認定－部門－ TIRP21

ASNITE 試験事業者 IT 公表用文書

ASNITE 試験事業者 IT 認定の一般要求事項

（第 ~~8~~9 版）

平成 19 年 ~~2~~4 月 1 日

独立行政法人製品評価技術基盤機構
認定センター

目　次

ASNITE 試験事業者 IT 認定の一般要求事項

第 1 部　総則

1.1　目的

この規程は、独立行政法人製品評価技術基盤機構（以下「NITE」という。）の認定センター（以下「認定機関」という。）が運営する製品評価技術基盤機構認定制度試験事業者 IT 認定~~サブ~~プログラム ~~IT~~（以下「ASNITE 試験事業者 IT」という。）において、試験事業者が認定を受けるために必要な要求事項、及び認定を受けた試験事業者がその認定を維持するために必要な要求事項を定めることを目的とする。

1.2　適用範囲

1.2.1　この規程は、ASNITE 試験事業者 IT の認定を希望する試験事業者（以下「申請事業者」という。）及び ASNITE 試験事業者 IT の認定を受けた試験事業者（以下「認定事業者」という。）に適用する。ただし、海外にある事業所により、1.2.2 で定める暗号モジュール試験を行う試験事業者には適用しない。

1.2.2　この規程を適用する試験事業者の認定分野及び認定区分は、下表のとおりとする。

認定分野	認定区分	（参考：認証制度上の区分）
情報技術	コモンクライテリア評価	JISEC（注 1）における評価機関
	暗号モジュール試験	JCMVP（注 2）における試験機関

（注 1）JISEC：IT セキュリティ評価及び認証制度
（注 2）JCMVP：暗号モジュール試験及び認証制度

1.2.3　この規程は、独立行政法人情報処理推進機構（以下「IPA」という。）が発行する、次に掲げる規程等と併せ読むことにより、ASNITE 試験事業者 IT の認定に係る要求事項がより明確になる。

(1) IT セキュリティ評価及び認証制度の基本規程~~（EC-01）~~
(2) 評価機関承認業務取扱規程~~（EC-06）~~
(3) 暗号モジュール試験及び認証制度の基本規程~~（JCM-01）~~
(4) 暗号モジュール試験機関承認業務取扱手順~~（CBM-01-B）~~

1.3　引用規格

この規程では、次に掲げる国際規格の最新版を引用する。ただし、これらの規格を翻訳し、技術的内容及び規格票の様式を変更することなく作成した日本工業規格に読み替えてもよい。

(1) ISO/IEC 17000 Conformity Assessment - Vocaburary and general principles（適合性評価－用語及び一般原則）
(2) ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories（試験所及び校正機関の能力に関する一般要求事項）
(3) ISO/IEC Guide 43-1 Proficiency testing by interlaboratory comparisons - Part 1: Development and operation of proficiency testing schemes（試

験所間比較による技能試験－第 1 部：技能試験スキームの開発及び運営）

(4) ISO/IEC Guide 43-2 Proficiency testing by interlaboratory comparisons - Part 2: Selection and use of proficiency testing schemes by laboratory accreditation bodies（試験所間比較による技能試験 第 2 部：試験所認定機関による技能試験スキームの選定及び利用）

(5) ISO/IEC 17011 Conformity assessment - General requirements for accreditation bodies accrediting conformity assessment bodies（適合性評価－適合性評価機関の認定を行う認定機関に対する一般要求事項）

(6) ISO/IEC 15408-1 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model（セキュリティ技術－情報技術セキュリティの評価基準－第 1 部：総則及び一般モデル）

(7) ISO/IEC 15408-2 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements（セキュリティ技術－情報技術セキュリティの評価基準－第 2 部：セキュリティ機能要件）

(8) ISO/IEC 15408-3 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements（セキュリティ技術－情報技術セキュリティの評価基準－第 3 部：セキュリティ保証要件）

(9) ISO/IEC 18045 Information Technology - Security Techniques - Methodology for IT Security Evaluation（情報技術セキュリティ評価のための共通方法）

(10) ISO/IEC 19790 Information technology -- Security techniques -- Security requirements for cryptographic modules（情報技術－セキュリティ技法－暗号モジュールのセキュリティ要求事項）

1.4 定義

1.4.1　CC 認証機関：JISEC に従って、TOE 及び PP のセキュリティ評価に係る認証並びに ST のセキュリティ評価に係る確認を行う IPA の認証機関組織をいう。CC 認証機関は、1.4.5 で定める IT セキュリティ評価基準への適合性について、1.4.3 で定める評価機関から提出される評価報告書等に基づき検証し、TOE 及び PP に対する認証並びに ST に対する確認を行う。

1.4.2　CM 認証機関：JCMVP に従って、暗号モジュールの認証を行う IPA の認証機関組織をいう。CM 認証機関は、1.4.11 で定める暗号モジュールセキュリティ要件への適合性について、1.4.4 で定める試験機関から提出される試験報告書等に基づき検証し、暗号モジュールに対する認証及び暗号アルゴリズム試験の結果に対する確認を行う。

1.4.3　評価機関：認定区分がコモンクライテリア評価の認定事業者をいう。評価機関は、TOE、PP 等に対する評価を行う。

1.4.4　試験機関：認定区分が暗号モジュール試験の認定事業者をいう。試験機関は、暗号モジュールに対する試験及び CM 認証機関から貸与される暗号アルゴリズム試験を行うことを目的としたツールを用いた暗号アルゴリズムに対する試験を行う。

1.4.5　IT セキュリティ評価基準：コモンクライテリア評価に用いる基準であって、次に掲げるものをいい、1.4.6 で定める IT セキュリティ評価基準補足文書を含む（以下

「CC」という。）。
(1) ISO/IEC 15408-1、ISO/IEC 15408-2 及び ISO/IEC 15408-3
(2) Common Criteria for Information Technology Security Evaluation
① Part 1: Introduction and general model
② Part 2: Security functional requirements
③ Part 3: Security assurance requirements
(3) CC 認証機関が公開する(2)の翻訳文書。この翻訳文書を使用する場合において、翻訳文書と JIS で使用される用語が異なるときは、翻訳文書に添付の対象表を参照すること。

1.4.6　IT セキュリティ評価基準補足文書：CC 認証機関が公開する補足文書であって、IT セキュリティ評価基準とともに用いなければならないものをいう。

1.4.7　IT セキュリティ評価方法：コモンクライテリア評価に用いる方法であって、次に掲げるものをいい、1.4.8 で定める IT セキュリティ評価方法補足文書を含む（以下「CEM」という。）。
(1) ISO/IEC 18045
(2) Common Methodology for Information Technology Security Evaluation
(3) CC 認証機関が公開する(2)の翻訳文書。この翻訳文書を使用する場合において、翻訳文書と JIS で使用される用語が異なるときは、翻訳文書に添付の対象表を参照すること。

1.4.8　IT セキュリティ評価方法補足文書：CC 認証機関が公開する補足文書であって、IT セキュリティ評価方法とともに用いなければならないものをいう。

1.4.9　申請者（Sponsor）：JISEC に基づき、コモンクライテリア評価及び認証の申請を行う者をいう。

1.4.10 暗号モジュール：CM 認証機関が承認した暗号モジュールセキュリティ機能（動作モードを伴う暗号アルゴリズム。）を実装し、物理的な境界が明示的に定義された暗号境界内において暗号処理を行うハードウェア、ソフトウェア、ファームウェア及び／又はこれらの組み合わせをいう。

1.4.11 暗号モジュールセキュリティ要件：暗号モジュール及びそれが実装する暗号アルゴリズムのためのセキュリティ要求事項であって、次に掲げるものをいう。
(1) ISO/IEC 19790
(2) 日本工業規格に定める暗号モジュールのセキュリティ要件に係る基準
(3) CM 認証機関が公開する(1)及び／又は(2)と同等の文書

1.4.12 暗号モジュール試験要件：暗号モジュール及びそれが実装する暗号アルゴリズムのための試験要求事項であって、次に掲げるものをいう。
(1) 国際標準化機構及び国際電気標準会議が定めた暗号モジュールの試験要件に係る基準
(2) 日本工業規格に定める暗号モジュールの試験要件に係る基準
(3) CM 認証機関が公開する(1)及び／又は(2)と同等の文書

