サポート文書
必須技術文書

ネットワークデバイス cPP の
評価アクティビティ

2015 年 2 月

バージョン 1.0

CCDB-2015-01-001

平成 28 年 1 月 15 日　翻訳 暫定第 0.2 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

序文

本書は、コモンクライテリアバージョン 3 及び関連する情報技術セキュリティ評価のための共通評価方法を補足することを意図した、サポート文書である。

サポート文書は、サポート文書の適用が相互承認上必須でない分野に対する具体的なやり方と規格の適用に注目した、それ自体が規格としての性質を持たない「ガイダンス文書」であってもよいし、またはサポート文書の適用範囲によりカバーされる評価において、その適用が必須とされるような「必須技術文書」であってもよい。後者の利用法は必須であるだけでなく、それらの適用の結果として発行される認証書は CCRA の下で承認される。

本サポート文書は、Network International Technical Community (NDFW-iTC) により開発されたものであり、またセクション 1.1 で識別される cPP に適合する製品の評価をサポートするために使用されるよう設計されている。

テクニカルエディタ：Network International Technical Community (NDFW-iTC)

文書履歴：

V1.0, 2015 年 2 月 27 日 (公開バージョン)

V0.4, 2015 年 1 月 26 日 (CCDB レビューから受け取ったコメントによる変更を取り込み)

V0.3, 2014 年 10 月 17 日 (公開レビュー後にリリースされたバージョン、CCDB レビュー用に提出)

V0.2, 2014 年 10 月 13 日 (公開レビューコメントに対応した内部ドラフト、iTC レビュー用)

V0.1, 2014 年 9 月 5 日 (公開レビューのための初期リリース)

一般的な目的：セクション 1.1 を参照されたい。

特定用途分野：本サポート文書は、ネットワークデバイスのコラボラティブプロテクションプロファイル [NDcPP] 及びステートフルトラフィックフィルタファイアウォールのコラボラティブプロテクションプロファイル [FWcPP] に適合を主張する TOE の評価に適用される。

謝辞：

本サポート文書は、産業界、政府機関、コモンクライテリア評価機関、及び学術会員からの代表者の参加する、Network international Technical Community によって開発された。

目次

表の目次

1 序説

1.1 サポート文書の技術分野と適用範囲

1 本サポート文書は、ネットワークデバイスのコラボラティブプロテクションプロファイル [NDcPP] に関連する評価アクティビティを定義する。

2 ネットワークデバイス技術分野には、プロトコルのセキュアな実装及び利用に関するもの、さまざまな種別の基盤となるデバイスの幅広い物理及び論理インタフェースにわたってリモート管理機能が評価される必要のある具体的な方法に関するものなど、数多くの特化した側面が存在する。この特化の程度、及び cPP の個別の SFR 間の関連のため、汎用の CEM アクティビティに見られるものよりも具体的な解釈が評価アクティビティに与えられることが、効率性及び有効性の両面から重要となる。

3 本サポート文書は、以下の 1 つまたは複数の cPP への適合を主張する製品の評価には必須となる：

a) ネットワークデバイスのコラボラティブプロテクションプロファイル [NDcPP]

b) ステートフルトラフィックフィルタファイアウォールのコラボラティブプロテクションプロファイル [FWcPP]。

4 評価アクティビティは、主に評価者が従うものとして定義されるが、本サポート文書における定義は、開発者、評価者及び利用者に対して、関連する cPP への適合評価において TOE のどの側面がテストされるのか、またどの程度深くテストが行われるかについての、共通の理解を提供することを目的としている。この共通の理解は、さらに、cPP への適合評価が、比較可能で、透明性のある、再現可能な結果が得られることを保証するという目標に寄与する。一般的に、評価アクティビティの定義は、開発者が、その TOE の具体的な要件を識別することにより、評価の準備をするためにも役立つことになる。評価アクティビティにおける具体的な要件は、場合によっては SFR の意味を明確化し、またセキュリティターゲット (特に TOE 要約仕様)、利用者ガイダンス文書、及び想定される補足情報 (例、エントロピー分析、または暗号鍵管理アーキテクチャ等—セクション 4 を参照されたい) の内容の具体的な要件を識別するかもしれない。

1.2 文書の構成

5 評価アクティビティは、セキュリティ機能要件とセキュリティ保証要件の両方について定義することができる。これらは、本サポート文書の別々のセクションで定義されている。

6 任意の評価アクティビティが評価中に成功裏に完了できなかった場合、その評価の総合判定は「不合格」となる。まれな場合には、評価アクティビティが修正され、または特定の TOE には適用できないとみなされ得る受け入れ可能な理由が存在するかもしれないが、このような場合には、その評価に関して認証機関と合意がなされなければならない。

7 一般的には、すべての評価アクティビティ (SFR と SAR の両方について) が評価中に成功裏に完了した場合、その評価の総合判定は「合格」となる。評価ア

クティビティが成功裏に完了した時に「不合格」の判定となるためには、その TOE について評価アクティビティがなぜ不十分であるかの理由について評価者からの具体的な正当化が必要とされる。

8 同様に、より粒度の細かい保証コンポーネントのレベルでは、ある保証コンポーネントに関する評価アクティビティ及びそれに関連する SFR の評価アクティビティのすべてが評価中に成功裏に完了した場合には、その評価コンポーネントの判定が「合格」となることが期待されるであろう。これらの評価アクティビティが成功裏に完了した際にその評価コンポーネントについて「不合格」の判定となるためには、その TOE について評価アクティビティが不十分であるかの理由について評価者からの具体的な正当化が必要とされる。

1.3 用語

9 標準的な CC 用語の定義については、 [CC] パート 1 を参照されたい。

10 **cPP—**コラボラティブプロテクションプロファイル

11 **CVE—**Common Vulnerabilities and Exposures (データベース)

12 **iTC—**International Technical Community

13 **SD—**サポート文書

14 **補足情報—**セキュリティターゲットまたはガイダンス文書に必ずしも含まれず、また必ずしも公開されないかもしれない情報。そのような情報の例としては、エントロピー分析、あるいは TOE で (またはそのサポートにおいて) 使用される暗号鍵管理アーキテクチャについての記述であろう。そのような補足情報に関する要件は、関連する cPP で識別される (セクション 4 の記述を参照されたい)。

2 SFR の評価アクティビティ

2.1 セキュリティ監査 (FAU)

2.1.1 FAU_GEN.1 監査データ生成

2.1.1.1 ガイダンス文書

15 評価者は、ガイダンス文書をチェックして、すべての監査対象事象が列挙されており、また監査記録のフォーマットが提供されていることを保証しなければならない。監査記録のフォーマット種別のそれぞれが、各フィールドの簡潔な記述とともに、カバーされなければならない。評価者は、cPP によって義務づけられるすべての監査事象種別が記述され、またフィールドの記述には FAU_GEN1.2 に要求される情報と、監査事象の表に特定される追加的情報が含まれることをチェックして確認しなければならない。

16 また評価者は、cPP の文脈において関連する管理アクションの判断を行わなければならない。評価者はガイダンス文書を検査して、サブコマンド、スクリプト、及び設定ファイルを含む、どの管理コマンドが、cPP に特定される要件を実施するために必要な TOE に実装されるメカニズムの設定 (有効化及び無効化を含む) に関連しているのか判断を行わなければならない。評価者は、cPP に関して管理ガイドのどのアクションがセキュリティ関連なのかを判断する際に採用した方法論またはやり方を文書化しなければならない。評価者はこのアクティビティを、対応するガイダンス文書がそれに関連する要件を満たしていることを保証することと関連付けられたアクティビティの一部として行ってもよい。

2.1.1.2 テスト

17 評価者は、管理事象の表に列挙された事象と、上に列挙された管理アクションに関して TOE に監査記録を生成させることによって、正しく監査記録を生成する TOE の能力をテストしなければならない。これには、事象のすべてのインスタンスが含まれるべきである : 例えば、システムにいくつかの異なる I&A メカニズムが存在する場合、各メカニズムについて FIA_UIA_EXT.1 事象が生成されなければならない。評価者は、ST に含まれる暗号プロトコルのそれぞれについて、チャネルの確立と終了に関して監査記録が生成されることをテストしなければならない。HTTPS が実装される場合、TLS セションの確立と終了を実証するテストが HTTPS セションのテストと組み合わされることは可能である。高信頼アップデートに関連するすべてのロギングは、最大の熱意と共に詳細にわたってテストされるべきである。テスト結果を検証する際に、評価者はテスト中に生成された監査記録がガイダンス文書に特定されたフォーマットと一致すること、及び各監査記録のフィールドが適切なエントリを有することを保証しなければならない。

18 ここでのテストは、セキュリティメカニズムを直接テストすることと組み合わせて達成できることに注意されたい。

2.1.2 FAU_GEN.2 利用者識別情報の関連付け

19 このアクティビティは、FAU_GEN.1.1 のテストと組み合わせて達成されるべきである。

2.1.3 FAU_STG.1 保護された監査証跡格納

2.1.3.1 TSS

20 評価者は TSS を検査して、ローカルに保存される監査データの量、及び監査記録が不正な改変または削除に対して保護される方法が記述されていることを保証しなければならない。評価者は、監査記録の正当な削除のために満たされなければならない条件が TSS に記述されていることを保証しなければならない。

2.1.3.2 ガイダンス文書

21 評価者は、ガイダンス文書を検査して、ローカルに保存されるデータを不正な改変または削除に対して保護するために要求される設定があればそれが記述されていることを判断しなければならない。

2.1.3.3 テスト

22 評価者は、以下のテストを行わなければならない：

a) テスト 1：評価者は、*不当な*管理者として監査証跡へアクセスし、監査記録の改変及び削除を試行しなければならない。評価者は、これらの試行が失敗することを検証しなければならない。

b) テスト 2：評価者は、正当な管理者として監査証跡へアクセスし、監査記録の削除を試行しなければならない。評価者は、これらの試行が成功することを検証しなければならない。評価者は、削除が許可された記録のみが削除されることを検証しなければならない。

2.1.4 FAU_STG_EXT.1 保護された監査事象格納

2.1.4.1 TSS

23 評価者は、TSS を検査して、監査データが外部監査サーバへ転送される手段、及び高信頼チャネルが提供される方法が記述されていることを保証しなければならない。

24 評価者は、TSS を検査して、ローカルに保存される監査データの量；ローカルな監査データ格納が満杯の際に何が起こるか；及びこれらの記録が不正なアクセスに対して保護される方法が TSS に記述されていることを保証しなければならない。

25 TOE が FAU_STG_EXT.2 に適合する場合、評価者は FAU_STG_EXT.2 の選択に従って TOE によって提供される数が FAU_STG_EXT.1.3 のテストを行う際に正しいことを検証しなければならない。

26 評価者は、TSS を検査して、監査データの格納領域が満杯の際の TOE のふるまいが詳述されていることを保証しなければならない。選択肢『以前の監査記録を上書き』が選択されている場合、この記述には監査データを上書きするためのルールの概要が含まれるべきである。外部 IT へ新たな監査データを送信するなど、『その他のアクション』が選ばれている場合、それに関連する TOE のふるまいもまた TSS に詳述されなければならない。

2.1.4.2 ガイダンス文書

27 また評価者は、ガイダンス文書を検査して、監査サーバへの高信頼チャネルが確立される方法が記述されていること、また監査サーバに関する何らかの要件が存在するならばその要件 (特定の監査サーバプロトコル、要求されるプロトコルのバージョンなど)、さらに監査サーバと通信するために必要とされる TOE の設定が記述されていることを保証しなければならない。

28 また評価者は、ガイダンス文書を検査して、ローカルな監査データと監査ログサーバへ送信される監査データとの間の関係が記述されていることを判断しなければならない。例えば、監査事象が生成される際、それが外部サーバとローカル格納へ同時に送信されるのか、あるいはローカル格納がバッファとして用いられ、監査サーバへデータを送信することによって定期的に「クリア」されるのか、といったことである。

29 また評価者は、FAU_STG_EXT.1.3 のすべての可能な設定オプション及び可能な設定のそれぞれについて生じる TOE のふるまいが記述されていることを保証しなければならない。可能な設定オプションの記述及び生じるふるまいは、TSS に記述されたものと対応していなければならない。

2.1.4.3 テスト

30 監査のための高信頼チャネルメカニズムのテストは、その特定の高信頼チャネルメカニズムに関連付けられた保証アクティビティに特定されるように行われる。評価者は、この要件に関して以下の追加的なテストを行わなければならない：

a) テスト 1：評価者は、提供された構成ガイダンスに従って TOE と監査サーバとの間のセションを確立しなければならない 。次に評価者は、監査サーバへ転送される監査データが生成されるようデザインされた評価者の選択による数回のアクティビティの間、監査サーバと TOE との間を通過するトラフィックを検査しなければならない。評価者は、これらのデータがこの転送の間平文で閲覧できないこと、そして監査サーバによる受信が成功することを確認しなければならない。評価者は、テスト中に監査サーバ上で用いられた特定のソフトウェア (名称、バージョン) を記録しなければならない。

31 評価者は、監査データを生成する操作を行い、このデータがローカルに保存されることを検証しなければならない。評価者は、ローカルな格納領域が超過するまで監査データを生成する操作を行い、TOE が FAU_STG_EXT.1.3 に定義されたふるまいに適合することを検証しなければならない。設定に応じて、これは監査データが最大まで満杯になった際の監査データの内容を評価者がチェックし、以下を検証しなければならない (has to) ことを意味する

a) 監査データは追跡されるべきすべての新たな監査対象事象について不変に保たれるが、監査データのローカルな保存が消去された後に監査データが

再び記録されること (FAU_STG_EXT.1.3 の選択肢『新たな監査データを破棄』について)。

b) 特定されたルールに従って、追跡されるべきすべての新たな監査対象事象によって既存の監査データが上書きされること (FAU_STG_EXT.1.3 の選択肢『以前の監査記録を上書き』について)

c) 特定されたように TOE がふるまうこと (FAU_STG_EXT.1.3 の選択肢『その他のアクション』について)。

2.1.5 FAU_STG_EXT.2 消失した監査データの集計

32 このアクティビティは、FAU_STG_EXT.1.2 及び FAU_STG_EXT.1.3 のテストと組み合わせて達成されるべきである。

2.1.5.1 TSS

33 評価者は、TSS を検査して、監査データの格納領域が満杯の場合に破棄、上書きなどされた監査記録の数についての情報に関して TOE がサポートする可能なオプションが詳述されていることを保証しなければならない。

2.1.5.2 ガイダンス文書

34 また評価者は、すべての可能な設定オプション及び可能な設定のそれぞれについて TOE から返される結果の意味がガイダンス文書に記述されていることを保証しなければならない。可能な設定オプションの記述及び結果の説明は、TSS に記述されたものと対応していなければならない。

35 評価者は、管理者が監査記録のローカルな保存を消去する際の監査データの消失に関する管理者への警告がガイダンス文書に含まれることを検証しなければならない。

2.1.5.3 テスト

36 評価者は、FAU_STG_EXT.2 の選択に従って TOE によって提供される数が FAU_STG_EXT.1.3 のテストを行う際に正しいことを検証しなければならない。

2.1.6 FAU_STG_EXT.3 ローカルの格納領域に関する警告の表示

37 このアクティビティは、FAU_STG_EXT.1.2 及び FAU_STG_EXT.1.3 のテストと組み合わせて達成されるべきである。

2.1.6.1 TSS

38 評価者は、TSS を検査して、監査データの格納領域が満杯になる前に利用者がどのように警告されるか詳述されていることを保証しなければならない。

2.1.6.2 ガイダンス文書

39 また評価者は、監査データのローカルな格納領域が満杯になる前に利用者がどのように警告されるか、そしてこの警告がどのように表示または保存されるか、ガイダンス文書に記述されていることを保証しなければならない (警告が発行された時点で管理者セションが実行中である保証は存在しないため、これはおそらくログファイルへ保存される)。ガイダンス文書における記述は、TSS の記述と対応していなければならない。

2.1.6.3 テスト

40 評価者は、監査データのローカルな格納領域が満杯になる前に TOE によって警告が発行されることを検証しなければならない。

2.2 暗号サポート (FCS)

2.2.1 FCS_CKM.1 暗号鍵生成

2.2.1.1 TSS

41 評価者は、TOE のサポートする鍵長が TSS に特定されていることを保証しなければならない。ST に 2 つ以上のスキームが特定されている場合、評価者は TSS を検査して各スキームの用途が識別されていることを検証しなければならない。

2.2.1.2 ガイダンス文書

42 評価者は、本 PP に定義されるすべての利用について、選択された 1 つまたは複数の鍵生成スキーム及び 1 つまたは複数の鍵長を用いるように TOE を設定する方法が AGD ガイダンスで管理者へ指示されていることを検証しなければならない。

2.2.1.3 テスト

43 注意：以下のテストには、工場製品には通常含まれないツールを評価者へ提供するテストプラットフォームへのアクセスを提供することが、開発者に要求される。

FIPS PUB 186-4 RSA スキームのための鍵生成

44 評価者は、鍵生成テストを用いて TOE による RSA 鍵生成の実装を検証しなければならない。このテストは、公開鍵検証指数 *e*、秘密素因数 *p* 及び *q*、公開モジュラス (modulus) *n* 及び秘密署名指数 *d* の計算を含めた鍵コンポーネントの値を正しく求める TSF の能力を検証する。

45 鍵ペア生成では、素数 *p* 及び *q* を生成するための 5 とおりの方法 (または手法) を特定している。これには、以下のものが含まれる。

a) ランダム素数：

- 証明可能素数
- 確率的素数

b) 条件付き素数：

- 素数 p1、p2、q1、q2、p 及び q を、すべて証明可能素数としなければならない
- 素数 p1、p2、q1、q2 及び q2 を証明可能素数とし、p 及び q を確率的素数としなければならない
- 素数 p1、p2、q1、q2、p 及び q を、すべて確率的素数としなければならない

46 ランダム証明可能素数手法とすべての条件付き素数手法の鍵生成手法をテストするため、評価者は決定論的に RSA 鍵ペアを生成するために十分なデータをシードとして TSF 鍵生成ルーチンに与えなければならない。これには、1 つまたは複数の乱数シード、RSA 鍵の公開鍵指数、及び望ましい鍵の長さが含まれる。サポートされている鍵の長さのそれぞれについて、評価者は 25 個の鍵ペアを TSF に生成させなければならない。評価者は、TSF によって生成された値を既知の良好な実装から生成された値と比較することによって、TSF の実装の正しさを検証しなければならない。

楕円曲線暗号 (ECC) のための鍵生成

FIPS 186-4 ECC 鍵生成テスト

47 サポートされている NIST 曲線、すなわち P-256、P-384 及び P-521 のそれぞれについて、評価者は 10 個の秘密鍵／公開鍵ペアを試験対象実装 (IUT) に生成させなければならない。秘密鍵は、承認済みランダムビット生成器 (RBG) を用いて生成されなければならない。正しさを判断するため、評価者は生成された鍵ペアを既知の良好な実装の公開鍵検証 (PKV) 機能へ提出しなければならない。

FIPS 186-4 公開鍵検証 (PKV) テスト

48 サポートされている NIST 曲線、すなわち P-256、P-384 及び P-521 のそれぞれについて、評価者は既知の良好な実装の鍵生成機能を用いて 10 個の秘密鍵／公開鍵ペアを生成し、5 個の公開鍵を不正な値となるように変更し、5 個を未変更の (すなわち、正しい) 値のままにしなければならない。評価者は、これに応じた 10 個の合格/不合格値のセットを取得しなければならない。

有限体暗号 (FFC) のための鍵生成

49 評価者は、パラメタ生成及び鍵生成テストを用いて TOE による FFC のためのパラメタ生成及び鍵生成の実装を検証しなければならない。このテストは、フィールド素数 p、暗号素数 q (p-1 を割り切る)、暗号群生成元 g、ならびに秘密鍵 x 及び公開鍵 y の計算の値を正しく求める TSF の能力を検証する。

50 パラメタ生成では、暗号素数 q 及びフィールド素数 p を生成するための 2 とおりの方法 (または手法) :

- 素数 q 及び p を両方とも証明可能素数としなければならない
- 素数 q 及びフィールド素数 p を両方とも確率的素数としなければならない

51 そして、暗号群生成元 g を生成するための 2 とおりの方法を特定している。

- 検証可能プロセスによって構築された生成元 g
- 検証不可能プロセスによって構築された生成元 g

52 鍵生成では、秘密鍵 x を生成するための 2 とおりの方法を特定している。

- RBG の len(q) ビットの出力、ここで 1 <=x <= q-1
- RBG の len(q) + 64 ビットの出力に、q-1 を法とする剰余演算を行ったもの、ここで 1<= x<=q-1

53 RBG のセキュリティ強度は、少なくとも FFC パラメタセットによって提供されるセキュリティの強度と同じでなければならない。

54 証明可能素数手法の暗号素数及びフィールド素数生成手法、または検証可能プロセスの群生成元 g、あるいはその両方をテストするため、評価者は決定論的にパラメタセットを生成するために十分なデータをシードとして TSF パラメタ生成ルーチンに与えなければならない。

55 サポートされている鍵の長さのそれぞれについて、評価者は 25 個のパラメタセットと鍵ペアを TSF に生成させなければならない。評価者は、TSF によって生成された値を既知の良好な実装から生成された値と比較することによって、TSF の実装の正しさを検証しなければならない。検証では、以下の

- g != 0,1
- q が p-1 を割り切ること
- g^q mod p = 1
- g^x mod p = y

56 もまた、FFC パラメタセットと鍵ペアのそれぞれについて、確認されなければならない。

2.2.2 FCS_CKM.2 暗号鍵確立

2.2.2.1 TSS

57 評価者は、サポートされる鍵確立スキームが FCS_CKM.1.1 に特定される鍵生成スキームと対応していることを保証しなければならない。ST に 2 つ以上のスキームが特定されている場合、評価者は TSS を検査して各スキームの用途が識別されていることを検証しなければならない。

2.2.2.2 ガイダンス文書

58 評価者は、選択された 1 つまたは複数の鍵確立スキームを用いるように TOE を設定する方法が AGD ガイダンスで管理者へ指示されていることを検証しなければならない。

2.2.2.3 テスト

鍵確立スキーム

59 評価者は、以下から該当するテストを用いて、TOE によってサポートされる鍵確立スキームの実装を検証しなければならない。

SP800-56A 鍵確立スキーム

60 評価者は、以下の機能及び検証テストを用いて、SP800-56A 鍵共有スキームの TOE の実装を検証しなければならない。各鍵共有スキーム向けのこれらの検証テストは、勧告における仕様に従った鍵共有スキームのコンポーネントが TOE に実装されていることを検証するものである。これらのコンポーネントには、DLC プリミティブ (共有秘密の値 Z) の計算と、鍵導出関数 (KDF) による導出鍵材料 (DKM) の計算が含まれる。鍵確認がサポートされる場合、評価者はまた以下に記述されるテスト手順を用いて、鍵確認のコンポーネントが正しく実装されていることも検証しなければならない。これには、DKM の解析、MAC データの生成、及び MAC タグの計算が含まれる。

機能テスト

61 機能テストは、鍵共有スキームを正しく実装する TOE の能力を検証する。このテストを行うために評価者は、TOE のサポートするスキームの既知の良好な実装からテストベクタを生成または取得しなければならない。サポートされている鍵共有スキーム・鍵共有役割の組み合わせ、KDF タイプと (サポートされている場合には) 鍵確認役割・鍵確認タイプの組み合わせのそれぞれについて、試験者は 10 セットのテストベクタを生成しなければならない。このデータセットは、10 セットの公開鍵あたり 1 セットのドメインパラメタ値 (FFC) または NIST が承認した曲線 (ECC) からなる。これらの鍵は、テストされるスキームに応じて静的鍵であるか、短期鍵であるか、またはその両方である。

62 評価者は、DKM、対応する TOE の公開鍵 (静的鍵または短期鍵、あるいはその両方)、1 つまたは複数の MAC タグ、及びその他の情報フィールド (OI) や TOE id フィールドなど KDF において用いられる任意の入力を取得しなければならない。

63 TOE が SP 800-56A に定義される KDF を利用しない場合、評価者は公開鍵と共有秘密のハッシュ値のみを取得しなければならない。

64 評価者は、既知の良好な実装を用いて共有秘密の値を計算し、鍵材料 DKM を導出し、そしてこれらの値から生成されるハッシュまたは MAC タグを比較することによって、所与のスキームの TSF の実装の正しさを検証しなければならない。

