

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14.1版)

平成~~30~~年~~8~~月~~20~~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

第 1 部 総則 .....	5
1.1 目的 .....	5
1.2 適用範囲 .....	5
1.3 引用規格等 .....	6
1.4 定義 .....	7
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	12
2.1 一般 .....	12
2.2 マネジメントシステムの対象範囲 (ISO/IEC 17025 4.1.3 項) .....	12
2.3 組織 (ISO/IEC 17025 4.1.4 項、4.1.5 b)項、4.1.5 d)項) .....	12
2.4 下請負契約 (ISO/IEC 17025 4.5.1 項、5.10.6 項) .....	13
2.5 技術的記録 (ISO/IEC 17025 4.13.2.1 項) .....	13
2.6 内部監査 (ISO/IEC 17025 4.14.1 項) .....	14
2.7 マネジメントレビュー (ISO/IEC 17025 4.15 項) .....	14
2.8 要員の適格性及び資格 (ISO/IEC 17025 4.1.5 h)項、5.2.1 項) .....	14
2.9 要員の教育・訓練 (ISO/IEC 17025 5.2.2 項) .....	15
2.10 要員の管理 (ISO/IEC 17025 5.2.3 項、5.2.4 項、5.2.5 項) .....	15
2.11 施設及び環境条件 (ISO/IEC 17025 4.1.5 c)項、5.3 項) .....	16
2.12 評価の方法 (ISO/IEC 17025 5.4.1 項) .....	17
2.13 規格外の方法 (ISO/IEC 17025 5.4.4 項) .....	17
2.14 方法の妥当性確認 (ISO/IEC 17025 5.4.5.2 項) .....	17
2.15 測定の不確かさの推定 (ISO/IEC 17025 5.4.6 項) .....	17
2.16 設備の保有及び設備の維持 (ISO/IEC 17025 5.5.1 項、5.5.2 項) .....	18
2.17 測定のトレーサビリティ (ISO/IEC 17025 5.6 項) .....	18
2.18 評価品目の取り扱い及び識別 (ISO/IEC 17025 5.8.2 項、5.8.4 項) .....	18
2.19 結果の報告に係る一般要求事項 (ISO/IEC 17025 5.10.1 項) .....	19
2.20 評価報告書 (ISO/IEC 17025 5.10.2 項、5.10.3 項、5.10.4 項) .....	19
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	20
3.1 一般 .....	20
3.2 マネジメントシステムの対象範囲 (ISO/IEC 17025 4.1.3 項) .....	20
3.3 組織 (ISO/IEC 17025 4.1.4 項、4.1.5 項、NIST HB 150-17 4.1 項) .....	21
3.4 マネジメントシステム (ISO/IEC 17025 4.2.1 項、NIST HB 150-17 4.2 項) .....	22
3.5 依頼、見積仕様書及び契約の内容の確認 (ISO/IEC 17025 4.4.1 項、4.4.2 項、4.4.3 項) .....	22
3.6 試験の下請負契約 (ISO/IEC 17025 4.5.1、NIST HB 150-17 4.5 項) .....	23
3.7 記録の管理 (ISO/IEC 17025 4.13.1 項、4.13.2 項) .....	23
3.8 内部監査 (ISO/IEC 17025 4.14.1 項、NIST HB 150-17 4.14 項) .....	25
3.9 マネジメントレビュー (ISO/IEC 17025 4.15.1 項、NIST HB 150-17 4.15 項) .....	25
3.10 要員の適格性及び資格 (ISO/IEC 17025 4.1.5 h)項、5.2.1 項、5.2.3 項) .....	25

3.11 要員の教育・訓練 (ISO/IEC 17025 5.2.2 項) .....	26
3.12 施設及び環境条件 (ISO/IEC 17025 4.1.5 c)項、5.3 項) .....	27
3.13 試験の方法 (ISO/IEC 17025 5.4.1 項) .....	29
3.14 規格外の方法 (ISO/IEC 17025 5.4.4 項) .....	29
3.15 方法の妥当性確認 (ISO/IEC 17025 5.4.5.2 項) .....	29
3.16 測定の不確かさの推定 (ISO/IEC 17025 5.4.6 項) .....	30
3.17 設備の保有 (ISO/IEC 17025 5.5.1 項) .....	30
3.18 設備の維持、校正 (ISO/IEC 17025 5.5.1 項、5.5.2 項、5.5.3 項) .....	30
3.19 測定のトレーサビリティ (ISO/IEC 17025 5.6 項) .....	31
3.20 試験品目の取り扱い及び識別 (ISO/IEC 17025 5.8.1 項) .....	33
3.21 試験品目の取り扱い及び保管 (ISO/IEC 17025 5.8.2 項、5.8.4 項) .....	33
3.22 結果の報告 (ISO/IEC 17025 5.10.1 項) .....	33
3.23 試験報告書 (ISO/IEC 17025 5.10.2 項、5.10.3 項) .....	34
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 .....	36
4.1 一般.....	36
4.2 マネジメントシステムの対象範囲 (ISO/IEC 17025 4.1.3 項) .....	36
4.3 内部監査 (ISO/IEC 17025 4.14.1 項) .....	36
4.4 要員の適格性及び資格 (ISO/IEC 17025 4.1.5 h)項、5.2.1 項) .....	36
4.5 要員の教育・訓練 (ISO/IEC 17025 5.2.2 項) .....	37
4.6 技術的記録 (ISO/IEC 17025 4.13.2.1 項) .....	38
4.7 施設及び環境条件 (ISO/IEC 17025 4.1.5 c)項、5.3 項) .....	38
4.8 テストの方法 (ISO/IEC 17025 5.4.1 項) .....	38
4.9 規格外の方法 (ISO/IEC 17025 5.4.4 項) .....	38
4.10 測定の不確かさの推定 (ISO/IEC 17025 5.4.6 項) .....	38
4.11 設備の保有 (ISO/IEC 17025 5.5.1 項) .....	38
4.12 設備の維持 (ISO/IEC 17025 5.5.2 項、5.5.3 項) .....	38
4.13 測定のトレーサビリティ (ISO/IEC 17025 5.6 項) .....	39
4.14 結果の報告に係る一般要求事項 (ISO/IEC 17025 5.10.1 項) .....	39
4.15 侵入テスト報告書 (ISO/IEC 17025 5.10.2 項、5.10.3 項) .....	39
第 5 部 雑則 .....	40
5.1 遵守事項.....	40
5.2 認定の申請に必要な手続き .....	40
5.3 技術的能力の定期的な確認.....	41
5.4 変更の届出 .....	41
5.5 認定に用いられる規格を用いた認証行為の禁止 (IAF-ILAC JGA2007 Sydney Resolution 7) .....	42
5.6 認定事業者の義務 (IAF-ILAC-A5:11/2013 M8.1.1 e) ) .....	42
5.7 事業の承継 .....	42

