暗号モジュール認証業務取扱手順

令和 2 年 11 月 9 日

IPA

CBM-01-A
Certification Body Management System

独立行政法人　情報処理推進機構

目次

暗号モジュール認証業務取扱手順

制定 平成 18 年 10 月 30 日
最終改正 令和 2 年 11 月 9 日 2020 情セ技第 1044 号 一部改正

1. 目的

本手順は、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***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***（CBM-01）（以下「***業務運営規程***」という。）に基づき、暗号モジュール認証を行う業務（以下「***認証業務***」という。）を適正に実施するために、必要な業務手順を定めることを目的とする。

2. 用語及び定義

本手順で使用する用語及び定義は、***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及び定義による。

3. 認証機関の認証業務実施のための準備

3.1 暗号モジュール認証等に関する情報

（1） 認証機関は、暗号モジュール試験機関（以下「試験機関」という。）及び申請者が、暗号モジュール認証及び暗号アルゴリズム確認（以下「暗号モジュール認証等」という。）の申請等を行うために必要な情報を、機構のホームページに公開する。

（2） 認証機関は、暗号モジュール認証等に係る規程又は手続に関して変更を行う場合は、13.1 に従って行う。

（3） 認証機関は、暗号モジュール認証のための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。）に関して変更を行う場合は、13.2 に従って行う。

3.2 認証業務実施のための準備

（1） 暗号モジュール業務担当者（以下「業務担当者」という。）は、「暗号モジュール認証申請受付簿」（様式 1-1）（以下「認証受付簿」という。）、「暗号アルゴリズム確認申請受付簿」（様式 1-2）（以下「確認受付簿」という。）、「暗号モジュール認証進捗状況管理表」（様式 2-1）（以下「認証管理表」という。）及び「暗号アルゴリズム確認進捗状況管理表」（様式 2-2）（以下「確認管理表」という。）を準備して、業務担当者は認証業務を行う。また、暗号モジュール認証案件に、プロジェクトコードを決定し、プロ

ジェクトコードを記したファイルを作成する。そのファイルを決められた書棚に保管する。

(2) 各業務の担当者は、各業務が終了した場合、その日付と、担当者の氏名を認証管理表に、記入することとする。

4. 申請受付業務取扱

4.1 暗号モジュール認証申請の受付

(1) 業務担当者は、暗号モジュール認証に係る申請の受付を行う。暗号モジュール認証申請受付時に申請内容の確認を行う。

(2) 申請時に受領する書類は次のものがある。次の書類は、各 1 部必要である。

① 暗号モジュール認証申請書（***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。）様式 1-1）

② 法人格を証明できる書類

③ 同意書（***認証申請手続規程***様式 2）

その他の書類を受領したときは、業務担当者は、認証管理表に、文書名を記入する。業務担当者は、受領書類の確認を行い、不備が無い場合は、認証管理表の摘要欄の[適]に〇を付ける。不備がある場合は、申請者に対して、1 週間を目途に期限を定めて必要な書類の再提出を指示し、摘要欄の[不適]に再提出指示日を記入する。受領書類の不備が解消するまで、確認日の記入は行わない。

(3) 業務担当者は、申請の受付可否について、必要に応じて、技術管理者及びマネジメントシステム責任者と相談する。必要がある場合には、技術管理者は、運営審議委員会に当該申請の受付可否について付議する。次のいずれかに該当する場合は、当該申請の受付を却下できるものとする。なお、認証機関として受付を却下する場合は、申請書類一式を返却する。

① 本制度での暗号モジュール認証実績又は暗号アルゴリズム確認実績がない場合であって、事前相談をしていない場合

② 期限までに必要な書類の再提出がなされない場合

③ 申請者から特別な負担を求められた場合

④ 運営審議委員会にて、受付受理が不適当、又は受付不受理が相当との助言がなされた場合

⑤ 適切な試験作業又は認証作業が実施できないと見込まれる場合

適切に実施できないと見込まれる場合の例として次を含むが、これらに限定されるものではない。

一 独立性及び公平性を確保できないと見込まれる場合

一 対象の暗号モジュールの試験に必要な力量及び能力を試験機関が欠いてい

ると認証機関が判断した場合

一 対象の暗号モジュールの認証に必要な力量及び能力を認証機関が欠いている場合

一 本制度の認証要求事項を満たしていないことが明らかな場合

⑥ 認証要求事項への不適合が、過去に複数回指摘された実績がある申請者の場合

⑦ 認証済暗号モジュールに係る届出、又は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。）としての変更の届出を怠った申請者の場合（他の類似の認証制度と比較して公平に届出を行っていない場合も含む）

⑧ 認証済暗号モジュール又は確認済暗号アルゴリズム実装への不適切な取り扱いがあった場合

⑨ 天災その他やむを得ない事由がある場合

(4) 業務担当者は、提出された「暗号モジュール認証申請書」の受付番号欄に、「M」の文字、「西暦年月」、「ハイフン」及び「2 桁の月別通し番号」で構成される受付番号を記入する。

【受付番号例】: M200807-01

(5) 業務担当者は、認証受付簿 に、受付番号、受付年月日、認証申請区分（新規）、暗号モジュール名称、バージョン、申請者名称、連絡担当者名及び電話番号を記入する。

(6) 業務担当者は、認証管理表に、受付番号、申請者名称、連絡担当者名、電話番号、暗号モジュール名称、バージョンを記入する。

(7) 業務担当者は、申請者及び試験機関に受付番号および受領した書類のリストを電子メールにて連絡する。

4.2 暗号アルゴリズム確認申請の受付

(1) 業務担当者は、暗号アルゴリズム確認に係る申請の受付を行う。暗号アルゴリズム確認申請受付時に申請内容の確認を行う。

(2) 申請時に受領する書類は次のものがある。次の書類は、各 1 部必要である。

① 暗号アルゴリズム確認申請書（***認証申請手続規程***様式 1-2）

② 法人格を証明できる書類

③ 同意書（***認証申請手続規程***様式 2）

その他の書類を受領したときは、業務担当者は、確認管理表に、文書名を記入する。業務担当者は、受領書類の確認を行い、不備が無い場合は、確認管理表の摘要欄の[適]に〇を付ける。不備がある場合は、申請者に対して、1 週間を目途に期限を定めて必要な書類の再提出を指示し、摘要欄の[不適]に再提出指示日を記入する。受領書類の不備が解消するまで、確認日の記入は行わない。

受領書類の不備の例として、暗号アルゴリズム確認申請書に記載されている暗号アル

ゴリズムのみでは実装が完結しない場合が挙げられる。

(3) 業務担当者は、申請の受付可否について、必要に応じて、技術管理者及びマネジメントシステム責任者と相談する。必要がある場合には、技術管理者は、運営審議委員会に受付可否について付議する。次のいずれかに該当する場合は、当該申請の受付を却下できるものとする。なお、認証機関として受付を却下する場合は、申請書類一式を返却する。

① 本制度での暗号モジュール認証実績又は暗号アルゴリズム確認実績がない場合であって、事前相談をしていない場合
② 期限までに必要な書類の再提出がなされない場合
③ 申請者から特別な負担を求められた場合
④ 運営審議委員会にて、受付受理が不適当、又は受付不受理が相当との助言がなされた場合
⑤ 認証要求事項への不適合が、過去に複数回指摘された実績がある申請者の場合
⑥ 確認済暗号アルゴリズム実装に係る届出、又は認証被許諾者としての変更の届出を怠った申請者の場合（他の類似の認証制度と比較して公平に届出を行っていない場合も含む）
⑦ 認証済暗号モジュール又は確認済暗号アルゴリズム実装への不適切な取り扱いがあった場合
⑧ 天災その他やむを得ない事由がある場合

(4) 業務担当者は、提出された「暗号アルゴリズム確認申請書」の受付番号欄に、「A」の文字、「西暦年月」、「ハイフン」及び「2 桁の月別通し番号」で構成される受付番号を記入する。

【受付番号例】: A200902-01

(5) 業務担当者は、確認受付簿 に、受付番号、受付年月日、暗号モジュール名称、バージョン、申請者名称、連絡担当者名及び電話番号を記入する。

(6) 業務担当者は、確認管理表に、受付番号、申請者名称、連絡担当者名、電話番号、暗号モジュール名称、バージョンを記入する。

(7) 業務担当者は、申請者及び試験機関に受付番号および受領した書類のリストを電子メールにて連絡する。

4.3 秘密保持契約の締結

(1) 業務担当者は、申請者の要請に基づき、申請責任者が押印又は署名した「秘密保持契約書」（***認証申請手続規程***様式 9）を 2 部受領し、秘密情報の取扱に関して、申請者との間で契約締結の手続を行う。業務担当者は、秘密保持契約を締結する場合、認証管理表の摘要欄の[有]に○を付け、原議番号を記入する。秘密保持契約を締結しない場合、摘要欄の[無]に○を付ける。当該秘密保持契約は、統括責任者の決裁を受けて、

機構の理事長名をもって締結する。秘密保持契約の締結は、暗号モジュール認証申請受付日をもって行う。

(2) 業務担当者は、「覚書」を締結する場合、認証管理表の摘要欄の[有]に○を付け、原議番号を記入する。「覚書」を締結しない場合、摘要欄の[無]に○を付ける。

(3) 業務管理者は、「秘密保持契約書」の 2 部のうち 1 部を申請者に送付し、もう 1 部をファイルに綴じ、決められた書棚に保管する。「覚書」がある場合も同様に行う。業務管理者は、認証管理表の摘要欄に保管日を記入する。

4.4 申請料

(1) 業務担当者は、申請手数料（***認証申請手続規程***別表）及び旅費等の必要経費を合計した申請料を徴収するために、機構の財務部へ申請受付の連絡を行う。申請料の請求は、財務部より申請者に請求書を送付して行う。申請料を免除するなど、特段の理由がある場合、業務担当者は、その理由を認証管理表又は確認管理票の摘要欄に記入する。

(2) 旅費等の必要経費に関しては、申請を受け付けた際に、必要性を勘案し、申請者との協議のうえで決定する。

(3) 業務担当者は、暗号モジュール認証等の業務を開始する前に、認証管理表又は確認管理票に申請料の免除等を行う理由が記載されている場合を除いて、申請料が過不足なく納付期限までに納付されたか財務部に問い合わせを行う。申請料が納付期限までに納付されなかった場合、業務担当者は、その事実を認証管理表又は確認管理票の摘要欄に記入し、11.3 に従って申請取下げを行う。

4.5 暗号モジュール認証要員の選任

(1) 暗号モジュール技術管理者（以下「技術管理者」という。）は、暗号モジュール認証申請書又は暗号アルゴリズム確認申請書を精査したうえで、申請者に対して制度の目的や申請者の権利及び義務を説明し、理解の違いが解消されていることを確認する。

(2) 技術管理者は、中立性・公平性などを総合的に勘案し、申請の受付を行った暗号モジュールの認証業務を行う担当の暗号モジュール認証要員（以下「認証要員」という。）を選任する。技術管理者は、認証管理表又は確認管理表の摘要欄に、選任した認証要員名を記入する。

(3) 技術管理者は、認証要員の氏名を試験機関に対して電子メールにて連絡する。

(4) 技術管理者は、「暗号モジュール認証申請受理通知書」（様式 3-1）又は「暗号アルゴリズム確認申請受理通知書」（様式 3-2）を作成し、技術管理者の印を押捺する。

(5) 業務担当者は、「暗号モジュール認証申請受理通知書」（様式 3-1）又は「暗号アルゴリズム確認申請受理通知書」（様式 3-2）を申請者へ配達の記録が残る方法で送付する。

4.6 運営審議委員会での受付可否の検討

*制度基本規程*の 2.2.1 に該当しない法人等からの申請、サプライチェーン等におけるサイバーセキュリティに影響する可能性がある等の疑義がある法人等からの申請、又は認証済暗号モジュールや確認済暗号アルゴリズムを不適切に取り扱う法人等からの申請等の場合には、原則として、運営審議委員会にて申請の受付可否について検討し、助言を得なければならない。その際、輸出貿易管理令、申請者についての国際的なルールの違反の有無、ワッセナーアレンジメント加盟国がそれぞれ定める個別の輸出許可を求める団体・個人のリスト等への掲載有無などの情報、申請者への第三国の政府等からの干渉の可能性、及び苦情又は異議申し立てへの対応等を参考に、総合的に判断できるように努めなければならない。

5. 暗号モジュール認証等の業務取扱

5.1 暗号アルゴリズム確認業務の実施

(1) 業務担当者は、「暗号アルゴリズム実装試験報告書」が試験機関から提出された場合、認証管理表又は確認管理表に、受理した日付及び業務担当者名を記入する。業務担当者は、認証要員に、「暗号アルゴリズム実装試験報告書」を渡す。また、受理した旨を、試験機関に対して電子メールにて伝える。

(2) 認証要員は、暗号アルゴリズム確認業務の継続について、必要に応じて、技術管理者及びマネジメントシステム責任者と相談する。サプライチェーン等におけるサイバーセキュリティに影響する可能性がある等の疑義が生じた場合には、必要に応じて、技術管理者は、運営審議委員会に確認業務の継続可否又は確認の許諾可否について付議し、委員会の助言を参考に当該確認業務の継続拒否、確認の許諾拒否又は取消等ができるものとする。なお、確認の取消等を行う場合には、10.に従って行う。

(3) 認証要員は、認証管理表の 4.4 に申請料納付日の記載がない場合、申請手数料の免除等を行う理由が記載されている場合を除いて、当該申請にかかる申請料が入金されたかの確認を業務担当者に指示ずる。指示された業務担当者は、機構の財務部へ確認する。

(4) (1) で受理した「暗号アルゴリズム実装試験報告書」が、既に受理済みの「暗号アルゴリズム実装試験報告書」の差し替え版の場合、又は「暗号アルゴリズム実装試験報告書」に対する補足が、試験機関から提出された場合、業務担当者は、既に***暗号アルゴリズム確認書***（***業務運営規程***様式 1）を発行しているかどうかを確認する。

