TIRP21－18

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18版）

2025年mm月dd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「IAJapan」という。）が運営する製品評価技術基盤機構認定制度（以下「ASNITE」という。）において、コモンクライテリア評価、暗号モジュール試験、システムLSI侵入テスト又はIoT製品のセキュリティ要件適合評価を行う事業者が認定を受けるために必要な認定要求事項、及び認定を受けた事業者がその認定を維持するために必要な認定要求事項を定めることを目的とする。認定要求事項全般は、認定スキーム文書(UIF03) 別紙11 (ASNITE-T(IT))において示すこととするが、本一般要求事項においても具体的な要求内容を示す。

1.2　適用範囲

1.2.1　この規程は、ASNITE の認定を希望する事業者（以下「申請事業者」という。）及び ASNITE の認定を受けた事業者（以下「認定事業者」という。）に適用する。

1.2.2　この規程を適用する事業者の認定区分は、下表のとおりとする。

<table>
<tr><th colspan="3">認定区分</th><th>（参考：認証制度上の区分）</th></tr>
<tr><td rowspan="5">情報技術</td><td rowspan="2">コモンクライテリア評価</td><td>ソフトウェア</td><td rowspan="2">JISEC（注1）における評価機関</td></tr>
<tr><td>ハードウェア
（スマートカード等）</td></tr>
<tr><td rowspan="2">暗号モジュール試験</td><td>暗号ソフトウェアモジュール</td><td rowspan="2">JCMVP（注2）における暗号モジュール試験機関</td></tr>
<tr><td>暗号ハードウェアモジュール</td></tr>
<tr><td colspan="3">システムLSI侵入テスト</td></tr>
<tr><td colspan="2">IoT製品のセキュリティ要件適合評価</td><td>JC-STAR（注3）における評価機関</td></tr>
</table>

（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
（注 3）JC-STAR：セキュリティ要件適合評価及びラベリング制度

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、次に掲げる規程と併せ読むことにより、ASNITE の認定に係る要求事項がより明確になる。これらの規程、関連する取り扱い手順等の最新版は、IPA から入手することができる。

（参考）これらの最新版は以下の Web サイトにて入手することができる。
URL: https://www.ipa.go.jp/security/jisec/prcdr.html
URL: https://www.ipa.go.jp/security/jcmvp/kitei.html

URL: https://www.ipa.go.jp/security/jc-star/kitei.html

注記 以下、参考情報として掲載する文書の入手先は当該文書情報公開先の都合によりその URL が変更される場合がある。

(1) IT セキュリティ評価及び認証制度の基本規程（CCS-01）
(2) IT セキュリティ評価機関承認等に関する要求事項（CCM-03）
(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申請手続等に関する規程（CBM-03）
(5) セキュリティ要件適合評価及びラベリング制度の基本規程（JSS-01）
(6) セキュリティ要件適合評価及びラベリング制度の評価機関承認等に関する要求事項（JSM-03）

1.3 引用規格、規程等

この規程では、次に掲げる国際規格、日本産業規格及び文書の発行年を記載しているものについてはその版を、それ以外のものについては最新版を引用する。ただし、国際規格については、これらの規格のその版を翻訳し、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産業規格に読み替えてもよい。

(1) ISO/IEC 17000 Conformity Assessment - Vocabulary and general principles（適合性評価－用語及び一般原則）
(2) ISO/IEC 17011 Conformity assessment -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）
(3) 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）
(4) ISO/IEC 15408-1 Information security, cybersecurity and privacy protection − Evaluation criteria for IT security − Part 1: Introduction and general model（情報セキュリティ,サイバーセキュリティ,プライバシー保護 − IT セキュリティの評価基準 − 第 1 部：概説及び一般モデル）
(5) ISO/IEC 15408-2 Information security, cybersecurity and privacy protection − Evaluation criteria for IT security - Part 2: Security functional components（情報セキュリティ,サイバーセキュリティ,プライバシー保護 − IT セキュリティの評価基準 − 第 2 部：セキュリティ機能要求事項）
(6) ISO/IEC 15408-3 Information security, cybersecurity and privacy protection − Evaluation criteria for IT security − Part 3: Security assurance components（情報セキュリティ,サイバーセキュリティ,プライバシー保護 − IT セキュリティの評価基準 − 第 3 部：セキュリティ保証コンポーネント）
(7) ISO/IEC 18045 Information security, cybersecurity and privacy protection −

Evaluation criteria for IT security − Methodology for IT security evaluation（情報セキュリティ,サイバーセキュリティ,プライバシー保護 − IT セキュリティの評価基準 − IT セキュリティ評価の方法論）

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

(9) ISO/IEC 24759 Information technology - Security techniques - Test requirements for cryptographic modules（情報技術 − セキュリティ技術 − 暗号モジュールのセキュリティ試験要件）

(10) 認定スキーム文書(UIF03) 別紙 11(ASNITE-T(IT))

(11) IAJapan 計量トレーサビリティに関する方針(URP23)

(12) IAJapan 技能試験 及び/又は技能試験以外の試験所間比較への参加に関する方針(URP33)

(13) IAJapan 認定シンボルの使用及び認定の主張等に関する方針(URP15)

(14) 適合性評価機関の権利及び義務(UIF02)

(15) ASNITE 試験事業者 IT 認定の取得と維持のための手引き(TIRP22)

(16) IAF-ILAC JGA 2007 Sydney Resolution 7 – Certification to accreditation standards(認定に用いられる規格を用いた認証行為の禁止)

(17) ILAC-R7 Rules for the Use of the ILAC MRA Mark(ILAC MRA マーク使用ルール)

(18) APAC MRA-001 Procedures for Establishing and Maintaining Mutual Recognition Amongst APAC Accreditation Bodies(APAC 認定機関間の相互承認の確立と維持のための手順)

(19) NIST Handbook 150-17 NVLAP Cryptographic and Security Testing(NIST HB 150-17)

（参考）NIST HB 150-17 の最新版は以下の Web サイトにて入手することができる。
URL: https://www.nist.gov/nvlap/cryptographic-and-security-testing-lap-0

1.4 定義

1.4.1 ASNITE 試験事業者(IT)認定：ASNITE において、1.4.7 の評価機関、1.4.8 の暗号モジュール試験機関、1.4.9 の侵入テスト実施機関及び 1.4.10 の JC-STAR 評価機関を認定するプログラム。

1.4.2 CC 認証機関：JISEC に従って、TOE（Target Of Evaluation 評価対象）及び PP（Protection Profile プロテクションプロファイル）のセキュリティ評価に係る認証並びに ST（Security Target セキュリティターゲット）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、1.4.11 で定める IT セキュリティ評価基準への適合性について、1.4.7 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。

1.4.3 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、1.4.16 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、1.4.8 で定める暗号モジュール試験機関から提出される試験報告書に基づき検証し、暗号モジュールに対する認証及び暗号アルゴリズム実装試験の結果に対する確認を行う。

1.4.4 JC-STAR 認証機関：JC-STAR に従って、IoT 製品の認証及び適合ラベルの交付を行う IPA の認証機関組織をいう。JC-STAR 認証機関は、1.4.19 で定める IoT 製品のセキュリティ要件への適合性について、1.4.10 で定める JC-STAR 評価機関から提出される適合評価報告書に基づき検証し、IoT 製品に対する認証及び適合ラベルの交付を行う。

1.4.5 CMVP: Cryptographic Module Validation Program。CMVP は、NIST (National Institute of Standards and Technology) /ITL（Information Technology Laboratory）と Communications Security Establishment of Canada (CSE) / Canadian Centre for Cyber Security により共同運営される米国政府及びカナダ政府の暗号モジュール試験及び認証プログラム。

1.4.6 NVLAP: National Voluntary Laboratory Accreditation Program。CMVP の承認試験機関となるためには NVLAP の認定が要求される。

1.4.7 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。

1.4.8 暗号モジュール試験機関：認定区分が暗号モジュール試験の認定事業者をいう。暗号モジュール試験機関は、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実装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。

1.4.9 侵入テスト実施機関：認定区分がシステム LSI 侵入テストの認定事業者をいう。侵入テスト実施機関は、主として CC ハードウェア評価の一部としてスマートカードに関する CC サポート文書等に基づき AVA_VAN に係るシステム LSI への侵入テスト等を行う。

1.4.10 JC-STAR 評価機関：認定区分が IoT 製品のセキュリティ要件適合評価の認定事業者をいう。JC-STAR 評価機関は、IoT 製品のセキュリティ要件への適合評価を行う。

1.4.11IT 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う（以下「CC」というが、1.4.13 に定める補足文書を明示的に区別する場合を除き、両者を合わせたものとして扱う。）。

(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 components

3) Part 3: Security assurance components

4)Part 4: Framework for the specification of evaluation methods and activities

5)Part 5: Pre-defined packages of security 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照表を参照すること。

（参考）当該文書は以下の Web サイトにて入手することができる。

URL: https://www.ipa.go.jp/security/jisec/about/kijun.html

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。

1.4.12 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う（以下「CEM」というが、1.4.13 に定める補足文書を明示的に区別する場合を除き、両者を合わせたものとして扱う。）。

(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照表を参照すること。

（参考）当該文書は以下の Web サイトにて入手することができる。

URL: https://www.ipa.go.jp/security/jisec/about/kijun.html

1.4.13 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。

1.4.14 CC サポート文書：CCRA が公開する文書。CC 認証プロセスに関し、特定技術の認証において、評価基準及び評価方法がどのように適用されるかを定める。主にスマートカードの評価／認証に関わるものが対象で、コモンクライテリア（ハードウェア）評価／認証及びシステム LSI 侵入テストを実施する際に適用される。

（参考）当該文書は、以下の Web サイトにて入手することができる。

URL:https://www.ipa.go.jp/security/jisec/hardware/cc_supporting_doc.html

1.4.15 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。

1.4.16 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) JIS X 19790

(3) Federal Information Processing Standards (FIPS) 140-2, 140-3 及びその後継版

（参考）当該文書は以下の Web サイトにて入手することができる。

URL: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/publications

1.4.17 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) ISO/IEC 24759

(2) JIS X 24759

(3) FIPS140-2, 140-3 及びその後継版のための Derived Test Requirements (DTR)
（参考）当該文書は以下の Web サイトにて入手することができる。
URL: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/publications

1.4.18 暗号アルゴリズム実装試験要件：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実装試験のための要求事項であって、次に掲げるものをいう。
(1) CM 認証機関が公開する文書（ATR-01）。
（参考）当該文書は以下の Web サイトにて入手することができる。
URL: https://www.ipa.go.jp/security/jcmvp/kitei.html
(2) JCMVP で承認されたセキュリティ機能向けの暗号アルゴリズム実装試験
（参考）当該文書は以下の Web サイトにて入手することができる。
URL: https://www.ipa.go.jp/security/jcmvp/algorithm.html

1.4.19 IoT 製品のセキュリティ要件への適合基準、評価手順：IoT 製品のセキュリティ要件適合評価に用いる基準及び評価手順であって、JC-STAR 認証機関が公開するレベル別、製品類型別の適合基準・評価手順文書のことをいう。
（参考）当該文書は以下の Web サイトにて入手することができる。
URL:https://www.ipa.go.jp/security/jc-star/tekigou-kizyun-guide/index.html

1.4.20 運用ガイダンス：
(1) CM 認証機関が公開する JCMVP 運用ガイダンス
（参考）当該文書は以下の Web サイトにて入手することができる。
URL: https://www.ipa.go.jp/security/jcmvp/kitei.html
(2) FIPS 140-2, 140-3 及びその後継版と Cryptographic Module Validation Program のための運用ガイダンス
（参考）当該文書は以下の Web サイトにて入手することができる。
URL: https://csrc.nist.gov/projects/cryptographic-module-validation-program

