IT セキュリティ評価及び認証制度の基本規程

平成３０年７月

CCS-01

独立行政法人情報処理推進機構

目 次

IT セキュリティ評価及び認証制度の基本規程

制定　平成 19 年 5 月 7 日　2007 情総第 12 号
最終改正　平成 30 年 6 月 28 日　2018 情総第 176 号　一部改正

第 1 章 総則

1.1 本規程の目的

本規程は、情報処理の促進に関する法律（昭和 45 年法律第 90 号）第 43 条第 1 項第 5 号（情報処理に関する安全性及び信頼性の確保を図るため、情報処理システム（電子計算機及びプログラムの集合体であって、情報処理の業務を一体的に行うよう構成されたものをいう。）に関する技術上の評価を行うこと。）に基づき、独立行政法人情報処理推進機構（以下「**機構**」という。）が運営する IT セキュリティ評価及び認証制度（以下「**本制度**」という。）について定めるとともに、本制度に関して、IT 製品及びシステム（以下「**IT 製品等**」という。）の供給者、利用者並びに本制度の運営に関係する者が遵守しなければならない基本的事項を定める。

1.2 本制度の目的

本制度は、認証識別機能、暗号化機能、アクセス制御機能等のセキュリティ機能を実装したハードウェア、ソフトウェア又はファームウェアから構成される **IT 製品等**及び **PP** が、保護を必要とする情報資産及びシステム資源を適切に保護していることを、第三者が評価及び認証することにより、**IT 製品等**又は **PP** の利用者が、正確かつ詳細に把握できるようにすることを目的とする。

1.3 本制度の原則

本制度が **IT 製品等**及び **PP** の利用者に信頼されるため、評価機関及び認証機関は、公正、非差別的で商業的利害に影響されることなく、本規程の***附属書 A*** に掲げる ***IT セキュリティ評価基準***、***IT セキュリティ評価方法***、***IT セキュリティ評価基準補足文書***及び ***IT セキュリティ評価方法補足文書***（以下「**CC/CEM**」という。）に従い、高い技術力に基づいて適正な**評価**、**認証**又はセキュリティターゲットの確認（以下「**ST 確認**」という。）を行わなければならない。

1.4 評価及び認証又は ST 確認の要求事項

本制度で行う**評価**及び**認証**又は **ST 確認**の要求事項（requirements)は、**CC/CEM** とする。

1.5 用語の定義

(1) 略語

CC：コモンクライテリア (Common Criteria)
本規程の***附属書 A*** に掲げる ***IT セキュリティ評価基準***及び ***IT セキュリティ評価基準補足文書***の総称（以下「**CC**」という。）。

CEM：コモンエバリュエーションメソドロジー (Common Evaluation Methodology)
本規程の***附属書 A*** に掲げる ***IT セキュリティ評価方法***及び ***IT セキュリティ評価方法補足文書***の総称（以下「**CEM**」という。）。

PP：プロテクションプロファイル (Protection Profile)
ある **TOE (後述)** の分野で、共通的に利用可能な**セキュリティ要件**の集合を記載した文書(以下「**PP**」という。）。

ST：セキュリティターゲット (Security Target)
特定の **TOE (後述)** を評価するときの基となる**セキュリティ要件**及びセキュリティに係る仕様を記載した文書（以下「**ST**」という。）。

TOE：評価対象 (Target of Evaluation)
本制度による**評価**、**認証**及び **ST 確認**の対象となる **IT 製品等**及びその取扱説明書（以下「**TOE**」という。）。ただし、**ST 確認**の場合、取扱説明書は含まない。

(2) 用語

CC 承認アレンジメント (Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security) ：
セキュリティ評価及び認証の相互承認に関する国際アレンジメント（以下「**CCRA**」という。）。

ST 確認：
TOE の**評価**が**本制度**の定めに従って実施されたこと、及び当該評価結果が **ST** と機能仕様を対象とした**保証パッケージ**に適合していることの証明。

