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

2017 年 5 月

バージョン 2.0

CCDB-2017-XX-XXX

平成 29 年 10 月 25 日　翻訳 第 1.0 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「ガイダンス証拠資料」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利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：

V2.0, 2017 年 5 月 5 日 (公開バージョン)

V1.1, 2016 年 7 月 21 日 (公開レビュー用に発行された改訂版ドラフト)

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)、利用者ガイダンス証拠資料、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 6 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(must)。

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 本サポート文書の適用

9 本サポート文書 (SD) は、3 つの種別の評価アクティビティ－TOE 要約仕様 (TSS) 、ガイダンス証拠資料、及びテストを定義し、cPP と併せて利用されるよう設計されている。本 SD に依拠する cPP は、それらの EA[1]の情報源として明示的に識別する。本 cPP で規定されるそれぞれのセキュリティ要件(SFR または SAR)は、それに関連する複数の EA を持つ可能性がある。セキュリティ要件命名表記法は、セキュリティ要件と評価アクティビティの間で 1 対 1 の明確な対応を保証するように cPP と SD の間で一貫している。

10 cPP と SD は、cPP が SFR と SAR を列挙し、SD がそれぞれの SFR と SAR と対応する EA のカタログとなるように、互いに関連して利用されるように設計されている。cPP に含まれるいくつかの SFR は、オプションまたは選択ベースの者である。したがって、本 cPP への適合主張する ST は、本 cPP で定義されるすべての可能な SFR を必ずしも含まなければならない(have to)とは限らない。

11 本 cPP に適合する ST において、いくつかの操作が実行される必要がある(主に選択と割付)。いくつかの EA は、SFR において選択されたまたは割付された、異なる値について別々のアクションを定義する。評価者は、ST で主張されないような SFR に関連する EA についても、ST で主張されないような具体的な選択された、または割付された値に関連する EA についても、実行してはならない(shall)。

12 EA は、互いに独立して実行されることは、必ずしも必要ではない。ガイダンス証拠資料の記述、またはあるテストケースは、例えば、EA が同じ SFR または異なる SFR に関連しているかどうかにかかわらず、複数の EA を一度にカバーすることが可能である。

[1] 一般に cPP は、SFR の異なるセットのための評価アクティビティについての情報源として、一つ以上の SD を参照するかもしれない。

1.4 用語

1.4.1 用語集

13 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。

用語	意味
管理者(Administrator)	セキュリティ管理者を参照
鍵チェイニング(Key Chaining)	データを保護するために暗号鍵の複数レイヤを使用する方法。上段レイヤの鍵がデータを暗号化するより下位のレイヤの鍵を暗号化する；この方法はいかなるレイヤ数でも持つことができる。
保証(Assurance)	TOE が SFR を満たしていることを信頼するための根拠[CC1]。
必須の補足情報 (Required Supplementary Information)	必ずしもセキュリティターゲットまたは操作ガイダンスに含まれる必要がない情報で、必ずしも公開される必要がないもの。このような情報の例として、TOE(または、TOE のサポート)で利用される、エントロピー分析、または暗号鍵管理アーキテクチャの記述。このような補足情報についての要件は、関連する cPP で識別される(セクション 6 での記述を参照)。
セキュリティ管理者 (Security Administrator)	用語「管理者」、「セキュリティ管理者」、及び「利用者」は現時点において本証拠資料の中で殆ど同じ意味で用いられており、そして設定と管理のタスクを実行するために TOE に許可されたアクセスをしている人物を表すために用いられる。
評価対象 (Target of Evaluation)	ガイダンスを伴うことがあるソフトウェア、ファームウェア及び／またはハードウェアのセット。[CC1]
TOE セキュリティ機能(TSF) (TOE Security Functionality) (TSF)	SFR の正しい実施のために必要とされる TOE のすべてのハードウェア、ソフトウェア、及びファームウェアの複合機能。[CC1]
TSF データ (TSF Data)	要件実施が依存する TOE のふるまいのためのデータ。
利用者(User)	セキュリティ管理者を参照

1.4.2 略語

頭字語	意味
cPP	collaborative Protection Profile コラボラティブプロテクションプロファイル
CA	Certificate Authority 認証局
CN	Certificate Name 証明書名称

CVE	Common Vulnerabilities and Exposures (database) 共通脆弱性データベース
DN	Domain Name ドメイン名
DNS	Domain Name Service ドメイン名サービス
EA	Evaluation Activity 評価アクティビティ
ECDHE	Elliptic Curve Diffie-Hellman Key Exchange 楕円曲線ディフィヘルマン鍵交換
iTC	International Technical Community 国際的な技術部会
NIST	National Institute of Standards and Technology
SAN	Storage Area Network
SAR	Security Assurance Requirement セキュリティ保証要件
SD	Supporting Document
SSL	Secure Socket Layer
TLS	Transport Layer Security

2 SFR の評価アクティビティ

14 本セクションの EA は、具体的な SAR (例、ASE_TSS.1、ADV_FSP.1、AGD_OPE.1、及び ATE_IND.1)をカバーする技術特有の観点に対処するため、評価者が実行するアクションを捉えているー これは、セクション 5 (SAR の評価アクティビティ)で実行されるような CEM ワークユニットに追加されたものである。

15 設計記述に関して (非公開として取り扱われるかもしれない必須の補足資料と同様に、TSS というラベルのサブセクションによって指定される)、評価者は、EA を満たすような具体的な情報があることを保証しなければならない(must)。TSS セクションに関する所見について、評価者の判定は、CEM ワークユニット ASE_TSS.1-1 と関係付けられている。補足の証拠資料に関連する評価者の判定も、ASE_TSS.1-1 と関係付けられる、なぜならこのような証拠資料を提供するための要件は、本 cPP の ASE で規定されているからである。

16 SFR に付随して、ガイダンス証拠資料が管理者／利用者に対して十分な情報を提供することを保証するため、評価者の判定は、CEM ワークユニット ADV_FSP.1-7、AGD_OPE.1-4、及び AGD_OPE.1-5 と関係付けられていること。

17 最終的に、テストとラベル付けされたサブセクションは、iTC が関連する SFR における製品のテストが必要であることを決定したところである。評価者は、テストを開発することが期待されるが、開発者がテストを作成することがより現実的な場合があるかもしれないし、または開発者が既存のテストを持っているかもしれない。ゆえに、テストの実行の代わりに、開発者の生成したテストに評価者が立ち会うことは受け入れ可能である。この場合、評価者は、開発者のテストが開発者によって宣言されたやり方及び EA によって義務付けられたやり方の両方で実行されていることを保証しなければならない(must)。本セクションで規定された EA に関連する CEM ワークユニットは以下のとおりである : ATE_IND.1-3、ATE_IND.1-4、ATE_IND.1-5、ATE_IND.1-6、及び ATE_IND.1-7。

分散型 TOE についての追加の注釈

18 分散型 TOE について、操作ガイダンス情報のすべての検査は、TOE 全体が正しく構築されるように個別のコンポーネントを設定するために十分な情報を定義していることの確認を含むよう拡張されるべきである(should)。

19 SFR の評価アクティビティは、SFR を実装するすべての分散型 TOE コンポーネントに対して実行されなければならない(must) (SFR からコンポーネントへのマッピングで定義されるとおりー参照、セクション 5.1.2)。これは、本セクションのコアな SFR と同様に、セクション 3 と 4 のオプション SFR と選択ベース SFR に適用される。

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 TSS

20 FAU_GEN.1.1c で定義されるとおり、暗号鍵の生成／インポート、変更、または削除の管理者タスクについて、TSS は、どの情報が関連する鍵を識別するためにログ出力されるかを識別するべきである(should)。

21 分散型 TOE について、評価者は、TOE コンポーネントによって監査対象事象が生成され、記録されることについて TSS に記述していることを保証するため、TSS を検査しなければならない(shall)。評価者は、特定の SFR についての監査情報を生成すると定義されたすべてのコンポーネントが、SFR から TOE コンポーネントへのマッピングにおいて定義されたように、その SFR にも寄与するべきある(should)こと、及びそれぞれのコンポーネントによって生成された監査記録が実装されるすべての SFR をカバーすることを確認しなければならない(shall)。

2.1.1.2 ガイダンス証拠資料

22 評価者は、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するため、ガイダンス証拠資料をチェックしなければならない(shall)。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(must)。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、監査事象の表で規定される追加的情報が含まれることを確認するため、チェックしなければならない(shall)。

23 評価者は、設定変更に関連する TSF データに関連する管理アクションについても決定しなければならない(shall)。評価者は、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、ガイダンス証拠資料を検査し、cPP で規定される要件を実施するために必要な TOE に実装されたサブコマンド、スクリプト、メカニズムの設定 (有効化及び無効化を含む) を含めて、管理コマンドを決定しなければならない(shall)。評価者は、管理者ガイドのどのアクションが設定変更に関連する TSF データに関連するかを決定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(shall)。評価者は、対応するガイダンス証拠資料がそれに関連する要件を満たしていることの保証に対応するアクティビティの一部として本アクティビティを実行してもよい。

2.1.1.3 テスト

24 評価者は、上記に列挙された監査事象と管理者アクションの表に列挙された事象についての監査記録を TOE に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(shall)。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(should) : 例えば、システムにいくつかの異なる I&A メカニズムがある場合、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(must)。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(shall)。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。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証拠資料で規定されたフォーマットと合致すること、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(shall)。

25 分散型 TOE について、評価者は、セキュリティターゲットにおける TOE コンポーネントへの監査対象事象のマッピングに従って、すべての TOE コンポーネントについて、テストを実行しなければならない(shall)。監査事象が発生するときに複数の TOE コンポーネントを含むようなすべての事象について、評価者は、事象が両方の側で監査されること(例、2 つのコンポーネント間のセキュアな通信チャネルの構築失敗)をチェックしなければならない(has to)。エラーの場合に限らないが、TOE コンポーネント間のセキュアな通信チャネルの構築／終了の成功のような、成功したアクションについての事象も含む。

26 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併せて達成できることに留意されたい。

2.1.2 FAU_GEN.2 利用者識別情報の関連付け

2.1.2.1 テスト

27 このアクティビティは、FAU_GEN.1.1 のテストと併せて達成されるべきである(should)。

28 分散型 TOE について、評価者は、監査対象事象が別のコンポーネントによって引き起こされるような状況で、その事象を記録するコンポーネントが扇動者の本人性を伴った事象と関係することを検証しなければならない(shall)。評価者は、別のコンポーネントが監査対象事象を引き起こすようなところで、1 つのコンポーネントについて少なくとも 1 つのテストを実行しなければならない(shall)。評価者は、その事象が期待されるとおりにそのコンポーネントによって記録されること及びその事象が引き起こしているコンポーネントと関係していることを検証しなければならない(shall)。別のコンポーネントによって引き起こされる事象が 2 つの TOE コンポーネント間のセキュアなチャネルを構築するために少なくとも生成可能であることが仮定されている。何らかの理由(例、TSS またはガイダンス証拠資料、の可能性がある)で、TOE 全体がその他のコンポーネントによって引き起こされた任意の事象を生成しないという評価者の結論に至った場合、本要件は省略されなければならない(shall)。

2.1.3 FAU_STG_EXT.1 保護された監査事象格納

2.1.3.1 TSS

29 評価者は、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するため、TSS を検査しなければならない(shall)。

30 評価者は、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ストアが満杯の際に何が起こるか ; 及びこれらの記録が許可されないアクセスに対して保護される方法について TSS に記述されていることを保証するため、TSS を検査しなければならない(shall)。

31 評価者は、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するため、TSS を検査しなければならない(shall)。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規則の概要が含まれるべきである(should)。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(shall)。

32 評価者は、外部 IT エンティティへの監査情報の送信がリアルタイムに、または定期的に実行可能であるかどうかについて詳述されていることを保証するため、TSS を検査しなければならない(shall)。TOE がリアルタイムに送信を実行しないような場合、評価者は、TSS に監査データの転送についての受け入れ可能な頻度と同様に実現可能な頻度についての詳細が提供されていることを検証する必要がある。

33 分散型 TOE について、評価者は、本 SFR が適用される TOE コンポーネントへ、及び外部監査サーバへの監査データ転送が異なる TOE コンポーネントの間でも実装されていることについて TSS に記述されていることを保証するため、TSS を検査しなければならない(shall) (例、すべての TOE コンポーネントは、それ自身の転送を行う、またはそのデータは外部監査サーバへすべての監査事象の集中転送のため、別のコンポーネントへ送信される)。

34 分散型 TOE について、評価者は、どのコンポーネントが監査情報をローカルに格納しているか、及びどのコンポーネントが監査データをバッファリングし、ローカル保存のために別の TOE コンポーネントへその情報を転送しているかについて TSS に記述されていることを保証するため、TSS を検査しなければならない(shall)。すべてのコンポーネントについて、TSS は、ローカル格納領域またはバッファ領域が使い尽くされるときのふるまいについて記述しなければならない(shall)。

2.1.3.2 ガイダンス証拠資料

35 評価者は、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するため、ガイダンス証拠資料についても検査しなければならない(shall)。

36 また評価者は、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決定するため、ガイダンス証拠資料についても検査しなければならない(shall)。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、ということである。

37 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についても保証しなければならない(shall)。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(shall)。

2.1.3.3 テスト

38 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対応して規定されるとおり実行されるだろう。評価者は、この要件に関して以下の追加的なテストを実行しなければならない(shall) :

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(shall) 。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クを検査しなければならない(shall)。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観測しなければならない(shall)。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(shall)。評価者は、TOE が管理者の仲介なしに監査データを外部監査サーバへ自動的に転送できることを検証しなければならない(shall)。

b) テスト 2 : 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(shall)。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(shall)。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

   1) 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 (FAU_STG_EXT.1.3 の選択肢『新たな監査データを破棄』について)。

   2) 既存の監査データは規定される規則に従って、追跡されるべきすべての新しい監査対象事象で上書きされる (FAU_STG_EXT.1.3 の選択肢『以前の監査記録を上書き』について)

   3) 規定されるとおり TOE がふるまう(FAU_STG_EXT.1.3 の選択肢『その他のアクション』について)。

c) テスト 3 : TOE が FAU_STG_EXT.2/LocSpace に適用する場合、評価者は、FAU_STG_EXT.2/LocSpace についての選択に従って TOE によって提供される数が FAU_STG_EXT.1.3 のテストを実行しているときに正しいことを検証しなければならない(shall)。

d) テスト 4 : 分散型 TOE について、上記で定義されたテスト 1 は、外部監査サーバへ監査データを転送するようなすべての TOE コンポーネントへ適用可能であるべきである (should) 。 FAU_STG_EXT.1.2 と FAU_STG_EXT.1.3 に従ったローカル格納について、上記で定義されたテスト 2 は、監査データをローカルに格納するようなすべての TOE コンポーネントへ適用されなければならない(shall)。監査データをローカルに格納し、FAU_STG_EXT.2/LocSpace に適合するすべての TOE コンポーネントについて、上記で規定されたテスト 3 は、適用されなければならない(shall)。評価者は、外部監査サーバへの監査データの転送が実装されることを検証しなければならない(shall)。

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

39 評価者は、TOE のサポートする鍵長について TSS が識別していることを保証しなければならない(shall)。ST が 2 つ以上のスキームを規定する場合、評価者は、各スキームの用途が識別されていることを検証するため、TSS を検査しなければならない(shall)。

2.2.1.2 ガイダンス証拠資料

40 評価者は、セキュリティターゲットで定義されるすべての暗号プロトコルについて、選択された鍵生成スキーム及び鍵長を TOE が利用するよう設定する方法について AGD ガイダンスが管理者に指示していることを検証しなければならない(shall)。

2.2.1.3 テスト

41 注釈：以下のテストは、工場製品に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を、開発者に要求する。

FIPS PUB 186-4 RSA スキームのための鍵生成

42 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(shall)。このテストは、公開検証指数 *e*、プライベート素因数 *p* 及び *q*、公開モジュラス (modulus) *n* 及びプライベート署名指数 *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。

43 鍵ペア生成は、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) を規定する。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(shall)
   - 素数 p1、p2、q1 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(shall)
   - 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(shall)

44 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値として TSF 鍵生成ルーチンに与えなければならない(must)。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(shall)。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(shall)。

楕円曲線暗号 (ECC) のための鍵生成

FIPS 186-4 ECC 鍵生成テスト

45 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 個のプライベート鍵／公開鍵ペアを試験対象実装 (IUT) に生成を要求しなければならない(shall)。プライベート鍵は、承認済み乱数ビット生成器 (RBG) を用いて生成されなければならない(shall)。正しいことを決定するため、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) 機能へ入力しなければならない(shall)。

FIPS 186-4 公開鍵検証 (PKV) テスト

46 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 個のプライベート鍵／公開鍵ペアを生成し、5 個の公開鍵を正しくない値となるように変更し、5 個を未変更の (即ち、正しい) 値のままにしなければならない(shall)。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(shall)。

有限体暗号 (FFC) のための鍵生成

47 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(shall)。このテストは、フィールド素数 p、暗号学的素数 q (p-1 を割り切る)、暗号群生成元 g、ならびにプライベート鍵 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。

48 パラメタ生成では、暗号学的素数 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(shall)
- 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(shall)

49 そして、暗号群生成元 g を生成するための 2 とおりの方法を規定する：

- 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

50 鍵生成では、プライベート鍵 x を生成するための 2 とおりの方法を規定する：

- 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 modulus とする剰余演算及び +1 演算を行ったもの、ここで 1<= x<=q-1

51 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(must)。

52 証明可能素数手法の暗号学的素数及びフィールド素数生成手法、及び／または

検証可能プロセスの群生成元 g 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値として TSF パラメタ生成ルーチンに与えなければならない(must)。

53 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(shall)。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(shall)。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

54 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(must)。

2.2.2 FCS_CKM.2 暗号鍵確立

2.2.2.1 TSS

55 評価者は、サポートされる鍵確立スキームが FCS_CKM.1.1 で識別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(shall)。ST が複数のスキームを規定する場合、評価者は、各スキームの用途が識別されていることを検証するため、TSS を検査しなければならない(shall) (TOE が送信者、受信者、または両方として動作するかどうかを含めて)。Diffie-Hellman group14 が FCS_CKM.2.1 から選択される場合、TSS にはその実装が RFC3526 セクション 3 をどのように満たすかについて記述しなければならない(shall)。

2.2.2.2 ガイダンス証拠資料

56 評価者は、選択された鍵確立スキームを TOE が利用するように設定する方法について AGD ガイダンスが管理者に指示していることを検証しなければならない(shall)。

2.2.2.3 テスト

鍵確立スキーム

57 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(shall)。

SP800-56A 鍵確立スキーム

58 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(shall)。各鍵共有スキームに対するこれらの検証テストは、推奨事項 (訳注 : SP 800-56A) 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(訳注 : 離散対数暗号 ; Discrete Logarithm Cryptography)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 (key confirmation) 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(shall)。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

59 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(shall)。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(shall)。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(static key)であるか、短期鍵(ephemeral key)であるか、またはその両方である。

60 評価者は、DKM、対応する TOE の公開鍵 (静的鍵及び／または短期鍵)、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(shall)。

61 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(shall)。

62 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(shall)。

63 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 は上記を実行しなければならない(shall)。

検証テスト

64 検証テストは、鍵確認あり、または鍵確認なしでの相手方の有効な及び無効な鍵共有の結果を認識する 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、TOE が認識可能であるべきエラーがどれかを決定するため、SP800-56A 鍵共有の実装に含まれる、サポートしている暗号機能のリストを取得しなければならない(shall)。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。

65 評価者は、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するため、テストベクタの一部にエラーを注入しなければならない(shall) : 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 の静的プライベート鍵へ個別にエラーを注入し、公開

鍵検証機能及び／または部分的な鍵検証機能 (ECC のみ)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改変されないままでなければならず(shall)、従って有効な鍵共有の結果をもたらすべきである(should) (それらは合格であるべきである(should))。

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

SP800-56B 鍵確立スキーム

67 TOE が送信者としてふるまう場合、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するため、以下の保証アクティビティが実行されなければならない(shall) :

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(shall)。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(shall)。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(shall)。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 が利用されなければならない(shall)) 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(shall)。

68 TOE が受信者としてふるまう場合、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するため、以下の保証アクティビティが実行されなければならない(shall) :

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(shall)。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(shall)。各テストベクタには RSA プライベート鍵、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(shall)。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(shall)。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(shall)。

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(shall)。NIST Special Publication 800-56B に従い、出力された、またはログ出力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、またはログ出力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(shall)。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、またはログ出力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(shall)。

Diffie-Hellman Group 14

69 評価者は、Diffie-Hellman group 14 を利用するような FTP_TRP.1/Admin、FTP_TRP.1/Join、FTP_ITC.1 及び FPT_ITT.1 で選択されたそれぞれのプロトコルについて、既知の良好な実行を用いることによって Diffie-Hellman group 14 の TSF の実装の正確さを検証しなければならない(shall)。

2.2.3 FCS_CKM.4 暗号鍵破棄

2.2.3.1 TSS

70 評価者は、関連するすべての鍵(それぞれの起源と格納場所を記述することで)、すべての関連する鍵破棄の状況 (例、工場設定へのリセットまたはデバイスワイプ機能、高信頼チャネルの切断、セキュアチャネルプロトコルの一部としての鍵変更) 及びそれぞれの場合に利用される破壊方法を列挙していることを保証するため、TSS を検査する。本評価アクティビティの目的について、関連する鍵はセキュリティターゲットの SFR のいずれかをサポートするために信頼されるようなそれらの鍵である。評価者は、鍵及び格納場所の記述が TOE によって実行される機能と一貫していることを確認する(例、TOE 特有のセキュアチャネルとプロトコル用のすべての鍵、または FPT_APW_EXT.1 及び FPT_SKP_EXT.1 をサポートするものの所在が確認される [2])。特に、TOE が平文の鍵を不揮発性メモリに格納しないと主張する場合、評価者は、これが TOE の動作と一貫していることをチェックする。

71 評価者は、TOE が不揮発性メモリに平文として保存された鍵を破壊する方法について TSS が識別すること、及び TOE が鍵を破壊するために利用するようなインタフェースの識別と記述をその記述に含むことを保証するため、チェックしなければならない(shall) (例、ファイルシステム API、鍵ストア API 等)。

[2] 鍵が別の鍵で暗号化またはラップされて格納される場合、評価者が鍵の記述が TOE 機能と一貫していることを確認できように、これについて説明される必要があるかもしれない。

72 選択肢に、「*参照の破壊*」(揮発性メモリについて) または 「*インタフェースの呼び出し*」(不揮発性メモリについて) を含む場合、関連するインタフェース定義が、インタフェースが TSS の選択肢と記述をサポートすることを保証するため、評価者によって検査されることに留意されたい。不揮発性メモリの場合、評価者は、平文の鍵が格納されるそれぞれのメディア種別についての関連インタフェース記述の検査を含める。OS レベル及びストレージデバイスレベルのスワップ及びキャッシュファイルの存在は、現在のバージョンの評価アクティビティでは検査されない。

73 TSS が平文でない形式で保存されるような鍵を識別する場合、評価者は、利用される暗号化方法と鍵暗号化鍵について TSS が識別していること、及び鍵暗号化鍵が暗号化された形式で自身が格納されるか、または FCS_CKM.4 の下で含まれる方法によって破壊されることをチェックしなければならない(shall)。

74 評価者は、鍵破壊要件に適合しないかもしれないようなあらゆる設定または状況について TSS で識別されていることをチェックしなければならない(shall) (以下のガイダンス証拠資料のさらなる説明を参照)。破壊が妨げられたり、遅延されたりするかもしれないようなケースについての詳細な記述についてのガイダンス証拠資料への参照がなされるかもしれないことに留意されたい。

75 鍵を上書きするための「任意の CSP を含まないような値」の利用を ST が規定する場合、評価者は、そのパタンが取得される方法及び利用方法について TSS に記述していること、及びこれがそのパタンに任意の CSP を含まないという主張を正当化することを保証するため、TSS を検査する。

2.2.3.2 ガイダンス証拠資料

76 TOE は、何らかの場合に鍵破壊を妨げる、または遅延させることが可能な状況の対象となるかもしれない。評価者は、鍵破壊要件に厳密に（訳注：正確に）適合しないかもしれない設定または状況についてガイダンス証拠資料に識別されていること、及びこの記述が TSS (及びその他の利用される補足情報) の関連する部分と一貫していることをチェックしなければならない(shall)。評価者は、鍵破壊が物理層で遅延されるかもしれないような状況についてのガイダンスをガイダンス証拠資料が提供することをチェックしなければならない(shall)。

77 例えば、TOE が物理メモリへフルアクセスしないとき、ストレージがウェアレベリング及びガーベージコレクションを実装している可能性がある。これは、論理的にアクセスできないが物理的に永続するような鍵の追加複製ができているかもしれない。可能であれば、TOE は、これらの永続的な複製の削除に際して、TRIM コマンド[3]の利用及びこれらを破壊するためのガーベージコレクションの利用について記述しているかもしれない(これは TSS 及び操作ガイダンスで説明される)。

2.2.4 FCS_COP.1/DataEncryption 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

[3] TRIM が利用される場合、TSS 及び／またはガイダンス証拠資料にも、TRIM へアクセスできないように鍵が格納される方法について記述していると期待される(例、それらは、マスターフィアルテーブルに完全に含まれるであろう 982 バイト以下のファイルには含まれる必要はない)。

78 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(shall)。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。正しいことを決定するため、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(shall)。

79 **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(shall)。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(shall)、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(shall)。

80 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実行しなければならない(shall)。

81 **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(shall)。5 個の鍵は 128 ビットの鍵としなければならず(shall)、それ以外の 5 個は 256 ビットの鍵としなければならない(shall)。

82 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実行しなければならない(shall)。

83 **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(shall)。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(shall)、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(shall)。[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(shall)。

84 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(shall)。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(shall)、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(shall)。[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(shall)。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(shall)。

85 **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(shall)。[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(shall)。

86 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実行しなければならない(shall)。

AES-CBC 複数ブロックメッセージテスト

87 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(shall)。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(shall)。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(shall)。

88 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(shall)。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(shall)。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(shall)。

AES-CBC モンテカルロテスト

89 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(shall)。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(shall)、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(shall)。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(shall)。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(shall)。

```
# 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]
```

90 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(shall)。

91 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(shall)。

AES-GCM テスト

92 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 の認証付き暗号化機能をテストしなければならない(shall)。

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(shall) (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(shall) (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(shall) (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(shall)。

93 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(shall)。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(shall)。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。

94 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(shall)。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(shall)。

95 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。正しいことを決定するため、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(shall)。

AES-CTR 既知解テスト

96 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、IV、及び暗号文の値は 128 ビットのブロックとしなければならない(shall)。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。正しいことを決定するため、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(shall)。

97 **KAT-1.** 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(shall)。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(shall)、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(shall)。復号機能をテストするため、評価者は入力として 10 個の暗号文の値を用いて、暗号化と同一のテストを実行しなければならない(shall)。