65 鍵確認がサポートされている場合、実装されている承認された MAC アルゴリズムのそれぞれについて、TSF は上記を行わなければならない。

検証テスト

66 検証テストは、相手方の有効及び無効な鍵共有結果を、鍵確認と共に、または鍵確認なしで、認識する TOE の能力を検証する。このテストを実施するため評価者は、SP800-56A 鍵共有実装に含まれるサポートする暗号機能のリストを取得し、どのエラーを TOE が認識可能であるべきかを判断しなければならない。評価者は、ドメインパラメタ値または NIST が承認した曲線、評価者の公開鍵、TOE の公開鍵／プライベート鍵ペア、MAC タグ、及びその他の情報フィールドや TOE id フィールドなど KDF において用いられる任意の入力を含むデータセットから構成される 24 個 (FFC) または 30 個 (ECC) のテストベクタのセットを生成する。

67 評価者は、テストベクタの一部にエラーを注入し、以下のフィールドが不正であるために生じる無効な鍵共有結果を TOE が認識することをテストしなければならない：共有秘密の値 Z、DKM、その他の情報フィールド OI、MAC 対象データ、または生成された MAC タグ。完全な、または部分的な (ECC のみ) 公開鍵検証が TOE に含まれる場合、評価者はまた両者の静的公開鍵、両者の短期公開鍵及び TOE の静的秘密鍵へ個別にエラーを注入し、公開鍵検証機能または部分的な鍵検証機能 (ECC のみ)、 あるいはその両方におけるエラーを TOE が検出することをも保証する。少なくとも 2 個のテストベクタは未変更のままでなければならず、従って有効な鍵共有結果をもたらすべきである (これらは合格すべきである)。

68 TOE は、これらの改変されたテストベクタを利用して、対応するパラメタを用いた鍵共有スキームをエミュレートしなければならない。評価者は TOE の結果を既知の良好な実装を用いた結果と比較して、TOE がこれらのエラーを検出することを検証しなければならない。

SP800-56B 鍵確立スキーム

69 評価者は、TOE が RSA ベースの鍵確立スキームについて送信者、受信者、またはその両方としてふるまうか TSS に記述されていることを検証しなければならない。

70 TOE が送信者としてふるまう場合、以下の保証アクティビティを行って、RSA ベースの鍵確立スキームのすべての TOE のサポートする組み合わせの正しい動作を保証しなければならない：

a) このテストを行うために評価者は、TOE のサポートするスキームの既知の良好な実装からテストベクタを生成または取得しなければならない。サポートされている鍵確立スキームとそのオプション (サポートされている場合には鍵確認ありまたはなし、鍵確認がサポートされている場合にはサポートされている鍵確認 MAC 関数のそれぞれ、そして KTS-OAEP がサポートされている場合にはサポートされているマスク生成関数のそれぞれ) の組み合わせのそれぞれについて、試験者は 10 セットのテストベクタを生成しなければならない。各テストベクタには RSA 公開鍵、平文の鍵材料、該当する場合は任意の追加入力パラメタ、鍵確認が組み込まれている場合には MacKey 及び MacTag、そして出力された暗号文が含まれなければならない。テストベクタのそれぞれについて、評価者は同一の入力 (鍵確認が組み込まれている場合、通常の操作で用いられるランダムに生成された

MacKey の代わりに、テストベクタからの MacKey が使われなければならない) を用いて TOE 上で鍵確立暗号操作を行い、出力された暗号文がテストベクタ中の暗号文と同等であることを保証しなければならない。

71 TOE が受信者としてふるまう場合、以下の保証アクティビティを行って、RSA ベースの鍵確立スキームのすべての TOE のサポートする組み合わせの正しい動作を保証しなければならない：

a) このテストを行うために評価者は、TOE のサポートするスキームの既知の良好な実装からテストベクタを生成または取得しなければならない。サポートされている鍵確立スキームとそのオプション (サポートされている場合には鍵確認ありまたはなし、鍵確認がサポートされている場合にはサポートされている鍵確認 MAC 関数のそれぞれ、そして KTS-OAEP がサポートされている場合にはサポートされているマスク生成関数のそれぞれ) の組み合わせのそれぞれについて、試験者は 10 セットのテストベクタを生成しなければならない。各テストベクタには RSA 秘密鍵、平文の鍵材料 (KeyData)、該当する場合は任意の追加入力パラメタ、鍵確認が組み込まれている場合には MacTag、そして出力された暗号文が含まれなければならない。テストベクタのそれぞれについて、評価者は TOE 上で鍵確立復号操作を行い、出力された平文鍵材料 (KeyData) がテストベクタ中の平文鍵材料と同等であることを保証しなければならない。鍵確認が組み込まれている場合、評価者は鍵確認ステップを行い、出力された MacTag がテストベクタ中の MacTag と同等であることを保証しなければならない。

b) 評価者は、TOE が復号エラーを取り扱う方法が TSS に記述されていることを保証しなければならない。NIST Special Publication 800-56B に従い、出力された、またはロギングされたエラーメッセージの内容を通しても、あるいはタイミングの変動を通しても、TOE は発生した具体的なエラーを開示してはならない (must not)。KTS-OAEP がサポートされている場合、評価者は NIST Special Publication 800-56B section 7.2.2.3 に記述される 3 種類の復号エラーチェックのそれぞれを引き起こすように計画された暗号文の値を作成し、復号試行結果のそれぞれがエラーとなることを保証し、そして任意の出力された、またはロギングされたエラーメッセージが互いに同一であることを保証しなければならない。KTS-KEM-KWS がサポートされている場合、評価者は NIST Special Publication 800-56B section 7.2.3.3 に記述される 3 種類の復号エラーチェックのそれぞれを引き起こすように計画された暗号文の値を作成し、復号試行結果のそれぞれがエラーとなることを保証し、そして任意の出力された、またはロギングされたエラーメッセージが互いに同一であることを保証しなければならない。

2.2.3 FCS_CKM.4 暗号鍵破棄

2.2.3.1 TSS

72 評価者は、平文鍵材料の各種別が、その生成元 (origin) 及び保存場所を含めて TSS に列挙されていることをチェックして保証しなければならない。

73 評価者は、鍵材料の各種別がいつクリアされるのか (例えば、システムの電源断の際、抹消機能の際、高信頼チャネルの切断の際、高信頼チャネルのプロトコルによってもはや必要とされなくなった際など) TSS に記述されていること

を検証しなければならない。

74 また評価者は、鍵の種別のそれぞれについて、行われるクリア手続きの種別(暗号技術的消去、ゼロで上書き、ランダムパターンで上書き、またはブロック消去) が列挙されていることも検証しなければならない。保護されるべき材料の保存に異なる種別のメモリが用いられる場合、評価者はデータが保存されるメモリに応じたクリア手続き (例えば、「フラッシュメモリ上に保存される共通鍵はゼロで 1 度上書きすることによってクリアされるが、内部永続的保存デバイス上に保存される共通鍵は書き込みごとに変化するランダムパターンを 3 度上書きすることによってクリアされる」) が TSS に記述されていることをチェックして保証しなければならない。

2.2.4 FCS_COP.1(1) 暗号操作 (AES データ暗号化／復号)

2.2.4.1 テスト

AES-CBC 既知解テスト

75 既知解テスト (KAT) には、以下に記述される 4 つがある。すべての KAT において、平文、暗号文、及び IV の値は 128 ビットのブロックとしなければならない。各テストの結果は、直接評価者によって、あるいは入力を実装者へ供給しその結果を受領することによって、取得され得る。正しさを判断するため、評価者は結果の値を、同一の入力を既知の良好な実装へ与えることによって得られた値と比較しなければならない。

76 **KAT-1.** AES-CBC の暗号化機能をテストするため、評価者は 10 個の平文の値のセットを供給し、すべてゼロの鍵の値とすべてゼロの IV を用いて所与の平文の AES-CBC 暗号化から得られる暗号文の値を取得しなければならない。5 個の平文の値は 128 ビットのすべてゼロの鍵で暗号化されなければならず、それ以外の 5 個は 256 ビットのすべてゼロの鍵で暗号化されなければならない。

77 AES-CBC の復号機能をテストするため、評価者は入力として 10 個の暗号文の値と AES-CBC 復号を用いて、暗号化と同一のテストを行わなければならない。

78 **KAT-2.** AES-CBC の暗号化機能をテストするため、評価者は 10 個の鍵の値のセットを供給し、所与の鍵の値とすべてゼロの IV を用いてすべてゼロの平文の AES-CBC 暗号化から得られる暗号文の値を取得しなければならない。5 個の鍵は 128 ビットの鍵としなければならず、それ以外の 5 個は 256 ビットの鍵としなければならない。

79 AES-CBC の復号機能をテストするため、評価者は入力としてすべてゼロの暗号文の値と AES-CBC 復号を用いて、暗号化と同一のテストを行わなければならない。

80 **KAT-3.** AES-CBC の暗号化機能をテストするため、評価者は以下に記述する 2 セットの鍵の値を供給し、所与の鍵の値とすべてゼロの IV を用いてすべてゼロの平文の AES 暗号化から得られる暗号文の値を取得しなければならない。第 1 の鍵のセットは 128 個の 128 ビットの鍵からなるものとしなければならず、第 2 のセットは 256 個の 256 ビットの鍵からなるものとしなければならない。[1,N] の範囲の *i* について、各セットの鍵 *i* の左端の i ビットは 1、右端の *N-i* ビットは 0 としなければならない。

81 AES-CBC の復号機能をテストするため、評価者は以下に記述する 2 セットの鍵と暗号文の値のペアを供給し、所与の鍵の値とすべてゼロの IV を用いて所与の暗号文の AES-CBC 復号から得られる平文の値を取得しなければならない。第 1 の鍵／暗号文のペアのセットは 128 個の 128 ビットの鍵／暗号文のペアからなるものとしなければならず、第 2 のセットは 256 個の 256 ビットの鍵／暗号文のペアからなるものとしなければならない。[1,N] の範囲の i について、各セットの鍵 i の左端の i ビットは 1、右端の N-i ビットは 0 としなければならない。各ペアの暗号文の値は、それに対応する鍵で復号された際にすべてゼロの平文が得られるような値としなければならない。

82 **KAT-4.** AES-CBC の暗号化機能をテストするため、評価者は以下に記述する 128 個の平文の値のセットを供給し、2 種類の暗号文の値 (それぞれ、すべてゼロの 128 ビットの鍵の値とすべてゼロの IV、及びすべてゼロの 256 ビットの鍵の値とすべてゼロの IV を用いて、所与の平文の AES-CBC 暗号化から得られる) を取得しなければならない。[1,128] の範囲の i について、各セットの平文の値 i の左端の i ビットは 1、右端の N-i ビットは 0 としなければならない。

83 AES-CBC の復号機能をテストするため、評価者は入力として暗号化テストにおける平文と同一の形式の暗号文の値と AES-CBC 復号を用いて、暗号化と同一のテストを行わなければならない。

AES-CBC 複数ブロックメッセージテスト

84 評価者は、*i* 個のブロックからなるメッセージ (ここで $1 < i <= 10$) を暗号化することによって、暗号化機能をテストしなければならない。評価者は鍵、IV 及び長さ *i* ブロックの平文メッセージを選び、試験すべきモードを用いて、選んだ鍵及び IV によってメッセージを暗号化しなければならない。暗号文は、既知の良好な実装を用いて同一の平文メッセージを同一の鍵と IV によって暗号化した結果と比較されなければならない。

85 また評価者は、*i* 個のブロックからなるメッセージ (ここで $1< i <= 10$) を復号することによって、各モードについて復号機能をテストしなければならない。評価者は鍵、IV 及び長さ *i* ブロックの暗号文メッセージを選び、試験すべきモードを用いて、選んだ鍵及び IV によってメッセージを復号しなければならない。平文は、既知の良好な実装を用いて同一の暗号文メッセージを同一の鍵と IV によって復号した結果と比較されなければならない。

AES-CBC モンテカルロテスト

86 評価者は、200 個の平文、IV、及び鍵の 3 つ組のセットを用いて、暗号化機能をテストしなければならない。これらのうち 100 個は 128 ビットの鍵を用いるものとしなければならず、100 個は 256 ビットの鍵を用いるものとしなければならない。平文と IV の値は、128 ビットのブロックとしなければならない。3 つ組のそれぞれについて、以下のように 1000 回の反復処理が実行されなければならない。

```
# 入力：PT, IV, Key
for i = 1 to 1000:
        if i == 1:
                CT[1] = AES-CBC-Encrypt(Key, IV, PT)
                PT = IV
        else:
                CT[i] = AES-CBC-Encrypt(Key, PT)
                PT = CT[i-1]
```

87 1000 回目の反復処理において計算された暗号文 (すなわち、CT[1000]) が、その試行の結果となる。この結果は、既知の良好な実装を用いて同一の値によって 1000 回反復処理を実行した結果と比較されなければならない。

88 評価者は、暗号化と同一のテストを用い、CT と PT とを入れ替え、AES-CBC-Encrypt を AES-CBC-Decrypt で置き換えて、復号機能をテストしなければならない。

AES-GCM テスト

89 評価者は、以下の入力パラメタ長の組み合わせのそれぞれについて、AES-GCM の認証済み暗号化機能をテストしなければならない。

128 ビット及び256 ビットの鍵

a) **2 とおりの平文の長さ**。ひとつの平文の長さは、128 ビットのゼロ以外の整数倍としなければならない (サポートされる場合)。他の平文の長さは、128 ビットの整数倍であってはならない (shall not) (サポートされる場合)。

b) **3 とおりの AAD 長**。1 つの AAD 長は 0 としなければならない (サポートされる場合)。1 つの AAD 長は、128 ビットのゼロ以外の整数倍としなければならない (サポートされる場合)。1 つの AAD 長は、128 ビットの整数倍であってはならない (shall not) (サポートされる場合)。

c) **2 とおりの IV 長**。96 ビットの IV がサポートされる場合、テストされる 2 とおりの IV の長さの一方を 96 ビットとしなければならない。

90 評価者は、上記のパラメタ長の組み合わせのそれぞれについて、10 個の鍵、平文、AAD、及び IV の組のセットを用いて暗号化機能をテストし、AES-GCM 認証済み暗号化から得られた暗号文の値とタグを取得しなければならない。サポートされているタグ長はそれぞれ、10 個のセットにつき少なくとも 1 度はテストされなければならない。IV の値は、それが既知である限り、評価者によって供給されても、テストされている実装によって供給されてもよい。

91 評価者は、上記のパラメタ長の組み合わせのそれぞれについて、10 個の鍵、暗号文、タグ、AAD、及び IV の 5 つ組のセットを用いて復号機能をテストし、認証に関する合格／不合格結果及び合格の場合には復号した平文を取得しな

ければならない。セットには、合格となる 5 組と不合格となる 5 組が含まれなければならない。

92 各テストの結果は、直接評価者によって、あるいは入力を実装者へ供給しその結果を受領することによって、取得され得る。正しさを判断するため、評価者は結果の値を、同一の入力を既知の良好な実装へ与えることによって得られた値と比較しなければならない。

2.2.5 FCS_COP.1(2) 暗号操作 (署名生成及び検証)

2.2.5.1 テスト

ECDSA アルゴリズムテスト

ECDSA FIPS 186-4 署名生成テスト

93 サポートされている NIST 曲線 (すなわち、P-256、P-384 及び P-521) と SHA 関数のペアのそれぞれについて、評価者は 10 個の 1024 ビットの長さのメッセージを生成し、各メッセージについて公開鍵ならびに得られた署名の値 R 及び S を取得しなければならない。正しさを判断するため、評価者は既知の良好な実装の署名検証機能を利用しなければならない。

ECDSA FIPS 186-4 署名検証テスト

94 サポートされている NIST 曲線 (すなわち、P-256、P-384 及び P-521) と SHA 関数のペアのそれぞれについて、評価者は 10 個の 1024 ビットの長さのメッセージ、公開鍵及び署名の組のセットを生成し、10 組のうち 5 組で値のいずれか (メッセージ、公開鍵または署名) を変更しなければならない。評価者は、これに応じた 10 個の合格/不合格値のセットを取得しなければならない。

RSA 署名アルゴリズムテスト

署名生成テスト

95 評価者は、署名生成テストを用いて TOE による RSA 署名生成の実装を検証しなければならない。このテストを行うために評価者は、TSF のサポートする法サイズ／SHA の組み合わせのそれぞれについて、高信頼リファレンス実装から 10 個のメッセージを生成または取得しなければならない。評価者は、TOE に自分の秘密鍵と法の値を用いてこれらのメッセージへ署名させなければならない。

96 評価者は、既知の良好な実装及び関連付けられた公開鍵を用いて署名を検証することによって、TSF の署名の正しさを検証しなければならない。

署名検証テスト

97 評価者は、署名検証テストを行って、相手方の有効及び無効な署名を認識する TOE の能力を検証しなければならない。評価者は、公開鍵 e、メッセージ、IR フォーマット、または署名、あるいはこれらのうち 2 つ以上にエラーを導入することによって、署名検証テスト中に作成されたテストベクタへエラーを注入しなければならない。TOE は署名の検証を試行し、成功または失敗を返す。

98 評価者はこれらのテストベクタを利用して、対応するパラメタを用いた署名検証テストをエミュレートし、TOE がこれらのエラーを検出することを検証しなければならない。

2.2.6 FCS_COP.1(3) 暗号操作 (ハッシュアルゴリズム)

2.2.6.1 TSS

99 評価者は、ハッシュ機能と他の TSF 暗号機能 (例えば、デジタル署名検証機能) との関連が TSS に文書化されていることをチェックしなければならない。

2.2.6.2 ガイダンス文書

100 評価者は AGD 文書をチェックして、必要とされるハッシュのサイズを設定するために必要とされる構成があれば、それが存在することを判断する。

2.2.6.3 テスト

101 TSF ハッシュ関数は、2 つのモードのいずれかで実装できる。第 1 のモードは、バイト指向モードである。このモードでは、TSF は長さがバイトの整数倍であるメッセージのみをハッシュする。すなわち、ハッシュされるべきメッセージのビット長が 8 で割り切れる必要がある。第 2 のモードは、ビット指向モードである。このモードでは、TSF は任意の長さのメッセージをハッシュする。各モードについて異なるテストが存在するため、ビット指向とバイト指向のテストについて、以下のセクションで指示を与える。

102 評価者は、TSF によって実装され、本 PP の要件を満たすために用いられるハッシュアルゴリズムのそれぞれについて、以下のテストをすべて行わなければならない。

ショートメッセージテスト—ビット指向モード

103 評価者は、m+1 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。メッセージの長さは、0 から m ビットまでシーケンシャルに変化する。メッセージの本文は、疑似ランダム的に生成されなければならない。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

ショートメッセージテスト—バイト指向モード

104 評価者は、m/8+1 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。メッセージの長さは 0 から m/8 バイトまでシーケンシャルに変化し、各メッセージは整数個のバイトとなる。メッセージの本文は、疑似ランダム的に生成されなければならない。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

選択されたロングメッセージテスト—ビット指向モード

105 評価者は、m 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である (例えば SHA-256 については 512 ビット)。i 番目のメッセージの長さは m + 99*i となる (ここで $1 \leq i \leq m$)。メッセージの本文は、疑似ランダム的に生成されなければならない。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

選択されたロングメッセージテスト—バイト指向モード

106 評価者は、m/8 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である (例えば SHA-256 については 512 ビット)。i 番目のメッセージの長さは m + 8*99*i となる (ここで $1 \leq i \leq m/8$)。メッセージの本文は、疑似ランダム的に生成されなければならない。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

疑似ランダム的に生成されたメッセージテスト

107 このテストは、バイト指向の実装にのみ行われる。評価者は、n ビットの長さのシードをランダムに生成する。ここで n はテストされるハッシュ関数によって作成されるメッセージダイジェストの長さである。次に評価者は、[SHAVS] の図 1 に示されるアルゴリズムに従って 100 個のメッセージと関連するダイジェストのセットを作成する。次に評価者は、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

2.2.7 FCS_COP.1(4) 号操作 (鍵付きハッシュアルゴリズム)

2.2.7.1 TSS

108 評価者は、TSS を検査して、HMAC 機能によって利用される以下の値が特定されていることを保証しなければならない : 鍵の長さ、用いられるハッシュ関数、ブロックサイズ、及び用いられる出力 MAC 長。

2.2.7.2 テスト

109 サポートされるパラメタセットのそれぞれについて、評価者は 15 セットのテストデータを構成しなければならない。各セットは、1 つの鍵とメッセージデ

ータから構成されるものとするしなければならない。評価者は、テストデータのこれらのセットについて TSF に HMAC タグを生成させなければならない。得られた MAC タグは、同一の鍵と IV によって既知の良好な実装を用いて HMAC タグを生成した結果と比較されなければならない。

2.2.8 FCS_RBG_EXT.1 拡張：暗号操作 (ランダムビット生成)

110 [NDcPP] の附属書 D に従って、文書が作成されなければならない (そして評価者はアクティビティを行わなければならない)。

2.2.8.1 テスト

111 評価者は、RNG 実装の 15 回の試行を行わなければならない。RNG が設定可能な場合、評価者は各設定について 15 回の試行を行わなければならない。また評価者は、RNG 機能を設定するための適切な指示がガイダンス文書に含まれていることも確認しなければならない。

112 RNG が有効な予測困難性を持つ場合、各回の試行は (1) DRBG をインスタンス化し、(2) ランダムなビットの最初のブロックを生成し、(3) ランダムなビットの 2 番目のブロックを生成し、(4) 非インスタンス化する、という手順になる。評価者は、ランダムなビットの 2 番目のブロックが期待された値であることを検証する。評価者は、各試行に 8 つの入力値を生成しなければならない。最初はカウント (0～14) である。次の 3 つはインスタンス化操作のエントロピー入力とノンス、そして Personalization String である。次の 2 つは、最初の生成呼び出しへの追加的入力とエントロピー入力である。最後の 2 つは、2 番目の生成呼出しへの追加的入力とエントロピー入力である。これらの値は、ランダムに生成される。「ランダムなビットのひとつのブロックを生成」とは、返されるビット数が (NIST SP800-90A に定義される) Output Block Length と等しいランダムなビットを生成することを意味する。

113 RNG が予測困難性を持たない場合、各回の試行は (1) DRBG をインスタンス化し、(2) ランダムなビットの最初のブロックを生成し、(3) シードを再供給し、(4) ランダムなビットの 2 番目のブロックを生成し、(5) 非インスタンス化する、という手順になる。評価者は、ランダムなビットの 2 番目のブロックが期待された値であることを検証する。評価者は、各試行に 8 つの入力値を生成しなければならない。最初はカウント (0～14) である。次の 3 つはインスタンス化操作のエントロピー入力とノンス、そして Personalization String である。5 番目の値は、最初の生成呼出しへの追加的入力である。6 番目と 7 番目は、シードを再供給する呼出しへの追加的入力とエントロピー入力である。最後の値は、2 回目の生成呼出しへの追加的入力である。

114 以下のパラグラフには、評価者によって生成／選択されるべき入力値のいくつかについて、より多くの情報が含まれている。

エントロピー入力 : エントロピー入力値の長さは、シードの長さと等しくなければならない。

ノンス：ノンスがサポートされている場合 (導出関数なしの CTR_DRBG はノンスを利用しない)、ノンスのビット長はシードの長さの半分となる。

Personalization String：Personalization String の長さは、シードの長さ以下でなければならない。実装が 1 とおりの Personalization String の長さしかサポートしていない場合には、両方の値に同一の長さが使用できる。2 とおり以上の文字列の長さがサポートされている場合、評価者は 2 つの異なる長さの Personalization String を用いなければならない。実装が Personalization String を用いない場合、値を供給する必要はない。

追加的入力：追加的入力のビット長は、Personalization String の長さと同一のデフォルトと制約を持つ。

2.2.9 FCS_HTTPS_EXT.1 HTTPS プロトコル

2.2.9.1 テスト

115 評価者は、以下のテストを行わなければならない：

a) テスト 1 : 評価者は、ウェブサーバとの HTTPS 接続を試行し、パケットアナライザでトラフィックを確認し、そして接続が成功しトラフィックが TLS または HTTPS と特定されることを検証しなければならない。

116 その他のテストは、TLS 保証アクティビティと組み合わせて行われる。

117 証明書の有効性は FIA_X509_EXT.1 のために行われるテストに従ってテストされなければならず、また評価者は以下のテストを行わなければならない：

b) テスト 2 : 評価者は、有効な認証パスのない証明書を使用すると、アプリケーション通知が発生することを実証しなければならない。管理ガイダンスを利用して、次に評価者は有効な認証パスを持つ証明書をロードし、その機能が成功することを実証しなければならない。次に評価者は証明書の 1 つを削除して、ST に列挙された選択が発生することを示さなければならない。

