリズム実装のヘルスチェックです。

質問

SHS アルゴリズム及び SHS アルゴリズムを実装した上位の暗号アルゴリズムを、承認された動作モードで使用可能にするために、既知解テストに課せられた最小限の要求事項は何ですか？また、パワーアップ時又はオンデマンドで実行される場合、公開鍵と秘密鍵の鍵ペア整合性テストに課せられた最小限の要求事項は何ですか？

回答

以下は、暗号アルゴリズムの既知解テストに特有のガイダンスです。

1.SHS アルゴリズムのための最小限の要求事項です。

- SHA-1 が実装される場合は既知解テストが必要です。
- SHA-256 が実装される場合は既知解テストが必要です。
- SHA-224 が SHA-256 の実装を使わずに実装される場合には、SHA-224 の既知解テストが必要です。
- SHA-512 が実装される場合は既知解テストが必要です。
- SHA-384 が SHA-512 の実装を使わずに実装される場合には、SHA-384 の既知解テス

トが必要です。

2.DSA 及び RSA が実装される場合は既知解テスト又は鍵ペア整合性テストが必要であり、以下の条件で実行する必要があります。

- 最小限、JCMVP で承認された範囲で暗号モジュールがサポートしている最小の法のビット長、又は DSA 素数で実行します。
- 最小限、上位の暗号のアルゴリズムによって使用されている、下位に実装された SHS アルゴリズムのいずれか一つを実行します。

3.RSAの既知解テストは、公開、及びプライベート指数（eとd）の両方を用いて、実行しなければなりません。この2つの指数は、$[d * e = 1(\mathrm{mod}(p - 1)(q - 1))]$を満足しなければなりません。

4.ECDSA が実装される場合は既知解テスト又は鍵ペア整合性テストが必要であり、少なくとも以下の条件で実行する必要があります。

- 2 種類の体（即ち素体 GF(p)と標数 2 の体 GF(2^m)）の内、実装されている種類の体上の少なくとも 1 個ずつの曲線で実行します。
- 上位の暗号のアルゴリズムによって使用されている、下位に実装された SHS アルゴリズムの任意のひとつを実行します。

5.HMAC が実装される場合は既知解テストが必要であり、最小限、下位に実装された SHS アルゴリズムの任意のひとつについて実行しなければなりません。

補足説明

3.10. 設計保証

現在、ガイダンスは発行されていません。

3.11. 他の攻撃への対処

現在、ガイダンスは発行されていません。

3.12. 文書化要求事項

現在、ガイダンスは発行されていません。

3.13. 暗号モジュールのセキュリティポリシ

3.13.1. 暗号サービスを記述するときの詳細度

暗号モジュール試験要件	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2008 年 1 月 28 日	2013 年 6 月 21 日
最終修正日：	2012 年 2 月 29 日	
個別要件：	AS01.02,AS01.03,AS01.12,AS01.16, AS01.17,AS09.19,AS12.01,AS12.02	AS01.02,AS01.03,AS01.12,AS01.16, AS03.14,AS10.06,AS14.02,AS14.03, AS14.04,AS14.06,AS14.07
試験手順要件：	TE01.03.01,TE01.03.02,TE01.17.01, TE09.19.01,TE12.01.01,TE12.02.01, TE12.02.02	TE01.03.01,TE01.03.02,TE01.16.01, TE03.14.01,TE10.06.01,TE14.07.01, TE14.07.02
ベンダ情報要件：	VE01.03.01,VE01.03.02,VE01.17.01, VE09.19.01,VE12.01.01,VE12.02.01, VE12.02.02,	VE01.03.01,VE01.03.02,VE01.16.01, VE03.14.01,VE03.14.02,VE10.06.01, VE14.07.01,VE14.07.02,VE14.07.03

質問

暗号モジュールに実装された暗号サービスを記述するために、公開セキュリティポリシはどの程度詳細にしなければなりませんか？

回答

暗号モジュール認証に含まれている暗号サービスに関する公開セキュリティポリシの情報を提出するとき、セキュリティポリシは、最低限各暗号サービスについて次の情報を含むようにして下さい。