(5) 認証要員は、「暗号アルゴリズム実装試験報告書」に記述に関して、次の調査を行う。

① 記述に齟齬が無いこと

② 動作環境に問題が無いこと

③ 使用している暗号アルゴリズム実装試験ツール JCATT のバージョンが最新版であること

④ 試験結果が正当であること

「暗号アルゴリズム実装試験報告書」の調査を行い、問題が無い場合、認証管理表又は確認管理表の摘要欄の[適]に○を付ける。認証要員は、***暗号アルゴリズム確認書***を作成する。認証要員は、技術管理者に「暗号アルゴリズム実装試験報告書」の調査が終了し、「暗号アルゴリズム実装試験報告書」に問題が無かったことを報告する。問題がある場合は、試験機関に対して、1 週間を目途に期限を定めて「暗号アルゴリズム実装試験報告書」の再提出を指示し、摘要欄の[不適]に再提出指示日を記入する。

(6) 技術管理者は、上記の報告を受け、最終的な判断を行い、問題がない場合は暗号アルゴリズム確認の決裁を行う。決裁する場合、認証管理表又は確認管理表の摘要欄の[適]に○を付け、業務担当者に対して、***暗号アルゴリズム確認書***等の作成を指示する。問題がある場合、摘要欄の[否]に差戻日を記入し、認証要員に（4）の再調査を行うように差戻す。

(7) 業務担当者は、***暗号アルゴリズム確認書***に関して「施行あり」にて起案し、認証管理表の摘要欄に原議番号を記入する。

(8) 認証機関は、***暗号アルゴリズム確認書***を発行する。業務担当者は、写しをファイルに綴じ決められた書棚に保管する。

(9) （4）で既に***暗号アルゴリズム確認書***を発行している場合、業務担当者は、当該暗号アルゴリズムに関する***暗号アルゴリズム確認書***を回収する。

(10) 業務担当者は、***暗号アルゴリズム確認書***を試験機関に、配達の記録が残る方法で送付する。

(11) 業務担当者は、上記文書を試験機関に対して発送した旨を、申請者に対して電子メールにて伝える。

(12) 業務担当者は、暗号アルゴリズム毎に作成された「暗号アルゴリズム確認登録簿」に、暗号アルゴリズム確認の情報を申請者の情報等と共にその都度登録する。

(13) 業務担当者は、「暗号アルゴリズム確認登録簿」に登録された内容を、週に 1 度、週末を基本として公開する。当該暗号アルゴリズム実装が利用者に未だ提供されていない場合、公開日時について、申請者の要望を考慮する。

5.2 暗号モジュール認証業務の実施

(1) 業務担当者は、「暗号モジュール試験報告書」が試験機関から提出された場合、認証管理表に、受理した日付及び業務担当者名を記入する。業務担当者は、認証要員に、「暗号モジュール試験報告書」を渡す。また、受理した旨を、試験機関に対して電子メールにて伝える。

(2) 認証要員は、暗号モジュール認証業務の継続について、必要に応じて、技術管理者及びマネジメントシステム責任者と相談する。サプライチェーン等におけるサイバーセキュリティに影響する可能性がある等の疑義が生じた場合には、必要に応じて、技術

管理者は、運営審議委員会に認証業務の継続可否又は認証の許諾可否について付議し、委員会の助言を参考に当該認証業務の継続拒否、認証の許諾拒否又は取消等ができるものとする。なお、認証の取消等を行う場合には、10.に従って行う。

(3) 認証要員は、「暗号モジュール試験報告書」に記述に関して、次の調査を行う。

① 記述に齟齬が無いこと（申請者の同意の署名があることも調査する。）

② 動作環境に問題が無いこと

③ 使用している報告書作成支援ツール CRYPTIPA のバージョンが最新版であること

④ 各章に対して、試験結果が正当であること

「暗号モジュール試験報告書」の調査を行い、問題が無い場合、認証管理表の摘要欄の[適]に○を付ける。問題がある場合は、試験機関に対して、1 週間を目途に期限を定めて質問を行い、回答を求める。摘要欄の[不適]に質問の識別番号を記入する。認証要員は、この回答を精査し、さらに疑問がある場合は、試験機関に対して再質問を行う。この作業を、疑問が無くなるまで繰り返す。尚、質問に使用する様式は、「暗号モジュール所見報告書」（***認証申請手続規程***様式 10）を準用する。認証要員は、「暗号モジュール試験報告書」の調査が終了した場合、***暗号モジュール認証書***（***業務運営規程***様式 2-1）及び***暗号モジュール認証報告書***（***業務運営規程***様式 2-2）を作成する。認証要員は、技術管理者に「暗号モジュール試験報告書」に問題が無かったことを報告する。

(4) 技術管理者は、上記の報告を受け、最終的な判断を行い、暗号モジュール認証の決裁を行う。決裁する場合、認証管理表の摘要欄の[適]に○を付け、業務担当者に対して、***暗号モジュール認証書***等の起案を指示する。決裁しない場合、摘要欄の[否]に差戻日を記入し、認証要員に（3）の再調査を行うように差戻す。

(5) 業務担当者は、***暗号モジュール認証書***及び***暗号モジュール認証報告書***に関して「施行あり」にて起案し、認証管理表の摘要欄に原議番号を記入する。

(6) 認証機関は、***暗号モジュール認証書***及び***暗号モジュール認証報告書***を発行する。業務担当者は、写しをファイルに綴じ決められた書棚に保管する。

(7) 業務担当者は、***暗号モジュール認証書***及び***暗号モジュール認証報告書***を申請者に、配達の記録が残る方法で送付する。

(8) 業務担当者は、上記文書を申請者に対して発送した旨を、申請者に対して電子メールにて伝える。

(9) 業務担当者は、「暗号モジュール認証製品リスト」に、暗号モジュール認証の情報を「セキュリティポリシ」及び申請者の情報等と共に登録する。

(10) 業務担当者は、「暗号モジュール認証製品リスト」を公開する。当該暗号モジュールが暗号モジュールの利用者に未だ提供されていない場合、公開日時について、申請者の要望を考慮する。

5.3 解釈等照会書の処理

(1) 暗号モジュール試験におけるセキュリティ要件等の解釈を照会するための「解釈等照会書」が、試験機関より提出された場合は、技術管理者は、当該「解釈等照会書」を受理し、認証管理表に、受理した日付及び識別番号を記入する。受理しない場合は、その理由を付し返却する。尚、「解釈等照会書」の様式は、*認証申請手続規程*様式 10 を準用する。

(2) 技術管理者及び認証要員は、会議を開き、「解釈等照会書」の内容を確認し、速やかに問題点等に対する対処方法を検討し、その暗号モジュール試験に関する暫定措置を策定する。

(3) 技術管理者は、暫定措置を「解釈等照会書」に記入し、試験機関に送付する。

(4) 技術管理者は、本制度の技術審議委員会において「解釈等照会書」の問題点の解決を図り、セキュリティ要件等の運用・解釈の提示のみで問題を解決できるもの及び本制度の運営等に関するガイダンスについては、「JCMVP 運用ガイダンス」を策定し公開する。運用ガイダンスの策定及び公開の手順については、6.に従って記述する。

(5) 技術管理者は、必要に応じ、関連標準化団体、専門委員会又は他の適切な機関と歩調をとって、セキュリティ要件等を変更する手続きをとる。

5.4 運営審議委員会での認証の許諾等についての検討

サプライチェーン等におけるサイバーセキュリティに影響する可能性がある等の疑義が生じた場合には、原則として、運営審議委員会にて認証業務の継続可否又は認証の許諾可否について検討し、助言を得なければならない。その際、輸出貿易管理令、申請者についての国際的なルールの違反の有無、ワッセナーアレンジメント加盟国がそれぞれ定める個別の輸出許可を求める団体・個人のリスト等への掲載有無などの情報、及び申請者への第三国の政府等からの干渉の可能性等を参考に、総合的に判断できるように努めなければならない。

6. 運用ガイダンスの策定及び公開

認証機関は、本制度の運営等に関するガイダンス又は*制度基本規程*の*附属書 A* に定めた*セキュリティ要件等*の運用・解釈に関わるガイダンスを発行する場合に、「*JCMVP 運用ガイダンス*」を策定し公開する。

6.1 運用ガイダンスの策定

(1) 運用ガイダンスを策定すべき事象が発生した場合、技術管理者は、自ら原案を作成するか又は原案作成を担当する認証要員を選任する。選任された場合、認証要員は、原

案を作成する。

(2) 技術管理者は、必要に応じて技術審議委員会に原案を諮問し、統括責任者に対する答申を得る。

(3) 統括責任者は、技術審議委員会の答申がある場合はそれを踏まえて、原案に対する決裁を行い、認証機関として「***JCMVP 運用ガイダンス***」を発行する。

6.2 運用ガイダンスの公開

(1) 業務担当者は、発行された「***JCMVP 運用ガイダンス***」を、機構のホームページ上で公開する。

7. 認証済暗号モジュール認証の再認証

認証済暗号モジュール認証の再認証は、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適用する。再認証の詳細については、「JCMVP 運用ガイダンス」に定める。なお、後続暗号モジュールに対する修正が最新の暗号モジュールセキュリティ要件に関連した事項に影響を与えない場合には、保証継続を申請することができる。保証継続については、8.に従って行う。

7.1 再認証業務実施のための準備

(1) 業務担当者は、認証受付簿及び「再認証進捗状況管理表」（様式 4-1）（以下「再認証管理表」という。）を準備する。また、再認証案件に、プロジェクトコードを決定し、プロジェクトコードを記したファイルを作成する。そのファイルを決められた書棚に保管する。

(2) 各業務の担当者は、各業務が終了した場合、その日付と、担当者の氏名を再認証管理表に記入することとする。

7.2 再認証の受付

(1) 業務担当者は、再認証に係る申請の受付を行う。再認証に係る申請受付時に申請内容の確認を行う。

(2) 申請時に受領する書類は次のものがある。次の書類は、各 1 部必要である。

① 「暗号モジュール認証申請書」（***認証申請手続規程***様式 1-1）

② 「同意書」（***認証申請手続規程***様式 2）

上記の①及び②の書類に加え、試験機関が作成した次の書類が各 1 部必要である。

a) 修正が「暗号モジュール試験報告書」の 30%以下のアサーションしか影響を与えない場合：

③ 変更箇所に関連する「暗号モジュール試験報告書」

b）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場合：

④ 「物理的変更分析報告書」（フリーフォーマット）

⑤ 変更箇所に関連する「物理的セキュリティ試験報告書」（フリーフォーマット）

上記以外の書類を受領したときは、業務担当者は、再認証管理表に、文書名を記入する。業務担当者は、受領書類の確認を行い、不備が無い場合は、再認証管理表の摘要欄の[適]に〇を付ける。不備がある場合は、再認証申請者に対して、1 週間を目途に期限を定めて必要な書類の再提出を指示し、摘要欄の[不適]に再提出指示日を記入する。受領書類の不備が解消するまで、確認日の記入は行わない。

(3) 業務担当者は、申請の受付可否について、必要に応じて、技術管理者及びマネジメントシステム責任者と相談する。必要がある場合には、技術管理者は、運営審議委員会に当該申請の受付可否について付議する。

(4) 業務担当者は、提出された「暗号モジュール認証申請書」の受付番号欄に、「S」の文字、「西暦年月」、「ハイフン」及び「2 桁の月別通し番号」で構成される受付番号を記入する。

【受付番号例】: S200807-01

(5) 業務担当者は、認証受付簿に、受付番号、受付年月日、認証申請区分（再）、暗号モジュール名称、バージョン、再認証申請者名称、連絡担当者名及び電話番号を記入する。

(6) 業務担当者は、再認証管理表に、受付番号、再認証申請者名称、連絡担当者名、電話番号、暗号モジュール名称、バージョンを記入する。

(7) 業務担当者は、再認証申請者及び試験機関に受付番号及び受領した書類のリストを電子メールにて連絡する。

7.3 再認証に伴う秘密保持契約の締結

認証機関は、再認証申請者の要請に応じて、再認証に伴う秘密保持契約の締結を行う。その際の手順は、4.3 と同様とする。

7.4 再認証に伴う申請料

認証機関は、再認証申請者に対して再認証に伴う申請料の請求を行う。その際の手順は、4.4 と同様とする。

7.5 再認証に伴う暗号モジュール認証要員の選任

認証機関は、再認証に伴う暗号モジュール認証要員の選任を行う。その際の手順は、4.5 と同様とする。

7.6 再認証に伴う暗号アルゴリズム確認業務の実施

認証機関は、必要に応じて、再認証に伴う暗号アルゴリズム確認業務の実施を行う。その際の手順は、5.1 と同様とする。

7.7 再認証に伴う暗号モジュール認証業務の実施

（1）a）修正が「暗号モジュール試験報告書」の 30%以下のアサーションしか影響を与えない場合：

認証要員は、変更箇所に関連する「暗号モジュール試験報告書」の記述に関して、次の調査を行う。

① 変更点に関する記述があること

② 最新の暗号モジュールセキュリティ要件、暗号モジュール試験要件及び「*JCMVP 運用ガイダンス*」が適用されていること

③ 記述に齟齬が無いこと（再認証申請者の同意の署名があることも調査する。）

④ 動作環境に問題が無いこと

⑤ 使用している報告書作成支援ツール CRYPTIPA のバージョンが最新版であること

⑥ 各章に対して、試験結果が正当であること

b）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場合：

認証要員は、「物理的変更分析報告書」及び変更箇所に関連する「物理的セキュリティ試験報告書」の記述に関して、次の調査を行う。

① 変更点に関する記述があること

② 最新の暗号モジュールセキュリティ要件、暗号モジュール試験要件及び「*JCMVP 運用ガイダンス*」が適用されていること

③ 記述に齟齬が無いこと

④ 物理的変更のみで、動作に影響が無かったことを確認する試験機関の分析が正当であること

⑤ 変更された物理的囲いが依然として同じ物理的保護特性を保持していることを確認する試験が、試験機関により行われており、その試験結果が正当であること

認証要員は、上記の調査を行い、問題が無い場合、再認証管理表の摘要欄の[適]に○を付ける。問題がある場合は、試験機関に対して、2 週間を目途に期限を定めて内容確認を行い、回答を求める。摘要欄の[不適]に質問の識別番号を記入する。認証要員は、この回答を精査し、さらに疑問がある場合は、試験機関に対して再度内容確認を行う。この作業を、疑問が無くなるまで繰り返す。尚、内容確認に使用する様式は、

「暗号モジュール所見報告書」（*認証申請手続規程*様式 10）を準用する。

(2) 認証要員は、上記の調査が終了した場合、技術管理者に「暗号モジュール試験報告書」、又は「物理的変更分析報告書」及び「物理的セキュリティ試験報告書」に問題が無かったことを報告する。また、a）の場合、認証要員は、***暗号モジュール認証書***及び***暗号モジュール認証報告書***を作成する。