1.4.13 暗号アルゴリズム試験要件：暗号モジュール試験の一部として実施される暗号アルゴリズム試験のための要求事項であって、CM 認証機関が公開する文書をいう。

1.4.14 運用ガイダンス：CM 認証機関が公開する JCMVP 運用ガイダンスをいう。

1.4.15 検証：規程要求事項に合致していることを検査及び証拠提示によって確認することをいう。

1.4.16 上記 1.4.1 から 1.4.15 までに掲げるもののほか、この規程に係る用語の定義は、ISO/IEC 15408、ISO/IEC 17000 及び ISO/IEC 19790 のうち該当する定義を適用する。

第 2 部　認定区分：コモンクライテリア評価の試験事業者に対する一般要求事項

2.1　一般

2.1.1　認定機関は、申請事業者及び評価機関に対し、ISO/IEC 17025 の該当する項目を、ASNITE 試験事業者 IT の認定（認定区分：コモンクライテリア評価）のための一般要求事項として適用する。

2.1.2　認定機関は、第 2 部に掲げる規定を、前項の規定に基づく一般要求事項の適用方針とする。

2.2　マネジメントシステムの対象範囲（ISO/IEC 17025 4.1.3 項）

申請事業者及び評価機関は、マネジメントシステムの対象となる範囲について、文書（品質マニュアル等）で明確にしなければならない。特に認定範囲については、次の(1)から(4~~5~~)までのいずれかの範囲としなければならない（注）。

(1) クラス APE、~~クラス ASE~~EAL 1 及び EAL ~~1~~2 ~~注 1~~

(2) クラス APE、~~クラス ASE 注 2~~、EAL 1、EAL 2~~1~~ 及び EAL 3~~2~~

(3) クラス APE、~~クラス ASE 注 2~~、EAL 1、EAL 2、EAL 3 及び EAL 4~~3~~

(4) クラス APE、~~クラス ASE 注 2~~、EAL 1、EAL 2、EAL 3、EAL 4 及び EAL 5~~4~~

~~(5) クラス APE、クラス ASE 注 2、EAL 1、EAL 2、EAL 3、EAL 4 及び EAL 5 注 3~~

注 ~~1~~：~~CC バージョン 3 にて認定を受ける場合、この(1)の範囲は適用できない。また、~~平成 19 年 4 月 2 日以降は、CC バージョン 2.3 以前のバージョン~~この(1)の範囲~~で認定申請することはできない。また、これらの EAL には、クラス ASE の該当コンポーネントが含まれる。~~

~~注 2：CC バージョン 3 の場合、クラス ASE は EAL に含まれるが、認定申請の際には(2)～(5)のようにクラス ASE が認定範囲に含まれることを明記すること。~~

~~注 3：CC バージョン 3 にて認定を受ける場合のみ適用される。~~

2.3　技術的記録（ISO/IEC 17025 4.13.2.1 項）

申請事業者及び評価機関は、技術的記録の保存期間について、申請者（Sponsor）が評価機関から返却された資料等を保存する期間、保証継続等の手続きを勘案して適切なものとしなければならない。

参考：IT セキュリティ評価及び認証制度の基本規程では、評価機関から返却された資料等は必要な期間保存するとともに、その資料等が開発者に帰属する場合は契約等により同等な期間、開発者に保存させることが申請者（Sponsor）の責務となっている。評価を行った TOE の市場における使用状況を勘案して、5 年間保存することは良い方法の一つである。

2.4　要員の適格性及び資格（ISO/IEC 17025 4.1.5 項 h)、5.2.1 項）

2.4.1　申請事業者及び評価機関の技術管理主体の適格性

(1) 技術管理主体は、評価業務の技術的事項の全責任を負う。

(2) 技術管理主体は、評価業務に係る十分な技術的知識を持ち、評価結果の正確な評価を行う能力を有すること。

(3) 技術管理主体は、下記の知識並びに評価者の教育・訓練及び適切な監督・指示を行う能力を有すること。

① 評価報告書の作成を含め、IT セキュリティ評価に係る一般要求事項
② CC に係る知識
③ CEM に係る知識

(4) 技術管理主体の管理者（技術管理者及びその代理者）は、下記の知識又は IT 製品等の開発経験若しくは ST の作成を含む評価業務に関連した分野で 3 年以上の経験を有することが望ましい。

なお、独立行政法人情報処理推進機構情報処理技術者試験センターが実施する基本情報技術者試験又はこれと同等以上の試験に合格することを以て、下記の知識又は IT 製品等の開発経験に代用することができる。

① コンピュータサイエンス
② コンピュータエンジニアリング
③ コンピュータセキュリティ
④ オペレーティングシステム
⑤ アルゴリズムとデータ構造
⑥ データベースシステム
⑦ プログラミング言語
⑧ コンピュータシステムアーキテクチャ
⑨ ネットワーク

(5) 上記(2)から(4)までの知識、経験等は、最近のものであることが望ましい。

2.4.2 申請事業者及び評価機関の評価者の適格性及び資格

(1) 評価者は、評価業務に係る内部資格を有すること。
(2) 評価者は、2.4.1(3)に定める知識を有し、その内部資格基準は適切であること。
(3) 評価者は、2.4.1(4)に定める知識又は IT 製品等の開発経験若しくは ST の作成を含む評価業務に関連した分野で 1 年以上の経験を有することが望ましい。

なお、2.4.1(4)なお書きに基づく試験に合格することを以て、これらの知識又は IT 製品等の開発経験に代用することができる。

(4) 上記(2)及び(3)の知識、経験等は、最近のものであることが望ましい。

2.4.3 CC 認証機関による資格付与

(1) 評価機関は、CC 認証機関の監督の下で行われる評価者資格を付与することを目的とした評価（試行評価）で良好な成績を収め、CC 認証機関により資格付与された評価者を 1 名以上置かなければならない。
(2) 上記(1)における資格付与の範囲は、2.2 に定めるすべての認定範囲を含まなければならない。

2.5 要員の教育・訓練（ISO/IEC 17025 5.2.2 項）

2.5.1 申請事業者及び評価機関の管理主体は、評価者を含めた要員に教育・訓練を提供するための方針及び手順を有しなければならない。当該教育・訓練プログラムは、申請事業者及び評価機関の業務に対して適切でなければならない。

2.5.2 前項の教育・訓練プログラムは、少なくとも 2.4.1(3)の項目について集中して行わなければならない。また、評価業務に必要な場合には、2.4.1(4)の項目に係る教育・訓練を行わなければならない。これらの教育・訓練は、継続して適切な評価が実施できるよう、又、最新の技術に対応できるように評価者に対して定期的かつ計画的に行わなければならない。

2.6 施設及び環境条件（ISO/IEC 17025 4.1.5 項 c)及び 5.3 項）

2.6.1　施設の機密保護及び所有権の保護

(1) 申請事業者及び評価機関は、少なくとも次に掲げる施設等について自ら管理するとともに、申請者（Sponsor）の機密保護及び所有権の保護を確実にするための方針及び手順を有しなければならない。

①　評価を行う施設（評価室）

②　評価に係る機密情報の保管場所

③　評価に係る機密情報の転送を行うツール（FAX、電子メール等）を有する施設

参考：上記②及び③は、①の中に設置してもよいし、①とは別の場所に設置してもよいが、いずれにおいても、機密保護及び所有権の保護を適切に行うこと。

(2) 申請事業者及び評価機関は、評価室について、機密保護及び所有権の保護の観点から評価作業に必要な最小限のものとすること。

(3) 保管場所に係る方針及び手順には、少なくとも次に掲げる項目を包含することが望ましい。

①　評価に係る機密情報は、やむを得ない場合（例えば、申請者（Sponsor）のサイトでテストを行う場合、CC 認証機関との連絡を行う場合等）を除き、持ち出さないこと。

