暗号モジュール認証申請手続等に関する規程

令和 2 年 10 月 16 日

IPA

CBM-02

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 19 号
最終改正　令和 2 年 10 月 16 日　2020 情総第 1126 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、申請者が暗号モジュール認証を得るための手順及び手続を定めることを目的とします。

２．用語及び定義

本規程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の例によります。

３．試験及び認証の規格

３．１ セキュリティ要件等

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。

３．２ 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、十分な周知期間をおいて予告されます。なお、この変更は、暗号モジュール認証申請中及び暗号アルゴリズム確認申請中のものに対しても、新たなセキュリティ要件等が公開された後の並立期間が終了した後に適用されます。また、既に認証を行った暗号モジュール、及び確認を行った暗号アルゴリズム実装については、適用猶予期間が経過した後に適用されます。

４．暗号モジュール認証申請前及び暗号アルゴリズム確認申請前の要求事項

４．１ 遵守すべき事項

(1) 申請者は、暗号モジュール認証の申請から許諾後、並びに暗号アルゴリズム確認の申請から許諾後にわたって、***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) 申請者は、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、認証機関に事前相談をしなければなりません。

４．２ 暗号モジュール認証申請及び暗号アルゴリズム確認申請に関する情報

申請者は、暗号モジュール認証申請及び暗号アルゴリズム確認申請に係る申請等の手続きを行うために必要な情報を、機構の Web ページから取得することができます。

４．３ 暗号モジュール認証申請準備の手順

申請者は、暗号モジュール認証申請に先立って、次に掲げる事項を準備する必要があります。

（1）暗号モジュールの決定

暗号モジュール試験を受ける暗号モジュールを特定し、暗号境界を明確にします。また、取得予定のセキュリティレベルを決定します。

（2）試験用提供物件の準備

申請者は、暗号モジュール試験に必要な試験用提供物件を、準備する必要があります。試験用提供物件には、次のものが含まれます。

a) 暗号モジュール（ハードウェア暗号モジュールの場合、物理的セキュリティに関する試験を実施するために必要な個数を用意しなければなりません。）

b) 公開セキュリティポリシ（ブロック図及び必要に応じて、暗号モジュールの写真を、セキュリティポリシに掲載する必要があります。また、このセキュリティポリシは、暗号モジュール認証取得後に公開されます。）

c) ***制度基本規程***の***附属書 A*** に掲げた***暗号モジュール試験要件***のうち、VE として識別される要件に対応するベンダ証拠資料

d) 状態遷移図及び状態遷移表

e) ソースコードを含め、暗号モジュール試験をサポートするドキュメント類

（3）試験機関の選定

申請者は、認証機関が公開する「暗号モジュール試験機関リスト」の中から暗号モジュール試験を依頼する試験機関を決定してください。また、選定した試験機関から「暗号モジュール試験実施計画書」等の提示を受け、その内容の妥当性を判断し、試験機関と暗号モジュール試験の実施に関する契約の締結をして下さい。

（4）申請前の事前相談

本制度での暗号モジュール認証実績がない場合、認証機関に事前相談の申し込みをメールで行ってください。

４．４ 暗号アルゴリズム確認申請準備の手順

申請者は、暗号アルゴリズム確認申請に先立って、次に掲げる事項を準備する必要があります。

(1) 暗号アルゴリズムの決定

暗号アルゴリズム実装試験の対象となる暗号アルゴリズム実装を特定し、その暗号アルゴリズム実装の境界を明確にします。その特定にあたっては、実装されている暗号アルゴリズムを、本制度の承認されたセキュリティ機能とそうでないセキュリティ機能とに整理します。

(2) 試験用提供物件の準備

申請者は、暗号アルゴリズム確認に必要な試験用提供物件を、準備する必要があります。試験用提供物件には、次のものが含まれます。

a) 暗号アルゴリズム実装

b) 暗号アルゴリズム実装試験をサポートするドキュメント類（機能仕様書、インタフェース仕様書等の情報を準備する必要があります。）

c) 暗号アルゴリズム実装に関するドキュメント類（暗号アルゴリズム実装の依存性、機能分割、及び使用する暗号支援命令に関する情報を準備する必要があります。）

d) 設計保証に関するドキュメント類（暗号アルゴリズム確認を再利用する目的で、ハードウェアの場合、プロセスルール、フロアプラン、配置配線、論理合成等に関する情報、ソフトウェア又はファームウェアの場合、ビルドオプション、呼出規約、実行時環境等に関する情報を準備する必要があります。適切な情報を提供しない場合、暗号アルゴリズム確認の再利用は認められません。）

(3) 試験機関の選定

申請者は、認証機関が公開する「暗号モジュール試験機関リスト」の中から暗号アルゴリズム確認を依頼する試験機関を決定してください。また、選定した試験機関から「暗号アルゴリズム実装試験実施計画書」等の提示を受け、その内容の妥当性を判断し、試験機関と暗号アルゴリズム確認の実施に関する契約の締結をして下さい。

(4) 申請前の事前相談

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、認証機関に事前相談の申し込みをメールで行ってください。

５．暗号モジュール認証申請時及び暗号アルゴリズム確認申請時の要求事項

５．１ 使用する言語

本制度で使用する言語は、原則日本語とします。申請者の提出書類、申請手続及び認証機関との連絡に使用する言語は、日本語又は英語とします。法人格を証明する書類等の原文が日本語又は英語のいずれでもない場合は、原文に加えて、日本語訳又は英語訳を提出しなければなりません。日本語訳又は英語訳のいずれかの提出がない場合、認証機関は、申請者からの暗号モジュール認証申請又は暗号アルゴリズム確認申請を受け付けません。

５．２ 暗号モジュール認証申請及び暗号アルゴリズム確認申請の手順

申請者は、申請に必要な書類を各 1 部作成し認証機関に提出しなければなりません。
申請に必要な書類は、次のとおりです。

① 本申請に関して権限及び責任を有する者（以下「申請責任者」という。）が署名又は押印した「暗号モジュール認証申請書」（様式 1-1）又は「暗号アルゴリズム確認申請書」（様式 1-2）。