5.8 契約検査.....	43
5.9 事業の廃止.....	43
5.10 認定の一時停止.....	43
5.11 認定の取消し.....	44
5.12 認定シンボルの使用（ILAC-R7）.....	44
5.13 苦情及び異議申立て.....	49
附 則.....	49
附属書 1 マルチサイト事業者の認定に対する特定要求事項.....	51

## 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（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、又はシステム LSI 侵入テストを行う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 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。

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	ソフトウェア	JISEC（注1）における評価機関
		ハードウェア（スマートカード等）	
	暗号モジュール試験	暗号ソフトウェアモジュール	JCMVP（注2）における暗号モジュール試験機関
		暗号ハードウェアモジュール	
システムLSI侵入テスト			

（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ウェブ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>

**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)

### 1.3 引用規格等

この規程では、次に掲げる国際規格、日本工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工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 17025:2005 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 17011:2004 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)
- (4) ISO/IEC 15408-1 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model (技術情報 - セキュリティ技術 - 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 technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components (技術情報 - セキュリティ技法 - IT セキュリティの評価基準 - 第2部: セキュリティ機能成分)
- (6) ISO/IEC 15408-3 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components (技術情報 - セキュリティ技法 - IT セキュリティの評価基準 - 第3部: セキュリティ保証成分)
- (7) ISO/IEC 18045 Information Technology - Security Techniques - Methodology for IT Security Evaluation (情報技術 - セキュリティ技術 - IT セキュリティ評価の方法論)
- (8) ISO/IEC 19790:2006 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)
- (9) ISO/IEC 19790:2012(+Cor1:2015Corrected version 2015-12-15) Information technology - Security techniques - Security requirements for cryptographic modules (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)

- (10) ISO/IEC 24759:2008 Information technology - Security techniques - Test requirements for cryptographic modules (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)
- (11) ISO/IEC 24759:2017 Information technology - Security techniques - Test requirements for cryptographic modules (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)
- (12) IAJapan 測定のトレーサビリティに関する方針 (URP23)
- (13) IAJapan 技能試験に関する方針 (URP24)
- (14) [IAJapan 認定シンボルの使用及び認定の主張等に関する方針\(URP15\)](#)
- (15) [適合性評価機関の権利及び義務\(UIF02\)](#)
- (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) [IAF-ILAC A5 IAF/ILAC Multi-Lateral Mutual Recognition Arrangements \(Arrangements\): Application of ISO/IEC 17011:2004](#)
- (18) [ILAC-R7 Rules for the Use of the ILAC MRA Mark \(ILAC MRA マーク使用ルール\)](#)
- (19) IT セキュリティ評価機関承認申請手続等に関する要求事項規程 (CCM-03)
- (20) NIST HAND BOOK 150-17 National Voluntary Laboratory Accreditation Program Cryptographic and Security Testing (NIST HB 150-17)

(参考) NIST HB 150-17 の最新版は以下のウェブ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>

<http://www.nist.gov/nvlap/nvlap-est-lap.cfm><https://www.nist.gov/nvlap/cryptographic-and-security-lap>

#### 1.4 定義

- 1.4.1 ASNITE 試験事業者 IT : ASNITE において、1.4.6 の評価機関、1.4.7 の暗号モジュール試験機関及び 1.4.8 の侵入テスト実施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 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、1.4.9 で定める IT セキュリティ評価基準への適合性について、1.4.6 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、1.4.7 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実装試験の結果に対する確認を行う。
- 1.4.4 CMVP: Cryptographic Module Validation Program。CMVP は、NIST(National Institute of Standards and Technology) /ITL ( Information Technology Laboratory)

により策定された ~~NIST/ITL~~ と Communications Security Establishment of Canada (CSEC) / [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。

- 1.4.5 NVLAP: National Voluntary Laboratory Accreditation Program。米国において CMVP の承認試験機関となるためには NVLAP の認定が要される。ただし、JCMVP と CMVP との共同認証を希望する場合は ASNITE 認定又は NVLAP 認定のどちらかを取得していればよい。
- 1.4.6 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。
- 1.4.7 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。
- 1.4.8 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。
- 1.4.9 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う（以下「CC」というが、1.4.10 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
  - (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）当該文書は以下のウェブサイトにて入手することができる。
- URL: <https://www.ipa.go.jp/security/jisec/cc/index.html>
- 1.4.10 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。
- 1.4.11 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、1.4.12 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) 当該文書は以下のウェブサイトにて入手することができる。

URL: <https://www.ipa.go.jp/security/jisec/cc/index.html>

- 1.4.12 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。
- 1.4.13 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、以下のウェブサイトにて入手することができる。

URL:

~~<http://www.ipa.go.jp/security/certification/smartcard/index.html>~~[https://www.ipa.go.jp/security/jisec/hardware/cc\\_supporting\\_doc.html](https://www.ipa.go.jp/security/jisec/hardware/cc_supporting_doc.html)

- 1.4.14 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。
- 1.4.15 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) ~~CM 認証機関が公開する(1)と同等の文書~~  
~~(参考) 当該文書は以下のウェブサイトにて入手することができる。~~  
URL: <https://www.ipa.go.jp/security/jemvp/kitei.html>
  - (4) Federal Information Processing Standards(FIPS) 140-1 及びその後継版
- (参考) 当該文書は以下のウェブサイトにて入手することができる。
- URL: <http://csrc.nist.gov/groups/STM/cmvp/index.html>
- 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) ~~CM 認証機関が公開する(1)と同等の文書~~  
~~(参考) 当該文書は以下のウェブサイトにて入手することができる。~~  
~~URL: <https://www.ipa.go.jp/security/jemvp/kitei.html>~~
  - (4) FIPS 140-1 及びその後継版のための Derived Test Requirements(DTR)
- (参考) 当該文書は以下のウェブサイトにて入手することができる。
- URL: <http://csrc.nist.gov/groups/STM/cmvp/index.html>