(3) 技術管理者は、上記の報告を受け、最終的な判断を行い、問題がない場合は暗号モジュール認証再認証の決裁を行う。決裁する場合、再認証管理表の摘要欄の[適]に○を付け、業務担当者に対して、上記の a）の場合は（4）以降の手順の実施を指示し、上記の b）の場合は「物理的変更分析報告書」に決裁した旨の裏書を施し、（4）以降の手順の実施を指示する。問題がある場合、摘要欄の[否]に差戻日を記入し、認証要員に（1）の再調査を行うように差戻す。

(4) 業務担当者は、***暗号モジュール認証書***及び***暗号モジュール認証報告書***に関して「施行あり」にて起案し、再認証管理表の摘要欄に原議番号を記入する。

(5) 認証機関は、上記の a）の場合は、***暗号モジュール認証書***及び***暗号モジュール認証報告書***を発行する。業務担当者は、それらの写しをファイルに綴じ決められた書棚に保管する。上記の b）の場合は、業務担当者は、決裁した旨の裏書を施した「物理的変更分析報告書」の写し及び「物理的セキュリティ試験報告書」をファイルに綴じ決められた書棚に保管する。

(6) 上記の a）の場合は、業務担当者は、***暗号モジュール認証書***及び***暗号モジュール認証報告書***を再認証申請者に、配達の記録が残る方法で送付する。上記の b）の場合は、業務担当者は、決裁した旨の裏書を施した「物理的変更分析報告書」を再認証申請者に、配達の記録が残る方法で送付する。

(7) 業務担当者は、上記文書を再認証申請者に対して発送した旨を、再認証申請者に対して電子メールにて伝える。

(8) 業務担当者は、「暗号モジュール認証製品リスト」の「セキュリティポリシ」及び再認証申請者の情報等を更新する。

(9) 業務担当者は、「暗号モジュール認証製品リスト」を公開する。

7.8 再認証に伴う解釈等照会書の処理

認証機関は、再認証申請者に対して再認証に伴う解釈等照会書の処理を行う。その際の手順は、5.3 と同様とする。

8. 認証済暗号モジュール認証の保証継続

認証済暗号モジュール認証の保証継続は、後続暗号モジュールに対する修正が、最新の暗号モジュールセキュリティ要件に関連した事項に影響を与えない場合に限り、7.の手続きに

よらずに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適用できる。

8.1 保証継続の事前対応

(1) 認証機関は、保証継続の申請に先立って、保証継続申請者から「暗号モジュール影響分析報告書」をもとに事前レビュー等を依頼された場合、迅速に対応する。

(2) 業務担当者は、保証継続申請者から保証継続の事前レビュー依頼を受け付け、「保証継続事前レビュー受付簿」(様式 4-2)(以下「保証継続管理表」という。)に必要事項を登録し、「事前レビュー受付番号」を採番する。「事前レビュー受付番号」は、「PAC」の文字、「西暦年月」、「ハイフン」及び「2 桁の月別通し番号」で構成される受付番号を記入する。

【受付番号例】: PAC202007-01

(3) 業務担当者は、保証継続申請者に事前レビュー受付番号及び受付日を電子メール等にて連絡する。

(4) 技術管理者は、当該案件の認証時の記録等をもとに暗号モジュール認証要員の選任を行う。

(5) 認証要員は、必要に応じて保証継続申請者に質問を行い「暗号モジュール影響分析報告書」の内容を確認する。「暗号モジュール影響分析報告書」の内容に不足がある場合又は問題がある場合は、保証継続申請者に「暗号モジュール影響分析報告書」の内容の追加、修正等を依頼する。

(6) 保証継続の申請が適当と判断できない又は適当ではないと判断した場合には、認証要員はその結果と理由を保証継続申請者に連絡する。その場合は、保証継続を申請することはできず、再認証又は新規の暗号モジュール認証が必要となる。なお、理由によっては、必要に応じて、認証済暗号モジュールに対するサーベイランスを実施する。サーベイランスを実施する場合には、9.1 に従って行う。

(7) 保証継続の申請が適当と判断した場合は、認証要員は保証継続申請者に保証継続申請が可能である旨連絡する。

8.2 保証継続の申請受付

(1) 業務担当者は、再認証に係る申請の受付を行う。再認証に係る申請受付時に申請内容の確認を行う。

① 「暗号モジュール認証申請書」(***認証申請手続規程***様式 1-1)

② 「同意書」(***認証申請手続規程***様式 2)

③ 事前レビューを受けた「暗号モジュール影響分析報告書」(***認証申請手続規程***様式 11)

上記以外の書類を受領したときは、業務担当者は、再認証管理表に、文書名を記入する。業務担当者は、受領書類の確認を行い、不備が無い場合は、再認証管理表の摘要

欄の[適]に○を付ける。不備がある場合は、保証継続申請者に対して、1 週間を目途に期限を定めて必要な書類の再提出を指示し、摘要欄の[不適]に再提出指示日を記入する。受領書類の不備が解消するまで、確認日の記入は行わない。

(2) 業務担当者は、提出された「暗号モジュール認証申請書」の受付番号欄に、「AC」の文字、「西暦年月」、「ハイフン」及び「2 桁の月別通し番号」で構成される受付番号を記入する。

【受付番号例】: AC202007-01

(3) 業務担当者は、認証受付簿に、受付番号、受付年月日、認証申請区分（保証)、暗号モジュール名称、バージョン、保証継続申請者名称、連絡担当者名及び電話番号を記録する。

(4) 業務担当者は、保証継続管理表に、受付番号、暗号モジュール名称、バージョンを記入する。

(5) 業務担当者は、保証継続申請者に受付番号及び受付日を電子メールにて連絡する。

8.3 保証継続に伴う秘密保持契約の締結

認証機関は、保証継続申請者の要請に応じて、保証継続に伴う秘密保持契約の締結を行う。その際の手順は、4.3 と同様とする。

8.4 保証継続に伴う申請料

認証機関は、保証継続申請者に対して保証継続に伴う申請料の請求を行う。その際の手順は、4.4 と同様とする。

8.5 保証継続に伴う暗号モジュール認証業務の実施

(1) 認証要員は、「暗号モジュール影響分析報告書」に記述に関して、次の調査を行う。

① 変更点に関する記述があること

② 記述に齟齬が無いこと

③ 暗号モジュールセキュリティ要件に関連する事項に影響が無かったことを確認する保証継続申請者の分析が正当であること

認証要員は、上記の調査を行い、問題が無い場合、再認証管理表の摘要欄の[適]に○を付ける。問題がある場合は、保証継続申請者に対して、2 週間を目途に期限を定めて内容確認を行い、回答を求める。摘要欄の[不適]に質問の識別番号を記入する。認証要員は、この回答を精査し、さらに疑問がある場合は、保証継続申請者に対して再度内容確認を行う。この作業を、疑問が無くなるまで繰り返す。尚、内容確認に使用する様式は、「暗号モジュール所見報告書」（***認証申請手引***様式 16）を準用する。

(2) 認証要員は、上記の調査が終了した場合、技術管理者に「暗号モジュール影響分析分析報告書」に問題が無かったことを報告する。また、認証要員は、***暗号モジュール認***

証書（*業務運営規程*様式 2-1）及び「保証継続報告書」（*業務運営規程*様式 2-3）を作成する。

(3) 技術管理者は、上記の報告を受け、最終的な判断を行い、問題がない場合は暗号モジュール認証保証継続の決裁を行う。決裁する場合、再認証管理表の摘要欄の[適]に○を付け、業務担当者に対して、「暗号モジュール影響分析報告書」に決裁した旨の裏書を施し、(4) 以降の手順の実施を指示する。問題がある場合、摘要欄の[否]に差戻日を記入し、認証要員に (1) の再調査を行うように差戻す。

(4) 業務担当者は、*暗号モジュール認証書*及び「保証継続報告書」に関して「施行あり」にて起案し、再認証管理表の摘要欄に原議番号を記入する。

(5) 認証機関は、*暗号モジュール認証書*及び「保証継続報告書」を発行する。業務担当者は、それらの写しをファイルに綴じ決められた書棚に保管する。業務担当者は、決裁した旨の裏書を施した「暗号モジュール影響分析報告書」の写しをファイルに綴じ決められた書棚に保管する。

(6) 業務担当者は、*暗号モジュール認証書*、「保証継続報告書」、及び決裁した旨の裏書を施した「暗号モジュール影響分析報告書」を、保証継続申請者に配達の記録が残る方法で送付する。

(7) 業務担当者は、上記文書を保証継続申請者に対して発送した旨を、保証継続申請者に対して電子メールにて伝える。

(8) 業務担当者は、「暗号モジュール認証製品リスト」の「セキュリティポリシ」及び保証継続申請者の情報等を更新する。

(9) 業務担当者は、「暗号モジュール認証製品リスト」を公開する。

8.6 保証継続に伴う解釈等照会書の処理

認証機関は、保証継続申請者に対して保証継続に伴う解釈等照会書の処理を行う。その際の手順は、5.3 と同様とする。

9. サーベイランス及び再試験

9.1 サーベイランスの実施

(1) マネジメントシステム責任者は、サーベイランスを行うことを決定する。

(2) マネジメントシステム責任者は、技術管理者と協議を行い、サーベイランスを行う 2 名以上の職員又は認証要員を選任し、これらの者の中から 1 名のチームリーダーを指名し、サーベイランスを行わせる。マネジメントシステム責任者は、サーベイランスで調査する項目について、電子メール等の記録が残る方法で指示をする。

(3) チームリーダーは、サーベイランスの目的及び内容等を記した「サーベイランス実施通知書」（様式 17）を作成し、マネジメントシステム責任者の承認を得る。

(4) チームリーダーは、認証書発行後の申請者に対し、「サーベイランス実施通知書」を配達の記録が残る方法で送付し、写しを保管する。

(5) (2) で選任された職員又は認証要員は、指示された項目について速やかにサーベイランスを行い、チームリーダーは、サーベイランスの結果を「サーベイランス実施結果報告書」に取りまとめ、マネジメントシステム責任者に報告する。また、当該暗号モジュールの認証管理表（様式 2-1）の特記事項に、サーベイランスの実施日、サーベイランスの結果概要、サーベイランスを実施した職員又は認証要員の全員の氏名を記入する。

(6) マネジメントシステム責任者は、サーベイランスの結果に基づいて再試験の要否を判定し、再試験を要すると判断したときは、「サーベイランス実施結果報告書」（様式 18）に再試験を要する理由、マネジメントシステム責任者の氏名及び日付を記載し、統括責任者に報告を行い、9.2 に従って行う。

9.2 サーベイランスの結果に基づく再試験

(1) マネジメントシステム責任者は、「再試験指示書」（様式 19）を認証書発行後の申請者に発行し、当該暗号モジュールの認証管理表（様式 2-1）の特記事項に、再試験指示書の発行日、「再試験指示書」を発行した旨及びマネジメントシステム責任者の氏名を記入する。また、業務担当者に対して、当該暗号モジュール認証の一時停止の実施を指示する。

(2) 業務担当者は、認証書発行後の申請者に対し、「再試験指示書」を配達の記録が残る方法で送付する。

(3) 再試験手続きに伴う「暗号モジュール試験報告書」等の受付は、7.の手順を準用する。

10. 暗号モジュール認証等の一時停止及び取消

10.1 暗号モジュール認証等の一時停止手順

(1) マネジメントシステム責任者は、暗号モジュール認証又は暗号アルゴリズム確認に関して、次のいずれかに該当する場合は、暗号モジュール認証等の一時停止手続きを開始する。

① 認証機関が、再試験の実施を決定した場合

② サプライチェーン等におけるサイバーセキュリティに影響する可能性がある等の疑義がある場合で、運営審議委員会への付議が行われることになった場合

③ 認証機関に提起された暗号モジュール認証に係る苦情又は異議申し立ての内容が正当であり、認証被許諾者又は試験機関に是正要求を出した場合

(2) マネジメントシステム責任者は、統括責任者の決裁を受けた後、業務担当者に対して、当該暗号モジュール認証等の一時停止の実施を指示する。

(3) 業務担当者は、当該暗号モジュール認証等の一時停止を機構のホームページに公表する。

(4) (1) の条件が解消された場合、マネジメントシステム責任者は、速やかに業務担当者に対して、当該暗号モジュール認証等の一時停止の解除を指示する。

(5) 業務担当者は、当該暗号モジュール認証等の一時停止解除を機構のホームページに公表する。

10.2 暗号モジュール認証の取消手順

(1) マネジメントシステム責任者は、暗号モジュール認証に関して次のいずれかに該当する場合は、暗号モジュール認証の取消手続きを開始する。

① 認証被許諾者が、9.2 に記載されている再試験の実施を拒否した場合
（認証被許諾者が、暗号モジュール認証の継続を望まない場合も含む）

② 再試験の指示から 1 年以内に再試験が完了しない場合

③ 再試験結果に基づいて***暗号モジュール認証書***の効力を継続することの当否を判定し、効力を継続することが適当でないと認証機関が認めた場合

④ 「同意書」（***認証申請手続規程***様式 2）に違反する事実が認められ、かつ、改善の指示の効果が認められない場合

⑤ 不正な手段により暗号モジュール認証を受けた場合

⑥ サプライチェーン等におけるサイバーセキュリティに影響する可能性がある等の疑義がある場合で、運営審議委員会にて認証の継続が不適当、又は認証の取消が適当との助言がなされた場合

⑦ 運営審議委員会にて認証の承継許可が相当との助言がなされなかった場合、又は承継却下が相当との助言がなされた場合

⑧ 暗号モジュール認証に係る苦情又は異議申し立てに対する認証機関からの是正要求に対して、定められた期間内に当該認証被許諾者又は当該試験機関が応じなかった場合

⑨ 当該暗号モジュールに実装されている暗号アルゴリズムが、全て非承認となった場合

(2) マネジメントシステム責任者は、統括責任者の決裁を受け、「暗号モジュール認証取消通知書」（様式 20）を認証被許諾者に発行し、当該暗号モジュールの認証管理表（様式 2-1）の特記事項に、「暗号モジュール認証取消通知書」の発行日、「暗号モジュール認証取消通知書」を発行した旨及びマネジメントシステム責任者の氏名を記入する。また、業務担当者に対して、当該暗号モジュール認証の取消の実施を指示する。

