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

令和 2 年 10 月 16 日

CBM-01

Certification Body Management System

IPA

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機関の組織及び業務運営に関する規程

制定　平成 19 年 5 月 9 日　2007 情総第 18 号
最終改正　令和 2 年 10 月 16 日　2020 情総第 1125 号　一部改正

1. 総則

1.1 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、暗号モジュール試験及び認証制度（以下「本制度」という。）について定めた***暗号モジュール試験及び認証制度の基本規程***（以下「***制度基本規程***」という。）に基づいて暗号モジュール認証機関（以下「認証機関」という。）として業務を行うために必要な組織及び認証業務の運営の方針及び手順について定めるものである。

1.2 方針

最高経営責任者は、認証機関による認証業務運営が、適切に行われることを確保するため、別途定める品質方針及び品質目標を誓約する。

1.3 用語及び定義

本規程において使用する用語及び定義は、***制度基本規程***及び JIS Q 17065 において使用する用語の例による。

2. 認証機関

2.1 組織

2.1.1 法的地位

認証機関は、独立行政法人通則法（平成 11 年法律第 103 号）及び情報処理の促進に関する法律に基づき設立された機構内に設置する組織である。

2.1.2 組織の構成

認証機関は、理事長、理事又は参事、セキュリティセンター センター長、セキュリティセンターの職員並びに 2.1.4 で規定する委員会及び委員で構成される。また、組織の構造を図 1 に示す。

認証機関の組織を構成する者の責任と権限について次のとおりとし、詳細について別表に定める。

なお、認証機関の組織を構成する者の管理に関し必要な事項については、***暗号モジュール認証機関要員管理手順***（以下「***要員管理手順***」という。）に定める。

① 最高経営責任者：機構の理事長
最高経営責任者は、認証機関を代表し、認証業務運営に係る経営資源の確保に責任を持つ。最高経営責任者は、品質方針及び品質目標を定め文書化を行い、認証機関でこの方針が確実に理解され、実施され、維持されるようにしなければならない。
② 統括責任者：機構の理事又は参事の中から、最高経営責任者が指名する者
統括責任者は、認証業務運営に係る業務の執行を統括し、執行の責任を持つ。
③ マネジメントシステム責任者：機構のセキュリティセンター センター長
マネジメントシステム責任者は、本規程に規定されている品質に関する要求事項を実行する。
④ 暗号モジュール技術管理者：機構の認証業務運営に関する技術的業務をつかさどる者
暗号モジュール技術管理者は、認証業務運営に関する技術的業務をつかさどり、技術的事項に係る諸課題を調整する。
⑤ 暗号モジュール認証要員：機構の職員のうち、***要員管理手順***に定める一定の要件に基づいて指名された者
暗号モジュール認証要員は、暗号モジュール認証に関する暗号モジュール試験結果を検証する。
⑥ 暗号モジュール業務担当者：機構の職員のうち、認証機関としての業務担当を行う者
暗号モジュール業務担当者は、申請受付、認証書発行等の認証業務運営に関する業務を行う。

2.1.3 認証業務運営に携わる者が遵守すべき事項

(1) 認証業務運営に携わる者は、次に掲げる事項を遵守しなければならない。
① 本規程を遵守し、良識をもって公平かつ公正にその職務を遂行すること。
② JIS Q 17065 又は法令によって要求される場合を除いて、職務を通じて知り得た情報（製品又は申請者に係る情報をいう。）を申請者の書面での同意がない限り第三者に開示しないこと。
③ 商業上、財政上その他の圧力又は利害対立の影響を受けないこと。
④ 申請者又はその関係者から不当な利益の供与を受けないこと。

(2) 認証機関は、認証業務運営に関する活動とその他の活動を区別する。また、次に掲げる事項を遵守する等、認証業務運営以外の活動によって**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。）の機密性、客観性又は公平性が影響されないことを確保する。
① **暗号モジュール認証等**の業務の対象製品と同種の製品、その他認証業務運営の機密性、客観性又は公平性を損なうような製品及びサービスの供給又は設計をしな

いこと。

② 申請者が**暗号モジュール認証等**を得るうえで障害となる事項への対処方法について、特定の申請者に対する助言、指導等のサービス業務を行わないこと。

③ 特定のコンサルティングを用いれば、暗号モジュール認証等が簡単、容易、迅速又は廉価になると明示又は暗示しないこと。

2.1.4 運営審議委員会及び技術審議委員会

(1) 認証業務運営の助言機関として、認証機関に、運営審議委員会及び技術審議委員会を設置する。各委員会の役割は次のとおりとする。

① 運営審議委員会は、認証業務運営の方針及びマネジメントシステムの維持に関する事項、並びに申請の受付可否、認証の許諾、拒否又は取消等に関する事項等の審議を行い、統括責任者に対する助言を行う。