98 **KAT-2.** 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(shall)。5 個の鍵は 128 ビットの鍵としなければならず(shall)、それ以外の 5 個は 256 ビットの鍵としなければならない(shall)。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を用いて、暗号化と同一のテストを実行しなければならない(shall)。

99 **KAT-3.** 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(shall)。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(shall)、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(shall)。[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(shall)。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復号から得られる平文の値を取得しなければならない(shall)。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(shall)、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(shall)。[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(shall)。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(shall)。

100 **KAT-4.** 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、所与の平文の暗号化から得られる) を取得しなければならない(shall)。[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(shall)。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を用いて、暗号化と同一のテストを実行しなければならない(shall)。

AES-CTR 複数ブロックメッセージテスト

101 評価者は、i 個のブロックからなるメッセージ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(shall)、ここで i は 1 より大きく、10 以下とする。それぞれの i について、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、試験されるべきモードを用いて、選んだ鍵を用いてメッセージを暗号化しなければならない(shall)。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(shall)。また評価者は、*i* 個のブロックからなるメッセージを復号することによって、復号機能をテストしなければならない(shall)、ここで i は 1 より大きく、10 以下とする。それぞれの i について、評価者は鍵及び長さ *i* ブロックの暗号文メッセージを選び、試験されるべきモードを用いて、選んだ鍵を用いてメッセージを復号しなければならない(shall)。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を用いて復号した結果と比較されなければならない(shall)。

AES-CBC モンテカルロテスト

102 評価者は、200 個の平文／鍵のペアを用いて、暗号化機能をテストしなければならない(shall)。これらのうち 100 個は 128 ビットの鍵を用いて、これらのうち 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(shall)。平文の値は、128 ビットのブロックとしなければならない(shall)。それぞれのペアについて、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(shall)：

```
# 入力：PT, IV, Key
for i = 1 to 1000:
```

CT[1] = AES-CTR-Encrypt(Key, PT) PT = CT[i]

103 1000 回目の反復処理において計算された暗号文が、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(shall)。

104 復号エンジンをテストする必要はない。

2.2.5 FCS_COP.1/SigGen 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

105 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(shall)。正しいことを決定するため、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(shall)。

ECDSA FIPS 186-4 署名検証テスト

106 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(shall)。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(shall)。

RSA 署名アルゴリズムテスト

署名生成テスト

107 評価者は、TOE のサポートする modulus 長／SHA の組み合わせのそれぞれについて、10 個のメッセージを生成または取得すること。TOE は、対応する署名を生成し、返す。

108 評価者は、署名検証アルゴリズムの信頼される参照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、TOE の署名の正しさを検証しなければならない(shall)。

署名検証テスト

109 選択されたそれぞれの modulus 長／ハッシュアルゴリズムについて、評価者は、modulus 及び 3 つの関連する鍵ペア、(*d, e*)を生成する。それぞれのプライベート鍵 *d* は、署名生成アルゴリズムの信頼される参照実装を用いてそれぞれ 1024 ビットの 6 つの疑似ランダムなメッセージに署名するために利用される。公開鍵 e、メッセージ、または署名のいくつかは、署名検証が失敗するように変更される。オリジナルのメッセージのセット及び変更されたメッセージのセットの両方について：modulus、ハッシュアルゴリズム、公開鍵 e の値、メッセージ、および署名が TOE に送られ、次に署名の検証を試行し、検証結果を返す。

110 評価者は、TOE がオリジナルメッセージ上の正しい署名を確認し、変更された

メッセージに導入されたエラーを検出することを検証する。

2.2.6 FCS_COP.1/Hash 暗号操作 (ハッシュアルゴリズム)

2.2.6.1 TSS

111 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(shall)。

2.2.6.2 ガイダンス証拠資料

112 評価者は、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決定するため、AGD 文書をチェックする。

2.2.6.3 テスト

113 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。

114 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(shall)。

ショートメッセージテスト—ビット指向モード

115 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(shall)。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

116 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(shall)。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

117 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(shall)。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

118 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(shall)。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

119 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/KeyedHash 号操作 (鍵付きハッシュアルゴリズム)

2.2.7.1 TSS

120 評価者は、HMAC 機能によって利用される以下の値が規定されていることを保証するため、TSS を検査しなければならない(shall) : 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

121 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(shall)。各セットは、1 つの鍵とメッセージデータから構成されなければならない(shall)。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(shall)。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(shall)。

2.2.8 FCS_RBG_EXT.1 拡張：暗号操作 (乱数ビット生成)

122 [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(shall) (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(shall))。

2.2.8.1 TSS

123 評価者は、DRBG の種別を規定すること、DRBG にシード値を供給するエントロピー源を識別すること、及びそれぞれの情報源によって別々に提供されるミニマムエントロピーまたは組み合わされたシード値に含まれるミニマムエント

ロピーのいずれかの推定または計算についての記述していることを決定するために、TSS を検査しなければならない(shall)。

2.2.8.2 ガイダンス証拠資料

124 評価者は、ガイダンス証拠資料に RNG 機能を設定するための適切な指示が含まれていることを確認しなければならない(shall)。

2.2.8.3 テスト

125 評価者は、RNG 実装に対して 15 回の試行を実行しなければならない(shall)。RNG が設定可能な場合、評価者は各設定について 15 回の試行を実行しなければならない(shall)。

126 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) 乱数ビットの最初のブロックを生成し、 (3) 乱数ビットの 2 番目のブロックを生成し、 (4) 非インスタンス化する、という手順からなる。評価者は、乱数ビットの 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(shall)。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。「乱数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 と等しい乱数ビットを生成することを意味する。

127 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) 乱数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) 乱数ビットの 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、乱数ビットの 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(shall)。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。

128 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、シード値の長さと等しくなければならない(shall)。

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値の長さの半分となる。

Personalization String： Personalization String の長さは、シード値の長さ以下でなければならない(shall)。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利用できる。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(shall)。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。

2.3 識別と認証 (FIA)

2.3.1 FIA_AFL.1 認証失敗管理

2.3.1.1 TSS

129 評価者は、リモート管理アクションのそれぞれのサポートされる方法について、連続する不成功の認証試行が検知され追跡される方法についての記述が TSS に含まれていることを決定するために TSS を検査しなければならない(shall)。TSS には、リモート管理者が TOE へのログイン成功を防止するための方法、及びこの能力をレストアするために必要なアクションについても記述されなければならない(shall)。

130 評価者は、TOE がリモート管理者による認証失敗が一切の管理者アクセスが利用可能でなくなる状況を永続的にも一時的にも招かないこと(例、ブロッキングの対象でないローカルログオンを提供することによって)を保証することを確認するために TSS を検査しなければならない(shall)。

2.3.1.2 ガイダンス証拠資料

131 評価者は、連続する認証試行失敗の回数を設定するための指示及び時間間隔(実装される場合) が提供されること、及びリモート管理者が再度ログオンに成功することを許容するプロセスが規定されたそれぞれの「アクション」(そのオプションが選択される場合) について記述されていることを保証するため、ガイダンス証拠資料を検査しなければならない(shall)。採用されるセキュアプロトコル(例、TLS vs. SSH) に依存して、異なるアクションまたはメカニズムが実装される場合、すべてが記述されなければならない(must)。

132 評価者は、リモート管理が FIA_AFL.1 の結果としてアカウントのブロッキングのために永続的または一時的に利用可能でなくなったとしても、管理者アクセスが常に維持されることを保証するために要求されるあらゆるアクションの重要性について、記述され、識別されていることを確認するため、ガイダンス証拠資料を検査しなければならない(shall)。

2.3.1.3 テスト

133 評価者は、リモート管理者が TOE をアクセスするそれぞれの方法について以下のテストを実行しなければならない(shall) (例、接続プロトコルの確立、またはリモート管理者アプリケーションの一部として入力されたあらゆるパスワード) :

a) テスト 1 : 評価者は、TOE によって許容される連続する認証試行失敗回数(及び、FIA_AFL.1.2 での時間周期選択が ST に含まれる場合、評価者はアクセスが再度有効化される時間周期を設定するためにも操作ガイダンスを利用しなければならない(shall))を設定するために、操作ガイダンスを利用しなければならない(shall)。評価者は、一度、制限値に達した場合、有効なクレデンシャルを用いて認証試行がもはや成功しないことをテストしなければならない(shall)。

b) テスト 2：上記テスト 1 のような認証試行失敗についての制限に達した後、評価者は、次のように進めなければならない(shall)。

FIA_AFL.1.2 での管理者アクションの選択が ST に含まれる場合、評価者は、操作ガイダンスに従って ST で規定されるそれぞれのアクションを実行するようなテストによってリモート管理者のアクセス結果がアクセス成功する(その管理者の有効なクレデンシャルを用いるときに)ように再度有効化することを確認しなければならない(shall)。

FIA_AFL.1.2 での時間周期選択が ST に含まれる場合、評価者はテスト 1 で設定された時間周期よりもほんの少し少ない時間待たなければならならず(shall)、有効なクレデンシャルを用いて許可試行がアクセス成功をもたらさないことを示さなければならない(shall)。評価者は次に、テスト 1 で設定された時間周期まで待たなければならず(shall)、有効なクレデンシャルを用いた許可試行がアクセス成功をもたらすことを示さなければならない(shall)。

2.3.2 FIA_PMG_EXT.1 パスワード管理

2.3.2.1 ガイダンス証拠資料

134 評価者は、以下であることを決定するため、ガイダンス証拠資料を検査しなければならない(shall)：

a) パスワードで利用されるかもしれない文字を識別子、強いパスワードの作成に関してセキュリティ管理者へのガイダンスを提供する、及び

b) 最小パスワード長のセッティングについての指示を提供し、サポートされる有効な最小パスワード長について記述する。

2.3.2.2 テスト

135 評価者は、以下のテストを実行しなければならない(shall)：

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(shall)。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(shall)。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、規則の特徴、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(shall)。

2.3.3 FIA_UIA_EXT.1 利用者の識別と認証

2.3.3.1 TSS

136 評価者は、製品にサポートされているログオン方法 (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決定するため、TSS を検査しなければならない(shall)。この記述には、許可される／用いられるクレデンシャル、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(shall)。

137 評価者は、利用者の識別と認証の前に許可されるアクションについて記述されていることを決定するために、TSS を検査しなければならない(shall)。その記述には、ローカルとリモートの TOE 管理のための認証と識別がカバーされなければならない(shall)。

138 分散型 TOE について、セキュリティ管理者がすべての TOE コンポーネントによって識別され認証される方法について TSS に詳述されることを検査しなければならない(shall)。評価者は、もし必ずしもすべての TOE コンポーネントがセキュリティ管理者の認証を FIA_UIA_EXT.1 及び FIA_UAU_EXT.2 に従ってサポートしない場合、TSS には、全体の TOE 機能が TOE コンポーネント間でそのように分離されるかについて、許可されないあらゆる TOE コンポーネントへのアクセスが一切発生不可能であることをどのように保証するかを含めて、記述されなければならない(shall)。

139 分散型 TOE について、評価者は、利用者識別と認証の前にアクションが許可される、それぞれの TOE コンポーネントについて TSS に記述されていることを決定するため、TSS を検査しなければならない(shall)。その記述は、ローカル及びリモートの TOE 管理のために許可と識別をカバーしなければならない(shall)。FIA_UIA_EXT.1 及び FIA_UAU_EXT.2 に従ってセキュリティ管理者の認証をサポートしないような、それぞれの TOE コンポーネントについて、TSS はそのコンポーネントによってサポートされる、あらゆる認証されないサービス／サービスについて記述しなければならない(shall)。

2.3.3.2 ガイダンス証拠資料

140 評価者は、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、証明書などのクレデンシャル材料の確立など) が記述されていることを決定するため、ガイダンス証拠資料を検査しなければならない(shall)。サポートされるログイン方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証拠資料に提供されていることを保証しなければならない(shall)。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証拠資料に提供されていることを決定しなければならない(shall)。

2.3.3.3 テスト

141 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、またログイン方法によってサポートされるクレデンシャルの種別のそれぞれについて、以下のテストを実行しなければならない(shall) :

a) テスト 1 : 評価者は、ログイン方法にサポートされる適切なクレデンシャルを設定するため、ガイダンス証拠資料を利用しなければならない(shall)。そのクレデンシャル／ログイン方法について、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(shall)。

b) テスト 2 : 評価者は、ガイダンス証拠資料に従って許可されるサービス (もしあれば) を設定しなければならず(shall)、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決定しなければならない(shall)。評価者は、利用可能なサービスのリストが本要件で規定されているものに制限されているこ

とを決定しなければならない(shall)。

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決定しなければならず(shall)、このリストが要件と一貫していることを確かめなければならない(shall)。

d) テスト 4 : 分散型 TOE について、必ずしもすべての TOE コンポーネントが FIA_UIA_EXT.1 及び FIA_UAU_EXT.2 に従ってセキュリティ管理者の認証をサポートしない場合、評価者は、TSS に記述されるとおりそのコンポーネントがセキュリティ管理者を認証することをテストしなければならない(shall)。

2.3.4 FIA_UAU_EXT.2 パスワードに基づく認証メカニズム

142 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規定される場合、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(shall)。

2.3.5 FIA_UAU.7 保護された認証フィードバック

2.3.5.1 テスト

143 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、以下のテストを実行しなければならない(shall) :

a) テスト 1 : 評価者は、TOE へローカルに認証しなければならない(shall)。この試行中に、評価者は、認証情報を入力している間に不可視化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(shall)。

2.4 セキュリティ管理 (FMT)

2.4.1 分散型 TOE の一般的な要件

2.4.1.1 TSS

144 分散型 TOE について、セキュリティ管理に関連するすべての機能がすべての TOE コンポーネントについて実現されており、異なる TOE コンポーネント間で共有されていることを保証するため、TSS を検証することが要求される。評価者は、それぞれの TOE コンポーネントのすべての関連する観点が FMT SFR によってカバーされていることを確認しなければならない(shall)。集中的に実装されるセキュリティ管理機能について、評価者のテストを定義しているときに(すべてのコンポーネントがサンプルによってカバーされることを保証しつつ)サンプリングが適用されるべきである(should)。

2.4.1.2 ガイダンス証拠資料

145 分散型 TOE について、それぞれの TOE コンポーネントの管理ガイダンス証拠資料が記述していることを検証することが要求される。評価者は、それぞれの TOE コンポーネントの関連するすべての関連が FMT SFR によってカバーされることを確認しなければならない(shall)。

2.4.1.3 テスト

146 セキュリティ管理機能の正しい実装を検証するために定義されるテストは、すべての TOE コンポーネントについて実行されなければならない(shall)。集中的に実装されるセキュリティ管理機能について、(すべてのコンポーネントがサンプルによってカバーされることを保証するような) 評価者のテストを定義しているときに、サンプリングが適用されるべきである(should)。

2.4.2 FMT_MOF.1/ManualUpdate

2.4.2.1 TSS

147 分散型 TOE については、チャプター2.4.1.1 を参照。非分散型 TOE については具体的な要件はない。

2.4.2.2 ガイダンス証拠資料

148 評価者は、手動アップデートを実行するために必要なあらゆるステップが記述されていることを決定するために、ガイダンス証拠資料を検査しなければならない(shall)。ガイダンス証拠資料は、アップデート中に動作を中止するかもしれないような機能についての警告も提供しなければならない(shall) (該当する場合)。

149 分散型 TOE について、ガイダンス証拠資料は、すべての TOE コンポーネントをアップデートする方法のすべてのステップについて記述しなければならない(shall)。これには、その順序がアップデートプロセスに関連する場合、アップデータされる必要がある TOE コンポーネントにおける順序についての記述を含んでいなければならない(shall)。ガイダンス証拠資料は、アップデート中に動作を中止するかもしれないような TOE コンポーネント及び TOE 全体の機能についての警告も提供しなければならない(shall) (該当する場合)。

2.4.2.3 テスト

150 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(shall)。このテストは失敗すべきである(should)。

151 評価者は、本物のアップデートイメージを用いて、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(shall)。このテストは成功すべきである(should)。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(should)。

2.4.3 FMT_MTD.1/CoreData TSF データの管理

2.4.3.1 TSS

152 評価者は、ガイダンス証拠資料で識別される管理機能それぞれについて、以下のとおりであることを決定するために TSS を検査しなければならない(shall)：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識別されていること。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、管理者でない利用者に対して、どのような方法で許可されないかについて TSS に詳述されていることを確認しなければならない(shall)。

2.4.3.2 ガイダンス証拠資料

153 評価者は、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識別されていること、及び管理者のみがその機能へアクセスすることを保証するために設定情報が提供されていることを決定するために、ガイダンス証拠資料をレビューしなければならない(shall)。

2.4.4 FMT_SMF.1 管理機能の特定

154 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_SSL_EXT.1 、 FTA_SSL3 、 FTA_TAB.1 、 FMT_MOF.1/ ManualUpdate 、FMT_MOF.1/AutoUpdate (ST に含まれる場合)、FIA_AFL.1、FIA_X509_EXT.2.2 (ST に含まれる場合)、及び FPT_TUD_EXT.1.2 & FPT_TUD_EXT.2.2 (ST に含まれる場合及びそれらに管理者の設定可能なアクションが含まれる場合)、FMT_MOF.1/Services、及び FMT_MOF.1/Functions (ST に含まれるこれらの SFR のすべてについて)、FMT_MTD、FPT_TST_EXT、及び参照規格で規定されるあらゆる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。

2.4.4.1 TSS (ガイダンス証拠資料及びテストに関する要件についても含む)

155 評価者は、TSS、ガイダンス証拠資料、及びその他のすべてのテスト中に観測されたものとしての TOS を検査しなければならない(shall)、また FMT_SMF.1 で規定された管理機能が TOE によって提供されることを確認しなければならない(shall)。評価者は、どのセキュリティ管理機能がどのインタフェース(ローカル管理インタフェース、リモート管理インタフェース)を通して利用可能であるかについて詳述することを確認しなければならない(shall)。

156 「TOE コンポーネント間の対話を構成するための能力」を持つ分散型 TOE について、評価者は、TOE コンポーネント間の対話を構成する方法が TSS 及びガイダンス証拠資料に詳述されていることを検査しなければならない(shall)。評価者は、構成された SFR のテスト中に観測される TOE ふるまいが TSS 及びガイダンス証拠資料に記述されたものであることをチェックしなければならない(shall)。

2.4.4.2 ガイダンス証拠資料

157 セクション 2.4.4.1.を参照。

2.4.4.3 テスト

158 評価者は、セクション 2.4.4.で識別された SFR のテストの一部として、管理機能をテストすること。FMT_SMF.1.1 の管理機能の 1 つが他のいずれかの SFR の下ですでに利用されてないときに限り FMT_SMF.1 についての別なテストは要求されない。

2.4.5 FMT_SMR.2 セキュリティ役割における制限

2.4.5.1 ガイダンス証拠資料

159 評価者は、リモート管理のためにクライアント上で実行さ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するため、ガイダンス証拠資料をレビューしなければならない(shall)。

2.4.5.2 テスト

160 評価のためテストアクティビティの実行に際して、評価者は、サポートされるすべてのインタフェースを利用しなければならない(shall) 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の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(shall)。例えば、TOE がローカルなハードウェアインタフェースを通して管理可能な場合 ; SSH ; 及び TLS/HTTPS ; 3 つの管理方法のすべてが評価チームのテストアクティビティの中で、動作確認されなければならない(shall)。

2.5 TSF の保護 (FPT)

2.5.1 FPT_SKP_EXT.1 TSF データの保護 (すべての事前共有鍵、対称鍵及びプライベート鍵の読み出し)

2.5.1.1 TSS

161 評価者は、任意の事前共有鍵、対称鍵、及びプライベート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決定するため、TSS を検査しなければならない(shall)。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／不可視化されるか記述されなければならない(shall)。

2.5.2 FPT_APW_EXT.1 管理者パスワードの保護

2.5.2.1 TSS

162 評価者は、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不可視化するために用いられる手法が詳述されていることを決定するため、TSS を検査しなければならない(shall)。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(shall)。

2.5.3 FPT_TST_EXT.1 TSF テスト

2.5.3.1 TSS

163 評価者は、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するため、TSS を検査しなければならない(shall)。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(shall)) が含まれるべきである(should)。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(shall)。

164 分散型 TOE について、評価者は、どのコンポーネントがどの自己テストを実行し、いつこれらの自己テストが実行されるかについて、TSS に詳述されていることを保証するため、TSS を検査しなければならない(shall)。

2.5.3.2 ガイダンス証拠資料

165 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証拠資料に記述されていることを保証しなければならない(shall)。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(shall)。

166 分散型 TOE について、評価者は、返されたエラーメッセージからどの TOE コンポーネントが自己テストに失敗したかを決定する方法について、ガイダンス証拠資料に記述されていることを保証しなければならない(shall)

2.5.3.3 テスト

167 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。

168 正式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(should)：

a) [FIPS 140-2], チャプター4.9.1, ファームウェア及び実行形式ソフトウェアの完全性検証ためのソフトウェア／ファームウェア完全性テスト。テストは、TOE の暗号機能に限定されないことに留意されたい。

b) [FIPS 140-2], チャプター4.9.1, 暗号機能の正しい動作の検証のための暗号アルゴリズムテスト。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の要件が、適宜考慮されるべきである(should)。

169 評価者は、上記の自己テストが初期起動中に実行されることを検証しなければならない(shall)、または開発者がこれからの逸脱を正当化することを検証かのいずれかでなければならない(shall)。

170 分散型 TOE について、評価者は、どの自己テストがどのコンポーネントによって実行されるかについての TSS での記述に従って、すべての TOE コンポーネントについての自己テストのテストを実行しなければなければならない(shall)。

2.5.4 FPT_TUD_EXT.1 高信頼アップデート

2.5.4.1 TSS

171 評価者は、現在アクティブなバージョンの問い合わせ方法について TSS に記述されていることを検証しなければならない(shall)。高信頼アップデートが TOE 上で遅延されたアクティベーションを伴ってインストール可能である場合、TSS には非アクティブなバージョンがどのように、いつアクティブになるかについて記述する必要がある。評価者はこの記述を検証しなければならない(shall)。

172 評価者は、システムファームウェア及びソフトウェア(単純にするため、用語「ソフトウェア」が以下において利用されるが、本要件はファームウェアとソフトウェアへ適用される)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(shall)。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(shall)。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(shall)。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、及び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(shall)。

173 選択肢「アップデートの自動チェックをサポート」または「自動アップデートをサポート」が FPT_TUD_EXT.1.2 の選択から選ばれる場合、評価者は、どのアクションがそれぞれ TOE による自動チェックまたは自動アップデートにふく

まれるかについてTSS で説明されていることを検証しなければならない(shall)。

174 分散型 TOE について、評価者は、すべての TOE コンポーネントがアップデートされる方法が TSS に記述されていること、アップデート中に TOE の継続的で適切の機能をサポートするようなすべてのメカニズム(個別の TOE コンポーネントへ別々にアップデートを適用するとき) 及び署名またはチェックサムの検証がそれぞれの TOE コンポーネントについて実行される方法が TSS に記述されていることを保証するため、TSS を検査しなければならない(shall)。あるいは、この記述がガイダンス証拠資料で提供されることも可能である。その場合、評価者は、ガイダンス証拠資料を代わりに検査するべきである(should)。

175 ソフトウェアアップデートデジタル署名検証用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(shall)。評価者は、必要に応じて、その証明書がインストール／アップデート／選択される方法について TSS (またはガイダンス証拠資料) に記述されていることも保証すること。

176 公開ハッシュが高信頼アップデートメカニズムを保護するために利用される場合、評価者は、高信頼アップデートメカニズムがセキュリティ管理者の能動的な許可ステップを含むこと、及び公開ハッシュ値のダウンロード、ハッシュの比較及びアップデートがセキュリティ管理者による能動的な許可を一切含まないような、完全に自動化された処理ではないことを検証しなければならない(shall)。特に、FMT_MOF.1/ManualUpdate に従ったセキュリティ管理者としての認証は、公開ハッシュを利用するとき、アップデートプロセスの一部である必要がある。

2.5.4.2 ガイダンス証拠資料

177 評価者は、現在アクティブなバージョンの問い合わせ方法についてガイダンス証拠資料に記述されていることを検証しなければならない(shall)。高信頼アップデートが TOE 上に遅延されたアクティベーションを伴ってインストール可能である場合、ガイダンス証拠資料は、ロードされるが非アクティブなバージョンの問い合わせ方法について記述する必要がある。

178 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) ガイダンス証拠資料に記述されていることを検証しなければならない(shall)。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(shall)。この記述は、TSS 中の記述と対応していなければならない(shall)。

179 高信頼アップデートメカニズムを保護するために公開ハッシュが利用される場合、評価者は、セキュリティ管理者がそのアップデートについての真正の公開ハッシュ値を取得できる方法について、ガイダンス証拠資料に記述されていることを検証しなければならない(shall)。

180 分散型 TOE について、評価者は、個別の TOE コンポーネントのバージョンが FPT_TUD_EXT.1 に対して決定される方法、すべての TOE コンポーネントがアップデートされる方法、及び適切なリカバリアクションに沿ったアップデートのチェックまたは適用から生じるかもしれないエラー条件(例、署名検証の失敗、または利用可能な格納領域の超過)について、ガイダンス証拠資料に記述されていることを検証しなければならない(shall)。ガイダンス証拠資料は、利用者に関

連した手順のみを記述しなければならない(has to)；アップデートを適用するときに実行される内部通信についての情報を与える必要はない。

181 これが TSS で提供されなかった情報であった場合：分散型 TOE について、評価者は、すべての TOE コンポーネントがアップデートされる方法について記述されていること、アップデート中に TOE の継続的な適切な機能をサポートするようなすべてのメカニズム(個別の TOE コンポーネントへの別々にアップデートを適用するとき)及びそれぞれの TOE コンポーネントに対して署名またはチェックサムの検証の実行方法について記述されていることを保証するため、ガイダンス証拠資料を検査しなければならない(shall)。

182 これが TSS で提供されなかった情報であった場合：ST 作成者が証明書ベースのメカニズムがソフトウェアアップデートデジタル署名検証のために利用されていることを示す場合、評価者はガイダンス証拠資料に証明書がデバイス上に含まれる方法についての記述が含まれていることを検証しなければならない(shall)。評価者は、必要に応じて、証明書がインストール／アップデート／選択される方法についてガイダンス証拠資料に記述されていることについても保証しなければならない(shall)。

2.5.4.3 テスト

183 評価者は、以下のテストを実行しなければならない(shall)：

a) テスト 1：評価者は、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決定するため、バージョン検証アクティビティを実行する (アップデート前は同一のバージョンであるべきである(should))。評価者は、ガイダンス証拠資料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 (デジタル署名が利用される場合)：評価者は、まず保留になっているアップデートがないことを確認し、次に製品の現在のバージョンを決定するために本テストで利用されるべきアップデートで主張されているバージョンと異なっていることを検証しつつ、バージョン検証アクティビティを行うこと (アップデート前は同一のバージョンであるべきである(should))。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改変されたバージョン(例えば、16 進エディタを用いて)