② 法人格を証明できる書類（発行日から 6 ヶ月以内かつ最新な書類の原本。6 ヶ月以内に、公的な機関が発行した正式な書類を提出していて、内容に変更がない場合には、その写しを提出してください。また、同日に複数申請を行う場合、2 件目以降は添付する必要はありません。）

③ 「同意書」（様式 2）

５．３ 秘密保持契約の締結

認証機関は、試験機関と包括的な秘密保持契約を結びますが、必要に応じて、申請者は、申請責任者が署名又は押印した「秘密保持契約書」（様式 9）を 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するように、認証機関に対して要請することができます。

５．４ 暗号モジュール認証及び暗号アルゴリズム確認の申請料

認証機関は、申請の受付後、別表に定める暗号モジュール認証又は暗号アルゴリズム確認の申請手数料及び旅費等の必要経費を合計した申請料の請求書を発行します。申請者は、請求書を受領したときは、速やかに、指定の口座へ申請料を入金して下さい。なお、一旦納付された申請料は、理由いかんを問わず、返金されません。
また、申請料が振り込まれない限り、認証機関は、実質的な作業に着手する義務を負いません。請求書に定める納付期限を過ぎても指定の口座に振り込まない場合、認証機関は申請者が当該申請を取り下げたものとみなし、取下げの手続を行います。

６．暗号モジュール認証申請又は暗号アルゴリズム確認申請の却下

以下のいずれかに該当する場合、暗号モジュール認証申請又は暗号アルゴリズム確認申請は却下される場合があります。

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 制度基本規程の 2.2.1 に該当しない法人等からの申請であって、運営審議委員会にて申

請受理が相当との助言がなされなかった場合

⑤ 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の場合であって、運営審議委員会にて申請不受理が相当との助言がなされた場合

⑥ 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

⑦ 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場合

⑧ 認証された暗号モジュールや確認された暗号アルゴリズム実装に係る必要な届出を怠った場合

⑨ 暗号モジュール認証又は暗号アルゴリズム確認が許諾された申請者（以下「認証被許諾者」という。）としての変更の届出を怠った法人等の場合（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）

⑩ 認証された暗号モジュールや確認された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

⑪ 天災その他やむを得ない事由がある場合

７．暗号モジュール認証及び暗号アルゴリズム確認申請後に行うべき事項

７．１ 試験機関の指摘事項への対応

申請者は、試験機関が***セキュリティ要件等***に基づき暗号モジュール試験作業並びに暗号アルゴリズム確認作業を実施する段階において、次に掲げる事項に対応する必要があります。

(1) 申請者は、試験機関又は認証機関から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情報の提供及び対応を要請された場合は、速やかに対処する必要があります。この対応には、暗号アルゴリズム実装試験を内包する暗号モジュール試験の実施において、試験機関による現認又は申請者による不正を行っていないことへの誓約を含みます。

(2) 申請者は、暗号モジュール試験における問題点を記した「暗号モジュール所見報告書」が、試験機関により発行された場合、速やかに問題の解決を図ってください。

(3) 申請者は、「暗号モジュール所見報告書」により指摘された問題の解決策及びその実施予定を「暗号モジュール所見報告書」に追記して、試験機関に提出する必要があります。

(4) 申請者は、「暗号モジュール所見報告書」の指摘事項に対応するために、当初の「暗号モジュール試験実施計画書」の内容を大幅に変更する必要が生じた場合は、試験機関と計画の見直しに係る協議を実施の上、解決を図らなければなりません。

(5) 申請者は、指摘された問題の解決に必要な処置が、***セキュリティ要件等***又は認証制度に関する場合は、認証機関の指示に従わなければなりません。

７．２ 暗号アルゴリズム確認書の受領

暗号アルゴリズム確認の申請者は、認証機関が発行した暗号アルゴリズム確認書（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。）様式 1）を原則として試験機関を経由して受領します。

７．３ 暗号モジュール試験報告書の確認

申請者は、試験機関が発行する暗号モジュール試験報告書の内容について、試験機関より照会があった場合、その内容を確認してください。申請者は、不正確な内容又は事実の誤認があると判断する場合、試験機関と協議して必要な対応をとる必要があります。

７．４ 暗号モジュール認証書等の受領

申請者は、認証機関が発行した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）を受領します。

８．暗号モジュール認証又は暗号アルゴリズム確認の認証拒否等

以下のいずれかに該当する場合、暗号モジュール認証又は暗号アルゴリズム確認に関する認証業務の継続中止、認証の許諾拒否又は取消等が行われる場合があります。

① 暗号アルゴリズム実装試験報告書の内容に問題がある場合で、かつ補正が行われる見込みがないと判断された場合

② 暗号モジュール試験報告書の内容に問題がある場合で、かつ補正が行われる見込みがないと判断された場合

③ 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であって、運営審議委員会にて認証業務の継続又は認証の許諾が不適当との助言がなされた場合

９．暗号モジュール認証等を許諾された申請者の責務

認証被許諾者は、次の事項を遵守する必要があります。

（1）認証被許諾者は、暗号モジュールを認証済であるとして供給するときは、認証機関から発行された暗号モジュール認証書及び暗号モジュール認証報告書で識別された暗号モジュールを、認証された条件の下で供給しなければなりません。認証された暗号モジュール以外の暗号モジュールあるいは製品等に対して、「暗号モジュール認証取得製品シリーズ」、「暗号モジュール認証取得製品と同等又は相当」といった、誤解を招くような宣伝・広告・表示等を行ってはなりません。

（2）認証された暗号モジュールに改変等を加えた後続バージョン（以下「後続暗号モジュ

ール」という。）を認証された暗号モジュールとして引き続き市場に供給したい場合には、当該後続暗号モジュールに対して再認証又は保証継続、もしくは新たに認証を取得する必要があります。再認証、保証継続又は新たな認証を取得する以前に、当該後続暗号モジュールを認証された暗号モジュールとして市場に供給してはなりません。

(3) 認証被許諾者は、暗号アルゴリズム確認書又は「暗号アルゴリズム確認登録簿」に記載された事項、暗号モジュール認証書又は「認証製品リスト」に記載された事項、その他、認証された暗号モジュールの品質に影響を与える可能性がある事項に変更が生じたときは、遅滞なく、その変更を認証機関に届け出なければなりません。