- 暗号サービス名称
- 暗号サービス目的／用途の簡潔な記述
- 暗号サービスの実施により使用され実装された承認されたセキュリティ機能（暗号アルゴリズム、鍵管理技術又は認証技術）のリスト
- 暗号サービス又は暗号サービスが使用する承認されたセキュリティ機能に関連した CSP のリスト
- 暗号サービスの使用を認可された各オペレータ役割に対するすべての CSP への個別のアクセス権を記述した情報と各役割の認証方法を記述した情報

文書の表現方法はベンダの任意です。

補足説明

3.14. 承認されたプロテクションプロファイル

現在、ガイダンスは発行されていません。

3.15. 承認されたセキュリティ機能

3.15.1. 擬似乱数生成器の仕様

暗号モジュール試験要件	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	適用対象外
発効日：	2008 年 1 月 28 日	
最終修正日：	2013 年 6 月 21 日	
個別要件：	AS07.05,AS07.06,AS07.07,AS07.08,AS08.20	
試験手順要件：	TE07.08.01-02, TE08.20.01-02	
ベンダ情報要件：	VE07.08.01,VE08.20.01	

背景

JIS X 19790 の細分箇条 7.7.1 には「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。」と規定されています。

質問

ISO/IEC 18031 の Hash_DRBG の内部関数 Hashgen()内の data の取扱いや CTR_DRBG の内部関数 Block_Cipher_df()内の内部変数 L,N,i の長さの取扱いなど不明確な点が多い。そのため、どのように実装したらよいですか？

回答

ISO/IEC 18031 Annex C.1 に「ISO/IEC 18031 の本文に記載されている機能要件を満足する DBRG は ISO/IEC 18031 に適合する」という主旨の記述があります。
本制度で承認している ISO/IEC 18031 以外の決定論的乱数生成器について、ISO/IEC 18031 に適合しているか検討した結果、以下の乱数生成器について ISO/IEC 18031 に適合していると確認されました。

・NIST SP800-90AのHash_DRBG, HMAC_DRBG, CTR_DRBG

本制度では、上記の 3 種類の乱数生成器のみを JIS X 19790 の下で承認されたセキュリティ機能とします。

補足説明

このガイダンスは JIS X 19790 の暗号モジュールセキュリティ要件のみに適用されます。
試験用提供物件に規格を明示する場合、ISO/IEC 18031 ではなく、NIST SP800-90A と記載して下さい。

3.16. 承認された鍵確立方法

3.16.1. 承認された鍵導出関数

暗号モジュール試験要件	JIS X 24759	FIPS140-2 DTR
適用レベル：	全て	全て
発効日：	2013 年 2 月 13 日	2013 年 6 月 21 日
最終修正日：		
個別要件：	AS09.19,AS09.38	AS10.06,AS10.24
試験手順要件：	TE09.19.01,TE09.38.01	TE10.06.01,TE10.25.01
ベンダ情報要件：	VE09.19.01,VE09.38.01,VE09.02.02,	VE10.06.01,VE10.25.01,VE10.25.02

背景

ある種のハッシュ関数には、length-extension 攻撃と呼ばれる攻撃が知られています。この攻撃は、$H(key \| message)$ のような構成でハッシュ関数が使用され、メッセージの内容、秘密情報(key)の長さ、$H(key \| message)$ の値が既知であるような場合が対象となり、$message$ をプレフィックスとするようなメッセージ $message'$ に対して、秘密情報(key)を知ることなく $H(key \| message')$ の値を知ることを可能とするものです。Merkle-Damgård 構造のハッシュ関数はこの種の攻撃が適用される可能性があります。SHA-1、SHA-256、SHA-512 はそれに該当します。SHA-224 は、出力の際に圧縮関数から削除される部分のビット数が少ないため、length-extension 攻撃の危険性が排除できないと考えられます。
鍵導出関数は、そのアルゴリズム中にハッシュ関数を使用するものが多く、ハッシュ関数に入力する内容に注意を払わないと、length-extension 攻撃に対して脆弱になる可能性があります。

質問

承認されたセキュリティ機能に記載された鍵導出関数には、length-extension 攻撃の懸念はありますか?

