# 運用ガイダンス
# 2006-03-31 版

平成 18 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: December 1, 2005) ”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。

[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

・2005 年 12 月 1 日： 1.8　DES 実装のリストへの掲載

・2005 年 12 月 1 日： 7.5　鍵確立方法の強度

・2005 年 9 月 12 日: G.11　エミュレータとシミュレータを使用した試験

・2005 年 9 月 12 日: 1.6　NIST 推奨ではない非対称鍵サイズと楕円曲線の使用

・2005 年 9 月 12 日: 1.7　複数の承認された動作モード

・2005 年 9 月 12 日: 5.2　タンパー証跡を残すシールの試験

・2005 年 9 月 12 日: 7.4　パワーアップ自己テストのための鍵のゼロ化

### 改訂されたガイダンス

・2005 年 11 月 17 日：G.2 試験報告書の完成：NIST 及び CSE に提出すべき情報

・2005 年 9 月 12 日: G.1　CMVP に対するガイダンスの要求

・2005 年 9 月 12 日: 1.2　FIPS 承認された動作モード

・2005 年 9 月 12 日: 7.1　許容される鍵確立プロトコル

・2005 年 9 月 12 日: 7.2　IEEE802.11i 鍵導出プロトコルの使用

・2005 年 7 月 25 日: G.2 試験報告書の完成：NIST 及び CSE に提出すべき情報

# 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認証プログラムの認証機関の役割を果たしている。この暗号モジュール認証プログラムは、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、暗号モジュール認証プログラムの説明、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　CMVP に対するガイダンスの要求

| | |
|---|---|
| 適用レベル： | すべて |
| 発効日： | 1997 年 2 月 25 日 |
| 最終改訂日： | 2005 年 9 月 12 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： | |

**背景**

暗号モジュール認証プログラム（CMVP）と暗号アルゴリズム認証プログラム（CAVP）への質問には、制度に関する質問と、試験特定の質問の二種類が定義されている。CMVP と CAVP は、非公式の要求と公式の要求の二つのタイプを定義している。

**質問／問題**

非公式の要求と公式の要求の違いは何か？　これらの質問は誰に対して行えばよいか？　質問に対する公式の回答を要求する場合、これらのタイプの要求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：**　暗号モジュール認証プログラム又は暗号アルゴリズム認証プログラムの一般的な運用に関する質問である。CMVP 及び CAVP は、既に回答が用意されている場合があるため、CMVP ウェブサイトに掲載されている CMVP に関するよく聞かれる質問（FAQ）のページ、CAVP に関するよく聞かれる質問（FAQ）のページ、アナウンス、告知を最初に参照することを勧める。CMVP ウェブサイトに掲載されている情報は、CMVP と CAVP の公式な見解を示している。

**試験特定の質問：**　暗号モジュール認証プログラム又は暗号アルゴリズム認証プログラムにおける特定の試験に関して議論となる質問である。これらの議論は、技術に関連する内容又は解釈に自由度がある標準の領域に関連する内容であってもよい。

**一般的なガイダンス：** 下記の適切な担当者連絡先に問い合わせることによって、CMVP 又は CAVP の制度に関する質問を、NIST 又は CSE に直接送ることができる。すべての質問に関して、コピーに NIST 及び CSE の担当者連絡先をすべて含めなければならない。

FIPS 140-2 あるいは特定の実装についてのアルゴリズム試験を行う暗号モジュール試験機関と契約を結んでいるベンダは、試験の要求事項についての質問及び、それらが実装の試験にどの程度影響があるかについては、契約している暗号モジュール試験機関に問い合わせなければならない。

暗号モジュール試験機関は、すべての試験に関する質問を下記の RFG フォーマットで提出しなければならない。これらの質問は担当者連絡先に記載されている全員に提出されなければならない。

政府機関、官署及び暗号モジュール試験機関と契約していないベンダが、FIPS 140-2 試験の要求事項、あるいは CMVP と CAVP に関する諸事項について特定の質問をする場合には、下記の適切な NIST および CSE の担当者連絡先に問い合わせるべきである。

質問は e メール、電話、FAX あるいは書面（電子文書の場合は、マイクロソフトワードの文書フォーマットが望ましい）で提出されてもよい。

**非公式の問い合わせ：** 非公式の問い合わせは FIPS 140-2 及び CMVP と CAVP の諸事項についての問題を明らかにするための一時的な質問と考えられる。CMVP による非公式の問い合わせに対する回答は、最終形ではなく、変更されることが多い。非公式の問い合わせは連絡先すべてに対して提出されることが望ましい。非公式の問い合わせへの回答として、正確で、一貫し、わかりやすい返答をタイムリーに行うためにあらゆる試みがなされる。

**公式の問い合わせ：** 公式な回答を要求する場合、公式な問い合わせは、下記のガイダンスのリクエスト（RFG）フォーマットに記述されて、CMVP 及び/又は CAVP に提出されなければならない。公式な回答は、NIST 及び CSE と、必要があれば他の機関も交えた内部レビューを必要とし、CMVP 及び/又は CAVP からの追跡の質問を要求する場合もある。したがってこのような問い合わせは、時間が問題となるにも関わらず、即座に処理されない場合もある。

**ガイダンスリクエストのフォーマット：** 現在のポリシあるいは解釈を定めている CMVP 及び CAVP からの公式の回答を求める場合、このフォーマットで質問を提出する。このフォーマットによって、CMVP 及び CAVP はその質問を明確に理解することができる。RFG は下記の内容を含む。

1. RFG が非公開であるか、あるいは公開であるかの、明確な表示
2. うまく描写した題名
3. FIPS 140-2 からの適用可能な規定
4. FIPS 140-2 DTR からの適用可能なアサーション
5. FIPS 140-2 DTR からの適用可能な試験要求手順
6. FIPS 140-2 運用ガイダンスからの適用可能な規定
7. アルゴリズム標準からの適用可能な規定
8. 適切な場合、過去のあらゆる CMVP あるいは CAVP の公式ルールあるいはガイダンスを含む、背景情報
9. 問題に関する明確で具体的な質問を伴う、問題の簡潔な記述
10. 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べきである。この情報には、実装の簡潔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べきである。これらのことすべてによって、CMVP 及び CAVP による、FIPS 140-2 関連質問の効率的でタイムリーな解決が可能になる。解決策の記述は、CMVP 及び CAVP が“YES”か“NO”で答えられるような形式で記述されなければならない。回答が提案された解決策と一致しない場合、CMVP は任意で根拠を示す場合もある。

適切な場合、CMVP 及び CAVP は、その問題と回答から一般的なガイダンスを抽出し、この文書にそのガイダンスを追加する。さらに、一般的な質問を提出してもよいが、これらの質問を、特定の認証業務に関係しないと識別すべきであることに留意すること。

回答がすべての暗号モジュール試験機関に配送されるように、なるべく質問は公開可能なものであるべきである。回答の配送は、場合によっては制限されることがある。

NIST 及び CSE の担当者連絡先：

・National Institute of Standards and Technology – CMVP

Randall J. Easter　reaster@nist.gov
(301) 975-4641

Allen Roginsky　aroginsky@nist.gov
(301) 975-3603

National Institute of Standards and Technology – CAVP

Sharon Keller　skeller@nist.gov
(301) 975-2910

・Communications Security Establishment – CMVP
(カナダ政府)

