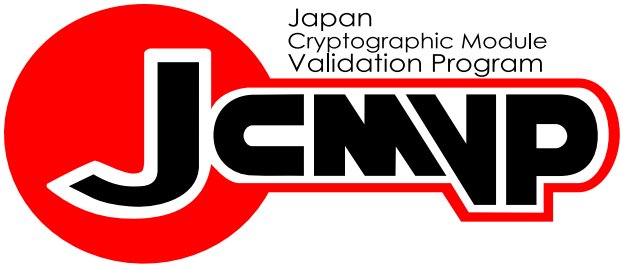

暗号モジュール試験及び認証制度の基本規程

令和 2 年 10 月 16 日

JCM-01

Japan Cryptographic Module Validation Program

独立行政法人　情報処理推進機構

目 次

第 1 章 総則 1
1.1 本規程の目的 1
1.2 本制度の目的 1
1.3 本制度の原則 1
1.4 試験及び認証の要求事項 1
1.5 用語及び定義 1
第 2 章 制度の体系 4
2.1 本制度に関する規程等 4
2.2 制度を構成する者 5
2.2.1 申請者 5
2.2.2 試験機関 6
2.2.3 認証機関 6
2.2.4 認定機関 6
第 3 章 暗号モジュール試験及び認証、並びに暗号アルゴリズム確認 6
3.1 暗号モジュール認証及び暗号アルゴリズム確認の申請 6
3.2 暗号モジュール試験 6
3.3 暗号モジュール認証 6
3.4 暗号アルゴリズム確認 7
3.5 認証済暗号モジュールの再認証及び保証継続 7
3.6 申請者が支払うべき費用 8
第 4 章 申請者の権利及び義務 8
4.1 暗号モジュール認証等の認証被許諾者の権利及び義務 8
第 5 章 暗号モジュール認証等の一時停止又は取消 8
5.1 サーベイランス 8
5.2 再試験 8
5.3 暗号モジュール認証等の一時停止又は取消 8
第 6 章 雑則 9
6.1 秘密保持 9
6.2 禁止事項 9
6.3 認証機関が行う本制度の円滑な運営に必要な業務 9
6.3.1 規程類の整備 9
6.3.2 ガイダンスの発行と公表 9
6.3.3 試験の進捗状況の聴取等 9
6.4 認証書等の所有権及び著作権 9

6.5 認証書等の不正利用等への対処 10
6.6 異議申し立て及び苦情の処理 10
附属書 A：本制度の要求事項 12

暗号モジュール試験及び認証制度の基本規程

制定　平成 19 年 5 月 9 日　2007 情総第 17 号
最終改正　令和 2 年 10 月 16 日　2020 情総第 1124 号　一部改正

第 1 章 総則

1.1 本規程の目的

本規程は、情報処理の促進に関する法律（昭和 45 年法律第 90 号）第 51 条第 1 項第 5 号『情報処理に関する安全性及び信頼性の確保を図るため、情報処理システムに関する技術上の評価及び情報処理サービス業を営む者の技術的能力その他事業の適正な実施に必要な能力に関する評価を行うこと。』に基づき、独立行政法人 情報処理推進機構（以下「機構」という。）が運営する暗号モジュール試験及び認証制度（JCMVP [Japan Cryptographic Module Validation Program]）（以下「本制度」という。）について定めるとともに、本制度に関して、暗号モジュールの申請者及び本制度の運営に関係する者が遵守しなければならない基本的事項を定める。

1.2 本制度の目的

本制度は、日本国内におけるセキュアな暗号モジュールの調達、購入及び利用に資するために、電子政府推奨暗号リスト等に記載されている暗号化機能、ハッシュ機能、署名機能等のセキュリティ機能を実装したハードウェア、ソフトウェア又はファームウェアから構成される**暗号モジュール**が、その内部に格納するセキュリティ機能及び暗号鍵、パスワード等の重要情報を適切に保護していることを、第三者が試験及び認証することにより、暗号モジュールの利用者が、正確かつ詳細に把握できるようにすることを目的とする。

