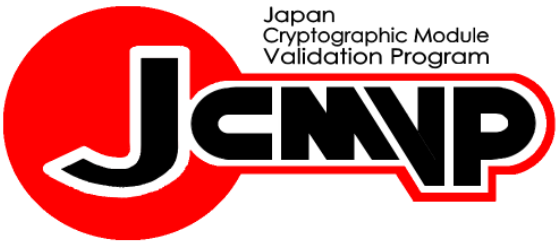

暗号モジュール試験機関承認申請手続等に関する規程

平成 30 年 7 月 1 日

IPA

CBM-03

Certification Body Management System

独立行政法人　情報処理推進機構

目次

１．目的 1
２．用語 1
３．試験及び認証の規格 1
４．暗号モジュール試験機関の承認の条件 1
５．暗号モジュール試験機関承認申請 1
５．１ 試験機関が遵守すべき事項 1
５．２ 暗号モジュール試験機関承認申請の手順 2
５．３ 秘密保持契約の締結 2
５．４ 試行試験の実施 2
５．５ 試験機関認定申請及び認定証の受領 2
６．暗号モジュール試験機関の承認 2
７．暗号モジュール試験機関承認書の再発行 2
８．暗号モジュール試験機関の承認の変更 2
９．暗号モジュール試験機関の承認の廃止 3
１０．暗号モジュール試験機関の承認の取消 3
１１．本規程の変更による処置 3
暗号モジュール試験機関承認手続に係る様式集 4
様式 1 暗号モジュール試験機関承認申請書 5
様式 2 暗号モジュール試験機関承認に係る遵守事項の誓約について 6
様式 3 暗号モジュール試験機関承認書再発行申請書 7
様式 4 暗号モジュール試験機関承認変更届 8
様式 5 暗号モジュール試験機関承認廃止届 9
様式 6 秘密保持契約書 10
様式 7 暗号モジュール試験機関承認書 13

暗号モジュール試験機関承認申請手続等に関する規程

制定　平成 19 年 5 月 9 日　2007 情総第 20 号
最終改正　平成 30 年 6 月 29 日　2018 情総第 182 号　一部改正

１．目的

本規程は、独立行政法人 情報処理推進機構 (以下「機構」という。) が暗号モジュール認証機関 (以下「認証機関」という。) として実施する暗号モジュール試験及び認証制度において、認証機関が暗号モジュール試験機関 (以下「試験機関」という。) に対して要求する事項及び試験機関が申請等の手続をするための事項を定めるものです。

２．用語

本規程で使用する用語は、「暗号モジュール試験及び認証制度の基本規程」(JCM-01)（以下「***制度基本規程***」という。）において使用する用語の例によります。

３．試験及び認証の規格

本制度で行う試験及び認証は、***制度基本規程***の附属書 A に掲げた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 (以下「***セキュリティ要件等***」という。) に基づきます。

４．暗号モジュール試験機関の承認の条件

本制度の認証機関が、試験機関を承認する条件は、次の事項です。

- 独立行政法人　製品評価技術基盤機構(以下「認定機関」という。)より ASNITE 試験事業者 IT による認定を受けていること。
- 認証機関から貸与される**暗号アルゴリズム実装試験ツール(JCATT)** を使用し、適切な**暗号アルゴリズム実装試験報告書**を作成できること。
- 認証機関から貸与される**暗号モジュール試験報告書作成支援ツール(CRYPTIPA)**を使用し、適切な**暗号モジュール試験報告書**を作成できること。

５．暗号モジュール試験機関承認申請

５．１ 試験機関が遵守すべき事項

(1) 試験機関は、***制度基本規程***及び本規程を常に遵守しなければなりません。

(2) 試験機関は、認証機関から貸与されたツール類の改竄、第三者への開示及び譲渡をしてはいけません。

５．２ 暗号モジュール試験機関承認申請の手順

「暗号モジュール試験機関承認申請書」（様式 1）（以下「申請書」という。）の必要事項を全て記入し、次に掲げる書類を添付して、権限を持った代表者が署名又は押印した正式なものを、認証機関に提出して下さい。

① 法人格を証明できる書類

② 「暗号モジュール試験機関承認に係る遵守事項の誓約について」（様式 2）

５．３ 秘密保持契約の締結

試験機関は、認証機関と包括的な秘密保持契約を結ばなければなりません。権限を持った代表が署名した正式な「秘密保持契約書」（様式 6）を認証機関に 2 部作成のうえ、認証機関との間で秘密情報の取扱に関して契約を締結して下さい。