2.2.10 FCS_IPSEC_EXT.1 IPsec プロトコル

2.2.10.1 TSS

FCS_IPSEC_EXT.1.1

118 評価者は、TSS を検査して、パケットが TOE によって処理される際に何が起こるか (例えばパケットを処理するために用いられるアルゴリズム) が記述されていることを判断しなければならない。TSS には、SPD がどのように実装されるか、及び IPsec ポリシーの観点から内向きと外向きの両方のパケットを処理するルールが記述される。TSS には、利用可能なルール及びルールにマッチした後にその結果として行われる利用可能なアクションが記述される。TSS には、これらのルールとアクションが RFC 4301 に定義される BYPASS (例えば暗号化なし)、DISCARD (例えばパケットの破棄)、及び PROTECT (例えば、そのパケットの暗号化) アクションの観点からどのように SPD を形成するかが記

述される。

119 RFC 4301 のセクション 4.4.1 に記されているように、SPD のエントリの処理は自明ではないため、TOE によって実装されるルール構造が与えられた際に TSS の記述によってどのルールが適用されるか十分に判断できることを評価者は判断しなければならない。例えば、TOE が範囲、条件付きルールなどの指定を許可している場合、ルール処理の記述 (内向きと外向きの両方のパケットについて) によって適用されるアクションが十分に判断できることを、特に 2 つの異なるルールが適用され得る場合について、評価者は判断しなければならない。この記述は、最初のパケット (すなわち、インタフェース上またはその特定のパケットについて SA が確立されていない) と確立された SA に属するパケットの両方をカバーしなければならない。

FCS_IPSEC_EXT.1.3

120 評価者は、TSS をチェックして、VPN が (FCS_IPSEC_EXT.1.3 に特定されるように) トンネルモードまたはトランスポートモード、あるいはその両方で確立できると言明されていることを保証する。

FCS_IPSEC_EXT.1.4

121 評価者は、TSS を検査して、アルゴリズム AES-CBC-128 及び AES-CBC-256 が実装されていることを検証しなければならない。ST 作成者が要件で AES-GCM-128 または AES-GCM-256 のいずれかを選択している場合には、評価者はそれらもまた TSS に記述されていることを検証する。さらに、評価者は SHA ベースの HMAC アルゴリズムが FCS_COP.1(4) 暗号操作 (鍵付きハッシュメッセージ認証) に特定されるアルゴリズムに適合していることを保証する。

FCS_IPSEC_EXT.1.5

122 評価者は、TSS を検査して、IKEv1 または IKEv2、あるいはその両方が実装されていることを検証しなければならない。

123 IKEv1 の実装について、評価者は TSS を検査して、IPsec プロトコルの記述で、IKEv1 フェーズ 1 交換にアグレッシブモードが使用されずメインモードのみが使用されることが言明されていることを保証しなければならない。これは構成可能なオプションであってもよい。

FCS_IPSEC_EXT.1.6

124 評価者は、IKEv1 または IKEv2 あるいはその両方のペイロードの暗号化に用いられるアルゴリズムが TSS に特定されていること、及びアルゴリズム AES-CBC-128、AES-CBC-256 が指定されていること、さらに要件の選択においてその他が選ばれている場合には、それらが TSS の議論に含まれていることを保証しなければならない。

FCS_IPSEC_EXT.1.7

125 評価者は、IKEv1 のフェーズ 1 SA ライフタイムまたは IKEv2 の SA ライフタイム、あるいはその両方を制限するために用いられるライフタイム設定手法が TSS に特定されていることを保証しなければならない。評価者は、ここで行われた選択が FCS_IPSEC_EXT.1.5 の選択と対応していることを検証しなければならない。

FCS_IPSEC_EXT.1.8

126 評価者は、IKEv1 のフェーズ 2 SA ライフタイムまたは IKEv2 の Child SA ライフタイム、あるいはその両方を制限するために用いられるライフタイム設定手法が TSS に特定されていることを保証しなければならない。評価者は、ここで行われた選択が FCS_IPSEC_EXT.1.5 の選択と対応していることを検証しなければならない。

FCS_IPSEC_EXT.1.9

127 評価者は、サポートされる DH グループのそれぞれについて、「x」を生成するプロセスが TSS に記述されていることをチェックして保証しなければならない。評価者は、本 PP の要件を満たす生成された乱数が使われること、及び「x」の長さが要件の規定を満たすことが、TSS に示されていることを検証しなければならない。

FCS_IPSEC_EXT.1.11

128 評価者は、要件に特定される DH グループがサポートされるものとして TSS に列挙されていることをチェックして保証しなければならない。2 つ以上の DH グループがサポートされる場合、評価者は特定の DH グループをピアとの間で指定／ネゴシエーションする方法が TSS に記述されていることをチェックして保証する。

FCS_IPSEC_EXT.1.12

129 評価者は、IKE 及び ESP 交換に許可されるアルゴリズムの潜在的な強度 (対称鍵のビット数の観点から) が TSS に記述されていることをチェックしなければならない。また TSS には、IKEv1 フェーズ 2 または IKEv2 CHILD_SA スイートあるいはその両方のネゴシエーション時に行われる、ネゴシエーションされたアルゴリズムの強度 (対称アルゴリズムにおける鍵のビット数の観点から) がネゴシエーションを保護する IKE SA の強度以下であることを保証するために行われるチェックについて記述されていなければならない。

FCS_IPSEC_EXT.1.13

130 評価者は、RSA または ECDSA あるいはその両方がピア認証を行うために使われるものとして TSS に特定されていることを保証する。この記述は、FCS_COP.1(2) 暗号操作 (暗号署名) に特定されるアルゴリズムと一貫していなければならない。

131 選択において事前共有鍵が選択されている場合、事前共有鍵が確立され IPsec 接続の認証に用いられる方法が TSS に記述されていることを評価者はチェックして保証しなければならない。また TSS の記述には、事前共有鍵を生成できる TOE と、単純に事前共有鍵を利用する TOE について、事前共有鍵の確立が達成される方法が示されていなければならない。

FCS_IPSEC_EXT.1.14

132 評価者は、証明書の DN が期待される DN と比較される方法が TSS に記述されていることを検証しなければならない。

2.2.10.2 ガイダンス文書

FCS_IPSEC_EXT.1.1

133 評価者は、ガイダンス文書を検査して、パケットを処理するルールを特定するエントリを SPD に構築する方法が管理者へ指示されていることを検証しなければならない。この記述には 3 つの場合すべて、つまりパケットが暗号化／復号されること、破棄されること、そして暗号化されずに TOE を通過して流れることを保証するルールが含まれる。評価者はガイダンス文書の記述が TSS の記述と一貫していること、及びあいまいさのない形で管理者が SPD を設定できるほどガイダンス文書が十分に詳細なレベルであることを判断しなければならない。これには、ルールの順序が IP パケットの処理にどのような影響を与えるかの議論が含まれる。

FCS_IPSEC_EXT.1.3

134 評価者は、選択された各モードにおいて接続を設定する方法に関する指示がガイダンス文書に含まれることを確認しなければならない。

FCS_IPSEC_EXT.1.4

135 評価者は、ガイダンス文書をチェックして、TOE がそれらのアルゴリズムを利用するように設定する方法に関する指示が与えられていること、そして AES-GCM-128 または AES-GCM-256 のいずれかが選択されている場合にはこれらを利用する方法もまたガイダンスに指示されていることを保証する。

FCS_IPSEC_EXT.1.5

136 評価者はガイダンス文書をチェックして、(選択されたように) IKEv1 または IKEv2 あるいはその両方を使用するように TOE を設定する方法が管理者へ指示されていることを保証しなければならず、またガイダンスを利用して NAT トラバーサルを行うよう TOE を構成し、以下のテストを行う (選択されている場合)。

137 IKEv1 フェーズ 1 モードがその動作前に TOE の設定を要求する場合、評価者はガイダンス文書をチェックしてこの設定の指示がそのガイダンスに含まれていることを保証しなければならない。

FCS_IPSEC_EXT.1.6

138 評価者は、必須のアルゴリズムの設定が (要件において選択された追加アルゴリズムがあればそれについても) ガイダンス文書に記述されていることを保証する。次にガイダンスを用いて TOE を構成し、選択された各暗号スイートについて以下のテストを行う。

FCS_IPSEC_EXT.1.7

139 評価者は、SA ライフタイムの値が設定可能であり、そうするための指示がガイダンス文書に存在することを検証しなければならない。時間ベースの制限がサポートされている場合、管理者がフェーズ 1 SA の値を 24 時間に設定できることを評価者は保証する。現時点ではバイト数に関して必須の値は存在しないため、要件にこれが選択された場合、評価者はこれが設定できることのみを保証する。

FCS_IPSEC_EXT.1.8

140 評価者は、SA ライフタイムの値が設定可能であり、そうするための指示がガイダンス文書に存在することを検証しなければならない。時間ベースの制限がサポートされている場合、管理者がフェーズ 2 SA の値を 8 時間に設定できることを評価者は保証する。現時点ではバイト数に関して必須の値は存在しないため、要件にこれが選択された場合、評価者はこれが設定できることのみを保証する。

FCS_IPSEC_EXT.1.11

141 評価者は、必須のアルゴリズムの設定が (要件において選択された追加アルゴリズムがあればそれについても) ガイダンス文書に記述されていることを保証する。次にガイダンスを用いて TOE を構成し、選択された各暗号スイートについて以下のテストを行う。

FCS_IPSEC_EXT.1.13

142 評価者は、RSA または ECDSA あるいはその両方の署名及び公開鍵を使用するよう TOE を設定する方法がガイダンス文書に記述されていることを保証する。

143 評価者は、事前共有鍵が生成され確立される方法がガイダンス文書に記述されていることをチェックしなければならない。またガイダンス文書の記述には、事前共有鍵を生成できる TOE と、単純に事前共有鍵を利用する TOE について、事前共有鍵の確立が達成される方法が示されていなければならない。

144 以下のテストのための環境を構築し TOE を設定するため、評価者は信頼済み CA へ接続するように TOE を構成する方法がガイダンス文書に記述されていることを保証し、またその CA の有効な証明書が TOE にロードされ「信頼済み (trusted)」とマークされることを保証すること。

FCS_IPSEC_EXT.1.14

145 評価者は、接続に期待される DN の設定がガイダンス文書に含まれることを保証しなければならない。

2.2.10.3 テスト

FCS_IPSEC_EXT.1.1

146 評価者は、ガイダンス文書を用いて TOE を構成し、以下のテストを実施する：

a) テスト 1：評価者は、パケットを破棄するルール、パケットを暗号化するルール、及びパケットが平文で流れることを許可するルールが存在するように SPD を設定しなければならない。パケットヘッダに適切なフィールド (ルールによって利用されるフィールド―例えば、IP アドレス、TCP/UDP ポート) を含むように評価者がパケットを生成し、ゲートウェイへパケットを送信できるように、ルールの構築に用いられるセレクタは異なっていなければならない。評価者は、各タイプのルールについてポジティブとネガティブの両方のテストケースを実施する (例えば、そのルールにマッチするパケットとそのルールにマッチしない別のパケット)。評価者は、監査証跡、及びパケットキャプチャによって、TOE が期待されたふるまいを示していることを確認する：期待されるふるまいとは、適切なパケットが破棄されたり、変更なしに通過を許可されたり、IPsec の実装によって暗号化さ

れたりすることである。

b) テスト 2：評価者は、パケット処理のさまざまなシナリオをカバーするいくつかのテストを考案しなければならない。テスト 1 と同様に、評価者はポジティブとネガティブの両方のテストケースが構築されることを保証する。これらのシナリオは、TSS 及びガイダンス文書に概説されるように SPD エントリ及び処理モードの幅広い可能性を行使しなければならない。カバーされる可能性のある領域としては、重なりのある範囲や相反するエントリを持つ複数のルール、内向きと外向きのパケット、及び SA を確立するパケットと確立された SA に属するパケットなどが挙げられる。評価者は、監査証跡及びパケットキャプチャによって、各シナリオについて期待されるふるまいが示されること、またそれが TSS とガイダンス文書の両方と一貫していることを検証しなければならない。

FCS_IPSEC_EXT.1.2

147 このエレメントの保証アクティビティは、FCS_IPSEC_EXT.1.1 の保証アクティビティと組み合わせて行われる。

148 評価者は、ガイダンス文書を用いて TOE を構成し、以下のテストを実施する：

149 評価者は、パケットを破棄するルール、パケットを暗号化するルール、及びパケットが平文で流れることを許可するルールが存在するように SPD を設定しなければならない。評価者は、FCS_IPSEC_EXT.1.1 を検証するために作成された SPD を使ってもよい。評価者は、パケットが平文で流れることを許可するルールにマッチするネットワークパケットを構築し、そのパケットを送信しなければならない。評価者は、ネットワークパケットが変更されずに適切な宛先インタフェースへ通過されることを確認すべきである。評価者は次に、もはや評価者が作成したエントリへはマッチしないようにパケットヘッダのフィールドを変更しなければならない (それ以前のエントリのどれにもマッチしなかったパケットを廃棄する「TOE によって作成された」最後のエントリが存在するかもしれない)。評価者はそのパケットを送信し、そしてそのパケットが破棄されることを確認する。

FCS_IPSEC_EXT.1.3

150 評価者は、選ばれた選択に応じて以下の 1 つまたは複数のテストを行わなければならない：

a) テスト 1 (条件付き)：トンネルモードが選択されている場合、評価者はガイダンス文書を用いて TOE をトンネルモードで動作するように設定し、また VPN ピアもトンネルモードで動作するように設定する。評価者は、任意の許容可能な暗号アルゴリズム、認証手法などを用いるように TOE 及び VPN ピアを構成し、許容可能な SA がネゴシエーションできることを保証する。評価者は次に、TOE からの接続を開始して VPN ピアへ接続しなければならない。評価者は、トンネルモードを用いた接続の確立が成功していることを (例えば、監査証跡及びキャプチャされたパケットで) 確認する。

b) テスト 2：評価者はガイダンス文書を用いて TOE をトランスポートモードで動作するように設定し、また VPN ピアもトランスポートモードで動作するように設定する。評価者は、任意の許容される暗号アルゴリズム、認証手法などを用いるように TOE 及び VPN ピアを構成し、許容可能な SA が

ネゴシエーションできることを保証する。評価者は次に、TOE からの接続を開始して VPN ピアへ接続する。評価者は、トランスポートモードを用いた接続の確立が成功していることを (例えば、監査証跡及びキャプチャされたパケットで) 確認する。

FCS_IPSEC_EXT.1.4

151 評価者は、ガイダンス文書に示されるように TOE を設定し、サポートされるアルゴリズムのそれぞれを TOE が用いるよう設定して、ESP を使用する接続の確立を試行し、その試行が成功することを検証しなければならない。

FCS_IPSEC_EXT.1.5

152 テストは、他の IPsec 評価アクティビティと組み合わせて行われる。

153 (条件付き) : 評価者はガイダンス文書に示されるように TOE を構成して、アグレッシブモードで IKEv1 フェーズ 1 接続を用いた接続の確立を試行しなければならない。この試行は失敗するはずである。評価者は次に、メインモードの交換がサポートされていることを示すべきである。

154 (条件付き) : 評価者は、TSS 及び RFC 5996 のセクション 2.23 に記述されるように NAT トラバーサル処理を行うよう TOE を設定しなければならない。評価者は IPsec 接続を開始し、NAT トラバーサルが成功することを判断しなければならない。

FCS_IPSEC_EXT.1.6

155 評価者は、IKEv1 または IKEv2 あるいはその両方のペイロードの暗号化にテスト対象の暗号スイートを用いるよう TOE を設定し、指示された暗号スイートを用いて暗号化されたペイロードのみを受け入れるように設定されたピアデバイスとの接続を確立しなければならない。評価者は、このアルゴリズムがネゴシエーションに用いられたものであることを確認すること。

FCS_IPSEC_EXT.1.7

156 この機能をテストするにあたって、評価者は双方の側が適切に設定されていることを保証する必要がある。RFC には以下のように記載されている。「IKEv1 と IKEv2 との違いは、IKEv1 SA のライフタイムがネゴシエーションされることである。IKEv2 においては、SA の両端が独自のライフタイムポリシーを SA に適用し、必要に応じて SA の鍵更新を行う責任がある。両端で異なるライフタイムポリシーが採用されている場合、その結果として、より短いライフタイムの側が常に鍵更新を要求することになるだろう。両端で同一のライフタイムポリシーが採用されている場合、同時に双方が鍵更新を開始することもあり得る (その結果、冗長な SA が生じることになる)。このようなことが起きる確率を減らすため、鍵更新要求のタイミングにはジッタを持たせるべきである。」

157 以下のテストはそれぞれ、FCS_IPSEC_EXT.1.5 プロトコル選択において選択された IKE のバージョンそれぞれについて行われなければならない。

a) テスト 1 (条件付き) : 評価者は、ガイダンス文書に従って許容されるバイト数に関して最大のライフタイムを設定しなければならない。評価者は、TOE のライフタイムを超えるバイトライフタイムをテストピアに設定しなければならない。評価者は TOE とテストピアとの間の SA を確立し、この SA の通過が許可されるバイト数を超過した際に、新たな SA がネゴシエーションされることを判断しなければならない。評価者は、TOE がフェーズ 1 ネゴシエーションを開始することを検証しなければならない。

b) テスト 2 (条件付き) : 評価者は、ガイダンス文書に従ってフェーズ 1 SA に 24 時間の最大のライフタイムを設定しなければならない。評価者は、TOE のライフタイムを超えるライフタイムをテストピアに設定しなければならない。評価者は TOE とテストピアとの間の SA を確立し、フェーズ 1 SA を 24 時間維持し、そして 24 時間が過ぎた際に、新たなフェーズ 1 SA がネゴシエーションされることを判断しなければならない。評価者は、TOE がフェーズ 1 ネゴシエーションを開始することを検証しなければならない。

FCS_IPSEC_EXT.1.8

158 この機能をテストするにあたって、評価者は双方の側が適切に設定されていることを保証する必要がある。RFC には以下のように記載されている。「IKEv1 と IKEv2 との違いは、IKEv1 SA のライフタイムがネゴシエーションされることである。IKEv2 においては、SA の両端が独自のライフタイムポリシーを SA に適用し、必要に応じて SA の鍵更新を行う責任がある。両端で異なるライフタイムポリシーが採用されている場合、その結果として、より短いライフタイムの側が常に鍵更新を要求することになるだろう。両端で同一のライフタイムポリシーが採用されている場合、同時に双方が鍵更新を開始することもあり得る (その結果、冗長な SA が生じることになる)。このようなことが起きる確率を減らすため、鍵更新要求のタイミングにはジッタを持たせるべきである。」

159 以下のテストはそれぞれ、FCS_IPSEC_EXT.1.5 プロトコル選択において選択された IKE のバージョンそれぞれについて行われなければならない。

a) テスト 1 (条件付き) : 評価者は、ガイダンス文書に従って許容されるバイト数に関して最大のライフタイムを設定しなければならない。評価者は、TOE のライフタイムを超えるバイトライフタイムをテストピアに設定しなければならない。評価者は TOE とテストピアとの間の SA を確立し、この SA の通過が許可されるバイト数を超過した際に、新たな SA がネゴシエーションされることを判断しなければならない。評価者は、TOE がフェーズ 2 ネゴシエーションを開始することを検証しなければならない。

b) テスト 2 (条件付き) : 評価者は、ガイダンス文書に従ってフェーズ 2 SA に 8 時間の最大のライフタイムを設定しなければならない。評価者は、TOE のライフタイムを超えるライフタイムをテストピアに設定しなければならない。評価者は TOE とテストピアとの間の SA を確立し、フェーズ 1 SA を 8 時間維持し、そして 8 時間が過ぎた際に、新たなフェーズ 2 SA がネゴシエーションされることを判断しなければならない。評価者は、TOE がフェーズ 2 ネゴシエーションを開始することを検証しなければならない。

FCS_IPSEC_EXT.1.10

160 (条件付き) 最初の選択が選ばれている場合、サポートされる DH グループそれぞれについて、各ノンスを生成するプロセスが TSS に記述されていることを、評価者はチェックして保証しなければならない。評価者は、本 PP の要件を満たす生成された乱数が使われること、及びノンスの長さが要件の規定を満たすことが、TSS に示されていることを検証しなければならない。

161 (条件付き) 2 番目の選択が選ばれている場合、サポートされる PRF ハッシュのそれぞれについて、各ノンスを生成するプロセスが TSS に記述されていることを、評価者はチェックして保証しなければならない。評価者は、本 PP の要件を満たす生成された乱数が使われること、及びノンスの長さが要件の規定を満たすことが、TSS に示されていることを検証しなければならない。

FCS_IPSEC_EXT.1.11

162 サポートされる DH グループそれぞれについて、評価者はその特定の DH グループを用いてすべてのサポートされる IKE プロトコルが成功裏に完了することをテストして保証しなければならない。

FCS_IPSEC_EXT.1.12

163 評価者は、単純にガイダンスに従って TOE を構成し、以下のテストを行う。

a) テスト 1：このテストは、サポートされる IKE の各バージョンについて行われなければならない。評価者は、要件に特定されたサポートされるアルゴリズムとハッシュ関数のそれぞれを用いて IPsec 接続のネゴシエーションを成功させなければならない。

b) テスト 2：このテストは、サポートされる IKE の各バージョンについて行われなければならない。評価者は、IKE SA に用いられるものよりも強度の大きい暗号化アルゴリズム (すなわち、IKE SA に用いられるものよりも大きい鍵長の対称アルゴリズム) を選択する ESP について SA の確立を試行しなければならない。そのような試行は失敗すべきである。

c) テスト 3：このテストは、サポートされる IKE の各バージョンについて行われなければならない。評価者は、要件に特定されたサポートされるアルゴリズムとハッシュ関数でないものを用いて IKE SA の確立を試行しなければならない。そのような試行は失敗すべきである。

d) テスト 4：このテストは、サポートされる IKE の各バージョンについて行われなければならない。評価者は、FCS_IPSEC_EXT.1.4 に特定されない暗号化アルゴリズムを選択する ESP (適切なパラメタが IKE SA の確立に用いられたことを前提として) について SA の確立を試行しなければならない。そのような試行は失敗すべきである。

FCS_IPSEC_EXT.1.13

164 効率性の観点から、ここで行われるテストは FIA_X509_EXT.1、FIA_X509_EXT.2 (IPsec 接続について)、及び FCS_IPSEC_EXT.1.1 のテストと組み合わせて行われてもよい。以下のテストは、上記 FCS_IPSEC_EXT.1.1 の選択において選択されたピア認証プロトコルそれぞれについて繰り返されなければならない。

a) テスト 1：評価者は、秘密鍵及び信頼済み CA によって署名された関連付けられた証明書を用いるように TOE を設定しなければならず、またピアとの IPsec 接続を確立させなければならない。

b) テスト 2 [条件付き]：評価者は、TOE 以外で事前共有鍵を生成し、ガイダンス文書に示されるようにピアとの IPsec 接続を確立させるために利用しなければならない。

FCS_IPSEC_EXT.1.14

165 評価者は、必要であれば、ガイダンス文書に従って期待される DN を設定しなければならない。評価者は、期待される DN にマッチしない DN を持つ信頼済み CA によって署名されたピア証明書を送信し、TOE が接続を拒否することを検証しなければならない。

2.2.11 FCS_SSHC_EXT.1 SSH クライアント

2.2.11.1 TSS

FCS_SSHC_EXT.1.2

166 評価者は、認証への利用が受容可能な公開鍵アルゴリズムの記述が TSS に含まれること、このリストが FCS_SSHC_EXT.1.5 に適合すること、そしてパスワードベースの認証手法もまた許可されることをチェックして保証しなければならない。

FCS_SSHC_EXT.1.3

167 評価者は、RFC 4253 の意味での「大きなパケット (large packets)」がどのように検出され取り扱われるか TSS に記述されていることをチェックしなければならない。

FCS_SSHC_EXT.1.4

168 評価者は、TSS のこのプロトコルの実装の記述をチェックして、オプションの特徴が特定され、またサポートされる暗号アルゴリズムも特定されていることを保証しなければならない。評価者は TSS をチェックして、特定された暗号化アルゴリズムがこのコンポーネントに列挙されたものと同一であることを保証しなければならない。

FCS_SSHC_EXT.1.5

169 評価者は、TSS のこのプロトコルの実装の記述をチェックして、オプションの特徴が特定され、またサポートされる公開鍵アルゴリズムも特定されていることを保証しなければならない。評価者は TSS をチェックして、特定された公開鍵アルゴリズムがこのコンポーネントに列挙されたものと同一であることを保証しなければならない。

FCS_SSHC_EXT.1.6

170 評価者は、TSS をチェックして、サポートされるデータ完全性アルゴリズムが列挙されていること、またそのリストがこのコンポーネントのリストと対応していることを保証しなければならない。

FCS_SSHC_EXT.1.7

171 評価者は、TSS をチェックして、サポートされる鍵交換アルゴリズムが列挙されていること、またそのリストがこのコンポーネントのリストと対応していることを保証しなければならない。