2) 署名されていないイメージ

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)

4) TOE がアップデートのインストールとアップデートされたコードを実行するために要求される再起動またはアクティベーションの間のギャップを許容する場合、TOE は、現在実行している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を表示できなければならない(must)。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、試行されたアップデートが拒否された時点に応じて異なる TOE の間では異なるかもしれない。評価者は、そのような場合のための市場案最近インストールされたバージョン情報を TOE がガイダンス証拠資料に記述されるとおりに取り扱うことを検証しなければならない(shall)。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(shall)。

c) テスト 3 (公開ハッシュが TOE 上で検証される場合)：公開ハッシュがセキュリティ管理者によって TOE へ提供され、公開ハッシュに対するアップデートファイルのハッシュ値の検証が TOE によって検証される場合、評価者は、以下のテストを実行しなければならない(shall)。評価者は、まず保留になっているアップデートがないことを確認し、次に製品の現在のバージョンを決定するために本テストで利用されるべきアップデートで主張されているバージョンと異なっていることを検証しつつ、バージョン検証アクティビティを行うこと。

1) 評価者は、アップデートのハッシュが公開ハッシュと一致しないような本物のアップデートを取得または生成する。評価者は、TOE の公開ハッシュ値を提供し、TOE 自身(その機能が TOE によって提供される場合)、または TOE 外のいずれかで、アップデートのハッシュを計算する。評価者は、ハッシュ値が異なることを確認し、次に TOE 上でアップデートのインストールを試行し、これが、ハッシュ値の相違により失敗することを検証する(かつ失敗はログがとられること)する。TOE の実装によって、TOE は、利用者にハッシュ値の検証が失敗した後で TOE をアップデート試行することさえも許可しないに違いない。その場合、TOE の正しいふるまいの十分な検証として、ハッシュ比較失敗と見なされる

2) 評価者は、本物のアップデートを利用し、TOE 上に公開ハッシュ値を格納せずにハッシュ値の検証を実行する試行を行うこと、評価者は、この試行が失敗することを確認すること。TOE の実装により、ハッシュ値を TOE へ提供することなしにハッシュ値の検証を試行することが可能でないかもしれない、例、ハッシュ値がコマンドラインメッセージのパラメタとして TOE に受けわたる必要がある場合、及びコマンドの文法チェックがハッシュ値の提供なしにコマンドの実行を防止する場合。その場合、このチェックの実行を防止するようなメカニズムがそれぞれテストされなければならない(shall)、例、文法チェックがハッシュ値の提供されないコマンドを拒否する場合、及び

試行の拒否がハッシュ値の検証を失敗するような正しいふるまいの十分な検証とみなされる。評価者は、次に TOE 上でアップデートのインストールを試行し(不成功のハッシュ検証にもかかわらず)、これが失敗することぉ確認する。TOE の実装によって、TOE は、ハッシュ値の検証が失敗した後、TOE のアップデートの試行すら許可されないかもしれない。その場合、ハッシュ比較失敗の検証は、TOE の正しいふるまいの十分な検証と見なされる。

3) TOE がアップデートのインストールとアップデートされたコードを実行するために要求される再起動またはアクティベーションの間のギャップを許容する場合、TOE は、現在実行している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を表示できなければならない(must)。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、試行されたアップデートが拒否された時点に応じて異なる TOE の間では異なるかもしれない。評価者は、そのような場合のための市場案最近インストールされたバージョン情報を TOE がガイダンス証拠資料に記述されるとおりに取り扱うことを検証しなければならない(shall)。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(shall)。

184 公開ハッシュに対するアップデートファイルのハッシュ値の検証が TOE によって実行されない場合、テスト 3 はスキップされなければならない(shall)。

185 評価者は、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、テスト 1、テスト 2 及びテスト 3(可能であるならば)を実行しなければならない(shall) (手動アップデート、アップデートの自動チェック、自動アップデート)。

186 分散型 TOE について、評価者は、すべての TOE コンポーネントについて、テスト 1、テスト 2 及びテスト 3(可能であるならば)を実行しなければならない(shall)。

2.5.5 FPT_STM.1 高信頼タイムスタンプ

2.5.5.1 TSS

187 評価者は、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するため、TSS を検査しなければならない(shall)。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。

2.5.5.2 ガイダンス証拠資料

188 評価者は、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ため、ガイダンス証拠資料を検査すること。TOE が NTP サーバの利用をサポートする場合、ガイダンス証拠資料には 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。

2.5.5.3 テスト

189 評価者は、以下のテストを実行しなければならない(shall)：

a) テスト 1：TOE がセキュリティ管理者による時刻の直接セッティングをサポートする場合、評価者は、時刻をセットするため、ガイダンス証拠資料を利用する。評価者は次に、時刻が正しく設定されたことを観測するため、利用可能なインタフェースを利用しなければならない(shall)。

b) テスト 2：TOE が NTP サーバの利用をサポートする場合、評価者は、TOE 上の NTP クライアントを設定するためにガイダンス証拠資料を利用しなければならず(shall)、NTP サーバとの通信パスをセットアップする。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観測する。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証拠資料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実行しなければならない(shall)。

190 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(shall)。

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 ガイダンス証拠資料

191 評価者は、ローカル管理者セションロックまたは終了がサポートされていること及び非アクティブな時間の設定についての指示がガイダンス証拠資料に記述されているかどうかを確認しなければならない(shall)。

2.6.1.2 テスト

192 評価者は、以下のテストを実行しなければならない(shall)：

a) テスト 1：評価者はガイダンス証拠資料に従って、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観測する。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 ガイダンス証拠資料

193 評価者は、ローカル管理者セションロックまたは終了がサポートされていること及び非アクティブな時間の設定についての指示がガイダンス証拠資料に記述されているかどうかを確認しなければならない(shall)。

2.6.2.2 テスト

194 評価者は、以下のテストを実行しなければならない(shall)：

a) テスト 1：評価者は、ガイダンス証拠資料に従って、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観測する。

2.6.3 FTA_SSL.4 利用者起動による終了

2.6.3.1 ガイダンス証拠資料

195 評価者は、ローカルまたはリモート管理者セションの終了方法についてガイダンス証拠資料に記述されていることを確認しなければならない(shall)。

2.6.3.2 テスト

196 リモート管理のそれぞれの方法について、評価者は、以下のテストを実行しなければならない(shall)：

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証拠資料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観測する。

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証拠資料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観測する。

2.6.4 FTA_TAB.1 デフォルト TOE アクセスバナー

2.6.4.1 TSS

197 評価者は、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するため、TSS をチェックしなければならない(shall)。

2.6.4.2 ガイダンス証拠資料

198 評価者は、バナーメッセージの設定方法についてガイダンス証拠資料に記述されていることを保証するため、ガイダンス証拠資料をチェックしなければならない(shall)。

2.6.4.3 テスト

199 評価者は、以下のテストについても実行しなければならない(shall) :

a) テスト 1 : 評価者は、ガイダンス証拠資料に従って、通知及び同意の警告メッセージを設定する。次に評価者は、TSS で規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(shall)。評価者は、インスタンスそれぞれに通知及び同意の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(shall)。

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

200 評価者は、本要件で識別される許可された 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識別されていることを決定するため、TSS を検査しなければならない(shall)。また評価者は、TSS に列挙されたすべてのプロトコルが規定され、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(shall)。

2.7.1.2 ガイダンス証拠資料

201 評価者は、許可された 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証拠資料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(shall)。

2.7.1.3 テスト

202 評価者は、以下のテストを実行しなければならない(shall) :

a) テスト 1 : 評価者は、ガイダンス証拠資料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、評価中に許可された 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(shall)。

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証拠資料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(shall)。

c) テスト 3 : 評価者は、許可された 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(shall)。

d) テスト 4 : 評価者は、テスト 1 でテストされた許可された 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(shall)。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(shall)。

203 さらなるの保証アクティビティは、具体的なのプロトコルと関連付けられる。

204 分散型 TOE について、評価者は、セキュリティターゲットにおける TOE コンポーネントへの外部セキュアチャネルのマッピングにしたがって、すべての TOE コンポーネントにおけるテストを実行しなければならない(shall)。

2.7.2 FTP_TRP.1/Admin 高信頼パス

2.7.2.1 TSS

205 評価者は、リモート TOE 管理の方法が、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決定するため、TSS を検査しなければならない(shall)。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で規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(shall)。

2.7.2.2 ガイダンス証拠資料

206 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証拠資料に含まれていることを確認しなければならない(shall)。

2.7.2.3 テスト

207 評価者は、以下のテストを実行しなければならない(shall) :

a) テスト 1 : 評価者は、ガイダンス証拠資料に記述されるように接続をセットアップし、通信が成功することを保証することによって、評価作業中に (ガイダンス証拠資料で) 規定されたリモート管理方法の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(shall)。

b) テスト 2 : 評価者は、許可された 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(shall)。

c) テスト 3 : 評価者は、テスト 1 でテストされた許可された 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(shall)。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(shall)。

208 さらなる保証アクティビティは、具体的なプロトコルと関連付けられる。

209 分散型 TOE について、評価者は、セキュリティターゲットにおける TOE コンポーネントへの外部セキュアチャネルのマッピングにしたがって、すべての TOE コンポーネントにおけるテストを実行しなければならない(shall)。

3 オプション要件の評価アクティビティ

3.1 セキュリティ監査 (FAU)

3.1.1 FAU_STG.1 保護された監査証跡格納

3.1.1.1 TSS

210 評価者は、ローカルに保存される監査データの量、及び監査記録が許可されない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するため、TSS を検査しなければならない(shall)。評価者は、監査記録の許可された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(shall)。

211 分散型 TOE について、評価者は、本 SFR がどの TOE コンポーネントに適用されるか、及び異なる TOE コンポーネントの間でローカルストレージが実装される方法 (例、すべての TOE コンポーネントが自身のローカルに格納する、またはデータはすべての監査事象の集中ローカルストレージのための別の TOE コンポーネントへ送信される) について TSS に記述されていることを保証するため、TSS を検査しなければならない(shall)。

3.1.1.2 ガイダンス証拠資料

212 評価者は、ローカルに保存されるデータを許可されない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決定するため、ガイダンス証拠資料を検査しなければならない(shall)。

3.1.1.3 テスト

213 評価者は、以下のテストを実行しなければならない(shall) :

a) テスト 1 : 評価者は、セキュリティ管理者としての認証なしに (サポートされる場合には非特権利用者としての認証によって、または全く認証なしに) 監査証跡をアクセスし、監査記録の改変及び削除の試行しなければならない(shall)。評価者は、これらの試行が失敗するのを検証しなければならない(shall)。実装に従い、セキュリティ管理者以外の一切の利用者が定義されておらず、あらゆる利用者認証なしにその利用者が監査証跡のアクセス試行が実行可能なポイントへ行くことはできないに違いない。そのような場合にセキュリティ管理者としての認証なしに到達可能なステップまでの実行をアクセス制御メカニズムが防止することが実証されなければならない(shall)。

b) テスト 2 : 評価者は、許可された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(shall)。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(shall)。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(shall)。

214 **分散型 TOE について、評価者は、本 SFR によってカバーされるため、TSS によって定義されるようなそれぞれのコンポーネントについてテスト 1 及びテスト 2 を実行しなければならない(shall)。**

3.1.2 FAU_STG_EXT.2/LocSpace 消失した監査データの集計

215 このアクティビティは、FAU_STG_EXT.1.2 及び FAU_STG_EXT.1.3 のテストと併せて達成されるべきである(should)。

3.1.2.1 TSS

216 評価者は、監査データのローカル格納領域が満杯の場合に、破棄、上書き等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するため、TSS を検査しなければならない(shall)。

217 分散型 TOE について、評価者は、どの TOE コンポーネントに本 SFR が適用されるかについて TSS に記述されていることを保証するため、TSS を検査しなければならない(shall)。本 SFR はオプションのため、ある TOE コンポーネントに喪に適用されるかもしれないがすべてに対して適用される訳ではない。これは、すべての TOE コンポーネントがそれら自身で監査情報を格納するが、FAU_STG_EXT.2/LocSpace は、コンポーネントの一つによってのみサポートされるような状況をもたらすかもしれない。

3.1.2.2 ガイダンス証拠資料

218 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証拠資料に記述されていることを保証しなければならない(shall)。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(shall)。

219 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証拠資料に含まれることを検証しなければならない(shall)。

3.1.2.3 テスト

220 評価者は、FAU_STG_EXT.2/LocSpace 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(shall)。

221 分散型 TOE について、評価者は、TSS の記述に従って本機能をサポートしているすべての TOE コンポーネントについての喪失した監査データの計数の正しい実装を検証しなければならない(shall)。

3.1.3 FAU_STG.3/LocSpace 監査データ喪失の可能性のある場合のアクション

222 本アクティビティは、FAU_STG_EXT.1.2 及び FAU_STG_EXT.1.3 のテストと併せて達成されるべきである(should)。

3.1.3.1 TSS

223 評価者は、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するため、TSS を検査しなければならない(shall)。

224 分散型 TOE について、評価者は、どの TOE コンポーネントに本 SFR が適用されるか、及びそれぞれの TOE コンポ―ネントが本 SFR を実現している方法に

ついて、TSS に記述されていることを保証するため、TSS を検査しなければならない(shall)。本 SFR はオプションのため、いくつかの TOE コンポーネントにのみ適用されるかもしれないが、すべてに対してではない。これは、すべての TOE コンポーネントがそれら自身で監査情報を格納するが、FAU_STG.3/LocSpace は、コンポーネントの一つによってのみサポートされるような状況をもたらすかもしれない。特に、評価者は、TSS に本機能をサポートしているすべてのコンポーネントについて、そのコンポーネント自身によって警告が生成されるか、または別のコンポーネント及び後者の場合に対応するコンポーネントを通して警告が生成されるかを検証しなければならない(has to)。評価者は、監査記録が「目に見えない喪失」であるかもしれないようなあらゆる状況について、TSS が明確化していることを検証しなければならない(has to)。

3.1.3.2 ガイダンス証拠資料

225 評価者は、監査データのローカル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、及びこの警告がどのように表示または保存されるかについて、ガイダンス証拠資料に記述されていることについても保証しなければならない(shall) (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一切ないため、これはおそらくログファイルへ保存される)。ガイダンス証拠資料における記述は、TSS の記述と一致していなければならない(shall)。

3.1.3.3 テスト

226 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(shall)。

227 分散型 TOE について、評価者は、TSS の記述に従って本機能をサポートしているすべての TOE コンポーネントについてのローカル格納領域についての警告表示の正しい実装を検証しなければならない(shall)。評価者は、TSS の記述に従って本機能をサポートするそれぞれのコンポーネントが自身で警告を表示できること、または別のコンポーネントを通して警告を表示できることを検証しなければならない(shall)。

3.2 識別と認証 (FIA)

3.2.1 FIA_X509_EXT.1/ITT X.509 証明書有効性確認

3.2.1.1 TSS

228 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、そして TOE によってサポートされないような(FIA_X509_EXT.1.1 における) extendedKeyUsage フィールドの規則のいずれかを TSS が識別するような(即ち、それらは自明で満たされることを ST が主張しているような)ことを保証しなければならない(shall)。選択された場合、どのように証明書失効チェックが実行されるのか TSS に記述されていなければならない(shall)。X.509 証明書がデバイス上にロードされるときのみ、X.509 証明書の状態を検証するだけでは不十分である。

3.2.1.2 テスト

229 評価者は、認証ステップにおいて証明書が利用されるときに、証明書の有効性

チェックが実行されることを実証しなければならない(shall)。X.509 証明書がデバイス上にロードされるときのみ、X.509 証明書の状態を検証するだけでは不十分である。評価者は、FIA_X509_EXT.1.1/ITT について以下のテストを実行しなければならない(shall) :

a) テスト 1a : 評価者は、本機能で利用されるべき証明書を検証するために必要とされるものとして、証明書の有効なチェイン(信頼された CA 証明書で終端する)をロードしなければならない(shall)、また本機能が成功することを実証するためにこのチェインを利用しなければならない(shall)。

   テスト 1b : 評価者は、次にチェインの中の証明書の一つを削除しなければならない(shall) (即ち、ルート CA 証明書またはその他の中間の証明書、しかし、エンドエンティティ証明書ではない)、そして、本機能が失敗することを示さなければならない(shall)。

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が、本機能の失敗をもたらすことを実証しなければならない(shall)。

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(shall) : もし両方とも選択されている場合には、それぞれの方法についてテストが行われなければならない(shall)。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(shall) 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(should)。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(shall)。次に評価者は、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ため、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すること。一切の失効方法が選択されない場合は、テストは要求されない。

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利用して 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(shall)。CRL が選択されている場合、評価者は cRLsign key usage 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(shall)。

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(shall)。(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(shall)。(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(shall)。(証明書のハッシュが検証されないこと。)

230 評価者は、FIA_X509_EXT.1.2/ITT について以下のテストを実行しなければならない(shall)。記述されたテストは、FIA_X509_EXT.2.1/ITT の機能を含め、他の証明書サービスの保証アクティビティと併せて実行されなければならない

(must)。extendedKeyUsage 規則についてのテストは、それらの規則を要求する用途と併せて実行される。TOE によってサポートされないような(FIA_X509_EXT.1.1 において) extendedKeyUsage フィールドの規則のいずれかを TSS が識別するような場合(即ち、それらは自明で満たされることを ST が主張しているような)、対応する extendedKeyUsage 規則のテストは省略されてもよい。

231 評価者は、少なくとも 2 つの証明書のチェインを作成しなければならない(shall):テストされるべきノード証明書、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 Extension が含まれないような証明書パスを構築しなければならない(shall)。この証明書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 Extension 中の cA フラグが FALSE にセットされているような証明書パスを構築しなければならない(shall)。この証明書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 Extension 中の cA フラグが TRUE にセットされているような証明書パスを構築しなければならない(shall)。この証明書パスの検証は成功する。

3.3 セキュリティ管理 (FMT)

3.3.1 FMT_MOF.1/Services

3.3.1.1 TSS

232 分散型 TOE について、チャプター2.4.1.1 を参照。非分散型 TOE についての具体的な要件はない。

3.3.1.2 テスト

233 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 (サポートされる場合、管理者特権のない利用者としての認証によって、または全く管理者特権なしに) FAU_GEN.1.1 の適用上の注釈で定義されるとおり、少なくとも 1 つのサービスの有効化と無効化を試行しなければならない(shall)。このサービス／これらのサービスの有効化・無効化の試行は、失敗するべきである(should)。実装に従って、セキュリティ管理者以外の一切の利用者は、このサービス／これらのサービスの有効化／無効化の試行が実行可能であるようなポイントへ利用者行くことはできないに違いない。そのような場合に、アクセス制御メカニズムがセキュリティ管理者として認証なしで到達可能であるようなステップまでの実行を防止することを実証しなければならない(shall)。

234 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、FAU_GEN.1.1 の適用上の注釈で定義されるとおり(TOE によってサポートされる場合)、少なくとも 1 つのサービスの有効化と無効化を試行しなければならない(shall)。このサービス／これらのサービスの有効化／無効化の試行は、成功するべきである(should)。

3.3.2 FMT_MTD.1/CryptoKeys TSF データの管理

3.3.2.1 TSS

235 分散型 TOE について、チャプター2.4.1.1 を参照。非分散型 TOE についての具

体的な要件はない。

3.3.2.2 テスト

236 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 (サポートされる場合、管理者特権のない利用者としての認証によって、または全く管理者特権なしに) 少なくとも 1 つの関連するアクション(改変、削除、生成／インポート)の実行を試行しなければならない(shall)。事前の認証なしの関連アクションの実行の試行は失敗すべきである(should)。実装に従ってセキュリティ管理者以外の一切の利用者は、定義されるに違いなく、あらゆる利用者認証なしに、暗号鍵を管理するための試行が実行可能であるようなそのポイントへ利用者が行くことはできないに違いない。そのような場合に、アクセス制御メカニズムがセキュリティ管理者として認証なしで到達可能であるようなステップまでの実行を防止することを実証しなければならない(shall)。

237 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(shall)。このテストは成功すべきである(should)。

3.4 TSF の保護 (FPT)

3.4.1 FPT_ITT.1 基本 TSF 内データ転送保護

238 TOE が分散型 TOE でない場合、評価者アクションは一切必要ではない。分散型 TOE について、評価者は、以下のアクティビティを実行する。

3.4.1.1 TSS

239 評価者は、分散型 TOE のコンポーネント間のすべての通信について、それぞれの通信メカニズムがその IT エンティティの許可されたプロコトルに関して識別されていることを決定するため、TSS を検査しなければならない(shall)。評価者は、これらのコンポーネント間通信用に TSS に列挙されたすべてのプロトコルが ST の要件に規定され、含まれていることについても確認しなければならない(shall)。

3.4.1.2 ガイダンス証拠資料

240 評価者は、許可された TOE コンポーネントのそれぞれのペアの間の関連する許可された通信チャネルとプロトコルを確立するための指示がガイダンス証拠資料に含まれ、また通信が意図せず切断された際の回復の指示が含まれていることを確認しなければならない(shall)。

3.4.1.3 テスト

241 評価者は、以下のテストを実行しなければならない(shall) :

a) テスト 1 : 評価者は、許可された TOE コンポーネントのそれぞれのペア間のそれぞれのプロコトルを用いて、ガイダンス証拠資料に記述されたとおり接続がセットアップされた通信が評価作業中にテストされることを保証しなければならない(shall) 、また通信が成功することを保証すること。

b) テスト 2 : 評価者は、許可された IT エンティティとのそれぞれの通信チャネルについて、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(shall)。

c) テスト 3：評価者は、テスト a)の間にテストされたそれぞれの許可された IT エンティティに関連するそれぞれのプロコトコルについて、接続が物理的に中断されなければならない(shall)。評価者は、物理的接続性が回復されるとき、通信が適切に保護されることを保証しなければならない(shall)。

242 さらなる保証アクティビティが具体的なプロトコルと関連している。

3.5 高信頼パス／チャネル (FTP)

3.5.1 FTP_TRP.1/Join 高信頼パス

3.5.1.1 TSS

243 **評価者は、その環境が通信の機密性を提供することを要求されるかどうか、または好感される登録データが機密性を要求しないかどうかの識別を含めて、それらの通信が保護される方法に加えて、コンポーネントがTOEへ参加する方法が識別されることを決定するためにTSSを検査しなければならない(shall)。登録データが機密性保護を要求しないことをTSSが断言する場合、評価者は、それを確認するために提供される正当化を検査しなければならない(shall)。**

244 評価者は、ST の SFR にこのプロセスが含まれることを支持して、すべてのプロトコルが TSS に列挙されていること、及び ST が登録チャネル用に FPT_TRP.1/Join を利用する場合にこのチャネルが通常のコンポーネント間通信チャネルとして再利用できないことについてもチェックしなければならない (shall)。

3.5.1.2 ガイダンス証拠資料

245 評価者は、チャネルの確立及び有効化及び登録のための指示がガイダンス証拠資料に含まれていること、及び登録プロセスのための AGD_PRE.1 の詳細化で要求される情報がガイダンス証拠資料に含まれていることを確認するため、ガイダンス証拠資料を検査しなければならない(shall)。評価者は、どのコンポーネントが通信を開始するかについて、ガイダンス証拠資料が明確化していることを確認しなければならない(shall)。評価者は、登録プロセス中に意図せずに接続が切断されたときに取られるに違いない回復のための指示がガイダンス証拠資料に含まれていることを確認しなければならない(shall)。

246 登録チャネルセキュリティのいくつかの観点についてセキュリティを提供するために運用環境に依拠するような分散型 TOE の場合、以下に列挙されるとおりの準備手続きに関する特定の要件がある。(この方法での運用環境への依存は、FTP_TRP.1.3/Join の割付における操作ガイダンスへの参照によって ST 内で示される。) この場合、評価者は、以下について確認するため、準備手続きを検査しなければならない (shall) ：

a) 登録チャネル自身によって提供される認証と暗号化の強度及び TOE へ参加するコンポーネントのために利用される環境における具体的な要件(例、機微なメッセージの傍受、IP なりすましの試行、中間者攻撃、またはレースコンディションを防止するために環境が依存するような要件)について明確に述べる

b) 機密性のある値のどれが有効化されたチャネル上で送信されたか (例、あらゆる鍵、鍵長、及びその目的)、あらゆる機密性のない鍵の利用 (例、開

発者が複数のデバイスまたはある種別またはファミリのすべてのデバイスに亘って、同じ鍵を利用するような)、及び認証されない識別データの利用 (例、IP アドレス、自己署名証明書) について識別する

c) 送信された値／鍵よりも低い強度の比較可能な鍵を利用するようなチャネル上で秘密の値／鍵が送信されるかもしれないようなあらゆる状況を強調する。比較可能な強度は、アルゴリズムまたは鍵を危殆化するために要求される作業の量として定義され、通常セキュリティの「ビット」として表現される。ST 作成者と評価者は、比較可能なアルゴリズム強度に関してさらなるガイダンスについて、NIST 800-57 (訳注 : NIST SP800-57 Part 1) 表 2 を参考にするべきである(should)。

3.5.1.3 テスト

247 評価者は、以下のテストを実行しなければならない(shall) :

a) テスト 1 : 評価者は、ガイダンス証拠資料に記述されるとおりに接続をセットアップし、通信が成功することを保証しつつ、TSF へ参加しているコンポーネントのための通信経路がそれぞれの区別される(同等でない)コンポーネント種別 [4]についてテストされることを保証しなければならない(shall)。特に、評価者は、登録プロセス用の環境保護における要件が一貫していることを確認しなければならない(shall) (例えば、登録中にコンポーネントをインターネットから隔離する要件は、コンポーネントをライセンスサーバにコンタクトする必要性と一貫しないかもしれない)。登録環境において機密性を保護する必要性として一切の要件が識別されない場合、評価者は、登録用に利用される鍵が有効化されている TSF 内チャネル用に利用される鍵と少なくとも同じ長さであるように(ガイダンス証拠資料の指示に従って)設定可能であることを確認しなければならない(shall)。評価者は、そのチャネル用に利用される鍵がコンポーネントのペアにとって一意であることを確認しなければならない(shall) (これは、登録テスト中に関連する鍵を識別することによって行われる : 鍵の値が検査される必要はない)。

b) テスト 2 : 評価者は、実際にその通信チャネルがガイダンス証拠資料においてすべての TOE コンポーネントが開始可能なものとして管理者によって有効化可能であることを保証するため、ガイダンス証拠資料に従わなければならない(shall)。

c) テスト 3 : 評価者は、チャネルデータが暗号化され、次にチャネル上で観測されるデータが平文でないことについて、ガイダンス証拠資料に記述されているかを保証しなければならない(shall)。

d) テスト 4 : 評価者は、登録チャネルを利用できるような同等でないコンポーネント種別の異なるそれぞれペアについて、接続が参加試行中に物理的に中断されることを保証しなければならない(shall)。評価者は、物理的接続性が回復されるとき、通信が適切に保護されることを保証しなけれ