1.4.21 アーティファクト試験：暗号モジュール試験機関の初回認定において実施される、CM 認証機関が CMVP と共同開発した模擬暗号モジュールを用いて実施する試験。

1.4.22 試行試験：暗号モジュール試験機関が CM 認証機関による承認を受けるために行う暗号モジュールの試験。

1.4.23 認定要求事項：認定スキーム文書(UIF03) 別紙 11 (ASNITE-T(IT))で定める認定要求事項。

1.4.24 ILAC MRA 組み合わせ認定シンボル：ILAC MRA マーク及び認定シンボル（認定機関ロゴに、認定識別及び付加情報を加えたもの。）との組み合わせで認定事業者の認定の地位を示すために IAJapan によって交付されるシンボル。認定事業者は ILAC MRA 組み合わせ認定シンボルを使用することができる。（下図１参照）

※ ASNITE 0000 Testing：認定識別

※ ILAC MRA マーク （国際登録番号：840857）

※ IAJapan 認定機関ロゴ（国内商標登録：登録第 5745621 号）
（国際登録番号：1264278）

図１ ILAC MRA 組み合わせ認定シンボル

1.4.25 マルチサイト：認定事業者の物理的事業所及びバーチャルサイトを含むすべての場所で実行される全活動は文書化され、ひとつのマネジメントシステムにより運用されていること。
備考：バーチャルサイトは例えば、クラウド環境において、プロセスを実行できるオンライン環境である。

1.4.26 検証：規定要求事項が満たされ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。

1.4.27 上記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、ISO/IEC 19790 及び ISO/IEC 24759 のうち該当する定義を適用する。

第2部　認定区分：情報技術－コモンクライテリア評価を行う事業者に対する一般要求事項

2.1　一般

2.1.1　IAJapan は、申請事業者及び評価機関（以下「評価機関等」という。）に対し、認定スキーム文書(UIF03) 別紙 11(ASNITE-T(IT))に記載した認定要求事項、ASNITE 試験事業者 IT の認定（認定区分：情報技術－コモンクライテリア評価）のための認定要求事項として適用する。

2.1.2　第 2 部に掲げる規定は、同要求事項の評価機関等への適用方針とする。

注記　評価機関等は、IT セキュリティ評価及び認証制度で定める「IT セキュリティ評価機関承認等に関する要求事項（CCM-03）」への参照をマネジメントシステム文書に含めて運用することが望ましい。

2.2　公平性（ISO/IEC 17025 4.1項、5.1項）

評価機関等は、評価業務（ラボラトリ活動）が公平に実行され、公平性を確保するように編成及び運営をしなければならない。この公平性を確保する手段には以下を含むものとするがこれらに限定されない。

(1) 原則、評価機関等は、評価用提供物件（PP、ST、TOE、開発者作成文書を含む。以下同じ）に関わるコンサルタントサービス等、評価の結果に影響を及ぼすと考えられる業務を実施してはならない。評価機関等が評価以外の活動も行う組織の一部分である場合であり、評価以外の活動が評価の結果に影響を及ぼすと考えられる場合は、その評価以外の活動を特定し、それらの活動と評価業務との間を分離すること。

(2) 評価機関等は、ある評価用提供物件に関わるコンサルタントサービスを評価担当者に提供させた場合、当該評価担当者にその評価用提供物件を評価させてはならない。

(3) 評価担当者は、評価の対象となる TOE の開発部門（又は評価用提供物件の作成支援作業を行う部門）と利害関係を有してはならない。

2.3　ラボラトリ活動の範囲（ISO/IEC 17025 5.3項）

評価機関等は、ラボラトリ活動の対象となる範囲について、文書化しなければならない。認定範囲は次のいずれかとする。以下の認定範囲を超える保証コンポーネントにおいて CC 認証機関により評価者資格が付与された場合は、認定範囲に保証コンポーネントを追加することができる。その場合、別途申請が必要となる。

なお、認定範囲に追加できる保証コンポーネントは、認定区分の分野がソフトウェアの場合は ALC_FLR.n（n = 1, 2, 3）を、ハードウェア（スマートカード等）の場合は ALC_DVS.2、AVA_VAN.4 及び AVA_VAN.5 とする。

注記　上記の追加可能な保証コンポーネント以外を追加する場合は個別に IAJapan に問い合わせること。

(1) クラス APE、EAL 1 及び ASE_SPD

(2) クラス APE、EAL 1 及び EAL 2

(3) クラス APE、EAL 1、EAL 2 及び EAL 3

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

2.4 要員の力量（ISO/IEC 17025 5.6項、6.2.1項、6.2.2項、6.2.6項）

2.4.1 評価機関等の技術管理要員の力量

(1) 技術面の管理に責任を有する要員（以下この文書では「技術管理要員」という。）は、評価業務の技術的事項の全責任を負う。
(2) 技術管理要員は、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) 技術管理要員は、下記の知識並びに評価者の力量基準、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) 評価対象の機能や構造を理解し、CC 評価者アクションエレメントに対応する CEM アクションとそのワークユニットを適切に実行する知識・能力
   5) 情報処理に係る一般知識（コンピュータセキュリティ、コンピュータシステムアーキテクチャ、プログラミング言語、アルゴリズムとデータ構造、オペレーティングシステム、データベースシステム、ネットワーク等）
(4) 技術管理要員は、上記(3)に示す知識、経験に加え、評価技術に関係のある IT 製品等の開発に係る知識又は経験を有すること。
   注記 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 評価機関等の評価者の力量

(1) 評価者は、評価業務に係る力量を有すること。
(2) 評価者は、2.4.1(3)に定める知識を有し、その内部力量基準は適切であること。
(3) 評価者は、担当する IT 製品等に対する深い知識を維持すること。
   注記 IT 製品等の開発経験を有することが望ましい。

2.4.3 CC 認証機関による資格付与

(1) 評価機関等は、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、2.1 に定めるすべての認定範囲を含まなければならない。

2.4.4 主要な要員（ラボラトリマネジメント、品質管理要員、技術管理要員、評価者）の一部又は全部が雇用契約以外の契約による場合は、これを特定し、リスト化した上で、すべての主要な要員のリストとともに申請時に提出すること。この要員に変更が生じた場合、この要員を直接監視ができなくなった場合、IAJapan に書面で通知しなければならない。
   注記 契約による要員に上述のような変更がある場合、評価機関の認定地位に影響する可能性がある。

2.5 要員の教育・訓練（ISO/IEC 17025 6.2.2項）

2.5.1 評価機関等は、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、評価機関等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)1)から 4)の項目について行い、必要な場合には 2.4.1(3)5)の項目に係る教育・訓練を行わなければならない。教育・訓練は、継続して適切な評価業務が実施でき、また、IT 製品等の評価業務で必要となる最新の技術に対応できるように評価者に対して計画的に行わなければならない。

2.5.3 評価機関等は、内部資格を有する各要員が内部資格の範囲において評価を実施できる能力があることを毎年確認すること。確認の方法は、マネジメントシステム文書に明記し、定期的に見直すこと。能力の確認方法は、要員が実施した評価案件のレビューによるほか、要員が評価を実施していない場合にはそれに代わる教育・訓練の結果を確認する方法でもよい。

2.6 要員の管理（ISO/IEC 17025 6.2.1項、6.2.4項、6.2.6項）

2.6.1 評価者は、事業者間の契約又は個人契約等の契約による場合がある。この場合でも評価機関等が評価者に対し教育及び能力の確認を行い、認定範囲で実施される評価結果に責任を負うこと。

2.6.2 評価機関等は、内部資格に対応する評価を実施することが困難となった評価者に対しては、付与した内部資格の範囲を見直す等の処置をとること。また、評価者が離職する場合の手順を有すること。

2.7 施設及び環境条件（ISO/IEC 17025 4.2項、6.3項、7.11.3項）

2.7.1 施設の機密保護及び所有権の保護

(1) 評価機関等は、少なくとも次に掲げる施設等を保有する場合は、自ら管理すること。また、これらの施設等を利用する場合には、顧客の機密情報の保護及び所有権の保護を確実に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 等）を有する施設
4) 3)の評価に係る機密情報の転送を行うツールに附帯する、インターネット等利用環境構築に供される施設（ただし、評価機関等内に限る。）

注記 上記 2)ないし 4)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。

(2) 評価室は、以下の要件を満たすこと。ただし、顧客サイトでの評価等により評価室以外の場所で評価を行う場合には、以下の要件に限定されない。

1) 入退室を管理するための認証システムを有すること。

注記 認証システムは、すべての入退室者及び入退室日時が確定できるものであることが望ましい。

(3) 保管場所は、少なくとも次の要件を満たすこと。
1) 評価機関等が、顧客等が所有権を有する情報を保管する場合は、その情報に直接関係のない者からのアクセスを制限すること。
2) 評価に係る機密情報は、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。
3) 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。顧客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) 評価機関等は、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) 評価機関等は、顧客の機密情報及び所有権の保護に係る倫理規程を整備しなければならない。

2.7.2 評価を行う施設及びその環境条件

(1) 評価機関等は、恒久的な施設以外の場所（例えば顧客のサイトなど）で評価を行う場合には、その環境を ISO/IEC 17025 6.3 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。評価を実施する前に、評価を行う施設が評価のための環境条件を満たしていることを確認すること。

(2) 評価機関等は、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。

2.8 設備（ISO/IEC 17025 6.4項）

2.8.1 評価機関等は、評価実施に用いるすべての設備又はテストアプリケーション一式（テストスーツ）に係る情報、構成、設定、操作方法等について管理手順を有し、記録を維持すること。評価機関等はこれらの設備等の構成、設定、操作等に責任を有すること。

2.8.2 評価機関等は、試験実施に用いるコンピュータ装置及びその他のプラットフォームの構成・設定を制御すること。試験に用いるいずれの設備（ハードウェア及びソフトウェア）も、試験に用いる前に既知の状態になっていることを確実なものとする

ための手続きが、評価機関等によって定められていること。

2.9 計量トレーサビリティ（ISO/IEC 17025 6.5項）

2.9.1 評価機関等が使用する設備において、適用がふさわしい場合には計量トレーサビリティが要求される。計量トレーサビリティの確保が求められる場合には、IAJapan が別に定める「IAJapan 計量トレーサビリティ方針(URP23)」に従うこと。このトレーサビリティは、ISO/IEC 17025 6.6 項に基づき評価業務又はその一部を外部提供者に依頼したとき、顧客の設備を用いたときも確保すること。

2.9.2 セキュリティ評価実施に用いる設備は、メーカー（製造事業者）の推奨に従って、若しくは、評価機関等の内部の手順に従って良好な状態に維持されるか、又は使用前に良好な状態であることが確認されなければならない。

2.9.3 評価機関等は、試験設備を校正しなければならない。コモンクライテリア評価において、校正とは設備が正確に試験結果を示すことの検証を意味する。評価に用いる試験ツールであって、かつ、評価においてユニットを構成しないものについては、単独で検証をすること。また、評価機関等は、試験設備の構成・設定の記録及び検証の記録を維持すること。

注記 試験ツールは試験の実施に影響を与えず、試験中に TOE の完全性に変更や影響を与えないことを確認することが望ましい。

2.9.4 評価機関等は、最初の評価のときと同等の評価が再現できることを保証すること。再評価のために顧客が所有する試験ツール等を使用することがあらかじめ想定される場合は、再評価に係る試験環境の再現について顧客と文書で合意をすること。

2.9.5 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 6.5.3b)項で規定する「規定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。

注記 評価機関等が行ったセキュリティ評価について CC 認証機関がこれを認証したとき、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。