1.3 本制度の原則

本制度が**暗号モジュール**の利用者に信頼されるため、試験機関、認証機関及びこれらの関係者が、公正、非差別的で商業的利害に影響されることなく、附属書 A に掲げる***暗号モジュールセキュリティ要件***及び***暗号モジュール試験要件***に従い、高い技術力に基づいて公正な試験及び認証を行わなければならない。

1.4 試験及び認証の要求事項

本制度で行う試験及び認証の要求事項は、附属書 A に掲げる***暗号モジュールセキュリティ要件***及び***暗号モジュール試験要件***とする。

1.5 用語及び定義

本規程において使用する用語及び定義は、特別の定めのある場合を除き、次によるほか、

附属書Aに掲げる関連規格による。

暗号モジュール認証機関：
本制度に基づいて、**暗号モジュール認証**を実施する組織。（以下「認証機関」という。）

暗号モジュール試験機関：
本制度に基づいて、**暗号モジュール試験**を実施する組織。（以下「試験機関」という。）

承認されたセキュリティ機能：
ブロック暗号、ストリーム暗号、非対称鍵、メッセージ認証コード、ハッシュ機能、乱数生成器、鍵確立等の、認証機関によって承認された動作モードを伴う暗号アルゴリズム。

暗号アルゴリズム確認対象非承認セキュリティ機能：
暗号アルゴリズム確認の対象となる暗号アルゴリズムであって、**承認されたセキュリティ機能**ではないもの。

暗号アルゴリズム実装試験：
承認されたセキュリティ機能及び**暗号アルゴリズム確認対象非承認セキュリティ機能**に対して、その入力値及び出力値の関係が所定の特性を示していることを確認するために、**承認されたセキュリティ機能**及び**暗号アルゴリズム確認対象非承認セキュリティ機能**の仕様を満たすかどうかを確認するための試験方法を定めた***附属書 A*** に掲げる***暗号アルゴリズム実装試験要件***に従った**暗号アルゴリズム実装試験ツール**（以下 **JCATT** [Japan Cryptographic Algorithm implementation Testing Tool]という。）を用いて、試験機関が試験すること。

暗号アルゴリズム実装試験報告書：
認証機関に対して**暗号アルゴリズム実装試験**の結果の報告を行うために、試験機関が発行する文書。

暗号アルゴリズム確認：
試験機関による**暗号アルゴリズム実装試験**が、本制度の定めに従って実施されたこと及び当該試験結果が正当であることを、認証機関が確認すること。

暗号アルゴリズム確認書：
試験機関による**暗号アルゴリズム実装試験**が、本制度の定めに従って実施されたこと及び当該試験結果が正当であると確認したことを示すために、認証機関が申請者に対して発行

する文書。

暗号モジュール：
承認されたセキュリティ機能を実装した、**暗号境界**内のハードウェア、ソフトウェア又はファームウェアの集合。

暗号境界：
暗号モジュールの物理的及び論理的な領域を確立し、かつ、**暗号モジュール**の全てのハードウェア、ソフトウェア又はファームウェアのコンポーネントをそのなかに含む、明確に定義された連続する境界線。

暗号モジュール試験：
暗号モジュールが、その内部に格納するセキュリティ機能及び暗号鍵、パスワード等の重要情報を適切に保護していることを判定するために、***暗号モジュールセキュリティ要件***を満たすかどうかを確認するための試験方法を定めた***附属書 A*** に掲げる規格（以下「***暗号モジュール試験要件***」という。）に従って、試験機関が試験すること。

暗号モジュール試験報告書：
認証機関に対して**暗号モジュール試験**の結果の報告を行うために、試験機関が発行する文書。**暗号モジュール試験報告書作成支援ツール**（以下 **CRYPTIPA** [Cryptographic Module Testing Report Supporting Tool by IPA]という。）を用いて作成するもののほか、物理的セキュリティに関する試験を行う場合には、様式を特に定めない「物理的セキュリティ試験報告書」もこの一部をなす。