[4] ここでの意図は、含まれるすべての異なるソフトウェアセクションをカバーすることである。例えば、太乙のソフトウェアイメージは、異なる TOE コンポーネント上にインストールされるかも s 例ないが、ハードウェアプラットフォームや通信スタックによって実行されるイメージの異なるセクションを持つかもしれない。このよう場合テストは、それぞれの異なるソフトウェアセクションに対して実行されるべきである(should)。

ばならない(shall)。

248 さらなる保証アクティビティは、具体的なプロトコルと関連付けられる。

3.6 通信 (FCO)

3.6.1 FCO_CPC_EXT.1 コンポーネント登録チャネル定義

249 TOE が分散型 TOE でない場合、一切の評価者アクションは必要とされない。分散型 TOE について、評価者は、以下のアクティビティを実行する。これらのアクティビティの実行において、評価者は、証拠資料の分析とテストの組み合わせに基づく以下の質問への答えを決定しなければならない(shall) (おそらく、FTP_TRP.1/Join のような、関連する登録チャネル用の評価アクティビティの実行からの入力についても利用しつつ)、またその答えを報告しなければならない(shall)。

a) 適切に認証され、TOE に参加する前に、コンポーネントが TOE コンポーネントとの正常に通信すること(TOE の一部として参加することを有効化する方法において)を何が止めさせる [5]か？

b) 有効化ステップとは何か？(どのインタフェースを利用しているかを記述せよ、操作ガイダンスにおける関連するセクションとステップへの参照と共に)。

1) セキュリティ管理者以外の誰かがこのステップを実行するのを何が止めさせるか？

2) 彼らが意図するコンポーネントが参加することを有効化しようとしていることをセキュリティ管理者がどのように知るか？(参加者の識別は、有効化アクション自身の一部であるかもしれないし、またはセキュアなチャネル確率の一部であるかもしれないが、意図しないコンポーネントの参加を防止しなければならない(must))

c) 管理者が有効化ステップを実行しなかった場合、何がコンポーネントの正常な参加を止めさせるか；または、同等的に、コンポーネントが正常に参加する前に、許可された管理者によるアクションが要求されることを TOE はどのように保証するか？

d) コンポーネントが異なるセキュアでないチャネルを介して登録プロセスを実行することを何が止めさせるか？

[5] 「何がセキュアにするか．．．」とは対照的に「何が止めさせるか．．．」のフレーズの意図は、評価者がその最低レベル、つまり適切な管理下にあるものに依存するように明確に見ることができるようなセキュリティのレベル、の依存性に対する答えを追及することである。例えば、チャネルは、自己署名された証明書内の信頼しているものへ提供される公開鍵によって保護されるかもしれない。これは、認証を提供するために適用される暗号メカニズムを有効化する(それゆえに、「公開鍵証明書のチェックは、．．．をセキュアにする」という答えを招く)が、攻撃者は自身の自己署名された証明書を生成可能であるので、攻撃者が明らかに認証することを最終的に止めることはない。「許可されないコンポーネントが．．．正常に通信することを何が止めさせるか」という質問は、攻撃者が攻撃する必要があるものに注意を集中する、それゆえに自己署名された証明書が攻撃者によって生成される可能性があるかどうかのレベルまで答えを導く。同様に、既知の鍵、または個人のデバイス以外のデバイス種別に共通の鍵は、機密性メカニズムで利用されるかもしれないが、攻撃者は、既知の鍵を見つけることが可能であるか、ユニークでない鍵を含むデバイスの自身のインスタンスを取得できるので、機密性を提供しない。

e) FTP_TRP.1/Join チャネル種別が FCO_CPC_EXT.1.2 で選択される場合、登録プロセスとそのセキュアチャネルは、どのようにして、そのデータが暴露から保護され、改変の検知を提供することを保証するか？

f) 登録チャネルが登録環境の保護に信頼を置かない場合、登録チャネルは、それを介して渡されるデータについての十分なレベルの保護(特に、機密性に関して)を提供するか？

g) 登録チャネルが TOE コンポーネント間の通常の内部通信に継続して利用される場合(即ち、参加者が登録を完了した後)、登録チャネルの認証または暗号機能のいずれかがこのようなチャネルの通常の FPT_ITT.1 要件よりも弱い保護を持つようなチャネルの利用をもたらすか？

h) 無効化ステップとは何か？(そのインタフェースが利用されるか記述せよ、操作ガイダンスにおける関連するセクションとステップへの参照と共に)。

i) 管理者が無効化ステップを実行した場合、コンポーネントがその他の TOE コンポーネントと正常に通信することを何が止めさせるか？

3.6.1.1 TSS

250 (注釈：パラグラフ 249 は、評価者が TSS、ガイダンス証拠資料、及びテスト評価アクティビティの組み合わせを通して、決定及び回答を報告する必要がある質問を列挙している)

251 評価者は、TSS が以下であることを確認するため、TSS を検査しなければならない(shall)：

a) セキュリティ管理者が TOE コンポーネントのペア間の通信を有効化及び無効化する方法を記述している。

b) FCO_CPC_EXT.1.2 でなされた主な選択におけるチャネル種別に従って関連する詳細について記述している：

- 第 1 の種別 : TSS が利用されるチャネルを規定する関連 SFR の繰り返しを識別する
- 第 2 の種別：TSS(FTP_TRP.1.3/Join で選択される場合、操作ガイダンスからのサポートと共に) が利用するチャネルとメカニズムの詳細を記述する (及びその鍵がコンポーネントのペアに対して一意であることをプロセスが保証する方法について記述する) － FTP_TRP.1/Join の評価アクティビティについても参照。

252 評価者は、登録チャネルのあらゆる観点が FTP_ITC.1 または FPT_ITT.1 を満たさないものとして識別される場合、ST が FCO_CPC_EXT.1.2 の主たる選択において FTP_TRP.1/Join 選択肢についても選択したことを確認しなければならない(shall)。

3.6.1.2 ガイダンス証拠資料

253 (注釈：パラグラフ 249 は、評価者が TSS、ガイダンス証拠資料、及びテスト評価アクティビティの組み合わせを通して、決定及び回答を報告する必要がある質問を列挙している)

254 評価者は、分散型 TOE のあらゆる個別のコンポーネントとの通信を有効化及び無効化するための指示について、ガイダンス証拠資料に含まれていることを確

認するために、ガイダンス証拠資料を検査しなければならない(shall)。評価者は、無効化方法が、その他のすべてのコンポーネントが (無効化されたコンポーネントへの通信の開始を試行するか、または無効化されたコンポーネントからの通信へ応答することのいずれかをコンポーネントが続けようとすることを防止しつつ) TOE から削除されようとしているコンポーネントとの通信を防止できるようになることを確認しなければならない(shall)。

255 評価者は、登録プロセス中に意図せずに接続が切断されるときに取られるべきである(should) 回復のための指示について、ガイダンス証拠資料に含まれていることを確認するためにガイダンス証拠資料を検査しなければならない(shall)。

256 コンポーネントを TOE への登録するために TOE が登録チャネル (即ち、ST 作成者が FCO_CPC_EXT.1.2 の主たる選択において FTP_ITC.1/FPT_ITT.1 または FTP_TRP.1/Join チャネル種別を利用するような) を利用する場合、評価者は、それらが以下であることを確認するため、準備手続きを検査しなければならない (shall) :

a) 登録チャネルのセキュリティ特性 (例、基礎となるプロコトル、鍵及び認証データ) について記述する、及び (FTP_ITC.1 または FPT_ITT.1 での) 安定した状態のコンポーネント間チャネルのための要件を満たさないあらゆる観点にについて強調しなければならない(shall)

b) 登録チャネルの設定とその後のコンポーネント間通信のセキュリティの間のあらゆる依存性を識別する (例、AES-256 コンポーネント間通信がコンポーネント間での 256 ビット鍵の送信に依存し、ゆえに同等な鍵長を用いて構成されている登録チャネルに依拠するような)

c) チャネルセキュリティを改善するためにあらゆる観点のチャネルが運用環境によって改変できることを識別する、及びこの改変がどの程度達成可能であるかについて記述しなければならない(shall) (例、新しい鍵ペアを生成、またはデフォルト公開鍵証明書を置き換える)。

257 登録チャネル記述の検査のためのバックグラウンドとして、上記要件は管理者がデフォルト登録プロセスから上がるあらゆるリスクの正しい判定を行うことができることを保証することを意図していることに留意されたい。例としては、自己署名証明書 (即ち、外部またはローカルの認証局へチェインがない証明書)、製造業者発行の証明書 (失効のような観点での管理、またはデバイスが承認された証明書と共に発行されるような、運用環境の管理外であるようなもの) の利用、包括的／一意でない鍵の利用 (例、同じ鍵がデバイスの複数のインスタンス上で存在するようなもの)、またはよく知られた鍵 (即ち、鍵の機密性が強く保護されることを意図しないようなものーこれは、積極的なアクションまたは鍵を公開する意図があることを意味する必要はないことに留意されたい)。

258 ST 作成者が FCO_CPC_EXT.1.2 の主な選択にいて FTP_TRP.1/Join チャネル種別を利用し、TOE が登録チャネルセキュリティのいくつかの観点でセキュリティを提供するために運用環境に依拠するような分散型 TOE の場合において、セクション 3.5.1.2 で記述されるような、準備手続きにおける追加の要件がある。

3.6.1.3 テスト

259 (注釈：パラグラフ 249 は、評価者が TSS、ガイダンス証拠資料、及びテスト評価アクティビティの組み合わせを通して、決定及び回答を報告する必要がある質問を列挙している)

260 評価者は、以下のテストを実行しなければならない(shall)：

a) テスト 1.1：評価者は、通信する必要があるような非同等な TOE コンポーネント[6](同等でない TOE コンポーネントは、分散型 TOE 用の最小限の構成において定義されたものである)のそれぞれとしてセキュリティ管理者によって非メンバーエンティティが有効化されるまで、現在分散型 TOE のメンバーでないような IT エンティティが TOE の任意のコンポーネントと通信できないことを確認しなければならない(shall)

b) テスト 1.2：評価者は、有効化の後、ある IT エンティティが有効化されたコンポーネントとのみ通信できることを確認しなければならない(shall)。これには、有効化された通信が有効化されたコンポーネントペア用に成功するようなテスト、及び通信が明示的に有効化されていないようなその他のコンポーネントと通信が不成功であるようなテストが含まれる

いくつかの TOE は、有効化ステップが実行される前に登録チャネルをセットアップするかもしれないが、このような場合にそのチャネルは、有効化ステップが完了した後まで、通信を許可してはならない(must not)。

261 評価者は、TOE で利用可能な有効化プロセスのそれぞれの異なる種別について、テスト 1.1 及び 1.2 を繰り返さなければならない(shall)。

c) テスト 2：評価者は、それぞれの TOE コンポーネントについて順番に別々に無効化しなければならない(shall)、またその他の TOE コンポーネントが、次に、無効化されたコンポーネントとの通信の開始を試行することによって、または無効化されたコンポーネントからの通信試行への応答によって、無効化されたコンポーネントと通信できないことを保証しなければならない(shall)。

d) テスト 3：評価者は、FCO_CPC_EXT.1.2 について ST でなされた主な(外側の)選択の値に対して適用するようなものに従って、以下のテストを実行しなければならない(shall)。

1) もし ST が FCO_CPC_EXT.1.2 における選択で通信チャネルの第一の種別を利用する場合、評価者は、第二の選択に従って、FTP_ITC.1 または FPT_ITT.1 の評価アクティビティ経由でそのチャネルをテストすること－評価者は、これらの SFR のテストカバレージが登録プロセスでのそれらの利用を含むことを保証しなければならない(shall)。

2) もし ST が FCO_CPC_EXT.1.2 における選択で通信チャネルの第二の種別を利用する場合、評価者は、FTP_TRP.1/Join の評価アクティビティ経由でそのチャネルをテストすること。

3) もし ST が「チャネルなし」選択肢を利用する場合、一切のテストは要

[6] 「同等な TOE コンポーネント」は、いくつかのそのたの TOE コンポーネントとして、TSF 内で同じセキュリティ特性、ふるまい及び役割を見せるようなある種の分散型 TOE コンポーネントである。原則的に、分散型 TOE は、それぞれの同様な TOE コンポーネントの唯一のインスタンスを用いて動作することが可能であるが、分散型 TOE の最小構成は、複数のインスタンスを含むかもしれない(セクション B.4 の、分散型 TOE の最小構成の説明を参照)。実際に TOE の配備は、性能また別のサブネットや VLAN のために別のインスタンスを持つ必要性などの現実的な理由から、いくつかの同等な複数 TOE コンポーネントを含むことがある。

求されない。

e) テスト 4：評価者は、TSS 及び捜査ガイダンスで識別された TOE の特徴に従って、以下のテストの 1 つを実行しなければならない(shall)：

1) 登録チャネルがその後コンポーネント間の通信のために利用されない場合、及び FCO_CPC_EXT.1.2 における第二の選択(即ち、FTP_TRP.1/Join を用いて)がなされるようなすべての場合において、評価者は、登録が完了した後に端点のそれぞれと通信するチャネルの利用を試行することによって、登録プロセスが完了した後に登録プロセスがもはや利用可能でないことを確認しなければならない(shall)

2) 登録チャネルがその後コンポーネント間の通信のために利用されない場合、評価者は、定常状態のコンポーネント間チャネル用の要件(FDP_ITC.1 または FTP_ITT.1 のような)を満たすために必要なものとして操作ガイダンスにて識別されたあらゆる観点が本当に実行されることを確認しなければならない(shall) (例、デフォルト鍵ペア及び／または公開鍵証明書を置き換えるための要件があるかもしれない)。

f) テスト 5：チャネルセキュリティを改善するために運用環境によって改変可能な、操作ガイダンスに記述されている、登録チャネルのセキュリティそれぞれの観点について(参照、(参照、チャプター3.6.1.2 の準備手続きの要件)の AGD_PRE.1 詳細化 項目 2)、評価者は、操作ガイダンスに記述された以下の手順によって、この改変が正常に実行可能であることを確認しなければならない(shall)。

4 選択ベース要件の評価アクティビティ

4.1 暗号サポート (FCS)

4.1.1 FCS_DTLSC_EXT.1 拡張：DTLS クライアントプロトコル

4.1.1.1 TSS

FCS_DTLSC_EXT.1.1

262 評価者は、サポートされる暗号スイートが規定されることを保証するため、TSS の本プロトコルの実装の記述をチェックしなければならない(shall)。評価者は、規定される暗号スイートが本コンポーネントについて列挙されたものを含むことを保証するため、TSS をチェックしなければならない(shall)。

FCS_DTLSC_EXT.1.2

263 評価者は、どの種別の参照識別子がサポートされるか(例、Common Name、DNS Name、URI Name、Service Name、またはその他のアプリケーション特有の Subject Alternative Name) 及び IP アドレスとワイルドカードがサポートされるかどうかを含めて、管理者／アプリケーション設定の参照識別子からすべての参照識別子を確立するためのクライアントの方法について、TSS に記述されることを保証しなければならない(shall)。評価者は、この記述がどの証明書ピンニングがサポートされているか、または TOE によって利用されているか及びそのやり方について識別していることを保証しなければならない(shall)。

264 DTLS チャネルが FPT_ITT.1 のための分散型 TOE のコンポーネント間で利用されている場合、利用者によって参照識別を確立させるための要件は緩和され、その識別子は、「ゲートキーパー」探索プロセスを通して確立されてもよいことに留意されたい。TSS には、その探索プロセスを記述し、その参照識別子が「参加している」コンポーネントへ供給される方法について強調すべきである(should)。

FCS_DTLSC_EXT.1.4

265 評価者は、Supported Elliptic Curves Extension 及びその要求されるふるまいがデフォルトで実行されるかまたは設定されるかもしれないかについて、TSS に記述されることを検証しなければならない(shall)。

4.1.1.2 ガイダンス証拠資料

FCS_DTLSC_EXT.1.1

266 評価者は、DTLS が TSS の記述に適合するように、TOE の設定に関する指示を含んでいることを保証するため、ガイダンス証拠資料についてもチェックしなければならない(shall)。

FCS_DTLSC_EXT.1.2

267 評価者は、DTLS での証明書検証の目的で利用されるように参照識別子をセッティングするための指示が 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(shall)。

FCS_DTLSC_EXT.1.4

268 本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(must)ことを TSS が示す場合、評価者は、AGD ガイダンスが Supported

Elliptic Curves Extension の設定を含んでいることを検証しなければならない(shall)。

4.1.1.3 テスト

269 明確化のため：DTLS について、通信パケットは、UDP プロトコルの利用ゆえに、送信された順序と異なる順序で受信されるかもしれない。具体的なテストステップの順序を要求しているすべてのテスト(「前に」、「後で」) はそれゆえに、DTLS パケットのシーケンス番号を参照すること。

FCS_DTLSC_EXT.1.1

270 テスト 1：評価者は、本要件によって規定される暗号スイートのそれぞれを用いて DTLS 接続を確立しなければならない(shall)。この接続は、より上位レベルのアプリケーションプロトコルの確立の一部として確立されてもよい、例、syslog セションの一部として。本テストの意図を満たすために、暗号スイートのネゴシエーション成功を観測すれば十分である；利用されている暗号スイートを見分けるための試行において暗号化されたトラフィクの特性を検査することは必ずしも必要ではない(例えば暗号アルゴリズムが 128 ビット AES であり、256 ビット AES でない等)。

271 テスト 2：評価者は、extendedKeyUsage フィールドに Server Authentication 目的を含むサーバ証明書を持つサーバを用いて接続の確立を試行して、接続が確立されることを検証しなければならない(shall)。評価者は、次にクライアントが extendedKeyUsage フィールドに Server Authentication 目的を持たない以外は有効なサーバ証明書を拒否し、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 フィールド以外同一であるべきである(should)。

272 テスト 3：評価者は、DTLS 接続において、サーバ選択された暗号スイートと合致しないようなサーバ証明書(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)を送信しなければならない(shall)。評価者は、TOE がサーバの Certificate ハンドシェイクメッセージを受信した後、接続を切断することを検証しなければならない(shall)。

273 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(shall)。FCS_DTLSS_EXT.1.1 または FCS_DTLSS_EXT.2.1 でのテスト 2 が本テストについての代替として利用可能である。

274 テスト 5：評価者は、そのトラフィクに対して以下の改変を実行する：

a) Server Hello においてサーバによって選択された DTLS バージョンをサポートされない DTLS バージョン (例えば、2 バイト 03 04 で表される 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) DHE または ECDHE を利用する場合、Server Hello ハンドシェイクメッセージにおいてサーバのノンスの少なくとも 1 バイトを改変し、クライアントが Server Key Exchange ハンドシェイクメッセージを拒否する(DHE または ECDHE 暗号スイートを利用する場合) またはサーバがクライアントの Finished ハンドシェイクメッセージを拒否することを検証する。

c) Server Hello ハンドシェイクメッセージにおけるサーバの選択された暗号スイートを Client Hello ハンドシェイクにおいて存在しない暗号スイートとなるように改変する。評価者は、Server Hello を受信後、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(shall)。

d) DHE または ECDHE を利用する場合、Server’s Key Exchange ハンドシェイクメッセージにおいて署名ブロックを改変し、クライアントが Server Key Exchange メッセージを受信後に接続を拒否することを検証する。このテストは、RSA key exchange を用いる暗号スイートには適用されない。TOE が TLS に関して RSA key exchange のみをサポートする場合、このテストは省略されなければならない(shall)。

e) Server Finished ハンドシェイクメッセージにおいて 1 バイトを改変し、クライアントが受信に際して fatal alert を送信性、あらゆるアプリケーションデータを送信しないことを検証する。

f) サーバが ChangeCipherSpec メッセージを発行した後、サーバから意味不明の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_DTLSC_EXT.1.2

275 DTLS チャネルが FPT_ITT.1 のための分散型 TOE のコンポーネント間で利用されている場合、利用者によって参照識別を確立させるための要件は緩和され、その識別子は、「ゲートキーパー」探索プロセスを通して確立されてもよいことに留意されたい。TSS には、その探索プロセスを記述し、その参照識別子が「参加している」コンポーネントへ供給される方法について強調すべきである(should)。

276 評価者は、AGD ガイダンスに従って、参照識別子を設定し、DTLS 接続中に以下のテストを実行しなければならない(shall)：

a) テスト 1：評価者は、参照識別子と合致するような Subject Alternative Name(SAN) または Common Name(CN)のいずれかに識別子を含まないようなサーバ証明書を提示しなければならない(shall)。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(shall)。

b) テスト 2：評価者は、参照識別子と合致する CN を含み、参照識別子と合致する SAN における識別子を含まないような SAN extension を含むようなサーバ証明書を提示しなければならない(shall)。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(shall)。評価者は、サポートされる 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(shall)。

c) テスト 3：評価者は、参照識別子と合致する CN を含む、SAN extension を含まないサーバ証明書を提示しなければならない(shall)。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(shall)。

d) テスト 4：評価者は、参照識別子と合致しない CN を含むが、合致する SAN における識別子を含むようなサーバ証明書を提示しなければならない(shall)。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(shall)。

e) テスト 5：評価者は、参照識別子のサポートされるそれぞれの種別を持つ以下のワイルドカードテストを実行しなければならない(shall)：

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

2) 評価者は、最左端のラベルにワイルドカードを含むサーバ証明書(例、

*.example.com) を提示しなければならない(shall)。評価者は、1 つの最左端ラベルを持つ参照識別子(例、foo.example.com)を設定し、その接続が成功することを検証しなければならない(shall)。評価者は、証明書に際左端のラベルがない参照識別子(例 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(shall)。評価者は、2 つの最左端ラベルを持つ参照識別子(例、bar.foo.example.com)を設定し、その接続が失敗することを検証しなければならない(shall)。

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とされる場合、評価者は、DNS 名およびサービス識別子を設定しなければならない(shall)。評価者は、URIName または SAN の SRVName フィールドに正しい DNS 名およびサービス識別子を含んでいる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(shall)。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(shall)。

g) テスト 7 : [条件付き] ピンニングされた証明書がサポートされる場合、評価者は、ピンニングされた証明書と合致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(shall)。

FCS_DTLSC_EXT.1.3

277 テスト 1 : 評価者は、有効な証明パスを持たない証明書の利用が機能の失敗をもたらすことを実証しなければならない(shall)。管理者ガイダンスを用いて、評価者は、次にこの機能で利用されるべき証明書について検証する必要のある 1 つまたは複数の証明書をロードしなければならず(shall)、また、この機能が成功することを実証しなければならない(shall)。証明書が検証され、高信頼チャネルが確立される場合、テストは合格する。評価者は、次に証明書の 1 つを削除しなければならず(shall)、その証明書が検証されないこと、及び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(shall)。

FCS_DTLSC_EXT.1.4

278 テスト 1 : ECDHE 暗号を利用中の場合、評価者は、サポートされない曲線(例えば P-192)を用いて DTLS 接続で ECDHE key exchange を実装するようサーバを設定しなければならず(shall)、TOE がサーバの Key Exchange ハンドシェイクメッセージを受信後に接続を切断することを検証しなければならない(shall)。

4.1.2 FCS_DTLS_EXT.1 拡張 : 認証付き DTLS クライアントプロトコル

4.1.2.1 TSS

FCS_DTLSC_EXT.2.1

279 評価者は、サポートされる暗号スイートが規定されることを保証するため、TSS におけるこのプロトコルの実装の記述をチェックしなければならない(shall)。評価者は、規定される暗号スイートが本コンポーネントについて列挙されたものを含むことを保証するため、TSS をチェックしなければならない(shall)。

FCS_DTLSC_EXT.2.2

280 評価者は、どの種別の参照識別子がサポートされるか(例、Common Name、DNS Name、URI Name、Service Name、またはその他のアプリケーション特有の Subject Alternative Name) 及び IP アドレスとワイルドカードがサポートされるかどうかを含めて、管理者／アプリケーション設定の参照識別子からすべての参照識

別子を確立するためのクライアントの方法について、TSS に記述されることを保証しなければならない(shall)。評価者は、この記述がどの証明書ピンニングがサポートされているか、または TOE によって利用されているか及びそのやり方について識別していることを保証しなければならない(shall)。

FCS_DTLSC_EXT.2.4

281 評価者は、Supported Elliptic Curves Extension 及びその要求されるふるまいがデフォルトで実行されるかまたは設定されるかもしれないかについて、TSS に記述されることを検証しなければならない(shall)。

FCS_DTLSC_EXT.2.5

282 評価者は、DTLS 相互認証のためのクライアント側証明書の利用について、FIA_X509_EXT.2.1 に従って要求される TSS 記述に含まれていることを保証しなければならない(shall)。

FCS_DTLSC_EXT.2.6

283 評価者は、DTLS サーバからの受信されたメッセージが MAC 完全性チェックに失敗する場合に取られるアクションについて TSS に記述されていることを検証しなければならない(shall)。

FCS_DTLSC_EXT.2.7

284 評価者は、リプレイが検知される方法、及びスライディングウィンドウに合わせるには古すぎるような、以前受信された DTLS メッセージレコードに対して、静かに廃棄する方法について、TSS に記述されていることを検証しなければならない(shall)。

4.1.2.2 ガイダンス証拠資料

FCS_DTLSC_EXT.2.1

285 評価者は、DTLS が TSS の記述に適合するように、TOE の設定に関する指示を含んでいることを保証するため、ガイダンス証拠資料についてもチェックしなければならない(shall)。

FCS_DTLSC_EXT.2.2

286 評価者は、DTLS での証明書検証の目的で利用されるように参照識別子をセッティングするための指示が 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(shall)。

FCS_DTLSC_EXT.2.4

287 本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(must)ことを TSS が示す場合、評価者は、AGD ガイダンスが Supported Elliptic Curves Extension の設定を含んでいることを検証しなければならない(shall)。

FCS_DTLSC_EXT.2.5

288 DTLS 相互認証のためのクライアント側証明書の利用について、FIA_X509_EXT.2.1 に従って要求される 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(shall)。

4.1.2.3 テスト

289 明確化のため：DTLS について、通信パケットは、UDP プロトコルの利用ゆえに、送信された順序と異なる順序で受信されるかもしれない。具体的なテストステップの順序を要求しているすべてのテスト(「前に」、「後で」) はそれゆえに、DTLS パケットのシーケンス番号を参照すること。