2.2.11.2 ガイダンス文書

FCS_SSHC_EXT.1.4

172 また評価者は、ガイダンス文書をチェックして、SSH が TSS の記述に適合するように TOE を設定するための指示 (例えば、TOE によって通知されるアルゴリズムのセットが、要件に合うよう制限されなければならないかもしれない) が含まれていることを保証しなければならない。

FCS_SSHC_EXT.1.5

173 また評価者は、ガイダンス文書をチェックして、SSH が TSS の記述に適合するように TOE を設定するための指示 (例えば、TOE によって通知されるアルゴリズムのセットが、要件に合うよう制限されなければならないかもしれない) が含まれていることを保証しなければならない。

FCS_SSHC_EXT.1.6

174 また評価者は、ガイダンス文書をチェックして、許可されるデータ完全性アルゴリズムのみが TOE との SSH 接続に用いられる (特に、MAC アルゴリズム「なし (none)」が許可されない) ことを保証する方法に関する管理者への指示が含まれていることを保証しなければならない。

FCS_SSHC_EXT.1.7

175 また評価者は、ガイダンス文書をチェックして、許可される鍵交換アルゴリズムのみが SSH 接続に用いられることを保証する方法に関する管理者への指示が含まれていることを保証しなければならない。

2.2.11.3 テスト

FCS_SSHC_EXT.1.2

176 テスト 1：評価者は、サポートされる公開鍵アルゴリズムそれぞれについて、その公開鍵アルゴリズムを用いた SSH サーバへの利用者接続の認証を TOE が

サポートすることを示さなければならない。このテストをサポートするために要求される設定アクティビティが存在する場合、それはガイダンス文書の指示に従って行われなければならない。

177 テスト 2 : ガイダンス文書を用いて、評価者は SSH サーバへのパスワードベースの認証を行うように TOE を設定し、認証子としてパスワードを用いて SSH サーバへの TOE による利用者の認証が成功することを実証しなければならない。

FCS_SSHC_EXT.1.3

178 評価者は、このコンポーネントに特定されたものよりも大きなパケットを TOE が受信すると、そのパケットが破棄されることを実証しなければならない。

FCS_SSHC_EXT.1.4

179 テスト 1:評価者は、要件に特定された暗号化アルゴリズムそれぞれを用いて、SSH 接続を確立しなければならない。テストの意図を満たすには、アルゴリズムのネゴシエーション成功を (通信路上で) 確認すれば十分である。

180 テスト 2 : 評価者は、SSH サーバを、3des-cbc 暗号化アルゴリズムのみを許し、その他の暗号化アルゴリズムを許さないように設定しなければならない。評価者は TOE から SSH サーバへの SSH 接続の確立を試行し、この接続が拒否されることを確認しなければならない。

FCS_SSHC_EXT.1.5

181 テスト 1:評価者は、要件に特定された公開鍵アルゴリズムそれぞれを用いて、SSH 接続を確立し、SSH サーバを TOE に対して認証しなければならない。テストの意図を満たすには、アルゴリズムのネゴシエーション成功を (通信路上で) 確認すれば十分である。

182 テスト 2 : 評価者は、SSH サーバを公開鍵アルゴリズム ssh-dsa のみを許し、その他の公開鍵アルゴリズムを許さないように設定しなければならない。評価者は TOE から SSH サーバへの SSH 接続の確立を試行し、この接続が拒否されることを確認しなければならない。

FCS_SSHC_EXT.1.6

183 テスト 1 : 評価者は、要件に特定されたデータ完全性アルゴリズムそれぞれを用いて、SSH 接続を確立しなければならない。テストの意図を満たすには、アルゴリズムのネゴシエーション成功を (通信路上で) 確認すれば十分である。

184 テスト 2 : 評価者は、SSH サーバを MAC アルゴリズム「なし (none)」のみを許可するように設定しなければならない。評価者は TOE から SSH サーバへの接続を試行し、この試行が失敗することを確認しなければならない。

185 テスト 3 : 評価者は、SSH サーバを MAC アルゴリズム hmac-md5 のみを許可するように設定しなければならない。評価者は TOE から SSH サーバへの接続を試行し、この試行が失敗することを確認しなければならない。

FCS_SSHC_EXT.1.7

186 テスト 1 : 評価者は、SSH サーバをすべての許可される鍵交換手法を許可するように設定しなければならない。評価者は許可される鍵交換手法それぞれを用いて TOE から SSH サーバへの接続を試行し、それぞれの試行が成功することを確認しなければならない。

FCS_SSHC_EXT.1.8

187 評価者は、TOE を鍵更新が行われた際にログエントリを作成するように設定しなければならない。評価者は SSH クライアントから TOE へ接続し、クライアントから TOE へ 2^28 個のパケットを送信させ、その後監査ログをレビューして鍵更新が行われたことを保証しなければならない。

FCS_SSHC_EXT.1.9

188 テスト 1 : 評価者は、認識済み SSH サーバホスト鍵の TOE のリストのすべてのエントリ及び、選択されている場合には信頼済み認証局の TOE のリストのすべてのエントリを削除しなければならない。評価者は、TOE から SSH サーバへの接続を開始しなければならない。評価者は、TOE がその接続を拒否するか、その SSH サーバの公開鍵 (鍵のバイト列そのもの、または任意の許可されるハッシュアルゴリズムを用いた鍵のハッシュ) を表示するかのどちらかであって、接続を継続する前にその鍵を受け入れるか拒否するかのプロンプトを利用者へ表示することを保証しなければならない。

189 テスト 2 : 評価者は、ホスト名を公開鍵と関連付けるエントリを TOE のローカルなデータベースへ追加しなければならない。評価者は、対応する SSH サーバ上で、サーバのホスト鍵を異なるホスト鍵と置き換えなければならない。評価者はパスワードベース認証を用いて TOE から SSH サーバへの接続を開始しなければならず、TOE がその接続を拒否することを保証しなければならず、そしてパスワードが SSH サーバへ送信されなかったことを保証しなければならない (例えば、受信したパスワードを出力するようなデバッグ機能を SSH サーバへ装備することによって)。

2.2.12 FCS_SSHS_EXT.1 SSH サーバ

2.2.12.1 TSS

FCS_SSHS_EXT.1.2

190 評価者は、認証への利用が受容可能な公開鍵アルゴリズムの記述が TSS に含まれること、このリストが FCS_SSHS_EXT.1.5 に適合すること、そしてパスワードベースの認証手法もまた許可されることをチェックして保証しなければならない。

FCS_SSHS_EXT.1.3

191 評価者は、RFC 4253 の意味での「大きなパケット (large packets)」がどのように検出され取り扱われるか TSS に記述されていることをチェックしなければならない。

FCS_SSHS_EXT.1.4

192 評価者は、TSS のこのプロトコルの実装の記述をチェックして、オプションの特徴が特定され、またサポートされる暗号アルゴリズムも特定されていること

を保証しなければならない。評価者は、TSS をチェックして、特定された暗号化アルゴリズムがこのコンポーネントに列挙されたものと同一であることを保証しなければならない。

FCS_SSHS_EXT.1.5

193 評価者は、TSS のこのプロトコルの実装の記述をチェックして、オプションの特徴が特定され、またサポートされる公開鍵アルゴリズムも特定されていることを保証しなければならない。評価者は、TSS をチェックして、特定された公開鍵アルゴリズムがこのコンポーネントに列挙されたものと同一であることを保証しなければならない。

FCS_SSHS_EXT.1.6

194 評価者は、TSS をチェックして、サポートされるデータ完全性アルゴリズムが列挙されていること、またそのリストがこのコンポーネントのリストと対応していることを保証しなければならない。

FCS_SSHS_EXT.1.7

195 評価者は、TSS をチェックして、サポートされる鍵交換アルゴリズムが列挙されていること、またそのリストがこのコンポーネントのリストと対応していることを保証しなければならない。

2.2.12.2 ガイダンス文書

FCS_SSHS_EXT.1.4

196 また評価者は、ガイダンス文書をチェックして、SSH が TSS の記述に適合するように TOE を設定するための指示 (例えば、TOE によって通知されるアルゴリズムのセットが、要件に合うよう制限されなければならないかもしれない) が含まれていることを保証しなければならない。

FCS_SSHS_EXT.1.5

197 また評価者は、ガイダンス文書をチェックして、SSH が TSS の記述に適合するように TOE を設定するための指示 (例えば、TOE によって通知されるアルゴリズムのセットが、要件に合うよう制限されなければならないかもしれない) が含まれていることを保証しなければならない。

FCS_SSHS_EXT.1.6

198 また評価者は、ガイダンス文書をチェックして、許可されるデータ完全性アルゴリズムのみが TOE との SSH 接続に用いられる (特に、MAC アルゴリズム「なし (none)」が許可されない) ことを保証する方法に関する管理者への指示が含まれていることを保証しなければならない。

FCS_SSHS_EXT.1.7

199 また評価者は、ガイダンス文書をチェックして、許可される鍵交換アルゴリズムのみが SSH 接続に用いられることを保証する方法に関する管理者への指示が含まれていることを保証しなければならない。

2.2.12.3 テスト

FCS_SSHS_EXT.1.2

200 テスト 1 : 評価者は、サポートされる公開鍵アルゴリズムそれぞれについて、その公開鍵アルゴリズムを用いた利用者接続の認証を TOE がサポートすることを示さなければならない。このテストをサポートするために要求される設定アクティビティが存在する場合、それはガイダンス文書の指示に従って行われなければならない。

201 テスト 2 : 評価者は、TOE のサポートする 1 つの公開鍵アルゴリズムを選ばなければならない。評価者は、認証のために公開鍵を認識するように TOE を設定することなしにそのアルゴリズムの新たな鍵ペアを生成しなければならない。評価者は、SSH クライアントを用いて新しい新たな鍵ペアと共に TOE への接続を試行し、その認証が失敗することを実証しなければならない。

202 テスト 3 : ガイダンス文書を用いて、評価者はパスワードベースの認証を受け入れるように TOE を構成し、認証子としてパスワードを用いて SSH 上で TOE への利用者の認証が成功することを実証しなければならない。

203 テスト 4 : 評価者は、SSH クライアントを用いて、正しくないパスワードを入力して TOE への認証を試行し、その認証が失敗することを実証しなければならない。

FCS_SSHS_EXT.1.3

204 評価者は、このコンポーネントに特定されたものよりも大きなパケットを TOE が受信すると、そのパケットが破棄されることを実証しなければならない。

FCS_SSHS_EXT.1.4

205 テスト 1:評価者は、要件に特定された暗号化アルゴリズムそれぞれを用いて、SSH 接続を確立しなければならない。テストの意図を満たすには、アルゴリズムのネゴシエーション成功を (通信路上で) 確認すれば十分である。

206 テスト 2 : 評価者は SSH クライアントを、3des-cbc 暗号化アルゴリズムのみを許し、その他の暗号化アルゴリズムを許さないように設定しなければならない。評価者は SSH クライアントから TOE への SSH 接続の確立を試行し、この接続が拒否されることを確認しなければならない。

FCS_SSHS_EXT.1.5

207 テスト 1:評価者は、要件に特定された公開鍵アルゴリズムそれぞれを用いて、SSH 接続を確立し、TOE を SSH クライアントに対して認証しなければならない。テストの意図を満たすには、アルゴリズムのネゴシエーション成功を (通信路上で) 確認すれば十分である。

208 テスト 2 : 評価者は、SSH クライアントを公開鍵アルゴリズム ssh-dsa のみを許し、その他の公開鍵アルゴリズムを許さないように設定しなければならない。評価者は、SSH クライアントから TOE への SSH 接続の確立を試行し、この接続が拒否されることを確認しなければならない。

FCS_SSHS_EXT.1.6

209 テスト 1 : 評価者は、要件に特定されたデータ完全性アルゴリズムそれぞれを用いて、SSH 接続を確立しなければならない。テストの意図を満たすには、アルゴリズムのネゴシエーション成功を (通信路上で) 確認すれば十分である。

210 テスト 2 : 評価者は、SSH クライアントを MAC アルゴリズム「なし (none)」のみを許可するように設定しなければならない。評価者は SSH クライアントから TOE への接続を試行し、この試行が失敗することを確認しなければならない。

211 テスト 3 : 評価者は、SSH クライアントを MAC アルゴリズム hmac-md5 のみを許可するように設定しなければならない。評価者は SSH クライアントから TOE への接続を試行し、この試行が失敗することを確認しなければならない。

FCS_SSHS_EXT.1.7

212 テスト 1 : 評価者は、SSH クライアントを diffie-hellman-group1-sha1 鍵交換のみを許可するように設定しなければならない。評価者は SSH クライアントから TOE への接続を試行し、この試行が失敗することを確認しなければならない。

213 テスト 2 : 許可される鍵交換手法それぞれについて、評価者は SSH をその鍵交換手法のみを許可するように設定し、クライアントから TOE への接続を試行し、そしてこの試行が成功することを確認しなければならない。

FCS_SSHS_EXT.1.8

214 評価者は、TOE を鍵更新が行われた際にログエントリを作成するように設定しなければならない。評価者は、SSH クライアントから TOE へ接続し、クライアントから TOE へ 2^28 個のパケットを送信させ、その後監査ログをレビューして鍵更新が行われたことを保証しなければならない。

2.2.13 FCS_TLSC_EXT.1 拡張：TLS クライアントプロトコル

2.2.13.1 TSS

FCS_TLSC_EXT.1.1

215 評価者は、TSS のこのプロトコルの実装の記述をチェックして、サポートされる暗号スイートが特定されていることを保証しなければならない。評価者は、TSS をチェックして、特定された暗号スイートがこのコンポーネントに列挙されたものを含むことを保証しなければならない。

FCS_TLSC_EXT.1.2

216 評価者は、どの種類の参照識別子がサポートされているか (例えば共通名、DNS 名、URI 名、サービス名、またはその他のアプリケーション特有のサブジェクトの別名) ならびに IP アドレス及びワイルドカードがサポートされているかどうかを含め、管理者／アプリケーションに設定された参照識別子からすべての参照識別子を確立するクライアントの手法が TSS に記述されていることを保証しなければならない。評価者は、この記述に TOE によって Certificate Pinning がサポートされるか、または利用されるかどうか、及びその方法が特定されていることを保証しなければならない。

FCS_TLSC_EXT.1.4

217 評価者は、Supported Elliptic Curves Extension について、そして要求されるふるまいがデフォルトで実施されるのか設定され得るのかのどちらであるか、TSS に記述されていることを検証しなければならない。

2.2.13.2 ガイダンス文書

FCS_TLSC_EXT.1.1

218 また評価者は、ガイダンス文書をチェックして、TLS が TSS の記述と適合するように TOE を設定するための指示が含まれることを保証しなければならない。

FCS_TLSC_EXT.1.2

219 評価者は、TLS における証明書有効性確認の目的に用いられる参照識別子を設定するための指示が AGD ガイダンスに含まれていることを検証しなければならない。

FCS_TLSC_EXT.1.4

220 この要件を満たすために Supported Elliptic Curves Extension が設定されなければならないことが TSS に示されている場合、評価者は AGD ガイダンスに Supported Elliptic Curves Extension の設定が含まれることを検証しなければならない。

2.2.13.3 テスト

FCS_TLSC_EXT.1.1

221 テスト 1 : 評価者は、要件に特定された暗号スイートのそれぞれを用いて、TLS 接続を確立しなければならない。この接続は、より高位のプロトコルの確立の一部として確立されてもよい (例えば、HTTPS セションの一部として)。テストの意図を満たすには、暗号スイートのネゴシエーション成功を確認すれば十分であり、利用されている暗号スイート (例えば、暗号アルゴリズムが 128 ビット AES であって 256 ビット AES でないこと) を識別するために暗号化されたトラフィックの特徴を検査する必要はない。

222 テスト 2 : 評価者は、extendedKeyUsage フィールドにサーバ認証目的を含むサーバ証明書を持ったサーバを用いて接続を確立する試行を行い、接続が確立されることを検証しなければならない。次に評価者は、extendedKeyUsage フィールドにサーバ認証目的を含まないこと以外は有効なサーバ証明書をクライアントが拒否し、接続が確立されないことを検証する。理想的には、2 つの証明書は extendedKeyUsage フィールドを除いて同一であるべきである。

223 テスト 3 : 評価者は、サーバによって選択された暗号スイートとマッチしないサーバ証明書を TLS 接続中に送信しなければならない (例えば、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートを利用しているのに ECDSA 証明書を送信する)。評価者は、TOE がサーバの証明書ハンドシェイクメッセージを受信した後に切断することを検証しなければならない 。

224 テスト 4 : 評価者は、TLS_NULL_WITH_NULL_NULL 暗号スイートを選択するようサーバを設定し、クライアントが接続を拒否することを検証しなければな

らない。FCS_TLSS_EXT.1.1 または FCS_TLSS_EXT.2.1 のテスト 2 を、このテストの代用として用いることができる。

225 テスト 5：評価者は、トラフィックに以下の改変を行う：

a) ServerHello のサーバによって選択される TLS バージョンを、サポートされない TLS バージョン (例えば 03 04 の 2 バイトによって表現される 1.3) に変更し、クライアントが接続を拒否することを検証する。

b) ServerHello ハンドシェイクメッセージでのサーバのノンスの少なくとも 1 バイトを改変して、ServerKeyExchange ハンドシェイクメッセージをクライアントが拒否すること (DHE または ECDHE 暗号スイートの場合) あるいはクライアントの Finished ハンドシェイクメッセージをサーバが拒否することを検証する。

c) ServerHello ハンドシェイクメッセージでのサーバの選択された暗号スイートを、ClientHello ハンドシェイクメッセージに提示されない暗号スイートに改変する。評価者は、クライアントが ServerHello を受信した後に接続を拒否することを検証しなければならない 。

d) サーバの KeyExchange ハンドシェイクメッセージの署名ブロックを改変して、クライアントが ServerKeyExchange の受信後に接続を拒否することを検証する。

e) Server Finished ハンドシェイクメッセージの 1 バイトを改変して、受信後にクライアントが fatal alert を送信しアプリケーションデータを全く送信しないことを検証する。

f) クライアントが ChangeCipherSpec メッセージを発行した後にサーバから歪曲されたメッセージを送信し、クライアントが接続を拒否することを検証する。

FCS_TLSC_EXT.1.2

226 評価者は、AGD ガイダンスに従って参照識別子を設定し、TLS 接続中に以下のテストを行わなければならない：

a) テスト 1：評価者は、参照識別子にマッチする識別子をサブジェクトの別名 (SAN) にも共通名 (CN) にも含まないサーバ証明書を提示しなければならない。評価者は、接続が失敗することを検証しなければならない。

b) テスト 2：評価者は、参照識別子にマッチする CN を含み、SAN 拡張を含むが、参照識別子にマッチする識別子を SAN に含まないサーバ証明書を提示しなければならない。評価者は、接続が失敗することを検証しなければならない。評価者は、SAN 種別のそれぞれについてこのテストを繰り返さなければならない。

c) テスト 3 : 評価者は、参照識別子にマッチする CN を含み、SAN 拡張を含まないサーバ証明書を提示しなければならない。評価者は、接続が成功することを検証しなければならない。

d) テスト 4 : 評価者は、参照識別子にマッチしない CN を含むが、SAN にはマッチする識別子を含むサーバ証明書を提示しなければならない。評価者は、接続が成功することを検証しなければならない。

e) テスト 5 : 評価者は、参照識別子のサポートされる種別それぞれについて、以下のワイルドカードテストを行わなければならない :

1) 評価者は、提示された識別子の左端のラベル以外にワイルドカードを含む (例えば、foo.*.example.com) サーバ証明書を提示し、接続が失敗することを検証しなければならない。

2) 評価者は、左端のラベルにワイルドカードを含む (例えば、*.example.com) サーバ証明書を提示しなければならない。評価者は、左端に単一のラベルを持つ参照識別子 (例えば、foo.example.com) を設定し、接続が成功することを検証しなければならない。評価者は、証明書の左端のラベルを持たない参照識別子 (例えば、example.com) を設定し、接続が失敗することを検証しなければならない。評価者は、左端に 2 つのラベルを持つ参照識別子 (例えば、bar.foo.example.come) を設定し、接続が失敗することを検証しなければならない。

f) テスト 6 : [条件付き] URI またはサービス名参照識別子がサポートされている場合、評価者は DNS 名及びサービス識別子を設定しなければならない。評価者は、SAN の URIName または SRVName フィールドに正しい DNS 名及びサービス識別子を含むサーバ証明書を提示し、接続が成功することを検証しなければならない。評価者は、間違ったサービス識別子 (しかし正しい DNS 名) を用いてこのテストを繰り返し、接続が失敗することを検証しなければならない。

g) テスト 7 : [条件付き] Pinning された証明書がサポートされている場合、評価者は Pinning された証明書にマッチしない証明書を提示し、接続が失敗することを検証しなければならない。

FCS_TLSC_EXT.1.3

227 テスト 1 : 評価者は、有効な認証パスのない証明書を使用すると、その機能が失敗することを実証しなければならない。管理ガイダンスを利用して、次に評価者はその機能で使われる証明書の検証に必要とされる 1 つまたは複数の証明書をロードし、その機能が成功することを実証しなければならない。証明書の有効性が確認され高信頼チャネルが確立された場合、テストは合格である。次に評価者はこれらの証明書の 1 つを削除して、証明書の有効性が確認されず高信頼チャネルが確立されないことを示さなければならない。

FCS_TLSC_EXT.1.4

228 テスト 1：評価者は、サポートされない曲線 (例えば P-192) を用いて TLS 接続中に ECDHE 鍵交換を行うようサーバを構成しなければならず、そして TOE がサーバの ServerKeyExchange ハンドシェイクメッセージを受信した後に切断することを検証しなければならない 。

2.2.14 FCS_TLSC_EXT.2 拡張：認証を伴う TLS クライアントプロトコル

2.2.14.1 TSS

FCS_TLSC_EXT.2.1

229 評価者は、TSS のこのプロトコルの実装の記述をチェックして、サポートされる暗号スイートが特定されていることを保証しなければならない。評価者は、TSS をチェックして、特定された暗号スイートがこのコンポーネントに列挙されたものを含むことを保証しなければならない。

FCS_TLSC_EXT.2.2

230 評価者は、どの種類の参照識別子がサポートされているか (例えば共通名、DNS 名、URI 名、サービス名、またはその他のアプリケーション特有のサブジェクトの別名) ならびに IP アドレス及びワイルドカードがサポートされているかどうかを含め、管理者／アプリケーションに設定された参照識別子からすべての参照識別子を確立するクライアントの手法が TSS に記述されていることを保証しなければならない。評価者は、この記述に TOE によって Certificate Pinning がサポートされるか、または利用されるかどうか、及びその方法が特定されていることを保証しなければならない。

FCS_TLSC_EXT.2.4

231 評価者は、Supported Elliptic Curves Extension について、そして要求されるふるまいがデフォルトで実施されるのか設定され得るのかのどちらであるか、TSS に記述されていることを検証しなければならない。

FCS_TLSC_EXT.2.5

232 評価者は、FIA_X509_EXT.2.1 によって要求される TSS 記述に、TLS 相互認証のためのクライアント側証明書の利用が含まれることを保証しなければならない。

2.2.14.2 ガイダンス文書

FCS_TLSC_EXT.2.1

233 また評価者は、ガイダンス文書をチェックして、TLS が TSS の記述と適合するように TOE を設定するための指示が含まれることを保証しなければならない。

FCS_TLSC_EXT.2.2

234 評価者は、TLS における証明書有効性確認の目的に用いられる参照識別子を設定するための指示が AGD ガイダンスに含まれていることを検証しなければならない。

FCS_TLSC_EXT.2.4

235 この要件を満たすために Supported Elliptic Curves Extension が設定されなければならないことが TSS に示されている場合、評価者は AGD ガイダンスに Supported Elliptic Curves Extension の設定が含まれることを検証しなければならない。

FCS_TLSC_EXT.2.5

236 評価者は、FIA_X509_EXT.2.1 によって要求される AGD ガイダンスに、TLS 相互認証のためのクライアント側証明書を設定するための指示が含まれることを検証しなければならない。

2.2.14.3 テスト

FCS_TLSC_EXT.2.1

237 テスト 1 : 評価者は、要件に特定された暗号スイートのそれぞれを用いて、TLS 接続を確立しなければならない。この接続は、より高位のプロトコルの確立の一部として確立されてもよい (例えば、HTTPS セションの一部として)。テストの意図を満たすには、暗号スイートのネゴシエーション成功を確認すれば十分であり、利用されている暗号スイート (例えば、暗号アルゴリズムが 128 ビット AES であって 256 ビット AES でないこと) を識別するために暗号化されたトラフィックの特徴を検査する必要はない。

238 テスト 2 : 評価者は、extendedKeyUsage フィールドにサーバ認証目的を含むサーバ証明書を持ったサーバを用いて接続を確立する試行を行い、接続が確立されることを検証しなければならない。次に評価者は、extendedKeyUsage フィールドにサーバ認証目的を含まないこと以外は有効なサーバ証明書をクライアントが拒否し、接続が確立されないことを検証する。理想的には、2 つの証明書は extendedKeyUsage フィールドを除いて同一であるべきである。