2.10 外部から提供される製品及びサービス（ISO/IEC 17025 6.6項、7.8.2.1p）項）

評価機関等は、認定の申請を行う範囲又は認定を受けた範囲の中で、業務の一部を、外部提供者に請け負わせることができる。この場合、評価機関等は、外部提供者が評価基準（CC）等及び ISO/IEC 17025 の関連する要求事項を満足し、技術的信頼性を持つことを確実にすること。また、確認した結果（記録）を評価機関自ら保持すること。これらの確認を行う場合において、外部提供者が ILAC MRA、APAC MRA に署名する IAJapan により認定を受けている場合は、マネジメントシステムに関する確認は省略することができる。

なお、システム LSI 侵入テストを外部提供者に請け負わせる場合は、評価機関等はコモンクライテリア評価ハードウェア（スマートカード等）で認定を受けているか又は認定の

申請を行う場合とし、2.2 に定める対象範囲のうち外部提供者に負わせる範囲をその認定範囲又は認定の申請範囲に含めていること。

注記 評価機関等は、外部提供者によって実施された評価結果及び／又は試験結果（以下、「評価結果等」という。）を評価報告書に引用する場合には、以下の全てを満たすこと。

(1) 外部提供者によって行われた評価結果等を含んでいる旨を評価報告書の ILAC MRA 組み合わせ認定シンボルを付した頁に明確に記載すること。

(2) 評価報告書の各評価結果等のうち、外部提供者によって実施された評価結果等は明確に識別すること。

2.11 評価の方法の選定（ISO/IEC 17025 7.2.1項）

2.11.1 評価機関等は、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。

2.11.2 評価機関等は、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。

2.11.3 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。

2.11.4 評価機関等は、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、必ず顧客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 5 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）

2.12 方法の妥当性確認（ISO/IEC 17025 7.2.2.1項）

ISO/IEC 17025 **7.2.2.1** 項 注記 2 のうち「a) 参照標準又は標準物質を用いた、校正又は偏り及び精度の評価。」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。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。

2.13 評価品目の取り扱い（ISO/IEC 17025 7.4.1項、7.4.2項）

2.13.1 評価機関等は、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。

2.13.2 評価機関等は、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。

2.14　技術的記録（ISO/IEC 17025 7.5.1項、7.11.3項、8.4.2項）

技術的記録は評価が CC 評価者アクションエレメントに対応する CEM アクションに従って行われたことが追跡できるものであること。技術的記録にはそれぞれのワークユニットに対しどのような評価が実施されたのかが客観的に分かるような十分な情報が含まれること。技術的記録には評価を実施した者及び評価結果のチェックに責任を持つ者の識別を含むこと。

データの改ざん防止、消失防止に備えてバックアップ機能を設けること。

注記 1　評価機関等が内部で規定する技術的記録の保存期間は、顧客が評価に係る資料等を保存する期間等を勘案して適切なものとすることが望ましい。

注記 2　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。

2.15　結果の報告（ISO/IEC 17025 7.8.1.2項）

2.15.1　コモンクライテリア評価において、ISO/IEC 17025 7.8.1.2 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、評価機関等が定めた様式であって、IAJapan に届出たものを使用すること。

2.15.2　評価機関等は、行った評価業務に係る評価報告書を発行する。顧客へ提出する評価報告書は、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。評価機関等は、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。

2.15.3　認定範囲外のセキュリティ評価（例えば EAL5 を超える保証コンポーネントに係る評価）の結果を ILAC MRA 組み合わせ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。

2.16　評価報告書（ISO/IEC 17025 7.8.2項、7.8.3項）

2.16.1　評価機関等は、評価報告書の発行（承認）に責任を有する者を、IAJapan 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、評価報告書にその識別を含めること。なお、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ができる。

2.16.2　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。

2.16.3　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評価報告書に固有の識別を必要とする。評価報告書の複写については、5.1 の遵守事項に従うものとする。

2.17　内部監査（ISO/IEC 17025 8.8項）

申請事業者は、初回認定審査の前に、内部監査を少なくとも 1 回は実施しなければならない。

評価機関等の要員のうち 1 名のみが評価業務のいくつかの技術について能力を有する場

合、又は係る者が特定の試験を実施するにあたっての唯一の専門家である場合には、この技術的側面の監査のために同等の技術レベルを持つ別の専門家が機関内部に存在する必要はないが、この監査にあたる者は、最低限、以下の監査を実施できる能力を有し、また、実施しなければならない。

(1) 文書化及び指示に係るレビュー
(2) 手続及び指示の遵守状況の確認
(3) 監査所見の文書化

2.18 マネジメントレビュー（ISO/IEC 17025 8.9項）

申請事業者は、初回認定審査の前に、マネジメントレビューを少なくとも 1 回は実施しなければならない。

マネジメントレビューでは、技能試験結果を含めてレビューすること。CC 認証機関による認証レビューを評価結果の品質の保証として用いる場合は、「認証レビュー」の指摘に対し組織的な対策が必要であるかどうかを検討し、マネジメントレビューにおいて報告をすること。

第3部　認定区分：情報技術－暗号モジュール試験を行う事業者に対する一般要求事項

3.1　一般

3.1.1　IAJapan は、暗号モジュール試験の申請事業者及び試験機関（以下「暗号モジュール試験機関等」という。）に対し、認定スキーム文書(UIF03) 別紙 11(ASNITE-T(IT))に記載した認定要求事項を、ASNITE 試験事業者 IT の認定（認定区分：情報技術－暗号モジュール試験）のための認定要求事項として適用する。

3.1.2　第 3 部に掲げる規定は、同要求事項の暗号モジュール試験機関等への適用方針とする。

3.2　公平性（ISO/IEC 17025 4.1項、5.1項）

暗号モジュール試験機関等は、暗号モジュール試験業務（ラボラトリ活動）が公平に実行され、公平性を確保するように編成及び運営をしければならない。この公平性を確保する手段には以下を含むものとする。

ただし、暗号モジュール試験機関等は、利益相反に該当しない場合には、試験要件及び関連文書の説明を提供することができる。

(1) 暗号モジュール試験機関等が暗号モジュール試験以外の活動も行う組織の一部分である場合であり、暗号モジュール試験以外の活動が試験の結果に影響を及ぼすと考えられる場合は、その試験以外の活動を特定し、それらの活動とその試験業務との間を（物理的及び電子的に）分離すること。

(2) 暗号モジュール試験機関等は、認定範囲内で実施する暗号モジュール試験作業において試験料金以外の金銭的利害関係をその顧客との間で持ってはならない。

(3) 暗号モジュール試験機関等は、暗号アルゴリズム実装又は暗号モジュールのいずれかの部分を自らが設計、文書作成、コード化、実装した場合、又は自らが何らかの所有権を有するか若しくは投資した場合、そのモジュールを試験してはならない。暗号モジュール試験機関等が暗号モジュールの開発事業者を所有しておらず、暗号モジュール試験機関等の経営陣が開発事業者から完全に独立している場合であり、開発事業者との取引が他の顧客と同様に契約上の合意に基づいて行われる場合には、試験を実施することができる。

(4) 暗号モジュール試験機関等は、暗号モジュール又は暗号アルゴリズム実装に関する既存の開発事業者文書（設計後及び開発後のもの）を入手し、その情報（複数の提供元から入手したもの）を統合し又は所定のフォーマットに再フォーマットすることがある。これが行われる場合には、試験報告書の提出時に CM 認証機関にその旨が通知されなければならない。

3.3　機密保持（ISO/IEC 17025 4.2項）

暗号モジュール試験機関等のマネジメントシステムは、顧客の機密情報の保護を確実にするための方針及び手順を含まなければならない。かかる方針及び手順には、顧客の機密情報について、暗号モジュール試験機関等の部外者、暗号モジュール試験機関等への訪問

者、知る必要のない暗号モジュール試験機関等の職員等（契約による要員を含む）及びその他の権限が付与されていない者からどのように保護するのかが規定されなければならない。

3.4 ラボラトリ活動の範囲（ISO/IEC 17025 5.3項）

暗号モジュール試験機関等は、ラボラトリ活動の対象となる範囲について、文書化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実装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。

認定範囲は次のいずれかとする。

(1) 基本暗号セキュリティ、暗号アルゴリズム実装試験
(2) 基本暗号セキュリティ、暗号アルゴリズム実装試験、暗号ソフトウェアモジュール試験３（セキュリティレベル１）
(3) 基本暗号セキュリティ、暗号アルゴリズム実装試験、暗号ソフトウェアモジュール試験４（セキュリティレベル２）
(4) 基本暗号セキュリティ、暗号アルゴリズム実装試験、暗号ソフトウェアモジュール試験５（セキュリティレベル３）
(5) 基本暗号セキュリティ、暗号アルゴリズム実装試験、暗号ソフトウェアモジュール試験３（セキュリティレベル１）、暗号ソフトウェアモジュール試験４（セキュリティレベル２）
(6) 基本暗号セキュリティ、暗号アルゴリズム実装試験、暗号ソフトウェアモジュール試験３（セキュリティレベル１）、暗号ソフトウェアモジュール試験４（セキュリティレベル２）、暗号ソフトウェアモジュール試験５（セキュリティレベル３）
(7) 基本暗号セキュリティ、暗号アルゴリズム実装試験、暗号ハードウェアモジュール試験３（セキュリティレベル１）
(8) 基本暗号セキュリティ、暗号アルゴリズム実装試験、暗号ハードウェアモジュール試験４（セキュリティレベル２）
(9) 基本暗号セキュリティ、暗号アルゴリズム実装試験、暗号ハードウェアモジュール試験５（セキュリティレベル３）
(10) 基本暗号セキュリティ、暗号アルゴリズム実装試験、暗号ハードウェアモジュール試験３（セキュリティレベル１）、暗号ハードウェアモジュール試験４（セキュリティレベル２）
(11) 基本暗号セキュリティ、暗号アルゴリズム実装試験、暗号ハードウェアモジュール試験３（セキュリティレベル１）、暗号ハードウェアモジュール試験４（セキュリティレベル２）、暗号ハードウェアモジュール試験５（セキュリティレベル３）
(12) 基本暗号セキュリティ、暗号アルゴリズム実装試験、暗号ソフトウェアモジュール試験３（セキュリティレベル１）、暗号ハードウェアモジュール試験３（セキュリティレベル１）
(13) 基本暗号セキュリティ、暗号アルゴリズム実装試験、暗号ソフトウェアモジュール試験３（セキュリティレベル１）、暗号ソフトウェアモジュール試験４（セキュリティ

レベル２）、暗号ハードウェアモジュール試験３（セキュリティレベル１）、暗号ハードウェアモジュール試験４（セキュリティレベル２）

(14) 基本暗号セキュリティ、暗号アルゴリズム実装試験、暗号ソフトウェアモジュール試験３（セキュリティレベル１）、暗号ソフトウェアモジュール試験４（セキュリティレベル２）、暗号ソフトウェアモジュール試験５（セキュリティレベル３）、暗号ハードウェアモジュール試験３（セキュリティレベル１）、暗号ハードウェアモジュール試験４（セキュリティレベル２）、暗号ハードウェアモジュール試験５（セキュリティレベル３）

3.5　要員の力量（ISO/IEC 17025 5.6項、6.2.1項、6.2.2項、6.2.3項）

3.5.1　暗号モジュール試験機関等の技術管理要員の力量

(1) 技術面の管理に責任を有する要員（以下この文書では「技術管理要員」という。）は、試験業務の技術的事項の全責任を負う。

(2) 技術管理要員は、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。

3.5.2　暗号モジュール試験機関等の試験要員の力量

(1) 暗号モジュール試験機関等は、技術系の学位（コンピューターサイエンス、コンピュータ工学、電気工学の学士号など）、同様の技術的訓練又は同等の経験（技術者認定など）といった、認定範囲に相当する知識及び技術を持つ試験要員を確保すること。