５．４ 試行試験の実施

試験機関は、認証機関より、**暗号アルゴリズム実装試験ツール(JCATT)**及び**暗号モジュール試験報告書作成支援ツール(CRYPTIPA)**の貸与を受けます。これらのツールを使用して、試験機関は、試行試験を実施し、**暗号アルゴリズム実装試験報告書**及び**暗号モジュール試験報告書**を認証機関に対して提出しなければなりません。

５．５ 試験機関認定申請及び認定証の受領

試験機関は、認定機関に対して、ASNITE 試験事業者 IT による認定を受けるべく、認定申請を実施しなければなりません。認定機関より、試験機関として認定を受けた場合には、試験機関は、遅滞無く認証機関に対して、認定書の写しを送付しなければなりません。

６．暗号モジュール試験機関の承認

試験機関は、認証機関が、4. の条件を満たしていると判断し、「暗号モジュール試験機関承認書」（様式 7）を発行した場合、「暗号モジュール試験機関承認書」を受領します。また、試験機関は、認証機関が、当該試験機関の情報を、「暗号モジュール試験機関リスト」に登録し、機構のホームページにて公表したことを確認しなければなりません。

７．暗号モジュール試験機関承認書の再発行

試験機関は、「暗号モジュール試験機関承認書再発行申請書」（様式 3）により「暗号モジュール試験機関承認書」の再発行の申請手続を行うことができます。

８．暗号モジュール試験機関の承認の変更

「暗号モジュール試験機関リスト」の情報に変更が発生した場合、試験機関は遅滞無く認証機関に対して「暗号モジュール試験機関承認変更届」（様式 4）を提出しなければなりま

せん。

９．暗号モジュール試験機関の承認の廃止

試験機関は、本制度の試験機関であることを辞退する場合、3 ヶ月前までに「暗号モジュール試験機関承認廃止届」（様式 5）を、認証機関に提出しなければなりません。また、試験機関は、認証機関に対して授与された「暗号モジュール試験機関承認書」を遅滞無く返納しなければなりません。

１０．暗号モジュール試験機関の承認の取消

次の事項が発生した場合、認証機関は、当該試験機関に対して、その旨の通知を行います。試験機関は、当該通知の内容に関し、認証機関に対して弁明の機会が与えられます。当該弁明を斟酌しても、その疑義が解消されないと認証機関が判断した場合、試験機関は、認証機関に対して授与された「暗号モジュール試験機関承認書」を遅滞無く返納しなければなりません。

- 試験機関が ASNITE 試験事業者 IT に適合しないとして認定機関によって認定が取消された場合
- 認証機関から貸与されたツール類の改竄、第三者への開示又は譲渡をしたと認められる場合

１１．本規程の変更による処置

試験機関は、認証機関から本規程が変更された旨の通知を受けた場合、妥当な期間内にその要求事項に適合するために必要な業務手順の変更等の処置を完了し、認証機関に当該処置の完了を通知しなければなりません。

附　則（平成 19 年 5 月 9 日　2007 情総第 20 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 117 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 11 月 4 日　2009 情総第 96 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 30 年 6 月 29 日　2018 情総第 182 号・一部改正）

この規程は、平成 30 年 7 月 1 日から施行する。

暗号モジュール試験機関承認手続に係る様式集

(注) 様式については、申請及び管理等の便宜に資するために
変更することがあり得ます。 最新の様式については、
認証機関の Web ページで公表します。

様式 1

暗号モジュール試験機関承認申請書

年　月　日

独立行政法人 情報処理推進機構
理事長　殿

住所

申請者の名称　　印

代表者名　　印

「暗号モジュール試験機関承認申請手続等に関する規程」(CBM-03) に基づき、別紙「暗号モジュール試験機関承認に係る遵守事項の誓約について」(様式 2)に誓約し、下記のとおり申請します。

＜申請区分＞ 暗号モジュール試験機関承認申請
＜「暗号モジュール試験機関リスト」に掲載する暗号モジュール試験機関の情報＞ ふりがな： 試験機関名： 郵便番号： 所在地： 試験機関責任者の役職名及び氏名： 試験機関責任者のメールアドレス： 電話番号： FAX 番号：
＜関連する事務所＞ 名称及び所在地：

