運用ガイダンス第０版

平成 17 年 3 月

独立行政法人 情報処理推進機構

独立行政法人 情報通信研究機構

本資料の利用にあたって

本資料は、米国NIST[1]が発行している“Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program(Initial Release: March 28, 2003, Last Update: September 22, 2004)”を翻訳したものである。

運用ガイダンスは、CMVP[2]、特にDTR[3]に関する、ベンダや試験機関等からの問合せに対して、米国NIST及びカナダCSE[4]が回答したコメントをCMVPに関するガイダンスとしてまとめたものであり、FIPS 140-2 及びDTRと同様に適宜改訂が行われている。

別冊の暗号モジュール評価基準第 0.1 版及び暗号モジュール試験基準第 0.1 版をあわせてご参照いただけると幸いである。

[1] National Institute of Standards and Technology
[2] Cryptographic Module Validation Program
[3] Derived Test Requirements for FIPS PUB 140-2, Security Requirement for Cryptographic Modules
[4] Communications Security Establishment

新しいガイダンス及び改訂されたガイダンス(最近 45 日以内に発行されたもの)

新しいガイダンス

・2004 年 8 月 19 日：1.5　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

・2004 年 8 月 19 日：9.4　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ための暗号アルゴリズムテスト

・2004 年 7 月 26 日：1.4　暗号アルゴリズム認証証明書の利用

改訂されたガイダンス

・2004 年 9 月 22 日：9.1　鍵付きハッシュアルゴリズムに対する既知解テスト
「既知解テストは、すべての HMAC に対して実装しなければならない。」という要求事項を削除

・2004 年 8 月 19 日：G.5　ソフトウエア暗号モジュール又はファームウエア暗号モジュールの認証適合状態の維持
ファームウエア暗号モジュールに対するリファレンスを追加

・2004 年 8 月 19 日：7.1　許容される鍵確立プロトコル
パスワードベースの鍵確立プロトコルに対するリファレンスを追加

・2004 年 8 月 19 日：9.1　鍵付きハッシュアルゴリズムに対する既知解テスト
HMAC-SHA-224，HMAC-SHA-256，HMAC-SHA-384，及び HMAC-SHA-512 に対するリファレンスを追加

・2004 年 8 月 19 日：9.2　組込み暗号アルゴリズムに対する既知解テスト
FIPS 186-2 RNG 内の SHA-1 についての追加コメント

・2004 年 7 月 26 日：G.1　NIST/CSE に対する運用ガイダンスの問い合わせ
すべての試験機関への試験機関ガイダンスの配布

・2004 年 7 月 26 日：G.5　ソフトウエア暗号モジュール又はファームウエア暗号モジュールの認証適合状態の維持
適合申請の追加

目次

概要

この運用ガイダンスは､米国政府の NIST 及びカナダ政府の CSE によって発行及び保守されている。この両者は、それぞれの政府のために暗号モジュール評価認証制度の認証機関の役割を果たしている。この暗号モジュール評価認証制度は、NVLAP によって認定された暗号モジュール試験機関が、暗号モジュールが FIPS 140-2（暗号モジュールに対するセキュリティ要求事項）に適合していることを試験するプログラムである。加えてこのプログラムは、FIPS によって承認された AES、DES、DSA、SHA-1、及び Skipjack を含む暗号アルゴリズムの試験も行っている。

この文書は、暗号モジュール評価認証制度の説明、特に、暗号モジュールの FIPS 140-2 への適合を試験するために暗号モジュール試験機関が使用する、Derived Test Requirements（DTR）に関係するガイダンス及び説明を提供することを意図している。この文書が提示するガイダンスは、暗号モジュール試験機関、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、NIST 及び CSE が行った回答に基づいている。しかしながら、この文書の情報は NIST 及び CSE によって変更されることがある。

この文書の各節は FIPS 140-2 の要求事項の節に対応しており、追加の最初の節には、特定の要求事項の節に対応しない一般的なガイダンスを載せている。各節のなかには、ガイダンスが主題に沿って掲げられている。主題には複数の要求事項の分野にあてはまるものもあるが、その場合には、最適な分野に掲げている。各主題の下には、そのガイダンスの発行日を含んだリストがあり、DTR に記載されている関連するアサーション、試験者に課せられる要求事項、及びベンダに課せられる要求事項を列記している（注記：各主題に、追加の試験者及びベンダに課せられる要求事項が適用されるかもしれない)。次に、質問又は問題の説明と、関連情報を添えた解答及び追加のコメントを載せた節がある。これが、リストされた項目についての運用ガイダンスである。

以下は、読者が FIPS 140-1 及び FIPS 140-2 で認証された暗号モジュールを見つけることができるリストである。

・暗号モジュール認証リスト

全般的な問題

G.1　NIST/CSE に対する運用ガイダンスの問い合わせ

適用レベル：	すべて
有効期間：	1997 年 2 月 25 日～
最終改訂日：	2004 年 7 月 26 日
関連するアサーション：	全般
関連する試験者に課せられる要求事項：	
関連するベンダに課せられる要求事項：	

質問／問題

運用ガイダンスの問合せは誰に行えばいいのか？　また、問い合わせに用いる指定された様式はあるか？

解答

・制度に関する質問の場合：

暗号モジュール評価認証制度の一般的な運用に関する質問は、NIST 又は CSE のいずれかに提出されたい。次に、この場合に適切な担当者を示す。

・NIST

Randall J. Easter
(301) 975-4641
Ray Snouffer
(301)975-4436

・CSE

Jean Campbell
(613)991-8121
Ken Lu
(613)991-8122

・試験に関する質問の場合：

ベンダが FIPS 140-2 又はアルゴリズム試験の契約を暗号モジュール試験機関と結んでいる場合、そのベンダは試験者に課せられる要求事項に関するどんな質問についても、その試験機関にコンタクトすべきである。これにより試験機関の担当者は、その質問に答えるために、彼らの FIPS 140-2 試験における能力を発揮することができる。そしてそのことが NIST 又は CSE への単純な質問を減らすことができる。

政府機関、官署、暗号モジュール試験機関と契約していないベンダ及び試験機関そのものが、FIPS 140-2 の試験者に課せられる要求事項に関する質問をするときは、この場合に適切な NIST 及び CSE の担当者にコンタクトされたい。

・NIST

Randall J. Easter
(301) 975-4641
Ray Snouffer
(301)975-4436

・CSE

Jean Campbell
(613)991-8121
Ken Lu
(613)991-8122

すべての暗号モジュール試験機関からの、試験に関する特定の運用ガイダンスを求める質問は、NIST 及び CSE がその質問をできるだけ明確に理解して適切な回答を提供できるように、次の書式を備えなければならない。

1. FIPS 140-2 からの適用可能な規定
2. FIPS 140-2 DTR からの適用可能なアサーション
3. FIPS 140-2 DTR からの適用可能な試験要求手順
4. 問題の簡潔な説明、及びその問題に関する明確で曖昧さのない質問
5. 求めようとしている解決策の記述

すべての質問は、学術的又は仮定的なものであるよりも、詳細で実装に固有なものとして提出されることが望ましい。この情報には、実装の簡単で公開可能な記述及び FIPS 140-2 の目標セキュリティレベルを含むことが望ましい。これらのことは、NIST 及び CSE による、FIPS 140-2 関連質問の効率的でタイムリーな解決を可能にする。そ