（例）

- 法人としての法律上、商業上、組織上の地位又は所有権の変更
- 組織内部又は経営層（特に認証された暗号モジュールに係る主要な担当部署の部門責任者）における重大な変更
- 認証された暗号モジュール又は確認された暗号アルゴリズム実装に係る担当部署の所属又は連絡先等の変更
- 製品又は生産方法、あるいは生産する事業所等の変更
- 品質マネジメントシステムの重大な変更

(4) 認証被許諾者は、１７．に定める認証された暗号モジュールについてのセキュリティに関する苦情の全てを記録しなければなりません。

(5) 認証被許諾者は、認証された暗号モジュールが、本制度の要件に適合していない可能性を示す何らかの情報を得た場合は、遅滞なく、その旨を認証機関に報告しなければなりません。認証被許諾者が暗号モジュール認証の継続を望む場合、当該報告の結果、認証機関から何らかの指示があった場合には、その指示に従わなければなりません。これには、認証機関からサーベイランス又は再試験の指示があった場合には、試験機関にサーベイランス又は再試験を依頼するとともに、それに係る費用を負担することを含みます。

１０．認証された暗号モジュールの再認証

再認証は、後続暗号モジュールに対して、改変等が次のいずれかに該当する場合に、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するものです。なお、改変等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ない場合には、１１．に定める保証継続の申請を行ってください。

a) 改変等が、暗号モジュール試験報告書に記載されている 30%以下の個別要件しか影響を与えない場合

b) 改変等が、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

１０．１ 再認証の準備

（1）再認証申請者は、再認証の申請に先立って、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します。再認証申請者は、試験機関から「暗号モジュール試験実施計画書」等の提示を受け、その内容の妥当性を判断し、試験機関と再認証に係る暗号モジュール試験の実施に関する契約の締結をして下さい。

（2）再認証申請者は、暗号モジュール試験の実施後に、試験機関から、上記 a）の場合は変更箇所に関連する暗号モジュール試験報告書を入手してください。上記 b）の場合は「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」を入手してください。

（3）暗号モジュール試験の結果、上記の a）又は b）に該当しないことが判明した場合、再認証の申請はできません。新しい暗号モジュールとして暗号モジュール認証申請を新規に行う必要があります。

１０．２ 再認証の申請

再認証申請者は、再認証に伴う暗号モジュール認証申請を行うにあたり、認証機関に対して、次の書類を各 1 部提出しなければなりません。

① 申請責任者が署名又は押印した「暗号モジュール認証申請書」（様式 1-1）。

② 「同意書」（様式 2）

③ １０．１（2）で入手した書類一式

１０．３ 再認証に伴う秘密保持契約の締結

認証機関は、試験機関と包括的な秘密保持契約を結びますが、必要に応じて、再認証申請者は、申請責任者が署名又は押印した「秘密保持契約書」（様式 9）を 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するように、認証機関に対して要請することができます。

１０．４ 再認証に伴う申請料

認証機関は、申請の受付後、別表に定める暗号モジュール認証又は暗号アルゴリズム確認申請手数料及び旅費等の必要経費を合計した申請料の請求書を発行します。再認証申請者は、請求書を受領したときは、速やかに、指定の口座へ申請料を入金して下さい。なお、一旦納付された申請料は、理由いかんを問わず、返金されません。

また、申請料が振り込まれない限り、認証機関は、実質的な作業に着手する義務を負いません。請求書に定める納付期限を過ぎても指定の口座に振り込まない場合、認証機関は再

認証申請者が当該申請を取り下げたものとみなし、取下げの手続を行います。

１０．５ 再認証に伴う暗号モジュール認証の許諾

認証機関は、試験機関から提出された再認証に伴う書類を精査し、内容確認を経て、適切であると判断した場合、後続暗号モジュールに対して暗号モジュール認証の再認証を認めます。

(1) 認証機関は、更新された情報及び更新された「セキュリティポリシ」を「暗号モジュール認証製品リスト」に再登録して公開します。

(2) 上記 a）の場合、再認証申請者は、認証機関が発行した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受領します。

(3) 上記 b）の場合、再認証申請者は、試験機関が作成した「物理的変更分析報告書」に、認証機関が裏書したものを受領します。

１１．認証された暗号モジュールの保証継続

保証継続は、後続暗号モジュールに対して、改変等が***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ないときに、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するものです。

１１．１ 保証継続の準備

保証継続申請者は、保証継続の申請に先立って、以下の準備を行う必要があります。

(1)「暗号モジュール影響分析報告書」（様式 11）の作成

保証継続申請者は、当該後続暗号モジュールが***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」を作成します。

(2)「暗号モジュール影響分析報告書」の事前レビュー

保証継続申請者は、「暗号モジュール影響分析報告書」をもとに、保証継続の妥当性を確認するための事前検討を認証機関に依頼しなければなりません。「暗号モジュール影響分析報告書」の内容について質問がある場合、不足がある場合又は問題がある場合には、認証機関から質問事項又は指摘事項を通知しますので、速やかに対応し、必要に応じて「暗号モジュール影響分析報告書」の内容を修正してください。

１１．２ 保証継続の申請

保証継続申請者は、保証継続に伴う暗号モジュール認証申請を行うにあたり、認証機関に対して、次の書類を各 1 部提出しなければなりません。なお、事前レビューの結果、保証継続の申請が可能と通知を受けた場合に限り、保証継続の申請ができます。

① 申請責任者が署名又は押印した「暗号モジュール認証申請書」（様式 1-1）
② 「同意書」（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」（様式 11）

１１．３ 保証継続に伴う秘密保持契約の締結

必要に応じて、保証継続申請者は、申請責任者が署名又は押印した「秘密保持契約書」（様式9)を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するように、認証機関に対して要請することができます。