暗号モジュール認証：
試験機関による**暗号モジュール試験**が、本制度の定めに従って実施されたこと及び当該試験結果が***附属書 A***に掲げる***暗号モジュールセキュリティ要件***にてらして正当であることを、認証機関が検証すると共に、試験結果の再現性（試験機関、試験要員等に関わらず試験結果が一致すること）を確保すること。

暗号モジュール認証書：
当該**暗号モジュール**が***附属書 A*** に掲げる***暗号モジュールセキュリティ要件***を満たしていることを証明するために認証機関が発行する文書。

暗号モジュール認証報告書：
暗号モジュール試験が本制度の定めに従って実施されたこと及び**暗号モジュール**に対する

試験結果が検証されたことを示すことを、申請者に対して、***附属書 A*** に掲げる***暗号モジュールセキュリティ要件***に関して検出した事項を報告するために、認証機関が発行する文書。試験機関が行った試験の結果を要約し、当該結果を確認したものとなる。

試験用提供物件：
暗号モジュールの試験又は認証を実行するために必要なものとして試験機関又は認証機関が申請者に要求する物件。

試行試験：
試験機関が、認証機関による承認を受けるために行う**暗号モジュール試験**。

セキュリティポリシ：
暗号モジュールが動作中に従わなければならないセキュリティのルールを明確にした仕様。そのセキュリティのルールは、***附属書 A*** に掲げる***暗号モジュールセキュリティ要件***から導出されたセキュリティの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のルールを含む。

セキュリティレベル：
取り扱うデータの重要度の違いや異なる使用環境に対応し、費用対効果のある解決策を提供するために設定された、**暗号モジュール**のセキュリティに関する 4 つのレベル。各**セキュリティレベル**は、下位のレベルで求められる事項に、より高度なセキュリティ要件を加える形で規定されている。各**セキュリティレベル**の詳細については、***附属書 A*** に掲げる***暗号モジュールセキュリティ要件***を参照すること。

製品評価技術基盤機構認定制度（ASNITE [Accreditation System of National Institute of Technology and Evaluation]）**試験事業者（IT）**：
ISO/IEC 17025:2017 等の国際基準に基づき認定された、IT 製品及びシステムのセキュリティ評価並びに暗号モジュール試験を行う試験事業者（以下「**ASNITE 試験事業者 IT**」という。）。

第 2 章 制度の体系

2.1 本制度に関する規程等

本制度に関する規程等は次のとおりである。

本制度に関して、暗号モジュールの申請者及び本制度の運営に関係する者が遵守しなけれ

ばならない基本的事項を定めた文書。

＜暗号モジュール試験及び認証制度における制度文書＞	
（JCM-01）暗号モジュール試験及び認証制度の基本規程	［***制度基本規程***］

認証機関を構成する者が遵守しなければならない事項を定めた文書。

＜認証業務の運営に関する文書＞	
（CBM-01）暗号モジュール認証機関の組織及び業務運営に関する規程	［***業務運営規程***］
（CBM-01-A）暗号モジュール認証業務取扱手順	［***業務取扱手順***］
（CBM-01-B）暗号モジュール試験機関承認業務取扱手順	［***試験機関承認取扱手順*** ］
（CBM-01-C）暗号モジュール認証機関要員管理手順	［***要員管理手順*** ］

認証申請を行う暗号モジュールの申請者が遵守しなければならない事項を定めた文書。

＜認証の申請等に関する文書＞	
（CBM-02）暗号モジュール認証申請手続等に関する規程	［***認証申請手続規程*** ］

試験機関の承認申請を行う者が遵守しなければならない事項を定めた文書。

＜試験機関の承認に関する文書＞	
（CBM-03）暗号モジュール試験機関承認申請手続等に関する規程	［***試験機関承認申請規程*** ］

注 1：[括弧]内は、略称を示す。
注 2：上記の英字 3 文字の記号は、次の頭文字を取ったものである。
JCM … Japan Cryptographic Module Validation Program
CBM … Certification Body Management System