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）当該文書は以下のウェブ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 付録で定められる FIPS 承認 / NIST 推奨のセキュリティ機能向けの暗号アルゴリズム実装確認試験

（参考）当該文書は以下のウェブサイトにて入手することができる。

URL: <http://csrc.nist.gov/groups/STM/cavp/index.html>

1.4.19 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）当該文書は以下のウェブ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 140-1 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）当該文書は以下のウェブサイトにて入手することができる。

<http://csrc.nist.gov/groups/STM/cmvp/index.html>

1.4.20 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。

1.4.21 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。

1.4.22 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

1.4.221.4.23 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 認定機関は、申請事業者及び評価機関（以下「評価機関等」という。）に対し、ISO/IEC 17025 を、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。
- 2.1.3 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。
- 2.1.4 評価機関等が、複数事業所をまとめて1つの認定対象組織として認定を取得しようとする場合又は維持する場合は、本文書附属書1に示す「マルチサイト事業者の認定に対する特定要求事項」に適合しなければならない。

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

評価機関等は、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。

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。これら以外の保証コンポーネントを追加する場合は個別に認定機関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

### **2.3 組織（ISO/IEC 17025 4.1.4項、4.1.5 b)項、4.1.5 d)項）**

評価機関等は、評価業務を実施する組織の独立性及び公平性を保つための方針及び手順をもたなければならない。この方針及び手順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。

#### **2.4 下請負契約（ISO/IEC 17025 4.5.1項、5.10.6項）**

評価機関は、認定を受けた範囲の中で、業務の一部を、下請負契約を結んだ他の事業者（以下「下請負契約者」という）に請け負わせることができる。この場合、評価機関等は、下請負契約者が評価基準（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、下請負契約者が ILAC-MRA、APLAC-MRA に署名する認定機関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、侵入テストを下請負契約者に請け負わせる場合は、評価機関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下請負契約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** 評価機関は、下請負契約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。）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) 下請負契約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、下請負契約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。

#### **2.5 技術的記録（ISO/IEC 17025 4.13.2.1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 アクションエレメント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。

評価機関等が内部で規定する技術的記録の保存期間は、申請者（Sponsor）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のが望ましい。

**注記** 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。

## **2.6 内部監査 (ISO/IEC 17025 4.14.1項)**

評価機関等の要員のうち1名のみがプログラム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

## **2.7 マネジメントレビュー (ISO/IEC 17025 4.15項)**

申請事業者は、初回現地審査の前に、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。

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

### **2.8.1 評価機関等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内部資格基準、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) 技術管理主体を構成する要員は、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。
- (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。

### **2.8.2 評価機関等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、2.8.1(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、担当する IT 製品等に対する深い知識を維持すること。IT 製品等の開発経験を有することが望ましい。

#### 2.8.3 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、2.2 に定めるすべての認定範囲を含まなければならない。

2.8.4 主要な要員（管理主体、評価要員はこれに含まれる）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、認定機関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、評価機関の認定地位に影響する可能性がある。

### 2.9 要員の教育・訓練（ISO/IEC 17025 5.2.2項）

2.9.1 評価機関等の管理主体は、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、評価機関等の業務に対して適切でなければならない。

2.9.2 前項の教育・訓練プログラムは、少なくとも 2.8.1 (3)1)から 4)の項目について行い、必要な場合には 2.8.1(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。

2.9.3 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。

### 2.10 要員の管理（ISO/IEC 17025 5.2.3項、5.2.4項、5.2.5項）

2.10.1 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。

2.10.2 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。

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

### 2.11.1 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、申請者 (Sponsor) の機密情報の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 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。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。
- 1) 評価機関等が、申請者 (Sponsor) 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、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。
  - 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。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) 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、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。

### 2.11.2 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。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。

### 2.12 評価の方法 (ISO/IEC 17025 5.4.1項)

2.12.1 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。

2.12.2 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。

### 2.13 規格外の方法 (ISO/IEC 17025 5.4.4項)

2.13.1 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。

2.13.2 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 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)

2.13.3 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。

### 2.14 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。

### 2.15 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。

## **2.16 設備の保有及び設備の維持 (ISO/IEC 17025 5.5.1項、5.5.2項)**

- 2.16.1 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文書化し、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。
- 2.16.2 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。

## **2.17 測定のトレーサビリティ (ISO/IEC 17025 5.6項)**

- 2.17.1 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計測トレーサビリティが要求される。計量計測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 測定の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 4.5 項に基づき評価業務又はその一部を下請負契約したとき、顧客の設備を用いたときも確保すること。
- 2.17.2 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、評価機関等の内部で文書化した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。
- 2.17.3 評価機関等は、保有する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、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。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。
- 2.17.4 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書面で合意をすること。
- 2.17.5 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。
- 2.17.6 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。

**注記** 評価機関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。

## **2.18 評価品目の取り扱い及び識別 (ISO/IEC 17025 5.8.2項、5.8.4項)**

- 2.18.1 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、不当に変更されたり、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に保護しなければならない。

- 2.18.2 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。

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

2.19.1 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、評価機関等が定めた様式であって、認定機関に届出したものを使用すること。

2.19.2 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。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。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。

2.19.3 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。

## **2.20 評価報告書 (ISO/IEC 17025 5.10.2項、5.10.3項、5.10.4項)**

2.20.1 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、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。 )。

2.20.2 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。

2.20.3 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、5.12.4(2)に定める規定に従うものとする。

2.20.4 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：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 認定機関は、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、ISO/IEC 17025 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 マネジメントシステムの対象範囲（ISO/IEC 17025 4.1.3項）**