１１．４ 保証継続に伴う申請料

認証機関は、申請の受付後、別表に定める暗号モジュール認証又は暗号アルゴリズム確認申請手数料及び旅費等の必要経費を合計した申請料の請求書を発行します。保証継続申請者は、請求書を受領したときは、速やかに、指定の口座へ申請料を入金して下さい。なお、一旦納付された申請料は、理由いかんを問わず、返金されません。
また、申請料が振り込まれない限り、認証機関は、実質的な作業に着手する義務を負いません。請求書に定める納付期限を過ぎても指定の口座に振り込まない場合、認証機関は保証継続申請者が当該申請を取り下げたものとみなし、取下げの手続を行います。

１１．５ 保証継続検査の実施

保証継続申請者は、認証機関から必要な情報の提供及び確認等、並びに「暗号モジュール影響分析報告書」の修正を求められた場合は速やかに対応する必要があります。

１１．６ 保証継続報告書の確認

保証継続申請者は、認証機関が作成した「保証継続報告書（案)」の内容について確認し、不正確な内容又は事実の誤認があると判断する場合は、認証機関にその旨を指摘することができます。

１１．７ 保証継続に伴う暗号モジュール認証の許諾

認証機関は、保証継続申請者から提出された保証継続に伴う書類を精査し、内容確認を経て、適切であると判断した場合、後続暗号モジュールに対して暗号モジュール認証の保証継続を認めます。

(1) 認証機関は、更新された情報及び更新された「セキュリティポリシ」を「暗号モジュール認証製品リスト」に再登録して公開します。
(2) 保証継続申請者は､認証機関が発行した暗号モジュール認証書及び｢保証継続報告書｣、並びに「暗号モジュール影響分析報告書」に裏書を施したものを受領します。

１２．サーベイランス

(1) 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、認証機関が、サーベイランスを行いますので、認証被許諾者は、サーベイランス、再試験などの実施のために必要な、暗号モジュールの提供、文書の調査、全ての場所への立ち入り、記録の閲覧、担当者等の面接のための準備等を含め、認証機関が行う業務の実施に必要な準備を全て行わなければなりません。

a) 認証された暗号モジュールの利用者、試験機関の要員、又はその他関係者からの苦情又は情報提供等により、暗号モジュールの***セキュリティ要件等***への適合性に疑義が生じたとき。

b) 認証された暗号モジュールの再認証又は保証継続の検査の過程で、認証された暗号モジュールのセキュリティ要件等への適合性に疑義が生じたとき。

c) 事業の承継等があった場合に、認証機関が必要と認めたとき。

d) その他、認証機関が必要と認めたとき。

(2) サーベイランスを実施する場合は、認証機関から認証被許諾者に対し、その目的及び内容等を文書により通知します。

(3) 当該通知を受けた認証被許諾者は、サーベイランスを受け入れなければなりません。サーベイランスを拒否した場合、暗号モジュール認証等の取消が行われる場合があります。

(4) 認証被許諾者は、サーベイランスが円滑に実施できるよう認証機関に協力しなければなりません。

(5) サーベイランスに係る費用は、認証機関が独自に負担するものを除き、認証被許諾者の負担とします。

１３．再試験

(1) 認証機関が、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、再試験を要すると認めた場合は、「再試験指示書」を発行しますので、認証被許諾者は、その内容に基づき、試験機関と協議の上、再試験を実施して下さい。

(2) 再試験を拒否した場合、暗号モジュール認証等の取消が行われる場合があります。

(3) 再試験に係る費用は、認証被許諾者の負担とします。

１４．暗号モジュール認証等の一時停止及び取消

１４．１ 暗号モジュール認証等の一時停止

(1) 次に該当する場合、当該暗号モジュール認証又は当該暗号アルゴリズム確認の一時停

止が認証機関から公表されます。

a) 再試験の実施が決定された場合

b) 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

c) 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、認証機関から認証被許諾者に是正要求が出された場合

(2) 認証機関からの一時停止の公表後、一時停止が解除されるまでの期間、認証被許諾者は、当該暗号モジュールを認証済として、又は当該暗号アルゴリズム実装を確認済として供給してはなりません。

１４．２ 暗号モジュール認証の取消

(1) 次に該当する場合、認証機関が、暗号モジュール認証を取消して「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に関する情報を削除しますので、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してはなりません。

a) 認証被許諾者が、１２．に記載されているサーベイランス又は１３．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）

b) 再試験の指示から 1 年以内に再試験が完了しない場合

c) 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

d) 本規程に定める「同意書」（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

e) 不正な手段により暗号モジュール認証を受けた場合

f) 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

g) 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

h) 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

j) 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) 認証被許諾者は、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」、「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）を認証機関に遅滞なく返納して下さい。

１５．暗号モジュール認証に関するその他の手続

１５．１ 英文暗号モジュール認証書等発行申請の手続

（1） 認証被許諾者は、「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）の発行申請を行う場合、「英文暗号モジュール認証書等発行申請書」（様式 8）を認証機関に提出する必要があります。

（2） 認証被許諾者は、別表に定める英文暗号モジュール認証書等発行申請手数料の請求書を認証機関から受領したときは、速やかに、指定の口座へ申請料を入金して下さい。なお、一旦納付された申請料は、理由いかんを問わず、返金されません。

１５．２ 暗号モジュール認証申請書等記載事項変更手続

認証被許諾者は、「暗号モジュール認証申請書」（様式 1-1）、「暗号アルゴリズム確認申請書」（様式 1-2）及び「英文暗号モジュール認証書等発行申請書」（様式 8）の記載事項の変更を行う場合は、「暗号モジュール認証申請書等記載事項変更届」（様式 4）を提出する必要があります。

１５．３ 申請取下げ手続

認証被許諾者は、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場合は、「暗号モジュール認証申請等取下げ届」（様式 5）を認証機関に提出する必要があります。なお、申請書及びその添付書類は、原則として返却されません。

１５．４ 暗号モジュール認証製品リスト等記載事項の変更手続

認証被許諾者は、「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に変更が生じた場合は、「暗号モジュール認証製品リスト等記載事項変更届」（様式 6）を認証機関に届出る必要があります。

１５．５ 暗号モジュール認証書等の再発行手続

（1） 認証被許諾者は、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」等の再発行申請を行う場合は、「暗号モジュール認証書等再発行申請書」（様式 7）を認証機関に提出する必要があります。