れが適切であれば、NIST 及び CSE は、この質問と回答から一般的なガイダンスを引き出して、それをこの文書に追加する。一般的な質問もまた提出してよいが、その質問が特定の認証業務に関係しないことが示されていることが望ましい。回答がすべての試験機関に配送されるように、その質問は公開可能なものであることが望ましい。回答の配送は、個別の理由で制限されることがある。その質問は次の担当者に提出されたい。

・NIST
Randall J. Easter
(301)975-4641
Ray Snouffer
(301)975-4436

・CSE
Ghislain Lagace
(613)991-8497
Jean Campbell
(613)991-8121

*** 注記：NIST 及び CSE は書面（E-Mail や FAX も可- MS Word 文書が望ましい）による問い合わせに対してのみ正式な書面による回答を出すことに留意されたい。

追加コメント

G.2　試験報告書の完成：NIST 及び CSE に提出すべき情報

適用レベル：	すべて
有効期間：	1997 年 2 月 25 日～2004 年 1 月 19 日
最終改訂日：	2004 年 1 月 9 日
関連するアサーション：	全般
関連する試験者に課せられる要求事項：	
関連するベンダに課せられる要求事項：	

質問／問題

NIST 及び CSE が認証作業を行うために、試験機関の適合試験が完了したとき、どのような情報を NIST 及び CSE に提出すべきか？

解答

試験機関は、次の情報を NIST 及び CSE の双方に提出しなければならない。

1. 公開セキュリティポリシ＜PDF＞
   要求事項については FIPS 140-2 の DTR 及び運用ガイダンス 14.1 を参照のこと。
   公開セキュリティポリシは、複写又は配布許可という表示をせずに Proprietary 又は Copyright と表示してはならない。

2. CRYPTIK v5.5（又はそれ以上の版）の報告書
   認証報告書の提出は NIST 提供の Cryptik ツールからの出力でなければならない。
   a. 署名ページ／カバーシート＜PDF 及び郵送する署名入りの署名ページ紙面＞
   b. 一般情報＜PDF＞
   c. 必要経費の請求書＜PDF：適用ある場合＞
   d. 所見を含めた概略報告書＜PDF＞
   e. 所見を含めた詳細報告書＜PDF＞
   f. 認証証明書＜RTF＞
   g. 定義／参考文書＜PDF：オプション＞

3. 物理試験報告書＜PDF 形式-レベル 2,3,4 では必須＞
   適切であれば写真や図面などをつけた、試験機関の物理試験報告書

4．節ごとの要約
　各節の要求事項がどのように満たされているかの簡単な記述

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選択肢をもつが、これはNIST及びCSEより要求されたものではない。所見を含めた概略報告書には、公開できない情報を含めてはならない。PDFファイルはロックしてはならない。オプションの節ごとの要約及び物理試験報告を含む、Cryptikによる PDF ファイルでのすべての提出成果物は、一つの PDF ファイルにマージされていなければならない。

提出文書は一つの ZIP ファイルに圧縮し、暗号化して次の NIST 及び CSE の担当者宛に送付しなければならない。

・NIST
　Janet Jing
　(301)975-4203
　Randall J. Easter
　(301)975-4641

・CSE
　Ghislain Lagace
　(613)991-8497
　Jean Campbell
　(613)991-8121

***注記：署名入りの署名ページ紙面及び必要経費の請求書（適用ある場合）は、認証証明書の発行前に受領されていなければならない。

追加コメント

暗号モジュール評価認証制度の審査の順番は、電子的提出文書を受領したことで決められ、署名入り紙面を受領したときによるのではない。

文書が提出されたときから最初の審査が開始されるとは限らない。

G.3 部分的認証

適用レベル：	すべて
有効期間：	1997 年 2 月 25 日～
最終改訂日：	
関連するアサーション：	全般
関連する試験者に課せられる要求事項：	
関連するベンダに課せられる要求事項：	

質問/問題

部分的認証に関する NIST 及び CSE の見解はどうか？

解答

NIST 及び CSE は暗号モジュールが FIPS 140-2 の４章のすべての分野で少なくともレベル１のセキュリティ要求事項を満たさなければ認証証明書を交付しない。ある場合には、要求事項の分野が試験される暗号モジュールに適用されない場合もある（例えば、他の攻撃への対処）ことに注意されたい。このような場合、認証証明書はその要求事項に対して N/A（適用除外）と記す。

追加コメント

G.4　暗号モジュールの設計及び試験

適用レベル：	すべて
有効期間：	1997 年 11 月 12 日～
最終改訂日：	2000 年 4 月 28 日
関連するアサーション：	全般
関連する試験者に課せられる要求事項：	
関連するベンダに課せられる要求事項：	

質問／問題

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るか？

解答

次の情報は NVLAP のガイダンスに対する補足情報である。そして更に試験機関の設計及びコンサルティング、試験役割の分離について規定する。この分野での暗号モジュール評価認証制度ポリシは次の通り。

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ならない。
   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る。
   a．試験機関がベンダ会社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

かつ、

   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 FIPS 140-2、DTR、及びその他の関連する文書の説明をするコンサルティングサービスを行ってもよい。

追加コメント

上記回答の 3 項ではその他の関連する文書に言及している。それに含まれるのは次のものである。

・暗号モジュール評価認証制度スタッフにより作成された暗号モジュール試験プログラムに関する文書（例えば、運用ガイダンス、暗号モジュール評価認証制度ポリシ、ハンドブック 150-17、暗号モジュール試験）

及び

・FIPS 140-2 の暗号モジュールに対するセキュリティ要求事項に関連する運用ガイダンス及びポリシ

また有限状態モデル及びセキュリティポリシの統合及び編成に関して、運用ガイダンス G.9 を参照されたい。

G.5　ソフトウエア暗号モジュール又はファームウエア暗号モジュールの認証適合状態の維持

適用レベル：	すべて
有効期間：	1997 年 11 月 12 日～
最終改訂日：	2004 年 8 月 19 日
関連するアサーション：	全般
関連する試験者に課せられる要求事項：	
関連するベンダに課せられる要求事項：	

質問/問題

認証されたソフトウエア暗号モジュール又はファームウエ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るか？

解答

1．試験/認証された構成は認証証明書に記述されている。認証証明書は暗号モジュールが適合する構成のための基準として役立つ。

2．レベル 1 の動作環境に対し、ソフトウエア暗号モジュールは、次の条件の汎用コンピュータ上で動作するとき、FIPS 140-2 の認証適合状態が保持される。

a．汎用コンピュータが認証証明書で規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こと。

かつ、

b．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にポーティングできるように再コンパイルするのに先立って、ソフトウエア暗号モジュールのソースコードを変更する必要がないこと。

3．レベル 2 の動作環境に対し、ソフトウエア暗号モジュールは、次の条件の汎用コンピュータ上で動作するとき、FIPS 140-2 認証状態が保持される。

a．汎用コンピュータが、規定された CC 評価保証レベル EAL2（又は、同等なもの）のオペレーティングシステム/モード/動作設定、又は類似のモード及び動作設定を有する、互換性のある CC 評価保証レベル EAL2（又は、同等なもの）の別のオペレーティングシステムを組込んでいること。

かつ、

b．別の互換性のある CC 評価保証レベル EAL2 のオペレーティングシステムにポーティングできるように再コンパイルするのに先立って、ソフトウエア暗号モジュールのソースコードを変更する必要がないこと。