②　評価に係る機密情報が不要となったときは、復元不可能な状態で廃棄又は消去すること。申請者（Sponsor）等に返却する必要があるときは、確実に返却すること。

例）復元不可能な状態での廃棄又は消去の例として、紙媒体にあってはシュレッダー等による廃棄又は紙の溶解処理装置による溶解、電子媒体にあっては当該媒体の初期化又は物理的な破壊がある。

(4) 申請事業者及び評価機関は、評価に係る機密情報の転送を行う場合には、送信側、受信側を含む転送経路における機密保護を確実にすること。その転送経路の一部又は全部の機密保護が確実ではない場合には、機密情報を保護するための手段をとること。

例）電子メールにて送受信する場合の機密保護として、機密情報は当該メール本文には包含せず添付ファイルに包含させた上で、その添付ファイルを暗号化する方法がある。

例）やむを得ず FAX にて送信する場合の機密保護として、送信前にあらかじめ受信者に電話連絡の上、FAX 機の前で待機して貰う方法がある。

(5) 申請事業者及び評価機関は、申請者（Sponsor）の機密情報及び所有権の保護に係る倫理規定を整備しなければならない。

2.6.2　評価を行う施設及びその環境条件

(1) 申請事業者及び評価機関は、恒久的な施設以外の場所（例えば申請者(Sponsor)のサイトなど）で評価を行う場合には、その環境を ISO/IEC 17025 5.3 項の要求事項を満たすものに適合させなければならない。

(2) 申請事業者及び評価機関は、権限のないものからのアクセスがあり得る環境において評価を行う場合には、評価の実施中はそのアクセスを禁止するような方法で評価環境を制御しなければならない。そのような評価環境に含まれるネットワークは、外部ネットワークと分離するか、少なくとも評価中はそのネットワークに権限のないものからのアクセスを禁止するような制御メカニズムを備えなければならない。

2.7　評価の方法（ISO/IEC 17025 5.4.1 項）

2.7.1　申請事業者及び評価機関は、評価の基準として CC を、評価の方法として CEM を用いなければならない。

2.7.2　申請事業者及び評価機関は、CC 及び CEM がそのままでは特定の IT 製品又はシ

ステムのセキュリティ評価に使用できない場合には、必要に応じて CC 及び CEM の規定と矛盾のない内容で文書化された手順を持つこと。

2.8　規格外の方法（ISO/IEC 17025 5.4.4 項）

2.8.1　コモンクライテリア評価への適用のために CC 認証機関が発行したガイド文書は、「規格に規定された方法」とみなされ、規格外の方法に該当しない。

2.8.2　申請事業者及び評価機関は、CEM で規定されていない規格外の方法を採用するときは、CC 認証機関によりその方法の妥当性が確認されたものについて、必ず申請者（Sponsor）の同意に基づき採用し、評価報告書にその詳細を記述しなければならない。このような規格外の方法としては、次のようなものが該当する。

(1) EAL 4 を超える保証コンポーネントのための評価方法

(2) 規格に規定された方法の変更（例えば、規格の組み合わせ、規格の適用範囲を越えた適用、規格の変更・拡張等）

2.8.3　ISO/IEC 17025 5.4.4 項 注記の a）から k）までの情報のうちいくつかの項目は、コモンクライテリア評価においては適用しない。この場合において、「…適用しない。」は、ISO/IEC 17025 では要求されている事項であるが、セキュリティ評価試験の特殊性にかんがみて、これらの項目について適用しなくても「要求事項を満足できる。」という趣旨である。以下「…適用しない。」という場合も同様とする。

2.9　方法の妥当性確認（ISO/IEC 17025 5.4.5.2 項）

ISO/IEC 17025 5.4.5.2 項 注記 2.のうち「参照標準又は標準物質を用いた校正」などの方法は、コモンクライテリア評価においては適用しない。

2.10　測定の不確かさの推定（ISO/IEC 17025 5.4.6 項）

ISO/IEC 17025 5.4.6 項は、コモンクライテリア評価においては適用しない。

2.11　設備の保有（ISO/IEC 17025 5.5.1 項）

2.11.1　申請事業者及び評価機関は、セキュリティ評価のために必要な設備を、購入、リース又はレンタルによって保有し、常時使用できるようにしなければならない。これらの設備には、セキュリティ評価を行うために申請事業者又は評価機関が使用するソフトウェア評価ツール、テストツール又は他の評価用機械装置を含めるものとする。

2.11.2　申請事業者及び評価機関は、テストツール等がソフトウェアの場合には、当該ソフトウェアが ISO/IEC 17025 5.4.7 項に適合することを確保しなければならない。

2.11.3　申請事業者及び評価機関は、申請者（Sponsor）などの顧客が所有する設備等、評価機関が恒久的に管理している設備以外の設備を一時的にセキュリティ評価に用いたときは、申請者（Sponsor）などの顧客等と契約を締結することにより、ISO/IEC 17025 5.5 項への適合性を確保しなければならない。

参考：契約の内容は、必要かつ十分なものであること。例えば、再評価のために申請者（Sponsor）が所有するツールを再度使用しなければならないときは、「最初の評価のときと同等のテスト環境を再現できること。」が確保できればよく、最初の評価で用いたツールの維持・保管まで契約で求める必要はない。

2.12　設備の維持（ISO/IEC 17025 5.5.2 項）

2.12.1　申請事業者及び評価機関は、セキュリティ評価を行うために用いる設備を、次に掲げる事項に従って維持しなければならない。

(1) 製造業者の推奨。
(2) 適用可能な場合、申請事業者及び評価機関が文書化した手順。

2.12.2　申請事業者及び評価機関は、評価行為を妨げたり、いかなる点においても評価中の IT 製品又はシステムのセキュリティ機能の完全性を損なわないことを確実にするために、設備を検証すること。

備考：セキュリティ評価に用いる設備の検証は、ある設備の指示値とそれに対する測定値の既知の値との差が、規格、法令又は当該設備の規定仕様書に定められた最大許容差より、一貫して小さいことを確かめるための手段となる。検証の結果、使用のために機能を回復させる、調整を行う、修理する、又は使用から取り外す、廃棄する、という判断を行うことになる。

2.13　測定のトレーサビリティ（ISO/IEC 17025 5.6 項）

2.13.1　申請事業者及び評価機関は、セキュリティ評価の結果の正確さ又は有効性に重大な影響をもつ設備について、確立された校正計画を持ち、適切な校正を実施することにより国際単位系（SI）への測定のトレーサビリティを確保すること。このトレーサビリティは、ISO/IEC 17025 4.5 項に基づきセキュリティ評価の下請負契約をしたとき、2.11.3 の規定に基づき顧客の設備を用いたときも確保すること。

ここで、「セキュリティ評価の結果の正確さ又は有効性に重大な影響をもつ」設備とは、セキュリティ評価に係る評価者テストに用いられる測定装置及びそれらの参照標準であって、評価者テストの結果のトレーサビリティの確保に不可欠なものをいう。

参考：トレーサビリティの確保が必要な設備の例としては、次のようなものがある。
(1) スマートカードが-200 ℃での使用に耐えうることを確認するため、そのスマートカードの評価者テストに用いる温度計
(2) 評価ツールである DPA（Differential Power Analysis）用の電力計の検証に用いる標準電圧発生装置等

2.13.2　申請事業者及び評価機関は、前項のトレーサビリティの証拠となる記録を保持しなければならない。可能な場合、次のいずれかの記録によって測定のトレーサビリティを証明すること。
(1) 国家計量標準研究所が CIPM-MRA（注 1）のもとで発行する校正証明書又はこれと同等の校正証明書（注 2）
(2) JCSS 標章付校正証明書（注 3）又は JCSS 認定シンボル付校正証明書（注 4）
(3) ASNITE 校正（注 5）の認定を受けた校正事業者が発行する ASNITE 認定シンボル付校正証明書
(4) ILAC（注 6）MRA に署名する認定機関の認定を受けた校正事業者が発行する認定シンボル付校正証明書
(5) ASNITE-RM（注 7）の認定を受けた標準物質生産者が発行する認証標準物質の認証書