（2） 認証被許諾者は、別表に定める暗号モジュール認証書等の再発行申請手数料の請求書を認証機関から受領したときは、速やかに、指定の口座へ申請料を入金して下さい。

なお、一旦納付された申請料は、理由いかんを問わず、返金されません。

１６．暗号モジュール認証等の承継

１６．１ 暗号モジュール認証等の承継手続

認証被許諾者が、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、又は暗号アルゴリズム確認書等に記載されている暗号アルゴリズム実装に係る事業の全てを譲渡しようとするとき、又は合併が見込まれるときは、認証被許諾者は、譲渡又は合併に先立って認証機関に事前相談を行わなければなりません。その際、認証被許諾者は、譲渡先又は合併後の法人等に対して、当該認証に係る事業の全てが承継される旨を明記した書類を作成して、認証機関に提出する必要があります。その上で、暗号モジュール認証等の承継が許可された場合には、認証被許諾者となる当該事業の全てを譲り受けた法人又は合併後の法人は、「暗号モジュール認証製品リスト記載事項変更届」（様式 6）及び「暗号モジュール認証書等再発行申請書」（様式 7）に加え、その事実を証明する以下の書類を添付して提出しなければなりません。

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

１６．２ 暗号モジュール認証等の承継の許可等

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が認められます。認証機関が、１２．に定めたサーベイランスを必要に応じて実施しますので、当該法人は、必要な準備を行ってください。

なお、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、運営審議委員会から承継許可が相当との助言がなされる必要があります。運営審議委員会から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には、当該承継申請が却下され、暗号モジュール認証等の取

消等が行われる場合があります。その際は、１４．に従わなければなりません。

１７．暗号モジュール認証の認証被許諾者に対する苦情の処理

(1) 認証被許諾者は、認証された暗号モジュールについてのセキュリティに関する苦情の全てを記録しなければなりません。

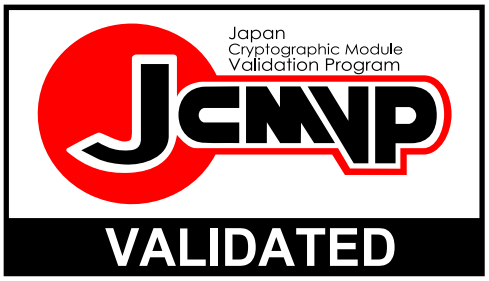
(2) 認証被許諾者は、認証された暗号モジュールについて寄せられた上記の苦情に対して適切な処置をとり、またその処置について記録しなければなりません。

(3) 認証機関から、認証された暗号モジュールについての上記の苦情及びそれに対する処置の記録提出の指示があった場合は、認証被許諾者は、認証機関にその記録を提出しなければなりません。何らかの理由でその記録を提出できない場合は、認証機関の要員による当該記録の閲覧を認めなければなりません。

(4) 苦情又は異議申し立てに関連して、認証機関から認証された暗号モジュール認証に係る是正要求が出された場合、認証被許諾者は、適切に是正措置を講じなければなりません。定められた期間内に是正措置が取られない場合、暗号モジュール認証の取消等が行われることがあります。その際は、１４．に従わなければなりません。

１８．暗号モジュール認証マーク

暗号モジュール認証マークは、次に掲げるものであり、暗号モジュール認証書が本制度の条件に従って発行されたことを示すものです。認証被許諾者の要請により、必要な手順を経て、認証機関から暗号モジュール認証マークの電子的なコピーが配付されます。



１９．暗号モジュール認証マーク等の取扱

(1) 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の所有権及び著作権は、機構が保有します。

(2) また、「暗号モジュール認証マーク」の使用に関する独占的な権利は、機構が保有します。

(3) 認証被許諾者は、暗号モジュールが、***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に適合していると認証されていることを示すためのみに暗号モジュール認証を使用しなければなりません。その際には、認証被許諾者は、暗号モジュール認証の対象となった認証範囲を逸脱して示してはなりません。

(4) 認証被許諾者は、暗号モジュール認証の信頼性を損なうような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及び「暗号モジュール認証マーク」の使い方をしてはなりません。

(5) 認証被許諾者は、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又はその一部分であっても、誤解を招くような方法で使用してはなりません。例えば、認証された暗号モジュール以外の暗号モジュールあるいは製品等に対して、「暗号モジュール認証取得製品シリーズ」、「暗号モジュール認証取得製品と同等又は相当」といった、誤解を招くような宣伝・広告・表示等を行ってはなりません。

(6) 認証被許諾者は、暗号モジュール認証書が発行された場合、「暗号モジュール認証マーク」を、書類、パンフレット、宣伝・広告、製品パッケージ等に使用するとき、「暗号モジュール認証マーク」の傍など、暗号モジュールの使用者が認識しやすい適切な場所に、当該暗号モジュール認証番号及びセキュリティレベルを示してください。また、認証された暗号モジュールの認証範囲を示し、当該暗号モジュール認証が、試験に用いた試験対象が所定の基準に基づく試験の結果、所定の要件に適合していることを示すものである旨の文言を記してください。

(7) 認証被許諾者は、暗号モジュール認証等の一時停止又は取消が行われた場合、当該暗号モジュール認証等を言及している全ての宣伝・広告などを中止しなければなりません。暗号モジュール認証の取消が行われた場合、認証機関の指示に従い、当該暗号モジュール認証によって交付された暗号モジュール認証書等の全てを返却しなければなりません。

２０．規程類及び手続の変更

認証機関は、法令、関連する規格の改正又は社会的な要請等に対応して、もしくは本制度の継続的な運営を目的として、本制度の規程類及び手続に係る条件を変更することがあります。本制度の規程類及び手続に関して変更しようとする場合は、十分な周知期間をおいて周知します。

なお、この変更は、適用猶予期間が別途設けられた場合を除き、既に認証された暗号モジュール及び確認された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も、周知期間終了後直ちに適用されます。

附　則（平成 19 年 5 月 9 日　2007 情総第 19 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 116 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 117 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 95 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 22 年 6 月 29 日　2010 情総第 42 号・一部改正）