以下は記入しないでください。

受付番号	

様式 2

暗号モジュール試験機関承認に係る遵守事項の誓約について

年　月　日

独立行政法人 情報処理推進機構
理事長　殿

住所

申請者の名称　　印

代表者名　　印

暗号モジュール試験及び認証制度による暗号モジュール試験機関 (以下「試験機関」という。) の承認の申請を行うに当たっては、「暗号モジュール試験機関承認申請手続等に関する規程」 (CBM-03) に基づき、以下の事項に従うことを誓約します。また、暗号モジュール試験機関承認取得後も、以下の事項に継続して従うことを誓約します。

1. 独立行政法人 情報処理推進機構 (以下「機構」という。) が定める「暗号モジュール試験及び認証制度の基本規程」及び「暗号モジュール試験機関承認申請手続等に関する規程」を常に遵守します。
2. 暗号モジュール試験機関の承認を取消された場合には、速やかに「暗号モジュール試験機関承認書」を認証機関に返納します。
3. 認証機関から貸与されたツール類の改竄、第三者への開示、譲渡はいたしません。
4. 暗号モジュール試験の瑕疵を理由に申請者から損害賠償請求を受けた場合、機構の行った暗号モジュール認証に故意又は重過失がない限り、機構には一切の責任を問いません。
5. 暗号モジュール試験の瑕疵を理由に申請者以外の暗号モジュールの使用者等から損害賠償請求を受けた場合、機構には一切の責任を問いません。

以上

様式 3

暗号モジュール試験機関承認書再発行申請書

年　月　日

独立行政法人 情報処理推進機構
理事長　殿

住所

申請者の名称　　印

代表者名　　印

「暗号モジュール試験機関承認申請手続等に関する規程」(CBM-03) に基づき、下記の理由により、「暗号モジュール試験機関承認書」の再発行を申請します。

＜申請区分＞ 暗号モジュール試験機関承認書の再発行
＜暗号モジュール試験機関の情報＞ 試験機関名： 所在地：
＜再発行申請理由＞

以下は記入しないでください。

受付日	
再発行承認者	
再発行承認日	

様式 4

暗号モジュール試験機関承認変更届

年　月　日

独立行政法人 情報処理推進機構
理事長　殿

住所

申請者の名称　　印

代表者名　　印

「暗号モジュール試験機関承認申請手続等に関する規程」(CBM-03) に基づき、暗号モジュール試験機関の承認内容を変更したいので、下記の通り届け出ます。

＜届出区分＞ 暗号モジュール試験機関承認内容の変更
＜「暗号モジュール試験機関リスト」に掲載する暗号モジュール試験機関の情報＞ ふりがな： 試験機関名： 郵便番号： 所在地： 試験機関責任者の役職名及び氏名： 試験機関責任者のメールアドレス： 電話番号： FAX 番号：
＜関連する事務所＞ 名称及び所在地：
＜変更理由＞

注：変更された部分に下線を引いて下さい。

以下は記入しないでください。

受付日	
変更確認者	
変更日	

様式 5

暗号モジュール試験機関承認廃止届

年　月　日

独立行政法人 情報処理推進機構
理事長　殿

住所

申請者の名称　　印

代表者名　　印

「暗号モジュール試験機関承認申請手続等に関する規程」(CBM-03) に基づき、下記の理由により、暗号モジュール試験及び認証制度の暗号モジュール試験機関であることを辞退します。

＜届出区分＞ 暗号モジュール試験機関承認の廃止
＜暗号モジュール試験機関の情報＞ 試験機関名： 所在地：
＜廃止理由＞
＜廃止期日＞ 年　月　日

以下は記入しないでください。

受付日	
廃止確認者	
廃止日	

様式 6

秘密保持契約書

（申請者）（以下「甲」という。）と、独立行政法人 情報処理推進機構（以下「乙」という。）とは、乙が行う暗号モジュール試験及び認証制度に関連する認証機関の業務その他これに付随する業務（以下「認証業務」という。）のために甲が乙に開示する甲の秘密情報の取扱に関し、次のとおり契約を締結する。

（目的）

第 1 条　本契約書は、乙が認証業務を行うにあたり、甲が乙に開示する、又は乙が知ることのある甲の秘密情報の取扱を定めることを目的とする。

（秘密保持義務）

第 2 条　乙は、次項において定義する秘密情報について、善良なる管理者の注意をもってその秘密を保持するものとし、事前の書面による甲の承諾を得ることなく、複製及び第三者への開示をしてはならない。

2　本契約書において秘密情報とは、認証業務に関連して甲が乙に開示する、又は乙が知ることのある甲の技術上又は営業上の情報であって、次に掲げるものをいう。

一　有体物であってその上に秘密である旨が明示された技術資料、図面その他の関係資料等で甲から乙に対して交付されたもの、又は乙が指定する電磁的方法により甲から乙に開示された情報。