Ken Lu　ken.lu@cse-cst.gc.ca
(613) 991-8122

Jean Campbell　jean.campbell@cse-cst.gc.ca
(613) 991-8121

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 |
| 発効日： | 1997 年 2 月 25 日 |
| 最終改訂日： | 2005 年 7 月 25 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＜署名入りの署名ページの PDF＞
   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＞
   該当する場合には写真や図面などをつけた、試験機関の物理試験報告書

4．再認証のための変更の要約＜PDF：適切な場合＞

5．節ごとの要約＜オプション＞
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<on copy>
(301)975-4641

・CSE
Lisa Payne
(613) 949-5298
Jean Campbell <on copy>
(613) 991-8122

＜事務局注＞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**

暗号モジュール認証プログラムの審査の順番は、電子的提出文書を受領したことで決められる。

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　部分的認証及び FIPS 140-2 の適用除外分野

| | |
|---|---|
| 適用レベル： | すべて |
| 発行日： | 1997 年 2 月 25 日 |
| 発効日： | |
| 最終改訂日： | 2005 年 1 月 21 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**

暗号モジュールは FIPS140-2 4 章の選択された分野のみ認証されることは可能か？
FIPS140-2 4 章のどの分野が N/A とすることができるか？

**解答**

NIST 及び CSE は暗号モジュールが、次に示すように N/A と指定することのできる分野を除いた 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。

・4.5 章、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 N/A と指定してもよい。
・4.6 章、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）N/A と指定してもよい。

そして

・4.11 章、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、N/A と指定してもよい。

試験機関は認証試験報告書で N/A と記入した章の根拠を提供しなければならない。

**追加コメント**

ある章が N/A である場合には、その暗号モジュールの認証証明書に N/A と記入される。4.6 章が N/A である場合でも、暗号モジュール実装によっては、構成情報は、やはり暗号モジュール認証証明書に要求されることがある。（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らない。）

## G.4　暗号モジュールの設計及び試験

| | |
|---|---|
| 適用レベル： | すべて |
| 発効日： | 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認証プログラムポリシは次の通り。

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。

・暗号モジュール認証プログラム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、暗号モジュール認証プログラムポリシ、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

| | |
|---|---|
| 適用レベル： | すべて |
| 発行日： | 1997 年 11 月 12 日 |
| 発効日： | |
| 最終改訂日： | 2005 年 1 月 21 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るか？

**解答**

試験/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。

このガイダンスは二つの別々のシナリオを扱う。一つはベンダが暗号モジュールの認証状態を維持していると主張できる行為、又はベンダが暗号モジュールの認証状態を維持して変更できる行為であり、もう一つはユーザが暗号モジュールの認証状態を維持していると主張できる行為である。

このガイダンスは **4.5 章 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しない。

**ベンダ**

1. 次の項目が維持される条件で、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、認証適合状態を維持

していると主張してよい。

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、次の条件を満たさなければならない。

i) **レベル 1 の動作環境**に対し、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、認証証明書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、FIPS 140-2 の認証適合状態が保持される。

ii) **レベル 2 の動作環境**に対し、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、特定された 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、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ときは、FIPS 140-2 認証状態が保持される。

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 N/A）を、その識別され、変更のない、試験済みのオペレーティングシステム（すなわち、同一バージョン又はレビジョン番号であるもの）と一緒に、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状態が保持される。

CMVP 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、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、認証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る。認証状態は、新しい OS 及び/又は汎用コンピュータ上での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言及しない。

ベンダは、新しい動作環境、汎用コンピュータ、又はプラットフォームへの参照を宣言し、その参照を含めることにより、新しいセキュリティポリシを提供してもよい。

2. 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）を必要とするものは、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、試験機関によるレビューとFIPS 140-2 IG G.8(1)による再認証を受けなければならない。

3. 認証証明書上の運用環境及び/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FIPS 140-2 IG G.8(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、FIPS 140-2 IG G.8 表G.8.1に含まれた機能テストのリグレッションテスト群を実行しなければならない。基礎となるアルゴリズム認証は、FIPS 140-2 IG 1.4 暗号アルゴリズム認証証明書に基づく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らない。

   再試験及び認証により、新しくリストされたOS及び/又はプラットフォーム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、CMVP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する。なお、新しくリストされたOS及び/又はプラットフォームは、暗号モジュール認証ウェブ・エントリに追加される。

ベンダは FIPS 140-2 4.10 章の中で適用可能な要求事項をすべて満たさなければならない。

このポリシは、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。

FIPS 140-2 IG 1.3 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間の用語の差について記述する。

## ユーザ

**ユーザは認証された暗号モジュールを改変してはならない。ユーザによるいかなる改変も暗号モジュールの認証を無効にする。**

次の項目が維持される条件で、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してよい。

1. レベル 1 の動作環境に対し、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ときは、FIPS 140-2 の認証適合状態が保持される。そして、

2. レベル 2 の動作環境に対し、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ときは、FIPS 140-2 認証状態が保持される。

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ェア暗号モジュールの移植を許している。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保持される。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触れていない。

## 追加コメント

ユーザには、認証証明書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 |
| 発効日： | 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 |
| 発効日： | 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、暗号モジュール認証プログラム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 |
| 発行日： | 2001 年 8 月 17 日 |
| 発効日： | |
| 最終改訂日： | 2005 年 1 月 21 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、暗号モジュール認証プログラム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)

下に示す変更シナリオ 1 及び 3 で変更される暗号モジュールは、オリジナルの認証時に満たされた全ての基準、運用ガイダンス及びアルゴリズム試験を満足しなければならない。 暗号モジュールは、オリジナルの認証時以降に削除された要求事項を継続して満足する必要はない。

下に示す変更シナリオ 2 及び 4 で変更される暗号モジュールは、CMVP への暗号モジュール報告書提出時に効力を有している全ての基準、運用ガイダンス及びアルゴリズム試験を満足しなければならない。試験機関は、暗号モジュールが現在の基準及び運用ガイダンスを満たすかどうか判断するために必要なすべての文書をベンダに要求する責任がある。 これは、NIST 及び CSE から特定の裁定を必要とする暗号モジュールの機構/サービスにとって特に重要である。

例えば、暗号モジュールは試験されていない Triple-DES を実装して認証されていたかも知れない。 同じ暗号モジュールが後でシナリオ 2 及び 4 の下の再認証に対して提出される場合、この Triple-DES 実装は FIPS 46-3 に対して試験され認証されなければならない。また、暗号モジュールは適用可能な FIPS 140-2 要求事項(例えば自己テスト)を満たさなければならない。

ここでは 4 通りの変更シナリオがあり得る。

1. 修正が **FIPS 140-1 又は 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。ベンダは、試験機関に修正箇所を識別する関連文書を提供する責任がある。文書は前の認証報告書、設計文書、ソースコードなどを含んでいてもよい。 試験機関はベンダから提供された文書をレビューし、追加の文書化要求事項を識別しなければならない。試験機関はさらに、FIPS 140-1 又は FIPS 140-2 セキュリティ関連項目が修正によって影響を受けてないこと確認するために、必要に応じて追加試験を決定しなければならない。