この規程は、平成 22 年 6 月 28 日から施行する。

附　則（平成 26 年 3 月 27 日　2013 情総第 164 号・全部改正）

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 181 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（令和元年 9 月 27 日　2019 情総第 315 号・一部改正）

この規程は、令和元年 10 月 1 日から施行する。

附　則（令和 2 年 10 月 16 日　2020 情総第 1126 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。

暗号モジュール認証手続に係る様式集

（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 1-1

暗号モジュール認証申請書

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

申請責任者名　　印

「暗号モジュール認証申請手続等に関する規程」（CBM-02）に基づき、別紙「同意書」（様式 2）に同意し、下記のとおり申請します。

＜申請区分＞　（いずれかにチェック） □暗号モジュール認証（新規） □再認証　（前回の暗号モジュール認証番号：　　） □保証継続（前回の暗号モジュール認証番号：　　）
＜「暗号モジュール認証製品リスト」（日本語版）に掲載する暗号モジュールの定義＞ 暗号モジュールの名称： ハードウェアバージョン： ファームウェアバージョン： ソフトウェアバージョン： 概略（*1）：
＜「暗号モジュール認証製品リスト」（英語版）に掲載する暗号モジュールの定義＞ Name of the cryptographic module： Hardware version(s)： Firmware version(s)： Software version(s)： Outline(*2)：

*1 暗号モジュール認証製品リスト（日本語版）に記載される内容を記入してください。
*2 暗号モジュール認証製品リスト（英語版）に記載される内容を記入してください。

以下は記入しないでください。

受付番号	

＜暗号モジュール認証申請を行う申請責任者＞ 申請責任者名（所属）： 申請責任者のメールアドレス： 電話番号：
＜希望する認証範囲＞ セキュリティレベル：１・２・３・４ 物理形態：シングルチップ・マルチチップ組込型・マルチチップスタンドアロン型 注：ソフトウェア暗号モジュールは、マルチチップスタンドアロン型となります。
＜暗号モジュール認証の基準となるセキュリティ要件等＞ 暗号モジュール認証の基準となる規格の名称：
＜「暗号モジュール認証製品リスト」（日本語版）に掲載する連絡先＞ 申請者の名称： URL： 住所：〒 申請者の連絡担当者名（所属）： 申請者の連絡担当者のメールアドレス： 電話番号： FAX 番号：
＜「暗号モジュール認証製品リスト」（英語版）に掲載する連絡先＞ Name of the applicant： URL： Address： Contact person (department/division)： E-mail of the contact person： Telephone number： Facsimile number：
＜暗号モジュール認証申請手数料の請求先＞ 請求先の名称： 住所：〒 担当者名（所属）： 担当者のメールアドレス： 電話番号： FAX 番号：

＜暗号モジュール試験機関の情報＞ 試験機関名： 責任者名： 責任者のメールアドレス： 電話番号： FAX 番号：
＜認証申請中の情報の公開＞ 認証申請時点から「認証申請中」である旨の情報公開を、 希望する・希望しない

様式 1-2

暗号アルゴリズム確認申請書

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

申請責任者名　　印

「暗号モジュール認証申請手続等に関する規程」（CBM-02）に基づき、別紙「同意書」（様式 2）に同意し、下記のとおり申請します。

＜申請区分＞ 暗号アルゴリズム確認
＜「暗号アルゴリズム確認登録簿」（日本語版）に掲載するバージョン等の定義＞ 暗号モジュールの名称（暗号アルゴリズム実装名）： ハードウェアバージョン： ファームウェアバージョン： ソフトウェアバージョン： 動作環境：
＜「暗号アルゴリズム確認登録簿」（英語版）に掲載するバージョン等の定義＞ Name of the cryptographic module, or of the cryptographic algorithm implementation： Hardware version(s)： Firmware version(s)： Software version(s)： Operational environment(s)：

以下は記入しないでください。

受付番号	

＜暗号アルゴリズム確認申請を行う申請責任者＞ 申請責任者名（所属）： 申請責任者のメールアドレス： 電話番号：
＜暗号アルゴリズム＞
＜暗号アルゴリズム確認の基準となるセキュリティ要件等＞ 暗号アルゴリズム確認の基準となる規格の名称：
＜「暗号アルゴリズム確認登録簿」（日本語版）に掲載する連絡先＞ 申請者の名称： URL： 住所：〒 申請者の連絡担当者名（所属）： 申請者の連絡担当者のメールアドレス： 電話番号： FAX 番号：
＜「暗号アルゴリズム確認登録簿」（英語版）に掲載する連絡先＞ Name of the applicant： URL： Address： Contact person (department/division)： E-mail of the contact person： Telephone number： Facsimile number：
＜暗号アルゴリズム確認申請手数料の請求先＞ 請求先の名称： 住所：〒 担当者名（所属）： 担当者のメールアドレス： 電話番号： FAX 番号：

＜暗号モジュール試験機関の情報＞

試験機関名：

責任者名：

責任者のメールアドレス：

電話番号：

FAX 番号：

様式 2

同　意　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

申請責任者名　　印

暗号モジュール認証申請又は暗号アルゴリズム確認申請にあたり、以下の事項に同意し、適切に実施致します。

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「暗号モジュール認証申請手続等に関する規程」を常に遵守します。

2. 「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」の所有権及び著作権は、機構が保有していることに同意します。

3. サーベイランス、再試験などの実施のために必要な、暗号モジュールの提供、文書の調査、全ての場所への立ち入り、記録の閲覧、申請者の要員の面接のための準備等を含め、暗号モジュール認証機関（以下「認証機関」という。）が行う業務の実施に必要な準備を全て行います。

4. 暗号モジュールが、「暗号モジュール試験及び認証制度の基本規程」の附属書 A に掲げた暗号モジュールセキュリティ要件に適合していると認証されていることを示すためのみに暗号モジュール認証を使用します。

5. 暗号モジュール認証の対象となった認証範囲についてのみ認証されていることを表明します。

6. 暗号モジュール認証の信頼性を損なうような「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」及び「暗号モジュール認証マーク」の

使い方をしません。

7. 「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」又はその一部分であっても、誤解を招くような方法で使用しません。