二　秘密である旨が告知された上で口頭その他の前号以外の方法によって甲から乙に対して開示された情報であって、当該開示後 30 日以内に書面により具体的に特定された上で秘密である旨が明示されたもの。

3　本条第 1 項及び第 2 項にかかわらず、次の各号のいずれかに該当する情報は本条による秘密保持義務の対象から除外する。

一　甲より開示を受けた時点において既に公知となっているもの。

二　甲より開示を受けた後に乙の故意又は過失によらず公知となったもの。

三　甲より開示を受ける前に乙が自ら知得し、又は正当な権限を有する第三者より秘密保持義務を負うことなく正当な手段により入手していたもの。

四　甲から書面により開示を承諾されたもの。

4　本条第 1 項の規定は、次に掲げる場合には適用されない。但し、乙は、甲に対し開

示した旨を通知するものとする。

一　法令の規定に基づき開示の義務が生じた場合であって、法令で定める範囲で法令で定める者に対して開示を行う場合。

二　官公署からの要請等、乙による開示に正当な理由があるものと乙が合理的に判断した場合であって甲から事前に開示を承諾された場合。

5　乙は、秘密情報を複製、改変又は編集したものについても、秘密情報として扱うものとする。

（秘密情報の使用目的）

第 3 条　乙は、事前の書面による甲の承諾を得ることなく、甲の秘密情報を、認証業務以外の目的に使用してはならないものとする。

（損害賠償）

第 4 条　乙が本契約に定める事項に違反したことにより、乙が通常予見しうる損害を甲が損害を被った場合、乙は甲に生じた損害を賠償する責を負うものとする。但し、前段の場合であっても特別損害及び逸失利益については、乙は何ら責任を負わないものとする。

（本契約書の作成にかかる費用）

第 5 条　本契約書の作成に関連して発生する費用は各当事者において負担する。

（契約の変更）

第 6 条　本契約のいかなる変更も、甲及び乙の権限ある代表者又は代理人が署名した書面によらない限り、効力を有しない。

（完全合意）

第 7 条　本契約は、その作成日現在における対象事項についての甲乙間の合意内容のすべてを規定したものであり、本契約作成日以前に甲乙間でなされた協議内容、合意事項又は一方当事者から相手方に提供された資料、申入れその他の通信と本契約の内容とが相違する場合は、本契約が優先するものとする。

（権利義務等の譲渡禁止)

第 8 条　甲及び乙は、事前の書面による他当事者の承諾を得ることなくして、本契約書に基づく権利若しくは義務又は本契約書上の地位を第三者に譲渡し、又は承継させてはならない。

（有効期間）

第 9 条　本契約は、別途甲乙間で特段の取り決めをしない限り、本契約調印の日より発効し、本認証業務が終了、中止若しくは中断した時から 5 年間が経過した時、又は乙が甲から本件書類の開示を最後に受けた時から 5 年間が経過した時のいずれか早い時点で終了する。

（準拠法）

第 10 条　本契約並びに本契約に基づき又はこれに関連して生じる各本契約当事者の一切の権利及び義務は、日本国の法律に準拠し、それに従い解釈される。

（管轄裁判所）

第 11 条　本契約に関連する訴訟については、東京地方裁判所をもって第一審の専属的合意管轄裁判所とする。

以上、本契約の成立を証するため本書二通を作成し、甲乙記名捺印のうえ各一通を保有する。

年　　月　　日

甲（申請者）

乙　　東京都文京区本駒込二丁目 28 番 8 号
独立行政法人 情報処理推進機構
理事長　　＜理事長名＞

様式 7

暗号モジュール試験機関
承認書

暗号モジュール試験及び認証制度に基づき、適合する暗号モジュール試験機関として、下記の通り承認する。

年　　月　　日

独立行政法人 情報処理推進機構

理事長名　　印

記

承認番号

承認された事業所の名称

所在地

承認の範囲　　暗号モジュール試験　セキュリティレベル 1
暗号モジュール試験　セキュリティレベル 2
暗号モジュール試験　セキュリティレベル 3
暗号モジュール試験　セキュリティレベル 4

以上

【変更履歴】

日付	摘要
年　　月　　日	新規発行

改訂履歴

識別番号	CBM-03

改訂年月日	作成者・承認者	改訂内容
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 11 月 2 日	櫻井・仲田	一部改正
平成 30 年 6 月 29 日	櫻井・江口	一部改正