4．再コンパイルされて別の汎用コンピュータ又は動作環境にポーティングされるためにソースコードの変更が必要なソフトウエア暗号モジュール又はファームウエア暗号モジュールは試験機関によりレビューされなければならず、運用ガイダンス G.8(1)[セキュリティに関係しない変更]により再試験されなければならない。

５．動作環境が適用されない(NA)場合には、ファームウエア暗号モジュール及びその識別された、変更されていない試験済みオペレーティングシステム（すなわち、同じバージョン又はリビジョン番号であるもの）は、暗号モジュールの認証を維持しながら、1 つの汎用コンピュータ又はプラットフォームから別の汎用コンピュータ又はプラットフォームにポーティングされてもよい。加えて、汎用コンピュータを除き、試験済みプラットフォームもまた、認証証明書で特定されなければならない。

このポリシは、ソフトウエア暗号モジュール又はファームウエア暗号モジュールの実行動作環境についてのみ述べたもので、FIPS 140-2 のその他の節の要求事項には影響を与えない。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要求事項を満たさなければならない。

追加コメント

CMVP は、認証証明書で特定されている 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エア暗号モジュールのポーティングを許している。認証状態は、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試験することなく維持される。しかしながら、CMVP は、認証証明書に記載されていない OS 及び/又は汎用コンピュータ上にポーティングされた際に、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触れていない。

用語上のソフトウエア暗号モジュールとファームウエア暗号モジュールの違いに関して

は、運用ガイダンスの 1.3 ソフトウエア指定 を参照のこと。

このガイダンスは、特にソフトウエア暗号モジュール又はファームウエア暗号モジュールを実装しようとしているユーザに関するものである。

G.6　FIPS モード及び非 FIPS モードを持つ暗号モジュール

（すなわち、FIPS 承認されたセキュリティ手法及び FIPS 承認されていないセキュリティ手法を搭載した暗号モジュール）

適用レベル：	すべて
有効期間：	1998 年 3 月 11 日～
最終改訂日：	1998 年 4 月 2 日
関連するアサーション：	全般
関連する試験者に課せられる要求事項：	
関連するベンダに課せられる要求事項：	

質問/問題

暗号モジュールが FIPS 承認されたセキュリティ手法及び FIPS 承認されていないセキュリティ手法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可能か？

解答

（1998 年 4 月 2 日）FIPS 承認された及び FIPS 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 FIPS 動作モードを持たなければならない。その動作モードは FIPS 承認されたセキュリティ手順の動作のみを許可する。このことは暗号モジュールが FIPS 承認されたモードにあるとき、FIPS 承認されていない手順は、FIPS 承認された手順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、FIPS 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らない）ことを意味する。オペレータがどのサービスが FIPS 140-2 に適合しているか分かるようにしなければならない。
FIPS 140-2 認証証明書は暗号モジュールの“FIPS 動作モード”を識別する。

“FIPS 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ない。しかし、いずれのオペレータも FIPS モードが選択されるかどうかを判定できなければならない。

FIPS モードが常時選択されている必要はない。

追加コメント

G.7　ベンダ、試験機関、及び NIST/CSE 間の関係

適用レベル：	すべて
有効期間：	1998 年 4 月 14 日～
最終改訂日：	
関連するアサーション：	全般
関連する試験者に課せられる要求事項：	
関連するベンダに課せられる要求事項：	

質問／問題

ベンダ、試験機関、及び NIST/CSE 間の関係に関して、暗号モジュール評価認証制度のポリシはどのようになっているか？

解答

試験機関は、暗号モジュールの FIPS 140-2 の適合性を判定するために、暗号モジュール認証試験を実行することを NVLAP により認定されている。NIST/CSE は試験機関が FIPS 140-2、DTR 及び運用ガイダンスに基づいた、健全で正確かつ独立した決定をするために、豊富な認証試験経験と能力を発揮することを期待している。ひとたびベンダが試験機関と試験契約を締結すると NIST/CSE は試験機関の窓口を経由してベンダの暗号モジュールに対して公式のガイダンスや説明を与えることのみとなる。

ベンダ及び試験機関が試験課題上解決できない袋小路に入った場合には、ベンダは NIST/CSE から直接説明／解決策を聞くことができる。ベンダは運用ガイダンス G.1 で要求された書式を使うべきで、試験機関の窓口には写しを送る必要がある。この件に関する NIST/CSE からベンダへのすべての連絡は試験機関の窓口を通して行われる。

追加コメント

G.8 再認証の要求事項

適用レベル：	すべて
有効期間：	2001 年 8 月 17 日～
最終改訂日：	2003 年 4 月 4 日
関連するアサーション：	全般
関連する試験者に課せられる要求事項：	
関連するベンダに課せられる要求事項：	

質問／問題

再認証の要求事項と以前認証された暗号モジュールのかなり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、暗号モジュール評価認証制度のポリシはどのようになっているか？

解答

以前に認証された暗号モジュールの改訂版は、以前認証された暗号モジュールからの変更部分の割合によってはフル認証よりもむしろ再認証と考えられる。(注：改訂版は例えば現在ある暗号モジュールの新しいバージョン又は現在あるモデルを元にした新しいモデルかもしれない)

ここでは 4 通りのシナリオがあり得る。

1. 変更が FIPS 140-2 のセキュリティに関連した事項に影響を与えないハードウエア、ソフトウエア及びファームウエアに対して行われる。試験機関はこの変更によって FIPS 140-2 セキュリティ関連項目が影響を受けないことを確認するために必要な文書を識別する責任がある。ベンダは試験機関に該当する文書を提供する責任がある。この文書には以前の認証報告書、設計文書、ソースコード等が含まれる。試験機関は、変更箇所及びベンダから提供された文書をレビューし、NIST/CSE に対して該当する TE リスト及び関連する所見を含めた説明レターを提出する。この所見には試験機関により実行された解析に、セキュリティ関連 TE が影響を受けなかったことを確認したことが含まれなければならない。改訂版情報やそのリリース情報が FIPS 140-2 の暗号モジュール認証リストに元の暗号モジュールと共に掲載される。新しい認証証明書は発行されない。

2．変更がいくらかの FIPS 140-2 セキュリティ関連項目に影響するハードウエア、ソフトウエア及びファームウエアに対して行われる。このシナリオでは、改訂された暗号モジュールがセキュリティポリシ及び有限状態モデルの軽微な変更を伴い、元の暗号モジュールと同等で、FIPS 140-１適合性試験報告書の 30%以下のアサーションしか影響を受けない場合(再試験と)と考えられる。試験機関は再試験で十分かどうかを判定するために必要な文書を確認する責任がある。またベンダは要求された文書を試験機関に提出する責任がある。文書には以前の試験報告書、該当する NIST/CSE 規則、設計文書、ソースコード等が含まれるかもしれない。

試験機関は変更により影響を受けるアサーションを割り出し、これらのアサーションに付随する試験を実行しなければならない。このことは試験機関に次を要求している。

1．暗号モジュールの形態とセキュリティレベルに対するアサーションの完全なリストをレビューすること。

2．以前の試験報告書から、変更により影響を受けるアサーションを識別すること。

3．以前に試験されておらず、変更により試験すべき追加のアサーションを識別すること。

4．その運用ガイダンスがまだ適用されるかどうか確認するために､特定の運用ガイダンスが規定されていたアサーションをレビューすること。

例えば、セキュリティ機能を追加するファームウエアコンポーネントの改訂は１章のアサーションの変更を要求するかも知れない。

影響を受けたアサーションに対する試験を行うことに加えて試験機関は、FIPS 140-2 及び FIPS 140-1 の対応表に含まれる動作試験のリグレッションテスト群を実行しなければならない。表に含まれているのは AS (AS1 は FIPS 140-1 に対するアサーション、AS2 は FIPS 140-2 に対するアサーション等)、TE、VE、セキュリティレベル、シングルチップ、マルチチップ組込型（ME)、マルチチップスタンドアロン型（MS)、動作試験（op -x は動作試験に使用され、r はリグレッション試験に使用される)、FIPS 140-2 への適用可能性（一致性）及びコメント（それには FIPS 140-1