   必要に応じたレビュー及び適用可能な試験を首尾よく完了すると、試験機関は、NIST 及び CSE へ署名付き説明レターを提出しなければならない。そこには修正箇所の記述を含み、影響を受けた TE 及びそれらの関連する試験機関による評価を記載しなければならない。その評価は、セキュリティに関連する項目は影響を受けなかったことを確認する試験機関による分析を含まなければならない。そのレターは、さらに修正された暗号モジュールが以前に認証された暗号モジュールを置き換えるのか、以前の暗号モジュールにそれらが追加されるのかどうか示さなければならない。 新しいアルゴリズム証明書が得られた場合、それらは記載されなければならない。

   NIST 及び CSE によるレビューが完了すると、最新バージョン又は公開情報は、オリジナルの暗号モジュールと共に、*認証された FIPS 140-1 及び FIPS 140-2 暗号モジュール一覧*ウェブサイト・エントリに掲示されるだろう。 新しい証明書は発行されない。

   暗号モジュールのバージョン番号を新しいバージョン番号で更新する登録のために、新しいセキュリティポリシを提供することを強く奨励する。

2. **修正がいくらかの FIPS140-2 セキュリティ関連項目に影響する**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。更新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、FIPS140-１又は FIPS 140-2 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、その暗号モジュールは、このシナリオに入ると見なすことができる。(文書変更は、30%の影響を受けたアサーションにはカウントされないことに注意。) 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識別する責任がある。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、適用可能な NIST 及び CSE の裁定、設計文書、ソースコード等が含まれるかもしれない。

＜事務局注＞　ここでは、全 AS のうち、30%以下の AS しか影響を受けない変更を行う場合、暗号モジュールの変更(更新)に関する 4 つのシナリオの中の 2 つ目に入ることを意味している。実際には、30%ルールが適用された場合、認証書の番号の変更は無く、NIST の Web 情報が更新されることとなる。

試験機関は、修正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。

a. 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。
b. 以前の試験報告書から、修正により影響を受けるアサーションを識別すること。
c. 以前に試験されておらず、修正により試験すべき追加のアサーションを識別すること。
d. 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ェ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、表 G.8.1-リグレッションテスト群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。

暗号モジュールが、FIPS 140-1 からFIPS 140-2 への再認証に関して試験される場

合、試験機関は、FIPS 140-2 試験報告書の準備のためのFIPS 140-1 試験報告書に含まれていた情報を再利用してもよい。 FIPS 140-2 からFIPS 140-1 への対応表にある表は、試験者をガイドするのに使用可能である。

注：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。試験機関は動作テスト(Op フィールドで、x 及び r でラベルが付けられた TE)をすべて実施しなければならない。

試験機関は、関連する評価の中で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、修正について記述し、修正され再試験された(CRYPTIK の中の再試験オプションを選択して)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なければならない。NIST 及び CSE によるレビューが完了すると、更新されたバージョンは FIPS 140-2 で再認証され、新しい認証証明書が発行される。

3. 修正が**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、さらに 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全面的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。
   a. 変更点を記述すること（図面が必要かもしれない)。
   b. セキュリティに関係する変更であることを述べること。
   c. 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。
   d. 修正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。セキュリティレベル 2、3 及び 4 については、更新された物理的セキュリティ試験報告書の提出は必須である。

それぞれの要求はケースバイケースで処理される。暗号モジュール認証プログラムは既に 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. 変更がハードウェア、ソフトウェア又はファームウェアに対して行われ、**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、認定された試験機関により全面的な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全面的な認証試験を受けなければならない。

**表 G.8.1-リグレッションテスト群**

| Regression Testing Table | | | | | |
|---|---|---|---|---|---|
| AS | TE | Security Level | | | |
| | | 1 | 2 | 3 | 4 |
| Section 1 - Cryptographic Module Specification | | | | | |
| AS01.03 | TE01.03.02 | x | x | x | x |
| Section 2 - Cryptographic Module Ports and Interfaces | | | | | |
| 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 |

| | | | | | |
|---|---|---|---|---|---|
| Section 3 - Roles, Services and Authentication | | | | | |
| 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 |
| Section 4 - Finite State Model | | | | | |
| AS04.03 | TE04.03.01 | x | x | x | x |
| AS04.05 | TE04.05.08 | x | x | x | x |
| Section 5 - Physical Security | | | | | |
| | NONE | | | | |
| Section 6 - Operational Environment | | | | | |
| 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 |
| Section 7 - Cryptographic Key Management | | | | | |
| 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 |
| Section 8 - EMI / EMC | | | | | |
| | As Required | | | | |
| Section 9 - Self Tests | | | | | |
| 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 |
| Section 10 - Design Assurance | | | | | |
| AS10.03 | TE10.03.02 | x | x | x | x |
| Section 11 - Mitigation of Other Attacks | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | NONE | | | | |
| Appendix C - Cryptographic Module Security Policy | | | | | |
| | As Required | | | | |

**追加コメント**

## 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 |
| 発効日： | 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**

有限状態モデル及びセキュリティポリシ

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 |
| 発効日： | 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。

## G.11 エミュレータとシミュレータを使用した試験

| | |
|---|---|
| 適用レベル： | すべて |
| 発行日： | 2005 年 9 月 12 日 |
| 発効日： | |
| 最終改訂日： | 2005 年 9 月 12 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： | |

**背景**

暗号モジュールのベンダは、そのモジュールに対する FIPS 140-2 要求事項の適合性試験を受けるにあたり、独立し認定された暗号モジュール試験（CMT）機関を利用する。試験の実行を希望する組織は、要求されるサービスを受けるために試験機関との契約を結ぶ。試験基準（DTR）文書は、その暗号モジュールが FIPS 140-2 の要求事項に適合しているかどうかを試験するために、認定された試験機関によって使用される方法を記述している。それは、試験者が従わなければならない詳細な試験手順、検査、文書及びソースコードレビュー、並びに運用試験及び物理試験を含み、暗号モジュールが FIPS PUB 140-2 要求事項への適合を満足するために達成しなければならない期待される結果を含む。これらの詳細な方法は、試験プロセスを通じて高度な客観性をもたらすことと、認定された試験機関の間に一貫性を確保することを意図している。

**定義：**

**エミュレータ**は暗号モジュールの“モデル”動作または“模倣”動作を試みる。エミュレータの動作の正確性は、エミュレータへの入力及びエミュレータの設計に依存する。他の多くの要因が正確にまたは確実にモデル化されないことがあるかもしれないので、実際の暗号モジュールの振る舞いと同一であることは保証されない。

**シミュレータ**は、暗号モジュールへの物理的な入力に先立ち、実際の暗号モジュールのソースコード（例えば、VHDL コード）を実行する（例えば、FPGA またはカスタム ASIC)。挙動の観点から、シミュレータにおけるソースコードの挙動は、暗号モジュールに実装された場合または論理ゲートにインスタンス化された場合と論理的に同一で

あるかもしれない。しかしながら、実際のふるまいを変えるかもしれない他の多くの要因が存在する（例えば、パス遅延、変換エラー、ノイズ、環境要因など）。他の多くの要因が同一であるとの確信が持てないため、暗号モジュールの実際のふるまいが同一であるとは保証されない。

**質問/問題**

暗号モジュール試験機関の試験者は、暗号モジュール試験を行うために暗号モジュールのエミュレーション手法及び/またはシミュレーション手法を使用してもよいか？

**解答**

暗号モジュールの試験において、注目すべき三つの広範な領域がある：　暗号モジュールの定義された境界における暗号モジュールの動作試験、アルゴリズム試験及び誤動作誘導エラー試験