② 技術審議委員会は、**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。）の策定等の技術的事項の審議を行い、統括責任者に対する助言を行う。

(2) 各委員会は、民間の有識者、学識経験者及び政府関係者のうちから、委員会の審議内容及び利害の均衡を考慮して任命する委員 15 名以内で構成する。

(3) 各委員会には委員長を各 1 名置き、委員長は委員会を総理する。また、委員会は、委員長が必要と判断した場合に開催する。委員会は、委員長が招集し、委員の半数以上の出席をもって成立する。なお、必要に応じ、委員会の一部又は全部をオンラインにより開催することができることとする。

(4) 委員会においては、委員長は、当該委員会の審議事項に係る重要問題又は緊急問題の検討のために必要と認められる場合、当該委員会の下に一時的な作業グループ（以下「WG」という。）を設置することができる。この場合、WG の委員のうち 1 名は、当該委員会の委員でなければならない。また、WG を総理する者として主査を置くこととし、主査は WG の委員の互選とする。この規程は、WG の運営について準用する。この場合において「委員会」とあるのは「WG」と読み替えるものとする。

(5) 委員会の事務局は、セキュリティセンターのセキュリティ技術評価部暗号グループに置くこととする。

(6) 委員の委嘱は、次により行う。

① 機構の理事長が委員を委嘱する。

② 委員の任期は、2 年とする。ただし、年度途中で委嘱する場合は、当該年度は 1 年とみなして任期の算定を行う。なお、委員の再任は妨げないものとする。

(7) 委員が委員会に出席した場合には、独立行政法人情報処理推進機構謝金等規程（2003 情総第 88 号）に基づき、当該委員に旅費及び委員謝金を支給する。ただし、委員が受領を辞退した場合は、この限りではない。なお、委員の代理の者が出席した場合であ

っても同様とする。

その他、運営審議委員会及び技術審議委員会に関し必要な事項については、***要員管理手順***に定める。

2.2 運営

2.2.1 運営方針

（1）認証機関は、その運営にあたり不当な差別的取扱を行わない。このために、次の事項を遵守する。

a）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ことを目的とし、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、認証済暗号モジュールや確認済暗号アルゴリズム実装の不適切な取扱い法人等からの申請、又は制度基本規程の 2.2.1 に該当しない法人等への認証譲渡のための申請等の場合には、申請受理や認証許諾等の取扱を決める前に、必要に応じて運営審議委員会に付議し、申請の受付可否、認証の許諾、拒否又は取消等に関する事項等の助言を得なければならない。

b）申請者に対し、a）による場合を除き、不当な財政的又は他の条件を課してはならない。

c）申請者の規模を条件にしたり、特定の団体等の会員であることを条件にしてはならない。

d）認証業務の実施において、申請者が保有する**暗号モジュール認証書**又は**暗号アルゴリズム確認書**の多寡によって差別的取扱を行ってはならない。

e）申請者からの問合せ、申請受付等に対して差別的な対応をとってはならない。

（2）認証機関は、**暗号モジュール認証等**を行うに際して、迅速な処理に努めなければならない。

（3）統括責任者は、認証業務運営に携わる全ての者について、守秘義務、利害衝突の排除等に係る「倫理誓約書」に署名した後でなければ当該業務に従事させてはならない。「倫理誓約書」の様式は、***要員管理手順***に定める。

2.2.2 運営のための資源

認証制度運営は、原則として、**暗号モジュール認証**等に係る手数料収入及び経済産業省から交付される運営費交付金による。

2.3 内部監査

2.3.1 内部監査の実施

（1）内部監査の準備

マネジメントシステム責任者は、必要に応じ、内部監査部と内部監査の実施日時、監査対象部署等の実施に係わる調整を行う。内部監査部は、次の（2）から（4）に基づき内部監査を実施する。

（2）内部監査の内容

内部監査は、**暗号モジュール試験及び認証制度**における**暗号モジュール認証業務**（以下「**認証業務**」という。）が、JIS Q 0065（ISO/IEC GUIDE65）並びに本規程に適合しているかどうかについて検証する。

（3）内部監査主体

① 内部監査は、内部監査部が実施する。

② 内部監査部は、認証業務の内部監査の実施について責任を負う。

（4）内部監査の実施方法等

① 定期の内部監査の実施間隔は原則として 1 年を超えないものとする。また、内部監査部が必要と認める場合は、臨時の内部監査を実施することができる。

② 監査員は、内部監査部の職員及び必要に応じて内部監査部長から指名された者とする。監査員は認証業務に従事していない者でなければならない。また監査員は秘密保持に留意する。