ST 確認報告書：
ST 及び **TOE** の機能仕様に対する**評価報告書**の概要及び**評価報告書**の検証過程で確認した事項を **IT 製品等**の利用者に対して提供するために**認証機関**が発行する文書。

確認書：
ST 確認の結果を証明するために**認証機関**が発行する文書。

機能パッケージ：
セキュリティ機能に係る要件をまとめたもの。**PP** において、調達者が求めるセキュリティ機能要件をまとめたもので、**ST** で参照するためのもの。

コモンエバリュエーションメソドロジー (Common Evaluation Methodology) ：
本規程の***附属書 A*** に掲げる ***IT セキュリティ評価方法***及び ***IT セキュリティ評価方法補足文書***の総称。

コモンクライテリア (Common Criteria) ：
本規程の***附属書 A*** に掲げる ***IT セキュリティ評価基準***及び ***IT セキュリティ評価基準補足文書***の総称。

サーベイランス：
既に**評価**及び**認証**又は **ST 確認**を受けた **IT 製品等**に対して、当該**評価**の妥当性を確認するための調査を**サーベイランス**という。

サポート文書 (Supporting Document) ：
特定の技術分野において CC/CEM に基づく評価方法、並びに関連する脆弱性、攻撃手法等の評価者が想定すべき情報についてまとめた技術文書。CCRA で承認を受けたサポート文書は CC/CEM に基づく**評価**において「必須（Mandatory）」又は「ガイダンス（Guidance）」が明記されるので、CC/CEM の補足文書として本制度において用いられる。

所見報告書：
評価機関が、**評価**の過程で **PP**、**ST** 若しくは**評価用提供物件**の問題点を発見したとき、又は**認証機関**に対して **CC/CEM** に関する問い合わせが必要となったときに作成する当該問題点又は **CC/CEM** に関する問い合わせ内容を記載した文書。

セキュリティターゲット (Security Target) ：
特定の **TOE** を評価するときの基となる**セキュリティ要件**及びセキュリティに係る仕様を記載した文書。

セキュリティ要件：

CC に規定されるセキュリティ機能に係る要件（requirements）及び**評価**すべき事項（保証コンポーネント）。

認証：
TOE 又は **PP** の**評価**が、**本制度**の定めに従って実施されたこと、及び当該評価結果が申請者（2.2.1 参照）の選択する**保証パッケージ**に適合していることの証明。

認証機関：
本制度に基づいて、**認証**及び **ST 確認**を実施する組織。

認証書：
認証の結果を証明するために**認証機関**が発行する文書。

認証報告書：
TOE 又は **PP** に対する**評価報告書**の概要及び**評価報告書**の検証過程で確認した事項を **IT 製品等**の利用者に対して提供するために**認証機関**が発行する文書。

認証レビュー：
認証機関が、**評価**の過程で **PP**、**ST** 若しくは**評価用提供物件**の問題点、又は評価内容の不備等を発見したときに**評価機関**に対して発行する当該問題点又は当該評価内容の不備等を記載した文書。

評価：
TOE、**PP** 又は **ST** の、**CC** への適合性を **CEM** に従って検査（assess）すること。

評価機関：
本制度に基づいて、**TOE**、**PP** 及び **ST** の**評価**を実施する組織。

評価対象 (Target of Evaluation)：
本制度による**評価**、**認証**及び **ST 確認**の対象となる **IT 製品等**及びその取扱説明書。ただし、**ST 確認**の場合、取扱説明書は含まない。

評価報告書：
申請者及び**認証機関**に対して**評価**の結果を報告するために、**評価機関**が発行する文書。

評価保証レベル（Evaluation Assurance Level）：

取り扱うデータの重要度の違いや異なる使用環境に対応し、費用対効果のある解決策を提供するために、あらかじめ 7 つのレベルに **CC** で定義された保証パッケージ（以下「**EAL**」という。）。各 **EAL** は、下のレベルの **EAL** で求められる事項に、より高度な評価すべき事項を加える形で定義されている。各レベルの詳細については、**CC** を参照すること。