1. 動作試験
   エミュレーションあるいはシミュレーションによって、暗号モジュールの動作試験を行うことは、禁止されている。暗号モジュールの実際の試験は、定義されたポート及びインタフェース、並びにモジュールが提供するサービスを利用して実行されなければならない。

2. 誤動作誘導
   エミュレータまたはシミュレータは、既に許可されているソースコードレビューの代用として、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誤動作誘導のために利用されてもよい。なぜ、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 TE に対して示さなければならない。

3. アルゴリズム試験
   定義されたポート及びインタフェース、並びにモジュールが提供するサービスを利用するアルゴリズム試験が行われることが望ましい。この方法はFIPS 140-2 IG 1.4の要求事項に明らかに適合する。

   暗号モジュールが定義するポート及びインタフェース並びにサービスのセットが内部のアルゴリズムエンジンへのアクセスを許可しないため、この望ましい方法が利用できない場合、次の二つの代替手法が利用されてもよい。

a. 試験を目的として、アルゴリズムエンジンへのアクセスを許可するように、暗号モジュール試験機関が､暗号モジュールを修正する｡(例えば､試験治具、試験 API)

b. 暗号モジュールシミュレータを使用する。

CAVP にアルゴリズム試験結果を提出する際、試験が実行された実際の動作環境を、詳細に示されなければならない（例えば、修正された暗号モジュールの識別又はシミュレーション環境を含む)。 CMVP にモジュール試験報告書を提出する際、なぜアルゴリズム試験が実際の暗号モジュールにおいて実施されなかったかを説明する根拠を、AS01.12 に含めなければならない。

エミュレータはアルゴリズム試験には使用されない。

**追加コメント**

# 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 |
| 発効日： | 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 |
| 発行日： | |
| 発効日： | 2004 年 3 月 15 日 |
| 最終改訂日： | 2005 年 9 月 12 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 ファームウェア指定

| | |
|---|---|
| 適用レベル： | すべて |
| 発効日： | 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ェア、ソフトウェア、及び/又はファームウェアの集合。

ファームウェア：暗号境界のなかにあるハードウェア（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ェアコンポーネント、ファームウェアコンポーネント、及び/又はハードウェ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ェア、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ェア)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ェア、又は汎用コンピュータで実行されるソフトウェア)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ェ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ェ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ェア及びファームウェ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認証プログラム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ェ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、ソフトウェ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、ファームウェ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。ファームウェア暗号モジュールが JAVA アプレットの場合には、ファームウェア暗号モジュール、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に基づく制約事項

| | |
|---|---|
| 適用レベル： | すべて |
| 発行日： | |
| 発効日： | |
| 最終改訂日： | 2005 年 1 月 21 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プログラム（CAVP）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（CMVP）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**

暗号モジュールの 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暗号アルゴリズムの実装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アルゴリズム評価ツール CAVS により試験された動作環境と、認定された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 |
| 発効日： | 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**

## 1.6 NIST 推奨ではない非対称鍵サイズと楕円曲線の使用

| | |
|---|---|
| 適用レベル： | すべて |
| 発行日： | 2005 年 9 月 12 日 |
| 発効日： | |
| 最終改訂日： | 2005 年 9 月 12 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プログラム（CAVP）は、NIST 推奨の非対称鍵サイズと楕円曲線に限り、DSA、RSA 及び ECDSA の実装を認証している。アルゴリズムの標準は、NIST 推奨ではない鍵サイズと楕円曲線の使用を許可している。CAVP によって暗号モジュール試験（CMT）機関に提供される暗号アルゴリズム認証システム（CAVS）は、暗号モジュールが実装する可能性のあるすべての鍵サイズと曲線を試験しない。

**質問/問題**

CMVP は、FIPS で承認された動作モードにおいて、NIST 推奨ではない DSA 及び RSA の鍵サイズ並びに ECDSA 曲線の使用を許可するか？　許可する場合、FIPS モードで使用するために、これらに対してどのような要求事項があるのか？

**解答**

CMVP は、次を条件として、FIPS で承認された動作モードにおいて、NIST 推奨ではない DSA 及び RSA の鍵サイズ、並びに ECDSA 曲線の使用を許可する。

- アルゴリズム実装は、少なくとも一つの NIST 推奨鍵サイズ（DSA と RSA の場合）及び NIST 推奨の曲線（ECDSA の場合）の試験及び認証を、該当する場合には受けていなければならない。

- セキュリティポリシは、実装されているすべての NIST 推奨ではない鍵サイズと曲線を記載しなければならない

- アルゴリズム実装は承認されたメッセージダイジェストアルゴリズムを使用しなければならない

**追加コメント**

FIPS で承認された動作モードにおいて使用するためには、すべての NIST 推奨曲線、鍵及びモジュラスサイズが試験されていなければならない。

動作環境の要求事項のガイダンスについては、IG 1.4 暗号アルゴリズム認証証明書に基づく制約事項を参照のこと。

このガイダンスは FIPS 186-3 の認可及び NIST Draft Special Publication 800-56 - *Recommendation for Key Establishment Schemes Using Discrete Logarithm Cryptography* のリリースの影響を受ける可能性があり、その場合、それらの文書に記述された要求事項によって置き換えられる。

## 1.7 複数の承認された動作モード

| | |
|---|---|
| 適用レベル： | すべて |
| 発行日： | 2005 年 9 月 12 日 |
| 発効日： | |
| 最終改訂日： | 2005 年 9 月 12 日 |
| 関連するアサーション： | AS.01.03; AS.01.04 |
| 関連する試験者に課せられる要求事項： | TE.01.03.01-02; TE.01.04.01-02 |
| 関連するベンダに課せられる要求事項： | VE.01.03.01-02; VE.01.04.01-02 |

**背景**

FIPS PUB 140-2 の 4.1 節は、ベンダが暗号モジュールに複数の承認された動作モードを実装することを排除しない。複数の承認された動作モードの例として、すべてのモードが同一のサービスのセットを持つとは限らないモジュールが挙げられる。

**質問/問題**

暗号モジュールが複数の承認された動作モードを実装してもよいか？　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への要求事項は何か？

**解答**

暗号モジュールは、複数の承認された動作モードをサポートするように設計されてもよい。

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場合、次が適用されなければならない。

- 異なる承認された動作モードで構成された場合でも、全体的なセキュリティレベルは変更されない
- セキュリティポリシに、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及びそれぞれの構成方法を記述しなければならない
- ある承認された動作モードから別のモードに再構成する場合、暗号モジュールは再初期化及びパワーアップ自己テストを実行しなければならない

- パワーアップ自己テストは、選択された承認された動作モードで使用される、すべての承認されたセキュリティ機能について実行されなければならない

- 再構成によって暗号モジュールの物理セキュリティレベルが変わる場合、再構成時に暗号モジュールはモジュール内のすべての CSP のゼロ化を実行しなければならない

それぞれの動作モードが正しく動作することを確認するために、試験者は次を行わなければならない。

- 文書にそれぞれの承認された動作モードが記述されていることの検証

- 公開セキュリティポリシに記述された、それぞれの承認された動作モードを呼び出すためのベンダが提供する取扱説明の使用

- それぞれの承認された動作モードにおいて、そのモードのために実装されたセキュリティ機能だけがアクセス可能であること、及びそのモードのために実装されていないセキュリティ機能はアクセス不可能であることの検証