(2) 試験要員は、試験業務に係る力量を有すること。

(3) 試験要員は、以下に定める知識を有し、その内部力量基準は適切であること。

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) 承認されたセキュリティ機能に係る知識
4) 暗号モジュール試験要件に係る知識
5) 暗号アルゴリズム実装試験要件に係る知識
6) 運用ガイダンスに係る知識
7) 認定範囲の FIPS、NIST SP (Special Publications) 及び NIST HB 150-17 と NVLAP が CMVP に関して公表する情報について熟知している。
8) 暗号用語及び一連の暗号アルゴリズムと、FIPS 承認／NIST 推奨のセキュリティ機能に精通している。
9) 暗号セキュリティ試験ツールに精通している。
10) 認定範囲の試験方法、試験基準、及び運用ガイダンスのすべてに精通している。

3.5.3　主要な要員（ラボラトリマネジメント、品質管理要員、技術管理要員、試験要員）の一部又は全部が雇用による契約以外の契約がある場合には、これを特定し、リスト化した上で、すべての主要な要員のリストとともに申請時に提出すること。この要員に変更が生じた場合、この要員を直接監視ができなくなった場合、IAJapan 及び CM 認証機関に書面で通知しなければならない。

注記　暗号モジュール試験機関等の主要な要員または施設に著しい変更、又は契

約による要員に上述のような変更がある場合、IAJapan は、必要な場合、臨時審査を実施する場合がある。速やかに適切な補充を行うことなく主要な要員を失った場合、暗号モジュール試験機関等の認定が一時停止される可能性がある。

3.5.4　暗号モジュール試験機関等は、各人に複数の職制を割り当て又は任命することができる。

注記　暗号モジュール試験機関等の長及び品質管理要員の職位には、専任の職員を配置することが望ましい。

3.5.5　品質管理要員は、マネジメントシステムに係る教育訓練として、可能であれば ISO/IEC 17025 に係るものを受けなければならない。ISO/IEC 17025 に係る教育訓練を受けることができない場合、最低でも ISO 9000 シリーズ（特に ISO 9001）又は内部監査員の教育訓練に特に重点を置いたものと同等の教育訓練を受けなければならない。

3.6　要員の教育・訓練（ISO/IEC 17025 6.2.2項）

3.6.1　暗号モジュール試験機関等は、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、暗号モジュール試験機関等の業務に対して適切でなければならない。

3.6.2　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。

3.6.3　暗号モジュール試験機関等の要員は、以下にリストされた領域に関する知見を有するか、その領域での訓練を前もって受けなければならない。

(1) 試験報告書の作成を含む試験方法に係る一般要件
(2) システムセキュリティの概念
(3) 物理的セキュリティ
(4) 識別及び認証技術及び技法
(5) 暗号及びセキュリティ用語への習熟
(6) 標準準拠
(7) CM 認証機関から貸与された試験ツールの操作及び維持
(8) 暗号鍵管理
(9) 構成管理
(10) 有限状態マシン
(11) NIST HB 150-17 の習熟度
(12) 評価プログラム（JCMVP 等）で義務づけられた試験ツールの運用及び保守

3.6.4　暗号モジュール試験機関等は、各要員に実施権限が与えられた試験方法に係るそれぞれの要員の能力についての評価及び維持のための能力のレビュープログラム及び手続きを有しなければならない。パフォーマンスの評価及び観察は、直属の上司又は暗号モジュール試験機関等の長に指名された者が、各要員に対して毎年実施すること。

3.7　施設及び環境条件（ISO/IEC 17025 4.2項、6.3項、7.11.3項）

3.7.1　施設の機密保護及び所有権の保護

(1) 暗号モジュール試験機関等は、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) 暗号モジュール試験を行う施設（試験室）

2) 同試験に係る機密情報の保管場所

3) 同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）

注記 1　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。

注記 2　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) 暗号モジュール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) 同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又は消去すること。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。

(2) 暗号モジュール試験機関等は、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) 暗号モジュール試験機関等は、暗号モジュール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。

(4) 暗号モジュール試験機関等は、顧客の機密情報及び所有権の保護に係る倫理規程を整備しなければならない。

3.7.2　暗号モジュール試験を行う施設及びその環境条件

(1) 暗号モジュール試験機関等は、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) 3.7.1(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) 暗号モジュール試験機関等は、同試験機関等の恒久的な施設以外の場所（例えば顧客のサイト、遠隔オフィスなど）で試験活動を行う場合には、その環境を ISO/IEC 17025 6.3 項の要求事項を満たすものに適合させなければならず、その確認は暗号モジュール試験機関等によって確認されなければならない。

(3) 暗号モジュール試験機関等は、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暗号モジュール試験を行う場合には、同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。

3.7.3　暗号モジュール試験機関等は、複数の暗号モジュール試験を同時に行う場合、開発事業者の暗号アルゴリズム実装及び暗号モジュールそれぞれの間のシステムの分離及び適合性試験実施の分離を必要に応じて維持しなければならない。

3.7.4　暗号モジュール試験機関等は、すべての適合性試験の実施において、暗号アルゴリズム実装及び暗号モジュールに係る過去の試験結果や試験プログラムを含む電子ファイルが現行の試験プログラム及び試験結果から分離されていることを確認する必要がある。

3.7.5　暗号モジュール試験機関等が暗号モジュール試験のために自らの認定（申請）範囲に含まれる施設以外の施設で試験活動を実施する場合、当該施設は、認定された試験施設として、暗号アルゴリズム実装又は暗号モジュールの試験に関するすべての要求事項を満たさなければならない。

注記　暗号モジュール試験機関等は、この要求事項を満たすために、IAJapan 若しくは NVLAP が提供するチェックリスト及び／又は顧客との契約書を使用することができる。

3.7.6　暗号モジュール試験機関等が自らの認定（申請）範囲に含まれる設備以外で顧客の機密情報を扱う場合、顧客に開示しなければならない。

3.7.7　すべての記録は恒久的施設で保管されなければならない

3.8　設備（ISO/IEC 17025 6.4項）

3.8.1　暗号モジュール試験機関等は、暗号モジュール試験のために必要なハードウェア、ソフトウェア、試験ツール、コンピュータ設備等の設備を、購入、リース又はレンタルによって利用可能とし、常時又は試験実施前までには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暗号モジュール試験機関等が使用する必要なソフトウェア試験一式、物理試験のための試験設備、適用規格の現行版に示される認定範囲のすべての試験の実施に必要な特定の装置等を含めるものとする。

3.8.2　暗号モジュール試験機関等は、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 7.11 項に適合することを確保しなければならない。

3.8.3　暗号モジュール試験機関等は、顧客が所有する設備等、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るときは、顧客等と契約を締結することにより、ISO/IEC 17025 6.4 項への適合性を確保しなければならない。

注記 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。

3.8.4 暗号モジュール試験機関等は、暗号及びセキュリティ試験の実施に用いられる試験ツールが、CM 認証機関の仕様に従って適切に稼働していることを確かなものとし、当該ツールが試験の実施を妨げておらず、暗号アルゴリズム実装又は暗号モジュールが変更され、また、影響を与えられていないことを確認しなければならない。

3.8.5 試験実施の前に、現行版で最新の試験ツールが確実に使用されるようにする。こうした確認の記録も維持しなければならない。

3.8.6 適合性試験時には、暗号モジュール試験機関等は、適宜、評価プログラム（JCMVP 等）で提供される試験ツールの複写物の所有、読み込み、実行や当該ツールを用いた試験結果の生成をすること。同評価プログラムから提供される試験ツールは改造したり変更したりしてはならず、当該試験プログラム以外の外部に配布してはならない。

3.8.7 試験ツールに大小を問わず変更を加える場合、暗号モジュール試験機関等は当該試験ツールの精確な実行及び適正なパフォーマンスを確かなものとするための手続きを持たなければならない。当該手続きには少なくとも当該試験ツールの回帰試験一式が含まれなければならない。整合性が維持されていることを確実とすることが必要であり、必要に応じて他の認定試験機関との整合性が確保され、関係する規格や仕様に準じて正確性が維持されている必要がある。

3.8.8 供与される試験ツールには認定の適用対象とされる試験所外で可能な適切な検証サービスがない場合があり、かつ、試験ツールを検証するために試験機関によって使用され得る適切な参照実証がない場合がある。このような場合、暗号モジュール試験機関等は当該試験ツールの正しい操作をチェックするために使用される手続きや方法を定義し、文書化しなければならず、当該試験ツールが変更される場合にこれらの手続き及び方法が適用される根拠を提示しなければならない。

3.8.9 暗号モジュール試験機関等は、試験ツールに不具合又は使用に適さないようなエラーを含むことが疑われる又は発見した場合の適切な手続きを文書化し、これを実施しなければならない。これらの手続には、真のエラーが存在することを確立するための及び適切な維持管理を行う著作権者又は CM 認証機関に当該エラーを報告するための手続を含まなければならない。試験ツールの矯正後に暗号アルゴリズム実装又は暗号モジュールへの適合性試験結果が変わる場合は、顧客及び CM 認証機関にその旨当該情報が伝達されなければならない。

3.8.10 暗号モジュール試験機関等は、試験設備の構成及びすべての分析の記録を維持し、要求される試験を実行するための試験設備の適合性を確保する。

3.8.11 日付、ハードウェア及びソフトウェアのアップグレードの範囲、更新及び使用期

限のそれぞれは記録として保管されなければならない。

3.9 設備の維持、校正（ISO/IEC 17025 6.4.3）

3.9.1 暗号モジュール試験機関等は、暗号モジュール試験を行うために用いる設備を、次に掲げる事項のいずれかに従って維持しなければならない。この場合の設備とは、暗号アルゴリズム実装又は暗号モジュールの試験をサポートするために使用されるソフトウェア製品、ハードウェア製品及び／又はその他の評価のための仕組みを言う。

(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) 該当する場合、暗号モジュール試験機関等の管理手順。

3.9.2 必要に応じ、適合試験の実施に用いられる設備は、製造元の推奨事項、試験方法で指定する方法、又は該当する試験方法に関する NIST HB 150-17 の附属書 B に指定された方法に従って、保守及び校正しなければならない。

3.9.3 暗号モジュール試験機関等は、試験行為を妨げ、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。

注記 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、法令又は当該設備を規定する仕様等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。

3.9.4 ハードウェア及びソフトウェアの校正は以下により実施される。

(1) すべてのハードウェア及びソフトウェアの構成管理　又は

(2) 版数管理システム。

3.10 計量トレーサビリティ（ISO/IEC 17025 6.5項）

3.10.1 暗号モジュール試験機関等が使用する設備において、適用がふさわしい場合には、計量トレーサビリティが要求される。計量トレーサビリティの確保が求められる場合には、認定センターが別に定める「IAJapan 計量トレーサビリティ方針(URP023)」に従い実施すること。

　このトレーサビリティは、ISO/IEC 17025 6.6 項に基づき暗号モジュール試験の外部提供者に依頼したとき、3.8.3 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。

3.10.2 暗号モジュール試験全体におけるトレーサビリティとは、検証のための試験ツールが適用される規格にトレーサブルであることと解釈される。これは、各理論上の試験事案及び関連する評価方法が所管の文書規格に掲載された暗号モジュール試験要件及び暗号アルゴリズム実装試験要件にトレーサブルであることを意味し、当該理論上の試験事案はアサーション及び使用中の試験ツールに記述された関連する試験要件（DTRs）を通して達成されることを意味する。暗号モジュール試験機関等に

よって生成された試験結果は、適切な場合、標準試験ツール一式にトレーサブルでなければならず、そうでない場合は、適用可能な権威ある試験ツール一式にトレーサブルでなければならない。よって、暗号モジュール試験のトレーサビリティは、ISO/IEC 17025 6.5.3b)項で規定する「規定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「規定された方法」とは、暗号モジュール試験要件及び暗号アルゴリズム実装試験要件をいう。