2.2 制度を構成する者

本制度を構成する者を以下に規定する。

2.2.1 申請者

本制度において申請者とは、***暗号モジュール認証申請手続等に関する規程***（以下「***認証申請手続規程***」という。）に基づき、**暗号モジュール**の認証又は暗号アルゴリズム実装の確認を申請する法人である。申請する対象は、原則として、日本又は輸出貿易管理令別表第 3 の地域で開発又は製造される暗号モジュール又は暗号アルゴリズム実装である。申請者は、原則として、日本又は輸出貿易管理令別表第 3 の地域に本社を有する開発又は製造する者、ベンダその他の法人、又は機関とする。なお、前述に該当しない暗号モジュールや暗号アルゴリズム実装、又は申請者からの申請等の場合には、運営審議委員会にて申請受理が相当と認められる必要がある。

2.2.2 試験機関

本制度において試験機関とは、本制度に基づいて、**暗号モジュール試験**を実施する組織である。試験機関は、認定機関によって **ASNITE 試験事業者 IT** に適合する試験機関として認定され、***暗号モジュール試験機関承認申請手続等に関する規程***（以下「***試験機関承認申請規程***」という。）の手続きに従って、認証機関から本制度の試験機関として承認を得なければならない。

2.2.3 認証機関

本制度において認証機関とは、機構内に設置され、試験機関が行った試験結果に基づき、**暗号モジュール認証**を行う組織である。認証機関は、本制度における認証を行うにあたっては、JIS Q 0065 で規定された要件を満たすように、組織化及び運営をするものとする。

2.2.4 認定機関

本制度において認定機関とは､独立行政法人製品評価技術基盤機構認定センター(IAJapan)とする。

第 3 章 暗号モジュール試験及び認証、並びに暗号アルゴリズム確認

3.1 暗号モジュール認証及び暗号アルゴリズム確認の申請

申請者は、***認証申請手続規程***に定めるところにより、認証機関に対して暗号モジュール認証又は暗号アルゴリズム確認申請の手続きを行わなければならない。認証機関は、***暗号モジュール認証機関の組織及び業務運営に関する規程***（以下「*業務運営規程*」という。）に定めるところにより、申請者からの暗号モジュール認証又は暗号アルゴリズム確認の申請を受付ける。

3.2 暗号モジュール試験

試験機関は、申請者が指定する***暗号モジュールセキュリティ要件***に基づき、**暗号モジュール試験**を行う。

試験機関は、**暗号モジュール試験**の結果に基づき、**暗号モジュール試験報告書**を作成し、申請者から提出された当該暗号モジュールの「セキュリティポリシ」を添えて、認証機関に提出しなければならない。

3.3 暗号モジュール認証

認証機関は、***業務運営規程***に定めるところにより、試験機関から提出される報告書に対して、次を実施する。

a) 試験機関から提出される**暗号アルゴリズム実装試験報告書**について**暗号アルゴリズム確認**を行い、**暗号アルゴリズム確認書**を作成し、試験機関を通じて、申請者に対して**暗号アルゴリズム確認書**を交付する。
b) 試験機関から提出される**暗号モジュール試験報告書**について**暗号モジュール認証**を行い、**暗号モジュール認証報告書**及び**暗号モジュール認証書**を申請者に交付する。

3.4 暗号アルゴリズム確認

認証機関は、***業務運営規程***に定めるところにより、試験機関から提出される報告書に対して、次を実施する。
試験機関から提出される**暗号アルゴリズム実装試験報告書**について**暗号アルゴリズム確認**を行い、**暗号アルゴリズム確認書**を作成し、試験機関を通じて、申請者に対して**暗号アルゴリズム確認書**を交付する。