③ 内部監査部長は、定期の内部監査を実施する場合において、内部監査の実施日、内部監査対象部等、内部監査内容、監査員等を内部監査対象部等に事前に通知する。

④ 内部監査対象部等は、内部監査の円滑な実施に協力する。

⑤ 内部監査部は、内部監査を終了したときは、監査調書を作成するとともに、本規程に定める統括責任者に対し内部監査結果を報告又は通知する。

（5）内部監査の結果

統括責任者は、内部監査部からの内部監査の結果報告を受け、マネジメントシステム責任者に通知する。

内部監査の実施に関し必要な事項については、***業務取扱手順***に定める。

2.3.2 マネジメント・レビュー等の実施

統括責任者は、マネジメントシステムへの適合を検証し、認証業務運営の信頼性を確保するため、マネジメント・レビュー及び不適合の管理を実施する。マネジメントシステム責任者は、不適合業務の顕在的な原因又は潜在的な原因を特定し、是正処置又は予防処置を実施し改善することとする。マネジメント・レビュー等の実施に関し必要な事項については、***業務取扱手順***に定める。

3. 認証機関の要員

3.1 認証機関の要員

認証機関の要員は、認証業務運営に際し、必要な専門的知識、公平性及び中立性に従った判断を行い、品質の高い業務の遂行に努める。

3.2 資格基準及び教育・訓練等

認証機関は、認証機関の要員に対して、必要に応じ教育・訓練を実施する。認証機関は、資格基準等に関し必要な事項について、***要員管理手順***に定める。

4. 暗号モジュール認証等の業務

4.1 暗号モジュール認証

4.1.1 暗号モジュール認証等の申請受付

認証機関は、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。受付に当たって、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実装の不適切な取扱い法人等からの申請等の場合には、必要に応じて、認証機関は、運営審議委員会に受付可否について付議し、委員会の助言を参考に当該申請の受付を許可又は却下できるものとする。**認証機関**は、申請の受付後、申請者に対して速やかに***暗号モジュール認証申請受理通知書***又は***暗号アルゴリズム確認申請受理通知***を発行する。**暗号モジュール認証等**の申請受付に関し必要な事項については、***業務取扱手順***に定める。

4.1.2 認証済暗号モジュールの再認証及び保証継続の申請受付

認証機関は、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。）からの認証済暗号モジュールの**再認証又は保証継続**の申請を受付ける。**再認証又は保証継続**の申請受付に関し必要な事項については、***業務取扱手順***に定める。

4.1.3 所見報告書への対応

認証機関は、試験機関から「所見報告書」が提出されたときには、その内容に基づき次に掲げる何れかの処置をとる。

a）迅速に問題を検討し、当該**暗号モジュール試験**に関する技術指導、解釈等を示す。

b）本制度の技術審議委員会で審議し、解決を図る。

c）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。

認証機関は、***セキュリティ要件等***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***を策定し、機構のホームページを通じて公開する。認証機関は、***JCMVP 運用ガイダンス***の策定に関し必要な事項について、***業務取扱手順***に定める。

4.1.4 暗号モジュール認証作業

認証機関は、暗号モジュール認証を行うにあたり、次を実施する。

a） 認証機関は、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**に基づいて、**暗号アルゴリズム確認**作業を実施する。**暗号アルゴリズム確認**に関し必要な事項については、***業務取扱手順***に定める。

b） 認証機関は、試験機関から提出される**暗号モジュール試験報告書**に基づいて**暗号モジュール認証**作業を実施する。**暗号モジュール認証**に関し必要な事項については、***業務取扱手順***に定める。

4.1.5 暗号アルゴリズム確認作業

認証機関は、暗号アルゴリズム確認を行うにあたり、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**に基づいて、**暗号アルゴリズム確認**作業を実施する。**暗号アルゴリズム確認**に関し必要な事項については、***業務取扱手順***に定める。

4.1.6 暗号モジュール認証書又は暗号アルゴリズム確認書の交付等

認証機関は、暗号モジュール認証書又は暗号アルゴリズム確認書の交付を行うにあたり、次を実施する。

a）試験機関が JCATT を使用して実施した暗号アルゴリズム実装試験の結果が適切であると判断した場合、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（様式 1）を交付する。

b）試験機関が、CRYPTIPA を用いて作成された暗号モジュール試験報告書の内容確認を経て、実施した暗号モジュール試験の結果が適切であると判断した場合、申請者に対して暗号モジュール認証書（様式 2-1）及び暗号モジュール認証報告書（様式 2-2）を交付する。

c）a）、b）に関わらず、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、認証機関は、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中止、認証及び確認の許諾拒否又は取消等ができるものとする。具体的な手順等に関し必要な事項について、業務取扱手順に定める。