8. 「暗号モジュール認証書」が発行された場合、「暗号モジュール認証マーク」を、書類、パンフレット、宣伝・広告、製品パッケージ等に使用するとき、「暗号モジュール認証マーク」の傍など暗号モジュールの使用者が認識しやすい適切な場所に、暗号モジュール認証番号及びセキュリティレベルとともに、必ず次に示す旨の文言を併記し、誤解を招くような方法で使用しません。

（暗号モジュールが、製品そのものである場合）

「本暗号モジュールが取得した暗号モジュール認証は、試験に用いた試験対象が所定の基準に基づく試験の結果、所定の要件に適合していることを示すものです。」

（暗号モジュールが、製品の一部である場合）

「本製品には、認証済み暗号モジュールが内蔵されています。本暗号モジュールが取得した暗号モジュール認証は、試験に用いた試験対象が所定の基準に基づく試験の結果、所定の要件に適合していることを示すものです。」

9. 暗号モジュール認証の一時停止又は取消の場合、暗号モジュール認証を言及しているすべての宣伝・広告などを中止し、認証機関の指示に従い、暗号モジュール認証によって得られた「暗号モジュール認証書」等のすべてを返却します。

10. 「暗号モジュール認証書」が発行された場合、次の暗号モジュール認証の認証被許諾者の責務を果たします。

a) 申請者は、暗号モジュールを認証済みであるとして供給するときは、認証機関から発行された「暗号モジュール認証報告書」及び「暗号モジュール認証書」で識別された暗号モジュールを、認証された条件の下で供給します。認証された暗号モジュールに改変を加えた場合、改変後のバージョンに再認証を適用した場合又は新たに認証を取得した場合を除いては、改変後のバージョンを認証された暗号モジュールとして市場に供給しません。
b) 申請者は、「暗号モジュール認証書」又は「暗号モジュール認証製品リスト」に記載された事項に変更が生じたときは、遅滞なくその変更を認証機関に届け出ます。
c) 申請者は、認証された暗号モジュールについてのセキュリティに関する苦情のすべてを記録します。申請者は、認証された暗号モジュールについて寄せられた上

記の苦情に対して適切な処置をとり、またその処置について記録します。認証機関から、認証された暗号モジュールについての上記の苦情及びそれに対する処置の記録提出の指示があった場合は、認証機関にその記録を提出します。何等かの理由でその記録を提出できない場合は、認証機関の要員による当該記録の閲覧を認めます。

d) 申請者は、認証済み暗号モジュールが、本制度の要件に適合していない可能性を示す何らかの情報を得た場合は、遅滞なく、その旨を認証機関に報告します。申請者が暗号モジュール認証の継続を望む場合、当該報告の結果、認証機関から何等かの指示があった場合には、その指示に従います。これには、認証機関から再試験の指示があった場合は、試験機関に再試験を依頼し、その原因が申請者にある場合、費用を負担することを含みます。

11. 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。

以上

様式 3

暗号モジュール試験実施計画書

発行日：　　年　月　日

版数：

＜申請者＞　殿

＜試験機関名＞

＜試験機関責任者名＞

暗号モジュール試験の実施にあたり、次の通り計画致します。

＜暗号モジュールの情報＞ 暗号モジュールの名称： ハードウェアバージョン： ファームウェアバージョン： ソフトウェアバージョン：
＜暗号モジュール試験機関の情報＞ 試験機関名： 責任者名： 責任者のメールアドレス： 電話番号： FAX 番号：
＜暗号モジュール試験の実施体制＞ 品質管理者： 技術管理者： 試験要員：
＜試験方法、技法、ツール及び基準＞

＜詳細暗号モジュール試験実施スケジュール＞

暗号モジュール試験開始予定日：　　年　月　日

第１週目～第〇週目：

第〇週目～第〇週目：

第〇週目～第〇週目：

第〇週目～第〇週目：

第〇週目～第〇週目：

第〇週目～第〇週目：

第〇週目～第〇週目：

第〇週目～第〇週目：

第〇週目～第〇週目：

第〇週目～第〇週目：

第〇週目～第〇週目：

＜備考＞

様式 4

暗号モジュール認証申請書等記載事項変更届

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
申請責任者

下記１．の申請書について、下記２．のとおり記載事項を変更したく届け出ます。

記

１．申請書の種別
・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
・英文暗号モジュール認証書等発行申請書

２．暗号モジュールの名称
暗号モジュールの名称：
バージョン：
申請日：
受付番号：
申請に係る責任者名：
変更箇所：

以上

［備考］
- １．については、該当するものに○印を付すものとする。
- 申請責任者は、暗号モジュール認証申請書に記載された者とする。
- 暗号モジュール認証申請書等の中でバージョンに関する記載事項変更届は不要とする。

様式 5

暗号モジュール認証申請等取下げ届

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
申請責任者名　　印

下記１．の申請について、下記２．のとおり申請を取下げたく届け出ます。

記

１．申請の種別
・暗号モジュール認証申請
・暗号アルゴリズム確認申請書
・英文暗号モジュール認証書等発行申請

２．暗号モジュールの名称
暗号モジュールの名称：
バージョン：
申請日：
受付番号：
取下げの理由：

以上

［備考］
- １．については、該当するものに○印を付すものとする。
- 申請責任者は、暗号モジュール認証申請書に記載された者とする。

様式6

暗号モジュール認証製品リスト等記載事項変更届

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
申請責任者名　　印

下記１．について、下記２．のとおり記載事項を変更したく届け出ます。

記

１．種別
・ 暗号モジュール認証製品リスト
・ その他（　　）

２．暗号モジュール認証を受けた暗号モジュール
暗号モジュールの名称：
暗号モジュール認証番号：
変更を希望する記載事項：

変更理由：

以上

［備考］
- １．については、該当するものに○印を付すものとする。
- 申請責任者は、暗号モジュール認証申請書に記載された者とする。

様式 7

暗号モジュール認証書等再発行申請書

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
申請責任者名　　印

下記１．について、下記２．の理由により再発行を請求します。

記

１．種別
・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・英文暗号モジュール認証報告書
暗号モジュールの名称：
バージョン：
暗号モジュール認証番号又は暗号アルゴリズム確認番号：