（注 1）CIPM-MRA：CIPM（Comité International des Poids et Mesures：国際度量衡委員会）のもと国家計量標準研究所間で締結された、国家計量標準と校正証明書の MRA（Mutual Recognition Arrangement：相互承認協定）。

（注 2）これと同等の校正証明書：外国の国家計量標準研究所が発行する校正証明書が含まれる。この場合、その国家計量標準研究所は、その校正を実施する分野において CIPM-MRA に参加し、かつ、CIPM、APMP 等の基幹比較（計量標準の国家計量標準研究所間の国際試験所間比較）等で良好な成績を残していることが必要である。この証明書には ASNITE-NMI（注 8）認定シンボル付校正証明書が含まれる。

（注 3）JCSS 標章付校正証明書：JCSS（計量法校正事業者登録制度）登録事業者が発行するもの。
（注 4）JCSS 認定シンボル付校正証明書：国際 MRA 対応 JCSS 認定事業者が発行するもの。
（注 5）ASNITE 校正：製品評価技術基盤機構認定制度 校正事業者認定サブプログラム
（注 6）ILAC：International Laboratory Accreditation Cooperation（国際試験所認定協力機構）
（注 7）ASNITE-RM：製品評価技術基盤機構認定制度 標準物質生産者認定サブプログラム
（注 8）ASNITE-NMI：製品評価技術基盤機構認定制度 国家計量標準研究所認定サブプログラム

2.13.3　コモンクライテリア評価において、ISO/IEC 17025 5.6.2.1 項は適用しない。

2.13.4　コモンクライテリア評価において、セキュリティ評価全体のトレーサビリティは、ISO/IEC 17025 5.6.2.2.2 項で規定する「合意された方法へのトレーサビリティ」を適用する。この場合、「セキュリティ評価活動が『CC に評価者アクションエレメントとして規定されている事項』及び『CEM に評価者アクションとして規定されている事項』にトレーサブルでなければならない。」と解釈する。

参考：評価機関が行ったセキュリティ評価及びその評価結果に基づき CC 認証機関が認証したとき、そのセキュリティ評価活動は、CC 及び CEM にトレーサブルであることが CC 認証機関によって証明されたといえる。

2.14　サンプリング（ISO/IEC 17025 5.7 項）

コモンクライテリア評価において、ISO/IEC 17025 5.7 項は適用しない。

2.15　評価品目の取り扱い及び識別（ISO/IEC 17025 5.8.2 項）

2.15.1　申請事業者及び評価機関は、評価用提供物件（PP、ST、TOE、開発者作成文書等を含む。以下同じ。）について、不当に改変されたり、権限のないものがアクセスして使用することがないよう保護しなければならない。

2.15.2　申請事業者及び評価機関は、同時に複数の TOE を評価する必要があるときは、個々の TOE、評価プラットフォーム及び周辺設備並びに関連記録が混同しないよう、評価品目を識別するシステムを維持しなければならない。

2.16　評価品目の取り扱い及び保管（ISO/IEC 17025 5.8.4 項）

2.16.1　申請事業者及び評価機関は、評価用提供物件に係る所有権保護システムを有すること。このシステムは、申請者（Sponsor）等に所有権があるもの（例えば、ハードウェア、ソフトウェア、評価データ、紙媒体若しくは電子媒体による文書及び記録、その他の資料等）を保護するために十分なものであること。

2.16.2　前項のシステムは、申請事業者若しくは評価機関への訪問者、情報を持つ必要のない関係職員及び権限のないものから、申請者（Sponsor）等に所有権があるものを保護できるものであること。

2.16.3　申請事業者及び評価機関は、TOE 又はその一部がソフトウェア部分で構成されているときには、構成管理システムを持ち適切に管理するとともに、評価中にソフトウェア部分が不注意で又は不当に改変されることがないよう、その構成管理システムが適切であることを確実にすること。

2.17　結果の報告に係る一般要求事項（ISO/IEC 17025 5.10.1 項）

2.17.1　コモンクライテリア評価において、ISO/IEC 17025 5.10.1 項の「試験報告書」に該当するのは「評価報告書」とする。評価報告書の様式は、申請事業者及び評価機関が定めた様式であって、認定機関に届出たものを使用すること。

2.17.2　申請事業者及び評価機関は、行った評価業務に係る評価報告書を発行する。申請者（Sponsor）へ提出する評価報告書は、申請者（Sponsor）との契約上必要な事項及びこの要求事項を満たすものであること。申請事業者及び評価機関は、セキュリティ評価の結果を裏付ける証拠を提供できること。

2.17.3　ISO/IEC 17011 8.3 項に認定の言及及び認定シンボルの使用についての要求事項がある。これに対応して認定機関は、認定シンボルの使用方法等を別途取り決め、発行する。認定範囲外のセキュリティ評価（例えば EAL5 以上の保証コンポーネントに係る評価）の結果を認定シンボル付評価報告書に含めることについては、それらの評価結果が認定範囲外のセキュリティ評価結果であることが明確に識別されていなければならない。

2.18　評価報告書（ISO/IEC 17025 5.10.2 項、5.10.3 項及び 5.10.4 項）

2.18.1　申請事業者及び評価機関は、評価報告書の発行（承認）に責任を有する者を、認定機関に評価報告書発行責任者として届出なければならない。評価報告書発行責任者は、評価報告書に署名又は捺印すること。また、評価報告書発行責任者の不在の場合に備えて代理者を指名すること（ISO/IEC 17025 4.1.5 項 注記を参照のこと。）。

2.18.2　TOE 等の評価の年月日については、評価に要したすべての実施年月日（期間であってもよい）又は実施期間のうち最終日を記載するものとする。

2.18.3　評価報告書は、一件の TOE 等に対して複数部発行してもよい。この場合においては個々の報告書に固有の識別を必要とする。報告書の複写については、4.10.4(2)に定める規定に従うものとする。

2.18.4　コモンクライテリア評価において、ISO/IEC 17025 5.10.4 項は適用しない。

第 3 部　認定区分：暗号モジュール試験の試験事業者に対する一般要求事項

3.1　一般

3.1.1　認定機関は、申請事業者及び試験機関に対し、ISO/IEC 17025 の該当する項目を、ASNITE 試験事業者 IT の認定（認定区分：暗号モジュール試験）のための一般要求事項として適用する。

3.1.2　認定機関は、第 3 部に掲げる規定を、前項の規定に基づく一般要求事項の適用方針とする。

3.2　マネジメントシステムの対象範囲（ISO/IEC 17025 4.1.3 項）

申請事業者及び試験機関は、対象となる範囲について、文書（品質マニュアル等）で明確にしなければならない。特に認定範囲については、取り扱う試験サービス（暗号モジュールの試験、暗号アルゴリズムの試験及びこれらの試験手順）及び取り扱う暗号モジュールの種類について明確にしなければならない。