4.1.7 認証済暗号モジュールの再認証

認証機関は、試験機関から提出される再認証手続に伴う**暗号モジュール試験報告書**等を精査し、内容を検査する。認証機関は、試験機関が実施した**暗号モジュール試験**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再認証手続に基づく当該**暗号モジュール認証**の再認証を許諾する。再認証に関し必要な事項については、***業務取扱手順***に定める。

4.1.8 認証済暗号モジュールの保証継続

認証機関は、認証被許諾者から提出される「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。認証機関は、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当該**暗号モジュール認証**の保証継続を許諾する。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。

4.2 暗号モジュール認証等の承継

認証被許諾者の地位を承継しようとする場合、認証機関は、認証被許諾者からの事前の申入れに基づき、当該**暗号モジュール認証等**の承継手続きを行う。**暗号モジュール認証等**の承継に関し必要な事項については、***業務取扱手順***に定める。

4.3 暗号モジュール認証等の範囲の縮小及び拡大

a）認証機関は、次のいずれかによって、暗号モジュール認証の範囲の縮小を行うことができる。

i） 承認されたセキュリティ機能の見直し

ii） サーベイランスの結果

iii）再認証の結果

b）認証機関は、次によって、暗号モジュール認証の範囲の拡大を行うことができる。

i） 再認証の結果

c）認証機関は、暗号アルゴリズム確認の範囲の縮小及び拡大は行わない。

4.4 暗号モジュール認証等の一時停止又は取消

4.4.1 サーベイランス

認証機関は、本制度の信頼性を確保するため、必要に応じ**認証被許諾者**に対してサーベイランスを行う。サーベイランスの手順等に関し必要な事項について、***業務取扱手順***に定める。

4.4.2 再試験

認証機関は、サーベイランスの結果により、必要に応じ**認証被許諾者**に再試験を指示する。再試験の手順等に関し必要な事項について、***業務取扱手順***に定める。

4.4.3 暗号モジュール認証等の一時停止

認証機関は、次の条件のいずれかに該当する場合、暗号モジュール認証等の一時停止を行う場合がある。

a）再試験が実施されている期間

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等に係る異議申し立て又は苦情の内容が正当であり、認証機関が認証被許諾者又は試験機関に是正要求を出した場合

暗号モジュール認証等の一時停止の手順等に関し必要な事項について、業務取扱手順に定める。

4.4.4 暗号モジュール認証の取消

次の条件が満たされなくなった場合、暗号モジュール認証は自動的に取消しとなる。

i）暗号モジュールに 1 つ以上の承認されたセキュリティ機能が実装されていること

また、認証機関は、次の条件のいずれかに該当する場合、**暗号モジュール認証**の取消を行う場合がある。

a）再試験の実施を拒否した場合

b）1 年以内に再試験が完了しない場合

c）再試験の結果、認証不合格と判断された場合

d）「同意書」に違反する事実が認められた場合

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）運営審議委員会にて暗号モジュール認証の継続が不適当、又は暗号モジュール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暗号モジュール認証等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）認証機関から出された是正要求に対して、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是正に応じなかった場合

暗号モジュール認証の取消の手順等に関し必要な事項について、***業務取扱手順***に定める。

4.5 試験機関の承認と試験機関承認の廃止

4.5.1 試験機関の承認

認証機関は、本制度の試験機関を承認することができる。試験機関の承認の手続について、

暗号モジュール試験機関承認業務取扱手順に定める。

4.5.2 試験機関承認の廃止

認証機関は、試験機関から提出される**暗号モジュール試験機関承認廃止届**を受け付け、試験機関承認を廃止することができる。試験機関承認の廃止の手続について***暗号モジュール試験機関承認業務取扱手順***に定める。

4.6 情報の提供及び文書の管理

認証機関は、本制度の利用者への情報の提供及び文書の取扱について、***業務取扱手順***に定める。

4.7 記録

認証機関は、本制度の信頼性を確保し、認証業務が適切かつ有効に機能していることを実証するために、各規程に定められた記録事項を適切に記録する。認証機関は、記録の方法に関し必要な事項について、***業務取扱手順***に定める。

4.8 秘密保持

(1) 認証機関は、ある特定の申請者に対する認証活動で得られた情報は、法令の規定に基づき開示の義務が生じた場合を除き、第三者に開示してはならない。
(2) 法令に基づき第三者に情報を開示した場合は、法令に従って開示した旨をその申請者に通知しなければならない。
(3) 認証機関は、試験機関との間で、秘密保持契約を締結するものとする。
(4) 認証機関は、申請者の要請に基づき、秘密保持契約を締結するものとする。
(5) 申請者以外から得られた情報であって、苦情にあたる場合、その内容について、認証機関と原因発生元との秘密として取り扱う。苦情等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。