評価用提供物件：
評価機関又は**認証機関**が、**TOE**、**PP** の**評価**及び**認証**又は **ST 確認**を実施するために、申請者又は開発者に要求する開発文書、取扱説明書等の物件。**TOE** の**評価**及び**認証**の場合、**評価用提供物件**には当該 **TOE** を含む。

プロテクションプロファイル (Protection Profile) :
ある **TOE** の分野で、共通的に利用可能なセキュリティ要件の集合を記載した文書。

保証継続 (Assurance Continuity) ：
評価及び**認証**を受けた IT 製品の**評価対象**が変更になった場合、先の**認証**について保証を継続すること。申請者又は開発者が作成した影響分析報告書及び開発環境の変更がある場合は評価機関から提出される評価報告書を認証機関が検査し、変更の度合いが小さくかつ**評価対象**のセキュリティ機能への影響が軽微であることを確認したときに、保証を継続する。

保証継続報告書：
申請者に対して**保証継続**の結果を報告するために**認証機関**が発行する文書。

保証パッケージ：
評価すべき事項（保証コンポーネント）の集合。申請者等は、**評価**すべき事項（保証コンポーネント）を組み合わせて**保証パッケージ**を作ることができる。

第２章 制度の体系

2.1 本制度に関する規程等

本制度に関する規程等は次のとおりである。

本制度に関して、申請者、利用者及び**本制度**の運営に関係する者が遵守しなければならない基本的事項を定めた文書。

＜IT セキュリティ評価及び認証制度における制度文書＞	
IT セキュリティ評価及び認証制度の基本規程(CCS-01)	「***制度基本規程***」

認証機関を構成する者が遵守しなければならない事項を定めた文書。

＜認証業務の運営に関する文書＞	
IT セキュリティ認証機関の組織及び業務運営に関する規程(CCM-01)	「***業務運営規程***」

認証申請を行う申請者が遵守しなければならない事項を定めた文書。

＜認証等に関する文書＞	
IT セキュリティ認証等に関する要求事項(CCM-02)	「***認証要求事項***」

評価機関の承認申請を行う者が遵守しなければならない事項を定めた文書。

＜評価機関の承認等に関する文書＞	
IT セキュリティ評価機関承認等に関する要求事項(CCM-03)	「***評価機関承認要求事項***」

ST 確認申請を行う申請者が遵守しなければならない事項を定めた文書。

＜ST 確認等に関する文書＞	
ST 確認等に関する要求事項(STM-01)	「***確認要求事項***」

注 1：「」内は、略称を示す。

注 2：上記 () 内の英字 3 文字の記号は、次の頭文字を取ったものである。

CCS ･･･ Common Criteria certification Scheme

CCM ･･･ Common Criteria certification body Management system

STM ･･･ Security Target evaluation and confirmation Manual for sponsors

2.2 制度を構成する者

本制度を構成する者を以下に規定する。

2.2.1 申請者

本制度において申請者とは、「***IT セキュリティ認証等に関する要求事項***」 (以下「***認証要求事項***」という。) 及び「***ST 確認等に関する要求事項***」 (以下「***確認要求事項***」という。) に基づき、**認証**又は **ST 確認**を申請する者である。原則として、CCRA 加盟国の、**PP** を用いて調達を実施する調達者、**TOE** 又は **PP** の供給者、ベンダその他の法人及び機関とする。

2.2.2 評価機関

本制度において**評価機関**とは、**CC/CEM** に基づいて **TOE**、**PP** 及び **ST** の**評価**を実施する組織である。**評価機関**は、**本制度**の**評価機関**として認定機関から認定を受け、「***IT セキュリティ評価機関承認等に関する要求事項***」 (以下「***評価機関承認要求事項***」という。) の手続に従って認証機関から当該製品分野に係る承認を得なければならない。