暗号モジュール試験機関等は、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。

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(17BCS)、暗号アルゴリズム実装試験(17CAV)、暗号ソフトウェアモジュール試験 1（セキュリティレベル 1～3）
- (2) 基本暗号セキュリティ(17BCS)、暗号アルゴリズム実装試験(17CAV)、暗号ハードウェアモジュール試験 1（セキュリティレベル 1～3）
- (3) 基本暗号セキュリティ(17BCS)、暗号アルゴリズム実装試験(17CAV)、暗号ハードウェアモジュール試験 1（セキュリティレベル 1～3）、暗号ハードウェアモジュール試験 2（セキュリティレベル 4）
- (4) 基本暗号セキュリティ(17BCS)、暗号アルゴリズム実装試験(17CAV)、暗号ソフトウェアモジュール試験 1（セキュリティレベル 1～3）、暗号ハードウェアモジュール試験 1（セキュリティレベル 1～3）
- (5) 基本暗号セキュリティ(17BCS)、暗号アルゴリズム実装試験(17CAV)、暗号ソフトウェアモジュール試験 1（セキュリティレベル 1～3）、暗号ハードウェアモジュール試験 1（セキュリティレベル 1～3）、暗号ハードウェアモジュール試験 2（セキュリティレベル 4）
- (65) 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）
- (76) 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）
- (87) 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）
- (98) 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）

- | (109) 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)
- | (110) 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)
- | (124) 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)
- | (132) 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)
- | (143) 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)
- | (156) 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)
- | (164) 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)
- | (175) 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)
- | (186) 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)

**注記** 暗号モジュール試験区分内の認定の範囲において括弧内に示す略称は、NIST HANDBOOK 150-17 の区分 (Scope) に対応する。

### 3.3 組織 (ISO/IEC 17025 4.1.4項、4.1.5項、NIST HB 150-17 4.1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を実施する組織の独立性及び公平性を保つための方針及び手順をもたなければならない。この方針及び手順には以下を含むものとする。

- (1) 暗号モジュール試験機関等は、暗号モジュール試験機関等又は同機関等がより大きな組織の一部である場合にはその親組織に属する他の部門が、暗号アルゴリズム実装及び/又は暗号モジュールに関するコンサルタントサービス (開発試験、設計の助言等)

を現在行っているか過去に行ったことがある場合は、当該暗号アルゴリズム実装及び / 又は暗号モジュールに係る試験)を実施してはならない。ただし、暗号モジュール試験機関等は、試験要件及び関連文書の説明を目的としたコンサルタントサービスについてはこれを行うことができる。

- (2) 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て文書化し、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。
- (3) 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。
- (4) 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。
- (5) 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できる。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。

CMVP との共同認証に係る認定を希望する場合は、暗号モジュール試験機関等の組織に関する追加の指針、利害の衝突に関する追加の解釈及び説明、並びに利害の衝突を避けるための方策について CMVP が提供する指針も含めてこれを参照することができる。その場合これを文書化すること。

### **3.4 マネジメントシステム (ISO/IEC 17025 4.2.1項、NIST HB 150-17 4.2項)**

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、顧客の機密情報を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)及びその他の無許可の者からどのように保護するのが規定されなければならない。

### **3.5 依頼、見積仕様書及び契約の内容の確認 (ISO/IEC 17025 4.4.1項、4.4.2項、4.4.3項)**

3.5.1 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。(NIST HB 150-17 4.4.1)

**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 NAV LAP 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。

3.5.2 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 **秘密度機密性の格付け** 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。(NIST HB 150-17 4.4.2)

3.5.3 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書面にて合意しなければならない。本プログラムの場合、環境は以下のものを含むがこれらに限定されない。(NIST HB 150-17 4.4.3)

- a) 特定の試験実施環境
- b) 試験構成
- c) 外部環境

### 3.6 試験の下請負契約（ISO/IEC 17025 4.5.1、NIST HB 150-17 4.5項）

CMVP との共同認証を希望する場合は、以下が適用される。

3.6.1 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（下請負事業者）が利用される場合、当該下請負事業者は、NAV LAP 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 ハンドブック 150、NIST ハンドブック 150-17、及び CMVP 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下請負業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。

- a) この特定の下請事業者を選定した理由と、当該下請事業者が 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、
- b) かつ、当該下請事業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。

### 3.7 記録の管理（ISO/IEC 17025 4.13.1項、4.13.2項）

3.7.1 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。(NIST HB 150-17 4.13.1.1)

- 3.7.2 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**秘密度機密性の格付け**に相応するように保管されなければならない。アクセス権（閲覧を含む）は許可された職員のみが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。(NIST HB 150-17 4.13.1.2)
- 3.7.3 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。(NIST HB 150-17 4.13.1.3)
- 3.7.4 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**機密性の格付け度**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。(NIST HB 150-17 4.13.1.4)
- 3.7.5 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。(NIST HB 150-17 4.13.1.5)
- 3.7.6 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書面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。(NIST HB 150-17 4.13.2.1)
- 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。
- 3.7.7 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。(NIST HB 150-17 4.13.2.2)
- 3.7.8 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

### 3.8 内部監査（ISO/IEC 17025 4.14.1項、NIST HB 150-17 4.14項）

暗号モジュール試験機関等の要員のうち 1 名のみがプログラム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。

- a) 文書化及び指示に係るレビュー
- b) 手続及び指示の遵守状況の確認
- c) 監査所見の文書化

### 3.9 マネジメントレビュー（ISO/IEC 17025 4.15.1項、NIST HB 150-17 4.15項）

申請事業者は、初回現地審査の前に、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。

### 3.10 要員の適格性及び資格（ISO/IEC 17025 4.1.5 h)項、5.2.1項、5.2.3項）

#### 3.10.1 暗号モジュール試験機関等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。

#### 3.10.2 暗号モジュール試験機関等の要員の適格性及び資格

- (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要員を確保すること。なお、CMVP との共同認証に係る認定を希望する場合は、各プログラムに係る要員に必要とされる専門知識の詳細については、NIST HB 150-17 附属書 B を参照のこと。（NIST HB 150-17 5.2.6）
- (2) 試験要員は、試験業務に係る内部資格を有すること。
- (3) 試験要員は、以下に定める知識を有し、その内部資格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**
  - 34) 暗号モジュール試験要件に係る知識
  - 45) 暗号アルゴリズム**実装**試験要件に係る知識
  - 56) 運用ガイダンスに係る知識

