暗号モジュール認証手続に係る様式集

# 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。」 |

1. 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。
2. 「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。

	1. 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。
	2. 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。
	3. 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。
	4. 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。
3. 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○週目：第○週目～第○週目：第○週目～第○週目：第○週目～第○週目：第○週目～第○週目：第○週目～第○週目：第○週目～第○週目：第○週目～第○週目：第○週目～第○週目：第○週目～第○週目：第○週目～第○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

３．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：

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：

４．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：

以上

# 様式9

# **秘密保持契約書**

（申請者の名称に置換え）（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、　　　　年　　月　　日付で申請受付された【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（保証継続含む。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、本契約が定める範囲を超えて複製及び第三者への開示をしてはならない。

2　本契約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　秘密である旨が事前または遅くとも申請時に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記されたもの。

3　前項にかかわらず、次の各号のいずれかに該当する情報は秘密情報に含まれないものとする。

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　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入手したもの。

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。

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、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。但し、認証申請件数の統計的処理、または円滑な認証業務実施体制の整備、改善等に資する場合を除く。

 (損害賠償)

第４条　乙が、その故意又は重大な過失によって本契約に違反した場合、乙は、それによって甲が現実に被った通常かつ直接の損害を賠償する責を負うものとする。なお、法的原因の如何を問わず、本条をもって本件認証業務に関する乙の責任の全てとする。

 (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記名押印又は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、その発効の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、右発効の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、本契約に基づく権利若しくは義務又は本契約上の地位を第三者に譲渡し、又は承継させてはならない。但し、行政組織に関する法令の改廃等により本件認証業務が乙から他の組織に承継等されることとなる場合は、自動的かつ当然に当該法令の定めに従うものとする。

 (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、甲乙双方の記名押印又は署名が揃った日に自動的に発効し、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、又は乙が甲から秘密情報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、甲乙記名押印又は署名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。