239 テスト 3 : 評価者は、サーバによって選択された暗号スイートとマッチしないサーバ証明書を TLS 接続中に送信しなければならない (例えば、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートを利用しているのに ECDSA 証明書を送信する。) 評価者は、TOE がサーバの証明書ハンドシェイクメッセージを受信した後に切断することを検証しなければならない 。

240 テスト 4 : 評価者は、TLS_NULL_WITH_NULL_NULL 暗号スイートを選択するようサーバを設定し、クライアントが接続を拒否することを検証しなければならない。FCS_TLSS_EXT.1.1 または FCS_TLSS_EXT.2.1 のテスト 2 を、このテストの代用として用いることができる。

241 テスト 5 : 評価者は、トラフィックに以下の改変を行う：

a) ServerHello のサーバによって選択される TLS バージョンを、サポートされない TLS バージョン (例えば 03 04 の 2 バイトによって表現される 1.3) に変更し、クライアントが接続を拒否することを検証する。

b) ServerHello ハンドシェイクメッセージのサーバのノンスの少なくとも 1 バイトを改変して、ServerKeyExchange ハンドシェイクメッセージをクライアントが拒否すること (DHE または ECDHE 暗号スイートの場合) あるいはクライアントの Finished ハンドシェイクメッセージをサーバが拒否することを検証する。

c) ServerHello ハンドシェイクメッセージのサーバの選択された暗号スイートを、ClientHello ハンドシェイクメッセージに提示されない暗号スイートに改変する。評価者は、クライアントが ServerHello を受信した後に接続を拒否することを検証しなければならない 。

d) サーバの KeyExchange ハンドシェイクメッセージの署名ブロックを改変して、クライアントが ServerKeyExchange の受信後に接続を拒否することを検証する。

e) Server Finished ハンドシェイクメッセージの 1 バイトを改変して、受信後にクライアントが fatal alert を送信しアプリケーションデータを全く送信しないことを検証する。

f) クライアントが ChangeCipherSpec メッセージを発行した後にサーバから歪曲されたメッセージを送信し、クライアントが接続を拒否することを検証する。

FCS_TLSC_EXT.2.2

242 評価者は、AGD ガイダンスに従って参照識別子を設定し、TLS 接続中に以下のテストを行わなければならない：

a) テスト 1：評価者は、参照識別子にマッチする識別子をサブジェクトの別名 (SAN) にも共通名 (CN) にも含まないサーバ証明書を提示しなければならない。評価者は、接続が失敗することを検証しなければならない。

b) テスト 2：評価者は、参照識別子にマッチする CN を含み、SAN 拡張を含むが、参照識別子にマッチする識別子を SAN に含まないサーバ証明書を提示しなければならない。評価者は、接続が失敗することを検証しなければならない。評価者は、SAN 種別のそれぞれについてこのテストを繰り返さなければならない。

c) テスト 3：評価者は、参照識別子にマッチする CN を含み、SAN 拡張を含まないサーバ証明書を提示しなければならない。評価者は、接続が成功することを検証しなければならない。

d) テスト 4：評価者は、参照識別子にマッチしない CN を含むが、SAN にはマッチする識別子を含むサーバ証明書を提示しなければならない。評価者は、接続が成功することを検証しなければならない。

e) テスト 5：評価者は、参照識別子のサポートされる種別それぞれについて、以下のワイルドカードテストを行わなければならない：

1) 評価者は、提示された識別子の左端のラベル以外にワイルドカードを含む (例えば、foo.*.example.com) サーバ証明書を提示し、接続が失敗することを検証しなければならない。

2) 評価者は、左端のラベルにワイルドカードを含む (例えば、*.example.com) サーバ証明書を提示しなければならない。評価者は、左端に単一のラベルを持つ参照識別子 (例えば、foo.example.com) を設定し、接続が成功することを検証しなければならない。評価者は、証明書の左端のラベルを持たない参照識別子 (例えば、example.com) を設定し、接続が失敗することを検証しなければならない。評価者は、左端に 2 つのラベルを持つ参照識別子 (例えば、bar.foo.example.come) を設定し、接続が失敗することを検証しなければならない。

f) テスト 6： [条件付き] URI またはサービス名参照識別子がサポートされている場合、評価者は DNS 名及びサービス識別子を設定しなければならない。評価者は、SAN の URIName または SRVName フィールドに正しい DNS 名及びサービス識別子を含むサーバ証明書を提示し、接続が成功することを検証しなければならない。評価者は、間違ったサービス識別子 (しかし正しい DNS 名) を用いてこのテストを繰り返し、接続が失敗することを検証しなければならない。

g) テスト 7： [条件付き] Pinning された証明書がサポートされている場合、評価者は Pinning された証明書にマッチしない証明書を提示し、接続が失敗することを検証しなければならない。

FCS_TLSC_EXT.2.3

243 テスト 1：評価者は、有効な認証パスのない証明書を使用すると、その機能が失敗することを実証しなければならない。管理ガイダンスを利用して、次に評価者はその機能で使われる証明書の検証に必要とされる 1 つまたは複数の証明書をロードし、その機能が成功することを実証しなければならない。証明書の有効性が確認され高信頼チャネルが確立された場合、テストは合格である。次に評価者はこれらの証明書の 1 つを削除して、証明書の有効性が確認されず高信頼チャネルが確立されないことを示さなければならない。

FCS_TLSC_EXT.2.4

244 テスト 1：評価者は、サポートされない曲線 (例えば P-192) を用いて TLS 接続中に ECDHE 鍵交換を行うようサーバを構成しなければならず、そして TOE がサーバの ServerKeyExchange ハンドシェイクメッセージを受信した後に切断することを検証しなければならない 。

FCS_TLSC_EXT.2.5

245 テスト 1：評価者は、トラフィックに以下の改変を行わなければならない：

a) 相互認証を要求するようサーバを設定し、次にサーバの CertificateRequest ハンドシェイクメッセージの CA フィールド中の 1 バイトを改変する。改変された CA フィールドは、クライアントの証明書の署名に用いられた CA であってはならない。評価者は、接続が失敗することを検証しなければならない。

2.2.15 FCS_TLSS_EXT.1 拡張：TLS サーバプロトコル

2.2.15.1 TSS

FCS_TLSS_EXT.1.1

246 評価者は、TSS のこのプロトコルの実装の記述をチェックして、サポートされる暗号スイートが特定されていることを保証しなければならない。評価者は、TSS をチェックして、特定された暗号スイートがこのコンポーネントに列挙されたものと同一であることを保証しなければならない。

FCS_TLSS_EXT.1.2

247 評価者は、古い SSL 及び TLS のバージョンの拒否の記述が TSS に含まれることを検証しなければならない。

FCS_TLSS_EXT.1.3

248 評価者は、サーバ鍵交換メッセージの鍵共有パラメタが TSS に記述されていることを検証しなければならない。

2.2.15.2 ガイダンス文書

FCS_TLSS_EXT.1.1

249 また評価者は、ガイダンス文書をチェックして、TLS が TSS の記述に適合するように TOE を構成するための指示 (例えば、TOE によって通知される暗号スイートのセットが、要件に合うよう制限されなければならないかもしれない) が含まれていることを保証しなければならない。

FCS_TLSS_EXT.1.2

250 評価者は、要件を満たすために必要な任意の設定が AGD ガイダンスに含まれなければならないことを検証しなければならない。

FCS_TLSS_EXT.1.3

251 評価者は、要件を満たすために必要な任意の設定が AGD ガイダンスに含まれなければならないことを検証しなければならない。

2.2.15.3 テスト

FCS_TLSS_EXT.1.1

252 テスト 1 : 評価者は、要件に特定された暗号スイートのそれぞれを用いて、TLS 接続を確立しなければならない。この接続は、より高位のプロトコルの確立の一部として確立されてもよい (例えば、HTTPS セションの一部として)。テストの意図を満たすには、暗号スイートのネゴシエーション成功を確認すれば十分であり、利用されている暗号スイート (例えば、暗号アルゴリズムが 128 ビット AES であって 256 ビット AES でないこと) を識別するために暗号化されたトラフィックの特徴を検査する必要はない。

253 テスト 2 : 評価者は、サーバの ST の暗号スイートのいずれをも含まない暗号スイートのリストと共に Client Hello をサーバへ送信し、サーバが接続を拒否することを検証しなければならない。さらに、評価者は TLS_NULL_WITH_NULL_NULL 暗号スイートのみを含む Client Hello をサーバ

へ送信し、サーバが接続を拒否することを検証しなければならない。

254 テスト 3：評価者は、クライアントを用いてサーバによって選択された暗号スイートとマッチしない鍵交換メッセージを TLS 接続中に送信しなければならない (例えば、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートを利用しているのに ECDSA 鍵交換を送信したり、ECDSA 暗号スイートのいずれかを使用しているのに RSA 鍵交換を送信したりする。) 評価者は、TOE が鍵交換メッセージを受信した後に切断することを検証しなければならない 。

255 テスト 4：評価者は、トラフィックに以下の改変を行わなければならない：

a) Client Hello ハンドシェイクメッセージのクライアントのノンスの 1 バイトを改変して、クライアントの Certificate Verify ハンドシェイクメッセージをサーバが拒否すること (相互認証を用いる場合) あるいはクライアントの Finished ハンドシェイクメッセージをサーバが拒否することを検証する。

b) クライアントの Key Exchange ハンドシェイクメッセージの署名ブロックを改変して、クライアントの Certificate Verify ハンドシェイクメッセージをサーバが拒否すること (相互認証を用いる場合) あるいはクライアントの Finished ハンドシェイクメッセージをサーバが拒否することを検証する。

c) Client Finished ハンドシェイクメッセージの 1 バイトを改変して、サーバが接続を拒否しアプリケーションデータを全く送信しないことを検証する。

d) クライアントが ChangeCipherSpec メッセージを送信する前にクライアントから Finished メッセージを送信することによって fatal alert を生成させた後、先ほどのテストからのセション識別子と共に Client Hello を送信し、サーバが接続を拒否することを検証する。

e) クライアントが ChangeCipherSpec メッセージを発行した後にクライアントから改変されたメッセージを送信し、サーバが接続を拒否することを検証する。

FCS_TLSS_EXT.1.2

256 評価者は、バージョン SSL 1.0 での接続を要求する Client Hello を送信し、サーバが接続を拒否することを検証しなければならない。評価者はこのテストを SSL 2.0、SSL 3.0、TLS 1.0、及び選択された TLS があればそれを用いて繰り返さなければならない。

FCS_TLSS_EXT.1.3

257 評価者は、ECDHE 暗号スイート及び設定された曲線を用いて接続を試行し、そしてパケットアナライザを用いて Key Exchange メッセージの鍵共有パラメタが設定されたものであることを検証しなければならない。(サイズが、設定された曲線に期待されるサイズと一致することを判断すれば十分である。) 評価者はこのテストを、サポートされる NIST 楕円曲線のそれぞれとサポートされる Diffie-Hellman 鍵長のそれぞれについて、繰り返さなければならない。

2.2.16 FCS_TLSS_EXT.2 拡張：相互認証を伴う TLS サーバプロトコル

2.2.16.1 TSS

FCS_TLSS_EXT.2.1

258 評価者は、TSS のこのプロトコルの実装の記述をチェックして、サポートされる暗号スイートが特定されていることを保証しなければならない。評価者は TSS をチェックして、特定された暗号スイートがこのコンポーネントに列挙されたものと同一であることを保証しなければならない。

FCS_TLSS_EXT.2.2

259 評価者は、古い SSL 及び TLS のバージョンの拒否の記述が TSS に含まれることを検証しなければならない。

FCS_TLSS_EXT.2.3

260 評価者は、サーバ鍵交換メッセージの鍵共有パラメタが TSS に記述されていることを検証しなければならない。

FCS_TLSS_EXT.2.4 及び FCS_TLSS_EXT.2.5

261 評価者は、FIA_X509_EXT.2.1 によって要求される TSS 記述に、TLS 相互認証のためのクライアント側証明書の利用が含まれることを保証しなければならない。

FCS_TLSS_EXT.2.6

262 評価者は、証明書の DN または SAN が期待される識別子と比較される方法が TSS に記述されていることを検証しなければならない。

2.2.16.2 ガイダンス文書

FCS_TLSS_EXT.2.1

263 また評価者は、ガイダンス文書をチェックして、TLS が TSS の記述に適合するように TOE を構成するための指示 (例えば、TOE によって通知される暗号スイートのセットが、要件に合うよう制限されなければならないかもしれない) が含まれていることを保証しなければならない。

FCS_TLSS_EXT.2.2

264 評価者は、要件を満たすために必要な任意の設定が AGD ガイダンスに含まれなければならないことを検証しなければならない。

FCS_TLSS_EXT.2.3

265 評価者は、要件を満たすために必要な任意の設定が AGD ガイダンスに含まれなければならないことを検証しなければならない。

FCS_TLSS_EXT.2.4 及び FCS_TLSS_EXT.2.5

266 評価者は、FIA_X509_EXT.2.1 によって要求される AGD ガイダンスに、TLS 相互認証のためのクライアント側証明書を設定するための指示が含まれることを検証しなければならない。

FCS_TLSS_EXT.2.6

267 DN が自動的にドメイン名または IP アドレス、利用者名、もしくは電子メールアドレスと比較されない場合には、評価者はその接続に期待される DN またはディレクトリサーバの設定が AGD ガイダンスに含まれることを保証しなければならない。

2.2.16.3 テスト

FCS_TLSS_EXT.2.1

268 テスト 1 : 評価者は、要件に特定された暗号スイートのそれぞれを用いて、TLS 接続を確立しなければならない。この接続は、より高位のプロトコルの確立の一部として確立されてもよい (例えば、HTTPS セションの一部として)。テストの意図を満たすには、暗号スイートのネゴシエーション成功を確認すれば十分であり、利用されている暗号スイート (例えば、暗号アルゴリズムが 128 ビット AES であって 256 ビット AES でないこと) を識別するために暗号化されたトラフィックの特徴を検査する必要はない。

269 テスト 2 : 評価者は、サーバの ST の暗号スイートのいずれをも含まない暗号スイートのリストと共に Client Hello をサーバへ送信し、サーバが接続を拒否することを検証しなければならない。さらに、評価者は、TLS_NULL_WITH_NULL_NULL 暗号スイートのみを含む Client Hello をサーバへ送信し、サーバが接続を拒否することを検証しなければならない。

270 テスト 3 : 評価者は、クライアントを用いてサーバによって選択された暗号スイートとマッチしない鍵交換メッセージを TLS 接続中に送信しなければならない (例えば、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートを利用しているのに ECDSA 鍵交換を送信したり、ECDSA 暗号スイートのいずれかを使用しているのに RSA 鍵交換を送信したりする。) 評価者は、TOE が鍵交換メッセージを受信した後に切断することを検証しなければならない 。

271 テスト 4 : 評価者は、トラフィックに以下の改変を行わなければならない :

a) Client Hello ハンドシェイクメッセージのクライアントのノンスの 1 バイトを改変して、クライアントの Certificate Verify ハンドシェイクメッセージをサーバが拒否すること (相互認証を用いる場合) あるいはクライアントの Finished ハンドシェイクメッセージをサーバが拒否することを検証する。

b) クライアントの Key Exchange ハンドシェイクメッセージの署名ブロックを改変して、クライアントの Certificate Verify ハンドシェイクメッセージをサーバが拒否すること (相互認証を用いる場合) あるいはクライアントの Finished ハンドシェイクメッセージをサーバが拒否することを検証する。

c) Client Finished ハンドシェイクメッセージ中の 1 バイトを改変して、サーバが接続を拒否しアプリケーションデータを全く送信しないことを検証する。

d) クライアントが ChangeCipherSpec メッセージを送信する前にクライアントから Finished メッセージを送信することによって fatal alert を生成させた後、先ほどのテストからのセション識別子と共に Client Hello を送信し、サーバが接続を拒否することを検証する。

e) クライアントが ChangeCipherSpec メッセージを発行した後にクライアントから歪曲されたメッセージを送信し、サーバが接続を拒否することを検証する。

FCS_TLSS_EXT.2.2

272 評価者は、バージョン SSL 1.0 での接続を要求する Client Hello を送信し、サーバが接続を拒否することを検証しなければならない。評価者はこのテストを SSL 2.0、SSL 3.0、TLS 1.0、及び選択された TLS があればそれを用いて繰り返さなければならない。

FCS_TLSS_EXT.2.3

273 評価者は、ECDHE 暗号スイート及び設定された曲線を用いて接続を試行し、そしてパケットアナライザを用いて Key Exchange メッセージの鍵共有パラメタが設定されたものであることを検証しなければならない。(サイズが、設定された曲線に期待されるサイズと一致することを判断すれば十分である。) 評価者はこのテストを、サポートされる NIST 楕円曲線のそれぞれとサポートされる Diffie-Hellman 鍵長のそれぞれについて、繰り返さなければならない。

FCS_TLSS_EXT.2.4 及び FCS_TLSS_EXT.2.5

274 テスト 1 : 評価者は、証明書要求をクライアントへ送信するようサーバを設定しなければならず、そしてクライアントから証明書を送信することなく接続を試行しなければならない。評価者は、その接続が拒否されることを検証しなければならない。

275 テスト 2 : 評価者は、クライアントの証明書によって用いられる supported_signature_algorithm なしで証明書要求をクライアントへ送信するようサーバを設定しなければならない。評価者はクライアント証明書を用いて接続を試行し、その接続が拒否されることを検証しなければならない。

276 テスト 3 : 評価者は、有効な認証パスのない証明書を使用すると、その機能が失敗することを実証しなければならない。管理ガイダンスを利用して、次に評価者はその機能で使われる証明書の検証に必要とされる 1 つまたは複数の証明書をロードし、その機能が成功することを実証しなければならない。次に評価者は、これらの証明書の 1 つを削除して、その機能が失敗することを示さなければならない。

277 テスト 4 : 評価者は、サーバの Certificate Request メッセージの認証局 (ルートまたは中間 CA のいずれか) の 1 つへチェインしない証明書を送信するよう、クライアントを設定しなければならない。評価者は、試行された接続が拒否されることを検証しなければならない。

278 テスト 5 : 評価者は、extendedKeyUsage フィールドに Client Authentication 目的を含む証明書を送信するようクライアントを設定し、サーバが試行された接続を受け入れることを検証しなければならない。評価者はこのテストを Client

Authentication 目的なしで繰り返さなければならず、サーバが接続を拒否することを検証しなければならない。理想的には、2 つの証明書は Client Authentication 目的を除いて同一であるべきである。

279 テスト 6：評価者は、トラフィックに以下の改変を行わなければならない：

a) 相互認証を要求するようサーバを設定し、次にクライアントの証明書の 1 バイトを改変する。評価者は、サーバが接続を拒否することを検証しなければならない。

b) 相互認証を要求するようサーバを設定し、次にクライアントの Certificate Verify ハンドシェイクメッセージの 1 バイトを改変する。評価者は、サーバが接続を拒否することを検証しなければならない。

FCS_TLSS_EXT.2.6

280 評価者は、期待される識別子とマッチしない識別子を持つクライアント証明書を送信し、サーバが接続を拒否することを検証しなければならない。

2.3 識別と認証 (FIA)

2.3.1 FIA_PMG_EXT.1 パスワード管理

2.3.1.1 ガイダンス文書

281 評価者はガイダンス文書を検査して、強いパスワードの構成に関してセキュリティ管理者へガイダンスが提供されていること、そして最小パスワード長の設定に関して指示が提供されていることを判断しなければならない。

2.3.1.2 テスト

282 評価者は、以下のテストを行わなければならない。

a) テスト 1：評価者は、要件を満たすか、何らかの形で要件を満たさないか、いずれかである複数のパスワードを作成しなければならない。パスワードのそれぞれについて、評価者は TOE がそのパスワードをサポートすることを検証しなければならない。評価者にはパスワードのすべてのあり得る組み合わせをテストすることは要求されない (それは不可能でもある) 一方で、評価者は要件に列挙されたすべての文字、ルールの特徴、及び最小の長さがサポートされていることを保証し、テストのために選ばれたこれらの文字のサブセットを正当化しなければならない。

2.3.2 FIA_UIA_EXT.1 利用者の識別と認証

2.3.2.1 TSS

283 評価者は、TSS を検査して、製品にサポートされているログオン手法 (ローカル、リモート(HTTPS、SSH 等)) のそれぞれについてログオンプロセスが記述されていることを判断しなければならない。この記述には、許可される／用いられる認証情報、発生する任意のプロトコルトランザクション、そして何が「ログオン成功」をもたらすのかに関する情報が含まれなければならない。

2.3.2.2 ガイダンス文書

284 評価者は、ガイダンス文書を検査して、ログインするために必要な任意の準備ステップ (例えば、事前共有鍵、トンネル、証明書などの認証情報材料の確立など) が記述されていることを判断しなければならない。サポートされるログイン手法のそれぞれについて評価者は、ログオンを成功させるための明確な指示がガイダンス文書に提供されていることを保証しなければならない。ログイン前に提供されるサービスが制限されることを保証するために設定が必要な場合、評価者は許可されるサービスの制限に関する十分な指示がガイダンス文書に提供されていることを判断しなければならない。

2.3.2.3 テスト

285 評価者は、管理者が TOE へ (ローカル及びリモートに) アクセスする手法のそれぞれについて、またログイン手法によってサポートされる認証情報の種別のそれぞれについて、以下のテストを行わなければならない：

a) テスト 1：評価者は、ガイダンス文書を用いてログイン手法にサポートされる適切な認証情報を設定しなければならない。その認証情報／ログイン手法について、評価者は正しい I&A 情報を提供するとシステムへアクセスできる能力がもたらされるが、正しくない情報を提供するとアクセスの拒否がもたらされることを示さなければならない。

b) テスト 2：評価者は、ガイダンス文書に従って許可されるサービス (もしあれば) を設定し、次に外部リモートエンティティに利用可能なサービスを判断しなければならない。評価者は、利用可能なサービスのリストが要件に特定されているものに制限されていることを判断しなければならない。

c) テスト 3：ローカルなアクセスについて、評価者はログイン前にどのサービスがローカル管理者に利用可能かを判断し、このリストが要件と一貫していることを確認しなければならない。

2.3.3 FIA_UAU_EXT.2 パスワードに基づく認証メカニズム

286 この要件の保証アクティビティは、FIA_UIA_EXT.1 の保証アクティビティの下でカバーされる。その他の認証メカニズムが特定される場合、評価者はそれらの手法を FIA_UIA_EXT.1 のアクティビティに含めなければならない。

2.3.4 FIA_UAU.7 保護された認証フィードバック

2.3.4.1 テスト

287 評価者は、許可されるローカルログインの手法それぞれについて、以下のテストを行わなければならない：

a) テスト 1：評価者は、TOE へローカルに認証を行わなければならない。この試行を行っている間、評価者は認証情報を入力する間にたかだか見えなくされたフィードバックしか提供されないことを検証しなければならない。

2.3.5 FIA_X509_EXT.1 X.509 証明書有効性確認

2.3.5.1 TSS

288 評価者は、どこで証明書の有効性のチェックが行われるか TSS に記述されていることを保証しなければならない。また評価者は、認証パス検証アルゴリズムの記述が TSS に提供されていることも保証する。

2.3.5.2 テスト

289 評価者は、FIA_X509_EXT.1.1 について以下のテストを行わなければならない:

a) テスト 1: 評価者は、有効な認証パスのない証明書の有効性を確認すると、その機能が失敗することを実証しなければならない。次に評価者は、信頼済み CA がその機能で用いられる証明書の有効性確認に必要とするような 1 つまたは複数の証明書をロードし、その機能が成功することを実証しなければならない。次に評価者は、これらの証明書の 1 つを削除して、その機能が失敗することを示さなければならない。

b) テスト 2: 評価者は、有効期限を過ぎた証明書の有効性確認を行うと、その機能が失敗することを実証しなければならない。

c) テスト 3: 評価者は、CRL と OCSP のどちらが選択されているかに応じて、TOE が失効した証明書を適切に処理できることをテストしなければならない。両方とも選択されている場合には、それぞれの手法についてテストが行われなければならない。評価者は TOE 証明書の失効及び TOE 中間 CA 証明書の失効をテストしなければならない すなわち、中間 CA 証明書はルート CA によって失効させられるべきである。評価者は、有効な証明書が用いられること、そして証明書有効性確認機能が成功することを保証しなければならない。次に評価者は、失効した証明書 (選択において選ばれた手法それぞれについて) を用いてテストを試行し、もはや証明書が有効ではない場合には証明書有効性確認機能が失敗することを保証する。

d) テスト 4 : OCSP が選択されている場合、評価者は OCSP サーバを設定するか中間者ツールを使用して OCSP 署名目的を持たない証明書を提示し、OCSP 応答の有効性確認が失敗することを検証しなければならない。CRL が選択されている場合、評価者は cRLsign 鍵使用ビットがセットされていない証明書を持つ CRL に CA が署名するよう設定し、CRL の有効性確認が失敗することを検証しなければならない。

e) テスト 5 : 評価者は、証明書の最初の 8 バイトにおける任意のバイトを改変し、その証明書の有効性確認が失敗することを実証しなければならない。(証明書が正しく解析されないこと。)

f) テスト 6 : 評価者は、証明書の最後のバイトにおける任意のバイトを改変し、その証明書の有効性確認が失敗することを実証しなければならない。(証明書の署名が検証されないこと。)

g) テスト 7 : 評価者は、証明書の公開鍵における任意のバイトを改変し、その証明書の有効性確認が失敗することを実証しなければならない。(証明書のハッシュが検証されないこと。)