(3) 業務担当者は、「暗号モジュール認証製品リスト」から当該暗号モジュールの情報を削除する。

(4) 業務担当者は、更新した「暗号モジュール認証製品リスト」を公開する。

（5） 業務担当者は、当該暗号モジュールに関する***暗号アルゴリズム確認書***、***暗号モジュール認証書***及び***暗号モジュール認証報告書***（「英文暗号モジュール認証書」及び「保証継続報告書」が発行されている場合は、当該文書も含む）を回収する。

10.3 運営審議委員会での認証の暗号モジュール取消についての検討

サプライチェーン等におけるサイバーセキュリティに影響する可能性がある等の疑義がある場合には、原則として、運営審議委員会にて暗号モジュール認証の取消是非について検討し、助言を得なければならない。その際、輸出貿易管理令、認証被許諾者についての国際的なルールの違反の有無、ワッセナーアレンジメント加盟国がそれぞれ定める個別の輸出許可を求める団体・個人のリスト等への掲載有無などの情報、及び認証被許諾者への第三国の政府等からの干渉の可能性等を参考に、総合的に判断できるように努めなければならない。

11. 暗号モジュール認証に関するその他業務取扱

11.1 英文暗号モジュール認証書等発行の業務取扱

（1） 業務担当者は、認証被許諾者から「英文暗号モジュール認証書等発行申請書」（***認証申請手続規程***様式 8）の提出があった場合、「英文暗号アルゴリズム確認書」（***業務運営規程***様式 3）、「英文暗号モジュール認証書」（***業務運営規程***様式 4-1）及び「英文暗号モジュール認証報告書」（***業務運営規程***様式 4-2）の発行手続を行う。

（2） 技術管理者は、当該発行の決裁を行い、認証管理表の特記事項に発行した文書名、原義番号、発行日及び技術管理者名を記載する。

（3） 当該申請書が提出された場合は、申請者に対する英文暗号モジュール認証書等発行手数料（***認証申請手続規程***別表）の請求を機構の財務部に依頼する。

11.2 暗号モジュール認証申請書等記載事項変更業務取扱

業務担当者は、認証被許諾者から「暗号モジュール認証申請書等記載事項変更届」（***認証申請手続規程***様式 4）が提出された場合は、内容を確認のうえ、該当する「暗号モジュール認証申請書」、「暗号アルゴリズム確認申請書」及び「英文暗号モジュール認証書等発行申請書」の申請書原本変更の手続を行う。技術管理者は、当該変更に関する決裁を行い、認証管理表の特記事項に変更箇所及び理由、変更日及び技術管理者名を記載する。

11.3 申請取下げ業務取扱

業務担当者は、「暗号モジュール認証申請等取下げ届」（***認証申請手続規程***様式 5）が提出された場合、又は申請料が納付期限までに納付されなかった場合は、内容を確認のうえ、暗号モジュール認証申請、暗号アルゴリズム確認申請及び英文暗号モジュール認証書等発行

申請の取下げ手続を行う。技術管理者は、当該取下げに関する決裁を行い、認証受付簿にその旨を記載し、認証管理表の特記事項に申請取下げ及び理由、取下げ日及び技術管理者名を記載する。この場合において、申請書及びその添付書類は、原則として、当該申請者に返却しない。

11.4 暗号モジュール認証製品リスト等記載事項変更業務取扱

業務担当者は、認証被許諾者から「暗号モジュール認証製品リスト等記載事項変更届」（***認証申請手続規程***様式 6）が提出された場合は、内容を確認のうえ、該当する「暗号モジュール認証製品リスト」等に記載されている内容の変更手続を行う。技術管理者は、当該変更に関する決裁を行い、認証管理表の特記事項に変更箇所及び理由、変更日及び技術管理者名を記載する。

11.5 暗号モジュール認証書等再発行業務取扱

（1） 業務担当者は、認証被許諾者から「暗号モジュール認証書等再交付申請書」（***認証申請手続規程***様式 7）の提出があった場合は、***暗号アルゴリズム確認書***、***暗号モジュール認証書***、***暗号モジュール認証報告書***、「英文暗号アルゴリズム確認書」、「英文暗号モジュール認証書」又は「英文暗号モジュール認証報告書」の再発行の手続を行う。

（2） 技術管理者は、当該再発行の決裁を行い、認証管理表の特記事項に再発行した文書名、原議番号、再発行日及び技術管理者名を記載する。

（3） ***暗号アルゴリズム確認書***、***暗号モジュール認証書***、***暗号モジュール認証報告書***、「英文暗号アルゴリズム確認書」、「英文暗号モジュール認証書」又は「英文暗号モジュール認証報告書」を再発行する場合、初回発行日並びに再発行日及び再発行である旨を当該書類上に記載する。また、以前発行した書類が存在する場合には、その書類を回収し差し替える。

（4） 当該申請書が提出された場合は、申請者に対する再発行手数料（***認証申請手続規程***別表）の請求を機構の財務部に依頼する。

12. 暗号モジュール認証等の承継

認証書発行後の認証被許諾者が、暗号モジュール認証又は暗号アルゴリズム確認に係る事業の全部を譲渡しようとするとき、又は合併が見込まれるときは、譲渡又は合併に先立って認証機関に事前相談が行われた上で、継続して認証要求事項が維持されている場合に限り、その事業の全部を譲り受けた法人若しくは合併後存続する法人又は合併により設立された法人に、その認証被許諾者の地位の承継を認める。この場合において、暗号モジュール認証等の承継手続は、11.4 及び 11.5 を準用し、「暗号モジュール認証製品リスト等記載事項変更届」及び「暗号モジュール認証書等再交付申請書」に加え、その事実を証する次

の書面の添付を求める。

① 交付された*暗号アルゴリズム確認書*、*暗号モジュール認証書*、*暗号モジュール認証報告書*等一式
② 譲渡先又は合併後の法人の法人格を証明する書類
③ 譲渡先又は合併後の法人の支配権（株式会社の場合、筆頭株主及び主要株主）に関する情報
④ 認証被許諾者から譲渡先又は合併後の法人に対して、*暗号モジュール認証書*等に記載されている暗号モジュール等に係る事業の全てが承継される旨を明記した書類であって、認証被許諾者の責任者による押印又は署名がなされたもの
⑤ OEM ライセンス契約に基づく暗号モジュール認証等を承継させる場合、譲渡先又は合併後の法人が、暗号モジュールの開発企業と製造企業との間で OEM ライセンス契約を締結していることを証明する書類

認証要求事項が維持されているかを判断するため、認証機関は、必要に応じて、9.1 に従ってサーベイランスを実施する。また、承継先が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法人等でない場合には、原則として、運営審議委員会にて承継の可否について検討し、助言を得なければならない。その際、輸出貿易管理令、承継先の法人等についての国際的なルールの違反の有無、ワッセナーアレンジメント加盟国がそれぞれ定める個別の輸出許可を求める団体・個人のリスト等への掲載有無などの情報、及び承継先の法人等への第三国の政府等からの干渉の可能性等を参考に、総合的に判断できるように努めなければならない。運営審議委員会の助言を参考に当該承継を却下し、**暗号モジュール認証等**の取消等ができるものとする。なお、**暗号モジュール認証等**の取消等を行う場合には、10.に従って実施する。

13. 規程類及び手続、セキュリティ要件等の変更

13.1 規程類及び手続の変更

認証機関は、暗号モジュール認証に係る規程類及び手続等を変更しようとする場合は、原則 2 週間以上の周知期間をおいて適切な予告を申請者に与えるようにするため、22.に定める手順に加え、次の手順に従う。

(1) 暗号モジュール認証に係る規程類及び手続等に関して重要な変更をしようとする場合、変更内容に関する審議を行うため、運営審議委員会を開催し、統括責任者への答申を得る。
(2) 運営審議委員会を開催せずに暗号モジュール認証に係る規程類及び手続等に関して変更をしようとする場合、運営審議委員会に対して当該規程類及び手続等を改正することを報告する。

(3) 改正後の規程類及び手続等を公開し、原則 2 週間以上の周知期間を経て、旧来の規程類及び手続等を廃止する。廃止の手続きは 23.に従って行う。
(4) この変更は、原則として、認証済暗号モジュール及び確認済暗号アルゴリズム実装、並びに認証申請中の暗号モジュール及び暗号アルゴリズム実装に対しても、周知期間終了後直ちに適用されるものとする。
(5) (4) にかかわらず、認証済暗号モジュール及び確認済暗号アルゴリズム実装に対して、やむを得ず適用を猶予する期間を設ける必要がある場合には、6 カ月を限度として適用猶予期間を設けることができる。

13.2 セキュリティ要件等の変更

認証機関は、暗号モジュール認証に係る***セキュリティ要件等***を変更しようとする場合は、少なくとも 1 ヶ月以上の十分な期間をおいて適切な予告を申請者に与えるようにするため、22.に定める手順に加え、次の手順に従う。

(1) ***制度基本規程***の***附属書 A*** に掲げる暗号モジュール認証に係る要求事項を変更しようとする場合、旧来の要求事項と新規の要求事項の両方を並立させるようにし、新規の要求事項に関する審議を行うため、技術審議委員会を開催し、統括責任者への答申を得る。
(2) 運営審議委員会に対して、***制度基本規程***の***附属書 A***に掲げる暗号モジュール認証に係る要求事項を改正することを報告する。
(3) 改正後の暗号モジュール認証に係る要求事項を公開し、少なくとも 6 ヶ月の並立期間を経て、旧来の要求事項の廃止手続きを開始する。廃止の手続きは 23.に従って行う。
(4) この変更は、認証申請中の暗号モジュール及び暗号アルゴリズム実装に対しても、並立期間終了後直ちに適用されるものとする。
(5) 認証済暗号モジュール及び確認済暗号アルゴリズム実装については、2 年を限度として適用猶予期間を設けることができる。この変更は、適用猶予期間が経過した後に適用されるものとする。

14. 内部監査

内部監査は、認証機関としての業務が「暗号モジュール試験及び認証制度における認証業務の品質を維持向上させるためのマニュアル」(以下「品質マニュアル」という。) 及びその他のマネジメントシステム文書に継続して適合しているかどうかを検証するため、機構の内部監査部 (以下「内部監査部」という。) が実施する。定期の内部監査は、通常、毎年１回とする。ただし、マネジメントシステム責任者が必要と認める場合は、臨時の内部監査を内部監査部に依頼することができる。マネジメントシステム責任者は、認証機関の内部監査及びそれに基づく是正処置等が確実に実施されることについて責任を負う。

14.1 内部監査の実施

マネジメント責任者は、***業務運営規程***に基づき、内部監査を内部監査部に依頼する。

14.2 内部監査の結果

内部監査において指摘事項がある場合、マネジメントシステム責任者は、17.及び 18.に従って是正処置を実施する。当該指摘事項に関連する是正処置が完了したとき、マネジメントシステム責任者は、「内部監査是正処置報告書」(様式 5) により、統括責任者に報告する。なお、是正処置の内容を勘案し、当該処置の効果等を詳細に検討する必要性がある場合、マネジメントシステム責任者は、臨時の内部監査の実施を内部監査部に依頼することができる。

15. マネジメント・レビュー

統括責任者は、業務見直しのためのマネジメント・レビューを実施することとし、マネジメントシステム責任者及び暗号モジュール技術管理者（以下「技術管理者」という。）をマネジメント・レビューに参加させる。また、必要に応じて、他の関係者を参加させることができる。

15.1 マネジメント・レビューの実施

統括責任者は、マネジメント・レビューを年１回実施することとする。また、統括責任者が必要と認めた場合は、随時開催することができる。

マネジメントシステム責任者及び技術管理者は、次の事項について、統括責任者に報告する。

① 業務報告及び決算報告
② 内部監査実施報告
③ 是正処置・予防処置報告
④ 苦情等に関する報告
⑤ 教育・訓練実施報告、暗号モジュール認証要員の業務査定報告
⑥ 適用セキュリティ要件等の改正状況
⑦ 現行の人的および設備資源の妥当性
⑧ その他、マネジメントシステムの確保に必要な事項

15.2 マネジメント・レビューの結果

統括責任者は、マネジメント・レビューの結果に基づいて、必要に応じて、品質方針の見直し、品質マニュアル及びその他のマネジメントシステム文書の改正を含め、マネジメン

トシステム責任者に 18.に従って是正処置の実施を指示する。統括責任者は、是正処置完了後、その有効性について確認を行う。マネジメントシステム責任者は、マネジメント・レビューの実施結果を「マネジメント・レビュー記録書」（様式 6）に記録し、管理する。

16. 予防処置

マネジメントシステム責任者は、技術面及びマネジメントシステムの両面において、必要とされる改良の機会及び不適合の潜在的原因を特定するため、年 1 回、暗号モジュール認証プログラムに従事する職員に対し、内部監査記録、暗号モジュール認証に係る記録及び関連する品質記録を調査させることとする。なお、不適合の潜在的原因を発見した職員は、直ちに、マネジメントシステム責任者に報告を行うこととする。

16.1 予防処置の実施

マネジメントシステム責任者は、予防処置が必要とされたものについて、潜在的原因を特定して予防処置を策定し、処置期限を定め、その業務を担当する適切な職員に予防処置の実施を指示する。

16.2 予防処置の結果

予防処置の実施を行った職員は、予防処置結果を「予防処置報告書」（様式 7）により、マネジメントシステム責任者に報告する。マネジメントシステム責任者は、「予防処置報告書」により、その予防処置の効果を確認する。必要に応じて、マネジメントシステム責任者は、予防処置の結果をマネジメント・レビューへ報告する。なお、「予防処置報告書」には、「Y」の文字、西暦、3 桁の連続する数字により番号を付番することとする。
例：Y2008001

17. 不適合管理

（1） 不適合の管理に関する責任者は、マネジメントシステム責任者とする。
（2） 不適合を発見した者は、その不適合を直ちにマネジメントシステム責任者に報告する。
（3） マネジメントシステム責任者は、不適合発生部署の責任者及び関係部署との協議により不適合処置責任者を定め、不適合の重大さを評価し、次に掲げる処置を確定し実施する。
① 不適合業務の一時的な停止
② 不適合の容認の可能性の決定
③ 不適合事項の修正
④ 過去の結果の回収