の試験結果の FIPS 140-2 への適用可能性と FIPS 140-2 の要求事項に関する情報が含まれるかもしれない）である。

試験機関は所見を伴った試験結果を文書化しなければならない、そしてすべての影響を受けた TE は“再試験された”と注記されなければならない。試験機関は変更され再試験されたアサーションを強調した差分の適合性試験報告書を提出してもよい。NIST/CSE により満足のいくレビューが実施されれば、新しい認証証明書が発行される。

3．変更が暗号モジュールを保護し、動作変更を伴わない物理的囲いにのみ行われる。試験機関は、その変更が物理的囲いにのみ影響して、暗号モジュールの動作には影響が無いことを確認する責任がある。試験機関はまた FIPS 140-2 の関連する要求に適合することを確認するために、新しい囲いの物理的セキュリティ特性を完全に試験する必要がある。そして試験機関は NIST/CSE に対して、次のレターを提出する必要がある。

1．変更点を記述すること（図面が必要かもしれない）。

2．セキュリティに関係する変更であることを述べること。

3．物理的変更のみで動作に影響がないことを裏付けるのに十分な情報を提供すること。

4．変更された囲いが依然として同じ物理的保護特性を持つことを確認する試験が試験機関により実行されたことを記述すること。

それぞれの要求はケースバイケースで処理される。暗号モジュール評価認証制度は既に FIPS 140-1 及び FIPS 140-2 で認証された暗号モジュールに対してそのようなレターを受付ける。認証証明書は再発行されない。

そのような変更例として、レベル２のトークンのプラスチックカプセル化されたもので成分を変えたり着色したものが当てはまるかもしれない。それにより成形特性や暗号境界が変更されたからである。この変更は、カプセル化されたものが不透明性やタンパー証跡を提供するため、セキュリティに関連したものである。しかし、これは新しい構成が以前のものと同じ物理的セキュリティ関連属性を持つという証拠と共にレターのみの変更で処理可能である。

4．変更がハードウエア、ソフトウエア又はファームウエアに対して行われ、上記基準を満たさない場合には、暗号モジュールは新しい暗号モジュールと考えられ、試験機関によりフル認証試験を受けなければならない。

暗号モジュールの全体のセキュリティレベルが変更されたり、物理的形態が、例えば、マルチチップスタンドアロン型からマルチチップ組込型に変更された場合には、暗号モジュールは新しい暗号モジュールと考えられ、認定された試験機関によりフル認証試験を受けなければならない。

追加コメント

再認証された暗号モジュールはすべての現行標準及び運用ガイダンスを満たさなければならない。試験機関はベンダから暗号モジュールが現行の標準及び運用ガイダンスを満足しているかどうかを判定するのに必要な文書を要求する責任がある。これは NIST/CSE から特定のルールが要求されている暗号モジュールの特徴／サービスについて特に重要である。例えば暗号モジュールが試験されていなかった T-DES を実装して認証されていたかもしれない。同じ暗号モジュールが後で再試験を依頼する場合には、この T-DES 実装は FIPS46-3 に照らして試験及び認証されなければならず、かつ、暗号モジュールは該当する FIPS 140-2 の要求事項、例えば、自己テストに合格しなければならない。

G.9 有限状態モデル、セキュリティポリシ、ユーザガイダンス、及びセキュリティオフィサガイダンスの文書

適用レベル：	すべて
有効期間：	2002 年 5 月 29 日～
最終改訂日：	
関連するアサーション：	
関連する試験者に課せられる要求事項：	
関連するベンダに課せられる要求事項：	

質問／問題

試験機関は FIPS 140-2 で規定された原本文書を作成することができるか？　質問の文書とは、有限状態モデル、セキュリティポリシ、ユーザガイダンス、及びセキュリティオフィサガイダンスである。

解答

<u>有限状態モデル及びセキュリティポリシ</u>

試験機関は既存の暗号モジュール（既に開発され設計されたもの）のベンダ作成文書を手に入れ、(多くの情報源から)既存の情報を統合又は再編成してもよい。この場合には、試験報告書が提出されるときに、NIST 及び CSE にそのことを知らせなければならない。個々の文書に対する追加の詳細については次に示されている。

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らない。

セキュリティポリシ：

ベンダから提供された文書には、FIPS 140-2 の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らない。

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原本のベンダ文書に戻れることを示さなければならない。この対応付けは試験機関により認証記録の一環として維持されなければならない。

統合及び再編成は次のように定義される。

・原本の文書はベンダ（又はベンダの外注先）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る

・試験機関は、原本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する。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る。技術表現の内容を変更することはできない。

・試験機関は、読み易さを改良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で用いるための暫定的な表現を作成してもよい。これらの暫定的な表現は対応付けの中で試験機関により作成されたことが示されなければならない。

ユーザガイダンス及びセキュリティオフィサガイダンス：

試験機関はユーザガイダンス、セキュリティオフィサガイダンス及び（開発及び設計済みの）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してもよい。この場合には、認証報告書提出時に NIST 及び CSE に知らせなければならない。

追加コメント

G.10　FIPS 140-1 から FIPS 140-2 への再認証のための物理的セキュリティ試験

適用レベル：	すべて
有効期間：	2004 年 3 月 29 日～
最終改訂日：	
関連するアサーション：	
関連する試験者に課せられる要求事項：	
関連するベンダに課せられる要求事項：	

背景

FIPS 140-2 の運用ガイダンス G.2 は、レベル 2、3 又は 4 に対してすべての報告書提出には個別の物理的セキュリティ試験報告書の節を含まなければならないことを規定している。

質問/問題

質問は、以前の個別の物理的セキュリティ試験報告書が存在していないか、又はイメージなどの証拠が元の試験報告書と共に提出されていなかった場合の再試験報告書に関して寄せられた。セキュリティ要求事項が変更されていなかった場合には、試験機関は何をするべきか？

解答

再試験を行っている暗号モジュールについて以前の個別の物理的セキュリティ試験報告書が存在せず、暗号モジュールの物理的セキュリティ特性が変更されていない場合には、試験機関は元の試験された暗号モジュールの記録から保管されている物理的セキュリティ試験の証拠を編集し、新たな個別の物理的セキュリティ試験報告書を作成し、提出しなければならない。記録が試験機関の品質マニュアルで規定された記録保存期間以前に生成されたためにもはや存在しない場合には、そのような証拠を提供するために再試験を要求しなければならない。試験機関が、保存されていなかったり元の試験時に作られていなかった新しい写真イメージを作るためだけに再試験を行う必要は無い。

追加コメント

試験機関が元の試験機関でなく、そのため以前の試験記録にアクセスできない場合には、暗

号モジュールはそのような証拠を提供できるようにするために再試験されなければならない。以前の記録なしに、新しい試験機関は物理的セキュリティが変更されたか、又は変更されていないかを決められない。