290 評価者は、FIA_X509_EXT.1.2 について以下のテストを行わなければならない。記述されるテストは、FIA_X509_EXT.2.1 中の機能を含め、他の証明書サービス保証アクティビティと組み合わせて行われなければならない。extendedKeyUsage ルールのテストは、これらのルールを要求する用途と組み合わせて行われる。

291 評価者は、少なくとも 4 つの証明書のチェインを作成しなければならない：テストされるノード証明書、2 つの中間 CA、及び自己署名されたルート CA である。

a) テスト 1：評価者は、TOE の証明書を発行する CA の証明書に basicConstraints 拡張が含まれないような認証パスを構築しなければならない。この認証パスの検証は失敗する。

b) テスト 2：評価者は、TOE の証明書を発行する CA の証明書の basicConstraints 拡張中の cA フラグが FALSE にセットされているような認証パスを構築しなければならない。この認証パスの検証は失敗する。

c) テスト 3：評価者は、TOE の証明書を発行する CA の証明書の basicConstraints 拡張中の cA フラグが TRUE にセットされているような認証パスを構築しなければならない。この認証パスの検証は成功する。

2.3.6 FIA_X509_EXT.2 X.509 証明書認証

2.3.6.1 TSS

292 評価者は、TSS をチェックして、TOE がどの証明書を利用するか選ぶ方法が記述されていること、及び TOE がその証明書を利用できるように運用環境を設定するために必要な指示が管理ガイダンスにあれば、それが記述されていることを保証しなければならない。

293 評価者は、TSS を検査して、高信頼チャネルの確立に用いられる証明書の有効性確認中に接続が確立できなかった際の TOE のふるまいが記述されていることを確認しなければならない。評価者は、高信頼チャネル間の相違があれば、それが記述されていることを検証しなければならない。管理者が、デフォルトのアクションを特定できるという要件が存在する場合には、この設定アクションを行う方法に関する指示がガイダンス文書に含まれていることを評価者は保証しなければならない。

2.3.6.2 テスト

294 評価者は、高信頼チャネルのそれぞれについて、以下のテストを行わなければならない：

295 評価者は、TOE 以外の IT エンティティとの通信によって、有効な証明書の使用には少なくとも一部の証明書有効性確認のチェック実行が必要とされることを実証しなければならない。次に評価者は、TOE が証明書の有効性を検証できないように環境を操作し、FIA_X509_EXT.2.2 で選択されたアクションが行われることを確認しなければならない。選択されたアクションが管理者によって設定可能である場合には、評価者は、ガイダンス文書に従って、サポートされているすべての管理者設定可能オプションが、文書化されているようにふる

まうことを判断しなければならない。

2.3.7 FIA_X509_EXT.3 拡張：X509 証明書要求

2.3.7.1 TSS

296 ST 作成者が「デバイス固有情報」を選択した場合、評価者は証明書要求に用いられるデバイス固有フィールドの記述が TSS に含まれることを検証しなければならない。

2.3.7.2 ガイダンス文書

297 評価者は、証明書要求メッセージの生成を含め、CA から証明書を要求することに関する指示がガイダンス文書に含まれていることをチェックして保証しなければならない。ST 作成者が「共通名 (Common Name)」、「組織 (Organization)」、「組織単位 (Organizational Unit)」、または「国 (Country)」を選択した場合、評価者は証明書要求メッセージを作成する前にこれらのフィールドを確立するための指示がこのガイダンスに含まれることを保証しなければならない。

2.3.7.3 テスト

298 評価者は、以下のテストを行わなければならない：

a) テスト 1：評価者は、ガイダンス文書を用いて TOE に証明書要求メッセージを生成させなければならない。評価者は生成されたメッセージをキャプチャして、指定されるフォーマットに適合していることを保証しなければならない。評価者は、証明書要求に公開鍵やその他の要求される情報が、任意の必要とされる利用者入力情報を含め、提供されることを確認しなければならない。

b) テスト 2：評価者は、有効な認証パスのない証明書応答メッセージの有効性を確認すると、その機能が失敗することを実証しなければならない。次に評価者は、信頼済み CA が証明書応答メッセージの有効性確認に必要とするような 1 つまたは複数の証明書をロードし、その機能が成功することを実証しなければならない。次に評価者は、これらの証明書の 1 つを削除して、その機能が失敗することを示さなければならない。

2.4 セキュリティ管理 (FMT)

2.4.1 FMT_MOF.1(1)/TrustedUpdate

2.4.1.1 テスト

299 評価者は、セキュリティ管理者としての事前の認証なしに (TOE の設定に応じて、管理者特権のない利用者としての認証によって、または一切の利用者認証なしに) 本物のアップデートイメージを用いたアップデートを試行しなければならない。このテストは失敗すべきである。

300 評価者は、本物のアップデートイメージを用い、セキュリティ管理者として事前認証を行った上で、アップデートを試行しなければならない。このテストは成功すべきである。このテストケースは、すでに FPT_TUD_EXT.1 のテストによってカバーされているべきである。

2.4.2 FMT_MOF.1(2)/TrustedUpdate

2.4.2.1 テスト

301 評価者は、セキュリティ管理者としての事前の認証なしに (TOE の設定に応じて、管理者特権のない利用者としての認証によって、または一切の利用者認証なしに) アップデートの自動チェックまたは自動アップデート (いずれか TOE のサポートするほう) の有効化及び無効化を試行しなければならない。このテストは失敗すべきである。

302 評価者は、セキュリティ管理者としての事前認証を行った上で、アップデートの自動チェックまたは自動アップデート (いずれか TOE のサポートするほう) の有効化及び無効化を試行しなければならない。このテストは成功すべきである。

2.4.3 FMT_MOF.1(1)/Audit

2.4.3.1 テスト

303 評価者は、セキュリティ管理者としての事前の認証なしに (TOE の設定に応じて、管理者特権のない利用者としての認証によって、または一切の利用者認証なしに) 外部 IT エンティティへ監査データを送信するための送信プロトコルを設定するすべてのパラメタの変更を試行しなければならない。このテストは失敗すべきである。

304 評価者は、セキュリティ管理者としての事前認証認証を行った上で、外部 IT エンティティへ監査データを送信するための送信プロトコルを設定するすべてのパラメタの変更を試行しなければならない。変更の結果が確認されるべきである。

305 評価者は、外部 IT エンティティへ監査データを送信するための送信プロトコルを設定するすべてのパラメタのすべての可能なパラメタ値を必ずしもテストしなければならないわけではなく、設定可能なパラメタにつき少なくとも 1 つの許可される値をテストすればよい。

2.4.4 FMT_MOF.1(2)/Audit

2.4.4.1 テスト

306 評価者は、セキュリティ管理者としての事前の認証なしに (TOE の設定に応じて、管理者特権のない利用者としての認証によって、または一切の利用者認証なしに) 監査データの取り扱いを設定するすべてのパラメタの変更を試行しなければならない。このテストは失敗すべきである。「監査データの取り扱い」という用語は、SFR FAU_STG_EXT.1.2 、 FAU_STG_EXT.1.3 、 及び FAU_STG_EXT.2 中の選択及び割付の異なる選択肢に対応する。

307 評価者は、セキュリティ管理者としての事前認証認証を行った上で、監査データの取り扱いを設定するすべてのパラメタの変更を試行しなければならない。変更の影響が確認されるべきである。「監査データの取り扱い」という用語は、SFR FAU_STG_EXT.1.2、FAU_STG_EXT.1.3、及び FAU_STG_EXT.2 中の選択及び割付の異なる選択肢に対応する。

308 評価者は、監査データの取り扱いを設定するすべての可能なパラメタを必ずしもテストしなければならないわけではなく、設定可能なパラメタにつき少なくとも 1 つの許可される値をテストすればよい。

2.4.5 FMT_MOF.1(1)/AdminAct

2.4.5.1 テスト

309 評価者は、セキュリティ管理者としての事前の認証なしに (TOE の設定に応じて、管理者特権のない利用者としての認証によって、または一切の利用者認証なしに) 少なくとも 1 つの関連するアクションの実行を試行しなければならない。これらの試行は失敗すべきである。

310 評価者は、セキュリティ管理者としての事前認証を行った上で、少なくとも 1 つの関連するアクションの実行を試行しなければならない。これらの試行は成功すべきである。

2.4.6 FMT_MOF.1(2)/AdminAct

2.4.6.1 テスト

311 評価者は、セキュリティ管理者としての事前の認証なしに (TOE の設定に応じて、管理者特権のない利用者としての認証によって、または一切の利用者認証なしに) 少なくとも 1 つの関連するアクションの実行を試行しなければならな

い。これらの試行は失敗すべきである。

312 評価者は、セキュリティ管理者としての事前認証を行った上で、少なくとも 1 つの関連するアクションの実行を試行しなければならない。これらの試行は成功すべきである。

2.4.7 FMT_MOF.1/LocSpace セキュリティ機能のふるまいの管理

2.4.7.1 テスト

313 評価者は、セキュリティ管理者としての事前の認証なしに (TOE の設定に応じて、管理者特権のない利用者としての認証によって、または一切の利用者認証なしに) 少なくとも 1 つの関連するアクションの実行を試行しなければならない。これらの試行は失敗すべきである。

314 評価者は、セキュリティ管理者としての事前認証を行った上で、少なくとも 1 つの関連するアクションの実行を試行しなければならない。これらの試行は成功すべきである。

2.4.8 FMT_MTD.1 TSF データの管理

2.4.8.1 TSS

315 評価者は、TSS を検査して、ガイダンス文書に特定される管理機能それぞれについて、管理者のログインに先立ってインタフェースを介してアクセス可能なものが特定されていることを判断しなければならない。またこれらの機能のそれぞれについて、評価者はこれらのインタフェースを介して TSF データを操作する能力が非管理ユーザにどのように禁じられているか TSS に詳述されていることを確認しなければならない。

2.4.8.2 ガイダンス文書

316 評価者は、ガイダンス文書をレビューして、cPP の要件に対応して実装された TSF データ操作機能のそれぞれが特定されていること、また管理者のみがその機能へアクセスできることを保証するための設定情報が提供されていることを判断しなければならない。

2.4.9 FMT_MTD.1/AdminAct TSF データの管理

2.4.9.1 テスト

317 評価者は、セキュリティ管理者としての事前の認証なしに (TOE の設定に応じて、管理者特権のない利用者としての認証によって、または一切の利用者認証なしに) 少なくとも 1 つの関連するアクションの実行を試行しなければならない。このテストは失敗すべきである。

318 評価者は、セキュリティ管理者としての事前認証を行った上で、少なくとも 1 つの関連するアクションの実行を試行しなければならない。このテストは成功すべきである。

2.4.10 FMT_SMF.1 管理機能の特定

319 FMT_SMF.1 のセキュリティ管理機能は cPP 全体にわたって分散しており、FTA_TAB.1 、 FTA_SSL.3 、 FTA_SSL.4 、 FMT_MOF.1(1)/TrustedUpdate 、 FMT_MOF.1(2)/TrustedUpdate (ST に含まれる場合)、FIA_X509_EXT.2.2 及び FPT_TUD_EXT.2.2 (ST に含まれる場合及びそれらに管理者によって設定可能なアクションが含まれる場合)、FMT_MOF.1(1)/Audit、FMT_MOF.1(2)/Audit、FMT_MOF.1.1(1)/AdminAct 、 FMT_MOF.1.1(2)/AdminAct 及び FMT_MOF.1/LocSpace (これらの SFR のうち ST に含まれるものすべてについて)、FMT_MTD、FPT_TST_EXT、ならびに参照標準の中に特定される任意の暗号管理機能の要件の一部として含まれる。これらの要件への適合によって、FMT_SMF.1 への適合が満たされる。

2.4.11 FMT_SMR.2 セキュリティ役割における制限

2.4.11.1 ガイダンス文書

320 評価者は、ガイダンス文書をレビューして、リモート管理のためにクライアント上で行われる必要のある任意の設定を含め、ローカルとリモートの両方で TOE を管理するための指示が含まれることを保証しなければならない。

2.4.11.2 テスト

321 評価のためテストアクティビティを行うにあたって、評価者はすべてのサポートされるインタフェースを利用しなければならない が、各インタフェースについて管理アクションを伴う各テストを繰り返す必要はない。しかし評価者は、本 cPP の要件に適合する TOE 管理のサポートされた手法それぞれがテストされることを保証しなければならない。例えば、TOE がローカルなハードウェアインタフェース、SSH、及び TLS/HTTPS を介して管理可能な場合には、評価チームのテストアクティビティ中で 3 つの管理手法すべてが行使されなければならない。

2.5 TSF の保護 (FPT)

2.5.1 FPT_SKP_EXT.1 TSF データの保護 (すべての対称鍵の読み出し)

2.5.1.1 TSS

322 評価者は、TSS を検査して、任意の事前共有鍵、対称鍵、及び秘密鍵がどのように保存されるか、そして特にその目的に設計されたインタフェースを通してそれらを閲覧できないことが詳述されていることを判断しなければならない。これらの値が平文で保存されない場合、TSS にはそれらがどのように保護／あいまい化されるか記述されなければならない。

2.5.2 FPT_APW_EXT.1 管理者パスワードの保護

2.5.2.1 TSS

323 評価者は、TSS を検査して、この要件の対象となるすべての認証データ、及び平文のパスワードデータを保存の際にあいまい化するために用いられる手法が詳述されていることを判断しなければならない。また TSS には、適用上の注釈に概略を記したように、特にその目的に設計されたインタフェースを通して閲覧することができないようにパスワードが保存されることも詳述されなければならない。

2.5.3 FPT_TST_EXT.1 TSF テスト

2.5.3.1 TSS

324 評価者は TSS を検査して、TSF によって実行される自己テストが詳述されていることを保証しなければならない。この記述には、実際に行われるテストの概要 (例えば、「メモリがテストされる」と言うだけではなく、「各メモリロケーションに値を書き込み、それを読み出して書き込んだ値と同一であることを保証することによってメモリがテストされる」のような記述が用いられなければならない) が含まれるべきである。評価者は、TSF が正しく動作していることをテストが十分に実証するという論拠が TSS に示されていることを保証しなければならない。

2.5.3.2 ガイダンス文書

325 また評価者は、そのようなテストに起因し得る可能性のあるエラーと、それに対応して管理者が取るべきアクションがガイダンス文書に記述されていることを保証しなければならない。これらの可能性のあるエラーは、TSS に記述されたものと対応していなければならない。

2.5.3.3 テスト

326 本 cPP の将来の版は、明確に定義された自己テストの最小限のセットを義務付けることになる。しかしまた cPP の本バージョンでは、少なくとも以下のテストが行われることが期待される：

a) TOE のファームウェア及び実行可能ソフトウェアの完全性の検証。

b) 任意の SFR を満たすために必要な暗号機能の正しい動作の検証。

327 形式的な適合は義務付けられないものの、行われる自己テストは以下と同等の信頼のレベルを目指すべきである：

a) FIPS 140-2, chap. 4.9.1, Software/firmware integrity test for the verification of the integrity of the firmware and executable software.

b) FIPS 140-2, chap. 4.9.1, Cryptographic algorithm test for the verification of the correct operation of cryptographic functions.
あるいは、任意の CCRA 加盟国の暗号機能のセキュリティ評価に関する国家的要件が、適宜考慮されるべきである。

328 評価者は、上記の自己テストが最初の起動中に行われるか、これからの任意の逸脱が開発者によって正当化されているか (該当する場合) のいずれかであることを検証しなければならない。

2.5.4 FPT_TST_EXT.2 証明書ベースの自己テスト

2.5.4.1 テスト

329 評価者は、FIA_X509_EXT.1 に従った証明書有効性確認及び extendedKeyUsage 中のコード署名目的のチェックが自己テストメカニズムに含まれることを検証しなければならない。

330 評価者は、無効な証明書を用いて自己テストを行わなければならない。このテストは失敗すべきである。評価者は、コード署名目的を持たない証明書を用いて、自己テストが失敗することを検証しなければならない。評価者は、有効な証明書とコード署名目的を含む証明書を用いてテストを繰り返し、自己テストが成功することを検証しなければならない。このエレメントのテストは、FPT_TST_EXT.1 の保証アクティビティと組み合わせて行われる。

2.5.5 FPT_TUD_EXT.1 高信頼アップデート

2.5.5.1 TSS

331 評価者は、システムソフトウェアをアップデートするためのすべての TSF ソフトウェアアップデートメカニズムが TSS に記述されていることを検証しなければならない。評価者は、その記述にインストール前のソフトウェアのデジタル署名検証が含まれること、及び検証が失敗した場合にインストールが失敗することを検証しなければならない。あるいは、公開ハッシュを利用するやり方を用いることもできる。この場合、デジタル署名検証メカニズムの代わりに、このメカニズムが TSS に詳述されなければならない。評価者は、アップデート候補が取得される方法、アップデートのデジタル署名または公開ハッシュの検証に関連した処理、そして署名検証または公開ハッシュ検証の成功と不成功の両方の場合について行われるアクションを含め、デジタル署名または公開ハッシュが検証される手法が、TSS に記述されていることを検証しなければならない。

332 ソフトウェアアップデートデジタル署名検証に証明書ベースのメカニズムが用いられることを ST 作成者が指示している場合、評価者は、デバイス上に証明書がどのように含まれるかの記述が TSS に含まれることを検証しなければならない。また評価者は、必要に応じて、証明書がどのようにインストール／アップデート／選択されるのか TSS (またはガイダンス文書) に記述されていることを保証する。

2.5.5.2 ガイダンス文書

333 評価者は、アップデートの真正性の検証がどのように行われるのか (デジタル署名検証または公開ハッシュの検証) ガイダンス文書に記述されていることを検証しなければならない。この記述には、検証の成功及び不成功の場合についての手順が含まれなければならない。この記述は、TSS 中の記述と対応していなければならない。

2.5.5.3 テスト

334 評価者は、以下のテストを行わなければならない：

a) テスト 1：評価者は、バージョン検証アクティビティを行って製品の現在のバージョン及び一番最近にインストールされたバージョンを判断する (アップデート前は同一のバージョンであるべきである)。評価者は、ガイダンス文書に記述されている手順を用いて本物のアップデートを取得し、その TOE へのインストールが成功することを検証する。一部の TOE では、アップデートの TOE 上へのロードとアップデートのアクティベーションが別のステップとなっている (『アクティベーション』は、例えば個別のアクティベーションステップによって、またはデバイスのリブートによって行われるかもしれない)。この場合、評価者は TOE 上へアップデートがロードされた後、しかしアップデートのアクティベーション前に、製品の現在のバージョンが変化しなかったこと、しかし一番最近にインストールされたバージョンは新たな製品バージョンに変化したことを検証する。アップデート後、評価者は再びバージョン検証アクティビティを行って、そのバージョンがアップデートのものと正しく対応していること、及び製品の現在のバージョンと一番最近にインストールされたバージョンが再び一致することを検証する。

b) テスト 2：評価者は、バージョン検証アクティビティを行って製品の現在のバージョン及び一番最近にインストールされたバージョンを判断する (アップデート前は同一のバージョンであるべきである)。評価者は、以下に定義されるような偽物のアップデートを取得または作成し、それらの TOE へのインストールを試行する。評価者は、すべての偽物のアップデートを TOE が拒否することを検証する。評価者は、以下の形態の偽物のアップデートすべてを用いてこのテストを行う：

    1) 本物の署名付きのアップデートの (例えば 16 進エディタを用いて) 改変されたバージョン (デジタル署名が用いられる場合) または公開ハッシュと一致しないバージョン (公開ハッシュが用いられる場合)。

    2) 署名されていないイメージ (デジタル署名が用いられる場合) または公開ハッシュのないイメージ (公開ハッシュが用いられる場合)。

    3) 無効な署名で署名されたイメージ (例えば、署名の作製に期待されるものと異なる鍵を用いることによって、または本物の署名を手作業で改変することによって) (デジタル署名が用いられる場合のみ)。

    4) 一番最近にインストールされたバージョンのバージョン情報の取り扱いは、異なる TOE の間では異なるかもしれない。試行されたアッ

プデートが拒否された時点に応じて、一番最近にインストールされたバージョンはアップデートされるかもしれないし、アップデートされないかもしれない。その場合には TOE がガイダンス文書に従って一番最近にインストールされたバージョンの情報を取り扱うことを評価者は検証しなければならない。TOE がアップデートを拒否した後、評価者は現在のバージョンと一番最近にインストールされたバージョンの両方が、アップデート試行以前と同一のバージョン情報を反映していることを検証しなければならない。

335 評価者は、テスト 1 及び 2 を、サポートされるすべての手法 (手作業によるアップデート、アップデートの自動チェック、自動アップデート) について行わなければならない。

2.5.6 FPT_TUD_EXT.2 証明書ベースの高信頼アップデート

2.5.6.1 TSS

336 評価者は、高信頼アップデートに X.509 証明書が用いられ、かつ有効期限の過ぎた証明書を用いた高信頼アップデートの実行を管理者が試行した場合に、TOE がどのように反応するか TSS に記述されていることを検証しなければならない。

2.5.6.2 ガイダンス文書

337 評価者は、高信頼アップデートに X.509 証明書が用いられ、かつ有効期限の過ぎた証明書を用いた高信頼アップデートの実行を管理者が試行した場合に、TOE がどのように反応するかガイダンス文書に記述されていることを検証しなければならない。この記述は、TSS 中の記述と対応していなければならない。

2.5.6.3 テスト

338 評価者は、FIA_X509_EXT.1 に従った証明書有効性確認及び extendedKeyUsage 中のコード署名目的のチェックがアップデートメカニズムに含まれることを検証しなければならない。

339 評価者は、無効な証明書でアップデートにデジタル署名し、アップデートのインストールが失敗することを検証しなければならない。評価者は、コード署名目的を持たない証明書でアプリケーションにデジタル署名し、アプリケーションのインストールが失敗することを検証しなければならない。評価者は、有効な証明書とコード署名目的を含む証明書を用いてテストを繰り返し、アプリケーションのインストールが成功することを検証しなければならない。評価者は、以前は有効だったが有効期限の過ぎた証明書を用いて TOE が TSS 及びガイダンス文書に記述されるとおり反応することを検証しなければならない。このエレメントのテストは、FPT_TUD_EXT.1 の保証アクティビティと組み合わせて行われる。

2.5.7 FPT_STM.1 高信頼タイムスタンプ

2.5.7.1 TSS

340 評価者は、TSS を検査して、時刻を利用するセキュリティ機能それぞれが列挙されていることを保証しなければならない。TSS には、時刻に関連する機能それぞれの文脈において、どのように時刻が維持管理され高信頼とみなされるかの記述が提供される。

341 評価者は、ガイダンス文書を検査して、時刻を設定する方法が管理者に指示されていることを保証する。TOE が NTP サーバの利用をサポートする場合、ガイダンス文書には TOE と NTP サーバとの間の通信パスが確立される方法、及び TOE 上の NTP クライアントがこの通信をサポートするための任意の構成が指示される。

2.5.7.2 テスト

342 評価者は、以下のテストを行わなければならない：

a) テスト 1 : 評価者は、ガイダンス文書を用いて時刻を設定する。次に評価者は、利用できるインタフェースを使って時刻が正しく設定されたことを確認しなければならない。

b) テスト 2 : TOE が NTP サーバの利用をサポートしている場合、評価者はガイダンス文書を用いて TOE 上の NTP クライアントを設定し、NTP サーバとの通信パスを設定しなければならない。評価者は、NTP サーバが期待されるように時刻を設定することを確認する。TOE が NTP サーバとの接続を確立するために複数のプロトコルをサポートしている場合、評価者はガイダンス文書に主張されるサポートされるプロトコルそれぞれを用いてこのテストを行わなければならない。

343 TOE の監査コンポーネントが独立の時刻情報を持つ複数の部分から構成される場合には、評価者は異なる部分の間で時刻情報が同期されているか、またはすべての監査情報について異なる部分の時刻情報を 1 つの基本情報にあいまいさなく関係づけることが可能であるか、どちらかであることを検証しなければならない。