2.2.3 認証機関

本制度において**認証機関**とは、機構内に設置され、**評価機関**が行った評価結果に基づき、**認証**及び **ST 確認**を行う組織である。**認証機関**は、JIS Q 17065 又は **CCRA** で規定された要件を満たすように、体制を整備し運営を行うものとする。

2.2.4 認定機関

認定機関は、JIS Q 17025 又は ISO/IEC 17025 に基づき本制度における**評価機関**の認定を行う以下に定める組織である。

(1) 独立行政法人製品評価技術基盤機構内に設置された組織

(2) CCRA 認証国において正式に承認されている認定機関

第３章 評価及び認証

3.1 認証の申請

申請者は、***認証要求事項***に定めるところにより、**認証機関**に対して認証申請の手続を行わなければならない。**認証機関**は、「***IT セキュリティ認証機関の組織及び業務運営に関する規程***」 (以下「***業務運営規程***」という。) に定めるところにより、申請者からの**認証**の申請を受け付ける。

3.2 評価

評価機関は、申請者が選択した **CC/CEM** に基づき、**ST** 及び**評価用提供物件、**又は **PP** の評価を行う。**評価機関**は、評価に際して設備が必要な場合には、申請者又は外部機関の協力を要請することができる。**評価機関**は、評価の結果に基づき、**評価報告書**を作成し**認証機関**に提出しなければならない。

3.3 認証

認証機関は、***業務運営規程***に定めるところにより、**評価機関**から提出される**評価報告書**について**認証**を行い、**認証書**及び**認証報告書**を作成し申請者に授与する。

3.4 保証継続

認証を授与された **IT 製品等**の申請者（以下「**登録者**」という。）は、認証済み TOE の後続バージョン（以下「**変更 TOE**」という。）に対して、当初の**認証**の効果を継続しようとする場合に、***認証要求事項***に従い保証継続手続をとることができる。**認証機関**は、***業務運営規程***に定めるところにより保証継続手順に基づき保証継続を適用する。ただし、**変更 TOE** に生じた変更が大きなものである場合は、**保証継続**は適用できない。この場合、当初と同じ**評**

価及び**認証**の手続を適用して**認証**を得なければならない。

3.5 申請者が支払うべき費用

申請者は、**評価**及び**認証**に必要な費用を負担しなければならない。申請者が**評価機関**に対して支払うべき費用は、両者の契約により定める。**認証機関**に対して支払うべき費用は、**機構**の Web サイト等を通じて別途公表する。

3.6 評価機関が支払うべき費用

評価機関は、**評価機関**の承認に必要な費用を負担しなければならない。**認証機関**に対して支払うべき費用は、**機構**の Web サイト等を通じて別途公表する。

第４章 評価及び ST 確認

4.1 ST 確認の申請

申請者は、***確認要求事項***に定めるところにより、**認証機関**に対して ST 確認申請の手続を行わなければならない。**認証機関**は、***業務運営規程***に定めるところにより、申請者からの **ST 確認**の申請を受け付ける。

4.2 評価

評価機関は、申請者が選択した **CC/CEM** に基づき、**ST** 及び**評価用提供物件**の評価を行う。**評価機関**は、評価の結果に基づき、**評価報告書**を作成し**認証機関**に提出しなければならない。

4.3 ST 確認

認証機関は、***業務運営規程***に定めるところにより、**評価機関**から提出される**評価報告書**について **ST 確認**を行い、**確認書**及び **ST 確認報告書**を作成し申請者に授与する。

4.4 申請者が支払うべき費用

申請者は、**評価**及び **ST 確認**に必要な費用を負担しなければならない。申請者が**評価機関**に対して支払うべき費用は、両者の契約により定める。**認証機関**に対して支払うべき費用は、**機構**の Web サイト等を通じて別途公表する。

4.5 評価機関が支払うべき費用

評価機関は、**評価機関**の承認に必要な費用を負担しなければならない。**認証機関**に対して支払うべき費用は、**機構**の Web サイト等を通じて別途公表する。