1章　暗号モジュールの仕様

1.1　暗号モジュールの名称

適用レベル：	すべて
有効期間：	2004年2月27日～
最終改訂日：	
関連するアサーション：	AS01.05、AS01.08、AS01.09
関連する試験者に課せられる要求事項：	TE01.08.03、04、05　TE01.09.01、02
関連するベンダに課せられる要求事項：	VE01.08.03、VE01.09.01

質問/問題

暗号モジュールの名前は定義された暗号境界とどのように関係づけなければならないか？

解答

暗号モジュールに与えられた名前(認証証明書に記述されるであろう)が試験報告書で定義される暗号境界の定義と一致しなければならない。

暗号モジュールの定義された暗号境界より多くのコンポーネントを持つ暗号モジュールを表すような暗号モジュール名を与えることは受け入れられない。より大きい実体を表す名前を持つのが望ましいなら、暗号境界はそれと一致してはならない。 暗号境界の中にあるすべてのコンポーネントは試験報告書に含まれるか(AS01.08)、又は除かれなければならない(AS01.09)。

追加コメント

例: 暗号モジュールに与えられた名前は「暗号カード」である。 しかしながら、試験報告書における定義された暗号境界はカードの隅に置かれた小さな黒いカプセルに入ったコンポーネントである。 また、命名されたカードには、参照されなかった追加コンポーネント(例えば、バッテリー、コネクタ)もある。 試験報告書における定義された境界が黒いカプセルのコンポーネントだけを指定するなら、それは明らかに「暗号カード」でない。 定義された境界と一致しているようにユニークな別の名前を与えなければならない。カード全体を表すためには、境界を再定義し、かつ、すべてのコンポーネントが含まれ、それらが適切に(含まれているか

又は除かれているか)記述されなければならない。

1.2 FIPS 承認された動作モード

適用レベル：	すべて
有効期間：	2004 年 3 月 15 日～
最終改訂日：	
関連するアサーション：	AS01.02、AS01.03、AS01.04
関連する試験者に課せられる要求事項：	TE01.03.01、02、TE01.04.01、02
関連するベンダに課せられる要求事項：	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モード(承認されたセキュリティ機能の DES CBC モードのような特定のモードと混同しないこと)。

質問/問題

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の切換を行うときに何か動作上の要求事項があるか？

解答

AS01.02、AS01.03、及び AS01.04 で規定された要求事項に加えて、暗号モジュールは動作モード(すなわち、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)間で CSP を共有してはいけない。

追加コメント

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ことによって生じるリスクから緩和される。

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切替えて、承認されたサービスにその生成された鍵を使用してはならない。
  鍵は承認されていない方法で生成されたかもしれないし、その完全性及び保護性は保証することができない。
- 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切り替えて、承認されたサービスにそれらの鍵を使用してはならない。

・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切替えて、承認されていないサービスに生成された鍵を使用してはならない。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性を保証することができない。

1.3 ファームウエア指定

適用レベル：	すべて
有効期間：	2004 年 4 月 28 日～
最終改訂日：	
関連するアサーション：	AS01.01
関連する試験者に課せられる要求事項：	
関連するベンダに課せられる要求事項：	

背景

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

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

暗号モジュールの動作環境とは、暗号モジュールが動作するために必要なソフトウエアコンポーネント、ファームウエアコンポーネント、及び/又はハードウエアコンポーネントの管理を指す。動作環境は、変更不可能(例えば、ROM に収められたファームウエア、又は入出力デバイスの機能を無効にしたコンピュータに収められたソフトウエア)であるか、又は変更可能(例えば、RAM に収められたファームウエア、又は汎用コンピュータで実行されるソフトウエア)である。

限定動作環境とは、汎用オペレーティングシステムを持たず、その上に動作環境がただひとつ存在する静的で変更不可能な仮想動作環境(例えば、プログラミング不可能なPCカード上でのJAVA仮想マシン)を指す。

動作環境が限定動作環境である場合には、4.6.1 節におけるオペレーティングシステム要求事項は適用されない。

質問/問題

限定動作環境で動くソフトウエア暗号モジュールはどのように指定されるか？

解答

動作環境が限定動作環境であり、認証証明書に NA と示される場合には、その暗号モジュールはファームウエア暗号モジュールとして指定されるものとする。

追加ノート

- 試験に使用された参照 OS はすべてのソフトウエア及びファームウエア暗号モジュールの認証証明書に示されなければならない。 それは暗号モジュール評価認証制度の認証リストウェブページにて、次のように引用される：
  - ・動作環境が適用される場合：
    動作環境：レベル X を満足するように以下の環境で試験されたと記述される。
    （-Operational Environment: Tested as meeting Level x with ...）
  - ・動作環境が適用されない場合：
    試験されたと記述される。
    （-Tested: ...）
- レベル 2 の暗号モジュールの場合には、動作試験に使用される参照ハードウエアプラットフォームも記載されなければならない。
- Java アプレットの場合には、試験された Java 環境(JRE、JVM)及びオペレーティングシステムが、すべてのセキュリティレベルで規定される必要がある。

FIPS 140-2 の運用ガイダンス G.5 で述べたように、ソフトウエア暗号モジュールのポーティングは汎用コンピュータ(GPC)上で動作する暗号モジュールに対してのみ適用可能であり、動作環境が適用可能なときである。暗号モジュールの認証はソースコードに変更が加えられない限り維持される。

動作環境が適用されない場合には、ファームウエア暗号モジュールと識別された試験用 OS は共に一つのプラットフォームから別のプラットフォームへ暗号モジュールの認証を維持しながら移植され得る。ファームウエア暗号モジュールが JAVA アプレットの場合には、ファームウエア暗号モジュール、識別された試験用 OS、及び試験用 JAVA 環境（JRE、JVM）は一つのプラットフォームから別のプラットフォームへ移植するときに、暗号モジュールの認証状態を維持するために一緒に移動しなければならない。

これら以外のすべての場合は、暗号モジュールの認証は維持されない。

1.4 暗号アルゴリズム認証証明書の利用

適用レベル：	すべて
有効期間：	2004 年 7 月 26 日～
最終改訂日：	
関連するアサーション：	AS01.12
関連する試験者に課せられる要求事項：	TE01.12.01
関連するベンダに課せられる要求事項：	VE01.12.01

背景

暗号アルゴリズムの実装は暗号アルゴリズム認証システムのもとで試験及び認証される。暗号アルゴリズム認証証明書は認証された実装の名前及びバージョン番号、並びに試験の動作環境が記されている。

暗号モジュールは、暗号モジュール認証制度のもとで試験及び認証される。暗号モジュール認証証明書は認証された暗号モジュールの名前及びバージョン番号、並びに試験の動作環境が記されている。

それらの認証証明書は、試験中に使われた構成及び動作環境のための基準として役立つ。

質問/問題

動作環境の FIPS 140-2 適合試験が実施されているとき、暗号モジュール内に組込まれている認証された暗号アルゴリズムの実装を利用するための構成管理及び動作環境に対する要求事項は何か？

解答

FIPS140-2 適合試験を実施しているソフトウエア暗号モジュール、ファームウエア暗号モジュール、又はハードウエア暗号モジュール内に組込まれている認証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らない：

1. 認証された暗号アルゴリズムの実装のソースコード又は実装が、試験中の暗号モジュールへの組込み時に修正されていないこと。

かつ、

2．認証された暗号アルゴリズムの実装が試験された動作環境と暗号モジュールが試験されている動作環境とが同一でなければならない。

追加コメント

1.5 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

適用レベル：	すべて
有効期間：	2004 年 8 月 19 日～
最終改訂日：	
関連するアサーション：	AS01.12
関連する試験者に課せられる要求事項：	TE01.12.01
関連するベンダに課せられる要求事項：	VE01.12.01