FCS_DTLSC_EXT.2.1

290 テスト 1：評価者は、本要件によって規定される暗号スイートのそれぞれを用いて DTLS 接続を確立しなければならない(shall)。この接続は、より上位レベルのアプリケーションプロトコルの確立の一部として確立されてもよい、例、syslog セションの一部として。本テストの意図を満たすために、暗号スイートのネゴシエーション成功を観測すれば十分である；利用されている暗号スイートを見分けるための試行において暗号化されたトラフィクの特性を検査することは必ずしも必要ではない(例えば、暗号アルゴリズムが 128 ビット AES であり、256 ビット AES でない等)。

291 テスト 2：評価者は、extendedKeyUsage フィールドに Server Authentication 目的を含むサーバ証明書を持つサーバを用いて接続の確立を試行して、接続が確立されることを検証しなければならない(shall)。評価者は、次にクライアントが extendedKeyUsage フィールドに Server Authentication 目的を持たない以外は有効なサーバ証明書を拒否し、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 フィールド以外同一であるべきである(should)。

292 テスト 3：評価者は、DTLS 接続において、サーバ選択された暗号スイートと合致しないようなサーバ証明書(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)を送信しなければならない(shall)。評価者は、TOE がサーバの Certificate ハンドシェイクメッセージを受信した後、接続を切断することを検証しなければならない(shall)。

293 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(shall)。FCS_DTLSS_EXT.1.1 または FCS_DTLSS_EXT.2.1 でのテスト 2 が本テストについての代替として利用可能である。

294 テスト 5：評価者は、そのトラフィクに対して以下の改変を実行する：

a) Server Hello においてサーバによって選択された DTLS バージョンをサポートされない DTLS バージョン (例えば、2 バイト 03 04 で表される 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) DHE または ECDHE を利用する場合、Server Hello ハンドシェイクメッセージにおいてサーバのノンスの少なくとも 1 バイトを改変し、クライアントが Server Key Exchange ハンドシェイクメッセージを拒否する(DHE または ECDHE 暗号スイートを利用する場合) またはサーバがクライアントの Finished ハンドシェイクメッセージを拒否することを検証する。

c) Server Hello ハンドシェイクメッセージにおけるサーバの選択された暗号スイートを Client Hello ハンドシェイクにおいて存在しない暗号スイートとなるように改変する。評価者は、Server Hello を受信後、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(shall)。

d) DHE または ECDHE を利用する場合、Server’s Key Exchange ハンドシェイ

クメッセージにおいて署名ブロックを改変し、クライアントが Server Key Exchange メッセージを受信後に接続を拒否することを検証する。このテストは、RSA key exchange を用いる暗号スイートには適用されない。TOE が TLS に関して RSA key exchange のみをサポートする場合、このテストは省略されなければならない(shall)。

e) Server Finished ハンドシェイクメッセージにおいて 1 バイトを改変し、クライアントが受信に際して fatal alert を送信性、あらゆるアプリケーションデータを送信しないことを検証する。

f) サーバが ChangeCipherSpec メッセージを発行した後、サーバから意味不明の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_DTLSC_EXT.2.2

295 DTLS チャネルが FPT_ITT.1 のための分散型 TOE のコンポーネント間で利用されている場合、利用者によって参照識別を確立させるための要件は緩和され、その識別子は、「ゲートキーパー」探索プロセスを通して確立されてもよいことに留意されたい。TSS には、その探索プロセスを記述し、その参照識別子が「参加している」コンポーネントへ供給される方法について強調すべきである(should)。評価者は、AGD ガイダンスに従って、参照識別子を設定し、DTLS 接続中に以下のテストを実行しなければならない(shall)：：

a) テスト 1：評価者は、参照識別子と合致するような Subject Alternative Name(SAN) または Common Name(CN)のいずれかに識別子を含まないようなサーバ証明書を提示しなければならない(shall)。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(shall)。

b) テスト 2：評価者は、参照識別子と合致する CN を含み、参照識別子と合致する SAN における識別子を含まないような SAN extension を含むようなサーバ証明書を提示しなければならない(shall)。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(shall)。評価者は、サポートされる 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(shall)。

c) テスト 3：評価者は、参照識別子と合致する CN を含む、SAN extension を含まないサーバ証明書を提示しなければならない(shall)。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(shall)。

d) テスト 4：評価者は、参照識別子と合致しない CN を含むが、合致する SAN における識別子を含むようなサーバ証明書を提示しなければならない(shall)。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(shall)。

e) テスト 5：評価者は、参照識別子のサポートされるそれぞれの種別を持つ以下のワイルドカードテストを実行しなければならない(shall)：

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

2) 評価者は、最左端のラベルにワイルドカードを含むサーバ証明書(例、*.example.com) を提示しなければならない(shall)。評価者は、1 つの最左端ラベルを持つ参照識別子(例、foo.example.com)を設定し、その接続が成功することを検証しなければならない(shall)。評価者は、証明書に際左端のラベルがない参照識別子(例 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(shall)。評価者は、2 つの最左端ラベルを持つ参照識別子(例、bar.foo.example.com)を設定し、その接続が失敗することを検証しなければならない(shall)。

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る場合、評価者は、DNS 名およびサービス識別子を設定しなければならない(shall)。評価者は、URIName または SAN の SRVName フィールドに正しい DNS 名およびサービス識別子を含んでいる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(shall)。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(shall)。

g) テスト 7 : [条件付き] ピンニングされた証明書がサポートされる場合、評価者は、ピンニングされた証明書と合致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(shall)。

FCS_DTLSC_EXT.2.3

296 テスト 1 : 評価者は、有効な証明パスを持たない証明書を用いて機能の失敗をもたらすことを実証しなければならない(shall)。管理者ガイダンスを用いて、評価者は、次に本機能で利用されるべき証明書を検証する必要がある証明書をロードし、機能が成功することを実証しなければならない(shall)。証明書が検証され、高信頼チャネルが確立される場合、テストは合格する。評価者は、次に証明書の 1 つを策書、その証明書が検証されず、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(shall)。

FCS_DTLSC_EXT.2.4

297 テスト 1 : ECDHE 暗号を利用中の場合、評価者は、サポートされない曲線(例えば P-192)を用いて DTLS 接続で ECDHE key exchange を実装するようサーバを設定しなければならず(shall)、TOE がサーバの Key Exchange ハンドシェイクメッセージを受信後に接続を切断することを検証しなければならない(shall)。

FCS_DTLSC_EXT.2.5

298 テスト 1 : 評価者は、そのトラフィクに対して次の改変を実行しなければならない(shall) :

a) 相互認証を要求するようにサーバを設定し、次に Server's Certificate Request ハンドシェイクメッセージにおける CA フィールドの 1 バイトを改変する。改変された CA フィールドがクライアントの証明書を署名するために利用される CA であってはならない(must not)。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(shall)。

FCS_DTLSC_EXT.2.6

299 テスト 1 : 評価者は、DTLS 接続を確立しなければならない(shall)。評価者は、次に、レコードメッセージの少なくとも 1 バイトを改変し、クライアントがそのレコードを廃棄するか、DTLS セションを終了することを検証しなければならない(shall)。

FCS_DTLSC_EXT.2.7

300 テスト 1 : 評価者は、DTLS サーバとの DTLS 接続をセットアップしなければならない(shall)。評価者は、次に DTLS サーバから TOE へ送信されるトラフィクをキャプチャしなければならない(shall)。評価者は、DTLS サーバになりすます

ために TOE へこのトラフィクの複製を再送しなければならない(shall)。評価者は、TSF がこれらのパケットを受信した応答としてのアクションを取らないこと、及び監査ログがリプレイされたトラフィクが廃棄されたことを示すことを観測しなければならない(shall)。

4.1.3 FCS_DTLSS_EXT.1 拡張：DTLS サーバプロトコル

4.1.3.1 TSS

FCS_DTLSS_EXT.1.1

301 評価者は、サポートされる暗号スイートが規定されることを保証するため、TSS におけるこのプロトコルの実装の記述をチェックしなければならない(shall)。評価者は、規定される暗号スイートが本コンポーネントについて列挙されたものを含むことを保証するため、TSS をチェックしなければならない(shall)。

FCS_DTLSS_EXT.1.3

302 評価者は、DTLS クライアントの IP アドレスが Server Hello メッセージを発行する前に有効化される方法について、TSS に記述されていることを検証しなければならない(shall)。

FCS_DTLSS_EXT.1.4

303 評価者は、server Key Exchange メッセージの鍵共有パラメタについて、TSS に記述されていることを検証しなければならない(shall)。

FCS_DTLSS_EXT.1.5

304 評価者は、DTLS クライアントからの受信されたメッセージが MAC 完全性チェックを失敗する場合に取るアクションについて、TSS に記述されていることを検証しなければならない(shall)。

FCS_DTLSS_EXT.1.6

305 評価者は、リプレイが検知される方法、及びスライディングウィンドウに合わせるには古すぎるような、以前受信された DTLS メッセージレコードに対して、静かに廃棄する方法について、TSS に記述されていることを検証しなければならない(shall)。

4.1.3.2 ガイダンス証拠資料

FCS_DTLSS_EXT.1.1

306 評価者は、DTLS が TSS の記述に適合するように、TOE の設定に関する指示を含んでいることを保証するため、ガイダンス証拠資料についてもチェックしなければならない(shall) (例えば、TOE によって公告された暗号スイートのセットは、本要件を満たすために制限されなければならない(have to)かもしれない)。

FCS_DTLSS_EXT.1.4

307 評価者は、本要件を満たすために必要なあらゆる設定が AGD ガイダンスに含まれなければならない(must) ことを検証しなければならない(shall)。

4.1.3.3 テスト

308 明確化のため：DTLS について、通信パケットは、UDP プロトコルの利用ゆえ

に、送信された順序と異なる順序で受信されるかもしれない。具体的なテストステップの順序を要求しているすべてのテスト(「前に」、「後で」) はそれゆえに、DTLS パケットのシーケンス番号を参照すること。

FCS_DTLSS_EXT.1.1

309 テスト 1 : 評価者は、本要件によって規定される暗号スイートのそれぞれを用いて DTLS 接続を確立しなければならない(shall)。この接続は、より上位レベルのアプリケーションプロトコルの確立の一部として確立されてもよい、例、syslog セションの一部として。本テストの意図を満たすために、暗号スイートのネゴシエーション成功を観測すれば十分である ; 利用されている暗号スイートを見分けるための試行において暗号化されたトラフィクの特性を検査することは必ずしも必要ではない(例えば、暗号アルゴリズムが 128 ビット AES であり、256 ビット AES でない等)。

310 テスト 2 : 評価者は、サーバの ST におけるあらゆる暗号スイートを含まないような暗号スイートのリストと共に Client Hello をサーバへ送信し、サーバがその接続を拒否することを検証しなければならない(shall)。さらに、評価者は、TLS_NULL_WITH_NULL_NULL 山号スイートのみを含む Client Hello をサーバへ送信し、サーバがその接続を拒否することを検証しなければならない(shall)。

311 テスト 3 : 評価者は、サーバ選択された暗号スイートに合致しない (例えば、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートを利用しているが ECDHE key exchange を送信する、または ECDSA 暗号スイートの 1 つを利用しているが RSA key exchange を送信する) ような DTLS 接続において key exchange メッセージを送信するためにクライアントを利用しなければならない(shall)。評価者は、key exchange メッセージの受信後に TOE が接続を切断することを検証しなければならない(shall)。

312 テスト 4 : 評価者は、そのトラフィクに対して次の改変を実行しなければならない(shall) :

a) 撤回される

b) 撤回される

c) Client Finished ハンドシェイクメッセージにおいて、1 バイト改変し、サーバが接続を拒否し、アプリケーションデータを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 を生成した後、以前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意味不明の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_DTLSS_EXT.1.3

313 サーバの HelloVerifyRequest メッセージからのクッキーにおいて少なくとも 1 バイトを改変し、サーバがクライアントのハンドシェイクメッセージを拒否することを検証する。

FCS_DTLSS_EXT.1.4

314 ECDHE 暗号を用いる場合、評価者は、ECDHE 暗号スイート及び設定された曲線及びパケットアナライザを用いて接続を試行し、Key Exchange メッセージにおける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(shall)。(鍵長が設定された曲線の期待される鍵長と合致することを決定すること。) 評価者は、このテストをそれぞれのサポートされる NIST 楕円曲線とそれぞれのサポートされる Diffie-Hellman 鍵長について、繰り返さなければならない (shall) 。

315 評価者は、FCS_DTLSS_EXT.1.4 で選択されるとおり、それぞれの主張されたパラメタ (RSA 鍵長、Diffie-Hellman パラメタ、サポートされる曲線) と共に、それぞれの主張された鍵確立プロトコル (RSA、DH、ECDHE) を用いて接続の確立を試行しなければならない(shall)。例えば、RSA 鍵長が主張された長さと合致することを決定することは、本テストを満たすために十分である。評価者は、それぞれのサポートされたパラメタの組み合わせがテストされることを保証しなければならない(shall)。

316 本テストがその他のテストアクティビティと併せて達成可能であることに留意されたい。

FCS_DTLSS_EXT.1.5

317 評価者は、クライアントを用いて接続を確立しなければならない(shall)。評価者は、次に 1 つのレコードメッセージにおいて少なくとも 1 バイトを改変し、サーバがそのレコードを廃棄するか、DTLS セションを終了することを検証する。

FCS_DTLSS_EXT.1.6

318 評価者は、DTLS 接続をセットアップしなければならない(shall)。評価者は、次に DTLS クライアントから TOE へ送信されたトラフィクをキャプチャしなければならない(shall)。評価者は、DTLS クライアントになりすますために、TOE へのこのトラフィクの複製を再送信しなければならない(shall)。評価者は、TSF がこれらのパケットの受信への応答としてアクションを取らないこと、及び監査ログがリプレイされたトラフィクが廃棄されたことを示すことについて、観測しなければならない(shall)。

4.1.4 FCS_DTLSS_EXT.2 拡張：相互認証付き DTLS サーバプロトコル

4.1.4.1 TSS

FCS_DTLSS_EXT.2.1

319 評価者は、サポートされる暗号スイートが規定されることを保証するため、TSS におけるこのプロトコルの実装の記述をチェックしなければならない(shall)。評価者は、規定される暗号スイートが本コンポーネントについて列挙されたものを含むことを保証するため、TSS をチェックしなければならない(shall)。

FCS_DTLSS_EXT.2.3

320 評価者は、DTLS クライアントの IP アドレスが ServerHello メッセージを発行する前に有効化される方法について、TSS に記述されていることを検証しなければならない(shall)。

FCS_DTLSS_EXT.2.4

321 評価者は、server Key Exchange メッセージの鍵共有パラメタについて、TSS に

記述されていることを検証しなければならない(shall)。

FCS_DTLSS_EXT.2.5

322 評価者は、DTLS クライアントからの受信されたメッセージが MAC 完全性チェックを失敗する場合に取るアクションについて、TSS に記述されていることを検証しなければならない(shall)。

FCS_DTLSS_EXT.2.6

323 評価者は、リプレイが検出される方法、及びスライディングウィンドウに合わせるには古すぎるような、以前受信された DTLS メッセージレコードに対して、静かに廃棄する方法について、TSS に記述されていることを検証しなければならない(shall)。

FCS_DTLSS_EXT.2.7 及び FCS_DTLSS_EXT.2.8

324 評価者は、DTLS 相互認証のためのクライアント側証明書の利用について、FIA_X509_EXT.2.1 に従って要求される TSS 記述に含まれていることを保証しなければならない(shall)。

FCS_DTLSS_EXT.2.9

325 評価者は、証明書における DN または SAN が期待された識別子とどのように比較されるかが TSS に記述されていることを検証しなければならない(shall)。

4.1.4.2 ガイダンス証拠資料

FCS_DTLSS_EXT.2.1

326 評価者は、DTLS が TSS の記述に適合するように、TOE の設定に関する指示を含んでいることを保証するため、ガイダンス証拠資料についてもチェックしなければならない(shall) (例えば、TOE によって公告された暗号スイートのセットは、本要件を満たすために制限されなければならない(have to)かもしれない)。

FCS_DTLSS_EXT.2.4

327 評価者は、本要件を満たすために必要なあらゆる設定が AGD ガイダンスに含まれなければならない(must) ことを検証しなければならない(shall)。

FCS_DTLSS_EXT.2.7 及び FCS_DTLSS_EXT.2.8

328 DTLS 相互認証のためのクライアント側証明書の利用について、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(shall)。

FCS_DTLSS_EXT.2.9

329 DN が Domain Name または IP アドレス、利用者名、または電子メールアドレスと自動的に比較されない場合、評価者は、期待される DN の設定または接続のためのディレクトリサーバについて AGD 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(shall)。

4.1.4.3 テスト

330 明確化のため：DTLS について、通信パケットは、UDP プロトコルの利用ゆえに、送信された順序と異なる順序で受信されるかもしれない。具体的なテストステップの順序を要求しているすべてのテスト(「前に」、「後で」) はそれゆえに、DTLS パケットのシーケンス番号を参照すること。

FCS_DTLSS_EXT.2.1

331 テスト 1：評価者は、本要件によって規定される暗号スイートのそれぞれを用いて DTLS 接続を確立しなければならない(shall)。この接続は、より上位レベルのアプリケーションプロトコルの確立の一部として確立されてもよい、例、syslog セションの一部として。本テストの意図を満たすために、暗号スイートのネゴシエーション成功を観測すれば十分である；利用されている暗号スイートを見分けるための試行において暗号化されたトラフィクの特性を検査することは必ずしも必要ではない(例えば、暗号アルゴリズムが 128 ビット AES であり、256 ビット AES でない等)。

332 テスト 2：評価者は、サーバの ST におけるあらゆる暗号スイートを含まないような暗号スイートのリストと共に Client Hello をサーバへ送信し、サーバがその接続を拒否することを検証しなければならない(shall)。さらに、評価者は、TLS_NULL_WITH_NULL_NULL 暗号スイートのみを含む ClientHello をサーバへ送信し、サーバがその接続を拒否することを検証しなければならない(shall)。

333 テスト 3：評価者は、サーバ選択された暗号スイートに合致しない (例えば、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートを利用しているが ECDHE key exchange を送信する、または ECDSA 暗号スイートの 1 つを利用しているが RSA key exchange を送信する) ような DTLS 接続において key exchange メッセージを送信するためにクライアントを利用しなければならない(shall)。評価者は、key exchange メッセージの受信後に TOE が接続を切断することを検証しなければならない(shall)。

334 テスト 4：評価者は、そのトラフィクに対して次の改変を実行しなければならない(shall)：

a) 撤回される

b) 撤回される

c) Client Finished ハンドシェイクメッセージにおいて、1 バイト改変し、サーバが接続を拒否し、アプリケーションデータを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 を生成した後、以前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意味不明の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_DTLSS_EXT.2.3

335 サーバの HelloVerifyRequest メッセージからのクッキーにおいて少なくとも 1 バイトを改変し、サーバがクライアントのハンドシェイクメッセージを拒否することを検証する。

FCS_DTLSS_EXT.2.4

336 評価者は、ECDHE 暗号スイート及び設定された曲線及びパケットアナライザを用いて接続を試行し、Key Exchange メッセージにおける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(shall)。(鍵長が設定された

曲線の期待される鍵長と合致することを決定すること。) 評価者は、このテストをそれぞれのサポートされる NIST 楕円曲線とそれぞれのサポートされる Diffie-Hellman 鍵長について、繰り返さなければならない (shall) 。

337 評価者は、FCS_DTLSS_EXT.2.4 で選択されるとおり、それぞれの主張されたパラメタ (RSA 鍵長、Diffie-Hellman パラメタ、サポートされる曲線) と共に、それぞれの主張された鍵確立プロトコル (RSA、DH、ECDHE) を用いて接続の確立を試行しなければならない(shall)。例えば、RSA 鍵長が主張された長さと合致することを決定することは、本テストを満たすために十分である。評価者は、それぞれのサポートされたパラメタの組み合わせがテストされることを保証しなければならない(shall)。

338 本テストがその他のテストアクティビティと併せて達成可能であることに留意されたい。

FCS_DTLSS_EXT.2.5

339 評価者は、クライアントを用いて接続を確立しなければならない(shall)。評価者は、次に 1 つのレコードメッセージにおいて少なくとも 1 バイトを改変し、サーバがそのレコードを廃棄するか、DTLS セションを終了することを検証する。

FCS_DTLSS_EXT.2.6

340 評価者は、DTLS 接続をセットアップしなければならない(shall)。評価者は、次に DTLS クライアントから TOE へ送信されたトラフィクをキャプチャしなければならない(shall)。評価者は、DTLS クライアントになりすますために、TOE へのこのトラフィクの複製を再送信しなければならない(shall)。評価者は、TSF がこれらのパケットの受信への応答としてアクションを取らないこと、及び監査ログがリプレイされたトラフィクが廃棄されたことを示すことについて、観測しなければならない(shall)。

FCS_DTLSS_EXT.2.7 及び FCS_DTLSS_EXT.2.8

341 テスト 1 : 評価者は、クライアントへ証明書要求を送信するようサーバを設定し、クライアントからの証明書なしに接続を試行しなければならない(shall)。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(shall)。

342 テスト 2 : 評価者は、クライアントへ証明書要求をクライアントの証明書により利用される supported_signature_algorithm なしに送信するようサーバを設定しなければならない(shall)。評価者は、クライアントの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(shall)。

343 テスト 3 : 評価者は、有効な証明パスを持たない証明書の利用が機能の失敗をもたらすことを実証しなければならない(shall)。管理者ガイダンスを用いて、評価者は次に、その機能で利用されるべき小飯書を検証するために必要な 1 つの証明書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(shall)。評価者は、次にそれらの証明書の 1 つを削除し、機能が失敗することを示さなければならない(shall)。

344 テスト 4 : 評価者は、サーバの証明書要求メッセージにおける認証局 (ルートまたは中間 CA) の 1 つへチェインしないような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(shall)。評価者は、施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(shall)。

345 テスト 5 : 評価者は、extendedKeyUsage フィールドにおける Client Authentication

目的を持つ証明書を送信するようクライアントを設定し、サーバが施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(shall)。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ない(shall)、またサーバがこの接続を拒否することを検証しなければならない(shall)。理想的には、2つの証明書は、Client Authentication 目的以外は同一であるべきである(should)。

346 テスト 6：評価者は、そのトラフィクに対して以下の改変を実行しなければならない(shall)：

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

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

FCS_DTLSS_EXT.2.9

347 評価者は、期待される識別子に合致しないような識別子を持つクライアントの証明書を送信し、サーバがこの接続を拒否することを検証しなければならない(shall)。

4.1.5 FCS_HTTPS_EXT.1 HTTPS プロトコル

4.1.5.1 TSS

348 評価者は、TSS を検査し、その実装が RFC2818 にどのように適合するかについて説明するために十分な詳細情報が提供されていることを決定しなければならない(shall)。

4.1.5.2 テスト

349 評価者は、以下のテストを実行しなければならない(shall)：

a) テスト 1：評価者は、HTTPS を活用するそれぞれの高信頼パスまたはチャネルの確立を試行し、パケットアナライザでトラフィクを観測し、接続が成功することを検証し、そのトラフィクが TLS または HTTPS として識別されることを検証しなければならない(shall)。

350 その他のテストは、TLS 保証アクティビティと併せて行われる。

351 TOE が X.509 クライアント認証を活用する HTTPS クライアントまたは HTTPS サーバである場合、証明書の有効性は FIA_X509_EXT.1 のために実行されるテストに従ってテストされなければならず(shall)、また評価者は以下のテストを実行しなければならない(shall)：

a) テスト 1：評価者は、有効な証明パスのない証明書を利用すると、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(shall)。管理ガイダンスを利用して、評価者は次に、有効な証明書と証明パスをロードし、その機能が成功することを実証しなければならない(shall)。評価者は次に、

これらの証明書の 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(shall)。

4.1.6 FCS_IPSEC_EXT.1 IPsec プロトコル

4.1.6.1 TSS

FCS_IPSEC_EXT.1.1

352 評価者は、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決定するため、TSS を検査しなければならない(shall)。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規則が記述される。TSS には、利用可能な規則及び規則の照合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、これらの規則とアクションが RFC 4301 に定義される BYPASS (例、暗号化なし)、DISCARD (例、パケットの破棄)、及び PROTECT (例、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。

353 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規則構造が与えられた際に TSS の記述によってどの規則が適用されるか十分に決定できることを評価者は決定しなければならない(shall)。例えば、TOE が範囲、条件付き規則などの指定を許可している場合、規則処理の記述 (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決定できることを、特に 2 つの異なる規則が適用され得る場合について、評価者は決定しなければならない(shall)。この記述は、最初のパケット (即ち、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(shall)。

FCS_IPSEC_EXT.1.3

354 評価者は、VPN が (FCS_IPSEC_EXT.1.3 に識別されるように) トンネルモード及び／またはトランスポートモードで確立できると言明されていることを保証するため、TSS をチェックする。

FCS_IPSEC_EXT.1.4

355 評価者は、選択されたアルゴリズムが実装されていることを検証するため、TSS を検査しなければならない(shall)。さらに、評価者は SHA ベースの HMAC アルゴリズムが FCS_COP.1/KeyedHash 暗号操作 (鍵付きハッシュメッセージ認証) で規定されるアルゴリズムに適合することを保証する。

FCS_IPSEC_EXT.1.5

356 評価者は、IKEv1 及び／または IKEv2 が実装されていることを検証するため、T SS を検査しなければならない(shall)。

357 IKEv1 の実装について、評価者は、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利用されず、メインモードのみが利用されることが言明されていることを保証するため、TSS を検査しなければならない(shall)。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

358 評価者は、IKEv1 及び／または IKEv2 のペイロードの暗号化に用いられるアルゴリズムが TSS に識別されていること、及び本要件の選択において選ばれたアルゴリズムが TSS の説明に含まれていることを保証しなければならない(shall)。

FCS_IPSEC_EXT.1.7

359 評価者は、IKEv1 のフェーズ 1 SA ライフタイム及び／または IKEv2 の SA ライフタイム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 で識別されていることを保証しなければならない(shall)。評価者は、ここでなされた選択が 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(shall)。

FCS_IPSEC_EXT.1.8

360 評価者は、IKEv1 のフェーズ 2 SA ライフタイム及び／または IKEv2 の Child SA ライフタイム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 で識別されていることを保証しなければならない(shall)。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(shall)。

FCS_IPSEC_EXT.1.9

361 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保証するため、チェックしなければならない(shall)。評価者は、本 PP の要件を満たすような、生成された乱数が利用されること、及び「x」の長さが本要件での規定を満たすことについて TSS に示されていることを検証しなければならない(shall)。

FCS_IPSEC_EXT.1.10

362 最初の選択肢が選ばれる場合、評価者は、サポートされる DH グループがについて、それぞれのノンスの生成のためのプロセスについて、TSS に記述されていることを保証するため、チェックしなければならない(shall)。評価者は、本 PP の要件を満たすような生成された乱数が利用されることが TSS に示されていること、及びノンスの長さが本要件の規定を満たすことを検証しなければならない(shall)。