(4) CMVP との共同認証に係る認定を希望する場合には、上記(1)ないし(3)に加え以下が適用される。(NIST HB 150-17 5.2.1)

- a) 認定範囲の FIPS、NIST SP (Special Publications) 及び NIST HANDBOOK150-17 と NVLAP が CMVP に関して公表する情報について熟知している。
- b) 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。
- c) 暗号セキュリティ試験ツールに精通している。
- d) 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。

3.10.3 主要な要員（管理主体、試験要員はこれに含まれる）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、認定機関及び CM 認証機関に書面で報告しなければならない。(NIST HB 150-17 5.2.3)

**注記** 契約による要員に上述のような変更がある場合、暗号モジュール試験機関等の認定地位に影響する可能性がある。

3.10.4 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。ただし、暗号モジュール試験機関等の長及び品質管理者の職位には、専任の職員を配置することが望ましい。(NIST HB 150-17 5.2.4)

3.10.5 品質管理者は、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。(NIST HB 150-17 5.2.5)

### **3.11 要員の教育・訓練（ISO/IEC 17025 5.2.2項）**

3.11.1 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。

3.11.2 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。

3.11.3 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。(NIST HB 150-17 5.2.7)

- a) 試験報告書の作成を含む試験方法に係る一般要件
- b) システムセキュリティの概念
- c) 物理的セキュリティ
- d) 識別及び認証技術及び技法
- e) 暗号及びセキュリティ用語への習熟

- f) 標準準拠
- g) CM 認証機関から貸与された試験ツールの操作及び維持
- h) インターネット及びインターネット関連ソフトウェアへの習熟、及び所定の Web サイトから参考資料及び情報を探して確実にダウンロードする能力
- i) 上記に加え、CMVP との共同認証に係る認定を希望する場合は、以下に係る知見を有するか事前の教育訓練を確実にしなければならない。
- j) 上記に加え、CMVP との共同認証に係る認定を希望する場合は、以下に係る知見を有するか事前の教育訓練を確実にしなければならない。
- k) NVLAP / 評価プログラムで義務づけられた試験ツールの運用及び保守  
暗号モジュール試験機関等は、CMVP との共同認証に係る認定を希望する場合は、認定範囲に係る特定の教育訓練要件について、NIST HB150-17 附属書 B を参照してその要員向けの適切な教育訓練を実施することを確実にしなければならない。

3.11.4 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。(NIST HB 150-17 5.2.8)

3.11.5 最新の認定審査又は検査に参加した暗号モジュール試験機関要員の 60%以上が当該暗号モジュール試験機関等を離職した場合、暗号モジュール試験機関等は認定機関に通知しなければならない。これは、認定に係る不適合事項に該当するため、暗号モジュール試験機関等は、是正処置及び予防処置を講じて、不適合に対処しなければならない。認定機関は、必要な場合、臨時検査を実施することがある。(NIST HB 150-17 5.2.9)

### **3.12 施設及び環境条件 (ISO/IEC 17025 4.1.5 c)項、5.3項)**

#### **3.12.1 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) 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** 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であること。
- (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) 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。
  - (4) 申請事業者及び試験機関は、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。
  - (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。
- 3.12.2 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) 3.12.1(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など）で暗号モジュール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。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。(NIST HB 150-17 5.3.1)

- 3.12.3 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。(NIST HB 150-17 5.3.2)
- 3.12.4 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。(NIST HB 150-17 5.3.5)

### 3.13 試験の方法 (ISO/IEC 17025 5.4.1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 5.3 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。(NIST HB 150-17 5.3.6、5.4.1)
- 3.13.4 CMVP との共同認証に係る認定を希望する場合は、暗号モジュール試験方法の選択に係る詳細情報について、NIST HB 150-17 附属書 B を参照すること。(NIST HB 150-17 5.3.7)

### 3.14 規格外の方法 (ISO/IEC 17025 5.4.4項)

- 3.14.1 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。
- 3.14.2 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。
- 3.14.3 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においては適用しない。

### 3.15 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、暗号モジュール試験においては適用しない。

### 3.16 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。

### 3.17 設備の保有 (ISO/IEC 17025 5.5.1項)

3.17.1 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保有し、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。なお、CMVP との共同認証に係る認定を希望する場合は、NIST HB 150-17 附属書 B を参照のこと。(NIST HB 150-17 5.5.4)

3.17.2 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 5.4.7 項に適合することを確保しなければならない。

3.17.3 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 5.5 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。

### 3.18 設備の維持、校正 (ISO/IEC 17025 5.5.1項、5.5.2項、5.5.3項)

3.18.1 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。(NIST HB 150-17 5.5.1)

- (1) CM 認証機関から貸与されたツールにあつては、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、申請事業者及び試験機関が文書化した手順。

3.18.2 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。なお、CMVP との共同認証に係る認定を希望する場合は、各試験に必要な試験ツールのリストは NIST HB 150-17 附属書 B を参照のこと。(NIST HB 150-17 5.5.3)

3.18.3 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なければならない。整合性が維持されていることを確実に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。(NIST HB 150-17 5.5.5)

3.18.4 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ない。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。(NIST HB 150-17 5.5.6)

3.18.5 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。(NIST HB 150-17 5.5.7)

3.18.6 暗号モジュール試験機関等は、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。

**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。

3.18.7 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。(NIST HB 150-17 5.5.8)

- a) 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
- b) 版数管理システム。

3.18.8 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。(NIST HB 150-17 5.5.9)

3.18.9 CMVP との共同認証に係る認定を希望する場合は、3.18 に規定する事項以外に要求される方法に特異な要求事項について NIST HB 150-17 附属書 B を参照のこと。(NIST HB 150-17 5.5.10)

### **3.19 測定のトレーサビリティ (ISO/IEC 17025 5.6項)**

3.19.1 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、計量計測トレーサビリティが要求される。計量計測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 測定の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 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、3.17.3 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。