背景

暗号アルゴリズム認証制度(CAVP)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) ごとに認証する。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る。

質問/問題

FIPS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か？

解答

FIPS承認された動作モードで使用されるためには、

- 実装されたSHSアルゴリズムごとに適切なOS上で試験及び認証されなければならない。
- DSA、RSA、ECDSA及びHMACに対しては、実装の組合せごとに適切なOS上で試験及び認証されなければならない。

アルゴリズム認証証明書には、FIPS承認された動作モードで使用できるすべての試験済み実装が注記される。

FIPS 140-2を満たす暗号モジュールに組込まれ、試験されていない実装されたアルゴリズム

は、FIPS承認された動作モードで使用されてはならない。試験されていない、FIPS承認されたアルゴリズムのサブセットが存在する場合には、FIPS 140-2の認証証明書には、非承認で、かつ不適合として記載される。

追加コメント

2章　暗号モジュールのポート及びインタフェース

3 章　役割、サービス及び認証

3.1　許可された役割

適用レベル：	すべて
有効期間：	2002 年 5 月 29 日～
最終改訂日：	
関連するアサーション：	全般
関連する試験者に課せられる要求事項：	
関連するベンダに課せられる要求事項：	

質問／問題

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）を実行するために許可された役割を担う必要は無い。

解答

許可された役割は、FIPS 承認された暗号アルゴリズムを使用したすべての呼び出し可能なサービスに適用される。

追加コメント

4章　有限状態モデル

5 章　物理的セキュリティ

5.1　レベル 2 におけるファン、換気口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

適用レベル：	2
有効期間：	2004 年 2 月 10 日～
最終改訂日：	
関連するアサーション：	AS05.49
関連する試験者に課せられる要求事項：	TE05.49.01
関連するベンダに課せられる要求事項：	VE05.49.01

背景

暗号モジュールは、通常、ファン、換気口又はスリットの使用を含めた放熱技術の使用を必要とする。暗号モジュールの囲いの中のこれらの開口部の大きさ又はファンの羽根の隙間の大きさが、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ない。

質問／問題

FIPS 140-2 の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するか。セキュリティレベル 2 の暗号モジュールは換気口又はスリットからのプロービングを阻止すべきか？

解答

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ある。

・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）

かつ

・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 では扱われていない。換気口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 で取り扱われる。(AS05.21)

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組立て又は実装方法の測定を阻止するために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防止することである。

人工光源を用いて、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、(特定の IC の型名のような) 内部コンポーネントの製造番号及び/若しくはモデル番号、並びに/又は（ワイヤーの形跡及び内部接続のような）設計情報及び組立て情報を判断できない場合にのみ、暗号モジュールは「不透明」としてみなされる。

コンポーネントの製造番号及び/若しくはモデル番号、並びに/又は組み立て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、コンポーネントの外形は、囲いの開口部又は半透明な表面から見えてもよい。

暗号モジュールの境界内のすべてのコンポーネントは、基準の不透明性の要求事項を満たさなければならない。除外された、セキュリティの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ない。

追加コメント

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

6 章　動作環境

6.1　単一オペレータモード及び複数同時オペレータ

有効期間：	2003 年 3 月 10 日～
最終改訂日：	2003 年 4 月 24 日
関連するアサーション：	AS06.04
関連する試験者に課せられる要求事項：	VE06.04
関連するベンダに課せられる要求事項：	TE06.04

背景

歴史的に、FIPS 140-1 及び FIPS 140-2 で認証されたサーバ上のソフトウエア暗号モジュールが、セキュリティレベル 1 の単一ユーザ要求事項を満たすために、サーバはある時点で単一ユーザのみがアクセスできるように構成されなければならなかった。このことは、ある時点で単一ユーザがサーバ上で処理（暗号処理を含む）を実行することができるようにサーバオペレーティングシステム（OS）を構成することを意味する。従って、サーバは設計意図通りに使用されなかった。

質問／問題

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）」と記載している。この文脈では複数同時オペレータの定義はどのようになっているか？　特に、レベル 1 のソフトウエア暗号モジュールはサーバに実装して FIPS 140-2 の認証を受けられるか？（注：この質問はまた、VPN、ファイアーウオールなどにも当てはまる）

解答

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エ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る。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る。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は暗号モジュールのユーザである。サーバアプリケーションは暗号モジュールを呼び出す。それ故、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る。

追加コメント

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らない。

6.2 動作環境要求事項の JAVA スマートカードに対する適用

適用レベル：	すべて
有効期間：	2003 年 4 月 08 日
最終改訂日：	2003 年 9 月 11 日
関連するアサーション：	AS06.01
関連する試験者に課せられる要求事項：	
関連するベンダに課せられる要求事項：	

背景

FIPS 140-2（4.6節 動作環境）では「限定動作環境とは、汎用オペレーティングシステムを持たず、その上に動作環境がただひとつ存在する静的で変更不可能な仮想動作環境(例えば、プログラミング不可能なPCカード上でのJAVA仮想マシン)を指す。」と記載している。

質問

FIPS 140-2 の記述は、JAVA アプレットを（それが認証されていてもいなくても）受け付け走らせている、変更不可能なオペレーティングシステム（例えば今日ほとんどのスマートカードで一般的に使用されているオペレーティングシステムのようなもの）を実装しているスマートカードが限定動作環境である事を意味しているか。

解答

暗号モジュール評価認証制度は、すべての 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ない。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ある。決定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る。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を保有していると見なされ、FIPS 140-2 の動作環境の要求事項が適用される。

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る。そして、暗号モジュール試験報告書の FIPS 140-2 の動作環境の要求事項の節は、“Not Applicable”と印される。

a)いかなるアプレットのローディングもできないように構成されている。

b)FIPS 140-1 又は FIPS 140-2 で試験及び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らない。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アサーションと同様に、AS09.34,AS09.35, AS10.03 及び AS10.04 の要求事項を満たさなければならない。暗号モジュールの認証は、スマートカード自身の認証過程で試験及び認証されたアプレットをロードするか又は独立した認証過程（すなわち、アプレット自身も自分の認証証明書番号を持っている）を通して維持される。

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らない。

・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らない。(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ひとたび認証されていないアプレットがロードされれば、もはや暗号モジュールの FIPS 140-1 又は FIPS 140-2 の認証は有効でないことを明確に示さなければならない。)

・認証された暗号モジュール内に格納されるアプレットはすべて、その名前とバージョン番号が登録されなければならない。

追加コメント

認証された暗号モジュール内に含まれるすべ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証明書及び暗号モジュール評価認証制度のウェブサイトに記載される。

6.3 オペレーティングシステムに関する CC 要求事項の訂正

適用レベル：	すべて
有効期間：	2004 年 3 月 29 日～
最終改訂日：	
関連するアサーション：	AS06.10、AS06.21、AS06.27
関連する試験者に課せられる要求事項：	TE06.10、TE06.21、TE06.27
関連するベンダに課せられる要求事項：	VE06.10、VE06.21、VE06.27

背景

どのようにアサーション AS06.10、AS06.21 及び AS06.27 が読まれるかによって、これらは暗号モジュールが動作している OS が、EAL2、EAL3、及び EAL4 のそれぞれについて Annex B に記載された PP のすべてを満たさなければならないように解釈されるかもしれない。これは、"Protection Profiles"が複数形であるためである。