- それぞれの認証された動作モードにおいて、前述の要求事項が満たされることの検証

- それぞれの認証された動作モードにおいて、AS01.03 及び/又は AS01.04 の要求事項が満たされることの検証

- 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の検証

**追加コメント**

## 1.8 DES 実装のリストへの掲載

| | |
|---|---|
| 適用レベル： | すべて |
| 発行日： | 2005 年 11 月 23 日 |
| 発効日： | 2005 年 2 月 9 日 |
| 最終改訂日： | 2005 年 11 月 23 日 |
| 関連するアサーション： | AS.01.12 |
| 関連する試験者に課せられる要求事項： | TE.01.12.01-02 |
| 関連するベンダに課せられる要求事項： | VE.01.12.01-02 |

### 背景

商務省
米国国立標準技術研究所
[協議事項　No. 040602169-5002-02]

米国連邦情報処理標準規格(FIPS)46-3；Data Encryption Standard (DES)、FIPS 74；Guidelines for Implementing and Using the NBS Data Encryption Standard 及び FIPS 81；DES Modes of Operation の撤回の承認の告知

### 質問／問題

DES 暗号アルゴリズムの撤回によって、DES アルゴリズムはどのように FIPS 140-2 認証書に掲載されるか？

### 解答

承認されたセキュリティ機能として DES を既に実装し、FIPS 140-1 又は FIPS 140-2 で認証された暗号モジュールは、モジュール認証リストにおけるそれらの DES アルゴリズムの登録を、「移行期間のみ－2007 年 5 月 19 日まで有効」との警告を含むように変更している。

認証されていない DES 実装を実装している暗号モジュールは、FIPS 承認された動作モードで、DES 実装を使用できない。

認証されていない DES 実装を実装している暗号モジュールは、DES アルゴリズムを、「非適合」の警告を付加した上で承認されていないアルゴリズムのリストに掲載することになる。

例.　承認されていないアルゴリズム：　DES（非適合）

再認証のために提出され、以前に認証された DES 実装が設計変更によって影響を受けない暗号モジュールの場合、その DES 実装は、「移行期間のみ－2007 年 5 月 19 日まで有効」との警告付きで承認されたアルゴリズムのリストに引き続き掲載される。

セキュリティに無関係な変更による再認証のために提出された暗号モジュールにおいて、それらの変更が DES 実装の動作環境に影響する場合、

１.修正された DES 実装は､DES アルゴリズムが認証されたときに有効だったバージョンの CAVS を使用した再試験に合格する。そして、認証書の承認アルゴリズムのリストにおける DES の登録及びその過渡期の使用における警告に影響はない。最初のアルゴリズム認証書における DES アルゴリズム認証の登録は、新しい動作環境の情報と共に更新される。

２．DES 実装の再試験は行わず、認証書の承認されたアルゴリズムのリストにおける DES の登録には、新しく再認証された暗号モジュールの DES 実装が再試験及び再認証されていないことを示す警告が追加される。また､「非適合」の警告付きの試験されていない DES 実装を含む、暗号モジュールのバージョン番号を識別する新しい登録が、承認されていないアルゴリズムに追加される。以下の例は、最初に認証された暗号モジュールのバージョンが依然として適用可能である状況と、新しいバージョンが認証書に加えられている状況を示している。

例 a.　承認されたアルゴリズム：　DES（移行期間のみ－2007 年 5 月 19 日まで有効；認証番号＃XXX；　バージョン　wy.z）

例 b.　承認されていないアルゴリズム：　DES（バージョン　wy.z；　非適合）

最初に認証された暗号モジュールが認証書に不掲載となり、DES 実装が再試験されない場合、DES の登録は認証書の承認されたアルゴリズムのリストから削除される。「非適合」の警告付きの試験されていないバージョンのために、新しい登録が承認されていないアルゴリズムリストに追加される。

例.　承認されていないアルゴリズム：　DES（非適合）

**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 |
| 発効日： | 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 |
| 発効日： | 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）設計情報及び構成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。

## 5.2 タンパー証跡を残すシールの試験

| | |
|---|---|
| 適用レベル： | 2、3 及び 4 |
| 発行日： | 2005 年 9 月 12 日 |
| 発効日： | |
| 最終改訂日： | 2005 年 9 月 12 日 |
| 関連するアサーション： | AS05.16, AS05.35, AS05.36, AS05.37, AS05.48, AS05.50 |
| 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**

タンパー証跡を残すシールを試験する場合、どのレベルの試験及びどの範囲の試験が適用されなければならないか？

**解答**

暗号モジュールがタンパー証跡を残すラベルを使用する場合、タンパー証跡を残さずにラベルを除去又は再適用することが不可能でなければならない。例えば、ラベルがタンパー証跡を残さずに除去可能で、タンパー証拠を残さずに同じラベルを再適用可能な場合、アサーションは不合格となる。

逆に、ラベルを除去するあらゆる試みが証跡を残す場合、除去及び再適用が証跡を残す場合、又は除去の途中にラベルが破壊される場合、アサーションは合格となる。これは、証跡を残すことなく及び元のラベルを破壊することなくラベルを除去するために、並びに、証跡を残さない方法で除去したラベルの再適用を可能にするために、暗号モジュール試験(CMT)機関は創造的な方法（例えば、化学的に、機械的に、熱的に）を使用しなければならないことを意味する。

**追加コメント**

攻撃の証跡を隠すために、攻撃者が新しい素材を導入するといった攻撃は範囲外である。

# 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

| | |
|---|---|
| 発効日： | 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ェ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 のソフトウェ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 |
| 発効日： | 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**

暗号モジュール認証プログラムは、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認証プログラム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 |
| 発効日： | 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**

## 6.4 承認された完全性技術

| | |
|---|---|
| 適用レベル： | すべて |
| 発行日： | 2005 年 1 月 21 日 |
| 発効日： | |
| 最終改訂日： | 2005 年 1 月 21 日 |
| 関連するアサーション： | AS06.08 |
| 関連する試験者に課せられる要求事項： | TE06.08.01、TE06.08.02 |
| 関連するベンダに課せられる要求事項： | 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か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、FIPS140-2 の 4.6.1 章に述べられている。

**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か、そしてそれはいつ実行されなければならないか？

**解答**

承認された完全性技術は、承認され、認証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ある。 これにはデジタル署名、HMAC又はMACを含んでいる。 承認されたセキュリティ機能はFIPS 140-2 Annex Aに記載されている。

承認された完全性技術は、パワーアップ自己テストで議論され、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らない。

**追加コメント**

# 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 |
| 発行日： | |
| 発効日： | 2004 年 2 月 10 日 |
| 最終改訂日： | 2005 年 9 月 12 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**

暗号モジュールは、暗号モジュール間のセキュアな通信接続を確立及び保守するために、各種非対称鍵確立プロトコルを使用する場合がある。FIPS 140-2 Annex D は、FIPS 140-2 に適用可能な承認された鍵確立技術のリストを提供する。

**質問／問題**

FIPS 140-2 Annex D には、現時点では承認された非対称鍵確立方法が無いと記載されている。承認された非対称鍵確立方法論が確立されるまでの間、暗号化と復号に用いる鍵を確立するために、FIPS で承認された動作モード（すなわち、FIPS モード）において、どの非対称鍵確立プロトコルを用いることができるか？