363 2 番目の選択肢が選ばれる場合、評価者は、サポートされる PRF ハッシュについて、それぞれのノンスの生成のためのプロセスについて TSS に記述されていることを保証するためチェックしなければならない(shall)。評価者は、本 PP の要件を満たすような生成された乱数が利用されることが TSS に示されていること、及びノンスの長さが本要件の規定を満たすことを検証しなければならない(shall)。

FCS_IPSEC_EXT.1.11

364 評価者は、本要件で規定された DH グループがサポートされているものとして TSS に列挙されていることを保証するため、チェックしなければならない(shall)。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 グループがどのように規定され／ピアとの間でネゴシエーションされるかについて TSS に記述されていることを保証するため、チェックする。

FCS_IPSEC_EXT.1.12

365 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(shall)。また TSS には、IKEv1 フェーズ 2 及び／または IKEv2 CHILD_SA スイート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(shall)。

FCS_IPSEC_EXT.1.13

366 評価者は、RSA 及び／または ECDSA がピア認証を行うために使われるものとして TSS が識別していることを保証する。この記述は、FCS_COP.1/SigGen 暗号操作 (暗号署名) で規定されるアルゴリズムと一貫していなければならない(shall)。

367 選択において事前共有鍵が選択されている場合、評価者は、事前共有鍵が確立され、IPsec 接続の認証で利用される方法が TSS に記述されていることを保証するため、チェックしなければならない(shall)。TSS の記述には、事前共有鍵を単に利用する TOE と同様に、事前共有鍵を生成できる TOE のために事前共有鍵の確立が達成される方法についても示されていなければならない(shall)。

FCS_IPSEC_EXT.1.14

368 評価者は、TOE がピアの提示された識別子を参照識別子と比較する方法が TSS に記述されていることを検証しなければならない(shall)。この記述には、証明書のどのフィールドが提示された識別子 (DN、Common Name、または SAN) として利用されるかが含まれなければならない(shall)。ST 作成者が追加の識別子種別を割り付けた場合、TSS 記述には、その種別及びその種別がピアの提示された証明書と比較される方法についても記述されなければならない(shall)。

4.1.6.2 ガイダンス証拠資料

FCS_IPSEC_EXT.1.1

369 評価者は、パケットを処理する規則を規定する SPD へのエントリを構築する方法について管理者へ指示していることを検証するため、ガイダンス証拠資料を検査しなければならない(shall)。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、破棄される、及び暗号化されずに TOE を通過して流れることを保証する規則が含まれる。評価者は、ガイダンス証拠資料の記述が 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証拠資料が十分に詳細なレベルであることを決定しなければならない(shall)。これには、規則の順序が 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

370 評価者は、それぞれの選択されたモードでの接続の設定方法に関する指示がガイダンス証拠資料に含まれることを確認しなければならない(shall)。

FCS_IPSEC_EXT.1.4

371 評価者は、選択されたアルゴリズムを利用するよう TOE を設定する方法についての指示を提供していることを保証するため、ガイダンス証拠資料をチェック

する。

FCS_IPSEC_EXT.1.5

372 評価者は、(選択されたように) IKEv1 及び／または IKEv2 を利用するように 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するため、ガイダンス証拠資料をチェックしなければならず(shall)、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)。

373 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、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するため、ガイダンス証拠資料をチェックしなければならない(shall)。

FCS_IPSEC_EXT.1.6

374 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) ガイダンス証拠資料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

375 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証拠資料に存在することを検証しなければならない(shall)。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

376 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証拠資料に存在することを検証しなければならない(shall)。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

377 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) ガイダンス証拠資料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

378 評価者は、RSA 及び／または ECDSA の署名及び公開鍵を利用するよう TOE を設定する方法がガイダンス証拠資料に記述されていることを保証する。

379 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証拠資料に記述されていることをチェックしなければならない(shall)。またガイダンス証拠資料の記述には、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(shall)。

380 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証拠資料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

381 評価者は、接続のために期待される DN の設定がガイダンス証拠資料に含まれることを保証しなければならない(shall)。

4.1.6.3 テスト

FCS_IPSEC_EXT.1.1

382 評価者は、ガイダンス証拠資料を用いて 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規則、パケットを暗号化する規則、及びパケットが平文で流れることを許可する規則が存在するように SPD を設定しなければならない(shall)。パケットヘッダに適切なフィールド (規則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、規則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(shall)。評価者は、各タイプの規則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、その規則に合致するパケットとその規則に合致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経由で、TOE が期待されたふるまいを示していることを観測すること：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(shall)。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 及びガイダンス証拠資料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(shall)。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規則、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 とガイダンス証拠資料の両方と一貫していることを検証しなければならない(shall)。

FCS_IPSEC_EXT.1.2

383 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併せて行われる。

384 評価者は、ガイダンス証拠資料を用いて TOE を構成し、以下のテストを実施する：

385 評価者は、パケットを破棄する規則、パケットを暗号化する規則、及びパケットが平文で流れることを許可する規則が存在するように SPD を設定しなけれ

ばならない(shall)。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規則に合致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(shall)。評価者は、ネットワークパケットが改変なしに適切な宛先インタフェースへ通過することを観測すべきである(should)。評価者は次に、もはや評価者が作成したエントリへは合致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(shall) (それ以前のエントリのどれにも合致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観測する。

FCS_IPSEC_EXT.1.3

386 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実行しなければならない(shall) :

a) テスト 1 (条件付き) : トンネルモードが選択される場合、評価者は 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ため、ガイダンス証拠資料を利用する。評価者は、任意の許容可能な暗号アルゴリズム、認証方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(shall)。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) 観測する。

b) テスト 2 (条件付き) : 評価者は、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ため、ガイダンス証拠資料を利用する。評価者は、任意の許容される暗号アルゴリズム、認証方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) 観測する。

FCS_IPSEC_EXT.1.4

387 評価者は、ガイダンス証拠資料に示されるように 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 を利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(shall)。

FCS_IPSEC_EXT.1.5

388 テストは、他の IPsec 評価アクティビティと併せて行われる。

a) (条件付き) : 評価者はガイダンス証拠資料に示されるように 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(shall)。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(should)。

b) (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(shall)。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決定しなければならない(shall)。

FCS_IPSEC_EXT.1.6

389 評価者は、IKEv1 及び／または IKEv2 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(shall)。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

390 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(should)。」

391 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(shall)。

a) テスト 1 (条件付き) : 評価者は、ガイダンス証拠資料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(shall)。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(shall)。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決定しなければならない(shall)。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(shall)。

b) テスト 2 (条件付き) : 評価者は、ガイダンス証拠資料に従ってフェーズ 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(shall)。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(shall)。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決定しなければならない(shall)。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(shall)。

FCS_IPSEC_EXT.1.8

392 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(should)。」

393 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(shall)。

a) テスト 1 (条件付き) : 評価者は、ガイダンス証拠資料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(shall)。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(shall)。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決定しなければならない(shall)。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(shall)。

b) テスト 2 (条件付き) : 評価者は、ガイダンス証拠資料に従ってフェーズ 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(shall)。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(shall)。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決定しなければならない(shall)。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(shall)。

FCS_IPSEC_EXT.1.10

394 次のテストのそれぞれは、FCS_IPSEC_EXT.1.5 プロトコル選択において選択された IKE のそれぞれのバージョンについて実行されなければならない(shall) :

a) テスト 1 : 最初の選択が選ばれている場合、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、各ノンスを生成するためのプロセスについて TSS に記述されていることを保証するため、チェックしなければならない(shall)。評価者は、本 PP の要件を満たすように生成された乱数が利用されること、及びノンスの長さが本要件での規定を満たすことについて TSS に示されていることを検証しなければならない(shall)。

b) テスト 2 : 2 番目の選択が選ばれている場合、評価者は、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ためのプロセスについて TSS に記述されていることを保証するため、チェックしなければならない(shall)。評価者は、本 PP の要件を満たすように生成された乱数が利用されること、及びノンスの長さが要件での規定を満たすことについて TSS に示されていることを検証しなければならない(shall)。

FCS_IPSEC_EXT.1.11

395 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保証するため、テストしなければならない(shall)。

FCS_IPSEC_EXT.1.12

396 評価者は、次のテストを実行するため、TOE を設定するためのガイダンスに単に従う。

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(shall)。評価者は、本要件で識別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(shall)。

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(shall)。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(shall)。そのような試行は失敗すべきである(should)。

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(shall)。評価者は、本要件で識別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(shall)。そのような試行は失敗すべきである(should)。

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(shall)。評価者は、FCS_IPSEC_EXT.1.4 で識別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(shall)。そのような試行は失敗すべきである(should)。

FCS_IPSEC_EXT.1.13

397 効率性の観点から、本テストは、FIA_X509_EXT.1、FIA_X509_EXT.2 (IPsec 接続について)、及び FCS_IPSEC_EXT.1.1 のテストと併せて実行されてもよい。次のテストは、上記 FCS_IPSEC_EXT.1.13 で選択されたピア認証方法のそれぞれについて繰り返されなければならない(shall)：

a) テスト 1：評価者は、プライベート鍵及びそれに対応する証明書で信頼済み CA によって署名されたものを利用するように TOE を設定しなければならず(shall)、またピアとの IPsec 接続を確立しなければならない(shall)。

b) テスト 2：事前共有鍵が選択される場合、評価者は、TOE 以外で事前共有鍵を生成し、ガイダンス証拠資料に示されるように、ピアとの IPsec 接続を確立するために、それを利用しなければならない(shall)。

FCS_IPSEC_EXT.1.14

398 それぞれのサポートされる識別子種別 (DN を除く) について、評価者は、次のテストを繰り返さなければならない(shall)：

a) テスト 1：比較のためにサポートされる証明書の各フィールドについて、評価者は、ピアの提示された証明書内のフィールドと合致するように (管理者ガイダンスに沿って) TOE 上のピアの参照識別子を設定しなければならず(shall) 、また IKE 認証が成功することを検証しなければならない(shall)。

b) テスト 2：比較のためにサポートされる証明書の各フィールドについて、

評価者は、ピアの提示された証明書内のフィールドと合致しないように(管理者ガイダンスに沿って) TOE 上のピアの参照識別子を設定しなければならず(shall) 、また IKE 認証が失敗することを検証しなければならない(shall)。

c) テスト 3 : (条件付き) TOE が DN 識別子種別をサポートする場合、評価者は、ピアの提示された証明書内の Subject DN と合致するように (管理者ガイダンスに沿って) TOE 上のピアの参照識別子を設定しなければならず(shall) 、また IKE 認証が成功することを検証しなければならない(shall)。DN のビット単位の比較を実証するため、評価者は、DN 内の単一ビットを変更しなければならない(shall) (望ましくは、DN 内の Object Identifier(OID)において)、また IKE 認証が失敗することを検証しなければならない(shall)。

4.1.7 FCS_SSHC_EXT.1 SSH クライアント

4.1.7.1 TSS

FCS_SSHC_EXT.1.2

399 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、及びこのリストが FCS_SSHC_EXT.1.5 に適合することを保証し、パスワードベースの認証方法が ST で選択された場合、これらについても記述されていることを保証するため、チェックしなければならない(shall)。

FCS_SSHC_EXT.1.3

400 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(shall)。

FCS_SSHC_EXT.1.4

401 評価者は、オプションの特性が規定され、またサポートされる暗号アルゴリズムも同様に規定されていることを保証するため、TSS のこのプロトコルの実装の記述をチェックしなければならない(shall)。評価者は、規定された暗号化アルゴリズムがこのコンポーネントで列挙されたものと同一であることを保証するため、TSS をチェックしなければならない(shall)。

FCS_SSHC_EXT.1.5

402 評価者は、オプションの特性が規定されること、及びサポートされる公開鍵アルゴリズムも同様に規定されることを保証するため、TSS のこのプロトコルの実装の記述をチェックしなければならない(shall)。評価者は、規定された公開鍵アルゴリズムがこのコンポーネントで列挙されたものと同一であることを保証するため、TSS をチェックしなければならない(shall)。

FCS_SSHC_EXT.1.6

403 評価者は、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するため、TSS をチェックしなければならない(shall)。

FCS_SSHC_EXT.1.7

404 評価者は、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するため、TSS をチェックしなければならない(shall)。

FCS_SSHC_EXT.1.8

405 評価者は、以下について TSS が規定していることをチェックしなければならない(shall)：

1. 両方のしきい値が TOE によってチェックされる。
2. 鍵変更 (Rekeying) が、最初に起こったしきい値への到達に際して実行される。

4.1.7.2 ガイダンス証拠資料

FCS_SSHC_EXT.1.4

406 評価者は、SSH が TSS の記述に適合する (例えば、TOE によって公告されるアルゴリズムのセットは、本要件を満たすように制限されなければならない(have to)かもしれない) ように TOE の設定についての指示がガイダンス証拠資料に含まれることを保証するため、ガイダンス証拠資料についてもチェックしなければならない(shall)。

FCS_SSHC_EXT.1.5

407 評価者は、SSH が TSS の記述に適合する (例えば、TOE によって公告されるアルゴリズムのセットは、本要件を満たすように制限されなければならない(have to)かもしれない) ように TOE の設定についての指示がガイダンス証拠資料に含まれることを保証するため、ガイダンス証拠資料をチェックしなければならない(shall)。

FCS_SSHC_EXT.1.6

408 また評価者は、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するため、ガイダンス証拠資料をチェックしなければならない(shall)。

FCS_SSHC_EXT.1.7

409 また評価者は、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するため、ガイダンス証拠資料をチェックしなければならない(shall)。

FCS_SSHC_EXT.1.8

410 本 SFR を満たすために TOE によってチェックされるような 1 つ以上のしきい値が設定可能な場合、評価者は、それらのしきい値の設定方法についてガイダンス証拠資料に記述されていることをチェックしなければならない(shall)。いずれかの許可された値がガイダンス証拠資料で規定され、かつ本 SFR で規定された制限を超えてはならない(must not) (1 時間のセション時間、1 ギガバイトの送信されたトラフィク)、または TOE は、本 SFR で規定された制限を超えた値を受け入れてはならない(must not)。評価者は、最初に達したしきい値に TOE が反応することについてガイダンス証拠資料に記述されていることをチェックしな

ければならない(shall)。

4.1.7.3 テスト

FCS_SSHC_EXT.1.2

411 テスト 1：パスワードベースの認証方法が ST で選択された場合、ガイダンス証拠資料を用いて、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(shall)。

注釈：公開鍵認証は FCS_SSHC_EXT.1.5 のテストの一部としてテストされる。

FCS_SSHC_EXT.1.3

412 評価者は、本コンポーネントで規定される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(shall)。

FCS_SSHC_EXT.1.4

413 評価者は、SSH 接続を確立するために主張された暗号と暗号プリミティブのみが利用されることを保証しなければならない(shall)。これを検証するため、評価者は、リモートサーバとの SSH 接続のためのセション確立を開始しなければならない(shall) (以下において「リモート端点」として参照される)。評価者は、プロトコルネゴシエーション中に TOE とリモート端点の間で交換されるトラフィクをキャプチャしなければならない(shall) (例、パケットキャプチャツール、または端点によって提供される情報をそれぞれ用いて)。評価者は、TOE が SSH セション用に TOE のために TSS で定義されたすべての暗号を提供するが、TSS の定義と比較に比較して一切の追加はないことをキャプチャされたトラフィクから検証しなければならない(shall) 評価者は、TOE が期待されるとおりふるまうことを検証するため、SSH セションのネゴシエーションを成功裏に実行しなければならない(shall)。本テストの意図を満たすには、セションのネゴシエーション成功を観測すれば十分である。評価者が SSH 用に TSS で定義されたすべての暗号が必ずしも TOE によってサポートされないこと、及び／または TOE が SSH 用に TSS で定義されない 1 つ以上の追加の暗号をサポートすることを検出する場合、本テストは、失敗したと見なされなければならない(shall)。

FCS_SSHC_EXT.1.5

414 テスト 1：評価者は、SSH サーバを TOE に対して認証するため、本要件で規定された公開鍵アルゴリズムそれぞれを用いて、SSH 接続を確立しなければならない(shall)。本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) 観測すれば十分である。

415 テスト 2：評価者は、ST の選択において含まれないような公開鍵アルゴリズムのみを許すように SSH サーバを設定しなければならない(shall)。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観測しなければならない(shall)。

FCS_SSHC_EXT.1.6

416 テスト 1：評価者は、本要件で規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(shall)。本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) 観測すれば十分である。

417 テスト 2：評価者は、ST 選択で含まれないような MAC アルゴリズムのみを許可するように SSH サーバを設定しなければならない(shall)。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観測しなければならない(shall)。

FCS_SSHC_EXT.1.7

418 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(shall)。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観測しなければならない(shall)。

FCS_SSHC_EXT.1.8

419 評価者は、TSS の記述に従って鍵変更が実行されるようなテストを実行する必要がある。評価者は、時間ベースのしきい値及びトラフィクベースのしきい値の両方についてテストしなければならない(shall)。

420 時間ベースのしきい値のテストについて、評価者は、SSH サーバへ接続するため、TOE を利用し、しきい値に達するまでセションをオープンのまま保持しなければならない(shall)。評価者は、SSH セションがしきい値より長くアクティブであること及び対応する監査事象が TOE によって生成されることを検証しなければならない(shall)。

421 テストは、1 時間のセション時間の最大許可値で設定されたしきい値を用いて実行される必要は必ずしもないが、テストで利用される値は、1 時間を超えてはならない(shall not)。評価者は、鍵変更が TOE によって開始されたこと及び TOE が接続される SSH サーバによって開始されていないことを保証する必要がある。

422 トラフィクベースのしきい値のテストについて、評価者は、SSH サーバに接続するため、TOE を利用しなければならない(shall)、また評価者は、送信されたトラフィクがしきい値に達するまで、アクティブな SSH セション内の TOE から及び TOE へのデータを送信しなければならない(shall)。送信されたトラフィクとは、送信と受信トラフィクからなる合計トラフィクである。

423 評価者は、許可されたしきい値より多いデータが SSH セション内で送信されたこと、及び対応する監査事象が TOE によって生成されたことを検証しなければならない(shall)。

424 テストは、1 ギガバイトの転送されたトラフィクの最大許可値で設定されたしきい値を用いて実行される必要は必ずしもないが、テストで利用される値は、1 ギガバイトを超えてはならない(shall not)。評価者は、鍵変更が TOE によって開始されたこと及び TOE が接続される SSH サーバによって開始されていないことを保証する必要がある。

425 SFR を満たすために TOE によってチェックされるような 1 つ以上のしきい値が設定可能な場合、評価者は、そのしきい値がガイダンス証拠資料に記述されたとおり設定可能であることを検証する必要がある、または評価者は、しきい値の改変がセキュリティ管理者に限定されることをテストする必要がある(FMT_MOF.1/Functions によって要求されるとおり)。

FCS_SSHC_EXT.1.9

426 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(shall)。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(shall)。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(shall)。

427 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(shall)。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(shall)。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(shall)、TOE がその接続を拒否することを保証しなければならず(shall)、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(shall) (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)。

4.1.8 FCS_SSHS_EXT.1 SSH サーバ

4.1.8.1 TSS

FCS_SSHS_EXT.1.2

428 評価者は、認証用の利用に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 に適合することを保証するためにチェックしなければならず(shall)、また、パスワードベースの認証方法についても許可されることを保証するためにチェックしなければならない(shall)。

FCS_SSHS_EXT.1.3

429 評価者は、RFC 4253 に関して「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(shall)。

FCS_SSHS_EXT.1.4

430 評価者は、オプションの特性が規定されること、及びサポートされる暗号アルゴリズムも同様に規定されることを保証するため、TSS における本プロトコルの実装の記述をチェックしなければならない(shall)。評価者は、規定された暗号化アルゴリズムが本コンポーネントで列挙されるものと同一であることを保証するため、TSS をチェックしなければならない(shall)。

FCS_SSHS_EXT.1.5

431 評価者は、オプションの特性が規定されること、及びサポートされる公開鍵アルゴリズムも同様に規定されることを保証するため、TSS における本プロトコルの実装の記述をチェックしなければならない(shall)。評価者は、規定された公開鍵アルゴリズムが本コンポーネントで列挙されるものと同一であることを保証するため、TSS をチェックしなければならない(shall)。

FCS_SSHS_EXT.1.6

432 評価者は、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、及びそのリストが本コンポーネントのリストと対応していることを保証するため、TSS をチェックしなければならない(shall)。

FCS_SSHS_EXT.1.7

433 評価者は、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、またそのリストが本コンポーネントのリストと対応していることを保証するため、TSS をチェックしなければならない(shall)。

FCS_SSHS_EXT.1.8

434 評価者は、以下について TSS が規定していることをチェックしなければならない(shall)：

1. 両方のしきい値が TOE によってチェックされる。
2. 鍵変更 (Rekeying) が、最初に起こったしきい値への到達に際して実行される。

4.1.8.2 ガイダンス証拠資料

FCS_SSHS_EXT.1.4

435 また評価者は、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するため、ガイダンス証拠資料をチェックしなければならない(shall)。

FCS_SSHS_EXT.1.5

436 また評価者は、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(have to)かもしれない) が含まれていることを保証するため、ガイダンス証拠資料をチェックしなければならない(shall)。

FCS_SSHS_EXT.1.6

437 また評価者は、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するため、ガイダンス証拠資料をチェックしなければならない(shall)。

FCS_SSHS_EXT.1.7

438 また評価者は、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するため、ガイダンス証拠資料をチェックしなければならない(shall)。

FCS_SSHS_EXT.1.8

439 SFR を満たすために TOE によってチェックされるような 1 つ以上のしきい値が設定可能な場合、評価者は、ガイダンス証拠資料にそれらのしきい値の設定方法について記述されていることをチェックしなければならない(shall)。どちらかの許可された値がガイダンス証拠資料に規定され、かつ SFR で規定された制限を超えてはならない(must not) (1 時間のセション時間、1 ギガバイトの送信トラフィク)、または TOE は、SFR で規定された制限を超えた値を受け入れてはならない(must not)。評価者は、ガイダンス証拠資料に TOE が最初に達したしきい値に反応することについて記述されていることをチェックしなければならない(shall)。

4.1.8.3 テスト

FCS_SSHS_EXT.1.2

440 テスト 1：ガイダンス証拠資料を用いて、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(shall)。

441 テスト 2：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(shall)。

注釈：公開鍵認証は FCS_SSHC_EXT.1.5 のテストの一部としてテストされる。

FCS_SSHS_EXT.1.3

442 評価者は、本コンポーネントで規定されるよりも大きなパケットを TOE が受信する場合に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(shall)。

FCS_SSHS_EXT.1.4

443 評価者は、主張された暗号と暗号プリミティブのみが SSH 接続を確立するために利用されることを保証しなければならない(must)。これを検証するため、評価者は、リモートクライアント(以下で「リモート端点」として参照される) からの SSH のためのセション確立を開始しなければならない(shall)。評価者は、プロトコルネゴシエーション中に TOE とリモート端点の間のトラフィクをキャプチャしなければならない(shall) (例、それぞれパケットキャプチャツールまたは端点によって提供された情報を用いて)。評価者は、TOE が SSH セションに対する TOE の TSS で定義されたすべての暗号を提供するが、TSS の定義と比較して一切の追加されたものがないことをキャプチャされたトラフィクから検証しなければならない(shall)。評価者は、TOE が期待されるとおりにふるまうことを検証するため、SSH セションの成功するネゴシエーションを実行しなければならない(shall)。テストの意図を満たすためには、セションのネゴシエーション成功を観測すれば十分である。評価者が SSH 用に TSS で定義されたすべての暗号が TOE によって必ずしもサポートされない、及び／または TOE が SSH 用に TSS で定義されない 1 つ以上の追加の暗号をサポートすることを検出する場合、テストは、失敗したと見なされなければならない(shall)。

FCS_SSHS_EXT.1.5

444 テスト 1：評価者は、TOE を SSH クライアントに対して認証するため、本要件によって規定された公開鍵アルゴリズムそれぞれを用いて、SSH 接続を確立しなければならない(shall)。本テストの意図を満たすには、そのアルゴリズムのネゴシエーション成功を (通信路上で) 観測すれば十分である。

445 テスト 2：評価者は、TOE によってサポートされる 1 つの公開鍵アルゴリズムを選ばなければならない(shall)。評価者は、認証用の公開鍵を認識するために TOE を設定することなしにそのアルゴリズムの新しい鍵ペアを生成しなければならない(shall)。評価者は、新しい鍵ペアを用いて TOE への接続試行するため、SSH クライアントを利用し、認証が失敗することを実証しなければならない (shall)。

446 テスト 3：評価者は、ST 選択に含まれないような、公開鍵アルゴリズムのみを許可するよう、SSH クライアントを設定しなければならない(shall)。評価者は、

SSH クライアントから TOE への SSH 接続を確立試行し、その接続が拒否されることを観測しなければならない(shall)。

FCS_SSHS_EXT.1.6

447 テスト 1：評価者は、本要件で規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(shall)。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) 観測すれば十分である。

448 テスト 2：評価者は、SSH クライアントを ST の選択に含まれないような MAC アルゴリズムのみを許可するように設定しなければならない(shall)。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観測しなければならない(shall)。

FCS_SSHS_EXT.1.7

449 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(shall)。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観測しなければならない(shall)。

450 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観測しなければならない(shall)。

FCS_SSHS_EXT.1.8

451 評価者は、TSS の記述に従って鍵変更が実行されるようなテストを実行する必要がある。評価者は、時間ベースのしきい値及びトラフィクベースのしきい値の両方について、テストしなければならない(shall)。

452 時間ベースのしきい値のテストについて、評価者は、TOE へ接続するために SSH クライアントを利用し、しきい値に達するまでそのセションをオープンのまま保持しなければならない(shall)。評価者は、SSH セションがしきい値よりも長くアクティブであること及び対応する監査事象が TOE によって生成されたことを検証しなければならない(shall)。

453 テストは、1 時間のセション時間の最大許可値で設定されたしきい値を用いて実行される必要は必ずしもないが、テストで利用される値は、1 時間を超えてはならない(shall not)。評価者は、鍵変更が TOE によって開始されたこと及び TOE へ接続される SSH クライアントによって開始されていないことを保証する必要がある。

454 トラフィクベースのしきい値のテストについて、評価者は、TOE に接続するため、SSH クライアントを利用しなければならない(shall)、また評価者は送信されたトラフィクがしきい値に達するまで、アクティブな SSH セション内の TOE から及び TOE へのデータを送信しなければならない(shall)。送信されたトラフィクとは、送信と受信トラフィクからなる合計トラフィクである。

455 評価者は、許可されたしきい値より多いデータが SSH セション内で送信されたこと、及び対応する監査事象が TOE によって生成されたことを検証しなければならない(shall)。