注記 暗号モジュール試験機関等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実装試験）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。

3.10.3 暗号モジュール試験機関等内で実行される校正の場合、使用される参考標準及び校正時の環境条件は、すべての校正について文書化するものとする。校正の記録、及び使用する参考標準に対するトレーサビリティの証拠は、認定審査時において使用できなければならない。

3.10.4 プログラムに固有な試験対象と試験ツールが想定する理論上の試験事例との間に相違がある技術分野においては、暗号モジュール試験機関等は、判定付与の維持又は対応する一連の観察（observations）のための測定（measurement）により、該当する規格から各試験事例の実現化がいかにして正確に導き出されているかを示さなければならない。

3.11 外部から提供される製品及びサービス（ISO/IEC 17025 6.6項）

暗号モジュール試験機関等による試験工程の完遂及び／又は向上のためにその工程の一部として下請負契約及び同契約の契約先（外部提供者）が利用される場合、当該外部提供者は、NVLAP の認定を受けた試験機関又は IAJapan の認定を受けた試験機関であってその認定範囲が適用される試験方法を含むこと。又は、ISO/IEC 17025 の要求事項及び／又は NIST HB 150、NIST HB 150-17、及び JCMVP に関するすべての文書に示されたすべての試験要求事項を満たす外部提供者が提供するサービスを利用しなければならない。後者の場合、暗号モジュール試験機関等は以下のことを遵守しなければならない。

(1) この特定の外部提供者を選定した理由と、当該外部提供者が ISO/IEC 17025 の該当する要求事項及び特定要求事項をどのようにして満たすのかを説明し、選定の正当性を示し、

(2) かつ、当該外部提供者が実施する試験の結果について全責任を負うものとする。

3.12 依頼、見積仕様書及び契約のレビュー（ISO/IEC 17025 4.2項、7.1項）

3.12.1 機密情報を含む文書、秘密保持契約（守秘義務に係る契約）の文書、「要保護」と標示される文書、又は著作権で保護される文書（及び契約書）の保存に関する方針は、それら文書の地位に応じて明確に規定されなければならない。これらの文書には、その種別及び／又は機密性の格付けに相応した保護が施されなければならない。また、当該文書へのアクセス権は許可された者のみに付与されなければならな

い。

3.12.2　暗号モジュール試験機関等と顧客は、暗号アルゴリズム実装又は暗号モジュールを構成する要素、及び当該暗号アルゴリズム実装内の環境を構成する要素について文書にて合意しなければならない。環境は以下のものを含むがこれらに限定されない。

(1) 特定の試験実施環境
(2) 試験構成
(3) 外部環境

3.13　試験の方法の選定（ISO/IEC 17025 7.2.1項）

3.13.1　暗号モジュール試験機関等は、試験方法として暗号モジュール試験要件、暗号アルゴリズム実装試験要件及び運用ガイダンスを用いなければならない。

3.13.2　暗号モジュール試験機関等は、必要な場合には、暗号モジュール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。

3.13.3　暗号モジュール試験は、顧客先、暗号モジュール試験機関等の試験施設又は両者が合意した別の場所で実施される。顧客先で当該試験が実施される場合、ISO/IEC 17025 6.3 で要求する事項が要求される。いかなる必須とされる試験ツールの読み込み（loading）、コンパイル（compiling）、設定（configuring）、実行（execution）を含む暗号モジュール試験実施及び結果の記録を行うために必要なすべての行為は、暗号モジュール試験機関等の要員によって実施されなければならない。

3.13.4　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。

3.13.5　暗号モジュール試験機関等は、3.13.1 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。

3.14　方法の妥当性確認（ISO/IEC 17025 7.2.2.1項）

ISO/IEC 17025 **7.2.2.1** 項 注記 2.のうち「a) 参照標準又は標準物質を用いた、校正又は偏り及び精度の評価。」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。

3.15　試験品目の取扱い（ISO/IEC 17025 7.4項）

3.15.1　暗号モジュール試験機関等は、すべての暗号アルゴリズム実装、暗号モジュール及び試験ツールについて、いかなる種類の変更や無許可のアクセスや使用がなされないよう保護しなければならない。

3.15.2　暗号モジュール試験機関等は、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。

3.15.3　前項のシステムは、暗号モジュール試験機関等への訪問者、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。

3.15.4　暗号アルゴリズム実装又は暗号モジュールの構成要素がソフトウェアで構成される場合、暗号モジュール試験機関等は、不注意等故意以外の変更から防護するための構成管理（configuration management）を設けることを確実にしなければならない。この構成管理により、各暗号アルゴリズム実装又は暗号モジュールは、固有に識別され構成されるソフトウェアそれぞれへのいかなる変更も管理され文書化されなければならない。

3.16　技術的記録（ISO/IEC 17025 4.2項、7.5項、7.11.3項、8.4項）

3.16.1　暗号モジュール試験機関等は、最終試験結果又は暗号セキュリティ試験用ツールを用いて生成された暗号アルゴリズム実装又は暗号モジュールに関する試験報告書を、当該試験終了後、当該暗号アルゴリズム実装又は暗号モジュールの有効期間を考慮した上で、CM 認証機関又は顧客が文書にて指定したとおりに保管しなければならない。記録には、公式の試験結果及び試験結果エラーファイルの紙媒体による記録、又は電磁的記録が含まれる。記録は、機密性、完全性及び可用性を保証する方法で保管されなければならない。

注記　暗号モジュール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。

3.16.2　最終試験結果又は暗号セキュリティ試験用ツールを用いて生成された暗号アルゴリズム実装又は暗号モジュールに関する試験報告書の写しが発行され、CM 認証機関に提出されなければならない。

3.16.3　暗号モジュール試験機関等は、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) 暗号モジュール試験方法及び同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

3.17　結果の報告（ISO/IEC 17025 7.8.1.2項）

3.17.1　試験報告書の様式は、暗号モジュール試験機関等が定めた様式であって、IAJapan に届け出たものを使用すること。

3.17.2　暗号モジュール試験機関等は、試験条件、標準手順から逸脱した場合は試験設定情報、試験結果及び試験を再度実施するために必要なその他のすべての情報を示す正確、明瞭、かつ曖昧な表現のない実施し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。暗号モジュール試験機関等は、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　認定範囲外の暗号モジュール試験の結果を ILAC MRA 組み合わせ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 7.8.2項、7.8.3項）

3.18.1　暗号モジュール試験機関等は、評価プログラム（JCMVP 等）に試験報告書を提出するにあたり、独立した技術品質レビューを実施しなければならない。ここでは、正確さ、完全さ、試験結果の十分な根拠及び整合性を扱う。このレビューの記録は維持されなければならない。

3.18.2　暗号モジュール試験機関等は、試験報告書の発行（承認）に責任を有する者を、IAJapan 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、試験報告書にその識別を含めること。なお、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ができる。

3.18.3　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。

3.18.4　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試験報告書に固有の識別を必要とする。試験報告書の複写については、「第 5 部 その他の遵守事項等」の「5.1 遵守事項」に従うものとする。

3.18.5　暗号モジュール試験機関等は、CM 認証機関の指示に従い、電子文書での試験報告書を提出することができる。電子文書での試験報告書は紙による試験報告書と同じ内容であり、CM 認証機関から貸与される暗号アルゴリズム実装試験を行うことを目的としたツールを使用して作成しなければならない。

3.18.6　CM 認証機関への試験報告書の電子的伝送が行われる場合であって受領すべき者以外の第 3 者が開封することができないことを確かなものとするために、試験報告書が変更されていないことを確かなものとするためのデータ完全性のための仕組みが存在する場合、暗号モジュール試験機関等は、データの機密性及び／又はプログラム要求事項及び／又は政府要求事項に適合した完全性及び秘匿性確保のための仕組みを確かなものとしなければならない。

3.18.7　CM 認証機関による評価を受けるために作成され CM 認証機関等認証プログラムに提出される試験報告書においては、暗号モジュール試験機関等は、試験報告書への修正又は追加を発行する場合には、補完文書の形でこれを行わなければならず、その際、例えば「文書発行番号〇〇の試験報告書への補遺」等の適切な表示を行う。その変更が試験の成立条件を含む場合は、当該文書は、どの試験成立条件が課題となったか、結果の内容、結果の説明及び結果受入れの理由を特定しなければな

らない。

3.19 記録の管理

3.19.1 暗号モジュール試験機関等は、記録管理のためのシステムを維持しなければならない。記録は、容易にアクセスでき、かつ、完全でなければならない。記録が電磁的記録媒体に記録されている場合は、記入、修正、削除等に係る行為者のログが取られ、かつ、適切に標識付けされなければならない。また、それらのバックアップが適切かつ確実に取られなければならない。紙媒体の記録の記入事項には、日付と署名又はイニシャルが付されなければならない。

3.19.2 秘密保持契約（守秘義務に係る契約）により保護され又は機密として分類されるソフトウェア及びデータは、開発事業者又は政府の要求に従って、データの機密性の格付けに相応するように保管されなければならず、アクセス権（閲覧を含む）は許可された職員のみに付与されるものとする。これらのソフトウェア及びデータについては、アクセス履歴記録ファイル（閲覧記録を含む）が維持されなければならない。

3.19.3 暗号モジュール試験対象の顧客のシステムが第三者から潜在的にアクセス可能な場合、暗号モジュール試験機関等は、第三者が当該試験中に当該システムにアクセスできないように試験環境が管理されることを確実にしなければならない。

3.19.4 教育訓練、内部監査及びマネジメントレビューを含むすべてのマネジメントシステム業務の記録は、確実に保存されなければならない。電磁的記録の完全性がデータの機密性の格付けに相応した手段によって保証されなければならない。紙媒体での記録は、標識付けされ、安全な場所に保管されなければならない。また、必要に応じ、紙媒体での記録の完全性を保ち無許可の変更を防止するために、すべての閲覧、変更又は追加の記録が維持されなければならない。

3.19.5 暗号モジュール試験機関等は、試験装置の適合性を確保して暗号モジュール試験を実施するために、試験装置の構成及びすべての解析の記録を維持しなければならない。

3.20 内部監査（ISO/IEC 17025 8.8項）

申請事業者は、初回認定審査の前に、内部監査を少なくとも 1 回は実施しなければならない。

暗号モジュール試験機関等の要員のうち 1 名のみが試験業務のいくつかの技術について能力を有する場合、又は係る者が特定の暗号モジュール試験を実施するにあたっての唯一の専門家である場合には、この技術的側面の監査を行うため、適切な技術を有する外部監査者が必要なことがある。この監査は最低限以下のものを含まなければならない。

(1) 文書化及び指示に係るレビュー
(2) 手続及び指示の遵守状況の確認
(3) 監査所見の文書化

3.21 マネジメントレビュー（ISO/IEC 17025 8.9項）

申請事業者は、初回認定審査の前に、マネジメントレビューを少なくとも 1 回は実施しなければならない。

第4部　認定区分：情報技術－システムLSI侵入テストを行う事業者に対する一般要求事項

4.1　一般

4.1.1　IAJapan は、申請事業者及び侵入テスト実施機関（以下、侵入テスト実施機関等という。）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：情報技術－システム LSI 侵入テスト）のための認定要求事項として適用する。

4.1.2 IAJapan は、第 4 部に掲げる規定を、前項の規定に基づく同要求事項の適用方針とする。

4.2　ラボラトリ活動の範囲（ISO/IEC 17025 5.3項）

侵入テスト実施機関等は、ラボラトリ活動の対象となる範囲について、文書化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について明確にしなければならない。認定範囲は以下とする。

(1) スマートカードに関する CC サポート文書に基づく AVA_VAN に係るシステム LSI への侵入テスト

注：侵入テスト実施機関等が CC 評価機関と外部提供者の契約を締結し、侵入テスト業務を受託する場合は、当該 CC 評価機関がテスト依頼者となる（以下、「テスト依頼者」という）。