⑤ 業務の再開

不適合処置責任者は、実施した処置を「不適合処置報告書」（様式 8）により、マネジメントシステム責任者に報告する。なお、「不適合処置報告書」には、「F」の文字、西暦、3 桁の連続する数字により番号を付番することとする。

例：F2008001

18. 是正処置

マネジメントシステム責任者は、不適合が再発しうること又は認証機関の品質方針及び手順に対する自らの操業の適合性に疑いがあることが示された場合、認証機関内の原因発生部署又は認証機関外の原因発生元に対して不適合又は苦情の原因調査を要請し、その報告を受ける。

18.1 是正処置の実施

(1) マネジメントシステム責任者は、不適合又は苦情の原因調査の結果、是正処置が必要とされたものについて、原因及び是正処置の方策を特定し、原因発生部署の責任者に対し是正処置の実施を指示する。

(2) 是正処置には、必要な範囲で次の項目を含める。

① 原因の除去

② 再発防止処置

③ 遡及処置

(3) 再発防止処置に関し、文書の変更が必要な場合、変更を行う。

18.2 是正処置の報告・確認・記録

(1) 原因発生部署の責任者は、是正処置を実施した後、是正処置結果を「是正処置報告書」（様式 9）により、マネジメントシステム責任者に報告する。

(2) マネジメントシステム責任者は、「是正処置報告書」により、その是正処置の妥当性を確認する。

(3) マネジメントシステム責任者は、「是正処置報告書」を保管する。

(4) マネジメントシステム責任者は、是正処置の結果を実施した後、その是正処置が問題の解決に効果的であることを確認するため、結果を監視する。

(5) 必要に応じて、マネジメントシステム責任者は、是正処置の結果をマネジメント・レビューに報告する。

なお、「是正処置報告書」には、「Z」の文字、西暦、3 桁の連続する数字により番号を付番することとする。

例：Z2008001

19. 苦情又は異議申し立ての処理

19.1 苦情又は異議申し立ての受付

認証機関に提起された苦情又は異議申し立ての受付を行った職員は、「苦情等受付票」（様式 10）によりマネジメントシステム責任者に報告する。マネジメントシステム責任者は、苦情又は異議申し立ての受付の報告を受けた場合、苦情等処理担当者を指名する。
必要に応じて、統括責任者、マネジメントシステム責任者及び技術管理者は、会合を開き、対応を協議する。
なお、「苦情等受付票」には、「U」の文字、西暦、3 桁の連続する数字により番号を付番することとする。
例：U2008001

19.2 苦情又は異議申し立ての処理の実施

苦情等処理担当者は、苦情又は異議申し立ての内容を精査し、原因及び事実関係を調査、記録し、次の手順で処理を行う。

(1) 申し立ての内容が正当であり、その原因が認証機関にある場合には、原因発生部署に対して苦情又は異議申し立ての処置の実施を指示し、原因の除去、苦情又は異議申し立てに対する処理を行う。

(2) 申し立ての内容は正当であるが、その原因が認証機関にない場合には、原因発生元に対して是正処置、原因の除去、苦情又は異議申し立てに対する処理を要求する。なお、苦情又は異議申し立ての情報源は認証機関の秘密とした上で、情報源が同意した場合を除き、原因発生元と共有しない。ただし、原因発生元との情報共有を禁止する条件で申し立てられた苦情であって原因発生元が認証機関ではない場合、認証機関では取り扱えない旨を申し立て者に通知し、苦情処理を終了する。

① 苦情又は異議申し立ての内容が、認証機関が発行した暗号モジュール認証に係る文書及び暗号モジュール認証マークの不正な使用等による場合、認証機関は、当該苦情又は異議申し立てに係る認証書発行後の認証被許諾者に対して是正要求をし、必要に応じて、10.に基づいて暗号モジュール認証の一時停止又は取消をすることができる。必要に応じて、法的措置をとる。

② 苦情又は異議申し立ての内容が、***暗号モジュール試験機関の承認手続等に関する規程***（CBM-03）に適合していない暗号モジュール試験機関業務に関連する場合、認証機関は、当該試験機関に対して是正要求をし、必要に応じて、10.に基づいて暗号モジュール認証の一時停止又は取消をすることができる。必要に応じて、法的措置をとる。

(3) 申し立ての内容が事実無根である場合は、その旨を申し立て者に文書で通知する。

19.3 苦情又は異議申し立ての処理の結果報告

苦情等処理担当者は、苦情又は異議申し立ての処理の結果を「苦情等処理報告書」(**様式 11**)によりマネジメントシステム責任者に報告する。認証機関は、苦情又は異議申し立ての処理について、その調査結果及び処理結果を、文書により申し立て者に通知する。

なお、「苦情等処理報告書」には、「K」の文字、西暦、3 桁の連続する数字により番号を付番することとする。

例：K2008001

20. 文書管理責任体制

(1) ***制度基本規程***の「本制度に関する規程等」に掲げる文書、***制度基本規程***の***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試験要件、並びに暗号アルゴリズム実装試験要件（以下「マネジメントシステム文書」という。）の制定改廃権者は、規程等については理事長、手順等については統括責任者とする。

(2) 統括責任者は、マネジメントシステム文書の発行承認を行う。

(3) マネジメントシステム責任者は、マネジメントシステム文書及び外部文書の管理について最終的な責任を有する。

(4) マネジメントシステム責任者は、(1) の文書を常に最新の状態で保管し、暗号モジュール試験及び認証制度の運用に従事する職員が必要に応じて利用できる状態に維持しなければならない。

(5) 技術管理者は、申請書類、記録、報告書等の管理について最終的な責任を有する。

21. マネジメントシステム文書の分類、管理番号、識別番号及び様式

(1) 文書体系は、次のとおり分類する。

① 規程、暗号モジュールセキュリティ要件等

② 手順、運用ガイダンス等

(2) マネジメントシステム文書には「(英字 3 文字) － (数字 2 文字) {－ (英字 1 文字)}」で表す識別番号を付すものとする。なお、{中括弧} は、手順を表す。

(3) マネジメントシステム文書の識別番号は、***制度基本規程***の「本制度に関する規程等」による。

(4) マネジメントシステム文書の版管理は、年月日で行う。

(5) マネジメントシステム文書には、改正内容を含んだ改正履歴を付すものとする。

22. マネジメントシステム文書の制定・改正の手順

マネジメントシステム文書の制定又は改正の手順は次による。

22.1 担当者の指名

マネジメントシステム責任者は、文書担当者を指名する。

22.2 マネジメントシステム文書の原案の作成

指名された文書担当者は、制定又は改正するマネジメントシステム文書の原案（以下「原案」という。）を作成する。

22.3 運営審議委員会での検討

制度基本規程及び***業務運営規程***については、原則として、運営審議委員会にて検討し、助言を得なければならない。

22.4 決裁及び施行

統括責任者は、マネジメントシステム文書が制定改廃権者により決裁を受けた後、決裁された文書を施行する。

22.5 文書の最新版の管理

文書担当者は、文書が制定又は改正されたときは、「マネジメントシステム文書管理表」（様式 12）に記載し、これを維持する。また、マネジメントシステム文書は非公開のものを除き、機構のホームページで公表するとともに、改正されたときは、速やかにこれを更新するものとする。

なお、旧版については、電子媒体にて保存することとする。この場合の保存期間は、5 年間とする。

22.6 公開文書

文書担当者は、公表文書を機構のホームページ上で公開する。

23. マネジメントシステム文書の廃止

（1） マネジメントシステム文書については、制定改廃権者の承認をもって、その廃止が決定される。

（2） 制度文書及び品質マニュアルについては、原則として、制定改廃権者の承認に先立って、運営審議委員会の助言を得なければならない。文書担当者は、助言を受け廃止手

続を行う。

(3) 廃棄文書については、電子媒体にて保存することとする。この場合の保存期間は、5年間とする。

24. 外部文書の管理

(1) 外部文書は、別表1に掲げるものとし、常に最新版を維持することとする。これらの文書は、外部文書ファイルとして整理する。

(2) マネジメントシステム責任者は、必要とする外部文書の部数を定め、確保する。

(3) マネジメントシステム責任者は、外部文書の版が改正された場合には、旧版については、電子媒体にて保存することとする。ただし、外部文書が紙媒体の場合は、表紙に赤字で「旧版」と表示して保存することとする。保存期間は5年間とする。

25. 申請書類及び記録・報告書等の管理

(1) マネジメントシステム文書に規定されている申請書類及び記録・報告書等を保存文書とする。文書担当者は、機構の「法人文書管理規程」(2013情総第155号)に従い管理する。

(2) 申請書類及び記録・報告書は、マネジメントシステム文書に特段の規定がない限り、原則としてファイルに綴じて保存する。この場合、保存期間は、マネジメントシステム文書に特に定められていない限り、5年間とする。

26. マネジメントシステム文書、記録・報告の閲覧

(1) 外部からのマネジメントシステム文書、申請書類、外部文書及び記録・報告書の閲覧要望については、認証機関が窓口となり、対応することとする。

(2) 認証機関は、(1)の閲覧の申し出を受けた場合は、これに応じなければならない。ただし、申請者の機密情報及びプライバシーに係ると判断される情報等については、公開しないこととする。

27. 秘密資料

申請者及び試験機関より受領した文書は、原則、秘密資料として取り扱う。但し、次の文書は、秘密資料として取り扱わない。

a) 申請者又は試験機関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。

b) 申請者又は試験機関より開示を受けた後に認証機関の故意又は過失によらず公知とな

ったもの。

c) 申請者又は試験機関より開示を受ける前に認証機関が自ら知得し、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。

d) 申請者又は試験機関から書面により開示を承諾されたもの。

27.1 秘密資料の入手時の取扱い及び保管

（1） 秘密資料を電子データで入手した場合は、外部ネットワークに接続された PC において、ウィルスが含まれていないかチェックする。その上で、原則として次の a)に従って取り扱うものとする。

a) 物理的に外部ネットワークから切断されている内部ネットワークにサーバ、ローカル PC を配置し、アクセス権を限定されたサーバの専用フォルダに、ウィルスチェックを行った秘密資料を暗号化して保管する。また、その利用もローカル PC に限定する。

b) 天災その他やむを得ない事由により、認証業務の継続が妨げられる場合に際し、マネジメントシステム責任者が許可した場合であって、且つ申請者が同意した場合に限り、認証機関の要員にアクセス権を制限し、通信の複数階層の暗号化を適用した上で、秘密資料への機構の執務室ネットワークからのアクセスが許容される。

（2） 紙媒体の場合には、鍵付き書庫に保管する。

上記の何れの場合にも、暗号モジュール認証案件毎に「秘密資料管理簿」（様式 13）を準備し、入手日等の必要事項を記録する。

27.2 秘密資料の開示

（1） 秘密資料は、秘密資料関係者以外に開示してはならない。

（2） 「暗号モジュール認証製品リスト」に登録された暗号モジュールに係る「セキュリティポリシ」等は、公開された時点で秘密資料としての取扱いを終了する。

27.3 秘密資料の持出し

秘密資料は、暗号モジュール認証業務に係る実務を行う施設（機構のセキュリティ技術評価部執務室のうち、評価ツール室を除くエリアを指す。以下「認証業務に係る施設」という。）以外への持出しを禁止する。但し、暗号モジュール認証業務等に必要な場合は、申請者が認めた施設に持出すことができる。この場合は、暗号モジュール認証案件毎に「秘密資料持出管理簿」（様式 14）を準備し、持出す当該秘密資料名等の必要事項を記録する。

27.4 秘密資料の返却・消去

（1） 紙媒体の秘密資料は、使用後、速やかに鍵付き書庫に返却することとする。

(2) アクセス権を限定されたサーバの専用フォルダ外のローカル PC にコピーされた秘密資料は、業務終了後、速やかに消去することとする。
(3) 秘密資料を暗号モジュール認証業務の終了時点で入手先に返却する際は、「秘密資料管理簿」（様式 13）に返却日を記録する。返却した秘密資料の受領確認の連絡を返却先から電子メール等により受け取り、「秘密資料管理簿」（様式 13）に返却確認日を記録する。
(4) 秘密資料は、不要になった時点で秘密資料管理簿に消去日を記入し、紙媒体の場合はシュレッダにより消去し、電子データの場合は内容を消去する。

27.5 その他

秘密資料に関連する情報を電子メールにより交換する場合は、暗号化する。ただし、情報を交換する相手先との間で、暗号化が不要との合意がされているときは、この限りでない。

28. 入室管理

(1) 認証業務に係る施設の入室用扉には、入室の許可を得た者のみが入室できるように、入室管理装置（生体認証装置）を設置する。
(2) マネジメントシステム責任者は、個人認証機器管理者を選任し、上記の入室管理装置（生体認証装置）を管理させる。
(3) 認証業務に係る施設への入室手続きについては別途定める。

附　則

この手順は、平成 18 年 10 月 30 日から施行し、平成 18 年 10 月 2 日から適用する。

附　則

この手順は、平成 19 年 11 月 14 日から施行し、平成 19 年 10 月 26 日から適用する。

附　則

この手順は、平成 20 年 5 月 2 日から施行する。

附　則

この手順は、平成 21 年 1 月 8 日から施行する。

附　則

この手順は、平成 22 年 8 月 17 日から施行する。

附　則

この手順は、平成 22 年 9 月 27 日から施行する。

附　則

この手順は、平成 23 年 12 月 21 日から施行する。

附　則（平成 29 年 4 月 10 日　2017 情セ第 12 号・一部改正）

この手順は、平成 29 年 4 月 10 日から施行する。

附　則（平成 30 年 6 月 28 日　2018 情セ第 234 号・一部改正）

この手順は、平成 30 年 7 月 1 日から施行する。

附　則（令和 2 年 11 月 9 日　2020 情セ技第 1044 号・一部改正）

この手順は、令和 2 年 11 月 9 日から施行する。

暗号モジュール認証業務取扱手順に係る様式集

(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 1-1

暗号モジュール認証申請受付簿

受付番号 受付年月日	新規 or 再(認証番号) 保証	暗号モジュール名称 バージョン	申請者名称 連絡担当者(TEL　　)	決裁(適・否) 決裁日	認証番号 交付日	摘要
M200807-01 2008/07/21	新規・ 再(No.　　) 保証	○○暗号モジュール Ver.1.2.3	○○株式会社 情推太郎(03-5978-7545)	適・否 2008/08/21	No.43 2008/08/31	(記述例)
	新規・ 再(No.　　) 保証			適・否		
	新規・ 再(No.　　) 保証			適・否		
	新規・ 再(No.　　) 保証			適・否		
	新規・ 再(No.　　) 保証			適・否		
	新規・ 再(No.　　) 保証			適・否		