2.5.8 FPT_FLS.1/LocSpace セキュアな状態を保持する障害

2.5.8.1 テスト

344 評価者は、監査データのローカルな格納領域が満杯でないことのテストを行わなければならない (例えば、ロギングされるアクションを実行し、それに従って監査データが更新されることを検証することによって)。評価者は、セキュリティ機能が適切に動作していることをテストしなければならない (ここで多少のサンプリングが必要とされるかもしれない)。次に評価者は、監査データのローカルな格納領域が満杯となるまでロギングされるアクションを実行しなければならない。評価者は、セキュリティ機能がもはや動作していないこと、またはもはやアクセスできないことを検証しなければならない。FPT_FLS.1/Local Audit Storage Space Full に従ってセキュアな状態を維持するために必要なセキュリティ機能はこのルールの例外とみなされなければならな

い。それらは要件そのものを満たすために適切に動作する必要があるためである。評価者が、監査データのローカルな格納領域が満杯でなかった際にセキュリティ機能が適切に動作していたことの検証にサンプリングを用いた場合には、評価者は同一のセキュリティ機能について、監査データのローカルな格納領域が満杯となった後で動作を停止したことを検証しなければならない。

2.6 TOE アクセス

2.6.1 FTA_SSL_EXT.1 TSF 起動によるセションロック

2.6.1.1 テスト

345 評価者は、以下のテストを行わなければならない：

a) テスト 1：評価者はガイダンス文書に従って、コンポーネント中に参照される非アクティブ継続時間をいくつかの異なる値に設定する。設定された時間間隔のそれぞれについて、評価者は TOE とのローカルな対話セションを確立する。次に評価者は、設定された時間間隔の後に、そのセションがロックされるか終了されるかのいずれかであることを確認する。コンポーネントからロックが選択された場合、次いで評価者はセションのロック解除を試行する際に再認証が必要であることを保証する。

2.6.2 FTA_SSL.3 TSF 起動による終了

2.6.2.1 テスト

346 評価者は、以下のテストを行わなければならない：

a) テスト 1：評価者は、ガイダンス文書に従って、コンポーネント中に参照される非アクティブ継続時間をいくつかの異なる値に設定する。設定された時間間隔のそれぞれについて、評価者は TOE とのリモート対話セションを確立する。次に評価者は、設定された時間間隔の後に、そのセションが終了されることを確認する。

2.6.3 FTA_SSL.4 利用者起動による終了

2.6.3.1 テスト

347 評価者は、以下のテストを行わなければならない：

a) テスト 1：評価者は、TOE との対話型ローカルセションを開始する。次に評価者はガイダンス文書に従ってセションを退出またはログオフし、セションが終了されることを確認する。

b) テスト 2：評価者は、TOE との対話型リモートセションを開始する。次に評価者はガイダンス文書に従ってセションを終了またはログオフし、セションが終了されることを確認する。

2.6.4 FTA_TAB.1 デフォルト TOE アクセスバナー

2.6.4.1 TSS

348 評価者は、TSS をチェックして、管理者に利用可能な (ローカル及びリモート) アクセスの手法それぞれ (例えば、シリアルポート、SSH、HTTPS) が詳述されていることを保証しなければならない。

2.6.4.2 テスト

349 また評価者は、以下のテストを行わなければならない：

a) テスト 1 : 評価者は、ガイダンス文書に従って、通知及び同意警告メッセージを設定する。次に評価者は、TSS に特定されるアクセスの手法それぞれについて、TOE とのセションを確立させなければならない。評価者は、インスタンスそれぞれに通知及び同意警告メッセージが表示されることを検証しなければならない。

2.7 高信頼パス／チャネル (FTP)

2.7.1 FTP_ITC.1 TSF 間高信頼チャネル

2.7.1.1 TSS

350 評価者は、TSS を検査して、要件中に特定される正当な IT エンティティとのすべての通信について、その IT エンティティに許可されるプロトコルの観点から、通信メカニズムそれぞれが特定されていることを判断しなければならない。また評価者は、TSS に列挙されたすべてのプロトコルが特定され、ST 中の要件に含まれていることを確認しなければならない。

2.7.1.2 ガイダンス文書

351 評価者は、正当な IT エンティティそれぞれに許可されるプロトコルを確立するための指示がガイダンス文書に含まれていること、及び万一接続が意図せず切断されてしまった際の回復指示が含まれていることを確認しなければならない。

2.7.1.3 テスト

352 評価者は、以下のテストを行わなければならない：

a) テスト 1 : 評価者は、ガイダンス文書に記述されるように接続を設定し、通信が成功することを保証することによって、評価中に正当な IT エンティティそれぞれとのプロトコルそれぞれを用いた通信がテストされることを保証しなければならない。

b) テスト 2 : 要件中に定義されるように TOE が開始できるプロトコルそれぞれについて、評価者はガイダンス文書に従って実際にその通信チャネルが TOE から開始できることを保証しなければならない。

c) テスト 3 : 評価者は、正当な IT エンティティとの通信チャネルそれぞれについて、チャネルデータが平文で送信されないことを保証しなければならない。

d) テスト 4 : 評価者は、テスト 1 でテストされた正当な IT エンティティそれぞれと関連付けられたプロトコルそれぞれについて、接続が物理的に中断されるようにしなければならない。評価者は、物理的な接続性が回復された際、通信が適切に保護されていることを保証しなければならない。

353 これ以外の保証アクティビティは、特定のプロトコルと関連付けられる。

2.7.2 FTP_TRP.1 高信頼パス

2.7.2.1 TSS

354 評価者は、TSS を検査して、リモート TOE 管理の手法が、これらの通信が保護される方法と共に示されていることを判断しなければならない。また評価者は、TOE 管理をサポートするものとして TSS に列挙されたすべてのプロトコルが要件中に特定されたものと一貫しており、ST 中の要件に含まれていることを確認しなければならない。

2.7.2.2 ガイダンス文書

355 評価者は、サポートされる手法それぞれについて、リモート管理セションを確立するための指示がガイダンス文書に含まれていることを確認しなければならない。

2.7.2.3 テスト

356 評価者は、以下のテストを行わなければならない :

a) テスト 1 : 評価者は、ガイダンス文書に記述されるように接続を設定し、通信が成功することを保証することによって、評価中に (ガイダンス文書に) 特定されたリモート管理手法それぞれを用いた通信がテストされることを保証しなければならない。

b) テスト 2 : 要件中に定義されるように TOE が開始できるプロトコルそれぞれについて、評価者は、ガイダンス文書に従って実際にその通信チャネルが TOE から開始できることを保証しなければならない。

c) テスト 3 : 評価者は、正当な IT エンティティとの通信チャネルそれぞれについて、チャネルデータが平文で送信されないことを保証しなければならない。

d) テスト 4 : 評価者は、テスト 1 でテストされた正当な IT エンティティそれぞれと関連付けられたプロトコルそれぞれについて、接続が物理的に中断されることを保証しなければならない。評価者は、物理的な接続性が回復された際、通信が適切に保護されていることを保証しなければならない。

357 これ以外の保証アクティビティは、特定のプロトコルと関連付けられる。

3 SAR の評価アクティビティ

358 以下のセクションでは、関連する cPP に含まれるセキュリティ保証要件の評価アクティビティを特定する (上記のセクション 1.1 を参照されたい)。評価アクティビティは、より一般的な CEM 保証アクティビティの解釈であり、特定の技術領域の TOE に適用される。

359 要件が技術に依存しない場合、評価者は CEM ワークユニットを行うことが期待され (例えば、ASE (セクション 3.1 にあるもの以外)、ALC_CMC.1、ALC_CMS.1)、これらのアクティビティはここで繰り返されることはなく、cPP の一部として表現される。

3.1 ASE：セキュリティターゲット評価

360 ここで定義される評価アクティビティは、セキュリティターゲット中の cPP に対する完全適合の主張を評価するためのものである。ASE のその他の側面は、[CEM, 10] に定義されるように保たれる。

3.1.1 適合主張 (ASE_CCL.1)

361 以下の表に、cPP との完全適合を判断するために特定の ASE_CCL.1 エレメントに対して取られるアクションを示す。

ASE_CCL.1 エレメント	評価者のアクション
ASE_CCL.1.8C	評価者は、PP 及び ST のセキュリティ課題定義のステートメントが同一であることをチェックしなければならない。
ASE_CCL.1.9C	評価者は、PP 及び ST のセキュリティ対策方針のステートメントが同一であることをチェックしなければならない。
ASE_CCL.1.10C	評価者は、ST のセキュリティ要件のステートメントに cPP のすべての必須 SFR、及び他の SFR でなされた選択によって課される選択ベースの SFR のすべてが (ST で追加された任意の SFR の繰返しを含めて) 含まれることをチェックしなければならない。評価者は、他の任意の SFR が ST に存在する場合には (cPP の SFR の繰返しを除いて) これらが cPP に特定されるオプションの SFR のリストのみから取られていることをチェックしなければならない (cPP には*必ずしも*オプションの SFR が含まれるわけではないが、含まれてもよい)。cPP からオプションの SFR が ST に含まれる場合、評価者は採択されたオプションの SFR によって課される任意の選択ベースの SFR もまた ST に含まれることをチェックしなければならない。

3.2 ADV：開発

3.2.1 基本機能仕様 (ADV_FSP.1)

362 この保証コンポーネントの評価アクティビティは、機能仕様に対応した形で TOE 要約仕様 (TSS) に提示されるインタフェースと、AGD 文書に提示されるインタフェースを理解することに焦点を絞る。本文書に関する特定の要件は (関連する) 各 SFR については上記のセクション 2 に、そして AGD、ATE 及び AVA SAR の評価アクティビティについては本サポート文書のセクション 3 の別の場所に、特定される。

3.2.1.1 評価アクティビティ

363 評価者は、インタフェース文書をチェックして、セキュリティ関連であると特定される各 TSFI について利用の目的と手法が記述されていることをチェックしなければならない。

364 この文脈において、TSFI は管理者によって TOE を設定するため、またはその他の管理機能 (例えば、監査レビューまたはアップデートの実施) を行うために用いられる場合にセキュリティ関連とみなされる。さらに、ST、またはガイダンス文書にセキュリティポリシーを順守すると特定される (SFR に提示されるように) インタフェースもまた、セキュリティ関連とみなされる。この意図は、これらのインタフェースが十分にテストされることであり、また TOE においてこれらのインタフェースがどのように利用されるかの理解を持つことは適切なテストカバレージの適用を保証するために必要である。

365 評価者は、インタフェース文書をチェックして、セキュリティ関連であると特定される各 TSFI についてパラメタが特定され記述されていることをチェックしなければならない。

366 従って評価中にこの保証コンポーネントについて検査されるべき文書はセキュリティターゲット、AGD 文書、及びエントロピー分析または暗号鍵管理アーキテクチャなどの側面について cPP によって要求される任意の補足情報である [1]：追加的な「機能仕様」文書は評価アクティビティを満たすために必要ではない。また評価が必要なインタフェースは各 SFR に列挙される保証アクティビティへの参照によって特定され、また特に CC 評価を目的とした別個のリストとしてではなく、セキュリティターゲット、AGD 文書、及び cPP によって要求される任意の補足情報の文脈で特定されることが期待される。また、文書要件の直接的な特定及び各 SFR の評価アクティビティの一部としてのそれらの評定は、ADV_FSP.1.2D に要求される追跡が暗黙的なものとして扱われ、またこのエレメントについて別個の対応付け情報が要求されないことをも意味する。

[1] セキュリティターゲット及び AGD 文書は、公開文書である。補足情報は、公開であっても独占的 (proprietary) であってもよい：cPP または評価アクティビティの記述あるいはその両方が、そのような補足文書が独占的かつ非公開であることが許可される場合を特定する。

367 しかし、不十分な設計及びインタフェース情報しか存在しなかったために他の何らかの要求される評価アクティビティを評価者が行うことができなかった場合には、十分な機能仕様が提供されておらず、従って ADV_FSP.1 保証コンポーネントの判定が「不合格」であると結論付ける権利が評価者に与えられる。

3.3 AGD：ガイダンス文書

368 AGD_OPE 及び AGD_PRE の個別要件を満たすために TOE が別個の文書を提供する必要はない。本セクションの評価アクティビティは伝統的な別個の AGD ファミリの下で記述されているが、実際の TOE 文書と AGD_OPE 及び AGD_PRE との対応付けは、TOE の一部として (適宜) 管理者及び利用者へ配付される文書においてすべての要件が満たされている限り、多対多であってもよい。

3.3.1 利用者操作ガイダンス (AGD_OPE.1)

369 利用者ガイダンス文書に関する具体的な要件及びチェックは、 (関連する) 各 SFR の個別評価アクティビティ中、及びその他いくつかの SAR (例えば ALC_CMC.1) に関して特定される。

3.3.1.1 評価アクティビティ：

370 評価者は、ガイダンス文書が以下を満たしていることをチェックしなければならない。

371 ガイダンス文書は、TOE の一部として (適宜) 管理者及び利用者へ配付されなければならないため、文書の存在及び評価される構成を確立し維持管理するにあたっての役割を管理者及び利用者が認識しているという合理的な保証が存在する。

372 ガイダンスは、セキュリティターゲットで主張されたとおり製品がサポートするすべての運用環境に関して提供されなければならず、またセキュリティターゲットで TOE について主張されたすべてのプラットフォームに十分対応していなければならない。

373 ガイダンス文書の内容は、以下に定義される評価アクティビティによって、また適宜上記のセクション 2 の個別 SFR それぞれについて検証されることになる。

374 SFR 関連の評価アクティビティに加えて、以下の情報もまた必要とされる。

a) ガイダンス文書には、TOE の評価される構成と関連付けられた任意の暗号エンジンを設定するための指示が含まれなければならない。TOE の CC 評価で、他の暗号エンジンの利用が評価もテストもされなかったという警告が、管理者へ与えられなければならない。

b) 文書には、デジタル署名の検証によって TOE へのアップデートを検証するためのプロセスが記述されなければならない。評価者は、このプロセスに以下のステップが含まれることを検証しなければならない。

   1) アップデートそのものを取得するための指示。これには、アップデートを TOE からアクセス可能とするための指示 (例えば、特定のディレクトリへの格納) が含まれるべきである。

   2) アップデートプロセスを開始するための、そしてそのプロセスが成功したか失敗したかを判別するための指示。これには、ハッシュ／デジタル署名の生成が含まれる。

c) 本 cPP の下での評価の適用範囲に含まれないセキュリティ機能が TOE に含まれることもあるだろう。どのセキュリティ機能が評価アクティビティによってカバーされているのかを、ガイダンス文書は管理者に対して明確にしなければならない。

3.3.2 準備手続き (AGD_PRE.1)

375 ガイダンス文書に関しては、準備手続きについての具体的な要件及びチェックは (関連する) 各 SFR の個別評価アクティビティに特定される。

3.3.2.1 評価アクティビティ：

376 評価者は、準備手続きが以下を満たしていることをチェックしなければならない。

377 準備手続きの内容は以下に定義される評価アクティビティによって、また適宜上記のセクション 2 の個別 SFR それぞれについて検証されることになる。

378 準備手続きは TOE の一部として (適宜) 管理者及び利用者へ配付されなければならない ため、文書の存在及び評価される構成を確立し維持管理するにあたっての役割を管理者及び利用者が認識しているという合理的な保証が存在する。

379 準備手続きの内容は以下に定義される評価アクティビティによって、また適宜上記のセクション 2 の個別 SFR のそれぞれについて検証されることになる。

380 SFR 関連の評価アクティビティに加えて、以下の情報もまた必要とされる。

381 準備手続きには、運用環境がセキュリティ機能に対する役割を果たすことができることを管理者がどのように検証するかの記述が含まれなければならない (セキュリティターゲットに特定される運用環境のセキュリティ対策方針の要件を含む)。この文書は、非形式的なスタイルであるべきであり、また対象とする聴衆 (これには通常、一般的な IT の経験はあるが必ずしも TOE 製品そのものについての経験は持たない IT スタッフが含まれる) が理解し利用できるように十分な詳細及び説明と共に作成されるべきである。

382 準備手続きは、セキュリティターゲットで主張されたとおり製品がサポートするすべての運用環境に関して提供されなければならず、またセキュリティターゲットで TOE について主張されたすべてのプラットフォームに十分対応していなければならない。

383 準備手続きは、以下を含まなければならない

a) 運用環境それぞれへの TSF のインストールを成功させるための指示、及び

b) 製品として、またより大規模な運用環境のコンポーネントとして、TSF のセキュリティを管理するための指示、ならびに

c) 保護された管理機能を提供するための指示。

3.4 ATE：テスト

3.4.1 独立テスト—適合 (ATE_IND.1)

384 テストは、TSS に記述された機能と、ガイダンス文書を確認するために行われる。テストで重視されるのは、SFR に特定された要件が満たされていることを確認することである。

385 評価者は、附属書 B を参照して、評価に供されるかもしれない TOE の複数のバリエーションまたはモデルをテストするための適切な戦略を判断すべきである。

386 SD の SFR 関連評価アクティビティは､SFR との適合を検証するために必要な、具体的なテストアクティビティを特定する。これらその他の評価アクティビティに特定されるテストは、ATE_IND.1.2E を満たす目的のために十分なテストのセットを構成する。評価アクティビティが行われるべき必要なテストを特定する一方で、各 SFR に特定されたセキュリティ機能についてインタフェースが十分にテストされたことを保証するのは評価者の責任であることに注意することは重要である。

3.4.1.1 評価アクティビティ：

387 評価者は TOE を検査して、ST に特定されるとおり評価に供される設定とテスト設定が一貫していることを判断しなければならない。

388 評価者は TOE を検査して、それが適切にインストールされ、既知の状態にあることを判断しなければならない。

389 評価者は､CEM の ATE_IND.1 に関するテストアクション及び SFR 関連評価アクティビティのテストアクションのすべてをカバーするテスト計画書を準備しなければならない。評価アクティビティに列挙されたテストそれぞれについて 1 つのテストケースを用意する必要はないが、評価者は SFR 関連評価アクティビティの該当するテスト要件それぞれがカバーされていることをテスト計画書に示さなければならない。

390 テスト計画書には、テストされるプラットフォームが特定され、そしてテスト計画書には含まれていないが ST に含まれているプラットフォームがあれば、そのプラットフォームをテストしないことについての正当化をテスト計画書が提供する。この正当化には、テストされるプラットフォームとテストされないプラットフォームとの相違を取り上げ、行われるべきテストにその相違が影響しないという論拠を示さなければならない。単にその相違が影響しないと主張するだけでは十分ではなく、根拠が提供されなければならない。ST に主張されるすべてのプラットフォームがテストされる場合には、根拠は必要とされない。

391 テスト計画書には、テストされるべき各プラットフォームの構成及び設定が記述され、また AGD 文書に含まれるもの以外に必要な設定アクションがあれば、それも記述される。評価者は、テストの一部として、または標準的なテスト前の条件として、AGD 文書に従って各プラットフォームの設置及び設定を行うことが期待されていることに、注意すべきである。これには、特別なテストドライバまたはツールが含まれるかもしれない。ドライバまたはツールそれぞれについて、そのドライバまたはツールが TOE 及びそのプラットフォームによる機能の実行に悪影響を与えないという、(単なる主張ではなく) 論拠が提供されるべきである。またこれには、用いられるべき任意の暗号エンジンの設定が含まれる (例えば、評価される暗号プロトコルのために)。

392 テスト計画書には、高レベルのテスト目的とともに、これらの目的を達成するために行われるべきテスト手順、及び期待される結果も特定される。

393 テスト報告書 (テスト計画書の単なるアップデートされたバージョンであってもよい) には、テスト手順が実施された際に行われたアクティビティが詳述され、またテストの実際の結果が含まれる。これは累積的な記述でなければならない。従って失敗に終わったテストの実行が存在し、修正がインストールされ、そして次にテストの再実行が成功した場合、報告には単なる「成功」の結果だけではなく、「失敗」及び「成功」の結果 (及びそれを支持する詳細) が示される。[2]

3.5 AVA：脆弱性評定

3.5.1 脆弱性調査 (AVA_VAN.1)

3.5.1.1 評価アクティビティ：

394 評価者は、本要件に関して存在する可能性のある脆弱性について、彼らの分析及びテストを文書化しなければならない。この報告書は ATE_IND のテスト報告書の一部に含まれてもよいし、あるいは別個の文書であってもよい。

395 評価者は、附属書 A に定義されるプロセスに従って仮説を策定する。評価者は、TOE について生成された欠陥仮説を、附属書 A.5 のガイドラインに従った報告書に文書化する。次に評価者は、附属書 A.4 に従って脆弱性分析を行わな

[2] テスト者またはテスト環境の側の過誤に起因した失敗をとらえる必要はない。ここでの意図は、計画されたテストの結果として、テスト計画書中にもともと指定されていたテスト設定への変更、ST 及びガイダンス文書中に特定された評価される構成への変更、または TOE 自体への変更が要求された際に、それを完全に明確に示すことである。

ければならない。分析の結果は、附属書 A.5 に従った報告書に文書化されなければならない。

4 要求される補足情報

396 本サポート文書ではさまざまな個所で、『補足情報』が評価に対する配付物の一部として支給される必要があるかもしれないという可能性について触れている。この用語は、セキュリティターゲットまたはガイダンス文書に必ずしも含まれず、また必ずしも公開されないかもしれない情報の記述を意図したものである。そのような情報の例としてはエントロピー分析、あるいは TOE に用いられる (または TOE を支援する) 暗号鍵管理アーキテクチャの記述が考えられる。任意のそのような補足情報に関する要件は、関連する cPP に特定されることになる。

397 本 SD に関連付けられた cPP は、 [NDcPP] 附属書 D に記述されるエントロピー分析を要求する。

5 参考資料

[CC1] 情報技術セキュリティ評価のためのコモンクライテリア、
パート 1：概説と一般モデル
CCMB-2012-09-001、バージョン 3.1 改訂第 4 版、2012 年 9 月

[CC2] 情報技術セキュリティ評価のためのコモンクライテリア、
パート 2：セキュリティ機能コンポーネント
CCMB-2012-09-002、バージョン 3.1 改訂第 4 版、2012 年 9 月

[CC3] 情報技術セキュリティ評価のためのコモンクライテリア、
パート 3：セキュリティ保証コンポーネント
CCMB-2012-09-003、バージョン 3.1 改訂第 4 版、2012 年 9 月

[CEM] 情報技術セキュリティ評価のための共通方法、
評価方法
CCMB-2012-09-004、バージョン 3.1 改訂第 4 版、2012 年 9 月

[FWcPP] ステートフルトラフィックフィルタファイアウォールのコラボラティブプロテクションプロファイル
バージョン 1.0、2015 年 2 月 27 日

[NDcPP] ネットワークデバイスのコラボラティブプロテクションプロファイル
バージョン 1.0、2015 年 2 月 27 日

[VAWP] ドラフト cPP 脆弱性分析ホワイトペーパー
バージョン 0.2 ドラフト

A. 脆弱性分析

A.1 序説

398 [VAWP] で述べられているように、脆弱性分析は本質的に主観的なアクティビティであるが、最小レベルの分析を定義することが可能であり、またある程度の客観性及び再現性 (または少なくとも比較可能性) を脆弱性分析プロセスに課すことも可能である。そのような客観性及び再現性を達成するために重要なのは、評価者が明確に定義されたアクティビティのセットに従い、また他の人々が彼の論拠に従って評価者と同一の結論に至ることが可能となるように、彼の結果を報告書に文書化することである。これは、異なる評価機関が全く同一の種類の脆弱性を特定することや、全く同一の結論に至ることを保証するものではないが、このやり方では最小レベルの分析及びその分析の適用範囲を定義し、その最小レベルの分析が評価機関によって行われるというある程度の保証をスキームに提供する。

399 この補足ガイダンスは [VAWP] に記述される情報をネットワークデバイス cPP へ、この技術種別に特有の変更と共に提供するものである。

400 以下のセクション「追加的な文書化」には iTC によって開発された、脆弱性評定アクティビティへの入力として提供されるべき文書のリストが含まれる。この文書のリストは、他の SAR または評価アクティビティによって義務付けられる文書に追加される (しかしそれによって部分的または全面的に複製されてもよい) ものである。

401 全体のプロセスは、欠陥仮説方法を用いて [CEM] に記述されるものに従っている : 評価者は潜在的な欠陥のリストを策定する (欠陥仮説) ; 評価者は欠陥を調査しそれらを処置する ; そして評価者は彼らの調査を詳述した報告書を作成する。以下のセクションは、これらのアクティビティそれぞれに対応している。セクション A.3 では、 [VAWP] に記述される 4 つのカテゴリのそれぞれにおける欠陥仮説を生成するために評価者が従うプロセスが詳述される。セクション A.4 では、欠陥を処置するにあたって評価者が従うプロセスが記述される。セクション A.5 では、脆弱性評定アクティビティに関して公言されることとされないことについての重要な詳細を含め、プロセスの報告の側面が記述される。セクション A.6 及び A.7 には、評価者が対応する必要のある欠陥仮説に関する情報であって、iTC によって作成されるものが含まれる。