4.3　要員の力量（ISO/IEC 17025 5.6項、6.2.1項、6.2.2項、6.2.6項）

4.3.1　侵入テスト実施機関等の技術管理要員の力量

(1) 技術面の管理に責任を有する要員（以下この文書では「技術管理要員」という。）は、侵入テスト業務の技術的事項の全責任を負う。

(2) 技術管理要員は、侵入テスト業務に係る十分な技術的知識を持ち、評価結果の正当性について検証を行う能力を有すること。

(3) 技術管理要員は、下記の知識並びに侵入テスト実施要員の教育・訓練及び適切な監督・指示を行う能力を有すること。

1) CC 評価に関する基礎的知識
2) システム LSI のセキュリティ上の脆弱性及び攻撃類型に関する知識
3) スマートカードに関する CC サポート文書に関する知識

注記　技術管理要員は、上記(3)に示す知識、経験に加え、システム LSI の開発経験、
又は CC 評価に関連した分野で 3 年以上の経験を有することが望ましい。

4.3.2　侵入テスト実施機関等の侵入テスト実施要員の適格性及び資格

(1) 侵入テスト実施要員は、同テスト業務に力量を有すること。

(2) 侵入テスト実施要員は、4.3.1(3)に定める知識を有し、その内部力量基準は適切であること。

(3) 侵入テスト実施要員は、侵入テストの下記の分野の一つ以上について、実施することができる専門的技能を有すること。

1) 差分電力解析攻撃
2) 電磁波解析攻撃
3) 故障利用解析攻撃
4) かく乱攻撃
5) 物理解析攻撃
6) ソフトウェア攻撃

注記 侵入テスト実施要員は、システム LSI の開発経験を有することが望ましい。

4.3.3 主要な要員（ラボラトリマネジメント、品質管理要員、技術管理要員及び侵入テスト実施要員）の一部又は全部が雇用契約以外の契約による場合は、これを特定し、リスト化した上で、すべての主要な要員のリストとともに申請時に提供すること。この要員に変更が生じた場合、この要員を直接監視ができなくなった場合、IAJapan に書面で報告しなければならない。

注記 契約による要員に上述のような変更がある場合、侵入テスト実施機関の認定地位に影響する可能性がある。

4.4 要員の教育・訓練（ISO/IEC 17025 6.2.2項）

4.4.1 侵入テスト実施機関等は、侵入テスト実施要員に教育・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、侵入テスト実施機関等の業務に対して適切でなければならない。

4.4.2 前項の教育・訓練プログラムは、少なくとも 4.3.1(3)の項目について行わなければならない。これらの教育・訓練は、継続して適切なテストが実施できるよう、又、最新の脆弱性攻撃に関する知識を習得できるように侵入テスト実施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。

4.4.3 侵入テスト実施機関等は、内部資格を有する侵入テスト実施要員が内部資格の範囲においてテストを実施できる能力があることを毎年確認すること。確認の方法はマネジメントシステム文書に明記し、定期的に見直すこと。能力の確認方法は、侵入テスト実施要員が実施したテスト結果のレビューによるほか、要員が侵入テストを実施していない場合にはそれに代わる教育・訓練の結果を確認する方法でもよい。

4.5 施設及び環境条件（ISO/IEC 17025 4.2項、6.3項）

2.7 項に準ずる。ただし、テスト依頼者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すること。

4.6 設備（ISO/IEC 17025 6.4.1項）

3.8 項に準ずる。

4.7 設備の維持（ISO/IEC 17025 6.4.3項、6.4.13項）

3.9.1、3.9.3、3.9.4 項に準ずる。

4.8 計量トレーサビリティ（ISO/IEC 17025 6.5項）

4.8.1 侵入テスト実施機関等が使用する設備において、適用がふさわしい場合には計量計測トレーサビリティが要求される。計量トレーサビリティの確保が求められる場合には、認定センターが別に定める「IAJapan 計量トレーサビリティ方針(URP23)」に従うこと。

4.9 テストの方法の選定（ISO/IEC 17025 7.2.1項）

4.9.1 侵入テスト実施機関等は、顧客又はテスト依頼者が予め指示、又は承認する基準と方法を用いて侵入テストを行わなければならない。

4.9.2 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。

4.9.3 侵入テスト実施機関等は、スマートカードに関する CC サポート文書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、必ず顧客の同意に基づき採用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) AVA_VAN.5 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）

4.10 技術的記録（ISO/IEC 17025 7.5.1項、8.4.2項）

侵入テスト実施機関等は、CC 評価に係る技術的記録の保存期間について、顧客又はテスト依頼者の要求に従わなければならない。

4.11 結果の報告（ISO/IEC 17025 7.8.1.2項）

4.11.1 侵入テストにおいて、ISO/IEC 17025 7.8.1.2 項の「試験報告書」に該当するのは「侵入テスト報告書」とする。侵入テスト報告書の様式は、侵入テスト実施機関等が定めた様式であって、IAJapan に届出たものを使用すること。

4.11.2 侵入テスト実施機関等は、行ったテスト業務に係る侵入テスト報告書を発行する。顧客又はテスト依頼者へ提出する侵入テスト報告書は、顧客又はテスト依頼者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。侵入テスト実施機関等は、侵入テストの結果を裏付ける証拠を提供できること。

4.11.3 認定範囲外の侵入テストの結果を ILAC MRA 組み合わせ認定シンボル付侵入テスト報告書に含めることについては、それらのテスト結果が認定範囲外のテスト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。

4.12 侵入テスト報告書（ISO/IEC 17025 7.8.2項、7.8.3項）

4.12.1 侵入テスト実施機関等は、侵入テスト報告書の発行（承認）に責任を有する者を、IAJapan に侵入テスト報告書発行責任者として届出なければならない。侵入テスト報告書発行責任者は、侵入テスト報告書にその識別を含めること。なお、侵入

テスト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ができる。

4.12.2　侵入テストの年月日については、当該テスト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。

4.13　内部監査（ISO/IEC 17025 8.8項）

申請事業者は、初回認定審査の前に、内部監査を少なくとも 1 回は実施しなければならない。

侵入テスト実施機関等の要員のうち 1 名のみがいくつかの技術について能力を有する場合、又は係る者が特定の試験を実施するにあたっての唯一の専門家である場合には、この技術的側面の監査を実施するために同等の技術レベルを有する別の専門家が当該機関内部に存在する必要はないが、この監査にあたる者は、最低限、以下の監査を実施できる能力を有し、また、実施しなければならない。

(1) 文書化及び指示に係るレビュー
(2) 手続及び指示の遵守状況の確認
(3) 監査所見の文書化

第5部　認定区分：情報技術－IoT 製品のセキュリティ要件適合評価を行う事業者に対する一般要求事項

5.1　一般

5.1.1　IAJapan は、申請事業者及び JC-STAR 評価機関（以下「JC-STAR 評価機関等」という。）に対し、認定スキーム文書(UIF03) 別紙 11(ASNITE-T(IT))に記載した認定要求事項、ASNITE 試験事業者 IT の認定（認定区分：情報技術－IoT 製品のセキュリティ要件適合評価）のための認定要求事項として適用する。

5.1.2　第 5 部に掲げる規定は、同要求事項の JC-STAR 評価機関等への適用方針とする。

注記　JC-STAR 評価機関等は、セキュリティ要件適合評価及びラベリング制度で定める「セキュリティ要件適合評価及びラベリング制度の評価機関承認等に関する要求事項（JSM-03）」への参照をマネジメントシステム文書に含めて運用することが望ましい。

5.2　公平性（ISO/IEC 17025 4.1項、5.1項）

JC-STAR 評価機関等は、評価業務（ラボラトリ活動）が公平に実行され、公平性を確保するように編成及び運営をしなければならない。この公平性を確保する手段には以下を含むものとするがこれらに限定されない。

(1) 原則、JC-STAR 評価機関等は、評価用提供物件（IoT 製品、開発者作成文書を含む。以下同じ）に関わるコンサルタントサービス等、評価の結果に影響を及ぼすと考えられる業務を実施してはならない。JC-STAR 評価機関等が評価以外の活動も行う組織の一部分である場合であり、評価以外の活動が評価の結果に影響を及ぼすと考えられる場合は、その評価以外の活動を特定し、それらの活動と評価業務との間を分離すること。

(2) JC-STAR 評価機関等は、ある評価用提供物件に関わるコンサルタントサービスを評価担当者に提供させた場合、当該評価担当者にその評価用提供物件を評価させてはならない。

(3) 評価担当者は、評価の対象となる製品の開発部門（又は評価用提供物件の作成支援作業を行う部門）と利害関係を有してはならない。

5.3　ラボラトリ活動の範囲（ISO/IEC 17025 5.3項）

JC-STAR 評価機関等は、ラボラトリ活動の対象となる範囲について、文書化しなければならない。認定範囲は★３（レベル３）の評価とする。

注記　★４（レベル４）の評価は適合基準が公表の後、追加を行う予定である。

5.4　要員の力量（ISO/IEC 17025 5.6項、6.2.1項、6.2.2項、6.2.6項）

5.4.1 JC-STAR 評価機関等の技術管理要員の力量

(1) 技術面の管理に責任を有する要員（以下この文書では「技術管理要員」という。）は、評価業務の技術的事項の全責任を負う。

(2) 技術管理要員は、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) 技術管理要員は、下記の知識並びに評価者の力量基準、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) 適合評価報告書の作成を含め、IoT 製品のセキュリティ適合評価に係る一般要求事項
2) 製品類型に応じた適合基準 に係る知識
3) 製品類型に応じた評価手順に係る知識
4) 評価対象の機能や構造を理解し、製品類型に応じた適合基準をもとに評価手順を適切に実行する知識
5) 情報処理に係る一般知識（コンピュータセキュリティ、コンピュータシステムアーキテクチャ、プログラミング言語、アルゴリズムとデータ構造、オペレーティングシステム、データベースシステム、ネットワーク等）
(4) 技術管理要員は、上記(3)に示す知識に加え、評価技術に関係のある IoT 製品の開発に係る知識又は経験を有すること。
注記 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。
(5) 技術管理要員は、上記(3)及び(4)に示す知識、経験に加え、JC-STAR と相互承認を実施している他国制度での適合基準及び評価手順に係る知識を有すること。
（参考）相互承認を実施している他国制度については、以下の Web サイトにて入手することができる。
URL: https://www.ipa.go.jp/security/jc-star/leverage.html

5.4.2 JC-STAR 評価機関等の評価者の力量
(1) 評価者は、評価業務に係る力量を有すること。
(2) 評価者は、5.4.1(3)に定める知識を有すること。
(3) 評価者は、IoT 製品に対する深い知識を維持すること。
注記 IoT 製品の開発経験を有することが望ましい。

5.4.3 主要な要員（ラボラトリマネジメント、品質管理要員、技術管理要員、評価者）の一部又は全部が雇用契約以外の契約による場合は、これを特定し、リスト化した上で、すべての主要な要員のリストとともに申請時に提出すること。この要員に変更が生じた場合、この要員を直接監視ができなくなった場合、IAJapan に届け出なければならない。
注記 契約による要員に上述のような変更がある場合、JC-STAR 評価機関の認定地位に影響する可能性がある。

5.5 要員の教育・訓練（ISO/IEC 17025 6.2.2項）

5.5.1 JC-STAR 評価機関等は、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、JC-STAR 評価機関等の業務に対して適切でなければならない。

5.5.2 前項の教育・訓練プログラムは、少なくとも 5.4.1 (3)1)から 4)の項目について行い、必要な場合には 5.4.1(3)5)の項目に係る教育・訓練を行わなければならない。教