様式 1-2

暗号アルゴリズム確認申請受付簿

受付番号 受付年月日	暗号アルゴリズム実装名称 バージョン	申請者名称 連絡担当者(TEL　　)	決裁(適・否) 決裁日	交付日	摘要
A200902-01 2009/02/20	○○暗号モジュール Ver.1.2.3	○○株式会社 情推太郎(03-5978-7545)	(適)・否 2009/03/21	2009/03/31	(記述例)
			適・否		
			適・否		
			適・否		
			適・否		
			適・否		
			適・否		
			適・否		

様式 2-1

暗号モジュール認証進捗状況管理表

識別情報	受付番号	
	申請者名称 連絡担当者(TEL　)	
	暗号モジュール名称 バージョン	

No.	項目	日付	担当者	摘要
4.1				
(1)	暗号モジュール認証申請受付		(業)	認証申請内容の確認
(2)	受領書類の確認日			確認日（　　） or 不適(再提出指示日)
	① 暗号モジュール認証申請書		(業)	適・不適(　　)
	② 法人格を証明できる書類		(業)	適・不適(　　)
	③ 同意書		(業)	適・不適(　　)
	その他(　　)		(業)	適・不適(　　)
(3)	暗号モジュール認証申請の受付についての運営審議委員会への付議の要否判断		(技)	必要(4.6 を実施)・不要
	暗号モジュール認証申請の受付可否の判断		(技)	受付可 or 受付不許可 決定日(　　)
(4)	受付番号欄に受付番号を記入		(業)	認証申請書に記入
(5)	暗号モジュール認証申請受付簿記入		(業)	様式 1-1
(6)	本表冒頭の識別情報欄に受付番号、申請者名称等を記入		(業)	
(7)	受付番号及び受領書類リストを送信		(業)	申請者と試験機関に送信
4.3				
(1)	秘密保持契約締結起案日 注：秘密保持契約の締結は、暗号モジュール認証申請受付日をもって行う。		(業)	有(　情セ技第　　号)・無
(2)	覚書締結起案日		(業)	有(　情セ技第　　号)・無
(3)	秘密保持契約書等送付日		(業)	保管日(　　)

No.	項目	日付	担当者	摘要
4.4				
(1)	申請料の請求 (財務部へ申請受付の連絡日)		(業)	免除等を行う理由 (　　)
(2)	必要経費の決定		(技)	決定・対象外
(3)	申請料納付の確認		(業)	納付日：
4.5				
(1)	申請者と誤解の無いことの確認		(技)	電話等で確認
(2)	認証要員選任日		(技)	認証要員名(　　)
(3)	認証要員の氏名を送信		(技)	試験機関へ電子メール
(4)	暗号モジュール認証申請受理通知書を作成し、技術管理者の印を押捺		(技)	様式 3-1（以下「認証申請受理通知書」という。）
(5)	認証申請受理通知書発送日		(業)	送付する
4.6				
	運営審議委員会での申請受付可否についての検討		(技)	開催日（　　）
5.1				
(1)	暗号アルゴリズム実装試験報告書受理日		(業)	電子メール送信日(　)
(2)	暗号アルゴリズム確認業務の継続についての運営審議委員会への付議の要否判断		(技)	必要(5.4 を実施)・不要
	暗号アルゴリズム確認業務の継続可否又は許諾可否の判断		(技)	継続可／許諾可 or 継続不可／許諾拒否 決定日(　　)
(3)	申請料の入金確認		(技)	納付済・未納付
(4)	既に暗号アルゴリズム確認書を発行しているか		(業)	未発行・発行済み
(5)	暗号アルゴリズム実装試験報告書調査日			適 or 不適(調査日)
	①記述に齟齬が無いか？		(認)	適・不適(　　)
	②暗号モジュール試験の要求事項に照らして、暗号アルゴリズム実装の構成要素と実装されている暗号アルゴリズムの関係が明確か？		(認)	適・不適(　　)
	③暗号モジュール試験の要求事項に照らして、開発に用いたツール及びツ		(認)	適・不適(　　)

No.	項目	日付	担当者	摘要
	ールのオプションは明確か？			
	④暗号アルゴリズムの依存性は満足されているか？		(認)	適・不適(　　)
	⑤確率的素数テストを用いるアルゴリズムについて、実装されている確率的素数テストの詳細について報告されているか？ また、暗号アルゴリズムの仕様に準拠していることを確認しているか？		(認)	適・不適(　　)
	⑥動作環境に問題が無いか？ 特に、暗号支援命令を使用している、動作環境にインストールされる特定の実行時環境を前提としているなどの事実は、動作環境の表記に反映されているか？		(認)	適・不適(　　)
	⑦ツールのバージョンが最新版か？		(認)	適・不適(　　)
	⑧試験結果が正当であるか？		(認)	適・不適(　　)
	調査結果		(認)	適・不適 再提出指示日(　　)

	暗号アルゴリズム確認書作成日		(認)	暗号アルゴリズム確認書
	調査完了報告日		(認)	技術管理者へ
(6)	暗号アルゴリズム確認決裁日		(技)	決裁 : 適・否(差戻日　　)
(7)	暗号アルゴリズム確認書起案日		(業)	原議(　情セ技第　　号)
(8)	暗号アルゴリズム確認書発行日		(業)	写しの保管日(　　)
(9)	既発行暗号アルゴリズム確認書回収		(業)	対象外・回収日（　　）
(10)	暗号アルゴリズム確認書発送日		(業)	試験機関に送付
(11)	試験機関に対して発送した旨送信日		(業)	申請者へ電子メール
(12)	暗号アルゴリズム確認登録簿登録日		(業)	暗号アルゴリズム毎に
(13)	暗号アルゴリズム確認登録簿公開日		(業)	機構ホームページで公開
5.2				
(1)	暗号モジュール試験報告書受理日		(業)	電子メール送信日(　　)
(2)	暗号モジュール認証業務の継続についての運営審議委員会への付議の要		(技)	必要(5.4 を実施)・不要

No.	項目	日付	担当者	摘要
	否判断			
	暗号アルゴリズム確認業務の継続可否又は許諾可否の判断		(技)	継続可／許諾可 or 継続不可／許諾拒否 決定日(　　)
(3)	暗号モジュール試験報告書調査日			適 or 不適(質問識別番号)
	①記述に齟齬が無いか？・同意の署名		(認)	適・不適(　　)
	②動作環境に問題が無いか？		(認)	適・不適(　　)
	③ツールのバージョンが最新版か？		(認)	適・不適(　　)
	④試験結果が正当であるか？		(認)	適・不適(　　)
	第 1 章		(認)	適・不適(　　)
	第 2 章		(認)	適・不適(　　)
	第 3 章		(認)	適・不適(　　)
	第 4 章		(認)	適・不適(　　)
	第 5 章		(認)	適・不適(　　)
	第 6 章		(認)	適・不適(　　)
	第 7 章		(認)	適・不適(　　)
	第 8 章		(認)	適・不適(　　)
	第 9 章		(認)	適・不適(　　)
	第 10 章		(認)	適・不適(　　)
	第 11 章		(認)	適・不適(　　)
	Appendix C		(認)	適・不適(　　)
	⑤正常系及び異常系のテストカバレッジが十分か		(認)	適・不適(　　)
	TE02.15.03			
	TE03.01.04			
	TE03.05.01			
	TE03.05.02			
	TE03.06.01			
	TE03.06.02			
	TE03.07.02			
	TE03.08.01			
	TE03.08.02			
	TE03.11.01			
	TE03.11.02			

No.	項目	日付	担当者	摘要
	TE04.20.03			
	TE04.37.02			
	TE04.38.02			
	TE04.39.03			
	TE04.39.04			
	TE04.43.02			
	TE04.44.02			
	TE04.45.02			
	TE04.55.02			
	TE11.08.02			
	TE11.08.06			
	TE11.08.07			
	TE11.08.08			
	TE11.08.09			
	TE06.08.03			
	TE06.06.02			
	TE09.01.02			
	TE09.02.02			
	TE09.03.02			
	TE09.03.03			
	TE09.14.02			
	TE09.25.02			
	TE10.08.02			
	TE10.08.03			
	---			
	⑥セキュリティポリシの記述は適切か?		(認)	適・不適(　　)
	暗号アルゴリズム確認番号は記載されているか?			
	承認動作モードを呼び出すための方法が記載されているか?			
	既定の役割が記載されているか? TEA.01.01			
	サービスのリストが記載されている			

No.	項目	日付	担当者	摘要
	か? TEA.01.01			
	認証メカニズム・強度が記載されているか?			
	アクセス制御ポリシが記載されているか?			
	物理的セキュリティポリシが記載されているか?			
	その他の攻撃への対処ポリシが記載されているか?			
	⑦報告書に CSP のリスト、CSP のアクセス制御ポリシが転記されているか?		(認)	適・不適(　　)
	⑧エントロピー収集の(最低限)機能仕様レベルの記述が含まれているか? エントロピー源が暗号モジュール境界の内側にあるか? TE09.08.01		(認)	適・不適(　　)
	⑨その他		(認)	適・不適(　　)
	TE02.15.01 ソフトウェア暗号モジュールでもその識別・バージョンが記載されているか?			
	暗号モジュール認証書作成日		(認)	暗号モジュール認証書
	暗号モジュール認証報告書作成日		(認)	認証報告書
	調査完了報告日		(認)	技術管理者へ
(4)	暗号モジュール認証決裁日		(技)	決裁 : 適・否(差戻日　　)
(5)	暗号モジュール認証書等起案日		(業)	原議(　情セ技第　　号)
(6)	暗号モジュール認証書等発行日		(業)	写しの保管日(　　)
(7)	暗号モジュール認証書等発送日		(業)	申請者に送付
(8)	申請者に対して発送した旨送信日		(業)	申請者へ電子メール
(9)	暗号モジュール認証製品リスト 登録日		(業)	セキュリティポリシ及び申請者の情報等も登録
(10)	暗号モジュール認証製品リスト 公開日		(業)	機構ホームページで公開

No.	項目	日付	担当者	摘要
5.3				
(1)	暗号モジュール所見報告書受理日		(技)	受理(識別番号　　)・ 不受理(理由　　)
(2)	暫定処置検討会議開催日		(技)	認証要員と会議
(3)	暗号モジュール所見報告書送付日		(技)	試験機関へ送付
(4)	技術審議委員会での問題点解決日		(技)	運用ガイダンス発行日( )
(5)	セキュリティ要件等変更手続開始日		(技)	必要に応じて
5.4				
	運営審議委員会での認証の許諾等についての検討		(技)	開催日（　　）

注）表の網掛けの部分は、暗号モジュール技術管理者が担当する部分を表す。

＜特記事項＞

様式 2-2

暗号アルゴリズム確認進捗状況管理表

識別情報	受付番号	
	申請者名称 連絡担当者(TEL　)	
	暗号モジュール名称 バージョン	

No.	項目	日付	担当者	摘要
4.2				
(1)	暗号アルゴリズム確認申請受付		(業)	確認申請内容の確認
(2)	受領書類の確認日			確認日（　　） or 不適(再提出指示日)
	① 暗号アルゴリズム確認申請書		(業)	適・不適(　　)
	② 法人格を証明できる書類		(業)	適・不適(　　)
	③ 同意書		(業)	適・不適(　　)
	その他(　　)		(業)	適・不適(　　)
(3)	暗号アルゴリズム確認申請の受付についての運営審議委員会への付議の要否判断		(技)	必要(4.6 を実施)・不要
	暗号アルゴリズム確認申請の受付可否の判断		(技)	受付可 or 受付不許可 決定日(　　)
(4)	受付番号欄に受付番号を記入		(業)	確認申請書に記入
(5)	暗号アルゴリズム確認申請受付簿記入		(業)	様式 1-2
(6)	本表冒頭の識別情報欄に受付番号、申請者名称等を記入		(業)	
(7)	受付番号及び受領書類リストを送信		(業)	申請者と試験機関に送信
4.3				
(1)	秘密保持契約締結起案日 注：秘密保持契約の締結は、暗号アルゴリズム確認申請受付日をもって行う。		(業)	有(　　情セ技第　号)・無
(2)	覚書締結起案日		(業)	有(　　情セ技第　号)・無

No.	項目	日付	担当者	摘要
(3)	秘密保持契約書等送付日		(業)	保管日(　　)
4.4				
(1)	申請料の請求 (財務部へ申請受付の連絡日)		(業)	免除等を行う理由 (　　)
(2)	必要経費の決定		(技)	決定・対象外
(3)	申請料納付の確認		(業)	納付日：
4.5				
(1)	申請者と誤解の無いことの確認		(技)	電話等で確認
(2)	認証要員選任日		(技)	認証要員名(　　)
(3)	認証要員の氏名を送信		(技)	試験機関へ電子メール
(4)	暗号アルゴリズム確認申請受理通知書を作成し、技術管理者の印を押捺		(技)	様式 3-2（以下「確認申請受理通知書」という。）
(5)	確認申請受理通知書発送日		(業)	送付する
4.6				
	運営審議委員会での申請受付可否についての検討		(技)	開催日（　　）
5.1				
(1)	暗号アルゴリズム実装試験報告書受理日		(業)	電子メール送信日(　)
(2)	暗号アルゴリズム確認業務の継続についての運営審議委員会への付議の要否判断		(技)	必要(5.4 を実施)・不要
	暗号アルゴリズム確認業務の継続可否又は許諾可否の判断		(技)	継続可／許諾可 or 継続不可／許諾拒否 決定日(　　)
(3)	申請料の入金確認		(技)	納付済・未納付
(4)	既に暗号アルゴリズム確認書を発行しているか		(業)	未発行・発行済み
(5)	暗号アルゴリズム実装試験報告書調査日			適 or 不適(調査日)
	①記述に齟齬が無いか？		(認)	適・不適(　　)
	②暗号モジュール試験の要求事項に照らして、暗号アル⑤リズム実装の構成要素と実装されている暗号アルゴリズムの関係が明確か？		(認)	適・不適(　　)
	③暗号モジュール試験の要求事項に		(認)	適・不適(　　)