- 3.19.2 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。
- 3.19.3 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ない。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 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**実装**試験要件をいう。（NIST HB 150-17 5.6.1.1）
- 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。
- 3.19.4 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するための検査をしなければならない。（NIST HB 150-17 5.6.2.1.1）
- 3.19.5 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。（NIST HB 150-17 5.6.2.1.2）
- 3.19.6 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。（NIST HB 150-17 5.6.2.2.1）
- 3.19.7 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 附属書 B で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。（NIST HB 150-17 5.6.2.2.2）
- 3.19.8 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、現地審査時の検査において使用できなければならない。（NIST HB 150-17 5.6.2.2.3）
- 3.19.9 暗号モジュール試験機関等は、CMVP との共同認証に係る認定を希望する場合は、



該当する特定の方法に関する NIST HB 150-17 附属書 B で説明する試験方法を用いるものとする。技術的な理由から例外が必要とみなされる場合、顧客及び CM 認証機関にその旨を通知し、試験報告書に詳細を記述する。試験方法に対して行われる例外については文書化を行い、プログラム固有の試験方法に関する正確かつ必要な精度と解釈を維持する。必要に応じて、CM 認証機関はこの報告書を使用して、試験方法とその関連文書を更新できる。試験方法の確認は、関係するプログラム固有の要件の仕様、関係するすべての規格、及び必要に応じて前回検証した試験方法と一致する結果が生成されることを、できる限り確認する工程である。(NIST HB 150-17 5.6.3.1)

- 3.19.10 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ん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。(NIST HB 150-17 5.6.3.2)

### 3.20 試験品目の取り扱い及び識別 (ISO/IEC 17025 5.8.1項)

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。(NIST HB 150-17 5.8.1)

### 3.21 試験品目の取り扱い及び保管 (ISO/IEC 17025 5.8.2項、5.8.4項)

- 3.21.1 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。

- 3.21.2 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。

- 3.21.3 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。(NIST HB 150-17 5.8.2)

### 3.22 結果の報告 (ISO/IEC 17025 5.10.1項)

- 3.22.1 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、認定機関に届け出たものを使用すること。

- 3.22.2 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。(NIST HB 150-17 5.10.1)

3.22.3 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。

### **3.23 試験報告書 (ISO/IEC 17025 5.10.2項、5.10.3項)**

3.23.1 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。(NIST HB 150-17 5.10.2.5)

3.23.2 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、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。 )。

3.23.3 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。

3.23.4 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、[5.121.4\(2\)](#)に定める規定に従うものとする。

3.23.5 暗号モジュール試験機関等は、CM 認証機関の指示に従い、電子文書での報告書を提出することができる。電子文書での報告書は紙による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。(NIST HB 150-17 5.10.3.1)

3.23.6 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。(NIST HB 150-17 5.10.3.2)

3.23.7 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ない、その際、例えば「文書発行番号 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。(NIST HB 150-17 5.10.4.1)

3.23.8 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 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 認定機関は、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）のための要求事項として適用する。
- 4.1.2 認定機関は、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。
- 4.1.3 侵入テスト実施機関等が、複数事業所をまとめて1つの認定対象組織として認定を取得しようとする場合又は維持する場合は、本文書附属書1に示す「マルチサイト事業者の認定に対する特定要求事項」に適合しなければならない。

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

侵入テスト実施機関等は、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、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 評価機関と下請負契約を締結し、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 内部監査（ISO/IEC 17025 4.14.1項）**

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

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

#### **4.4.1 侵入テスト実施機関等の技術管理主体の適格性**

- (1) 技術管理主体は、侵入テスト業務の技術的事項の全責任を負う。
- (2) 技術管理主体は、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) 技術管理主体は、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
- (4) 技術管理主体を構成する要員は、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。

#### 4.4.2 侵入テスト実施機関等の要員の適格性及び資格

- (1) 要員は、同テスト業務に係る内部資格を有すること。
- (2) 要員は、4.4.1(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) 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) 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スキルを有すること。
  - 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

#### 4.4.3 主要な要員（管理主体及び要員はこれに含まれる）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、認定機関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。

### 4.5 要員の教育・訓練（ISO/IEC 17025 5.2.2項）

- 4.5.1 侵入テスト実施機関等の管理主体は、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。
- 4.5.2 前項の教育・訓練プログラムは、少なくとも 4.4.1(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。
- 4.5.3 侵入テスト実施機関等は、内部資格を有する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、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。

#### 4.6 技術的記録 (ISO/IEC 17025 4.13.2.1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。

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

2.11 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。

#### 4.8 テストの方法 (ISO/IEC 17025 5.4.1項)

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 規格外の方法 (ISO/IEC 17025 5.4.4項)

4.9.1 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。

4.9.2 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 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、侵入テスト実施機関等が、保有する参照標準等を用いて内部校正を行う場合を除き適用しない。内部校正を行う場合は ISO/IEC 17025 5.4.6.1 項が適用される。

#### 4.11 設備の保有 (ISO/IEC 17025 5.5.1項)

3.17 項に準ずる。ただし、CMVP との共同認証に係る事項を除く。

#### 4.12 設備の維持 (ISO/IEC 17025 5.5.2項、5.5.3項)

3.18.1、3.18.6、3.18.7、3.18.8 項に準ずる。

#### **4.13 測定のトレーサビリティ (ISO/IEC 17025 5.6項)**

- 4.13.1 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。計量計測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 測定のトレーサビリティ方針 (URP23)」に従うこと。
- 4.13.2 侵入テストにおいて、ISO/IEC 17025 5.6.2.1 項は適用しない。

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

- 4.14.1 侵入テストにおいて、ISO/IEC 17025 5.10.1 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、認定機関に届出したものを使用すること。
- 4.14.2 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。
- 4.14.3 認定範囲外の侵入テストの結果を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。

#### **4.15 侵入テスト報告書 (ISO/IEC 17025 5.10.2項、5.10.3項)**

- 4.15.1 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、認定機関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署名又は捺印すること。また、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 (ISO/IEC 17025 4.1.5 項 注記を参照のこと。 )。
- 4.15.2 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。
- 4.15.3 侵入テストにおいて、ISO/IEC 17025 5.10.4 項は適用しない。

## 第5部 雑則

### 5.1 遵守事項

5.1.1 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 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。

5.1.2 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。

### 5.2 認定の申請に必要な手続き

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ある場合は、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ある場合は、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ある場合は、認定機関に認定申請書訂正願を提出すること。