育・訓練は、継続して適切な評価業務が実施でき、また、必要となる最新の技術に対応できるように評価者に対して計画的に行わなければならない。

5.5.3 JC-STAR 評価機関等は、内部資格を有する各要員が内部資格の範囲において評価を実施できる能力があることを毎年確認すること。確認の方法は、マネジメントシステム文書に明記し、定期的に見直すこと。能力の確認方法は、要員が実施した評価案件のレビューによるほか、要員が評価を実施していない場合にはそれに代わる教育・訓練の結果を確認する方法でもよい。

5.6 要員の管理（ISO/IEC 17025 6.2.1項、6.2.4項、6.2.6項）

5.6.1 評価者は、事業者間の契約又は個人契約等の契約による場合がある。いずれの場合でも JC-STAR 評価機関等が評価者に対し教育及び能力の確認を行い、認定範囲で実施される評価結果に責任を負うこと。

5.6.2 JC-STAR 評価機関等は、内部資格に対応する評価を実施することが困難となった評価者に対しては、付与した内部資格の範囲を見直す等の処置をとること。また、評価者が離職する場合の手順を有すること。

5.7 施設及び環境条件（ISO/IEC 17025 4.2項、6.3項、7.11.3項）

5.7.1 施設の機密保護及び所有権の保護

(1) JC-STAR 評価機関等は、少なくとも次に掲げる施設等を保有する場合は、自ら管理すること。また、これらの施設等を利用する場合には、顧客の機密情報の保護及び所有権の保護を確実に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及びそれに附帯する、インターネット等利用環境構築に供される施設（ただし、JC-STAR 評価機関等内に限る。）

注記 上記 2)ないし 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。

(2) 評価室は、入退室を管理するための認証システムを有すること。ただし、顧客サイトでの評価等により評価室以外の場所で評価を行う場合には、以下の要件に限定されない。

注記 認証システムは、すべての入退室者及び入退室日時が確定できるものであることが望ましい。

(3) 保管場所は、少なくとも次の要件を満たすこと。

1) JC-STAR 評価機関等が、顧客等が所有権を有する情報を保管する場合は、その情報に直接関係のない者からのアクセスを制限すること。

2) 評価に係る機密情報は、やむを得ない場合（例えば、顧客のサイトでテストを行う場合、JC-STAR 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。

3) 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。顧客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、暗号化消去がある。

(4) JC-STAR 評価機関等は、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 電子メール以外で送受信する場合の機密保護として、JC-STAR 認証機関又は JC-STAR 評価機関が指定する安全なファイル転送サービスを利用して、機密情報をファイルに包含させた上で、そのファイルをパスワード指定したうえで送付する方法がある。

(5) JC-STAR 評価機関等は、顧客の機密情報及び所有権の保護に係る倫理規程を整備しなければならない。

5.7.2 評価を行う施設及びその環境条件

(1) JC-STAR 評価機関等は、恒久的な施設以外の場所（例えば顧客のサイトなど）で評価を行う場合には、その環境を ISO/IEC 17025 6.3 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。評価を実施する前に、評価を行う施設が評価のための環境条件を満たしていることを確認すること。

(2) JC-STAR 評価機関等は、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。

5.8 **設備**（ISO/IEC 17025 6.4項）

5.8.1 JC-STAR 評価機関等は、評価実施に用いるすべての設備又はテストアプリケーション一式に係る情報、構成、設定、操作方法等について管理手順を有し、記録を維持すること。JC-STAR 評価機関等はこれらの設備等の構成、設定、操作等に責任を有すること。

5.8.2 JC-STAR 評価機関等は、評価実施に用いるコンピュータ装置及びその他のプラットフォームの構成・設定を制御すること。評価に用いるいずれの設備（ハードウェア及びソフトウェア）も、試験に用いる前に既知の状態になっていることを確実なものとするための手続きが、JC-STAR 評価機関等によって定められていること。

5.9 **計量トレーサビリティ**（ISO/IEC 17025 6.5項）

5.9.1 JC-STAR 評価機関等が使用する設備において、適用がふさわしい場合には計量トレーサビリティが要求される。計量トレーサビリティの確保が求められる場合に

は、IAJapan が別に定める「IAJapan 計量トレーサビリティ方針(URP23)」に従うこと。このトレーサビリティは、ISO/IEC 17025 6.6 項に基づき評価業務又はその一部を外部提供者に依頼したとき、顧客の設備を用いたときも確保すること。

5.9.2 セキュリティ評価実施に用いる設備は、メーカー（製造事業者）の推奨に従って、若しくは、JC-STAR 評価機関等の内部の手順に従って良好な状態に維持されるか、又は使用前に良好な状態であることが確認されなければならない。

5.9.3 JC-STAR 評価機関等は、評価に用いる試験ツールについて検証をすること。また、JC-STAR 評価機関等は、試験ツールの検証の記録を維持すること。

注記 試験ツールは試験の実施に影響を与えず、試験中に IoT 製品の完全性に変更や影響を与えないことを確認することが望ましい。

5.9.4 JC-STAR 評価機関等は、最初の評価のときと同等の評価が再現できることを保証すること。再評価のために顧客が所有する試験ツール等を使用することがあらかじめ想定される場合は、再評価に係る試験環境の再現について顧客と文書で合意をすること。

5.10 外部から提供される製品及びサービス（ISO/IEC 17025 6.6項、7.8.2.1p）項）

JC-STAR 評価機関等は、認定の申請を行う範囲又は認定を受けた範囲の中で、業務の一部を、外部提供者に請け負わせることができる。この場合、JC-STAR 評価機関等は、外部提供者が JC-STAR の適合基準、評価手順及び ISO/IEC 17025 の関連する要求事項を満足し、技術的信頼性を持つことを確実にすること。また、確認した結果（記録）を JC-STAR 評価機関自ら保持すること。これらの確認を行う場合において、外部提供者が ILAC MRA、APAC MRA に署名する IAJapan により認定を受けている場合は、マネジメントシステムに関する確認は省略することができる。

注記 JC-STAR 評価機関等は、外部提供者によって実施された評価結果及び／又は試験結果（以下、「評価結果等」という。）を適合評価報告書に引用する場合には、以下の全てを満たすこと。

(1) 外部提供者によって行われた評価結果等を含んでいる旨を適合評価報告書の ILAC MRA 組み合わせ認定シンボルを付した頁に明確に記載すること。

(2) 適合評価報告書の各評価結果等のうち、外部提供者によって実施された評価結果等は明確に識別すること。

5.11 評価の方法の選定（ISO/IEC 17025 7.2.1項）

5.11.1 JC-STAR 評価機関等は、JC-STAR 認証機関が公表する製品類型に応じた適合基準、評価手順を用いなければならない。

5.12 方法の妥当性確認（ISO/IEC 17025 7.2.2.1項）

ISO/IEC 17025 **7.2.2.1** 項 注記 2 のうち「a) 参照標準又は標準物質を用いた、校正又は偏り及び精度の評価。」などの方法は、セキュリティ要件適合評価においては適用しない。

5.13 評価品目の取り扱い（ISO/IEC 17025 7.4.1項、7.4.2項）

5.13.1 JC-STAR 評価機関等は、評価用提供物件について、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したりすることがないよう保護しなければならない。

5.13.2 JC-STAR 評価機関等は、同時に複数の IoT 製品を評価する必要があるときは、個々の製品、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。

5.14 技術的記録（ISO/IEC 17025 7.5.1項、7.11.3項、8.4.2項）

技術的記録は、JC-STAR 認証機関が公表する評価手順に従って行われたことが追跡できるものであること。技術的記録には評価項目に対しどのような評価が実施されたのかが客観的に分かるような十分な情報が含まれること。技術的記録には評価を実施した者及び評価結果のチェックに責任を持つ者の識別を含むこと。

データの改ざん防止、消失防止に備えてバックアップ機能を設けること。

注記 1 JC-STAR 評価機関等が内部で規定する技術的記録の保存期間は、顧客が評価に係る資料等を保存する期間等を勘案して適切なものとすることが望ましい。ただし、当該製品に対する適合ラベルの有効期間よりも長くなければならない。

注記 2 評価を行った IoT 製品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。

5.15 結果の報告（ISO/IEC 17025 7.8.1.2項）

5.15.1 セキュリティ要件適合評価において、ISO/IEC 17025 7.8.1.2 項の「試験報告書」に該当するのは「適合評価報告書」とする。適合評価報告書の様式は、JC-STAR 評価機関等が定めた様式であって、IAJapan に届出たものを使用すること。

5.15.2 JC-STAR 評価機関等は、行った評価業務に係る適合評価報告書を発行する。顧客へ提出する適合評価報告書は、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。JC-STAR 評価機関等は、セキュリティ要件適合評価の結果を裏付ける証拠を提供できること。

5.15.3 認定範囲外のセキュリティ要件適合評価（例えば諸外国の規格に基づく評価）の結果を ILAC MRA 組み合わせ認定シンボル付適合評価報告書に含めることについては、JC-STAR と相互承認を実施している制度での規格に基づく評価である場合に限る。また、それらの評価結果が認定範囲外のセキュリティ要件適合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。

5.16 適合評価報告書（ISO/IEC 17025 7.8.2項、7.8.3項）

5.16.1 JC-STAR 評価機関等は、適合評価報告書の発行（承認）に責任を有する者を、IAJapan に適合評価報告書発行責任者として届出なければならない。適合評価報告書発行責任者は、適合評価報告書にその識別を含めること。なお、適合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ができる。

5.16.2 IoT 製品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。

5.16.3 適合評価報告書は、一件の評価用提供物件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適合評価報告書に固有の識別を必要とする。適合評価報告書の複写については、6.1 の遵守事項に従うものとする。

5.17 内部監査（ISO/IEC 17025 8.8項）

申請事業者は、初回認定審査の前に、内部監査を少なくとも 1 回は実施しなければならない。

JC-STAR 評価機関等の要員のうち 1 名のみが評価業務のいくつかの技術について能力を有する場合、又は係る者が特定の試験を実施するにあたっての唯一の専門家である場合には、この技術的側面の監査のために同等の技術レベルを持つ別の専門家が機関内部に存在する必要はないが、この監査にあたる者は、最低限、以下の監査を実施できる能力を有し、また、実施しなければならない。

(1) 文書化及び指示に係るレビュー
(2) 手続及び指示の遵守状況の確認
(3) 監査所見の文書化

5.18 マネジメントレビュー（ISO/IEC 17025 8.9項）

申請事業者は、初回認定審査の前に、マネジメントレビューを少なくとも 1 回は実施しなければならない。

第6部　その他遵守事項等

申請事業者及び認定事業者は、第 2 部、第 3 部、第 4 部及び第 5 部に規定する一般要求事項に加え、以下の事項を適用する。

6.1　遵守事項

(1) 申請事業者及び認定事業者は、認定スキーム文書(UIF03) 別紙 11 (ASNITE-T(IT))に記載された全ての規定、要求事項に適合すること。
(2) 申請事業者及び認定事業者は、認定を取得し、維持するために別に定める「適合性評価機関の権利及び義務(UIF02)」３．適合性評価機関の義務に定める事項を遵守すること。
(3) 申請事業者は、「ASNITE 試験事業者 IT 認定の取得と維持のための手引き (TIRP22)」（以下この文書では「手引き」という。）に規定する認定申請書及び添付書類を作成し、提出すること。
(4) 申請事業者は、手引きに規定する「誓約書」を申請時に申請書類とともに IAJapan に提出すること。合わせて、IAJapan との間で、「機密保持に関する合意書」を締結すること。また、認定が授与される前に、IAJapan との間で、手引きに規定する「認定契約書」を締結すること。
(5) 申請事業者は、審査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、手引きの規定に従い届出ること。
(6) 申請事業者は、審査の過程で、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、手引きの規定に従い届出ること。
(7) 申請事業者及び認定事業者は、「認定スキーム文書 (UIF03)」に規定する審査を受けること。
(8) 申請事業者及び認定事業者は、認定（申請）書類に変更が生じた場合は、手引きに規定する届出が必要な事例及び提出書類を確認のうえ、届出ること。
(9) 申請事業者及び認定事業者は、この文書で規定する要求事項、認定要求事項及びその他 IAJapan が規定する要求事項に関する変更について、IAJapan から正当な通知を受けた場合には、指示された期間内にその業務手順について必要な変更を行うこと。また、変更が完了した時点で、その旨を手引きに従い届出ること。
(10) 申請事業者及び認定事業者は、認定審査のために必要が生じた場合、IAJapan が認定審査目的で当該事業者の顧客のサイトに立ち入ること及び当該顧客の依頼に基づき当該事業者が行う評価活動又は試験活動に IAJapan が立ち会うことを認める内容であってかつ当該顧客に対し強制力のある取り決めを、当該顧客との間で締結しなければならない。
(11) 認定事業者は、認定の地位の主張に関し、別に定める「IAJapan 認定シンボルの使用及び認定の主張等に関する方針(URP15)」に掲げる事項を遵守すること。また、以下の事項を遵守すること。
    1) ILAC MRA 組み合わせ認定シンボルを付していない評価報告書、試験報告書、侵入テスト報告書（以下「試験報告書等」という。）には、認定されている旨の表記