２．再発行申請理由

以上

〔備考〕
- １．については該当するものに○印を付すものとする。
- 申請責任者は、暗号モジュール認証申請書に記載された者とする。

様式 8

英文暗号モジュール認証書等発行申請書

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
申請責任者名　　印

「暗号モジュール認証申請手続等に関する規程」に基づき発行された下記の認証書について、「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」及び「英文暗号モジュール認証報告書」の発行を申請します。

記

１．暗号モジュールの名称：

２．暗号モジュール認証年月日：

３．暗号モジュール認証番号：

以上

様式 9

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、甲乙間で締結された　　年　月　日付申請【受付番号　　】に基づき、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「本件認証業務」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、乙が本件認証業務を行うにあたり、甲が乙に直接又は試験機関を通じて開示する、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、本件認証業務に関連して甲が乙に直接又は試験機関を通じて開示する、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、本件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、本件認証業務が終了、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　住所
申請者の名称　　印
所属、役職名
申請責任者名　　印

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
理事長名

様式 10

暗号モジュール所見報告書

識別番号	
暗号モジュール名	○○暗号モジュール
バージョン	ハードウェアバージョン ○.○.○ ソフトウェアバージョン ○.○.○
指摘箇所名	「○○ソースコード」
標題	○○関数は、○○できない。
関連する AS	
関連する TE	

発行機関	○○試験機関
発行担当者名	
発行責任者名	
発行日	年　月　日

所見内容：

「○○ソースコード」の○○行目に記述されている○○関数は、○○することができませんので、TE○○.○○.○○の要件の「○○できなければならない。」に適合していません。

TE○○.○○.○○の要件にご対応下さいます様、宜しくお願いします。

対応機関	○○株式会社
希望対応期日	年　月　日まで
発行機関	○○株式会社
発行担当者名	
発行責任者名	
発行日	年　月　日

所見内容：

「○○ソースコード」の○○行目に記述されている○○関数を、TE○○.○○.○○の要件の「○○できなければならない。」に適合するように改訂し、ソフトウェアバージョンを○.○.○+1 に致しました。

宜しくご査収下さい。

対応機関	○○試験機関
希望対応期日	年　月　日まで

発行機関	○○試験機関
発行担当者名	
発行責任者名	
発行日	年　月　日
所見内容： 本件所見報告書の内容は、ソフトウェアバージョン○.○.○+1 の「○○ソースコード」を検査した結果、要件を満足するように改訂されていることを確認しました。	
対応機関	なし
希望対応期日	完了

様式 11

暗号モジュール影響分析報告書

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

報告書作成者の名称　　印

下記の暗号モジュールの保証継続を申請するにあたり、暗号モジュールの変更が与える影響について、下記のとおり分析を行いました。その結果、暗号モジュールセキュリティ要件に関連した事項について、影響を与えないことを確認しました。

記

＜暗号モジュール影響分析報告書識別＞ 文書名　　： バージョン： 作成日　　： 作成者　　：
＜暗号モジュール識別＞ 暗号モジュールの名称　　： ハードウェアバージョン　： ファームウェアバージョン： ソフトウェアバージョン　： 開発者　　：
＜認証済み暗号モジュール識別＞ 認証番号　　： 暗号モジュールの名称　　： ハードウェアバージョン　： ファームウェアバージョン： ソフトウェアバージョン　： 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　　：

影響分析の詳細：別紙に記載のとおり。

以上

様式 11 別紙

1. 変更内容の記述（*1）

2. 影響のある開発文書及び変更の詳細（*2）

3. 変更がセキュリティ要件に与える影響の分析（*3）

以上

*1：1 つまたは複数の変更を記述し、それぞれについて、原因、目的を文書化してください。

*2：変更のそれぞれについて、影響のある開発文書を示し、どこがどのように変更されたか文書化してください。

*3：変更のそれぞれが、セキュリティ要件に与える影響を分析し、保証継続が適用できる証拠を示してください。

別表

申請手数料料金表

<table>
<tr><td>暗号モジュール認証申請等の種類</td><td colspan="2">認証申請等の料金（税込）</td></tr>
<tr><td rowspan="4">暗号モジュール認証申請</td><td>セキュリティレベル 1</td><td>275,000 円</td></tr>
<tr><td>セキュリティレベル 2</td><td>392,800 円</td></tr>
<tr><td>セキュリティレベル 3</td><td>550,000 円</td></tr>
<tr><td>セキュリティレベル 4</td><td>770,000 円</td></tr>
<tr><td rowspan="4">再認証
（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）
保証継続
（修正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ない場合）</td><td>セキュリティレベル 1</td><td>82,800 円</td></tr>
<tr><td>セキュリティレベル 2</td><td>117,800 円</td></tr>
<tr><td>セキュリティレベル 3</td><td>165,000 円</td></tr>
<tr><td>セキュリティレベル 4</td><td>231,000 円</td></tr>
<tr><td>暗号アルゴリズム確認申請</td><td colspan="2">22,000 円</td></tr>
<tr><td>英文暗号アルゴリズム確認書発行申請
英文暗号モジュール認証書発行申請
英文暗号モジュール認証報告書発行申請</td><td colspan="2">3,900 円/枚</td></tr>
<tr><td>暗号アルゴリズム確認書再発行申請
暗号モジュール認証書再発行申請
暗号モジュール認証報告書再発行申請
英文暗号アルゴリズム確認書再発行申請
英文暗号モジュール認証書再発行申請
英文暗号モジュール認証報告書再発行申請</td><td colspan="2">3,900 円/枚</td></tr>
</table>

注 1：上記申請手数料料金は、申請 1 件あたりの料金です。

注 2：申請手数料は、申請の取下げがされても返金しません。

注 3：暗号モジュール認証の場合において、旅費等の必要経費が生じたときは、暗号モジュール認証申請等の料金の他に別途当該必要経費を請求することがあります。

改正履歴

識別番号	CBM-02

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 22 年 6 月 28 日	櫻井・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
令和元年 9 月 27 日	櫻井・江口	一部改正
令和 2 年 10 月 16 日	神田・戸高	一部改正