3.5 認証済暗号モジュールの再認証及び保証継続

暗号モジュール認証を許諾された申請者（以下「**認証被許諾者**」という。なお、認証被許諾者には暗号アルゴリズム確認を許諾された申請者も含む。）は、認証済**暗号モジュール**の後続バージョン（以下「**後続暗号モジュール**」という。）に対して、当初の**暗号モジュール認証**の効果を継続しようとする場合に、***認証申請手続規程***に従い再認証手続を行う。再認証手続を行うにあたって、**認証被許諾者**は、**後続暗号モジュール**の変更内容が、***暗号モジュールセキュリティ要件***に関連した事項に与える影響の有無を判断し、次の手続を行う。
a) 影響があると判断した場合、**認証被許諾者**は、後続暗号モジュールの変更内容を分析するために、試験機関に変更箇所を明示した試験用提供物件を提供する。試験機関は、必要に応じて、再認証手続に基づく**暗号モジュール試験**を行う。認証機関は、***業務運営規程***に定めるところにより再認証手続に基づく**暗号モジュール認証**を許諾する。
ただし、**後続暗号モジュール**に生じた変更が極めて大きなものである場合は、再認証手続は、適用できない。この場合は、当初と同じ**暗号モジュール試験及び認証**の手続を適用して**暗号モジュール認証**を得なければならない。
b) 影響がないと判断した場合、**認証被許諾者**は、**後続暗号モジュール**が認証に影響を与えないことを証明するものとして、「暗号モジュール影響分析報告書」を作成し、認証機関に事前検討を依頼する。認証機関は、提出された「暗号モジュール影響分析報告書」を精査し、内容を検査する。認証機関によって、認証被許諾者が実施した影響分析の結果が適切であると判断した場合、認証被許諾者に対して**暗号モジュール認証**の保証継続を認める。保証継続に関し必要な事項については、***業務取扱手順***に定める。
ただし、**後続暗号モジュール**に生じた変更が***暗号モジュールセキュリティ要件***に関連した事項に影響を与えると判断された場合は、保証継続は適用できない。この場合は、再認証手続又は当初と同じ**暗号モジュール試験及び認証**の手続を適用して**暗号モジュ**

ール認証を得なければならない。

3.6 申請者が支払うべき費用

申請者は、**暗号モジュール試験及び認証**、並びに暗号アルゴリズム確認に必要な費用を負担しなければならない。申請者が試験機関に対して支払うべき費用は、両者の契約により定める。認証機関に対して支払うべき費用は、***認証申請手続規程***に定める。

第 4 章 申請者の権利及び義務

4.1 暗号モジュール認証等の認証被許諾者の権利及び義務

認証被許諾者は、当該暗号モジュールに関して次の権利及び義務を有する。

a）**認証被許諾者**は、***認証申請手続規程***に定める「暗号モジュール認証等を許諾された申請者の責務」を遵守しなければならない。

b）**認証被許諾者**は、当該暗号モジュールを認証済であるとして供給することができる。

c）**認証被許諾者**は、当該暗号モジュールを認証済であるとして供給するときに、***認証申請手続規程***に定める「暗号モジュール認証マーク」を使用することができる。この場合に、***認証申請手続規程***に定める「暗号モジュール認証マーク等の取扱」を遵守しなければならない。

第 5 章 暗号モジュール認証等の一時停止又は取消

5.1 サーベイランス

認証機関は、**暗号モジュール認証**に関して***業務運営規程***に定めるところにより、サーベイランスを実施することがある。

5.2 再試験

認証機関は、サーベイランスの結果に基づいて***業務運営規程***に定めるところにより、再試験を指示することがある。

5.3 暗号モジュール認証等の一時停止又は取消

認証機関は、***業務運営規程***に定めるところにより、**暗号モジュール認証**又は暗号アルゴリズム確認の一時停止又は取消を行うことがある。

第 6 章 雑則

6.1 秘密保持

試験機関及び認証機関は、秘密情報が**暗号モジュール試験及び認証**の過程で無権限の者に伝わり、情報の機密性が損なわれることがないようにしなければならない。認証機関における秘密保持手続きについては、***業務運営規程***に定める。