3.3　技術的記録（ISO/IEC 17025 4.13.2.1 項）

3.3.1　申請事業者及び試験機関は、技術的記録の保存期間について、顧客が試験機関か

ら返却された資料等を保管する期間、顧客が要求した保存期間等を勘案して適切なものとしなければならない。

参考：試験を行った暗号モジュールの市場における使用状況を勘案して、5 年間保存することは良い方法の一つである。

3.3.2　申請事業者及び試験機関は、少なくとも次に掲げる技術的記録について、保存期間を定めて保存しなければならない。

(1) ソフトウェアのバージョン及び更新に係る記録

(2) 試験方法及び試験データに係る記録

① 試験の方針及び条件に係る記述

② 試験用に提出された暗号モジュールの、暗号モジュールセキュリティ要件への適合／不適合

③ 試験品目及び試験活動のトレーサビリティに係る包括的な記録

④ 試験データ（該当する場合、図表、暗号アルゴリズムの試験スイート、写真、画像等を含む。）及び正式な試験報告書の写し

⑤ 試験機関から CM 認証機関に対する質問とそれに対する回答の通信ファイル

(3) 参照標準、試験設備及び試験装置並びにこれらの校正又は検証の記録

① 名称及びその補足説明

② 型式、形式、連番及びその他の識別等

③ 製造者名

④ 受領日及び稼働開始日

⑤ 現在の設置場所（該当する場合）

⑥ 受領時の状況（新品、中古品、修理品等）

⑦ 入手可能な場合、製造者による指示書のコピー

⑧ 測定のトレーサビリティとその根拠（校正証明書）

⑨ 校正又は検証の範囲

⑩ 分解能及び許容可能なエラー

⑪ 校正又は検証の有効期間

⑫ これまでに行った保守及び今後予定している保守に係る事項

⑬ 損傷、不具合、変更、又は修理の履歴

⑭ 試験設備、試験装置又はこれらを組み合わせた試験システムに係る問題点、これらが試験業務への使用から取り外されたことを示す記録、問題点の修正又は解決を示す記録等

⑮ 校正又は検証を担当する試験機関の要員又は外部業者の識別

3.4　要員の適格性及び資格（ISO/IEC 17025 4.1.5 項 h)、5.2.1 項）

3.4.1　申請事業者及び試験機関の技術管理主体の適格性

(1) 技術管理主体は、試験業務の技術的事項の全責任を負う。

(2) 技術管理主体は、試験業務に係る十分な技術的知識を持ち、試験結果の正確な評価を行う能力を有すること。

(3) 技術管理主体は、下記の知識並びに試験要員の教育・訓練及び適切な監督・指示を行う能力を有すること。

① CM 認証機関から貸与される暗号モジュール試験報告書の作成を支援することを目的としたツールを用いた試験報告書の作成を含む、暗号モジュール試験に係る一般要求事項

② 暗号モジュールセキュリティ要件に係る知識

③　暗号モジュール試験要件に係る知識
④　暗号アルゴリズム試験要件に係る知識
⑤　運用ガイダンスに係る知識

(4) 技術管理主体の管理者（技術管理者及びその代理人）は、下記の知識及び試験業務に関連した分野で 2 年以上の経験を有することが望ましい。

①　ハードウェアプラットフォーム（ソフトウェアベースの暗号アルゴリズムの場合）
②　EFP/EFT（環境故障保護／環境故障試験）における電圧及び温度測定
③　コンピュータセキュリティ
④　有限状態マシン（FSM：Finite State Machine）モデルの分析
⑤　改ざん防止及び改ざん検知手法
⑥　高級プログラム言語及び形式モデルなどのソフトウェア設計仕様書
⑦　暗号自己テスト技術
⑧　暗号モジュールセキュリティ要件に係る暗号アルゴリズム及び暗号関連の専門知識（CM 認証機関から貸与される暗号アルゴリズム試験を行うことを目的としたツールの取り扱いを含む）
⑨　オペレーティングシステム
⑩　IT セキュリティ評価基準及び IT セキュリティ評価方法
⑪　CM 認証機関から貸与される暗号モジュール試験報告書の作成を支援することを目的としたツールの取り扱い及び保守
⑫　インターネット及びネットワーク

(5) 前(2)から(4)までの知識、経験等は、最近のものであることが望ましい。

3.4.2　申請事業者及び試験機関の試験要員の適格性及び資格

(1) 試験要員は、試験業務に係る内部資格を有すること。
(2) 試験要員は、3.4.1(3)に定める知識を有し、その内部資格基準は適切であること。
(3) 試験要員は、3.4.1(4)に定める知識及び試験業務に関連した分野で 1 年以上の経験を有することが望ましい。
(4) 上記(2)及び(3)の知識、経験等は、最近のものであることが望ましい。

3.5　要員の教育・訓練（ISO/IEC 17025 5.2.2 項）

3.5.1　申請事業者及び試験機関の管理主体は、試験要員を含めた要員に教育・訓練を提供するための方針及び手順を有しなければならない。当該教育・訓練プログラムは、申請事業者及び試験機関の業務に対して適切でなければならない。

3.5.2　前項の教育・訓練プログラムは、少なくとも 3.4.1(3)の項目について集中して行わなければならない。また、試験業務に必要な場合には、3.4.1(4)の項目に係る教育・訓練を行わなければならない。これらの教育・訓練は、継続して適切な試験が実施できるよう、又、最新の技術に対応できるように試験要員に対して定期的かつ計画的に行わなければならない。

3.6　施設及び環境条件（ISO/IEC 17025 4.1.5 項 c)及び 5.3 項）

3.6.1　施設の機密保護及び所有権の保護

(1) 申請事業者及び試験機関は、少なくとも次に掲げる施設等について自ら管理するとともに、顧客の機密保護及び所有権の保護を確実にするための方針及び手順を有しなければならない。

①　試験を行う施設（試験室）

② 試験に係る機密情報の保管場所
③ 試験に係る機密情報の転送を行うツール（FAX、電子メール等）

参考：上記②及び③は、①の中に設置してもよいし、①とは別の場所に設置してもよいが、いずれにおいても、機密保護及び所有権の保護を適切に行うこと。

(2) 申請事業者及び試験機関は、試験室について、機密保護及び所有権の保護の観点から試験作業に必要な程度のものとすること。

(3) 保管場所に係る方針及び手順には、少なくとも、次に掲げる項目を包含することが望ましい。

① 試験に係る機密情報は、やむを得ない場合（例えば、顧客のサイトで試験を行うとき、CM 認証機関と連絡するとき等）を除き、持ち出さないこと。

② 試験に係る機密情報が不要となったときは、復元不可能な状態で廃棄若しくは消去すること。顧客に返却する必要があるときは、確実に返却すること。

例）復元不可能な状態での廃棄又は消去の例として、紙媒体にあってはシュレッダー等による廃棄又は紙の溶解処理装置による溶解、電子媒体にあっては当該媒体の初期化又は物理的な破壊がある。

(4) 申請事業者及び試験機関は、試験に係る機密情報の転送を行う場合には、送信側、受信側を含む転送経路における機密保護を確実にすること。その転送経路の一部又は全部の機密保護が確実ではない場合には、機密情報を保護するための手段をとること。

例）電子メールにて送受信する場合の機密保護として、機密情報は当該メール本文には包含せず添付ファイルに包含させた上で、その添付ファイルを暗号化する方法がある。

例）やむを得ず FAX にて送信する場合の機密保護として、送信前にあらかじめ受信者に電話連絡の上、FAX 機の前で待機して貰う方法がある。

(5) 申請事業者及び試験機関は、顧客の機密情報及び所有権の保護に係る倫理規定を整備しなければならない。

3.6.2　試験を行う施設及びその環境条件

(1) 申請事業者及び試験機関は、少なくとも、次に掲げる施設を試験環境として整備しなければならない。

① 3.6.1(1)③の条件を満たす電子メール使用環境
② インターネット使用環境（CM 認証機関が情報発信する試験に係る情報、認証済み製品リスト等へのアクセスのため）

(2) 申請事業者及び試験機関は、試験機関の恒久的な施設以外の場所（例えば顧客のサイトなど）で試験を行う場合には、その環境を ISO/IEC 17025 5.3 項の要求事項を満たすものに適合させなければならない。

(3) 申請事業者及び試験機関は、権限のないものからのアクセスがあり得る試験環境において試験を行う場合には、試験の実施中はそのアクセスを禁止するような方法で試験環境を制御しなければならない。そのような評価試験環境に含まれるネットワークは、外部ネットワークと分離するか、少なくとも評価試験中はそのネットワークに権限のないものからのアクセスを禁止するような制御メカニズムを備えなければならない。

3.7　試験の方法（ISO/IEC 17025 5.4.1 項）

3.7.1　申請事業者及び試験機関は、試験方法として暗号モジュール試験要件、暗号アルゴリズム試験要件及び運用ガイダンスを用いなければならない。

3.7.2　申請事業者及び試験機関は、必要な場合には、試験方法の規定と矛盾のない内容

で文書化された手順を持つこと。

3.8　規格外の方法（ISO/IEC 17025 5.4.4 項）

3.8.1　暗号モジュール試験への適用のために CM 認証機関が発行したガイド文書は、「規格に規定された方法」とみなされ、規格外の方法に該当しない。

3.8.2　申請事業者及び試験機関は、3.7.1 に掲げる方法で規定されていない規格外の方法を採用するときは、必ず顧客の同意に基づき採用し、試験報告書にその詳細を記述しなければならない。