第５章 申請者の権利及び義務

5.1 認証を授与された申請者の権利及び義務

登録者は、**TOE** 又は **PP** に関して以下の権利及び義務を有する。

a) **登録者**は、***認証要求事項***に定める**認証**を授与された申請者の責務を遵守しなければならない。

b) **登録者**は、**TOE** 又は **PP** を認証済みであるとして供給することができる。

c) **登録者**は、**TOE** 又は **PP** を認証済みであるとして供給するときに、***認証要求事項***に定める「認証マーク」及び「CCRA 認証マーク」を使用することができる。この場合に、***認証要求事項***に定める「認証マーク及び CCRA 認証マーク等の使用」を遵守しなければならない。

5.2 ST 確認を授与された申請者の権利及び義務

ST 確認を授与された **TOE** の申請者（以下「**ST 登録者**」という。）は、**TOE** の供給に関して以下の権利及び義務を有する。

a) **ST 登録者**は、***確認要求事項***に定める **ST 確認**を授与された申請者の責務を遵守しなければならない。

b) **ST 登録者**は、**TOE** を ST 確認済みであるとして供給することができる。

c) **ST 登録者**は、**TOE** を ST 確認済みであるとして供給するときに、***確認要求事項***に定める「認証マーク」を使用することができる。この場合に、***確認要求事項***に定める「認証マーク等の使用」を遵守しなければならない。

第６章 認証及び ST 確認の一時停止又は取消し

6.1 サーベイランス

認証機関は、**認証**又は **ST 確認**に関して***業務運営規程***に定めるところにより、**サーベイランス**を実施することがある。

6.2 再評価

認証機関は、**認証書**及び**確認書**の発行後に必要に応じて、***業務運営規程***に定めるところにより、再評価の実施を指示することがある。

6.3 一時停止又は取消し

認証機関は、**サーベイランス**及び再評価の結果、認証若しくは ST 確認済みの **TOE** に対して、***業務運営規程***に定めるところにより、**認証**若しくは **ST 確認**の一時停止又は取消しを行うことがある。

第 7 章 雑則

7.1 秘密保持

評価機関及び**認証機関**は、秘密情報が**評価**、**認証**及び **ST 確認**の過程で無権限の者に伝わり、情報の機密性が損なわれることがないようにしなければならない。**認証機関**における秘密保持手順については、***業務運営規程***に定める。

7.2 禁止事項

評価機関及び**認証機関**並びにこれらの職員は、次に掲げる事項を行ってはならない。

a) 正当な活動への対価以外の**評価**、**認証**及び **ST 確認**の結果に影響する利益を得ること。

b) **評価**、**認証**及び **ST 確認**の対象となる **TOE** の開発を行うこと。

c) 申請者に対するコンサルティングサービスの提供をすること。
なお、このコンサルティングサービスには、申請者が作成した多くの既存の文書等の情報を統合又は再編成を行うことを含まない。

7.3 認証機関が行う本制度の円滑な運営に必要な業務

7.3.1 規程類の整備

認証機関は、**本制度**を定め、**本制度**の運用のための方針及び規則を規定した規程類の作成、発行、配付、改定、更新及び廃止をするとともに、必要に応じて、**本制度**の方針及び規則の解釈を行う。

7.3.2 ガイダンスの発行と公表

認証機関は、**CC/CEM** 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、**機構**の Web サイト等で公表する。

7.3.3 評価の進捗状況の聴取等

認証機関は、必要に応じて、申請者若しくは**評価機関**又は両者に対し、**評価**の進捗状況及び評価結果の詳細を聴取することができる。
また、必要に応じて、申請者若しくは**評価機関**又は両者に対し、制度運営の観点から中立かつ公正な意見を述べることができる。

7.4 認証書等の著作権

認証書、**認証報告書**及び**保証継続報告書**に関する著作権は**認証機関**が保有する。ただし申請者は、**認証書**、**認証報告書**及び**保証継続報告書**を完全に複写する限りにおいて、複製し