質問/問題

暗号モジュール上で実行している OS は、EAL2、EAL3、EAL4 のそれぞれについて Annex B で記載されているすべての PP を満たさなければならないか？

解答

いいえ、要求事項は次のように読むと解釈すべきである。

・AS.06.10 の場合：

Annex B に記載された PP の１つで規定された機能要件を満足するオペレーティングシステムで、かつ、CC 評価保証レベル EAL2 で評価されたもの

・AS.06.21 の場合、最初の文章：

Annex B に記載された PP の１つで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

・AS.06.27 の場合、最初の文章：

Annex B に記載された PP の１つで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

追加ノート

７章　暗号鍵管理

7.1　許容される鍵確立プロトコル

適用レベル：	すべて
有効期間：	2004 年 2 月 10 日～
最終改訂日：	2004 年 8 月 19 日
関連するアサーション：	AS07.21
関連する試験者に課せられる要求事項：	TE07.21.01
関連するベンダに課せられる要求事項：	VE07.21.01 -02

背景

暗号モジュール間のセキュアな通信経路を確立し維持するために暗号モジュールは Secure Socket Layer (SSL)、Transport Layer Security (TLS)、IP Security (IPSec)及びパスワードベースの鍵確立プロトコルを使用している。

質問／問題

SSL、TLS、IPSEC 及びパスワードベースの鍵確立のどのプロトコルが、データの暗号化及び復号に用いるための鍵確立のために、FIPS モードで用いることができるか？

解答

次のパラグラフは、データの暗号化及び復号に用いるための鍵の確立のために、FIPS モードでの使用に関する各プロトコルのステータスを記述したものである。

- SSL:SSL プロトコルのどのバージョンも FIPS モードでは使用されない。プロトコルでの操作における承認された暗号アルゴリズム及び承認されていない暗号アルゴリズムの使い方では、そのプロトコルの使用が禁止されている。
- TLS:TLS プロトコルは FIPS モードで使用可能である。そのプロトコルは SSL プロトコルと同じ暗号アルゴリズムを使用しているが、そのアルゴリズムの使われ方が FIPS モードでの使用を可能にしている。
- IPSEC:IPSEC プロトコルは、その実装に用いられる暗号アルゴリズムが FIPS 承認されたものである限り、FIPS モードで使用可能である。
- パスワードベースの鍵確立プロトコル：PKCS#5 のようなすべてのパスワードベースの鍵

確立プロトコルはFIPSモードでは使用されない。

暗号モジュールで用いられる鍵確立プロトコルはAS07.21の下に記載されなければならない。

追加コメント

この運用ガイダンスでは認証技術で用いられる鍵確立は取り上げない。

FIPS 140-2 Annex D は承認された鍵確立技術を参照している。鍵確立プロトコルはいくつかの異なる技術とアルゴリズムから成り、それゆえプロトコルはAnnex Dでは識別されない。

8章　電磁妨害/電磁両立性（EMI/EMC）

9章　自己テスト

9.1　鍵付きハッシュアルゴリズムに対する既知解テスト

適用レベル：	すべて
有効期間：	2004年2月10日～
最終改訂日：	2004年9月22日
関連するアサーション：	AS09.07
関連する試験者に課せられる要求事項：	TE09.07.01
関連するベンダに課せられる要求事項：	VE09.07.01

背景

いくつかの鍵付きハッシュアルゴリズム（例えばDES MAC, HMAC-SHA-1）は、FIPS承認されており、電源ON時の既知解テストの要求事項を判定する複雑さの異なるレベルがある。

質問／問題

FIPSモードで鍵付きハッシュ関数を実装したとき、既知解テストの要求事項は何か？

解答

次の表は最低限の既知解テストの要求事項をまとめたものである。

既知解テストの要求事項	鍵付きハッシュアルゴリズム	下位のアルゴリズム
DES MAC / Triple-DES MAC	無し	有り
HMAC-SHA-1	有り	無し
HMAC-SHA-224	有り	無し
HMAC-SHA-256	有り	無し
HMAC-SHA-384	有り	無し
HMAC-SHA-512	有り	無し

根拠

DES MAC及びTriple-DES MACアルゴリズムは、下位のアルゴリズムエンジン（例えば、DES及びTriple-DES）に対して、余り多くの付加的な複雑性が含まれていない。しかし、

HMAC-SHA-1 のような鍵付きハッシュアルゴリズムは下位のアルゴリズムエンジン（例えば、SHA-1）に対して付加的な複雑性が含まれている。DES 又は Triple-DES アルゴリズムに対して行われる既知解テストは、関連するハッシュアルゴリズムを適切に検証する。これは、下位の SHS アルゴリズムに加えて、いくつかのその他の機能を実装した SHS アルゴリズムを使用した鍵付きハッシュアルゴリズムに対する事例ではない。

追加コメント

FIPS 140-2 の運用ガイダンス 9.3 で議論されているように、HMAC-SHA-1 が、AS06.08 で規定されたソフトウエアコンポーネント又はファームウエアコンポーネントを検証するために、承認された完全性技術として使用される場合には、既知解テストは、HMAC-SHA-1 又は下位の SHA-1 アルゴリズムに対して要求されない。

9.2 組込み暗号アルゴリズムに対する既知解テスト

適用レベル：	すべて
有効期間：	2004 年 2 月 10 日～
最終改訂日：	2004 年 8 月 19 日
関連するアサーション：	AS09.19
関連する試験者に課せられる要求事項：	TE09.19.01、02、03
関連するベンダに課せられる要求事項：	VE09.19.01、02

背景

核となる暗号アルゴリズムは FIPS 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込まれる（例えば、HMAC-SHA-1 及び DSA に組込まれた SHA-1 アルゴリズム、RNG に組込まれた DES 又は Triple-DES アルゴリズム)。FIPS 140-2 は、FIPS モードで使用される FIPS 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が、電源投入時の自己テストの一部として既知解テスト（KAT）を実行することを要求している。この要求事項は、核となる暗号アルゴリズム実装においても有効である。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、組込まれた核となる暗号アルゴリズムもまた自己テストが実施されてもよい。

質問／問題

組込まれている核となる暗号アルゴリズムが、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、既に評価された暗号アルゴリズムの実装のために、暗号モジュールが既知解テストを実装する必要があるか？

解答

もし、次の条件が満たされれば、暗号モジュールが組込まれた核となる暗号アルゴリズム上の既知解テストを実施しなくても受け入れられる。

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電源投入時に既知解テストを実施している。
3. 核になる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 DES 及び Triple-DES に対する暗号化及び復号)。

追加コメント

暗号モジュールが核となる暗号アルゴリズムのいくつかの実装を含み（例えば、SHA-1 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 FIPS 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らない。

すべての DES 又は 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 生成で実行されるが、復号は実行されない）、ANSI X9.31 のような RNG 内の DES 又は Triple-DES の実装は上記第 3 項を満たさない。

ハッシュ機能が完全には実行されていないため、FIPS 186-2 乱数生成アルゴリズム内の SHA-1 実装は上記第 3 項を満たさない。

9.3 完全性テスト技術で使用される暗号アルゴリズムに対する既知解テスト

適用レベル：	すべて
有効期間：	2004 年 2 月 10 日～
最終改訂日：	
関連するアサーション：	AS06.08、AS09.16
関連する試験者に課せられる要求事項：	TE06.08.01～02、TE09.16.01～02
関連するベンダに課せられる要求事項：	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エアコンポーネント及び暗号ファームウエアコンポーネントに対して適用されなければならないことを要求している。AS09.16 は、既知解テストを用いた暗号アルゴリズムテストが暗号モジュールに実装され、FIPS 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る。