3.8.3　ISO/IEC 17025 5.4.4 項 注記の a）から k）までの情報のうちいくつかの項目は、暗号モジュール試験・認証においては適用しない。

3.9　方法の妥当性確認（ISO/IEC 17025 5.4.5.2 項）

ISO/IEC 17025 5.4.5.2 項 注記 2.のうち「参照標準又は標準物質を用いた校正」各などの方法は、暗号モジュール試験においては適用しない。

3.10　測定の不確かさの推定（ISO/IEC 17025 5.4.6 項）

ISO/IEC 17025 5.4.6 項は、暗号モジュール試験においては適用しない。

3.11　設備の保有（ISO/IEC 17025 5.5.1 項）

3.11.1　申請事業者及び試験機関は、暗号モジュール試験のために必要な設備を、購入、リース又はレンタルによって保有し、常時使用できるようにしなければならない。これらの設備には、暗号モジュール試験を行うために申請事業者又は試験機関が使用する次に掲げる設備を含めるものとする。

(1) 標準的な作業台
(2) ハードウェア
(3) ソフトウェア
(4) セキュリティの物理的な試験を実施するためのツール
(5) 電源（電圧が可変であるもの）
(6) 温度チャンバ
(7) 電気計測器（例えば、抵抗計、電圧計、電力計、オシロスコープ、ロジックアナライザ、温度チャンバの温度計等）
(8) CM 認証機関から貸与される暗号アルゴリズム試験を行うことを目的としたツール
(9) CM 認証機関から貸与される暗号モジュール試験報告書の作成を支援することを目的としたツール
(10) その他の試験用機械装置（例えば、物理的試験用の試験設備及び測定設備）

3.11.2　申請事業者及び試験機関は、試験ツール等がソフトウェアの場合には、当該ソフトウェアが ISO/IEC 17025 5.4.7 項に適合することを確保しなければならない。ただし、上記(8)及び(9)のツールは「設計上の適用範囲内においては、CM 認証機関により十分に妥当性確認されたもの。」とみなす。

3.11.3　申請事業者及び試験機関は、顧客が所有する設備等、試験機関が恒久的に管理している設備以外の設備を一時的に暗号モジュール試験に用いたときは、顧客等と契約を締結することにより、ISO/IEC 17025 5.5 項への適合性を確保しなければならない。

参考：契約の内容は、必要かつ十分なものであること。例えば、再試験のために顧客が所有するツールを再度使用しなければならないときは、「最初の試験のときと同等の試験環境を再現できること。」が確保できればよく、最初の試験で用いたツールの維持

・保管まで契約で求める必要はない。

3.12　設備の維持（ISO/IEC 17025 5.5.2 項）

3.12.1　申請事業者及び試験機関は、暗号モジュール試験を行うために用いる設備を、次に掲げる事項に従って維持しなければならない。

(1) CM 認証機関から貸与されたツールにあっては、CM 認証機関が定める要求事項。

(2) 製造業者の推奨。

(3) 適用可能な場合、申請事業者及び試験機関が文書化した手順。

3.12.2　申請事業者及び試験機関は、試験行為を妨げたり、いかなる点においても試験中の暗号モジュール機能の完全性を損なわないことを確実にするために、設備を検証すること。

備考：暗号モジュール試験に用いる設備の検証は、ある設備の指示値とそれに対する測定値の既知の値との差が、規格、法令又は当該設備の規定仕様書に定められた最大許容差より、一貫して小さいことを確かめるための手段となる。検証の結果、使用のために機能を回復させる、調整を行う、修理する、又は使用から取り外す、廃棄する、という判断を行うことになる。

3.13　測定のトレーサビリティ（ISO/IEC 17025 5.6 項）

3.13.1　申請事業者及び試験機関は、暗号モジュール試験の結果の正確さ又は有効性に重大な影響をもつ設備について、確立された校正計画を持ち、適切な校正を実施することにより国際単位系（SI）への測定のトレーサビリティを確保すること。このトレーサビリティは、ISO/IEC 17025 4.5 項に基づき暗号モジュール試験の下請負契約をしたとき、3.11.3 の規定に基づき顧客の設備を用いたときも確保すること。

ここで、「暗号モジュール試験の結果の正確さ又は有効性に重大な影響をもつ」設備とは、暗号モジュール試験に用いられる測定装置及びそれらの参照標準であって、その試験結果のトレーサビリティの確保に不可欠なものをいう。

参考：トレーサビリティの確保が必要な設備の例としては、3.11.1(7)の電気計測器などがある。

3.13.2　申請事業者及び試験機関は、前項のトレーサビリティの証拠となる記録を保持しなければならない。可能な場合、次のいずれかの記録によって測定のトレーサビリティを証明すること（注 1 から注 7 までの説明は、2.13.2 を参照のこと。）。

(1) 国家計量標準研究所が CIPM-MRA（注 1）のもとで発行する校正証明書又はこれと同等の校正証明書（注 2）

(2) JCSS 標章付校正証明書（注 3）又は JCSS 認定シンボル付校正証明書（注 4）

(3) ASNITE 校正（注 5）の認定を受けた校正事業者が発行する ASNITE 認定シンボル付校正証明書

(4) ILAC（注 6）MRA に署名する認定機関の認定を受けた校正事業者が発行する認定シンボル付校正証明書

(5) ASNITE-RM（注 7）の認定を受けた標準物質生産者が発行する認証標準物質の認証書

3.13.3　暗号モジュール試験において、ISO/IEC 17025 5.6.2.1 項は適用しない。

3.13.4　暗号モジュール試験全体のトレーサビリティは、ISO/IEC 17025 5.6.2.2.2 項で規定する「合意された方法へのトレーサビリティ」を適用する。この場合における「合意された方法」とは、暗号モジュール試験要件及び暗号アルゴリズム試験要件をいう。

参考：試験機関が行った暗号モジュール試験及びその試験結果に基づき CM 認証機関が

認証したとき、その暗号モジュール試験は、暗号モジュール試験（及び暗号アルゴリズム試験）にトレーサブルであることが CM 認証機関によって証明されたといえる。

3.14　サンプリング（ISO/IEC 17025 5.7 項）

暗号モジュール試験において、ISO/IEC 17025 5.7 項は適用しない。

3.15　試験品目の取り扱い及び識別（ISO/IEC 17025 5.8.2 項）

3.15.1　申請事業者及び試験機関は、試験品目について、不当に改変されたり、権限のないものがアクセスして使用することがないよう保護しなければならない。

3.15.2　申請事業者及び試験機関は、試験品目、試験プラットフォーム及び周辺設備並びに関連記録が混同しないよう、試験品目を識別するシステムを維持しなければならない。

3.16　試験品目の取り扱い及び保管（ISO/IEC 17025 5.8.4 項）

3.16.1　申請事業者及び試験機関は、試験品目に係る所有権保護システムを有すること。このシステムは、顧客に所有権があるもの（例えば、ハードウェア、ソフトウェア、試験データ、紙媒体若しくは電子媒体による文書及び記録、その他の資料等）を保護するために十分なものであること。

3.16.2　前項のシステムは、申請事業者若しくは試験機関への訪問者、情報を持つ必要のない関係職員及び権限のないものから、顧客に所有権があるものを保護できるものであること。

3.16.3　申請事業者及び試験機関は、暗号モジュール又はその一部がソフトウェア部分で構成されているときには、構成管理システムを持ち適切に管理するとともに、試験中にソフトウェア部分が不注意で又は不当に改変されることがないよう、その構成管理システムが適切であることを確実にすること。

3.17　結果の報告に係る一般要求事項（ISO/IEC 17025 5.10.1 項）

3.17.1　試験報告書の様式は、申請事業者及び試験機関が定めた様式であって、認定機関に届出たものを使用すること。

3.17.2　申請事業者及び試験機関は、行った試験業務に係る試験報告書を発行する。CM 認証機関に対して提出する試験報告書は、CM 認証機関から貸与される暗号モジュール試験報告書の作成を支援することを目的としたツールを用いて作成し、JCMVP で認められるものであること。また、顧客へ提出する試験報告書は、顧客との契約上必要な事項及びこの要求事項を満たすものであること。申請事業者及び試験機関は、暗号モジュール試験の結果を裏付ける証拠を提供できること。