No.	項目	日付	担当者	摘要
	照らして、開発に用いたツール及びツールのオプションは明確か？			
	④暗号アルゴリズムの依存性は満足されているか？		(認)	適・不適(　　)
	⑤確率的素数テストを用いるアルゴリズムについて、実装されている確率的素数テストの詳細について報告されているか？ また、暗号アルゴリズムの仕様に準拠していることを確認しているか？		(認)	適・不適(　　)
	⑥動作環境に問題が無いか？ 特に、暗号支援命令を使用している、動作環境にインストールされる特定の実行時環境を前提としているなどの事実は、動作環境の表記に反映されているか？		(認)	適・不適(　　)
	⑦ツールのバージョンが最新版か？		(認)	適・不適(　　)
	⑧試験結果が正当であるか？		(認)	適・不適(　　)
	調査結果		(認)	適・不適 再提出指示日(　　)

	暗号アルゴリズム確認書作成日		(認)	暗号アルゴリズム確認書
	調査完了報告日		(認)	技術管理者へ
(6)	暗号アルゴリズム確認決裁日		(技)	決裁：適・否(差戻日　　)
(7)	暗号アルゴリズム確認書起案日		(業)	原議(　　情セ第　　号)
(8)	暗号アルゴリズム確認書発行日		(業)	写しの保管日(　　)
(9)	既発行暗号アルゴリズム確認書回収		(業)	対象外・回収日（　　）
(10)	暗号アルゴリズム確認書発送日		(業)	試験機関に送付
(11)	試験機関に対して発送した旨送信日		(業)	申請者へ電子メール
(12)	暗号アルゴリズム確認登録簿登録日		(業)	暗号アルゴリズム毎に
(13)	暗号アルゴリズム確認登録簿公開日		(業)	機構ホームページで公開
5.4				
	運営審議委員会での認証の許諾等についての検討		(技)	開催日（　　）

注）表の網掛けの部分は、暗号モジュール技術管理者が担当する部分を表す。

＜特記事項＞

様式 3-1

暗号モジュール認証申請受理通知書

年　　月　　日

(申請者名称)
(責任者名)　殿

独立行政法人 情報処理推進機構
セキュリティセンター セキュリティ技術評価部暗号グループ
(暗号モジュール技術管理者名)　　印

暗号モジュール認証申請を受理しましたので、以下のように通知します。

記

暗号モジュール名称：
バージョン：

受付番号：

以上

様式 3-2

暗号アルゴリズム確認申請受理通知書

年　　月　　日

(申請者名称)
(責任者名)　殿

独立行政法人 情報処理推進機構
セキュリティセンター セキュリティ技術評価部暗号グループ
(暗号モジュール技術管理者名)　　印

暗号アルゴリズム確認申請を受理しましたので、以下のように通知します。

記

暗号モジュール名称：
バージョン：

受付番号：

以上

様式 4-1

再認証進捗状況管理表

識別情報	受付番号	
	再認証申請者名称 連絡担当者(TEL　)	
	暗号モジュール名称 バージョン	

No.	項目	日付	担当者	摘要
7.2				
(1)	暗号モジュール再認証申請受付		(業)	認証申請内容の確認
(2)	受領書類の確認日			確認日（　　） or 不適(再提出指示日)
	① 暗号モジュール認証申請書		(業)	適・不適(　　)
	② 同意書		(業)	適・不適(　　)
	a) 修正が暗号モジュール試験報告書 30%以下のアサーションしか影響を与えない場合			
	③ 変更箇所に関連する暗号モジュール試験報告書		(業)	適・不適(　　)
	b) 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場合			
	④ 物理的変更分析報告書		(業)	適・不適(　　)
	⑤ 変更箇所に関連する物理的セキュリティ試験報告書		(業)	適・不適(　　)
	その他(　　)		(業)	適・不適(　　)
(3)	申請の受付についての運営審議委員会への付議の要否判断		(技)	必要(4.6 を実施)・不要
	運営審議委員会での申請受付可否についての検討		(技)	開催日（　　）
	申請の受付可否の判断		(技)	受付可 or 受付不許可 決定日(　　)
(4)	受付番号欄に受付番号を記入		(業)	認証申請書に記入
(5)	暗号モジュール認証申請受付簿記入		(業)	様式 1-1
(6)	本表冒頭の識別情報欄に受付番号、申請者名称等を記入		(業)	
(7)	受付番号及び受領書類リストを送信		(業)	申請者と試験機関に送信

No.	項目	日付	担当者	摘要
7.3	4.3 秘密保持契約の締結 と同様の手順に従う。			
(1)	秘密保持契約締結起案日 注：秘密保持契約の締結は、再認証申請受付日をもって行う。		(業)	有(　　情セ技第　号)・無
(2)	覚書締結起案日		(業)	有(　　情セ技第　号)・無
(3)	秘密保持契約書等送付日		(業)	保管日(　　)
7.4	4.4 申請料 と同様の手順に従う。			
(1)	申請料の請求 (財務部へ申請受付の連絡日)		(業)	免除等を行う理由 (　　)
(2)	必要経費の決定		(技)	決定・対象外
(3)	申請料納付の確認		(業)	納付日：
7.5	4.5 暗号モジュール認証要員の選任 と同様の手順に従う。			
(1)	認証要員選任日		(技)	認証要員名(　　)
(2)	認証要員の氏名を送信		(技)	試験機関へ電子メール
(3)	暗号モジュール認証申請受理通知書を作成し、技術管理者の印を押捺		(技)	様式 3-1（以下「認証申請受理通知書」という。）
(4)	認証申請受理通知書発送日		(業)	送付する
7.6	5.1 暗号アルゴリズム確認業務の実施 と同様の手順に従う。			
(1)	暗号アルゴリズム実装試験報告書受理日		(業)	電子メール送信日(　　)
(2)	暗号アルゴリズム確認業務及び暗号モジュール認証業務の継続についての運営審議委員会への付議の要否判断		(技)	必要(5.4 を実施)・不要
	運営審議委員会での認証の許諾等についての検討		(技)	開催日（　　）
	暗号アルゴリズム確認業務及び暗号モジュール認証業務の継続可否又は許諾可否の判断		(技)	継続可／許諾可 or 継続不可／許諾拒否 決定日(　　)
(3)	申請料の入金確認		(技)	納付済・未納付
(4)	既に暗号アルゴリズム確認書を発行しているか		(業)	未発行・発行済み
(5)	暗号アルゴリズム実装試験報告書調査日			適 or 不適(調査日)
	①記述に齟齬が無いか？		(認)	適・不適(　　)
	②暗号モジュール試験の要求事項に		(認)	適・不適(　　)

No.	項目	日付	担当者	摘要
	照らして、暗号アルゴリズム実装の構成要素と実装されている暗号アルゴリズムの関係が明確か？			
	③暗号モジュール試験の要求事項に照らして、開発に用いたツール及びツールのオプションは明確か？		(認)	適・不適(　　)
	④暗号アルゴリズムの依存性は満足されているか？		(認)	適・不適(　　)
	⑤確率的素数テストを用いるアルゴリズムについて、実装されている確率的素数テストの詳細について報告されているか？ また、暗号アルゴリズムの仕様に準拠していることを確認しているか？		(認)	適・不適(　　)
	⑥動作環境に問題が無いか？ 特に、暗号支援命令を使用している、動作環境にインストールされる特定の実行時環境を前提としているなどの事実は、動作環境の表記に反映されているか？		(認)	適・不適(　　)
	⑦ツールのバージョンが最新版か？		(認)	適・不適(　　)
	⑧試験結果が正当であるか？		(認)	適・不適(　　)
	⑨デグレードテストは実施されているか?		(認)	適・不適(　　)
	調査結果		(認)	適・不適 再提出指示日(　　)

	暗号アルゴリズム確認書作成日		(認)	暗号アルゴリズム確認書
	調査完了報告日		(認)	技術管理者へ
(6)	暗号アルゴリズム確認決裁日		(技)	決裁：適・否(差戻日　　)
(7)	暗号アルゴリズム確認書起案日		(業)	原議(　情セ技第　　号)
(8)	暗号アルゴリズム確認書発行日		(業)	写しの保管日(　　)
(9)	既発行暗号アルゴリズム確認書回収		(業)	回収日（　　）
(10)	暗号アルゴリズム確認書発送日		(業)	試験機関に送付

No.	項目	日付	担当者	摘要
(11)	試験機関に対して発送した旨送信日		(業)	申請者へ電子メール
(12)	暗号アルゴリズム確認登録簿登録日		(業)	暗号アルゴリズム毎に
(13)	暗号アルゴリズム確認登録簿公開日		(業)	機構ホームページで公開
7.7				
(1)	修正に関する調査日			適 or 不適(質問識別番号)
	a) 修正が暗号モジュール試験報告書 30%以下のアサーションしか影響を与えない場合			
	①変更点に関する記述があるか？		(認)	適・不適(　　)
	②最新の暗号モジュールセキュリティ要件、暗号モジュール試験要件及び「JCMVP 運用ガイダンス」が適用されているか？		(認)	適・不適(　　)
	③記述に齟齬が無いか？・同意の署名		(認)	適・不適(　　)
	④動作環境に問題が無いか？		(認)	適・不適(　　)
	⑤ツールのバージョンが最新版か？		(認)	適・不適(　　)
	⑥試験結果が正当であるか？		(認)	適・不適(　　)
	第 1 章		(認)	適・不適(　　)
	第 2 章		(認)	適・不適(　　)
	第 3 章		(認)	適・不適(　　)
	第 4 章		(認)	適・不適(　　)
	第 5 章		(認)	適・不適(　　)
	第 6 章		(認)	適・不適(　　)
	第 7 章		(認)	適・不適(　　)
	第 8 章		(認)	適・不適(　　)
	第 9 章		(認)	適・不適(　　)
	第 10 章		(認)	適・不適(　　)
	第 11 章		(認)	適・不適(　　)
	Appendix C		(認)	適・不適(　　)
	⑦正常系及び異常系のテストカバレッジが十分か		(認)	適・不適(　　)
	TE02.15.03			
	TE03.01.04			
	TE03.05.01			
	TE03.05.02			
	TE03.06.01			

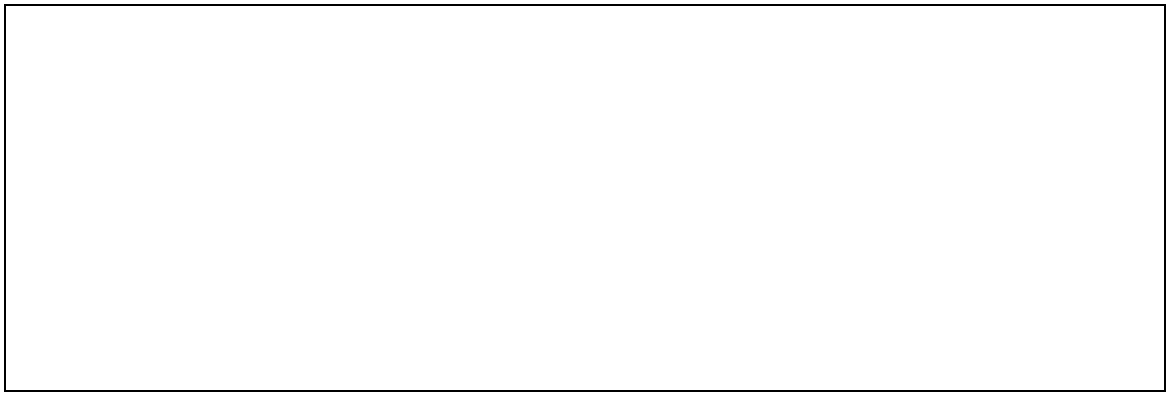
No.	項目	日付	担当者	摘要
	TE03.06.02			
	TE03.07.02			
	TE03.08.01			
	TE03.08.02			
	TE03.11.01			
	TE03.11.02			
	TE04.20.03			
	TE04.37.02			
	TE04.38.02			
	TE04.39.03			
	TE04.39.04			
	TE04.43.02			
	TE04.44.02			
	TE04.45.02			
	TE04.55.02			
	TE11.08.02			
	TE11.08.06			
	TE11.08.07			
	TE11.08.08			
	TE11.08.09			
	TE06.08.03			
	TE06.06.02			
	TE09.01.02			
	TE09.02.02			
	TE09.03.02			
	TE09.03.03			
	TE09.14.02			
	TE09.25.02			
	TE10.08.02			
	TE10.08.03			

	暗号モジュール認証書作成日		(認)	暗号モジュール認証書
	暗号モジュール認証報告書作成日		(認)	認証報告書
	b) 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場合			

No.	項目	日付	担当者	摘要
	①変更点に関する記述があるか？		(認)	適・不適(　　)
	② 最新の暗号モジュールセキュリティ要件、暗号モジュール試験要件及び「JCMVP 運用ガイダンス」が適用されていることか？		(認)	適・不適(　　)
	③記述に齟齬が無いか？		(認)	適・不適(　　)
	④試験機関の分析が正当であるか？		(認)	適・不適(　　)
	⑤物理的試験結果が正当であるか？		(認)	適・不適(　　)
(2)	調査完了報告日		(認)	技術管理者へ
	a)の場合、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作成		(認)	済・未・対象外
(3)	暗号モジュール再認証決裁日		(技)	決裁：適・否(差戻日　　)
	b)の場合、裏書も行う。		(技)	済・未・対象外
(4)	暗号モジュール認証書等起案日		(業)	原議(　情セ技第　　号)
(5)	暗号モジュール認証書等発行日		(業)	写しの保管日(　　)
(6)	暗号モジュール認証書等発送日		(業)	申請者に送付
(7)	申請者に対して発送した旨送信日		(業)	申請者へ電子メール
(8)	暗号モジュール認証製品リスト更新日		(業)	セキュリティポリシ及び申請者の情報等も登録
(9)	暗号モジュール認証製品リスト公開日		(業)	機構ホームページで公開
7.8	5.3 解釈等照会書の処理 と同様の手順に従う。			
(1)	暗号モジュール所見報告書受理日		(技)	受理(識別番号　　)・不受理(理由　　)
(2)	暫定処置検討会議開催日		(技)	認証要員と会議
(3)	暗号モジュール所見報告書送付日		(技)	試験機関へ送付
(4)	技術審議委員会での問題点解決日		(技)	運用ガイダンス発行日( )
(5)	セキュリティ要件等の変更手続開始日		(技)	必要に応じて