を含める事ができるが、その試験報告書等に認定範囲外の結果を含む場合には、認定範囲外の記載事項が認定範囲内であるかのような誤解を与える表現をしないこと。

2) 認定事業者は、外部提供者が発行する試験報告書等、カタログ、事務用品等に認定事業者（元請負）の認定資格を引用しないように努めること。

(12) 認定事業者は、ILAC MRA 組み合わせ認定シンボル付きの試験報告書等を発行する場合には、その様式を事前に IAJapan に届出ること。

(13) 認定事業者は、試験報告書等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、その報告書等を利用する者に対して通知すること。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。

(14) 認定事業者は、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、手引きの規定に従い届出ること。

(15) 認定事業者は、認定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、手引きの規定に従い届出ること。

(16) 認定事業者は、認定に用いられる規格（例えば、ISO/IEC 17025）を用いて認証行為を行わないこと。試験業務サービス提供者が ISO/IEC 17025 を含む認定規格に適合しているかの評価を行わなければならない場合があるが、試験業務サービス提供者に対して文書を発行する場合、この文書は試験業務サービス提供者を評価する目的で発行するものであって、ISO/IEC 17011 に基づく認証又は認定ではない旨を明記すること。(IAF ILAC JGA 2007 Sydney Resolution 7)

6.2 技術的能力の定期的な確認

申請事業者及び認定事業者は、以下に定める技能試験等(IAJapan 技能試験 及び/又は技能試験以外の試験所間比較への参加に関する方針(URP33)に定める技能試験等)を受けなければならない。

(1) 申請事業者

1) コモンクライテリア評価機関

2.4.3 に定める試行評価

2) 暗号モジュール試験機関

CM 認証機関が実施するアーティファクト試験、試行試験

3) 侵入テスト実施機関

IAJapan が情報提供する技能試験又はこれと同等と IAJapan が同意する試験等

4) セキュリティ要件適合評価機関

JC-STAR 認証機関が実施するまたは同意する技能試験等

注記　申請範囲が★3（レベル 3）の場合、CC 認証機関の監督の下で行われる過去 3 年以内の認証製品等の評価の実績を技能試験とみなすことができる。

(2) 認定事業者

1) コモンクライテリア評価機関

以下のいずれかを実施すること。

a)CC 認証機関の監督の下で行われる認証申請製品等の評価
b) 認定審査において実施される、認定範囲における技術的知識の確認
c) CC 認証機関が実施する技能に係る質疑応答

2) 暗号モジュール試験機関
以下のうち１つ以上の技能試験に参加すること。
a) 認定審査において実施される、CM 認証機関から貸与される暗号アルゴリズム実装試験を行うことを目的としたツールを用いた試験
b) 認定審査において実施される、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ツールを用いた試験
c) 認定審査において実施される、試験ツールによるデータ変換及び試験結果についての理解と解釈の確認
d) 認定審査において実施される、認定範囲における技術的知識の確認
e) CM 認証機関が実施する技能に係る質疑応答
f) CM 認証機関が実施するアーティファクト試験

3) 侵入テスト実施機関
IAJapan が情報提供する技能試験又はこれと同等と IAJapan が同意する試験等。

4) セキュリティ要件適合評価機関
a) JC-STAR 認証機関の監督の下で行われる IoT 製品の評価
b) 認定審査において実施される、認定範囲における技術的知識の確認
c) JC-STAR 認証機関が実施する技能に係る質疑応答

6.3 認定の取得と維持

審査の種類（初回認定審査、認定維持審査、再認定審査、区分追加審査及び臨時審査）、認定周期及び審査時期は、は、認定スキーム文書(UIF03)を参照のこと。

6.4 変更の届出

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 IAJapan 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。認定を受けた試験所を移転した際に IAJapan が必要と判断する場合は、認定試験事業者に対して臨時審査を行う。
(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) 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、区分を追加する場合、区分内の製品分野を追加する場合又は EAL の数値を大きくする場合には区分追加申請となる。

6.5 認定の一時停止、取消し又は縮小

(1) 認定の一時停止

認定試験事業者が認定要求事項に適合していないおそれがある場合又は認定の規則に従っていないおそれがある場合は、その内容の重大性を勘案して、その認定の一時停止を行う場合がある。また、認定の一時停止後、認定試験事業者から合理的な理由の説明がないまま、一時停止が 3 ヶ月を超えた場合は、認定試験事業者に状況を確認した上で、臨時審査の実施、認定の取消しの手続きの開始等の次のプロセスに移行する。

(2) 認定の取消し

以下のいずれかに該当する場合、認定が取り消されることがある。

1) 認定試験事業者が一時停止に係る是正処置を行わず認定要求事項に適合していなかった場合、又は認定の規則に従わなかった場合。
2) 不正行為の証拠が存在する場合、又は認定を受けた試験所が意図的に虚偽の情報を提出した場合、若しくは情報を隠蔽した場合。
3) 審査が拒まれ、妨げられ、又は忌避されたとき。
4) 審査に要する費用を負担しない場合。
5) 認定スキーム文書(UIF03)に規定する審査を受けない、IAJapan 技能試験 及び/又は技能試験以外の試験所間比較への参加に関する方針(URP33)に適合しない等、認定要求事項の要件を満たさなかった場合。
6) 認定の地位の表明又は IAJapan 認定シンボルの使用及び認定の主張等に関する方針(URP15)に適合しない等、ILAC MRA 組み合わせ認定シンボルの使用に当たって、IAJapan の評判を落とすような若しくは認定事実と異なる表明又は使用があった場合。

認定試験事業者は、当該認定の一時停止又は取消しを受けた場合は、直ちに一切の認定の地位の主張及び ILAC MRA 組み合わせ認定シンボルの使用を停止又は中止すること。また、取消しを受けたときには、認定証が発行されている場合、その認定証を速やかに IAJapan に返却すること。

(3) 認定の縮小

IAJapan は、認定維持審査、再認定審査又は臨時審査の結果、認定試験事業者が認定要求事項の一部ついて必要な能力を有していないことを IAJapan が定めるルールに基づき認めた場合、これまでに授与した認定の範囲の一部について取り消す場合がある。また、一部について取消しを受けたときには、認定証が発行されている場合、その認定証を速やかに IAJapan に返却すること。

6.6 ILAC MRA組み合わせ認定シンボルの使用（ILAC-R7）

認定事業者は、認定された範囲について、別に定める「IAJapan 認定シンボルの使用及び認定の主張等に関する方針(URP15)」に規定する認定シンボル及びこの規程の図１の ILAC MRA 組み合わせ認定シンボルの使用及び認定要求事項に適合している旨の記載ができる。

認定事業者は、「IAJapan 認定シンボルの使用及び認定の主張等に関する方針(URP15)」に従い、報告書等への認定シンボルの使用及び認定の地位の主張の方法の管理方針を持たなければならない。また、広告物、パンフレット、その他の文書等において認定シンボルの使用及び／又は認定の地位の主張をする場合には、管理方針を持たなければならない。

6.7 苦情及び異議申立て

認定に係る苦情及び異議申立ては、「適合性評価機関の権利及び義務(UIF02)」に従い、苦情及び異議申立てができる。

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。

附　則
この規程は、平成19年10月15日から施行する。

附　則
この規程は、平成24年3月23日から施行する。ただし、本規程第3部に定める要求事項の適用は、JCMVPとCMVPとの共同認証に係る規定の適用日及びそれ以降とし、同適用日までは従前のとおり、すなわち、本規程第10版（TIRP21-10）第3部に定める要求事項を適用する。

附　則
この規程は、平成26年11月1日から施行する。

附　則
この規程は、平成28年1月1日から施行する。

附　則
この規程は、平成30年8月20日から施行する。

附　則
この規程は、2019年4月1日から施行する。
認定要求事項がISO/IEC 17025:2017の場合においては、本規程第15版を適用する。

附　則
この規程は、2019年4月1日から施行する。
ただし、本規程の施行日から2年間は、本規程第3部に定める要求事項を本規程第10版(TIRP21-10)第3部に定める要求事項に置き換えてもよいこととする。

附　則
この規程は、2021年1月1日から施行する。

附　則
この規程は、2024年6月26日から施行する。

附　則
この規程は、2025年1月16日から施行する。

附　則
この規程は、2025年mm月dd日から施行する。

参考：本規程第 3 部と NIST HB 150-17:2022 との項目対照表

ASNITE 試験事業者 IT 認定の一般要求事項 第 3 部	NIST HB 150-17:2022
3.2	4.1,5
3.3	4.2
3.5.1	6.2.7
3.5.3	6.2.2, 6.2.3
3.5.4	6.2.4
3.5.5	6.2.5
3.6.3	6.2.7
3.6.4	6.2.9
3.7.2 (3)	6.3.1
3.7.3	6.3.2
3.7.4	6.3.5
3.7.5	6.3.6
3.7.6	6.3.7.6
3.7.7	6.3.7.7
3.8.1	6.4.2 NOTE 1, NOTE 2
3.8.4	6.4.1
3.8.5	6.4.2
3.8.6	6.4.3
3.8.7	6.4.4
3.8.8	6.4.5
3.8.9	6.4.6
3.8.10	6.4.7
3.8.11	6.4.8
3.9.1	6.3.7.3,6.4.2 NOTE 2, 6.4.3 NOTE
3.9.2	6.5.2.1
3.10.2	6.5.1
3.10.4	6.5.3.4
3.11	6.6
3.12.1	7.1.1, 7.1.2
3.12.2	7.1.4
3.13	6.2.8, 6.3.7
3.14	7.2
3.15.1	7.4.1
3.15.4	7.4.3
3.16.1	7.5.1, 7.5.2
3.16.2	7.5.4
3.17.2	7.8.2.2
3.17.3	7.8.2.3
3.18.1	7.8.2.7
3.18.5	7.8.3.1
3.18.6	7.8.3.2, 7.8.3.3 NOTE 1, NOTE 2
3.18.7	7.8.4

ASNITE 試験事業者 IT 認定の一般要求事項 第 3 部	NIST HB 150-17:2022
3.19.1	8.4.1
3.19.2	8.4.2
3.19.3	8.4.3
3.19.4	8.4.4
3.19.5	8.4.5
3.20	8.8
3.21	8.9

改正ポイント

主な改正内容
◆「認定区分：情報技術－IoT製品のセキュリティ要件適合評価を行う事業者に対する一般要求事項」の追加に伴う修正

本規程第17版からの改正箇所には、下線を付しています。