回答

鍵導出関数に対する length-extension 攻撃が有効な状況は、鍵導出関数の入力パラメータを制御可能な状況に対応します。鍵導出関数の入力パラメータは、通常、暗号モジュールの中で構成されるものですので、length-extension 攻撃には暗号モジュールで対抗すべきものです。
次の仕様書に記載された鍵導出関数を、SHA-1、SHA-224、SHA-256、あるいは SHA-512 と組み合わせて暗号モジュールの中で使用する場合、length-extension 攻撃への対策が必要になります。

- ANS X9.42
- ANS X9.63-2001
- NIST SP800-56A
- NIST SP800-56B

暗号モジュールが暗号ライブラリである場合、鍵導出関数の入力パラメータが暗号境界から直接入力される状況では、暗号モジュールのユーザガイダンス文書に対策が必要である旨の記述が必要です。

補足説明

4. 取消された運用ガイダンス

付録 1 暗号モジュール試験報告書一般情報の様式

(注) 表紙と改訂履歴は試験機関が任意に作成して下さい。

1.**概要**

1.1 **暗号モジュール名称及びバージョン**

暗号モジュール名称：
暗号モジュールバージョン：
ハードウェアバージョン　：
ソフトウェアバージョン　：
ファームウェアバージョン：
物理形態　　：

1.2 **試験結果**

適合規格：
試験要件：

暗号モジュールの仕様	**レベル**
暗号モジュールのポート及びインタフェース	**レベル**
役割、サービス及び認証	**レベル**
有限状態モデル	**レベル**
物理的セキュリティ	**レベル**
動作環境	**レベル**
暗号鍵管理	**レベル**
電磁妨害/電磁両立性	**レベル**
自己テスト	**レベル**
設計保証	**レベル**
その他の攻撃への対処	**レベル**
全体的なセキュリティレベル	**レベル**

ハードウェア環境 1：
ソフトウェア環境 1：

ハードウェア環境 2：
ソフトウェア環境 2：

ハードウェア環境 3：
ソフトウェア環境 3：

ハードウェア環境 4：
ソフトウェア環境 4：

ハードウェア環境 5：
ソフトウェア環境 5：

ハードウェア環境 6：
ソフトウェア環境 6：

ハードウェア環境 7：
ソフトウェア環境 7：

ハードウェア環境 8：
ソフトウェア環境 8：

ハードウェア環境 9：
ソフトウェア環境 9：

ハードウェア環境 10：
ソフトウェア環境 10：

1.3 **申請者**
申請者：
所在地：
担当者：

1.4 **試験機関**
試験機関名：
所在地：

1.5 暗号モジュール試験報告書作成支援ツール(CRYPTIPA)
CRYPTIPA バージョン：

2.**試験用提供物件一覧**

No.	名称	識別情報	備考
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			

3.暗号モジュールの暗号アルゴリズム実装一覧

3.1 承認された暗号アルゴリズム実装一覧

No.	承認された暗号アルゴリズム	暗号アルゴリズム確認番号	備考
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			

3.2 非承認の暗号アルゴリズム実装一覧

No.	非承認の暗号アルゴリズム	備考
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		

4.特記事項

以上

改訂履歴

識別番号	JIG-01	
改訂年月日	作成者・承認者	改訂内容
平成 20 年 1 月 28 日	井上・占部	新規制定
平成 20 年 2 月 20 日	井上・占部	一部改正
平成 20 年 8 月 7 日	井上・仲田	一部改正
平成 21 年 3 月 18 日	井上・仲田	一部改正
平成 21 年 8 月 7 日	井上・仲田	一部改正
平成 21 年 11 月 10 日	橋本・仲田	一部改正
平成 24 年 2 月 29 日	櫻井・仲田	一部改正 (3.2.7 及び 3.7.4 を追加)
平成 25 年 2 月 13 日	橋本・仲田	一部改正 (3.16.1 を追加)
平成 25 年 6 月 21 日	橋本・仲田	一部改正 (3.1.3 を追加、3.8.1 を 3.15.1 に移動の上修正)
平成 26 年 1 月 17 日	橋本・立石	一部改正 (2.10 を追加)
平成 30 年 6 月 28 日	櫻井・江口	一部改正（組織変更等）