4.9 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、あるい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できる。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適切な予告を申請者に与えるよう留意する。認証機関は、規程類及び手続の変更に関し必要な事項について、業務取扱手順に定める。

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、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。

4.10 要求事項の変更

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適切な予告を申請者に与えるよう留意する。認証機関は、要求事項の変更に関し必要な事項について、***業務取扱手順***に定める。

なお、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、新たなセキュリティ要件等が公開された後の並立期間終了後直ちに適用されるものとする。また、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、業務取扱手順を通じて定める適用猶予期間が経過した後に適用されるものとする。

4.11 異議申し立て及び苦情の処理

認証機関は、本制度の信頼性を確保するため、申請者、試験機関又はその他**暗号モジュール認証**に関係する当事者からの認証機関に対する異議申し立て及び苦情に係る処理を適切に行う。認証機関は、その処理に関し必要な事項について、***業務取扱手順***に定める。

附　則（平成 19 年 5 月 9 日　2007 情総第 18 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 115 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 116 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 94 号・一部改正）

この規程は、平成 21 年 11 月 2 日から施行する。

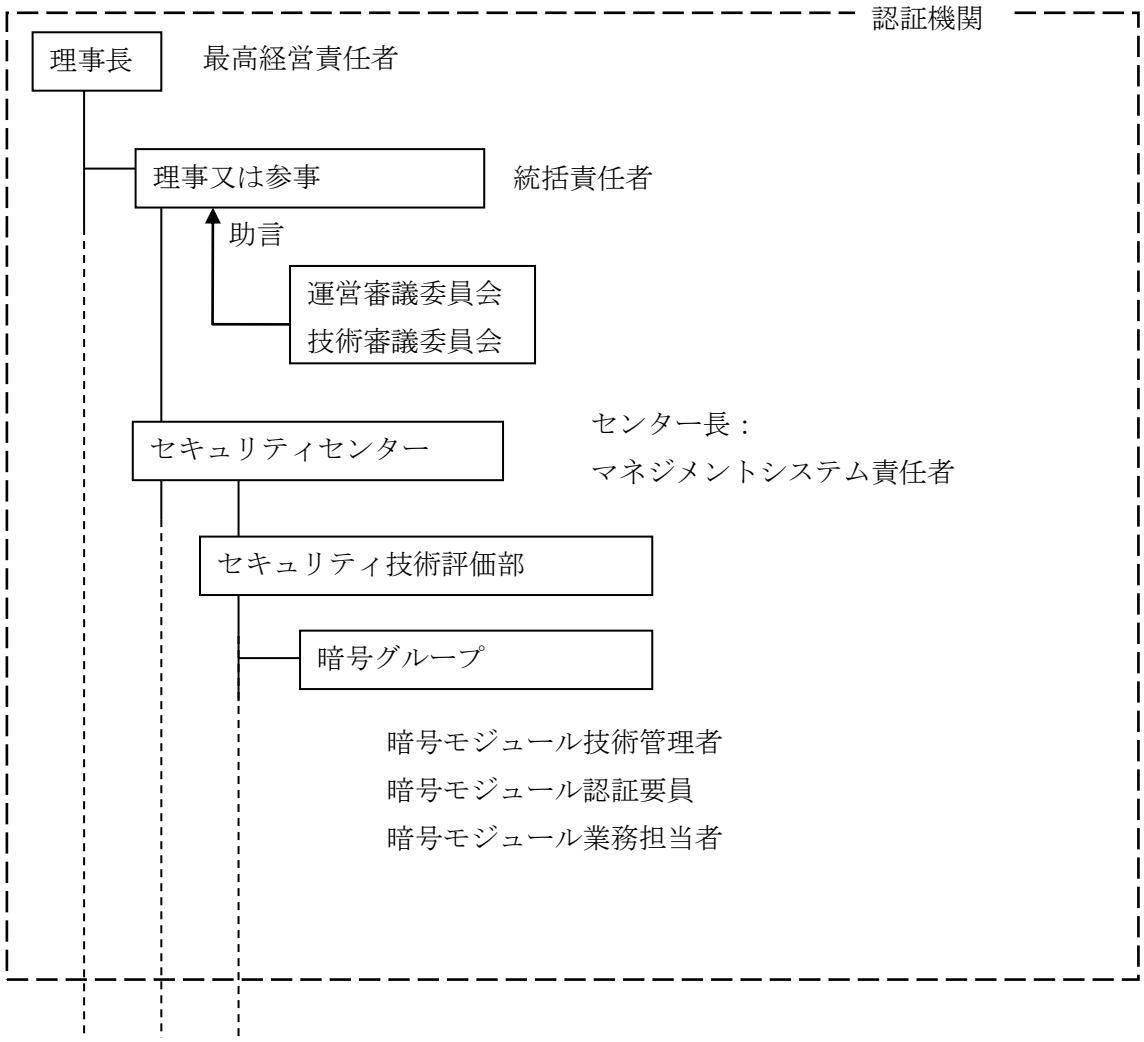
附　則（平成 30 年 6 月 29 日　2018 情総第 183 号・一部改正）