6.2 禁止事項

試験機関及び認証機関並びにこれらの職員は、次に掲げる事項を行ってはならない。

a）正当な活動への対価以外の**暗号モジュール試験及び認証**の結果に影響する利益を得ること。

b）**暗号モジュール試験及び認証**の対象となる**暗号モジュール**の開発を行うこと。

c）申請者に対するコンサルティングサービスの提供をすること。なお、このコンサルティングサービスには、申請者が作成した文書等の多くの既存の情報を統合又は再編成を行うことを含まない。

6.3 認証機関が行う本制度の円滑な運営に必要な業務

6.3.1 規程類の整備

認証機関は、本制度を定め、本制度の運用のための方針及び規則を規定した規程類の作成、発行、配布、改定、更新および廃止をするとともに、必要に応じて、本制度の方針及び規則の解釈を行う。

認証機関は、次のツールを開発し、試験機関へ貸与する。

a）**暗号アルゴリズム実装試験**の実施に必要な JCATT

b）**暗号モジュール試験報告書**の作成を支援する CRYPTIPA

6.3.2 ガイダンスの発行と公表

認証機関は、***暗号モジュールセキュリティ要件***及び***暗号モジュール試験要件***の運用・解釈や**本制度**の運営等に関するガイダンスを示すときには、***JCMVP 運用ガイダンス***を発行し、**本機構**のホームページ等で公表する。

6.3.3 試験の進捗状況の聴取等

認証機関は、必要に応じて、申請者又は試験機関若しくは両者に対し、**暗号モジュール試験**の進捗状況を聴取することがある。また、必要に応じて、申請者又は試験機関若しくは両者に対し、制度運営の観点から中立かつ公正な意見を述べることがある。

6.4 認証書等の所有権及び著作権

暗号アルゴリズム確認書に関する所有権及び著作権は認証機関が保有する。ただし、申請

者は、**暗号アルゴリズム確認書**を完全に複写する限りにおいて、複製して配布する権利が許諾される。
暗号モジュール認証書及び**暗号モジュール認証報告書**に関する所有権及び著作権は認証機関が保有する。ただし、申請者は、**暗号モジュール認証書**及び**暗号モジュール認証報告書**を完全に複写する限りにおいて、複製して配布する権利が許諾される。

6.5 認証書等の不正利用等への対処

認証機関は、**認証被許諾者**が「暗号モジュール認証マーク」、**暗号モジュール認証書**、**暗号モジュール認証報告書**及び**暗号アルゴリズム確認書**又はその写しを不正に使用すること、誤解を招くような方法で広告及び説明に使用すること等、***認証申請手続規程***に定める***同意書***に違反する事実が認められた場合、改善の指示を行う。改善の指示を行った結果、その改善の効果が認められない場合、当該**暗号モジュール認証**を取消すことがある。当該**暗号モジュール認証**の取消に関し必要な事項について、***業務運営規定***に定める。

6.6 異議申し立て及び苦情の処理

認証機関は、認証サービスに対する異議申し立て及び苦情を***業務運営規程***に定められた手順に従って処理する。
試験機関は、試験サービスに対する異議申し立て及び苦情の処理に関する手続きを整備しなければならない。

附　則（平成 19 年 5 月 9 日　2007 情総第 17 号・全部改正）
この規程は、平成 19 年 5 月 15 日から施行する。

附　則（平成 19 年 10 月 29 日　2007 情総第 114 号・一部改正）
この規程は、平成 19 年 10 月 29 日から施行し、平成 19 年 10 月 26 日から適用する。