### 5.3 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 技能試験に関する方針 (URP024) 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
    - 2.8.3 に定める試行評価
  - 2) 暗号モジュール試験機関
 

CM 認証機関又は NVLAP 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
- (2) 認定事業者
  - 1) コモンクライテリア評価
 

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
  - 2) 暗号モジュール試験
 

以下のうち 1 つ以上の技能試験に参加すること。

    - a) 認定審査及び検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) 認定審査及び検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) 認定審査及び検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) 認定審査及び検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。

### 5.4 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) 認定を受けた範囲のうち、区分内の製品分野又は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。

#### **5.5 認定に用いられる規格を用いた認証行為の禁止（IAF-ILAC JGA2007 Sydney Resolution 7）**

申請事業者及び認定事業者は、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。下請負事業者が 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、下請事業者に対して文書を発行する場合、この文書は下請負の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。

#### **5.6 認定事業者の義務（IAF-ILAC-A5:11/2013 M8.1.1 e）**

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、認定機関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認定機関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。

#### **5.7 事業の承継**

- 5.7.1 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。
- 5.7.2 前項の場合には、認定事業者の地位を承継した者は、5.4 の変更の届出のほか、次の手続きを行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。

## 5.8 契約検査

5.8.1 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。

5.8.2 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

5.8.3 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 年以内実施する。

5.8.4 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、認定機関のトップマネジメント、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、暗号モジュール試験、若しくは脆弱性試験の品質に関して著しい疑義を呈している場合
- (2) 認定範囲の変更、技術管理主体の変更、評価者の退職、事業所の移転又は試験施設・設備の移転・変更等、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

## 5.9 事業の廃止

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。

## 5.10 認定の一時停止

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。
- (3) 認定の地位の表明又は認定シンボルの使用に当たって、認定機関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。

### 5.11 認定の取消し

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) 5.8 項で定める契約検査又は 5.3 項で定める技能試験等を受けなかった場合
- (2) 5.8 項で定める契約検査又は 5.3 項で定める技能試験等の費用を負担しなかった場合
- (3) 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。）
- (4) 契約検査、技能試験等の結果、技術的能力がないと判明した場合
- (5) 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
- (6) 契約検査などにおいて、過去の契約検査など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
- (7) 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

### 5.12 認定シンボルの使用に係る要求事項 (ILAC-R7:05/2015)

#### 5.12.1 認定の主張について

認定事業者は、認定された範囲について、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。ILAC MRA 組み合わせ認定シンボルを使用する場合は、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。

#### 5.12.2 ILAC MRA 組み合わせ認定シンボルを使用しない認定の主張について

認定事業者は、ILAC MRA 組み合わせ認定シンボルを使用せずに認定の地位を主張する場合は、「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)」に掲げる事項、及び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てはならない。
- (2) 認定事業者は、下請負事業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なければならない。

#### 5.12.3 試験報告書等の書式

認定機関は、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、以下に掲げる要求事項を適用する。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。~~

~~—定義~~

~~認定シンボル~~

~~ここでは、ILAC R7:05/2015 で規定されている「認定 CAB 複合 ILAC MRA マーク」を指す。ILAC MRA 署名機関によって認定された適合性評価機関（CAB：Conformity Assessment Body）が用いる。~~

~~—方針~~

~~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。~~

~~認定事業者は、評価報告書又は試験報告書への認定シンボルの付記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シンボルの使用及び認定の引用方法について管理方針を持たなければならない。~~

~~認定事業者は、認定証の発行後に認定機関から提供される認定シンボルの清刷（画像データ）を適切に管理し、清刷を元に認定事業者が使用する認定シンボルを複製（全体サイズの変更は可能、比率の変更は不可）、管理しなければならない。~~

~~認定事業者は、印刷物の作成等のため業者等に認定機関が提供した清刷の複製を提供した場合、提供を受けた業者等が、認定事業者と同様に清刷を適切に管理することを確保しなければならない。~~

~~認定事業者は、自身の顧客に対して、認定シンボルを顧客の製品、広告物等に使用してはならないことを徹底しなければならない。~~

~~認定事業者は、認定シンボル（5.12.3のもの）の使用に当たっては、あらかじめ「ASNITE 試験事業者 IT 認定の一般要求事項の遵守について」を認定機関に提出しなければならない。~~

~~この要求事項に規定する場合を除き、何人も認定シンボル又はこれと紛らわしい標章類などを使用してはならない。~~

~~—認定シンボル~~

~~認定シンボルのひな形は、図1のとおり、また比率は図2のとおりとする。~~

~~認定シンボルの清刷（画像データ）は、認定後、認定機関から認定事業者に提供される。~~

~~認定シンボルの複製は清刷を元とし、他の文書等にある認定シンボルのコピーを使用してはならない。~~

~~認定シンボルは、認定機関が提供した一体の状態で使用しなければならない。また、分解、組み替え等を行って使用してはならない。~~

~~認定シンボルは、通常の水平方向で使用し、回転させてはならない。~~

~~認定シンボルを縮小又は拡大して表示する場合は、与えられた清刷の縦横比を維持し、これを変更してはならない。~~

~~清刷は、解像度を低めるなど、認定機関が提供した状態よりも画像を劣化させる改変を行ってはならない。~~

~~認定シンボルは、ILAC-MRA の文字、IAJapan の文字及び認定番号は読み取れる大きさ以上とし、認定シンボルが識別できないような背景で使用してはならない。~~

~~認定シンボルの色は、原則として、認定機関が清刷により指定する色とするが、シンボル全体同一色（黒）を用いることも可能とする。~~



~~0000：認定番号、XX：付加情報（試験事業者の場合は「T」）~~  
~~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 認定事業者が評価報告書又は試験報告書に表示できる認定シンボル~~