注）表の網掛けの部分は、暗号モジュール技術管理者が担当する部分を表す。

＜特記事項＞



様式 4-2

保証継続事前レビュー受付簿

識別情報	事前レビュー受付番号	
	受付番号	
	保証継続申請者名称 連絡担当者(TEL　)	
	暗号モジュール名称 バージョン	

No.	項目	日付	担当者	摘要
8.1				
(1)	事前レビューの受付		(業)	事前レビュー内容の確認
(2)	本表冒頭の識別情報欄に事前レビュー受付番号、申請者名称等を記入		(業)	
(3)	事前レビュー受付番号及び受付日を送信		(業)	申請者に送信
(4)	認証要員選任日		(技)	認証要員名(　　)
	認証要員の氏名を送信		(技)	申請者へ電子メール
(5)	暗号モジュール影響分析報告書の内容を確認		(認)	適・不適(　　)
(6)	保証継続の申請が適当と判断できない又は適当ではないと判断した場合には、結果と理由を連絡		(認)	申請者へ電子メール or 対象外
	サーベイランスの実施要否を判断		(認)	必要・不要
(7)	保証継続の申請が適当と判断した場合は、保証継続申請可能と連絡		(認)	申請者へ電子メール or 対象外
8.2				
(1)	暗号モジュール認証申請受付		(業)	認証申請内容の確認
	受領書類の確認日			確認日（　　） or 不適(再提出指示日)
	① 暗号モジュール認証申請書		(業)	適・不適(　　)
	② 同意書		(業)	適・不適(　　)
	③ 事前レビューを受けた暗号モジュール影響分析報告書		(業)	適・不適(　　)

No.	項目	日付	担当者	摘要
	その他(　　)		(業)	適・不適(　　)
(2)	受付番号欄に受付番号を記入		(業)	認証申請書に記入
(3)	暗号モジュール認証申請受付簿記入		(業)	様式 1-1
(4)	本表冒頭の識別情報欄に受付番号、暗号モジュール名称等を記入		(業)	
(5)	受付番号及び受領書類リストを送信		(業)	申請者に送信
8.3	4.3 秘密保持契約の締結 と同様の手順に従う。			
(1)	秘密保持契約締結起案日 注 : 秘密保持契約の締結は、保証継続申請受付日をもって行う。		(業)	有(　情セ技第　号)・無
(2)	覚書締結起案日		(業)	有(　情セ技第　号)・無
(3)	秘密保持契約書等送付日		(業)	保管日(　　)
8.4	4.4 申請料 と同様の手順に従う。			
(1)	申請料の請求 (財務部へ申請受付の連絡日)		(業)	免除等を行う理由 (　　)
(2)	必要経費の決定		(技)	決定・対象外
(3)	申請料納付の確認		(業)	納付日 :
8.5				
(1)	修正に関する調査日			適 or 不適(質問識別番号)
	①変更点に関する記述があるか？	a)	(認)	適・不適(　　)
	②記述に齟齬が無いか？	a)	(認)	適・不適(　　)
	③試験機関の分析が正当であるか？	a)	(認)	適・不適(　　)
(2)	調査完了報告日		(認)	技術管理者へ
	暗号モジュール認証書及び保証継続報告書を作成		(認)	済・未
(3)	暗号モジュール認証保証継続決裁		(技)	決裁 : 適・否(差戻日　)
	暗号モジュール影響分析報告書に裏書も行う		(技)	済・未
(4)	暗号モジュール認証書等起案日		(業)	原議(　情セ技第　号)
(5)	暗号モジュール認証書等発行日		(業)	写しの保管日(　　)
(6)	暗号モジュール認証書等発送日		(業)	申請者に送付
(7)	申請者に対して発送した旨送信日		(業)	申請者へ電子メール

No.	項目	日付	担当者	摘要
(8)	暗号モジュール認証製品リスト 更新日		(業)	セキュリティポリシ及び 申請者の情報等も登録
(9)	暗号モジュール認証製品リスト 公開日		(業)	機構ホームページで公開
8.6	5.3 解釈等照会書の処理 と同様の手順に従う。			
(1)	暗号モジュール所見報告書受理日		(技)	受理(識別番号)・ 不受理(理由)
(2)	暫定処置検討会議開催日		(技)	認証要員と会議
(3)	暗号モジュール所見報告書送付日		(技)	試験機関へ送付
(4)	技術審議委員会での問題点解決日		(技)	運用ガイダンス発行日( )
(5)	セキュリティ要件等の変更手続開始日		(技)	必要に応じて

注）表の網掛けの部分は、暗号モジュール技術管理者が担当する部分を表す。

＜特記事項＞

様式 5

内部監査是正処置報告書

年　月　日

（統括責任者名）　殿

品質システム責任者名

暗号モジュール認証業務管理要領に基づき、下記のとおり、内部監査の結果、指摘された事項に対する是正処置の結果を取りまとめましたので報告します。

記

１．監査実施の概要

⑴ 実施日

⑵ 対象部署

⑶ 監査員

２．指摘事項に対する処置の概要と所見

３．処置の詳細（是正処置、予防処置及び提言への対応）

以上

様式 6

マネジメント・レビュー記録書

マネジメント・レビュー実施日	年　　月　　日
マネジメント・レビュー参加者	
統括責任者	
マネジメントシステム責任者	
暗号モジュール技術管理者	
その他	
報告事項	報告内容
① 業務報告及び決算報告	
② 内部監査実施報告	
③ 是正処置・予防処置報告	
④ 苦情等に関する報告	
⑤ 教育・訓練実施報告、暗号モジュール認証要員業務査定報告	
⑥ 適用セキュリティ要件等の改正状況	
⑦ 現行の人的および設備資源の妥当性	
⑧ その他、マネジメントシステムの確保に必要な事項	
統括責任者の指摘事項：	
上記指摘事項に対する予防処置・是正処置・不適合処置報告書番号：	

様式 7

予防処置報告書

予防処置報告書番号	
不適合の潜在的原因発見日	年　　月　　日
不適合の潜在的原因発見者	
不適合の潜在的原因	
処置期限	年　　月　　日まで
予防処置の実施者	
不適合の潜在的原因への対策	
結果	
備考	
予防処置確認日	年　　月　　日
マネジメントシステム責任者	

様式 8

不適合処置報告書

不適合処置報告書番号	
不適合の発見日	年　　月　　日
不適合の発見者	
不適合の内容	
不適合処置責任者	
不適合業務の一時的な停止日	年　　月　　日
不適合の原因	
不適合の容認の可能性の決定	容認可・不可
不適合の原因への対策	
不適合事項の修正結果	
過去の結果の回収	回収しない・回収する(回収実施日：　　)
業務の再開日	年　　月　　日
備考	
不適合処置確認日	年　　月　　日
マネジメントシステム責任者	

様式 9

是正処置報告書

是正処置報告書番号	
是正処置の種別	① 不適合が再発しうる ② 適合性に疑いがある
原因の発見日	年　　月　　日
原因の内容	
原因の発生元	
原因調査依頼先	
原因調査報告日	年　　月　　日
原因調査報告内容	
是正処置の必要性の決定	必要・不必要
是正処置指示日	年　　月　　日
原因発生元の責任者	
原因の除去の方策	
再発防止処置内容	
遡及処置内容	
備考	
是正処置確認日	年　　月　　日
マネジメントシステム責任者	

様式 10

苦情等受付票

苦情等受付票番号	
苦情等受付日	年　　月　　日
苦情等受付者	
苦情等の種別	苦情・異議申し立て
苦情等の申し立て者 名称： 住所： 担当者： 連絡先： e-mail アドレス：	
苦情等の内容	

様式 11

苦情等処理報告書

苦情等処理報告書番号	
苦情等受付票番号	
苦情等受付日	年　　月　　日
苦情等受付者	
苦情等の種別	苦情・異議申し立て
苦情等の申し立て者	
苦情等の内容	
苦情等処理指示日	年　　月　　日
苦情等処理担当者	
苦情等の調査	①　申し立ての内容が正当であり、原因が認証機関にある ②　申し立ての内容が正当であり、原因が認証機関にない ③　申し立ての内容が事実無根である
苦情等処理の必要性の決定	必要・不必要
苦情等の原因	
原因除去依頼日	年　　月　　日
原因発生元の責任者	
原因の除去の方策等 苦情等に対する処理内容	
備考	
苦情等処理確認日	年　　月　　日
マネジメントシステム責任者	

様式 12

マネジメントシステム文書管理表

年　月　日

識別番号	名称	最新版制定年月日	公開・非公開

様式 13

秘密資料管理簿

受付番号：

申請者名：

暗号モジュールの名称：

管理担当者：

識別子	秘密資料名	媒体形式	入手日	消去・返却日	返却確認日

注：秘密情報を消去した場合、返却確認日の欄に“/”を記入すること。

様式 14

秘密資料持出管理簿

受付番号：
申請者名：
暗号モジュールの名称：
管理担当者：

識別子	秘密資料名	持出者	持出場所	持出日	返却日

様式 17

サーベイランス実施通知書

(申請者名称)
(責任者名)　様

独立行政法人 情報処理推進機構
セキュリティセンター
（マネジメントシステム責任者名）

■サーベイランス対象となる暗号モジュール
認証番号：
名称：
バージョン：

■サーベイランスの背景
認証番号 XXXXX の暗号モジュールについて、以下のような、要求事項に対する不適合の懸念があるという指摘を XXXX から受けました。
●
●

■サーベイランスの目的
認証番号 XXXXX の暗号モジュールが、暗号モジュールのセキュリティ要求事項を満たす実装となっているのかどうかを確認するためのサーベイランスを実施致します。

■サーベイランスの内容
暗号モジュールのセキュリティ要求事項への不適合につながる上記のような実装となっているのかどうかを確認致します。
具体的に、次の観点での報告を求めます。
- 観点 1
- 観点 2
- …
- 観点 n

以上

様式 18

サーベイランス実施結果報告書

報告日：　　年　　月　　日

実施日		年　　月　　日
実施チーム		○○　○○(チームリーダ)、 ○○　○○、 ○○　○○
実施場所		
立ち会い者		
サーベイランス対象 暗号モジュール	名称	
	バージョン	

■苦情

苦情内容		
懸念		
関連 AS		
関連 TE		
サーベイランス実施内容	観点 1	
	観点 2	
再試験の要否判定及びその理由		

様式 19

再試験指示書

(申請者名称)
(責任者名)　様

独立行政法人 情報処理推進機構
セキュリティセンター
（マネジメントシステム責任者名）

御社より暗号モジュール認証申請を受け、暗号モジュール認証を授与した下記の暗号モジュールについて、セキュリティ要件等への適合性が疑われる下記事象の報告がありました。

これを受けて、　　年　　月　　日にサーベイランスを実施し、その結果、下記のとおり再試験を要すると判断いたしました。つきましては、「暗号モジュール認証申請手続等に関する規程」(CBM-02)の「13.再試験」に基づいて、本再試験指示書を発行いたします。本書の内容をご確認いただき、試験機関と協議の上、再試験を実施してください。また、再試験が完了するまでの間、暗号モジュール認証は一時停止されますので、当該暗号モジュールを認証済みであるとして供給しないで下さい。

― 記 ―

1. 暗号モジュール識別
1.1 暗号モジュール認証申請受付番号：
1.2 暗号モジュール名称：
1.3 認証番号：　　XXXXX
1.3 認証日：　　年　　月　　日

2. 事象

3. 再試験を要する理由
3.1 理由 1：
以上から、当該暗号モジュールは、暗号モジュールのセキュリティ要求事項を満たしておらず、暗号モジュールを修正の上、再試験の必要があると判断いたしました。

3. 再試験指示日：　　年　　月　　日

4. 再試験終了期限：　　再試験指示日から 1 年後

以上

様式 20

年　　月　　日

(申請者名称)

(責任者名)　様

独立行政法人 情報処理推進機構

（理事長名）

暗号モジュール認証取消通知書

暗号モジュール認証申請手続等に関する規程(CBM-02)「14.2 暗号モジュール認証の取消」の　　に基づき、　　年　　月　　日に下記の認証を取消したことを通知します。

― 記 ―

暗号モジュールの名称：

バージョン：

認証番号：

申請者：

認証年月日：　　年　　月　　日

認証取消日：　　年　　月　　日

以上

別表 1

管理する外部文書一覧

文書種類	識別子	発行年	名称
JIS	JIS Q 0065	1997	製品認証機関に対する一般要求事項
JIS	JIS Q 17025	2005	試験所及び校正機関の能力に関する一般要求事項
JIS	JIS X 19790:2007	2007	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
JIS	JIS X 19790:2007 /Amd.1:2009	2009	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 （追補 1）
JIS	JIS X 24759:2009	2009	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
JIS	JIS Q 17065:2012	2012	適合性評価―製品, プロセス及びサービスの認証を行う機関に対する要求事項
JIS	JIS X 19790:2015	2015	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
JIS	JIS X 24759:2017	2017	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
JIS	JIS Q 17025:2018	2018	試験所及び校正機関の能力に関する一般要求事項
ISO	ISO/IEC 19790	2006	Security requirements for cryptographic modules
ISO	ISO/IEC 19790:2006/Cor.1:2008	2008	Information technology — Security techniques — Security requirements for cryptographic modules TECHNICAL CORRIGENDUM 1
ISO	ISO/IEC 24759:2008	2008	Information technology — Security techniques — Test requirements for cryptographic modules
ISO	ISO/IEC 19790:2012	2015	Security requirements for cryptographic modules
ISO	ISO/IEC 24759:2017	2017	Information technology — Security techniques — Test requirements for cryptographic modules

改正履歴

識別番号	CBM-01-A

改正年月日	作成者・承認者	改正内容
平成 18 年 10 月 30 日	上野・仲田	新規制定
平成 19 年 10 月 1 日	上野・占部	一部改正
平成 19 年 11 月 14 日	櫻井・占部	一部改正
平成 20 年 5 月 2 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 22 年 8 月 17 日	櫻井・仲田	一部改正
平成 22 年 9 月 27 日	櫻井・仲田	一部改正
平成 23 年 12 月 21 日	櫻井・仲田	一部改正
平成 29 年 4 月 10 日	橋本・頓宮	一部改正
平成 30 年 6 月 28 日	櫻井・江口	一部改正
令和 2 年 11 月 9 日	神田・戸高	一部改正