3.17.3　ISO/IEC 17011 8.3 項に認定の言及及び認定シンボルの使用についての要求事項がある。これに対応して認定機関は、認定シンボルの使用方法等を別途取り決め、発行する。認定範囲外の暗号モジュール試験の結果を認定シンボル付試験報告書に含めることについては、それらの試験結果が認定範囲外の暗号モジュール試験結果であることが明確に識別されていなければならない。

3.18　試験報告書（ISO/IEC 17025 5.10.2 項、5.10.3 項及び 5.10.4 項）

3.18.1　申請事業者及び試験機関は、試験報告書の発行（承認）に責任を有する者を、認定機関に試験報告書発行責任者として届出なければならない。試験報告書発行責任者は、試験報告書に署名又は捺印すること。また、試験報告書発行責任者の不在の場合に備えて代理者を指名すること（ISO/IEC 17025 4.1.5 項 注記を参照のこと。）。

3.18.2　暗号モジュール試験の年月日については、試験に要したすべての実施年月日（期間であってもよい）又は実施期間のうち最終日を記載するものとする。
3.18.3　試験報告書は、一件の暗号モジュール試験に対して複数部発行してもよい。この場合においては個々の報告書に固有の識別を必要とする。報告書の複写については、4.10.4(2)に定める規定に従うものとする。
3.18.4　暗号モジュール試験において、ISO/IEC 17025 5.10.4 項は適用しない。

第 4 部　雑則

4.1　遵守事項（ISO/IEC 17011 8 項）

4.1.1　申請事業者及び認定事業者は、次に掲げる事項を遵守しなければならない。
(1) 常に、ISO/IEC 17025 の関係条項に適合すること。
(2) ISO/IEC 17025 及び ISO/IEC 17011 の関係条項に基づき認定機関が定めた要求事項（認定機関が定めた手数料の支払いを含む。）に適合すること。
(3) 認定されていることに言及する場合は、認定が授与された事業範囲内で行う業務についてのみ主張すること。
(4) 認定機関の信用を落とすような方法で認定を引用しないこと。また、認定機関が、誤解を招くと判断する、又は、認めていない内容の認定に係るいかなる表明もしないこと。
(5) 認定が一時停止され、又は、取り消された場合、直ちに認定の引用を含む広報物の使用を停止すること。
(6) 認定が一時停止され、又は、取り消された場合、速やかに認定証を認定機関に返納すること。
(7) 認定機関によって製品の品質が保証されていると誤解されるような方法で認定を利用しないこと。
(8) 評価報告書若しくは試験報告書又はその一部が誤解を招くような方法で利用されることがないように努めること。
(9) 評価報告書若しくは試験報告書への認定シンボル及び認定の引用方法並びに広告物、パンフレット、その他の文書等の媒体における認定の引用方法は、認定機関が定める規定に従うこと。
(10) 認定の要件への適合性を認定機関が確認のため実施する審査及び契約検査並びに苦情の解決を目的とする文書の審査、認定事業に係るすべての区域への立入り、記録の閲覧、職員との接見などにおいて、必要な便宜を図り協力すること。
(11) 認定機関から認定の要求事項が変更された旨の通知を受けた場合、妥当な期間内にその要求事項に適合するために必要な業務手順の変更等の措置を完了し、認定機関に措置の完了を知らせること。
4.1.2　申請事業者は、申請時に申請書類とともに「ASNITE 試験事業者 IT 認定の一般要求事項の確認について」に記名・押印の上、認定機関に提出しなければならない。

4.2　認定の申請に必要な手続き（ISO/IEC 17011 7.2 項）

申請事業者は、認定の申請に当たって、次に掲げる手続きをしなければならない。
(1) 認定申請書及び添付書類（別に定める認定申請等の手引きに掲げる書類）を作成し、提出すること。
(2) 品質マニュアル及び要求される場合にはその附属書類を提出すること。

(3) 認定の要件への適合性を確認するために実施する現地審査（認定事業に係るすべての区域への立入り、文書の審査、記録の閲覧、職員との接見等）を受け入れること。
(4) 認定の要件に適合していないと指摘された事項について、改善し、その結果を報告すること。
(5) 認定申請の過程で、申請事業者の都合により認定申請手続きを中断する必要が生じた場合は、認定機関に認定申請手続中断願を提出すること。
(6) 認定申請の過程で、申請事業者の都合により認定申請を取り下げる必要が生じた場合は、認定機関に認定申請取下願を提出すること。
(7) 認定申請の過程で、認定申請書類の訂正をする必要が生じた場合は、認定機関に認定申請書訂正願を提出すること。

4.3　技術的能力の定期的な確認（ISO/IEC 17011 7.15 項）

申請事業者及び認定事業者は、認定機関が ISO/IEC Guide 43 に適合する技能試験を受けることを要求する場合には、認定区分ごとに次のいずれかの技能試験を受けなければならない。
(1) 認定機関自らが行う技能試験
(2) アジア太平洋試験所認定協力機構（APLAC）等、認定に係る国際機関が行う技能試験
(3) 国際試験所認定協力機構（ILAC）/MRA、APLAC/MRA に署名する認定機関が行う又は承認する技能試験
(4) 国の機関、IPA、独立行政法人産業技術総合研究所、IT セキュリティ評価等に係る研究会、著名な外国機関又は学会等が行う IT セキュリティ評価等に係る技能試験であって、認定機関が認めたもの
(5) 申請事業者又は認定事業者自らが、各認定区分に係る技術的能力があると立証できる技能試験であって、かつ、認定機関があらかじめ認めたもの

4.4　変更の届出（ISO/IEC 17011 8.1.2 項）

認定事業者は、事業所の状態又は運営面の変更が発生して、次の何れかに該当する場合には、変更の事実が発生した日から概ね 30 日以内に、認定内容等変更届を認定機関に提出しなければならない。
(1) 認定事業者の名称又は所在を変更したとき。所在の変更には、所在地の変更（認定事業者の移転）のほか、住居表示の変更も含まれる。
(2) 認定事業の実施の方法に係る事項（手順書のほか、品質マニュアルを含む。）を定めた書面を変更したとき。
(3) 認定事業に用いる設備、施設、組織及び従事者に係る事項を変更したとき。
(4) コモンクライテリア評価の認定区分にあっては、認定を受けた範囲のうち、セキュリティ保証コンポーネントを変更したとき（ただし、EAL の数値を大きくする場合には再申請となる。）。

4.5　事業の承継（ISO/IEC 17011 8.1.2 項）

4.5.1　認定事業者が認定事業のすべてを譲渡したとき、又は認定事業者について合併があったときは、その事業のすべてを譲受した法人又は合併後の法人は、認定事業者の地位を承継することができる。

4.5.2　前項の場合には、認定事業者の地位を承継した者は、4.4 の変更の届出のほか、次の手続きを行なわなければならない。

(1) 事業のすべてを譲受したことによって認定事業者の地位を承継した法人は、事業譲渡の届出。
(2) 合併によって認定事業者の地位を承継した法人は、事業承継の届出。

4.6　契約検査（ISO/IEC 17011 7.11 項）

4.6.1　認定事業者は、継続して認定の要件に適合していることを確認するため、認定機関が行う契約検査を受け入れなければならない。契約検査には、定期検査と臨時検査とがある。

4.6.2　認定機関は、認定後第 1 回目の定期検査（部分検査）を、原則として、認定を受けた日から 1 年以内に実施する。

部分検査は、ISO/IEC 17025 のすべての要求事項のうち、次に掲げる事項について行う。

(1) 初回認定審査における不適合事項（観察事項を含む。）の改善状況の確認
(2) 初回認定審査以降の変更点
(3) マネジメントレビュー、内部監査の実施状況等の管理システム面の適合状況の確認