**解答**

鍵確立は、二段階のプロセスである。**第一段階**は、二つの相手の非対称鍵から共通の秘密を導出することに関係する。鍵確立プロトコルの**第二段階**は、第一段階の実行の間に確立された共通の秘密からの鍵の導出である。

第一段階

FIPS モードにおいて共通の秘密を確立するために、次の非対称鍵確立方法論が許可されている。

- Diffie-Hellman（鍵共有）
- EC Diffie-Hellman（鍵共有）
- 非対称鍵を使用した鍵配送（鍵包み）
- MQV
- EC MQV

**第二段階**

鍵確立プロトコルの**第二段階**は、**第一段階**の実行の間に確立された共通の秘密からの鍵の導出である。この鍵は暗号化と復号に用いられる。FIPS モードにおいて、次の鍵導出方法が許可されている。

- FIPS 140-2 IG 7.2で規定されている鍵導出機能
- 導出結果として要求される鍵のエントロピーを損なわない鍵導出方法

提出された試験報告書は、その方法を記述し、根拠を示さなければならない。

鍵確立プロトコルは、いくつかの異なる技術から構成され、両方の段階を包含してもよい。

次のプロトコルは、暗号化と復号に用いられる鍵を確立するために FIPS モードで使用することについて、許容可能である。

- SSL: SSL v3.1 に限り、FIPS モードで使用することについて、許容可能である。

- TLS 及び EAP-TLS： これら二つのプロトコルは 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 モードでの使用を許容可能にしている。

- 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承認されたセキュリティ機能である限り、FIPS モードで使用可能である。

- SSH： SSH プロトコル v2 は、その実装に用いられる暗号アルゴリズムが承認されたセキュリティ機能である限り、FIPS モードで使用可能である。

次のプロトコルは、暗号化及び復号に用いられる鍵を確立するための第一段階を満たさないため、FIPS モードでの使用を許容できない。

- SSL： SSL v3.1[1] を除くSSLプロトコルの全バージョンはFIPSモードで使用されない。SSLプロトコルがその動作において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を混在させる使い方をしているので、FIPSモードでSSLプロトコルを使用することは、禁止されている[2]。

  注 1： TLS v1.0 と同等とみなせるので、SSL v3.1 は許可される。

  注 2： 「例えばSSL 3.0 で問題となっているのは、SSL 3.0 のすべての暗号スイートに適用する鍵導出プロセスである。SSL鍵交換の間に設定されるマスター鍵の半分は、MD5 ハッシュ機能に完全に依存している。MD5 はFIPS承認されているアルゴリズムではなく、最近衝突耐性特性がAntoine Jouxによって破られている。SSL3.0 において、どのような暗号スイートが選択されていても、MD5 が使用されているのは事実である。その暗号スイートでMD5 が使用されていると明記されていない場合においても。TLSも鍵配送/鍵導出においてMD5 を用いているが、マスター鍵のすべてはMD5 とSHA-1 の両方に依存している点が異なる。よって、暗号モジュール認証プログラムは、TLSはそのセキュリティにおいて実際のところ、MD5 には依存してはおらず（適切な暗号スイートが選択されている場合)、適切な暗号スイートを使用するTLSの実装はFIPS 140-2 のもとで認証されると判定した。よって、どの暗号スイートが選択されたとしても、SSL3.0 が認証されないのに対して、TLSは機微であるが機密ではない情報を守るために使用されてもよい。既知のように、TLSは実際、SSLのバージョン 3.1 であり、多くの現在のサーバ及びクライアントはSSL 3.0 及びTLSの両方に対応している。」
  William Burr, NIST Security Technology Group

- パスワードベースの鍵確立プロトコル：PKCS#5 など、すべてのパスワードベースの鍵確立プロトコルは FIPS モードで使用することはできない。

CMVP は、FIPS モードで用いられる他の技術及び/又はプロトコルを許可する可能性があるが、それらは次のすべての要求事項を満たさなければならない。

- 業界で容認されている
- 商業利用可能である
- 政府及び業界において幅広く利用されている
- 公知である

FIPS モードでの使用において、許可される技術及び/又はプロトコルの最終決定は、CMVP によってなされる。

承認された非対称鍵確立手法が確立された場合、提供された運用ガイダンスは変更される場合がある。

**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。

暗号モジュールによって用いられる鍵確立プロトコルは AS07.21 において列挙されなければならない。

## 7.2 IEEE802.11i 鍵導出プロトコルの使用

| | |
|---|---|
| 適用レベル： | すべて |
| 発行日： | 2005 年 1 月 21 日 |
| 発効日： | 2005 年 1 月 21 日 |
| 最終改訂日： | 2005 年 9 月 12 日 |
| 関連するアサーション： | AS07.17 |
| 関連する試験者に課せられる要求事項： | TE07.17.01 及び TE07.17.02 |
| 関連するベンダに課せられる要求事項： | VE07.17.01 |

**背景**

FIPS140-2 Annex D に FIPS 140-2 に適用できる鍵確立技術のリストが提供されている。

FIPS140-2 Annex D で参照される商用利用可能なスキームは共有する秘密情報（“鍵生成材料”と呼ばれることがある）の導出に関わっている。IEEE802.11i 規格は二者間で共有する秘密情報から鍵を導出する方法を記述している。しかしそれは秘密情報を共有する方法については規定していない。

**質問／問題**

Annex D で規定された鍵確立技術を用いて秘密情報の共有ができたとして、暗号モジュールはデータ保護鍵、鍵暗号鍵、及びその他の FIPS 承認された動作モードで使用する鍵を導出するために IEEE802.11i 鍵導出技術を利用することは可能か？

**解答**

確立された鍵生成材料から鍵を導出する方法を規定する FIPS 又は NIST 推奨方式ができるまでは、共有する秘密情報から鍵を導出するのに使用される IEEE 802.11i で規定された鍵導出機能は IEEE 802.11i プロトコルの中の FIPS 動作モードで使用可能である。

**追加ノート及び条件**

NIST はパブリックコメントのために SP800-56 ドラフトを発行する予定である。この文書は最終的には承認された鍵生成材料の導出方法を提供する予定である。

FIPS 承認された動作モードで動作する IEEE 802.11i プロトコルの実装は次の要求事項を満

足しなければならない。

1. 鍵が共有する秘密情報から導出される場合、
   a) 共有された秘密情報（鍵生成材料）は FIPS 140-2 Annex D に規定された FIPS 承認手法を用いて確立されること、及び
   b) IEEE 802.11i で定義された鍵導出機能を用いること。

2. IEEE 802.11i プロトコルがデータ保護に使用される場合、データ保護方法は AES CCM でなければならない。これは FIPS 140-2 Annex A で規定された、FIPS 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のひとつである。

3. 鍵生成材料は FIPS 140-2 で規定された手動の方法によって確立されてもよい。また、IEEE 802.11i で規定された鍵導出機能が適用されてもよい。

**参考**

Amendment 6：IEEE 802.11Medium Access Control (MAC) Security Enhancements, IEEE P802.11i/D10.0, April 2004. Section 8.5.1.2. Pairwise Key Hierarchy.