456 テストは、1 ギガバイトの転送されたトラフィクの最大許可値で設定されたし

きい値を用いて実行される必要は必ずしもないが、テストで利用される値は、1 ギガバイトを超えてはならない(shall not)。評価者は、鍵変更が TOE によって開始されたこと及び TOE へ接続される SSH クライアントによって開始されていないことを保証する必要がある。

457 SFR を満たすために TOE によってチェックされるような 1 つ以上のしきい値が設定可能な場合、評価者は、そのしきい値がガイダンス証拠資料に記述されたとおり設定可能であることを検証する必要がある、または評価者は、しきい値の改変がセキュリティ管理者に限定されることをテストする必要がある(FMT_MOF.1/Functions によって要求されるとおり)。

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

4.1.9.1 TSS

FCS_TLSC_EXT.1.1

458 評価者は、サポートされる暗号スイートが規定されることを保証するため、TSS における本プロトコルの実装の記述をチェックしなければならない(shall)。評価者は、規定される暗号スイートが本コンポーネントで列挙されたものを含むことを保証するため、TSS をチェックしなければならない(shall)。

FCS_TLSC_EXT.1.2

459 評価者は、どの種別の参照識別子がサポートされるか (例、アプリケーション特有の Subject Alternative Name) 及び IP アドレスとワイルドカードがサポートされるかどうかを含めて、管理者／アプリケーション設定される参照識別子からすべての参照識別子をクライアントが確立する方法について TSS に記述されることを保証しなければならない(shall)。評価者は、この記述に TOE によって証明書ピンニングがサポートされるか、または利用されるかどうか、及びその方法が識別されていることを保証しなければならない(shall)。

460 FPT_ITT.1 について、分散型 TOE のコンポーネント間で TLS チャネルが利用されているような場合、利用者によって確立される参照識別子を持つための要件は緩和され、その識別子は、「ゲートキーパー」探索プロセスを通して確立されてもよいことに留意されたい。TSS には、探索プロセスについて記述されるべきであり、参照識別子が「参加している」コンポーネントへ供給される方法について強調するべきである(should)。

FCS_TLSC_EXT.1.4

461 評価者は、Supported Elliptic Curves Extension について、そして要求された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、のいずれかであるかについて、TSS に記述されていることを検証しなければならない(shall)。

4.1.9.2 ガイダンス証拠資料

FCS_TLSC_EXT.1.1

462 また評価者は、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するため、ガイダンス証拠資料をチェックしなければならない(shall)。

FCS_TLSC_EXT.1.2

463 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(shall)。

FCS_TLSC_EXT.1.4

464 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(shall)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(shall)。

4.1.9.3 テスト

FCS_TLSC_EXT.1.1

465 テスト 1：評価者は、本要件で規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(shall)。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観測すれば十分であり、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クの特徴を検査する必要はない。

466 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(shall)。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(should)。

467 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合致しないサーバ証明書を TLS 接続で送信しなければならない(shall) (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(shall)。

468 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(shall)。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。

469 テスト 5：評価者は、トラフィクに以下の改変を行う：

a) Server Hello 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 06 の 2 バイトによって表現される 1.5) 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) Server Hello 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、Server Key Exchange 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) Server Hello 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、Client Hello 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 Server Hello 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(shall)。

d) DHE または ECDH を用いる場合は、サーバの 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、クライアントが Server Key Exchange の受信後に接続を拒否することを検証する。このテストは RSA 鍵交換を用いる暗号スイートには適用しない。もし TOE が TLS と共に RSA 鍵交換のみをサポートする場合は、このテストは省略されなければならない(shall)。

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) サーバが 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

470 FPT_ITT.1 について、分散型 TOE のコンポーネント間で TLS チャネルが利用されている場合、利用者によって確立される参照識別子を持つための要件は緩和され、識別子は、「ゲートキーパー」探索プロセスを通して確立されてもよいことに留意されたい。

471 評価者は、AGD ガイダンスに従って参照識別子を設定し、TLS 接続の間に以下のテストを実行しなければならない(shall)：

a) テスト 1: 評価者は、参照識別子に合致する識別子を Subject Alternative Name (SAN) にも Common Name (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(shall)。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(shall)。

b) テスト 2：評価者は、参照識別子に合致する CN を含み、SAN Extension を含むが、参照識別子に合致する識別子を SAN に含まないサーバ証明書を提示しなければならない(shall)。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(shall)。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(shall)。

c) テスト 3：評価者は、参照識別子に合致する CN を含み、SAN Extension を含まないサーバ証明書を提示しなければならない(shall)。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(shall)。

d) テスト 4：評価者は、参照識別子に合致しない CN を含むが、SAN には合致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(shall)。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(shall)。

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実行しなければならない(shall)：

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(shall)。

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(shall)。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(shall)。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(shall)。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(shall)。

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(shall)。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(shall)。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(shall)。

g) テスト 7: [条件付き] ピンニングされた証明書がサポートされている場合、評価者はピンニングされた証明書に合致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(shall)。

FCS_TLSC_EXT.1.3

472 テスト 1 : 評価者は、有効な証明書パスのない証明書を利用すると、その機能が失敗することを実証しなければならない(shall)。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(shall)。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(shall)。

FCS_TLSC_EXT.1.4

473 テスト 1 : ECDHE 暗号を用いる場合、評価者は、サポートされない曲線 (例えば P-192) を用いて TLS 接続の間に ECDHE key exchange を行うようサーバを構成しなければならず(shall)、そして TOE がサーバの Key Exchange 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(shall)。

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

4.1.10.1 TSS

FCS_TLSC_EXT.2.1

474 評価者は、サポートされる暗号スイートが規定されることを保証するため、TSS における本プロトコルの実装の記述をチェックしなければならない(shall)。評価者は、規定される暗号スイートが本コンポーネントで列挙されたものを含むことを保証するため、TSS をチェックしなければならない(shall)。

FCS_TLSC_EXT.2.2

475 評価者は、どの種別の参照識別子がサポートされるか (例、アプリケーション特有の Subject Alternative Name) 及び IP アドレスとワイルドカードがサポートされるかどうかを含めて、管理者／アプリケーション設定される参照識別子からすべての参照識別子をクライアントが確立する方法について TSS に記述されることを保証しなければならない(shall)。評価者は、この記述に TOE によって

証明書ピンニングがサポートされるか、または利用されるかどうか、及びその方法が識別されていることを保証しなければならない(shall)。

FCS_TLSC_EXT.2.4

476 評価者は、Supported Elliptic Curves Extension について、そして要求された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、のいずれであるかについて、TSS に記述されていることを検証しなければならない(shall)。

FCS_TLSC_EXT.2.5

477 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(shall)。

4.1.10.2 ガイダンス証拠資料

FCS_TLSC_EXT.2.1

478 また評価者は、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するため、ガイダンス証拠資料をチェックしなければならない(shall)。

FCS_TLSC_EXT.2.2

479 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(shall)。

FCS_TLSC_EXT.2.4

480 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(shall)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(shall)。

FCS_TLSC_EXT.2.5

481 X.509v3 証明書を用いる相互認証が利用されることを TSS が示す場合、評価者は、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(shall)。

4.1.10.3 テスト

FCS_TLSC_EXT.2.1

482 テスト 1：評価者は、本要件で規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(shall)。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観測すれば十分であり、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クの特徴を検査する必要はない。

483 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(shall)。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(should)。

484 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合致しないサーバ証明書を TLS 接続の間に送信しなければならない(shall) (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 (shall) 。

485 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(shall)。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。

486 テスト 5 : 評価者は、トラフィクに以下の改変を行う：

a) Server Hello 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 06 の 2 バイトによって表現される 1.5) 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) Server Hello 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、Server Key Exchange 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) Server Hello 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、Client Hello 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 Server Hello 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(shall)。

d) DHE または ECDH を用いる場合は、サーバの 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、クライアントが Server Key Exchange の受信後に接続を拒否することを検証する。このテストは RSA 鍵交換を用いる暗号スイートには適用しない。もし TOE が TLS と共に RSA 鍵交換のみをサポートする場合は、このテストは省略されなければならない(shall)。

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) サーバが 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

487 評価者は、AGD ガイダンスに従って参照識別子を設定し、TLS 接続の間に以下のテストを実行しなければならない(shall) :

a) テスト 1 : 評価者は、参照識別子に合致する識別子を Subject Alternative Name (SAN) にも Common Name (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 (shall)。

b) テスト 2：評価者は、参照識別子に合致する CN を含み、SAN Extension を含むが、参照識別子に合致する識別子を SAN に含まないサーバ証明書を提示しなければならない(shall)。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(shall)。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(shall)。

c) テスト 3：評価者は、参照識別子に合致する CN を含み、SAN Extension を含まないサーバ証明書を提示しなければならない(shall)。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(shall)。

d) テスト 4：評価者は、参照識別子に合致しない CN を含むが、SAN には合致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(shall)。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(shall)。

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実行しなければならない(shall)：

   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(shall)。

   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(shall)。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(shall)。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(shall)。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(shall)。

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(shall)。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(shall)。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(shall)。

g) テスト 7： [条件付き] ピンニングされた証明書がサポートされている場合、評価者はピンニングされた証明書に合致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(shall)。

FCS_TLSC_EXT.2.3

488 テスト 1：評価者は、有効な証明書パスのない証明書を利用すると、その機能が失敗することを実証しなければならない(shall)。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(shall)。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(shall)。

FCS_TLSC_EXT.2.4

489 テスト 1：DHE または ECDH を用いる場合、評価者は、サポートされない曲線 (例えば P-192) を用いて TLS 接続の間に ECDHE 鍵交換を行うようサーバを構成しなければならず(shall)、そして TOE がサーバの Key Exchange 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(shall)。

FCS_TLSC_EXT.2.5

490 テスト 1：評価者は、トラフィクに以下の改変を行わなければならない(shall)：

a) 相互認証を要求するようにサーバを設定し、次にサーバの Certificate Request 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(must not)。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(shall)。

4.1.11 FCS_TLSS_EXT.1 拡張：TLS サーバプロトコル

4.1.11.1 TSS

FCS_TLSS_EXT.1.1

491 評価者は、サポートされる暗号スイートが規定されることを保証するため、TSS における本プロトコル実装の記述をチェックしなければならない(shall)。評価者は、規定された暗号スイートが本コンポーネントで列挙されたものと同一であることを保証するため、TSS をチェックしなければならない(shall)。

FCS_TLSS_EXT.1.2

492 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(shall)。

FCS_TLSS_EXT.1.3

493 評価者は、server Key Exchange 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(shall)。

4.1.11.2 ガイダンス証拠資料

FCS_TLSS_EXT.1.1

494 評価者は、TLS が TSS の記述に適合するように、TOE の設定に関する指示 (例えば、TOE によって公告される暗号スイートのセットが要件を満たすように制限されなければならない(have to)かもしれない) が含まれることを保証するため、ガイダンス証拠資料をチェックしなければならない(shall)。

FCS_TLSS_EXT.1.2

495 評価者は、本要件を満たすために必要なあらゆる設定が AGD ガイダンスに含まれなければならない(must)ことを検証しなければならない(shall)。

FCS_TLSS_EXT.1.3

496 評価者は、本要件を満たすために必要なあらゆる設定が AGD ガイダンスに含まれなければならない(must)ことを検証しなければならない(shall)。

4.1.11.3 テスト

FCS_TLSS_EXT.1.1

497 テスト 1 : 評価者は、本要件で規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(shall)。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観測すれば十分であり、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クの特徴を検査する必要はない。

498 テスト 2 : 評価者は、サーバの ST の暗号スイートを全く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 (shall) 。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(shall)。

499 テスト 3 : 評価者は、サーバ選択された暗号スイートと合致しないような TLS 接続において key exchange メッセージを送信するためにクライアントを利用しなければならない(shall) (例えば、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートを利用中に ECDSA key exchange を送信する、または ECDSA 暗号スイートの 1 つを利用中に RSA key exchange を送信する。) 評価者は、key exchange メッセージの受信後に、TOE が接続を切断することを検証しなければならない (shall) 。

500 テスト 4 : 評価者は、トラフィクに対して次の改変を実行しなければならない (shall) :

a) 撤回された

b) 撤回された

c) Client Finished ハンドシェイクメッセージにおける 1 バイトを改変し、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 を生成した後、以前のテストからのセション識別子を持つ 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意味不明の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

501 評価者は、SFR におけるすべての必須及び選択されたプロトコルバージョン(例、テストクライアントにおけるプロトコルバージョンの列挙によって)についての接続を要求するような Client Hello を送信し、サーバがそれぞれの試行に対して、接続を拒否することを検証しなければならない(shall)。

FCS_TLSS_EXT.1.3

502 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(shall)。(長さが、設定された曲線に期待される長さと一致することを決定すれば十分である。) 評価

者はこのテストを、サポートされる各 NIST 楕円曲線とサポートされる各 Diffie-Hellman 鍵長について、繰り返さなければならない (shall) 。

503 評価者は、FCS_TLSS_EXT.1.3 で選択されるとおり、それぞれの主張されたパラメタ(RSA 鍵長、Diffie-Hellman パラメタ、サポートされた曲線)を用いて、主張された各鍵確立プロトコル(RSA、DH、ECDHE)を用いて、接続確立を試行しなければならない(shall)。例えば、RSA 鍵長が主張された長さと合致することの決定は、本テストを満たすことで十分である。評価者は、サポートされるそれぞれのパラメタの組み合わせがテストされることを保証しなければならない(shall)。

504 本テストがその他のテストアクティビティと併せて達成可能であることに留意されたい。

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

4.1.12.1 TSS

FCS_TLSS_EXT.2.1

505 評価者は、サポートされる暗号スイートが規定されることを保証するため、TSS における本プロトコル実装の記述をチェックしなければならない(shall)。評価者は、規定された暗号スイートが本コンポーネントで列挙されたものと同一であることを保証するため、TSS をチェックしなければならない(shall)。

FCS_TLSS_EXT.2.2

506 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(shall)。

FCS_TLSS_EXT.2.3

507 評価者は、server Key Exchange 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(shall)。

FCS_TLSS_EXT.2.4 及び FCS_TLSS_EXT.2.5

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

FCS_TLSS_EXT.2.6

509 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(shall)。

4.1.12.2 ガイダンス証拠資料

FCS_TLSS_EXT.2.1

510 評価者は、TLS が TSS の記述に適合するように、TOE の設定に関する指示 (例えば、TOE によって公告される暗号スイートのセットが要件を満たすように制限されなければならない(have to)かもしれない) が含まれることを保証するため、ガイダンス証拠資料をチェックしなければならない(shall)。

FCS_TLSS_EXT.2.2

511 評価者は、本要件を満たすために必要なあらゆる設定が AGD ガイダンスに含まれなければならない(must)ことを検証しなければならない(shall)。

FCS_TLSS_EXT.2.3

512 評価者は、本要件を満たすために必要なあらゆる設定が AGD ガイダンスに含まれなければならない(must)ことを検証しなければならない(shall)。

FCS_TLSS_EXT.2.4 及び FCS_TLSS_EXT.2.5

513 X.509v3 証明書を用いる相互認証が利用されることを TSS が示す場合、評価者は、TLS 相互認証用のクライアント側証明書を設定するための指示が AGD ガイダンスに含まれることを検証しなければならない(shall)。

FCS_TLSS_EXT.2.6

514 DN が Domain Name または IP アドレス、利用者名、または電子メールアドレスと自動的に比較されない場合、評価者は、その接続用に期待される 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(shall)。

4.1.12.3 テスト

FCS_TLSS_EXT.2.1

515 テスト 1：評価者は、本要件で規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(shall)。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観測すれば十分であり、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クの特徴を検査する必要はない。

516 テスト 2：評価者は、サーバの ST の暗号スイートを全く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 (shall) 。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(shall)。

517 テスト 3：評価者は、サーバ選択された暗号スイートと合致しないような TLS 接続において key exchange メッセージを送信するためにクライアントを利用しなければならない(shall) (例えば、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートを利用中に ECDHE key exchange を送信する、または ECDSA 暗号スイートの 1 つを利用中に RSA key exchange を送信する。) 評価者は、key exchange メッセージの受信後に、TOE が接続を切断することを検証しなければならない (shall) 。

518 テスト 4：評価者は、トラフィクに対して、次の改変を実行しなければならない (shall)：

a) 撤回された

b) 撤回された

c) Client Finished ハンドシェイクメッセージにおける 1 バイトを改変し、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 を生成した後、以前のテストからのセション識別子を持つ 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意味不明の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

519 評価者は、SFR におけるすべての必須及び選択されたプロトコルバージョン(例、テストクライアントにおけるプロトコルバージョンの列挙によって)についての接続を要求するような Client Hello を送信し、サーバがそれぞれの試行に対して、接続を拒否することを検証しなければならない(shall)。

FCS_TLSS_EXT.2.3

520 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なければならない(shall)。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(shall)。(鍵長が設定された曲線に期待される鍵長と合致することを決定すれば十分である。) 評価者は、サポートされる各 NIST 楕円曲線とサポートされる各 Diffie-Hellman 鍵長について本テストを繰り返さなければならない (shall) 。

521 評価者は、FCS_TLSS_EXT.1.3 で選択されるとおり、それぞれの主張されたパラメタ(RSA 鍵長、Diffie-Hellman パラメタ、サポートされた曲線)を用いて、主張された各鍵確立プロトコル(RSA、DH、ECDHE)を用いて、接続確立を試行しなければならない(shall)。例えば、RSA 鍵長が主張された長さと合致することの決定は、本テストを満たすことで十分である。評価者は、サポートされるそれぞれのパラメタの組み合わせがテストされることを保証しなければならない(shall)。

522 本テストがその他のテストアクティビティと併せて達成可能であることに留意されたい。

FCS_TLSS_EXT.2.4 及び FCS_TLSS_EXT.2.5

523 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(shall)、また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(shall)。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(shall)。

524 テスト 2：評価者は、クライアントの証明書によって利用される supported_signature_algorithm なしに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(shall)。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(shall)。

525 テスト 3：評価者は、有効な証明書パスのない証明書の利用がその機能が失敗をもたらすことを実証しなければならない(shall)。管理ガイダンスを用いて、評価者は次に、その機能で利用さ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(shall)。評価者は次に、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(shall)。

526 テスト 4 : 評価者は、サーバの証明書要求メッセージにおいて、認証局 (ルート CA または中間 CA のいずれか) の 1 つと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(shall)。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(shall)。

527 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(shall)。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(shall)、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(shall)。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(should)。

528 テスト 6 : 評価者は、トラフィクに以下の改変を行わなければならない(shall) :

a) 相互認証を要求するようにサーバを設定し、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(shall)。

b) 相互認証を要求するようにサーバを設定し、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(shall)。

FCS_TLSS_EXT.2.6

529 評価者は、期待される識別子と合致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(shall)。

4.2 識別と認証 (FIA)

4.2.1 FIA_X509_EXT.1/Rev X.509 証明書有効性確認

4.2.1.1 TSS

530 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、及び TOE によってサポートされないような、(FIA_X509_EXT.1.1 における) extendedKeyUsage フィールドのあらゆる規則が TSS に識別されていることを保証しなければならない(shall) (即ち、ST において、それらは自明に満たされることが主張されているような)。認証ステップで証明書が利用されるとき、及び高信頼アップデートの実行時 (選択された場合) に、失効チェックが実行されることが想定されている。証明書がデバイスにロードされるときにのみに X.509 証明書の状態を検証するのでは十分ではない。必ずしも電源投入時の自己テスト中に X.509 証明書の失効状態を検証する必要はない(自己テスト用に X.509 証明書を利用するためのオプションが選択される場合)。

4.2.1.2 テスト

531 評価者は、証明書が認証ステップで利用されるとき、または高信頼アップデートの実行時(FPT_TUD_EXT.2 が選択される場合)に、証明書の有効性のチェックが実行されることを実証しなければならない(shall)。証明書がデバイスにロードされるときにのみに X.509 証明書の状態を検証するのでは十分ではない。電源投入時の自己テスト中に X.509 証明書の失効状態を検証する必要はない(自己テスト用に X.509 証明書を利用するためのオプションが選択される場合)。評価者は、FIA_X509_EXT.1.1/Rev について以下のテストを実行しなければならない

(shall) :

a) テスト 1a : 評価者は、本機能において利用されるべき証明書を検証する必要があるものとして、証明書の有効なチェイン (信頼された CA 証明書で終端) をロードしなければならない(shall)、また、本機能が成功することを実証するためにこのチェインを利用しなければならない(shall)。

テスト 1b : 評価者は、チェインにおける証明書の 1 つ (即ち、ルート CA 証明書またはその他の中間の証明書、ただし、エンドエンティティの証明書でないもの) 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(shall)。

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により、その機能の失敗をもたらすことを実証しなければならない(shall)。

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 ー 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(shall) ; 両方とも選択されている場合、それぞれの方法についてテストが実行されなければならない(shall)。評価者はピア証明書の失効及びピア中間 CA 証明書の失効をテストしなければならない(shall) 即ち、中間 CA 証明書は、ルート CA によって失効されるべきである(should)。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の機能が成功することを保証しなければならない(shall)。次に評価者は、その証明書がもはや有効ではないときに、証明書有効性確認の機能が失敗することを保証するため、(選択において選ばれたそれぞれの方法について) 失効した証明書を用いてテストを試行する。

d) テスト 4 : OCSP が選択される場合、評価者は、OCSP 署名目的を持たないような証明書を提示するため、OCSP サーバを設定するかまたは中間者ツールを利用し、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(shall)。CRL が選択される場合、評価者は、cRLsign key usage ビットがセットされていない証明書を持つ CRL に CA が署名するように設定し、その 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 (shall)。

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 (shall)。(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 (shall)。(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(shall)。(証明書のハッシュが検証されないこと。)

532 評価者は、FIA_X509_EXT.1.2/Rev に対する次のテストを実行しなければならない(shall)。記述されるテストは、FIA_X509_EXT.2.1/Rev 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併せて実行されなければならない(must)。TOE によってサポートされない(即ち、それらが自明に満たされることをゆえに ST が主張している)ような、(FIA_X509_EXT.1.1 における) extendedKeyUsage シ

ールドに対する任意の規則を TSS が識別する場合、対応する extendedKeyUsage 規則のテストは、省略されてもよい。

533 評価者は、少なくとも 3 つの証明書のチェインを作成しなければならない(shall) : テストされるノード証明書、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 Extension が含まれないような、証明書パスを構築しなければならない(shall)。この証明書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 Extension における cA フラグが FALSE にセットされているような、証明書パスを構築しなければならない(shall)。この証明書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 Extension における cA フラグが TRUE にセットされているような、証明書パスを構築しなければならない(shall)。この証明書パスの検証は成功する。

534 評価者は、それぞれの証明書の用途について、これらのテストを繰り返さなければならない(shall)。従って、例えば、TLS 接続用の証明書の用途は、高信頼アップデート用の証明書の用途は異なるので、これらの用途の両方についてテストされるだろう。しかし、FTP_ITC.1 及び FTP_TRP.1/Admin におけるそれぞれの別々の TLS チャネル用のテストを繰り返す必要はない(そのチャネルが TLS の別々の実装を利用しない限り)。

4.2.2 FIA_X509_EXT.2 X.509 証明書認証

4.2.2.1 TSS

535 評価者は、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の管理者ガイダンスにおける必要な指示が TSS に記述されていることを保証するため、TSS をチェックしなければならない(shall)。

536 評価者は、高信頼チャネルの確立で利用される証明書の有効性チェック中に接続が確立できないときの TOE のふるまいが TSS に記述されていることを確認するため、TSS を検査しなければならない(shall)。評価者は、高信頼チャネル間のあらゆる相違について記述されていることを検証しなければならない(shall)。管理者がデフォルトのアクションを規定できるという要件が存在する場合、評価者は、この設定アクションが実行される方法に関する指示がガイダンス証拠資料に含まれていることを保証しなければならない(shall)。

4.2.2.2 テスト

537 評価者は、それぞれの高信頼チャネルに対して、次のテストを実行しなければならない(shall) :

538 評価者は、有効な証明書の利用が TOE 以外の IT エンティティとの通信によって少なくとも一部の証明書有効性チェックが実行されることを要求することを実証しなければならない(shall)。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実行されることを観測しなければならない(shall)。選択されたアクションが管理者設定可能である場合、評価者は、サポートされるすべての管理者設定可能なオ

プションが文書化されているようなやり方でふるまうことを決定するため、ガイダンス証拠資料に従わなければならない(shall)。

4.2.3 FIA_X509_EXT.3 拡張：X509 証明書要求

4.2.3.1 TSS

539 ST 作成者が「デバイス固有情報」を選択する場合、評価者は、証明書要求で利用さ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(shall)。

4.2.3.2 ガイダンス証拠資料

540 評価者は、証明書要求メッセージの生成を含めて、CA からの証明書要求に関する指示がガイダンス証拠資料に含まれることを保証するため、チェックしなければならない(shall)。ST 作成者が「Common Name」、「Organization」、「Organizational Unit」、または「Country」を選択する場合、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(shall)。

4.2.3.3 テスト

541 評価者は、次のテストを実行しなければならない(shall)：

a) テスト 1：評価者は、証明書要求メッセージを TOE に生成させるため、ガイダンス証拠資料を利用しなければならない(shall)。評価者は、生成されたメッセージをキャプチャし、規定される形式に適合することを保証しなければならない(shall)。評価者は、必要とされるあらゆる利用者入力の情報を含めて、公開鍵とその他の要求される情報が証明書要求により提供されることを確認しなければならない(shall)。

b) テスト 2：評価者は、有効な証明パスを持たない証明書応答メッセージの検証がその機能の失敗をもたらすことを実証しなければならない(shall)。次に評価者は、証明書応答メッセージの検証を必要とされる信頼済み CA として 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(shall)。

4.3 TSF の保護 (FPT)

4.3.1 FPT_TST_EXT.2 証明書ベースの自己テスト

4.3.1.1 テスト

542 評価者は、FIA_X509_EXT.1 に従って証明書有効性確認及び extendedKeyUsage における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(shall)。

543 評価者は、無効な証明書を用いて自己テストを実行しなければならない(shall)。このテストは失敗すべきである(should)。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(shall)。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(shall)。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併せて行われる。

544 電源投入中に X.509 証明書の失効状態を検証する必要はない。

4.3.2 FPT_TUD_EXT.2 証明書ベースの高信頼アップデート

4.3.2.1 TSS

545 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(shall)。

546 TSS には、失効チェックが実行される時点について記述されなければならない(shall)。高信頼アップデート実行時の証明書が利用されるときに失効チェックが実行されることが想定される。証明書がデバイスにロードされるときのみ X.509 証明書の状態を検証するだけでは不十分である。

4.3.2.2 ガイダンス証拠資料

547 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証拠資料に記述されていることを検証しなければならない(shall)。この記述は、TSS 中の記述と対応していなければならない(shall)。

4.3.2.3 テスト

548 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(shall)。

549 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(shall)。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(shall)。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(shall)。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 及びガイダンス証拠資料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(shall)。本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併せて行われる。