A.2 追加文書

402 [VAWP] には、TOE 開発者によって評価チームへ提供されることになる適切な追加文書を、技術種別に基づいて iTC が決定することが示されている。この文書は、cPP 評価アクティビティ及びその他の SAR において指示されるものへの追加である。

403 ND cPP に関しては、追加文書には最低限、TOE を構成するソフトウェア及びハードウェア構成要素のリストが含まれる。ハードウェア構成要素は ST において主張されるすべてのシステムに該当し、また最小限、TOE によって利用されるネットワークハードウェア及びプロセッサが特定されるべきである。ソフトウェア構成要素には、基盤となる運用環境／オペレーティングシステムに加え、ウェブサーバ、プロトコルまたは暗号ライブラリほかのライブラリ等、主

要な構成要素が含まれる。この追加文書は構成要素の名称及びバージョン番号の単なるリストであり、分析中に仮説を策定するために評価者によって用いられることになる。

A.3 脆弱性情報の情報源

404 [VAWP] に概説されるようにcPPの脆弱性分析に用いられる手法は欠陥仮説法に基づいており、評価チームが欠陥仮説を立て、その後それらの欠陥を証明するか、反証するかのいずれかを行う。欠陥は、4つのソース (タイプ) から導かれる：

a) cPPによって記述される技術 (ここでは、ネットワークデバイス) に適用される欠陥仮説のリストであって、Common Vulnerability Enumeration (CVE) (訳注：共通脆弱性識別情報、Common Vulenerabilities and Exposures)または同様の情報源に由来するもの—cPP／補足ガイダンスには、iTCによって合意され定められた一連のものが存在する。さらに、これはCVE、またはTOEやその特定の構成要素へ直接適用される (以下に示すような) 同一の情報源へのエントリによって、補足される。また評価者は、cPP の公開日以降に発行されたそれらの情報源CVEにおける該当するエントリを、彼らの評定に含める。

b) cPP／補足ガイダンスに列挙される欠陥仮説のリストであって、その技術に特有の教訓及びその他の iTC インプットから導出されたもの (例えば、その他の公開情報源及び脆弱性データベースから導出されたものかもしれない) ；及び

c) 参照された公的な参考資料を含め、cPP／補足ガイダンス (セクション A.2 を含む)に記述されるベンダによって提供されるベースライン証拠資料及び SFR に基づいて評価者へ提供される情報から導出された欠陥仮説のリスト。

d) TC によって定義されたツール (例えば、nmap やファズテスタ、それらのアプリケーションもまた含まれるかもしれない) の利用によって生成された欠陥仮説のリスト。

A.3.1 タイプ 1 仮説—公開脆弱性データベースに基づくもの

405 セクション A.6 には、公開された脆弱性情報源のリストと、これらのソースのエントリであって上記タイプ 1 の欠陥仮説とみなされるべきものが含まれる。本リストを補足するために、評価者は、セクション A.6 の情報源であってcPPの公開日付よりも新しいもの、及び上記の追加の文書に特定されるとおりTOE及びそのコンポーネントに特有なものについても検索を行わなければならない。特定のエントリ、あるいは同一または異なる情報源からのエントリから生成された欠陥仮説に重複があれば、評価チームは、それを記録した上で考慮から外すことができる。A.6のリストはすべてのTOEに適用されると共に考慮されるべき欠陥の種別を示すものであり、それについて評価者は検索基準 (以下に示す) を用いて TOE に*具体的に*適用されるエントリのリストを収集することに注意すべきである。CVE エントリと関連付けられた分析の例については [VAWP] 附属書を参照されたい。

406 cPP の公開日以降に公開された情報源を検索する時に用いられるべき検索基準には、以下のものが含まれなければならない：

- 「ルータ (router)」及び「スイッチ (switch)」という用語
- 以下のプロトコル：TCP
- 上記に列挙されていない、TOE が (SFR によって) サポートする任意のプロトコル (これにはリモート管理プロトコル (IPsec, TLS, SSH) の少なくとも 1 つが含まれる)

407 TOE の特定構成要素のタイプ 1 欠陥仮説生成の一部として、評価者は、構成要素製造業者のウェブサイトについても検索し、これを基盤として欠陥仮説が作成できるかどうかを決定しなければならない (例えば、評価中の構成要素のバージョンにセキュリティパッチがリリースされている場合、これらのパッチの対象が欠陥仮説の基盤を形成するかもしれない)。

A.3.2 タイプ 2 仮説—iTC によって作成されたもの

408 セクション A.7 には、iTC によって本 cPP のために作成された欠陥仮説のリストが含まれる。タイプ 3 またはタイプ 4 の欠陥であって、本 cPP の将来のバージョンではセクション A.7 に含めることを考慮されるべきと評価者が確信するものを発見した場合、評価者は、iTC による検討のため、非独占的な欠陥の追加事項を提出すること。

A.3.3 タイプ 3 仮説—評価チームによって作成されたもの

409 タイプ 3 の欠陥については、製品によって提示された情報 (オンラインヘルプ、製品文書及び利用者ガイドなど) 及び (機能) テストアクティビティでの製品のふるまいに基づいて、評価者が自由に欠陥を策定できる。また評価者は、ベースライン証拠資料の一部ではない資料 (例えば、インターネットのメーリングリストから、あるいは開発者によって提供されたセットには含まれないインタフェースに関するインタフェース文書を読んで得た情報) に基づいて自由に欠陥を策定できるが、そのようなアクティビティは製品及び分析を行う評価機関によって大きく異なる可能性がある。

A.3.4 タイプ 4 仮説—ツールによって作成されたもの

410 評価者は、以下のアクティビティを行ってタイプ 4 欠陥仮説を生成しなければならない：

- ファジングテスト
  - 以下の送信の影響を検査する：
    - 各「Type」及び「Code」の値が、ICMPv4 (RFC 792) 及び ICMPv6 (RFC 4443) のそれぞれに対応する RFC において未定義であるような、変形したパケット
    - 各「トランスポート層プロトコル」の値が、IPv4 に対応する RFC (RFC 791) において未定義であるような変形したパケット。IPv6

(RFC 2460) もまた、これが TOE によりサポートされ、主張されている場合、網羅されるべきである。

これらのパケットはいずれも許可されるセションには属さないため、パケットは TOE によって処理されるべきではなく、また TOE はこのトラフィックによって悪影響を受けるべきではない。予期されない結果 (例、コアダンプ等) は、欠陥仮説の候補となる。

- 要求されるプロトコルヘッダの残りのフィールドについての変形ファジングテスト。このテストには、注意深く選択された値とランダムな値の両方が各ヘッダフィールドへ順番に挿入された整形されたパケットの変形したものを送信することを要求する (すなわち、テストには注意深く選択されたテストケースとランダムに挿入されたテストケースの両方が含まれる)。元の整形されたパケットは、通常の既存の通信ストリームの一部として受け入れられるであろうし、注意深く選択された変形が行われた際にも依然として有効なパケットとして受け入れられるかもしれない (個別のパケットだけでは有効となるだろうが、その内容は前後のパケットでは有効でないかもしれない) が、ランダムな値がフィールドへ挿入された際には有効なパケットではなくなることが多い。注意深く選択された値には、そのフィールドが表すデータの種別から決定できるような意味のある重要な値、例えば正負の整数、境界条件、無効な 2 値の組み合わせ (例、ビット間に依存関係のある一連のフラグ) を示す値、及び開始値または終了値を欠いたもの等が含まれるべきである。ランダムに選択された値によって整形されたパケットを得られないかもしれないが、それでもなお、それによってデバイスがセキュアでない状態になるかどうかを確認するために含まれている。予期されない結果 (例、コアダンプ等) は、欠陥仮説の候補となる。

411 iTC は、上記の欠陥仮説の作成アクティビティを達成するために用いられる具体的なツールを識別していないため、評価チームによって用いられる任意のツールが受け入れ可能である。評価チームは、このアクティビティで使用されたすべてのテストツールの名称、バージョン、パラメタ、及び結果をテスト報告書に記録しなければならない。

A.4 評価者脆弱性分析のプロセス

412 欠陥仮説が上記のアクティビティから作成されると、評価チームはこれらを処置する；すなわち、その仮説の証明、反証、または適用不可能の決定を試行する。このプロセスは [VAWP] に概説されるとおり、以下のようになる。

413 評価者は、TOE の各欠陥仮説を詳細化し、開発者より提供される情報を用いて、または侵入テストによって、反証しようと試みることになる。このプロセス中、評価者は、欠陥が存在するかどうかを決定するため、認証機関 (CB) に相談することなく自由に開発者と対話することができる。これには、開発者に追加の証拠資料 (例、詳細な設計情報、技術スタッフへの相談等) を要求することが含まれる；しかし、これらの要求のすべてについて、CB はコピーを受領するべきである。開発者が、評価アクティビティ／cPP の全体的なレベルに適合していないとして情報が要求されることを拒んだり、提出されていれば欠陥が反

証できたはずの証拠資料を提供できなかったりした場合、評価者は、一連の適切な資料を以下のように準備する：仮説の策定に使用された情報源の文書、及びそれが特定の TOE 機能に対するセキュリティ侵害の可能性を示す理由；それまで提供された証拠資料によって欠陥仮説が証明も反証もできなかった理由;ならびに欠陥仮説をさらに調査するために要求される情報の種別。次に CB が、追加の情報についての要求を承認または却下のいずれかをする。承認された場合、開発者は、欠陥仮説を反証するために、要求された証拠資料を提供する (または、もちろん欠陥を認めてもよい)。

414 各仮説について、評価者は、その欠陥仮説の反証が成功したか、識別された欠陥があることの証明に成功したか、または侵入テストの取り組みの一部として実施されるべきさらなる調査を要求するかについて、記録することになる。ここでも、これはミーティングや図表の作成によって行われてもよい。重要なのは、結果が文書化されることである。

415 欠陥が見つかった場合 (開発者が文書の分析に同意したことによって、あるいは侵入テストの取り組みによって)、評価者は、これらの欠陥をベンダへ報告することになる。確認されたすべての欠陥は、開発者によって対処されるべきであり、また解決策は、評価者によって合意され、評価報告書の一部として記録されるべきである。

416 セクション A.5 に示されるように、cPP に適合する TOE について実施された脆弱性分析に関する公開ステートメントは、タイプ 1 及び 2 (セクション A.3 に定義される) 欠陥仮説のみに関連付けられた欠陥のカバレージに限定される。iTC がこれらの仮説の候補を作成したという事実は、基本的な攻撃能力を持つ攻撃者によって悪用可能であるため、これらは対処されなければならないことを示している。

417 タイプ 3 及び 4 の欠陥については、欠陥が TOE の環境において悪用可能かどうかを決定する目的で、何が基本的な攻撃能力に相当するかを決定する責任は各 CB にある。これは CB によるアクティビティであるため、タイプ 3 及び 4 の欠陥に対する特定の TOE の耐性に関して公的な主張はなされない;むしろ、本附属書に概説されたアクティビティが実施されたこと、また任意の残存する脆弱性が基本的攻撃能力を有する攻撃者によって悪用可能なものではないことに評価チーム及び CB が合意したことについて主張される。

A.5 報告

418 評価者は、テストの取り組みに関して 2 つの報告書を作成しなければならない； ひとつは公開向けの (すなわち、機密情報を含まない評価報告書) もの、もうひとつは監督している CB へ配付されるものである。

419 公開向けの報告書は、評価者が製品に適用される CVE (セクション A.6 に加えて、セクション A.3.1 に従って評価者により作成された追加の CVE ベースの仮説を加えたもの) 及び iTC により cPP において特定されセクション A.7 に含まれるもの (これは上記のタイプ 1 及び 2 の仮説を包含する) を検査したことを示す単なるステートメントである。さらに、評価チームがタイプ 3 及び 4 の欠陥仮説をセクション A.3 に従って開発したこと、及び CEM のガイダンスに従って CB により定義されるように基本的な攻撃能力を有する攻撃者によって悪用可能な残存脆弱性が存在しないことを示すステートメントも存在する。そ

の他の情報は、公開向けの報告書には提供されない。

420 (内部の) CB 報告書については、作成されたすべての欠陥仮説；欠陥仮説を作成するために用いられたすべての文書；及び各欠陥仮説がどのように解決されたかについて評価チームが報告しなければならないことを提案する (これには、元の欠陥仮説が確認されたか反証されたか、及び残存脆弱性が基本的な攻撃能力を有する攻撃者によって悪用可能かどうかに関する任意の分析が含まれる)。 欠陥仮説を作成するために用いられた文書を識別するにあたり、評価チームは、それがサポート文書／評価アクティビティ (すなわち、それがベースライン証拠資料の一部を形成する) によって厳密に要求されるかどうか、及び文書の性質 (設計情報、開発者の技術ノート、等) を読者が決定できるように、文書を特徴付けなければならない。 評価の締めくくりに当たって、関心を持つ複数の CB (すべての当事者間の交渉の対象) 、及びおそらく iTC のその他のメンバーが、この情報をレビューし、その cPP へ適合する将来の評価のためのサポート文書への影響の決定を行える (例えば、大量の欠陥仮説が特定の種別の文書に基づいて生成された場合には、この分野における追加の文書が iTC によって将来の評価のために要求されるかもしれない)。

A.6 欠陥仮説のための CVE エントリ

421 このリストには、現在のところエントリが定義されていない。

A.7 追加の欠陥仮説

422 このリストには、現在のところエントリが定義されていない。

A.8 iTC のアクティビティ—cPP 及びサポート文書の維持管理

423 これまでのセクションに示されたように、何が公開され報告されるのかに関して脆弱性分析の適用範囲を決定するにあたり iTC が重要な役割を果たす。本セクションでは、評価チームにより調査されるべき欠陥が識別され、本 PP に適合する TOE の全般的な保証レベルと同等であり、かつこの技術について iTC によって懸念される領域を網羅することを保証するために iTC が行わなければならないアクティビティが詳述されている。

424 iTC によって達成される必要のある、4 つのアクティビティ (及び関連するアウトプット) が存在する：

1) iTC は、その脆弱性評定において評価チームが検査するために、どのような追加の文書が必要なのかを決定しなければならない。cPP 及び関連するサポート文書は、利用可能でなければならない情報について詳述する (例えば、サポート文書におけるさまざまな評価アクティビティで TSS により求められる情報)。iTC は、cPP またはサポート文書ではまだ網羅されていない (または部分的にしか網羅されていない) 追加の文書が必要であると感じた場合、その情報を定義し、セクション A.2 に含める。

2) iTC は、どの公開された脆弱性データベースがタイプ 1 (セクション A.3) 仮説の基盤として使用されるべきなのか、またこれらのデータベースのどの

エントリが該当するのかについて、決定しなければならない。本アクティビティを実行するにあたり、iTC はまず利用される情報源に関して合意する；例えば、Common Vulnerability Enumeration (CVE) のリスト。これが完全なリストであるとは期待されていないことに注意されたい；単に、その技術種別に関して脆弱性の良い表現を与えると iTC が感じるリストである。

情報源を識別した上で、各情報源について、iTC はリストのエントリを選択する基準を定義する。このリストと基準は、評価者が、cPP が発行された後に作成されたエントリを選択するため、同一の情報源と基準を評価時に利用できるように、セクション A.3.1 に識別されるべきである。基準を満たす各エントリについて、iTC は、評価チームによって考慮されるべきリストにそれを含めるかどうかを決定する。これにはおそらく、iTC によって合意されるエントリを判定するために、何らかの基準の作成が必要とされることになる。例えば、バッファオーバーフローに関連した欠陥仮説を作成するような CVE は、おそらく一般的な欠陥仮説としては拒絶されることになるだろう。

本アクティビティのアウトプットは、欠陥仮説の作成に当たって評価チームが適用可能とみなすであろうエントリのリストとなる。CVE データベースを用いてファイアウォールに適用されるこの分析アクティビティの例については [VAWP] の附属書を参照されたい。

3) iTC は、セクション A.6 に含まれていない、評価者が考慮すべき、任意の技術特有の脆弱性または脆弱性の種別が存在するかどうかを考慮しなければならない。これは、cPP に適合する以前の評価、iTC メンバーの経験、またはその他の要因に基づくものであってもよい。この一連の脆弱性 (タイプ 2) は、セクション A.7 に取り込まれるであろうし、評価チームによって考慮される必要があるであろう。cPP に関してより多くの経験が得られるまで、この種別について識別されるエントリはほとんどないか全く存在しないだろう。

4) iTC が実行しなければならない最後のアクティビティは、欠陥仮説 (タイプ 4) の作成を示唆する任意のツールまたはテストの識別である。iTC は、形成される必要のあるテストを単に概説することを選択でき、及びまたはそれららが特定のツールとそれらのツールを用いて行われるべきテストを識別することもできる。この定義において、iTC はまた欠陥仮説が作成されるべきことを示すテスト結果についても示す (本セクションの目的は、機能テストの実施や再実行ではない；欠陥仮説の候補となる異常を起こし得るような方法でテストすることである)。iTC 文書及び特定のツール；実行されるべき手順、設定、及びテスト；ならびにセクション A.3.4 におけるこれらの結果から欠陥仮説を作成するための基準。

B. ネットワークデバイスの等価性の考察

B.1 序説

425 本附属書は、ネットワークデバイスのコラボラティブプロテクションプロファイルへの適合を主張しようと望む製品のさまざまなモデルの等価性についてのベンダの要求に関して評価者が決定するための根拠を提供する。別個の TOE モデルには、各モデルにわたる別個のテストを必要とするかもしれない差異が含まれる可能性がある。以下に列挙するカテゴリのいずれにもバリエーションが存在しない場合、それらのモデルは等価であるとみなされ得る。

426 モデル間の等価性の決定は、セクション B.3 に記述されるように、さまざまなテスト結果をもたらす可能性がある。

427 いくつかの TOE が等価であると決定される場合、テストは TOE のひとつのバリエーションで実行されればよい。しかし、TOE のバリエーションがセキュリティに関連する機能上の相違がある場合、機能的または構造的な相違を持つ TOE モデルのそれぞれについて別々にテストされなければならない。一般的に、TOE の各バリエーション間での相違のみがテストされなければならない。その他の等価な機能については、代表的なモデルについてテストされればよく、複数のプラットフォームにわたる必要はない。

428 ベンダが等価性についての評価者の調査に同意しない場合、認証者は、等価性が存在するかどうかににについて、2 者間の調停を行う。

B.2 等価性を決定するための評価者ガイダンス

429 以下の表は、評価者が TOE のモデルのバリエーション間及び運用環境にわたる等価性に影響する要素のそれぞれについて考慮すべき記述を提供する。さらに、この表には、複数のモデルにわたる追加の別個のテストに至るシナリオも識別している。

要因	同一／同一でない	評価者ガイダンス
プラットフォーム／ハードウェア依存性	独立性	プラットフォーム／ハードウェア依存性が識別されない場合、評価者は、等価であるべき複数のハードウェアプラットフォームでのテスト考慮しなければならない。
	依存性	プラットフォーム／ハードウェアの間で具体的な相違がある場合、評価者は cPP 特有のセキュリティ機能に影響を与える相違があるか、またはそれらが cPP 特有でない機能に該当するか、について識別しなければならない。cPP で規定された機能がプラットフォーム／ハードウェアの提供するサービスに依存する場合、その製品が特定のハードウェアの組み合わせについて検証されたとみなされるためには、異なるプラットフォームのそれぞれにおいてテストされなければな

要因	同一／同一でない	評価者ガイダンス
		らない。このような場合、評価者は、プラットフォーム／ハードウェアの提供する機能に依存する機能のみを再テストするという選択肢を有する。相違が cPP 特有でない機能のみに影響する場合、それらのバリエーションは依然として等価であると考えられる。相違のそれぞれについて、評価者はなぜその相違が cPP 特有の機能に影響するか、または影響しないかの説明を提供しなければならない。
TOE ソフトウェアバイナリの相違	同一	モデルのバイナリが同一の場合、それらのモデルバリエーションは等価と考えなければならない。
	相違	モデルのソフトウェアバイナリ間に相違が存在する場合、その相違が cPP 特有のセキュリティ機能に影響するかどうかの決定が行われなければならない。cPP 特有の機能が影響を受ける場合、それらのモデルは等価でないとは考えられ、また別々にテストされなければならない。評価者は、ソフトウェアの相違に影響される機能のみを再テストするという選択肢を有する。相違が PP 特有でない機能のみに影響する場合、それらのモデルは依然として等価であると考えられる。相違のそれぞれについて、評価者はなぜその相違が cPP 特有の機能に影響するか、または影響しないかの説明を提供しなければならない。
TOE 機能を提供するために用いられるライブラリの相違	同一	さまざまな TOE モデルで使用されるライブラリ間で相違がない場合、それらのモデルバリエーションは等価であると考えられなければならない。
	相違	モデルのバリエーション間で別々のライブラリが使用される場合、cPP 特有の機能に影響を与えるライブラリによって機能が提供されるかどうかの決定がなされなければならない。cPP 特有の機能が影響を受ける場合、モデルは等価であるとは考えられず、別々にテストされなければならない。評価者は、含まれるライブラリにおける相違によって影響を受けた機能のみを再テストするという選択肢を有する。異なるライブラリが PP 特有でない機能のみに影響する場合、モデルは依然として等価であると考えられる。それぞれの異なるライブラリについて、評価者はなぜその異なるライブラリが cPP 特有の機能に影響を与えるのか、または影響を与えないのかについての説明を提供しなければならない。
TOE 管理インタフェースの相違	一貫性	さまざまな TOE モデル間で管理インタフェースの相違がない場合、モデルバリエーションは等価であると考えなければならない。

要因	同一／同一でない	評価者ガイダンス
	相違	製品がモデルのバリエーションに応じて別々のインタフェースを提供する場合、cPP 特有のセキュリティ機能がその異なるインタフェースによって設定可能かどうかの決定がなされなければならない。インタフェースの相違が cPP に特有の機能に影響する場合、それらのバリエーションは等価であるとは考えられず、別々のテストを行わなければならない。評価者は、異なるインタフェースによって設定可能な機能 (及び当該機能の設定) のみを再テストするという選択肢を有する。異なる管理インタフェースのみが PP に特有でない機能に影響する場合、それらのモデルは依然として等価であると考えられる。各管理インタフェースの相違について、評価者はなぜ異なる管理インタフェースが cPP 特有の機能に影響を与えるのか、または与えないのかについての説明を提供しなければならない。
TOE 機能の相違	同一	異なる TOE のモデルバリエーションによって提供される機能が同一の場合、それらのモデルバリエーションは等価であるとみなされなければならない。
	相違	異なる TOE モデルバリエーションによって提供される機能が異なる場合、機能的な相違が cPP 特有の機能に影響を与えるかどうかの決定がなされなければならない。cPP に特有の機能がモデル間で相違する場合、それらのモデルは等価であるとは考えられず、別々にテストされなければならない。これらの場合、評価者は、モデル間で相違する機能のみを再テストするという選択肢を有する。相違が cPP 特有でない機能のみに影響を与える場合、それらのバリエーションは依然として等価であると考えられる。それぞれの相違について、評価者はなぜその相違が cPP 特有の機能に影響を与えるのか、または与えないのかについての説明を提供しなければならない。

表 1 — 評価等価性分析

B.3 戦略

430 等価性分析を行うにあたって、評価者は各要因を独立に検討するべきである。個別の要因分析によって、それぞれ以下の 3 つの結果の 1 つがもたらされる。

- 個別の要因について、サポートされるすべてのプラットフォーム上の TOE のすべてのバリエーションは、等価である。この場合、テストは 1 つのテスト環境で行われてもよく、サポートされるすべてのモデルと環境で行われもよい。
- 個別の要因について、他のすべての等価な TOE と同一の動作をすることを保証するための別々のテストを要求するため、製品のあるサブセット

が識別される。分析によって、テストが必要なモデル／テスト環境の具体的な組み合わせが識別されることになる。

- 個別の要因について、TOE のどのバリエーションも等価ではなく、従ってテストはすべてのモデルと環境について行われる。

431 製品の完全な CC テストは、識別された要因のそれぞれについて行われる個別の分析それぞれの全体を包含することになる。

B.4 テストプレゼンテーション／告知における真実

432 何をテストすべきかを決定することに加えて、評価結果及びそれによって得られる認証報告書は、テストされた実際のモジュールとテスト環境の組み合わせが識別しなければならない。テストするサブセットを決定するために用いられた分析は機密であると考えられ、オプションとしてのみ公開情報に含められること。