て配付する権利が許諾される。
確認書及び **ST 確認報告書**に関する著作権は**認証機関**が保有する。ただし申請者は、**確認書**及び **ST 確認報告書**を完全に複写する限りにおいて、複製して配付する権利が許諾される。

7.5 認証書等の不正利用等への対処

認証機関は、**登録者**及び **ST 登録者**が「認証マーク」、「CCRA 認証マーク」、**認証書**、**認証報告書**、**保証継続報告書**、**確認書**若しくは **ST 確認報告書**、若しくはその写しを不正に使用すること、又は誤解を招くような方法で広告及び説明に使用することなど、**認証機関**が定める***誓約書***に違反する事実が認められた場合、改善の指示を行う。改善の指示を行った結果、その改善の効果が認められない場合、当該**認証**及び **ST 確認**を取り消すことができる。当該**認証**及び **ST 確認**の取消しに関し必要な事項について、***業務運営規程***に定める。

7.6 異議申立て、苦情及び紛争の処理

認証機関は、認証サービスに対する異議申立て、苦情及び紛争を***業務運営規程***に定められた手順に従って処理する。
評価機関は、**評価**に対する異議申立て、苦情及び紛争の処理に関する手続及び手順を整備しなければならない。

附　則（平成 19 年５月７日　2007 情総第 12 号・全部改正）

（施行期日）

１　この規程は、平成 19 年５月 15 日から施行する。

（IT セキュリティ認証に係る保証継続ガイドラインの廃止）

２　IT セキュリティ認証に係る保証継続ガイドライン　（平成 17 年７月 29 日　2005 情総第 39 号）は、廃止する。

附　則（平成 23 年１月 25 日　2010 情総第 160 号・一部改正）

この規程は、平成 23 年２月１日から施行する。

附　則（平成 24 年４月３日　2011 情総第 160 号・一部改正）

この規程は、平成 24 年３月 29 日から施行する。

附　則（平成 26 年３月 28 日　2013 情総第 170 号・一部改正）

この規程は、平成 26 年４月１日から施行する。

附　則（平成 27 年５月 28 日　2015 情総第 51 号・一部改正）

この規程は、平成 27 年 6 月 1 日から施行する。

附　則（平成 30 年 6 月 28 日　2018 情総第 176 号・一部改正）
この規程は、平成 30 年 7 月 1 日から施行する。

附属書 A：本制度の要求事項

本制度で用いる要求事項として、以下の (1) から (4) に示す規格を定める。規格を使用する者は、(1) 及び (2) の各々から使用する規格を選択するものとする。これらの規格を使用するときに (3) 、(4) に掲げる関連規格が存在する場合は、併用しなければならない。これらの規格において有効な規格バージョン等の情報は、認証機関が機構の Web サイト等を通じて別途公表する。

(1) ITセキュリティ評価基準
- ① ISO/IEC 15408 Information technology - Security techniques – Evaluation criteria for IT security
- ② Common Criteria for Information Technology Security Evaluation
  注：国際的なITセキュリティ評価及び認証の相互承認体制「CC承認アレンジメント」(CCRA) が発行したITセキュリティ評価の規格である。
- ③　②の日本語版を規格として制定したもの。

(2) ITセキュリティ評価方法
- ① ISO/IEC 18045 Information technology - Security techniques - Methodology for IT security evaluation
- ② Common Methodology for Information Technology Security Evaluation
  注：国際的なITセキュリティ評価及び認証の相互承認体制「CC承認アレンジメント」(CCRA) が発行したITセキュリティ評価方法の規格である。
- ③　②の日本語版を規格として制定したもの。

(3) ITセキュリティ評価基準補足文書
認証機関が公表する、ITセキュリティ評価基準を補足する文書。

(4) ITセキュリティ評価方法補足文書
認証機関が公表する、ITセキュリティ評価方法を補足する文書。