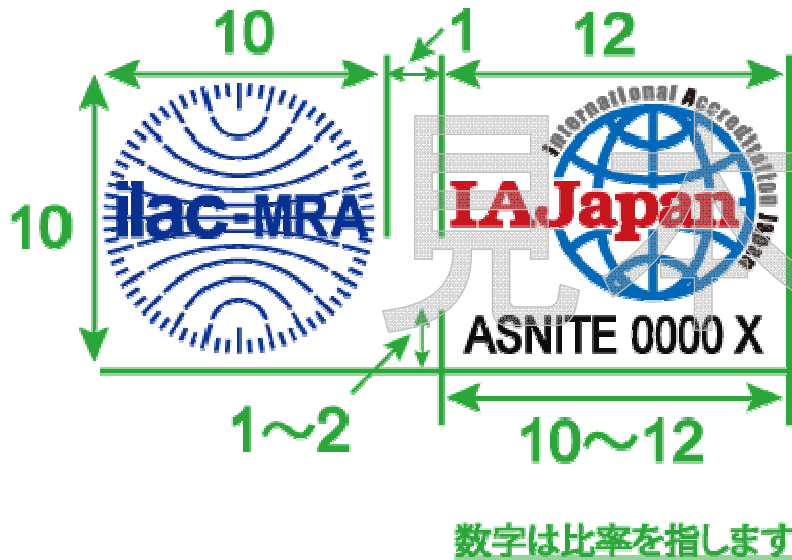


図2—認定事業者が評価報告書又は試験報告書に表示できる認定シンボルの比率

—認定シンボルの使用に係る運用  
報告書の書式

認定事業者は、ILAC MRA 組み合わせ認定シンボル付きの評価報告書又は試験報告書等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。

5.12.15.12.4 報告書の複写

認定事業者は、評価報告書又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。

5.12.2—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。
- (1) 認定事業者は、以下の条件を満たす場合に限り、カタログ、レターヘッド、各



~~刺—その他の宣伝文書に、5.12.3 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。~~

~~1) 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。~~

~~2) 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、5.12.3 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-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-XXXXは、当社セキュリティセンターの認定番号です。~~

#### 5.12.3—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。~~

#### 5.12.4—第三者による認定シンボルの不正使用

~~認定事業者は、第三者によって認定シンボルが不正に使用された場合は、認定機関と密に連絡し、そのような第三者に対し取られるすべての処置について協力しなければならない。また、認定事業者が法的処置を起こすことを決めた場合は、認定機関に書面による承認を得なければならない。~~

#### 5.12.5—第三者からの苦情

~~認定事業者は、第三者からの認定シンボルに対するすべての苦情について、即座に認定機関に報告しなければならない。また、認定事業者が法的処置をとるための承認は、認定事業者が認定機関に書面で要求しなければならない。さらに、この通告はその後のいかなる法的処置においても認定機関が参加する機会を与えるものとする。~~

#### 5.12.6—認定シンボルの不正使用による是正処置等

~~認定機関は、認定事業者による認定シンボルの不正使用が発覚した場合、それが同事~~



~~業者の故意によるものである場合は認定の取消し、認定シンボルの使用取消し措置を講じる。また、不正使用が同事業者の過失によるものである場合には、認定シンボルの使用を一時停止するとともに書面により是正処置を要求する。是正処置が要求された認定事業者は、可及的速やかに認定シンボルの使用を一時停止し、また、認定シンボルの使用再開のため必要な是正報告又は是正計画を定められた期限までに認定機関に提出しなければならない。是正報告又は是正計画が提出されない場合、認定機関は、認定シンボルの使用を取り消すとともに、認定の一時停止、取消しの措置に係る手続きを開始する。~~

### 5.13 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おり、すなわち、本規程第~~10-1-0~~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、平成 年 月 日から施行する。

認定要求事項がISO/IEC17025:2017の場合においては、本規程第15-1-5版を適用する。

## 附属書 1 マルチサイト事業者の認定に対する特定要求事項

### 1. 目的・適用範囲

この附属書は、複数事業所をまとめて、1つの認定対象組織として認定を取得しようとする場合又は維持する場合の要求事項を規定する。

### 2. 用語

この附属書で用いる用語の定義は次のとおりとする。

#### 2.1 マルチサイト事業者：一つ又は複数の主要な活動を複数の事業所で分担して実施する事業者

**注記** 試験活動の主要な活動には、試験報告書の発行、方針の作成、プロセス及び/又は手順の開発、契約内容の確認、適合性評価の計画、適合性評価の結果のレビュー、承認及び決定が含まれる。

**例** ひとつの事業所でプラスチック中の重金属類の化学分析試験を実施し、それ以外の事業所でプラスチックの物性試験を実施する。

**例** ひとつの事業所で機器分析を実施し、それ以外の事業所でサンプリングを実施する。

#### 2.2 主たる事業所：マルチサイト事業者のマネジメントシステムを管理し、品質管理者をおく事業所。

### 3. マルチサイト事業者認定の要求事項

#### 3.1 一般

##### 3.1.1 申請単位は、1法人とすること。

#### 3.2 マネジメントシステム

##### 3.2.1 全ての事業所において、ひとつのマネジメントシステムにより運用すること。

##### 3.2.2 マネジメントシステム文書には、事業所毎の業務範囲、内容、要員（どの事業所で、誰が、何をするのか）を明確に規定すること。

なお、事業所間で相互に作用する活動（データやサンプルの受け渡し、機器や要員の移動等）が行われる場合は、その手順をマネジメントシステム文書に明確に規定すること。

#### 3.3 記録の管理

##### 3.3.1 全ての記録は、ひとつのマネジメントシステムの下で、文書化された手順に従って管理すること。

#### 3.4 内部監査及びマネジメントレビュー

##### 3.4.1 内部監査及びマネジメントレビューは、全ての事業所を対象に実施すること。

#### 3.5 試験結果の品質の保証

##### 3.5.1 技能試験については、試験を行う全ての事業所は、この文書の 5.3 で定める要求事項に基づく技能試験に参加すること。

#### 3.6 結果の報告

##### 3.6.1 試験報告書には、試験活動を行った全ての事業所とその所在地を記載すること。

#### 3.7 初回審査・契約検査

3.7.1 初回審査及び契約検査（全項目検査）は、主要な活動を行っている全ての事業所で審査・検査の訪問を受け入れること。

3.7.2 初回認定後 1 年以内の契約検査（部分検査）は、主たる事業所で検査の訪問を受け入れること。

改正ポイント

主な改正内容

ISO/IEC17011:2017適用のための改正  
その他、字句修正

改正か所には、下線を付しています。