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 10 月 16 日　2020 情総第 1125 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。

図１ 組織の構造


認証機関
理事長
最高経営責任者
理事又は参事
統括責任者
助言
運営審議委員会
技術審議委員会
センター長：
マネジメントシステム責任者
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
暗号モジュール認証要員
暗号モジュール業務担当者

別表

認証業務運営に係る要員の責任及び権限

役割	責任及び権限
最高経営責任者	① 認証制度に係る品質方針及び品質目標を定め文書化すること。 ② 認証機関に係る規程類の整備に関すること。 ③ 認証業務運営に必要な予算等の経営資源を確保すること。 ④ 必要な資質をもち、教育・訓練を受け、かつ、技術的知識・経験を有する十分な数の暗号モジュール認証要員を配置するよう努めること。 ⑤ 認証業務運営に係る認証書等の証書の交付に関すること。 ⑥ 認証業務運営から生じる賠償責任等の債務に対して適切な備えを確保すること。 ⑦ その他認証業務運営に係る重要事項に対応すること。
統括責任者	① 認証機関の認証業務運営が確実に履行されるように、次の事項を監督すること。 ● 適用する暗号モジュールセキュリティ要件を明確にして、暗号モジュール認証の品質を維持管理すること。 ● 暗号モジュール認証の手順を明確にして、適正な実施を管理すること。 ● 暗号モジュール認証の業務の公平な実施を管理すること。 ● マネジメントシステムの運用に必要な責任と権限の体制を確立すること。 ● 機密情報を守秘すること。 ● 認証機関の財務管理を監督すること。 ● 一貫した信頼できる方法で確実に運営するために必要な措置を講ずること。 ② 暗号モジュール認証の許諾、一時停止及び取消に関する最終決裁を行うこと。 ③ 暗号モジュール試験機関の承認、承認取消等に関する最終決裁を行うこと。 ④ 技術的知識及び経験を有する者を確保し、認証要員として登録すること。 ⑤ 運営審議委員会及び技術審議委員会を運営すること。 ⑥ 認証業務運営に関して、出版物、インターネット等による広報活動をすること。

	⑦ マネジメント・レビューを実施すること。
マネジメントシステム責任者	① 認証業務のマネジメントシステムの確立、実行及び維持をすること。 ② 業務運営の再検討及び改善の根拠とするため、統括責任者及び関係者に対し、認証業務のマネジメントシステムの実施状況に関する報告及び提言をすること。 ③ 認証業務のマネジメントシステムの文書化、品質文書の維持管理、最新版文書の利用等を確実にすること。 ④ 認証機関に従事する職員の氏名、資格、経験及び業務分担の一覧表を作成し、常に最新の状態に維持管理すること。 ⑤ 内部監査の実施に係る調整をすること。 ⑥ 苦情処理に対応して処理すること。 ⑦ ⑤及び⑥に係る是正措置及び予防措置を実行管理すること。 ⑧ 認証要員及び職員の管理並びに認証要員の教育・訓練を行うこと。 ⑨ 認証業務に係る各職務を担当する職員に対し、機密情報の取扱及び倫理事項について、その重要性を周知徹底すること。 ⑩ その他認証業務運営の品質に係る事項に対応すること。
暗号モジュール技術管理者	① 認証業務運営の技術的事項に係ること。 ② 業務運営の再検討及び改善の根拠とするため、マネジメントシステム責任者及び関係者に対し、技術的事項の状況に関する報告及び提言をすること。 ③ 暗号アルゴリズム確認の許諾に関する決定を行うこと。 ④ 暗号モジュール認証の許諾、一時停止及び取消に関する決定を行うこと。 ⑤ 暗号モジュール試験機関の承認、承認取消等に関する決定を行うこと。 ⑥ 認証要員の技術及び能力の開発並びにその維持のため、年度初めに教育・訓練計画を立案し、当該年度において実施すること。 ⑦ 技術的公表文書等を確認すること。 ⑧ ***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に関連する技術的事項に対応すること。 ⑨ 認証要員の業務を査定すること。 ⑩ その他認証業務運営に係る技術的事項に対応すること。
暗号モジュール認証要員	① 暗号モジュール試験機関が実施する暗号モジュール試験活動を監督すること。 ② 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審査して、試験結果の妥当性を検証すること。