## 7.3 ANSI X9.31 乱数生成器における他の核となる共通鍵暗号アルゴリズムの使用

| | |
|---|---|
| 適用レベル： | すべて |
| 発行日： | 2005 年 1 月 21 日 |
| 発効日： | 2005 年 1 月 28 日 |
| 最終改訂日： | 2005 年 1 月 21 日 |
| 関連するアサーション： | AS07.10 |
| 関連する試験者に課せられる要求事項： | TE07.10.01 |
| 関連するベンダに課せられる要求事項： | VE07.10.01 |

**背景**

ANSI X9.31 Appendix A.2.4 は、決定論的乱数生成器の核となる共通鍵暗号アルゴリズムとして 2-key Triple-DES を指定している。

**質問／問題**

ANSI X9.31 Appendix A.2.4 乱数生成器の核となるアルゴリズムとして他の FIPS 承認された共通鍵暗号アルゴリズムを使用してもよいか？

**解答**

2-key Triple-DES に加えて、ANSI X9.31 乱数生成器の核となるアルゴリズムとして、次の FIPS 承認された共通鍵暗号アルゴリズムは使用可能である:

- AES
- 3-key Triple-DES
- SKIPJACK

アルゴリズム評価ツール CAVS を用いたテストは、2-key Triple-DES、3-key Triple-DES 及び AES に利用可能である。SKIPJACK アルゴリズムを用いた乱数生成器テストに CAVS が利用可能になるまでの間、モジュール試験目的のために、核となる暗号のアルゴリズム SKIPJACK は認証されなければならないが、乱数生成器への実装は“vendor affirmed”のように記述されるだろう。

**追加コメント**

3-key Triple-DES 及び AESを実装するためのNIST 乱数生成器仕様の参照先としてANSI X9.31 Appendix A.2.4 を含むようにFIPS 140-2 Annex Cが更新された。

## 7.4 パワーアップ自己テストのための鍵のゼロ化

| | |
|---|---|
| 適用レベル： | すべて |
| 発行日： | 2005 年 9 月 12 日 |
| 発効日： | |
| 最終改訂日： | 2005 年 9 月 12 日 |
| 関連するアサーション： | AS07.41 |
| 関連する試験者に課せられる要求事項： | TE07.41.01, 02, 03 及び 04 |
| 関連するベンダに課せられる要求事項： | VE07.41.01 |

**背景**

FIPS 140-2 の 4.7.6 節は、「暗号モジュールは、暗号モジュール内における平文の秘密鍵及びプライベート鍵の全て、並びにその他の保護されていない CSP の全てをゼロ化するための方法を提供しなければならない。」と規定している。

**質問/問題**

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、4.7.6 節に基づいて、ゼロ化が要求されるか？

**解答**

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 とはみなされず、よって暗号モジュールによって使用される他の CSP と共にゼロ化されることを要求されない。

**追加コメント**

## 7.5 鍵確立方法の強度

| | |
|---|---|
| 適用レベル： | すべて |
| 発行日： | 2005 年 11 月 23 日 |
| 発効日： | 2005 年 6 月 29 日 |
| 最終改訂日： | 2005 年 11 月 23 日 |
| 関連するアサーション： | AS07.19 |
| 関連する試験者に課せられる要求事項： | TE07.19.01-02 |
| 関連するベンダに課せられる要求事項： | VE07.19.01 |

**背景**

FIPS 140-2 AS07.19 は「鍵確立の方法のセキュリティを危殆化すること(例えば、鍵確立に使用されるアルゴリズムのセキュリティを危殆化すること)は、鍵配送又は鍵共有された暗号鍵の値を決定するのと同じ数の操作を必要としなければならない。」と明記している。

NIST Special Publication 800-57, Recommendation for Key Management - Part 1: General, Section 5, Sub-Section 5.6.1, Comparable Algorithm Strength, は、承認されたアルゴリズムの比較可能なセキュリティ強度を規定している表 2 を含む。

表２： 比較可能な強度

| セキュリティビット | 対称鍵アルゴリズム | FFC （例 DSA、D-H） | IFC （例 RSA） | ECC （例 ECDSA） |
|---|---|---|---|---|
| 80 | 2TDEA[18] | L=1024<br>N=160 | k=1024 | Ff=160-223 |
| 112 | 3TDEA | L=2048<br>N=224 | k=2048 | Ff=224-255 |
| 128 | AES-128 | L=3072<br>N=256 | k=3072 | Ff=256-383 |
| 192 | AES-192 | L=7680<br>N=384 | k=7680 | Ff=384-511 |
| 256 | AES-256 | L=15,360<br>N=512 | k=15360 | Ff=512+ |

[18] 2TDEA の 80 ビットセキュリティは、攻撃者に対して、$2^{40}$ の平文及び暗号文ブロックの組み

合わせが有効であることに基づいている。([ANSIX9.52]、Annex B を参照)

1. 列 1 は、アルゴリズム及び特定の行の鍵サイズによって規定されるセキュリティのビット数を示している。計算上の優位となる、それらのアルゴリズムへの攻撃によっては、セキュリティビットが、必ずしもそのアルゴリズムに対する他の列での鍵サイズと同じである必要はないことに注意。
2. 列 2 は、示されたセキュリティレベル（最低限）を提供する対称鍵アルゴリズムを識別する。2TDEA 及び 3TDEA は[SP800-67]に規定されており、AES は[FIPS197]に規定されている。2TDEA は二つの異なる鍵を用いる TDEA である。3TDEA は三つの異なる鍵を用いる TDEA である。
3. 列 3 は、有限フィールド暗号（FFC）を使用する標準に関係するパラメータの最小サイズを示している。このようなアルゴリズムの例には、デジタル署名に用いる[FIPS 186-3]で定義されている DSA、並びに[ANSIX9.42]及び[SP800-56]に定義されている Diffie-Hellman(DH)及び MQV 鍵共有が含まれる。ここで、L は公開鍵のサイズであり、N はプライベート鍵のサイズである。
4. 列 4 は、素因数分解暗号（IFC）に基づくアルゴリズムで使用される k（モジュラス n のサイズ）の値を示す。このタイプの主なアルゴリズムは、RSA アルゴリズムである。RSA は[ANSIX9.31]及び[PKCS#1]に規定されている。デジタル署名についてのこれらの仕様は[FIPS186-3]に参照されている。k の値は、通常、鍵サイズと考えられている。
5. 列 5 は、[ANSIX9.62]でデジタル署名のために規定され及び[FIPS186-3]に採用された楕円曲線暗号（ECC）に基づくアルゴリズム用の、並びに[ANSIX9.63]及び[SP800-56]で規定されている鍵確立用の f （n のサイズ、なお n は基点 G の配列）の範囲を示している。f の値は、通常、鍵サイズと考えられている。

例えば、256 ビット AES が RSA によって送られた場合、RSA 鍵ペアの k の値は 15,360 である。256 ビット AES の鍵配送用鍵は 256 ビット AES 鍵を包むために使用される。

**上記の表 2 に掲載されていない鍵の強度では、**RSA 又は Diffie-Hellman 鍵の鍵長と同一の強度を持つ対称鍵の鍵長の対応は以下のように計算される。

RSA 鍵又は DH 鍵の鍵長が N の場合、およそ同じ強度の対称鍵の鍵長 x は以下のように計算される。

$$x = \frac{1.923 \times \sqrt[3]{N \times \ln(2)} \times \sqrt[3]{\left[\ln\left(N \times \ln(2)\right)\right]^2} - 4.69}{\ln(2)}$$

したがって、512 ビット又は 4096 ビット Diffie-Hellman を使用して確立された鍵の強度、あるいは 512 ビット又は 4096 ビット包み鍵の RSA を使用して配送された鍵の強度は、それぞれ、およそ 56 又は 150 ビットである。