附　則（平成 21 年 1 月 21 日　2008 情総第 115 号・一部改正）
この規程は、平成 21 年 1 月 8 日から施行する。

附　則（平成 21 年 11 月 4 日　2009 情総第 93 号・一部改正）
この規程は、平成 21 年 11 月 2 日から施行する。

附　則（平成 25 年 5 月 17 日　2013 情総第 37 号・一部改正）
この規程は、平成 25 年 5 月 17 日から施行する。

附　則（平成 26 年 3 月 27 日　2013 情総第 163 号・一部改正）

この規程は、平成 26 年 4 月 1 日から施行する。

附　則（平成 30 年 6 月 29 日　2018 情総第 180 号・一部改正）

この規程は、平成 30 年 7 月 1 日から施行する。

附　則（令和 2 年 5 月 12 日　2020 情総第 88 号・一部改正）

この規程は、令和 2 年 5 月 15 日から施行する。

附　則（令和 2 年 10 月 16 日　2020 情総第 1124 号・一部改正）

この規程は、令和 2 年 10 月 16 日から施行する。なお、令和 2 年 10 月 15 日に改正告知を行い、令和 2 年 11 月 1 日から適用する。

附属書 A：本制度の要求事項

本附属書では、本制度で用いる要求事項として以下の規格を定める。これらの規格において有効な規格バージョン等の情報は、認証機関がウェブページ等を通じて別途公表する。

A.1　JIS X 19790（ISO/IEC 19790）関連規格

A.1.1　暗号モジュールセキュリティ要件

A.1.1.1　ISO/IEC 19790 Information technology — Security techniques — Security requirements for cryptographic modules

A.1.1.2　JIS X 19790　セキュリティ技術－暗号モジュールのセキュリティ要求事項

ただし、セキュリティ機能については、認証機関により発行された「承認されたセキュリティ機能に関する仕様（ASF-01）」による。

A.1.2　暗号モジュール試験要件

A.1.2.1　ISO/IEC 24759　Information technology — Security techniques — Test requirements for cryptographic modules

A.1.2.2　JIS X 24759　セキュリティ技術－暗号モジュールのセキュリティ試験要件

A.1.3　暗号アルゴリズム実装試験要件

A.1.3.1　JCMVP 暗号アルゴリズム実装試験要件（ATR-01）

A.2　CMVP 関連規格

A.2.1　暗号モジュールセキュリティ要件

A.2.1.1　Federal Information Processing Standards (FIPS) PUB 140-2 Security Requirements for Cryptographic Modules 及びその後継版

A.2.2　暗号モジュール試験要件

A.2.2.1　Derived Test Requirements for FIPS PUB 140-2 及びその後継版

A.2.2.2　Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program 及びその後継版

A.2.3　暗号アルゴリズム実装試験要件

A.2.3.1　JCMVP 暗号アルゴリズム実装試験要件（ATR-01）又は認証機関が同等と認める規格

A.3　暗号アルゴリズム確認関連規格

A.3.1 承認されたセキュリティ機能に関する仕様（ASF-01）

A.3.2 暗号アルゴリズム確認対象非承認セキュリティ機能に関する仕様（LSF-01）

A.3.3　暗号アルゴリズム実装試験要件

A.3.3.1　JCMVP 暗号アルゴリズム実装試験要件（ATR-01）

注：上記の英字 3 文字の記号は、次の頭文字を取ったものである。

ASF … Approved Security Functions

LSF … Limited Security Functions

ATR … Cryptographic Algorithm Implementation Testing Requirements

改正履歴

識別番号	JCM-01

改正年月日	作成者・承認者	改正内容
平成 18 年 10 月 16 日	上野・仲田	新規制定
平成 19 年 5 月 9 日	上野・仲田	全部改正
平成 19 年 10 月 29 日	櫻井・占部	一部改正
平成 21 年 1 月 21 日	井上・仲田	一部改正
平成 21 年 11 月 2 日	櫻井・仲田	一部改正
平成 25 年 5 月 17 日	中田・仲田	一部改正
平成 26 年 3 月 27 日	中田・立石	一部改正
平成 30 年 6 月 29 日	櫻井・江口	一部改正
令和 2 年 5 月 12 日	今木・戸高	一部改正
令和 2 年 10 月 16 日	神田・戸高	一部改正