	③ 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等の案を作成すること。
暗号モジュール業務担当者	① 暗号モジュール認証申請等の受付及び暗号モジュール認証書等の発送に関すること。 ② 試験機関承認申請等の受付及び「暗号モジュール試験機関承認書」等の発送に関すること。 ③ 暗号モジュール認証、試験機関承認等の情報公開に関すること。 ④ 認証業務運営に関する委員会並びに認証業務運営の関連会議の事務局に関すること。

暗号モジュール認証機関の業務運営に係る様式集

（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

暗号アルゴリズム確認書

暗号モジュール試験及び認証制度に基づき、以下のとおり確認する。

年　月　日
独立行政法人 情報処理推進機構
理事長名 印

暗号アルゴリズム実装名：
バージョン：

確認番号	暗号アルゴリズム	確認条件

動作環境：

申請者：

試験機関の名称：

適用した試験ツール：

注意事項：本暗号アルゴリズム確認書で識別される暗号アルゴリズム実装は、「暗号モジュール試験及び認証制度」で承認された試験機関による、暗号アルゴリズム実装試験要件に基づく暗号アルゴリズム実装試験結果が、適合していることを示す。本暗号アルゴリズム確認書は、暗号アルゴリズム実装試験を受けた構成及び動作環境に関して、暗号アルゴリズム実装の特定のバージョンのみに適用される。暗号アルゴリズム実装試験は「暗号モジュール試験及び認証制度」の規程に従って実施され、暗号アルゴリズム実装試験報告書の試験機関による結論は、暗号アルゴリズム実装試験に用いた提供物件にのみ対応している。この暗号アルゴリズム確認書は独立行政法人 情報処理推進機構による暗号モジュール製品等の保証書ではない。また、独立行政法人 情報処理推進機構は、明示、黙示を問わず、本暗号アルゴリズム実装を用いた暗号モジュール製品等に関していかなる保証も行わない。暗号アルゴリズム確認に関する詳細な情報については、「暗号アルゴリズム確認登録簿」を参照すること。

様式 2-1

暗号モジュール認証書

暗号モジュール試験及び認証制度に基づき、以下のとおり認証する。

年　　月　　日
独立行政法人 情報処理推進機構
理事長名 印

認証番号 XXXXX

日本語名：

英語名：

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：
物理形態：

適合規格：
試験要件：

申請者：
所在地：
特記事項：

注意事項：本暗号モジュール認証書で識別される暗号モジュールは、「暗号モジュール試験及び認証制度」で承認された試験機関による、暗号モジュール試験要件に基づく暗号モジュール試験結果が、適合していることを示す。本暗号モジュール認証書は、暗号モジュール試験を受けた構成及び動作環境に関して、暗号モジュールの特定のバージョンのみに適用される。暗号モジュール試験は「暗号モジュール試験及び認証制度」の規定に従って実施され、暗号モジュール試験報告書の試験機関による結論は、暗号モジュール試験に用いた提供物件にのみ対応している。この暗号モジュール認証書は独立行政法人 情報処理推進機構による暗号モジュール製品等の保証書ではない。また、独立行政法人 情報処理推進機構は、明示、黙示を問わず、本暗号モジュールを用いた暗号モジュール製品等に関していかなる保証も行わない。なお、本認証書を、不正に使用した場合、並びに誤解を招くような方法で広告又は説明等に使用した場合には、暗号モジュール認証の取消を行うことがある。

様式 2-2

暗号モジュール認証報告書

年　月　日
独立行政法人 情報処理推進機構
理事長名 印

記

暗号モジュール名：
バージョン：
暗号モジュール試験機関名：
暗号モジュール試験報告書
作成支援ツールバージョン：

暗号モジュール試験の結果、上記の暗号モジュールは、以下の暗号モジュールセキュリティ要件を満足することを認証したので報告します。

年　月　日

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

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：

暗号モジュールの仕様：	暗号モジュールのポートとインタフェース：
役割、サービス、及び認証：	有限状態モデル：
物理的セキュリティ：	動作環境：
暗号鍵管理：	自己テスト：
設計保証：	その他の攻撃への対処：

全体的なセキュリティレベル：

暗号モジュール試験時の構成：

暗号モジュールに搭載されている承認暗号アルゴリズム：

暗号モジュールに搭載されている非承認暗号アルゴリズム：

結果：

以上

様式 2-3

保証継続報告書

年　月　日
独立行政法人 情報処理推進機構
理事長名 印

記

認証番号　　：
暗号モジュール名：
バージョン　　：
適合規格：
試験要件：

上記の暗号モジュールについて、以下のとおり保証継続の結果を報告します。
年　月　日
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