**質問／問題**

FIPS 140-2 アサーション　AS07.19 は NIST Special Publication 800-57 の文脈において何を意味するか？

**解答**

その要求事項は 4.7 節にある鍵確立技術に適用される。

鍵共有又は鍵配送方法によって鍵が確立される場合、配送鍵又は鍵確立技術は、配送される又は確立される鍵以上の強度でなければならない。例えば、2 キーTriple-DES の鍵（80 ビットの強度）を配送するために、2048 ビット RSA 鍵（112 ビットの強度）を使用することは適切である。

暗号モジュールによって確立できる（額面通りに取った）最大の鍵の見かけの強度が、実装された鍵確立技術の比較しうる最大の強度以上である場合、モジュールの認証書及びセキュリティポリシは、他の要求されている警告に加えて、鍵確立技術について　”（鍵確立方法論はｘｘビットの暗号強度を提供する）”　の警告を注釈で付けられる。例えば、256 ビット AES が、RSA 鍵ペア用に k=1024 の値の RSA を使用して配送された場合、”RSA（PKCS#1、鍵包み、鍵確立方法論は 80 ビットの暗号強度を提供する ”　と警告に記載する。

さらに、ある特定の鍵確立技術のために、モジュールがいくつかの鍵強度をサポートする場合、FIPS モードで操作される間、鍵によって提供される強度の範囲を警告に記載する。例えば、モジュールが 512 及び 1024 ビット Diffie-Hellman を実装する場合、”Diffie-Hellman（鍵共有、鍵確立方法論は 56 ビットと 80 ビット間の暗号強度を提供する）”と警告に記載する。たとえ下記の表 4 に強度は十分であると記載されていたとしても、これらの警告は、連邦政府のユーザに対して、モジュールが提供する実際の強度を明確に示す。

**追加コメント**

NIST Special Publication 800-57, Recommendation for Key Management - Part 1: General (August 2005) は、5.6.2 節の以下の情報も提供する。

表 4 は、連邦政府の機密ではないアプリケーションで用いるアルゴリズム及び鍵サイズの適切な組み合わせを選択するために使用できる。少なくとも 80 ビットのセキュリティが、2010 年まで提供されなければならない。2011 年から 2030 年の間、少なくとも 112 ビットのセキュリティが提供されなければならない。その後、少なくとも 128 ビットのセキュリティが提供されなければならない。

1. 列 1 は、特定の暗号アルゴリズムによって保護されているデータがセキュアに保たれる、予想期間を示している。(すなわち、アルゴリズムセキュリティのライフタイム)
2. 列 2 は、適切な対称鍵アルゴリズムと鍵サイズを示している。2TDEA 及び 3TDEA は、[SP800-67]で規定され、AES アルゴリズムは[FIPS197]で規定され、ブロック暗号を使用したメッセージ認証コード(MACs) の計算は[SP800-38]で規定されている。
3. 列 3 は、[FIPS186-3]で規定されている DSA などの、FFC に関連するパラメータの最小サイズを示している。
4. 列 4 は、[ANSIX9.31]及び[PKCS#1]で規定され、並びにデジタル署名用に[FIPS186-3]に採用されている IFC で用いるモジュラスの最小値を示している。
5. 列 5 は、[ANSIX9.62]でデジタル署名のために規定され及び[FIPS186-3]に採用された楕円曲線暗号 (ECC) に基づくアルゴリズム用の、並びに[ANSIX9.63]及び[SP800-56]で規定されている鍵確立用の f (n のサイズ、なお n は基点 G の配列) の範囲を示している。f の値は、通常、鍵サイズと考えられている。

表 4：推奨アルゴリズムと最小鍵サイズ

| **アルゴリズムセキュリティライフタイム** | **対称鍵アルゴリズム(暗号化及び MAC)** | **FFC (例 DSA、D-H)** | **IFC (例 RSA)** | **ECC (例 ECDSA)** |
|---|---|---|---|---|
| 2010 年まで (最小 80 ビットの強度) | 2TDEA[21]<br>3TDEA<br>AES-128<br>AES-192<br>AES-256 | 最小値：<br>L=1024;<br>N=160 | 最小値：<br>k=1024 | 最小値：<br>f=160 |

| | | | | |
|---|---|---|---|---|
| 2030 年まで（最小 112 ビットの強度） | 3TDEA<br>AES-128<br>AES-192<br>AES-256 | 最小値：<br>L=2048;<br>N=224 | 最小値：<br>k=2048 | 最小値：<br>f=224 |
| 2030 年以後（最小 128 ビットの強度） | AES-128<br>AES-192<br>AES-256 | 最小値：<br>L=3072;<br>N=256 | 最小値：<br>k=3072 | 最小値：<br>f=256 |

[21] 2TDEA の 80 ビットセキュリティは、平文及び暗号文ブロックの照合において $2^{40}$ の推測可能性が攻撃者に対してあることに基づいている。([ANSIX9.52]、Annex B を参照)

テーブル内のアルゴリズムと鍵サイズは、与えられた期間の間、データを保護するために適切であると考えられる。与えられた年数範囲に対して示されていないアルゴリズム又は鍵サイズはその期間の間、情報を保護するために使用されてはならない。情報のセキュリティライフが表に規定されているある期間を超えて次の期間（より後の期間）に及ぶ場合、より後の期間のために規定されているアルゴリズムと鍵サイズが使用されなければならない。以下の例は表の使用方法を明確にするために提供される。

a. 情報が 2005 年に暗号化され、そのデータの期待される最長のセキュリティ寿命が 5 年だけであるならば、表のアルゴリズム又は鍵サイズのどれを使用してもよい。しかし、情報が 2005 年に保護されており、データの期待されるセキュリティ寿命が 6 年であるならば、2TDEA は適切ではない。
b. CA 署名鍵及びすべての証明書が、鍵が 2005 年に期限切れになるという条件で発行される場合は、証明書に署名するために用いられる署名及びハッシュアルゴリズムは、少なくとも 5 年間はセキュアである必要がある。1024 ビット DSA 及び SHA-1 を用いて 2005 年に発行された証明書は、許容できる。
c. 情報が 2009 年に最初に署名されて、最長 10 年間（すなわち、2009 年から 2019 年まで）セキュアであることが要求される場合、1024 ビット RSA 鍵では 2011 年と 2019 年の間十分な保護を提供しない。したがってこの場合において、1024 ビット RSA の使用は勧められない。暗号の保護を提供するために「2030 年まで」の行にあるアルゴリズム及び鍵サイズ（例えば、2048 ビット RSA）の使用を勧める。それに加えて、署名は、SHA-224 又は SHA-256 などの、比較しうる又はそれ以上の強度のハッシュアルゴリズムを使用して生成されなければならない。

CMVP は、表 4 の情報についての、追加のガイダンスと移行期間を提供する予定である。

# 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 |
| 発効日： | 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決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。しかし、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はそうではない。

**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 |
| 発効日： | 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 |
| 発効日： | 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なくてもよい。

**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る。

例：HMAC-SHA-1 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-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、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 |
| 発効日： | 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:推奨ソフトウェア開発手順

# 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 |
| 発効日： | 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ェアコンポーネント、ソフトウェアコンポーネント、及びファームウェ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 |
| 発効日： | 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**

その他の攻撃に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、その他の攻撃に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

以上