4.6.3　認定機関が行う定期検査（全項目検査）は、ISO/IEC 17025 のすべての要求事項の項目について行う。全項目検査は、初回認定を受けた日から 3 年以内に 1 回、また初回認定を受けた日から 4 年以内に 1 回実施される。その後は前回全項目検査日から原則として 2 年以内に実施する。

4.6.4　認定機関は、認定事業者に次に掲げる事項が生じた又は生じたと認められた場合であって、認定機関の品質管理者又は評定委員会が必要と認めた場合には、臨時検査を実施することができる。

(1) 重大な苦情が発生したか又は他の状況により、認定基準への適合性又はセキュリティ評価若しくは暗号モジュール試験の品質に関して著しい疑義を呈している場合
(2) 技術管理主体の変更、主任評価者の退職等、技術的能力に影響する変更があった場合
(3) 事業の承継があった場合
(4) 技能試験の結果、認定事業者としての技術的能力に疑義があった場合

4.7　事業の廃止（ISO/IEC 17011 8.1.2 項）

認定事業者は、事業のすべてを廃止若しくは縮小したとき又は事業の一部を廃止したときは、廃止等の日から概ね 30 日以内に、認定証を添えて認定機関に事業廃止の届出をしなければならない。

4.8　認定の一時停止（ISO/IEC 17011 7.13 項）

認定事業者は、次の何れかに該当する場合には、認定が一時停止されるものとする。認定が一時停止された試験事業者は、認定機関によってその事実が公表される。

(1) 契約検査等の結果、この要求事項に対する重大な不適合事項があり、評定委員会で認定の一時停止をすることが評定されたとき（例えば､不適合事項の改善に概ね 30 日以上要すると認められたとき､発行した評価報告書に重大な誤りがある等の理由により過去にさかのぼり影響調査を必要とするとき、などは認定の一時停止が評定される。）。
(2) 技能試験等の結果、認定事業者としての技術的能力に疑義を呈している場合。

4.9　認定の取消し（ISO/IEC 17011 7.13 項）

認定事業者は、次の何れかに該当する場合には、認定が取り消されるものとする。認定が取り消された試験事業者は、認定機関によってその事実が公表される。また、認定証を返却しなければならない。

(1) 認定の範囲を超えて、認定シンボル付きの評価報告書又は試験報告書を発行したことが判明した場合（ただし、認定範囲外の結果について、認定範囲外であることを報告書の中で明確に識別している場合を除く。）

(2) 契約検査又は技能試験等の結果、技術的能力がないと判明した場合

(3) この要求事項から著しく逸脱して業務を実施していることが判明した場合

(4) 契約検査等において、過去の契約検査等で改善を要求された事項と同じ内容の改善を要求されることが反復された場合

(5) 不正な手段により認定を受けていることが判明した場合

4.10　認定シンボルの取り扱いに係る要求事項（ISO/IEC 17011 8.3 項）

4.10.1　認定機関は、申請事業者及び認定事業者に対して、認定シンボルの使用方法及び使用の制限の取扱いについて、4.10.2 から 4.10.6 までに掲げる要求事項を適用する。申請事業者及び認定事業者は、これらのすべての要求事項に適合しなければならない。

4.10.2　方針

(1) 認定事業者は、認定された事業の範囲のセキュリティ評価又は暗号モジュール試験を行った場合には、認定シンボルを付した評価報告書又は試験報告書を発行することができる。

(2) ILAC-MRA マークのついた認定シンボル（4.10.3 のもの）の使用に当たっては、あらかじめ「ILAC 試験所組合せ MRA マークサブライセンス契約書」を提出しなければならない。

(3) この要求事項に規定する場合を除き、何人も評価報告書又は試験報告書に認定シンボル又はこれと紛らわしい標章類などを付してはならない。

4.10.3　認定シンボル

(1) 認定シンボルの形状については、次のとおりとする。

(2) 認定シンボルの色は、次に示すものと同等の色又はシンボル全体同一色を原則とする。

(3) 認定シンボル中「ASNITE XXXX」の部分には、~~の下には、”ASNITE TI-”に続けて 4 桁の~~各認定事業者の認定された事業所の認定番号を~~付~~記載すること。
「ASNITE」と「XXXX」との間は、半角文字以上のスペースを空けること。

(4) 「ASNITE XXXX」の右横「〇〇」の部分には、評価報告書又は試験報告書を発行する場合における「認定シンボルの付加情報」として、試験事業者の識別記号「T」を記載すること。認定事業者が、複数の分野で認定されている場合における識別記号の記載方法については、認定機関に問い合わせること。この識別記号は、評価報告書又は試験報告書に認定シンボルを付すとき以外は、記載する必要はない。

4.10.4　認定シンボルの使用に係る運用

(1) 報告書の書式

申請事業者及び認定事業者は、認定シンボル付きの評価報告書又は試験報告書を発行する場合には、その様式を事前に認定機関に届出なければならない。

(2) 報告書の複写

認定事業者は、評価報告書又は試験報告書のカラーコピー等による複写は正本と紛らわしいので禁止されていることを、その報告書を提出する者に対して通知しなければならない。ただし、その複写の表面に「COPY」、「複写」、「写し」等の明瞭な表示を求め、正本と区別できるようにさせる場合は、この限りでない。

4.10.5　認定事業者は、次に定める宣伝等における認定シンボルの使用に係る要求事項を遵守しなければならない。

(1) 認定事業者は、製品そのものの品質等が承認・保証等されたものと誤解されるような紛らわしい認定シンボルの使用をしてはならない。特に、CC 認証機関又は CM 認証機関から発行される認証書と混同されるような記載は避けなければならない。

(2) 認定事業者は、以下の条件を満たす場合に限って、カタログ、レターヘッド、名刺を除くその他の宣伝文書に、4.10.3 で定める認定シンボルを使用してもよい。ただし、その使用に当たっては、事前に認定機関に照会し、承認を得ること。

① 認定シンボルは、認定シンボルを説明する文章の中で用いる。

② 説明する文章の文字の大きさは、読みとれる大きさ以上とする。

(3) 認定事業者は、上記(2)①及び②の条件を満たす場合に限って、名刺その他の宣伝文書に、以下に定める認定シンボルを使用してもよい。ただし、その使用に当たっては、事前に認定機関に照会し、承認を得ること。

例）以下は、認定シンボルを説明する文章の例である。

【名刺を除く宣伝媒体に認定シンボルを使用するときの説明文の例】
当社は、ISO/IEC 17025 を認定基準として用い、ISO/IEC 17011 に従って認定スキームが運営されている製品評価技術基盤機構認定制度（ASNITE）の下で認定され

ています。ASNITE を運営している認定機関（IAJapan）は、アジア太平洋試験所認定協力機構（APLAC）及び国際試験所認定協力機構（ILAC）の相互承認に署名しています。
　当社セキュリティセンターは、国際 MRA 対応 ASNITE 認定事業者です。ASNITE ~~IT-~~XXXX は、当社セキュリティセンターの認定番号です。

【名刺に認定シンボルを使用するときの説明文の例】
　当社セキュリティセンターは、国際 MRA 対応 ASNITE 認定事業者です。ASNITE ~~IT-~~XXXX は、当社セキュリティセンターの認定番号です。

4.10.6　認定シンボルの使用停止及び禁止

　認定事業者は、認定の一時停止若しくは取り消しになった場合又は認定に係る事業を廃止した場合には、直ちに一切の認定シンボルの使用を停止又は中止しなければならない。

附　則
　この規程は、平成 13 年 12 月 12 日から施行する。

附　則
　この規程は、平成 14 年 4 月 1 日から施行する。

附　則
　この規程は、平成 14 年 12 月 1 日から施行する。

附　則
　この規程は、平成 16 年 1 月 5 日から施行する。

附　則
　この規程は、平成 16 年 4 月 1 日から施行する。

附　則
　この規程は、平成 16 年 6 月 15 日から施行する。

附　則
　この規程は、平成 17 年 6 月 1 日から施行する。

附　則
　この規程は、平成 19 年 2 月 1 日から施行する。

附　則
　この規程は、平成 19 年 4 月 1 日から施行する。