全体的なセキュリティレベル：

暗号モジュールに搭載されている承認暗号アルゴリズム：

暗号モジュールに搭載されている非承認暗号アルゴリズム：

認証結果：

1 全体要約

1.1 はじめに

1.2 保証継続識別

1.2.1 後続暗号モジュール識別

本保証継続の対象とする後続暗号モジュールは、次のとおりである。

暗号モジュール名称：
バージョン：
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 ：

1.2.2 認証済み暗号モジュールセキュリティポリシ識別

本保証継続の認証済み暗号モジュールのセキュリティポリシは、以下のとおりである。

名称 ：
バージョン：
作成日 ：
作成者 ：

1.2.3 認証済み暗号モジュール認証報告書識別

本保証継続の認証済み暗号モジュールの認証報告書は、以下のとおりである。

暗号モジュール名称：
バージョン：
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 ：
受付番号：
認証番号：
作成日 ：
作成者 ：

1.3 報告概要

1.3.1 変更の記述

1.3.2 変更された開発文書

2 認証機関による保証継続の実施内容

2.1 実施概要

2.2 検証項目

3 結論

4 用語

5 参照

Cryptographic Algorithm Verification Certificate

Cryptographic Algorithm Implementation Name :
Version :

Cert#	Cryptographic Algorithm	Verified Configurations

Operational Environment(s) :

Vendor :

Accredited Cryptographic Module Testing Laboratory :
Applied Testing Tool(s) :

Notes : The cryptographic algorithm implementation identified in this certificate has been tested at the accredited Cryptographic Module Testing Laboratory in the Japan Cryptographic Module Validation Program, and the testing results have been validated in accordance with the Cryptographic Algorithm implementation Testing Requirements. This certificate applies only to the specific version of the cryptographic algorithm implementation in its tested configurations and operational environments. The Cryptographic Algorithm Implementation Tests have been conducted in accordance with the provisions of the Japan Cryptographic Module Validation Program and the conclusions of the testing laboratory in the testing report are consistent with evidence adduced. This certificate is not an endorsement of the cryptographic module by the Information-technology Promotion Agency or by any other organization that recognizes or gives effect to this certificate, and no warranty of the cryptographic module that uses this Cryptographic Algorithm Implementation by the Information-technology Promotion Agency or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied. The detailed information for the Cryptographic Algorithm Verification is addressed under the Register of Cryptographic Algorithm Verification.

Signature :_____ Date :_____
Name :_____
Title :_____
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

Cryptographic Module Validation Certificate

Certificate No.

Cryptographic Module Name :
Version :

Hardware Version :
Firmware Version :
Software Version :

Physical Embodiment :
Security Requirements :
Testing Requirements :

Vendor :
Address of Vendor :
Special Affairs :

Notes : The cryptographic module identified in this certificate has been tested at an accredited Cryptographic Module Testing Laboratory in the Japan Cryptographic Module Validation Program, and the testing results have been validated in accordance with the Cryptographic Module Testing Requirements. This certificate applies only to the specific version of the Cryptographic Module in its tested configurations and operational environments. The Cryptographic Module Tests have been conducted in accordance with the provisions of the Japan Cryptographic Module Validation Program and the conclusions of the testing laboratory in the testing report are consistent with evidence adduced. This certificate is not an endorsement of the cryptographic module by the Information-technology Promotion Agency or by any other organization that recognizes or gives effect to this certificate, and no warranty of the cryptographic module by the Information-technology Promotion Agency or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.
The misuse of this certificate, including the use of certificate for publications, such as advertisements and catalogs, in an incorrect or misleading manner may result in withdrawal of this certificate.

Signature : _____ Date : _____
Name : _____
Title : _____
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

Cryptographic Module Validation Report

The cryptographic module identified in this report has been validated in the following.

Cryptographic Module Name :
Version :

Accredited Cryptographic Module Testing Laboratory :
CRYPTIPA Version :

Cryptographic Module Specification :
Cryptographic Module Ports and Interfaces :
Roles, Services, and Authentication :
Finite State Model :
Physical Security :
Operational Environment :
Cryptographic Key Management :
Self-Tests :
Design Assurance :
Mitigation of Other Attacks :

tested in the following configuration(s) :

Overall Level Achieved :

The following Approved Cryptographic Algorithms are used :

The cryptographic module also contains the following non approved algorithms :

Test Results : Pass
The cryptographic module identified in this report has been tested on the basis of the testing requirements specified by the Japan Cryptographic Module Validation Program, and has achieved the scope of conformance to the specified security requirements from the test results.

Signature :_____ Date :_____
Name :_____
Title :_____

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

改正履歴

識別番号	CBM-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 30 年 6 月 29 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