質問／問題

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別の既知解テストを実装する必要があるか？

解答

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、Triple-DES 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別の既知解テストを実装してはならない。

根拠

暗号モジュールはソフトウエア/ファームウエ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エア/ファームウエアの完全性テストは既知解テストと考えられる。

例：HMAC-SHA-1 が、ソフトウエアコンポーネント又はファームウエアコンポーネントを検

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-1 又は下位の SHA-1 アルゴリズムに対して要求されない。

例:完全性テストは Triple-DES の暗号化及び復号の両方を使用しないため、Triple-DES MACが、ソフトウエアコンポーネント又はファームウエアコンポーネントを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、既知解テストは下位のTriple-DES に対してやはり要求される。

例：完全性テストは RSA の署名生成機能を使用しないため、RSA が、ソフトウエアコンポーネント又はファームウエアコンポーネントの署名を検証するために使用される場合には、既知解テストは下位の RSA に対してやはり要求される。しかしながら、下位のSHA-1 ハッシュ関数の既知解テストは要求されない。

追加コメント

9.4 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ための暗号アルゴリズムテスト

適用レベル：	すべて
有効期間：	2004 年 8 月 19 日～
最終改訂日：	
関連するアサーション：	AS09.16
関連する試験者に課せられる要求事項：	TE09.16.01
関連するベンダに課せられる要求事項：	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らない。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ること、及び演算された出力と過去に生成された出力（既知解）とを比較することを伴う。計算された出力が既知解と異なる場合には、既知解テストは失敗でなければならない。

与えられる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（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（以下で定義）を用いてテストされなければならない。

FIPS 承認された動作モードで使用される各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らない。暗号アルゴリズムテストは、パワーアップ時又は要求時に実行されるアルゴリズム実装のヘルスチェックである。

質問/問題

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、FIPS 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か？パワーアップ時又は要求時に実行される場合、（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か？

解答

次はアルゴリズムの既知解テストに特有の運用ガイダンスの一部分である:

・次は SHS アルゴリズムのための最小限の要求事項である:

・SHA-1(もしあれば)のための既知解テストが必要である;

・SHA-256(もしあれば)のための既知解テストが必要である;

・SHA-224 が SHA-256 なしで実装される場合には、SHA-224(もしあれば)のための既知解テストが必要である;

・SHA-512(もしあれば)のための既知解テストが必要である;

かつ、

・SHA-384 が SHA-512 なしで実装される場合には、SHA-384(もしあれば)の既知解テストが必要である。

・DSA 及び RSA(もしあれば) のための既知解テスト又は鍵ペア整合性テストが必要であり、以下の条件で実行される必要がある。

・最小限、暗号モジュールでサポートされている NIST 推奨の最小の法サイズで、

かつ、

・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。

・ECDSA(もしあれば) のための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される必要がある。

・実装された 2 種類の体（即ち素体GF(p)と拡大体GF(2^m)）のそれぞれについて、いずれか一つの曲線で、

かつ、

・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。

・HMAC（もしあれば）のための既知解テストが必要であり、最小限、下位に実装された SHS アルゴリズムのいずれか一つについて実行しなければならない。

追加コメント

FIPS 140-2 IG 9.2 組込み暗号アルゴリズムに対する既知解テストがあてはまる。

この運用ガイダンスは、FIPS 140-2 IG 9.1 鍵付きハッシュアルゴリズムの既知解テストと整合が取れている。

根拠:

既知解テストの目的は、電源オフ/オンの合間（パワーサイクルの間）に暗号モジュールの修復不可能な故障又は改変を特定するために、暗号モジュールのヘルスチェックを実行することであり、実装が正しいことの確認ではない。 実装の検証は、暗号アルゴリズムテスト及び認証期間で実行される。

10 章　設計保証

11 章　他の攻撃への対処

12 章　Appendix A:文書要求事項のまとめ

13 章　Appendix B:推奨ソフトウエア開発手順

14章　Appendix C:暗号モジュールのセキュリティポリシ

14.1　暗号サービスを報告するときの詳細度

適用レベル：	すべて
有効期間：	2001年11月15日
最終改訂日：	
関連するアサーション：	AS01.02, AS01.03, AS01.12, AS01.16, AS03.14, AS10.06, AS14.02, AS14.03, AS14.04, AS14.06, AS14.07
関連する試験者に課せられる要求事項：	TE01.03.01, TE01.03.02, TE01.16.01, TE03.14.01, TE10.06.01, TE14.07.01, TE14.07.02
関連するベンダに課せられる要求事項：	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／問題

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らないか？

解答

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、最低限各サービスについて次の情報を含まなければならない。

- サービス名称
- サービス目的／用途の簡潔な記述（サービス名称のみでも場合によってはこの情報を提供するかも知れない。）
- サービスの実施により使用されたり実装される、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

・サービス又は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暗号鍵及び/又はその他の CSP のリスト
・サービスを使用することを認可された各オペレータ役割に対して、
　・すべての暗号鍵及び/又はその他の CSP への個別のアクセス権を記述した情報
　・各役割を認証するために使用される方法を記述した情報

文書の表現方法はベンダに任される。FIPS 140-2 Appendix C には、本標準の文書要求事項を満たすために含まれる情報の種類について、部分的なサンプルとイラストを提供する表形式のテンプレートが含まれている。

追加コメント

FIPS 140-2 は、次の情報が暗号モジュールのセキュリティポリシに含まれる事を要求している。

・ユーザ（オペレータ）が、承認された動作モードが選択されていることを判定できるようにすること。(AS01.06, AS01.16)
・承認されているかどうかに関わらず、暗号モジュールで提供され、オペレータが利用可能なすべてのセキュリティサービス、操作又は機能をリスト化すること。(AS01.12, AS03.07, AS03.14, AS14.03)
・暗号モジュールのハードウエアコンポーネント、ソフトウエアコンポーネント、及びファームウエアコンポーネント間の対応を提供すること。(AS10.06)
・FIPS 140-2 の要求事項に基づくセキュリティルールを含む、暗号モジュールが動作中に従うべきセキュリティルールの規定を提供すること。(AS14.02)
・それぞれのサービスにおいて、サービス入力、それに対応するサービス出力、及びそれらのサービスを実行できる許可された役割の詳細な仕様を規定すること。(AS03.14, AS14.03)

FIPS 140-2 の承認された動作モード及び承認されたセキュリティ機能の定義も参照すること。

14.2　攻撃の対処を報告するときの詳細度

適用レベル：	すべて
有効期間：	2001 年 11 月 15 日～
最終改訂日：	
関連するアサーション：	AS14.09
関連する試験者に課せられる要求事項：	TE14.09.01
関連するベンダに課せられる要求事項：	VE14.09.01

質問／問題

その他の攻撃を対処するために暗号モジュールに実装されるセキュリティメカニズムについて、公開セキュリティポリシにどの程度詳細に記述しなければならないか？

解答

セキュリティポリシに含まれることが要求される、その他の攻撃を対処するために暗号モジュールに実装されたセキュリティメカニズムの記述の詳細度は、広告文書（製品説明）に見られるものと同等でなければならない。

追加コメント

取消された運用ガイダンス