550 評価者は、高信頼アップデート実行時の証明書が利用されるときに証明書の有効性チェックが実行されることを実証しなければならない(shall)。証明書がデバイスにロードされるときのみ X.509 証明書の状態を検証するだけでは不十分である。

4.4 セキュリティ管理 (FMT)

4.4.1 FMT_MOF.1/AutoUpdate

4.4.1.1 TSS

551 分散型 TOE について、チャプター2.4.1.1 を参照。分散型以外の TOE については、具体的な要件はない。

4.4.1.2 テスト

552 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 (管理者特権のない利用者としての認証によって、または利用者認証なしに) アップデートの自動チェックまたは自動アップデート (TOE によってサポートされるいずれか) の有効化及び無効化を試行しなければならない(shall)。アップデートの自動チェックの有効化／無効化の試行は、失敗するべきである(should)。実装に従って、セキュリティ管理者以外の利用者が誰も定義されず、利用者認証なしに、利用者がアップデートの自動チェックの有効化／無効化の試行が実行可能であるようなポイントまでたどり着けないに違いない。そのような場合に、アクセス制御メカニズムがセキュリティ管理者としての認証なし到達可能であるようなステップまでの実行を防止することが実証されなければならない(shall)。

553 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 (TOE によってサポートされるいずれか) の有効化と無効化を試行しなければならない(shall)。アップデートの自動チェックの有効化／無効化の試行は、成功すべきである(should)。

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

4.4.2.1 TSS

554 分散型 TOE について、チャプター2.4.1.1 を参照。分散型以外の TOE については、具体的な要件はない。

4.4.2.2 テスト

555 テスト 1 (2 番目の選択から「外部 IT エンティティへの監査データの送信」が、最初の選択での「のふるまいを改変」と共に、選択される場合) : 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 (管理者特権のない利用者としての認証によって、または全く利用者認証なしに) 外部 IT エンティティへ監査データの送信用の送信プロトコルを設定するためのセキュリティ関連のすべてのパラメタの改変を試行しなければならない(shall)。事前認証なしでのパラメタ改変の試行は失敗すべきである(should)。実装に従って、セキュリティ管理者以外の利用者が誰も定義されず、利用者認証なしに、利用者がセキュリティ関連のパラメタ改変の試行が実行可能であるようなポイントまでたどり着けないに違いない。そのような場合に、アクセス制御メカニズムがセキュリティ管理者としての認証なし到達可能であるようなステップまでの実行を防止することが実証されなければならない(shall)。

556 テスト 2 (2 番目の選択から「外部 IT エンティティへの監査データの送信」が、最初の選択での「のふるまいを改変」と共に、選択される場合) : 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、外部 IT エンティティへ監査データの送信用の送信プロトコルを設定するためのセキュリティ関連のすべてのパラメタの改変を試行しなければならない(shall)。改変の影響は確認されるべ

きである(should)。

557 評価者は、外部 IT エンティティへの監査データの送信用の送信プロトコルの設定のために、セキュリティ関連のすべてのパラメタの、必ずしもすべての可能性のある値をテストする必要はないが、パラメタ毎に少なくとも 1 つの許可された値についてはテストする必要がある。

558 テスト 1 (2 番目の選択から「監査データの取り扱い」が、最初の選択での「のふるまいを改変」と共に、選択される場合) : 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 (管理者特権のない利用者としての認証によって、または全く利用者認証なしに) 監査データの取り扱いを設定するためのセキュリティ関連のすべてのパラメタの改変を試行しなければならない(shall)。事前認証なしでのパラメタ改変の試行は失敗すべきである(should)。実装に従って、セキュリティ管理者以外の利用者が誰も定義されず、利用者認証なしに、利用者が、試行が実行可能であるようなポイントまでたどり着けないに違いない。そのような場合に、アクセス制御メカニズムがセキュリティ管理者としての認証なし到達可能であるようなステップまでの実行を防止することが実証されなければならない(shall)。用語「監査データの取り扱い」は、SFR の、FAU_STG_EXT.1.2、FAU_STG_EXT.1.3 及び FAU_STG_EXT.2/LocSpace における選択及び割付のための異なる選択肢を参照する。

559 テスト 2 (2 番目の選択から「監査データの取り扱い」が、最初の選択での「のふるまいを改変」と共に、選択される場合) : 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、監査データの取り扱いを設定するためのセキュリティ関連のすべてのパラメタの改変を試行しなければならない(shall)。改変の影響は確認されるべきである(should)。用語「監査データの取り扱い」は、SFR の FAU_STG_EXT.1.2、FAU_STG_EXT.1.3 及び FAU_STG_EXT.2/LocSpace における選択及び割付のための異なる選択肢を参照する。

560 評価者は、監査データの取り扱いの設定のためのセキュリティ関連のすべてのパラメタの必ずしもすべての可能性のある値をテストする必要はないが、少なくとも 1 つのパラメタ毎に許可された値についてはテストする必要がある。

561 テスト 1 (2 番目の選択から「ローカル監査格納領域が満杯のときの監査機能」が、最初の選択での「のふるまいを改変」と共に、選択される場合) : 評価者は、ローカル監査格納領域が満杯のときに、セキュリティ管理者としての事前認証なしに (管理者特権のない利用者としての認証によって、または全く利用者認証なしに) そのふるまいの改変を試行しなければならない(shall)。この試行は失敗するべきである(should)。実装に従って、セキュリティ管理者以外の利用者が誰も定義されず、利用者認証なしに、利用者が、試行が実行可能であるようなポイントまでたどり着けないに違いない。そのような場合に、アクセス制御メカニズムがセキュリティ管理者としての認証なし到達可能であるようなステップまでの実行を防止することが実証されなければならない(shall)。

562 テスト 2 (2 番目の選択から「ローカル監査格納領域が満杯のときの監査機能」が、最初の選択での「のふるまいを改変」と共に、選択される場合) : 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、ローカル監査格納領域が満杯のときに、そのふるまいの改変を試行しなければならない(shall)。変更の影響は検証されるべきである(should)。

563 評価者はローカル監査格納領域が満杯のとき、必ずしもすべての可能性のある値をテストする必要はないが、少なくとも 1 つのふるまい毎に許可された値の

間の変更についてはテストする必要がある。

564 テスト 3 (最初の選択で「のふるまいを決定」が、2 番目の選択でいずれかの選択肢と共に、選択される場合) : 評価者は、セキュリティ管理者としての事前認証なしに (管理者特権のない利用者としての認証によって、または全く利用者認証なしに) 2 番目の選択から選ばれたすべての選択肢のふるまいの決定を試行しなければならない(shall)。これは、1 つのテストまたは別々のテストで行うことが可能である。管理者認証なしに選択された機能のふるまいを決定する試行は、失敗しなければならない(shall)。実装に従って、セキュリティ管理者以外の利用者が誰も定義されず、利用者認証なしに、利用者が、試行が実行可能であるようなポイントまでたどり着けないに違いない。そのような場合に、アクセス制御メカニズムがセキュリティ管理者としての認証なし到達可能であるようなステップまでの実行を防止することが実証されなければならない(shall)。

565 テスト 4 (最初の選択で「のふるまいを決定」が、2 番目の選択でいずれかの選択肢と共に、選択される場合) : 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、2 番目の選択から選ばれたすべての選択肢のふるまいの決定を試行しなければならない(shall)。これは、1 つのテストまたは別々のテストで行うことが可能である。管理者認証を行った上での選択された機能のふるまいを決定する試行は、成功しなければならない(shall)。

5 SAR の評価アクティビティ

566 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(SAR) を規定する (上記のセクション 1.1 を参照)。セクション 2 (SFR の評価アクティビティ)、セクション 3 (オプション要件の評価アクティビティ)、セクション 4 (選択ベース要件の評価アクティビティ) における EA (評価アクティビティ) は、より一般的な CEM 保証要件についての特定技術分野の TOE に適用される解釈である。

567 本セクションでは、cPP に含まれるそれぞれの SAR が列挙され、1 つの SFR にも対応しないような EA (評価アクティビティ) ここに取り込まれるか、CEM への参照がなされている、また評価者は、CEM ワークユニットを実行すると期待される。

5.1 ASE：セキュリティターゲット評価

5.1.1 一般的な ASE

568 セキュリティターゲットの評価中、評価者は、CEM に存在するワークユニットを実行する。さらに、評価者は、セクション 2 (SFR の評価アクティビティ)で規定される EA を ST における TSS の内容が満たすことを保証する。

5.1.2 分散型 TOE の TOE 要約仕様 (ASE_TSS.1)

569 分散型 TOE について、「すべて」と格付けされる SFR のみがすべての TOE 部分によって満たされなければならない(have to)。「1 つ」または「機能依存」として格付けされる SFR のみが、1 つまたはいくつかの TOE 部分によって、それぞれ満たされなければならない(have to)。全体としての分散型 TOE がすべての SFR を満たすことを確認するため、ASE_TSS.1 についての以下のアクションが ASE_TSS.1.1E の一部として実行されなければならない(have to)。

ASE_TSS.1 エレメント	評価者のアクション
ASE_TSS.1.1C	評価者は、どの TOE コンポーネントがそれぞれの SFR に寄与するか、またはどのように複数のコンポーネントが共同してそれぞれの SFR を満たすかについて決定するため、TSS を検査しなければならない(shall)。 評価者は、関連する SFR を満たすためにその十分制について検証しなければならない(shall)。これには、TOE が全体としてすべての SFR をカバーすること、及び監査されるために要求されるようなすべての機能がそれを実行するようなコンポーネントにかかわらず、実際に監査されることをチェックすることが含まれる。

570 分散型 TOE の場合の TSS についての追加の評価アクティビティがセクション B.4.1.1 で定義されていることに留意されたい。

5.2 ADV：開発

5.2.1 基本機能仕様 (ADV_FSP.1)

571 この保証コンポーネントの EA は、AGD 証拠資料に記述され、及び SFR に対応する TOE 要約仕様 (TSS) で識別されるかもしれないインタフェース(例、アプリケーションプログラミングインタフェース、コマンドラインインタフェース、グラフィカルユーザインタフェース、ネットワークインタフェース)を理解することに焦点を絞る。本証拠資料に対して実行されるべき具体的な評価者アクションは、セクション 2 のそれぞれの SFR について(関連する場合)、及びセクション 5 のその他の部分で AGD、ATE 及び AVA の SAR についての EA において識別される。

572 本セクション委存在する EA は、CEM ワークユニット ADV_FSP.1-1、ADV_FSP.1-2、ADV_FSP.1-3、及び ADV_FSP.1-5 に対処する。

573 EA は、それらが評価者による、より客観的で再現性のあるアクションとなるように、CEM ワークユニットを明確に言い換え、解釈を与えている。本 SD における EA は、評価者が一貫して、同等なアクションを実行することを保証することを意図している。

574 評価において本保証コンポーネントのために検査されるべき証拠資料は、ゆえにセキュリティターゲット、AGD 証拠資料、及び任意の本 cPP で必須の補足情報 : 追加の「機能仕様書」証拠資料は本 EA を満たすために一切必要ではない。評価される必要があるインタフェースは、それぞれの SFR について列挙された EA への参照によっても識別され、また特に CC 評価の目的で別のリストとしてよりもむしろ、セキュリティターゲット、AGD 証拠資料、及び本 cPP で定義された任意の必須の補足情報の文脈において識別される。それぞれの SFR についての EA の一部として、証拠資料要件及びそれらの評価の直接的な識別は、ADV_FSP.1.2D(ワークユニット ADV_FSP.1-4、ADV_FSP.1-6 および ADV_FSP.1-7)で要求されるトレースが本エレメントについて要求されることも意味する。

CEM ADV_FSP.1 ワークユニット	評価アクティビティ
ADV_FSP.1-1 評価者は、機能仕様が SFR 支援及びSFR 実施の各TSFI の目的を記述していることを決定するために、その仕様を***検査しなければならない***。	5.2.1.1 評価アクティビティ：*評価者は、セキュリティ関連として特定される各 TSFI についての目的及び使用方法が記述されていることを保証するため、インタフェース証拠資料を検査しなければならない。*
ADV_FSP.1-2 評価者は、SFR 支援及びSFR 実施の各TSFI の利用方法が記述されていることを決定するために、機能仕様を***検査しなければならない***。	5.2.1.2 評価アクティビティ：*評価者は、セキュリティ関連として特定される各 TSFI についての目的及び使用方法が記述されていることを保証するため、インタフェース証拠資料を検査しなければならない。*
ADV_FSP.1-3 評価者は、TSFI の提示がSFR 実施及びSFR 支援の各TSFI に関連するすべてのパラメタを識別していることを決定するために、その提示	5.2.1.3 評価アクティビティ：*評価者は、セキュリティ関連であると識別されるような各 TSFI についてのパラメタが識別され、記述されているこ*

を***検査しなければならない***。	*とを保証するため、インタフェース証拠資料をチェックしなければならない*。
ADV_FSP.1-4 評価者は、暗黙的にSFR 非干渉として分類されているインタフェースについて、その分類が正しいことを決定するために、開発者によって提供される根拠を***検査しなければならない***。	CEMのパラグラフ561：「このコンポーネントの残りのワークユニットで要求される分析を行うのに十分な証拠資料が開発者によって提供されていて、SFR 実施及びSFR 支援のインタフェースは明示的に識別されていない場合、このワークユニットは満たされているものとみなされるべきである。」ADV_FSP.1の残りのワークユニットがこれらのEAの完了で満たされるので、本ワークユニットは同様に満たされることに従う。
ADV_FSP.1-5 評価者は、追跡によってSFR が対応するTSFI にリンクされることを***チェックしなければならない***。	5.2.1.4 評価アクティビティ：*評価者は、SFR へのインタフェースのマッピングを作るため、インタフェース証拠資料を検査しなければならない*。
ADV_FSP.1-6 評価者は、機能仕様がSFR の完全な具体化であることを決定するために、その仕様を***検査しなければならない***。	セクション 2、及び適用可能であれば、セクション 3 と 4 における SFR と関係する EA は、セキュリティ機能が外部から見えるようなすべてのSFR(TSFI)がカバーされることを保証するために実行される。ゆえに、本ワークユニットの意図がカバーされる。
ADV_FSP.1-7 評価者は、機能仕様がSFR の正確な具体化であることを決定するために、その仕様を***検査しなければならない***。	セクション 2、及び適用可能であれば、セクション 3 と 4 における SFR と関係する EA は、セキュリティ機能が外部から見えるようなすべてのSFR(TSFI)が対処されること、及びSFR で取り込まれた利用に関してインタフェースの記述が正しいことを保証するために実行される。 ゆえに、本ワークユニットの意図がカバーされる。

表 1：ADV_FSP.1 CEM ワークユニットの評価アクティビティへのマッピング

5.2.1.1 評価アクティビティ：

575 *評価者は、セキュリティ関連として識別される各 TSFI についての目的及び利用方法が記述されていることを保証するため、インタフェース証拠資料を検査しなければならない(shall)*。

576 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、またはガイダンス証拠資料においてセキュリティポリシーを順守すると識別される (SFR で提示されるように) 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。

577 評価証拠として提供される TSFI のセットは、管理者ガイダンス及び利用者ガイダンスに含まれる。

5.2.1.2 評価アクティビティ

578 *評価者は、セキュリティ関連であると識別される各 TSFI についてのパラメタが識別され、記述されていることを保証するため、インタフェース証拠資料をチェックしなければならない (shall)。*

5.2.1.3 評価アクティビティ

579 *評価者は、セキュリティ関連であると識別される各 TSFI についてのパラメタが識別され、記述されていることを保証するため、インタフェース証拠資料をチェックしなければならない (shall)。*

580 評価者は、提供された証拠資料を用いて、まず識別し、次にそのインタフェースのテストに関連する EA を含めて、セクション 2 にある EA を実行するために、インタフェースの代表的なセットを検査する。

581 求められる機能を起動するために明示的に「マップ」されるようなインタフェースを持たないような SFR がいくつかあるかもしれないことに留意されるべきである(should)。例えば、乱数ビット列の生成、もはや不要である暗号鍵の破壊、またはセキュアな状態でない TSF、これらは SFR で規定されるかもしれない機能であるが、インタフェースによって起動されない。

582 しかし、不十分な設計及びインタフェース情報しか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。

5.3 AGD：ガイダンス文書

583 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 EA は伝統的な別個の AGD ファミリの下で記述されているが、開発者によって提供される証拠資料と AGD_OPE 及び AGD_PRE 要件との対応付けは、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。

584 分散型 TOE の場合のガイダンス証拠資料に対する追加の評価アクティビティは、セクション B.4.1.1 に定義されることに留意されたい。

5.3.1 利用者操作ガイダンス (AGD_OPE.1)

585 評価者は、SAR の AGD_OPE.1 に関連する CEM ワークユニットを実行する。ガイダンス証拠資料に関する具体的な要件及び EA は、(関連する場合) 各 SFR についての個別 EA で識別される。

586 さらに、評価者は、以下に規定された EA を実行すること。

5.3.1.1 評価アクティビティ：

587 *評価者は、操作ガイダンス証拠資料が、TOE の一部として (適宜) 管理者及び利用者へ配付されることを保証しなければならない(shall)、そのため管理者及び利用者が、評価される構成の確立と維持における証拠資料の存在と役割を周知されていることの合理的な保証が存在する。*

5.3.1.2 評価アクティビティ

588 *評価者は、操作ガイダンスが、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ついて提供されることを保証しなければならず(shall)、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(shall)。*

5.3.1.3 評価アクティビティ

589 *評価者は、操作ガイダンスに TOE の評価される構成に関連するあらゆる暗号エンジンの設定についての指示が含まれることを保証しなければならない(shall)。その他の暗号エンジンの利用は、TOE の CC 評価中に評価もテストもされなかったことを管理者に対して警告を与えなければならない(shall)。*

5.3.1.4 評価アクティビティ

590 *評価者は、操作ガイダンスが管理者に対してどのセキュリティ機能とインタフェースが EA によって評価及びテストされたかについて、明確化することを保証しなければならない(shall)。*

5.3.1.5 評価アクティビティ

591 さらに、評価者は、以下の要件もまた満たされることを保証しなければならない(shall)。

a) ガイダンス証拠資料には、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(shall)。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を、管理者へ提供しなければならない(shall)。

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(must)。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(shall)。

   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(should)。

   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、ガイダンス証拠資料は管理者に対して明確にしなければならない(shall)。

5.3.2 準備手続き (AGD_PRE.1)

592 評価者は、SAR の AGD_PRE.1 に関連する CEM ワークユニットを実行すること。準備の(訳注：設置に関する) 証拠資料についての具体的な要件及び EA は各 SFR の個別 EA において識別されている(また、関連する場合、EA のガイダンス証拠資料に取り込まれている)。

593 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る、ゆえに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。

594 さらに、評価者は、以下に規定された EA を実行すること。

5.3.2.1 評価アクティビティ

595 *評価者は、運用環境がセキュリティ機能(セキュリティターゲットで規定された運用環境のセキュリティ対策方針の要件を含む)をサポートするためにその役割を満たすことができることを管理者が検証する方法についての記述が準備手続きに含まれることを保証するため、準備手続きを検査しなければならない(shall)。*

596 証拠資料は、非形式的なスタイルであるべき(should)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(should)。

5.3.2.2 評価アクティビティ

597 *評価者は、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ついて準備手続きが提供されることを保証するため、準備手続きを検査しなければならない(shall)、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(shall)。*

5.3.2.3 評価アクティビティ

598 *評価者は、準備手続きに、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が含まれることを保証するため、準備手続きを検査しなければならない(shall)。*

5.3.2.4 評価アクティビティ

599 *評価者は、準備手続きに、製品及び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が含まれていることを保証するため、準備手続きを検査しなければならない(shall)。*

5.3.2.5 評価アクティビティ

600 さらに、評価者は、以下の要件についても満たされることを保証しなければならない(shall)。

601 準備手続きは以下を満たさなければならない(must)

a) 保護された管理機能を提供するための指示を含むこと；及び

b) それらに関連するデフォルト値を持つような TOE パスワードを識別すること、またそれらがどのように変更可能であるかについての指示が提供されなければならない(shall)。

5.4 ALC：ライフサイクルサポート

5.4.1 TOE のラベル付け (ALC_CMC.1)

602 TOE が提供され、一意の参照でラベル付けされていることを評価するとき、評価者は CEM で提示されるとおりワークユニットを実行すること。

5.4.2 TOE の CM 範囲 (ALC_CMS.1)

603 開発者の CM システムにおいて彼らの TOE のカバレージを評価するとき、評価者は、CEM で提示されるとおりワークユニットを実行すること。

5.5 ATE：テスト

5.5.1 独立テスト—適合 (ATE_IND.1)

604 テストで重視されるのは、SFR で規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。さらに、テストは、操作ガイダンス証拠資料が正しいことについての依存性と同様に、TSS に記述された機能を確認するために実行される。

605 評価者は、SAR の ATE_IND.1 に関連する CEM ワークユニットを実行すること。具体的なテスト要件と EA は、セクション 2.3 及び 4 でそれぞれの SFR について取り込まれている。

606 評価者は、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決定するとき、附属書 B を参考にすべきである(should)。

607 分散型 TOE の場合の評価者テストに関連する追加の評価アクティビティは、セクション B.4.3.1 で定義されることに留意されたい。

5.6 AVA：脆弱性評定

5.6.1 脆弱性調査 (AVA_VAN.1)

608 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、最小レベルの分析が定義可能であり、客観性と再現性(または少なくとも比較可能性)についての何らかの尺度が脆弱性分析処理に導入可能である。このような客観性と再現性を達成するために、評価者が良く定義されたアクティビティ集に従い、所見を

文書化し、他の人々がその議論を追うことができ、評価者の報告書における評価者として同じ結論へたどり着くことができる。これによって、異なる複数の評価機関が同じ種別の脆弱性を完全に識別し、または完全に同じ結論を得ることを保証しないが、そのやり方は最小レベルの分析とその分析の適用範囲を定義し、複数の評価機関によって実施されているような保証の尺度を複数の認証機関に提供する。

609 これらの目標を満たすため、AVA_VAN.1 の CEM ワークユニットの何らかの詳細化が必要とされる。以下の表は、AVA_VAN.1 の CEM ワークユニットのそれぞれについて、CEM ワークユニットが書かれたとおり実行されるべきである (should) か、または評価アクティビティによって明確化されるかを示している。明確化が提供される場合、明確化への参照が表において提供される。

610

CEM AVA_VAN.1 ワークユニット	評価アクティビティ
AVA_VAN.1-1 評価者は、テスト構成が ST に特定されたとおりに評価における構成と一貫していることを決定するために、TOE を***検査しなければならない***。	評価者は、規定されたとおりの CEM アクティビティを実行しなければならない(shall)。 CEM のパラグラフ 1418 で規定されたテスト資源の構成は、セクション A.1.4 で列挙されたツールに適用される。
AVA_VAN.1-2 評価者は、TOE が適切に設置され、定義された状態にあることを決定するために、その TOE を***検査しなければならない***。	評価者は、規定されたとおりの CEM アクティビティを実行しなければならない(shall)。
AVA_VAN.1-3 評価者は、TOE の潜在的脆弱性を識別するために、公開の場で利用できる情報源を***検査しなければならない***。	CEM ワークユニットをセクション A.1 で概説されたアクティビティに置き換える。
AVA_VAN.1-4 評価者は、ETR 内で、テストの候補となり、運用環境の TOE に適用できる識別された潜在的な脆弱性を***記録しなければならない***。	CEM ワークユニットをセクション A.1 の潜在的な脆弱性のリストにおける分析アクティビティ、及びセクション A.3 で規定されるとおりの証拠資料に置き換える。
AVA_VAN.1-5 評価者は、潜在的な脆弱性に対する独立探索に基づいて、侵入テストを***考えださなければならない***。	CEM ワークユニットをセクション A.2 で規定されたアクティビティに置き換える。
AVA_VAN.1-6 評価者は、潜在的な脆弱性のリストに基づき、テストを再現可能にするために十分に詳細に侵	CEM ワークユニットは、セクション A.3 で取り込まれている；(訳注：CEM ワークユニットとセクション

入テスト証拠資料を***作成しなければならない***。テスト証拠資料には、次のものを含めなければならない： a) TOE はどの潜在的な脆弱性の調査のためにテストされるか、その脆弱性の識別； b) 侵入テストを実施するために必要となるすべての必要なテスト装置を接続し、セットアップするための指示； c) すべての侵入テスト前提初期条件を確立するための指示； d) TSF を刺激するための指示； e) TSF のふるまいを観察するための指示； f) すべての期待される結果と、期待される結果と比較するために観察されたふるまいに実施する必要がある分析の記述； g) TOE のテストを終了し、終了後の必要な状態を確立するための指示。	A.3 との間に) 実質的な違いは一切ない。
AVA_VAN.1-7 評価者は、侵入テストを***実施しなければならない***。	評価者は、規定されたとおりの CEM アクティビティを実行しなければならない(shall)。確認された瑕疵についての攻撃能力に関するガイダンスについては、セクション A.2 のパラグラフ 642 を参照。
AVA_VAN.1-8 評価者は、侵入テストの実際の結果を***記録しなければならない***。	評価者は、規定されたとおりの CEM アクティビティを実行しなければならない(shall)。
AVA_VAN.1-9 評価者は、ETR に、テスト手法、構成、深さ、及び結果を概説して評価者の侵入テストの成果を***報告しなければならない***。	CEM ワークユニットをセクション A.3 で求められている報告に置き換える。
AVA_VAN.1-10 評価者は、TOE が、運用環境において、基本的な攻撃能力を持つ攻撃者に耐えられることを決定するために、すべての侵入テストの結果を***検査しなければならない***。	本ワークユニットは、iTC による本サポート文書に含めることは基本攻撃能力を持つ攻撃者を対象とするこれらの欠陥に起因する確認された脆弱性を抽出させるので、タイプ 1 及びタイプ 2 の欠陥には適用されない(セクション A.1 で規定されるとおり)。本ワークユニットは、タイプ 3 及びタイプ 4 欠陥に対して、セクシ

	ョン A.2、パラグラフ 642 で定義されるアクティビティに置き換えられる。
AVA_VAN.1-11　評価者は、ETR に、すべての悪用され得る脆弱性と残存脆弱性を、次のそれぞれを詳細に述べて***報告しなければならない***: a) 出所(例えば、脆弱性が予想されたとき実行していた CEM アクティビティ、評価者に既知である、公表されたものを読んで知った、など); b) 満たされていない SFR (1 つまたは複数); c) 記述; d) 運用環境で悪用されるか否か(つまり、悪用される可能性があるか残存か); e) 識別された脆弱性を実行するために必要な時間量、専門知識のレベル、TOE に関する知識のレベル、機会のレベル、及び装置。及び附属書 B.4 の表 3 及び 4 を使用した対応する値。	CEM ワークユニットをセクション A.3 で求められる報告に置き換える。

表 2：AVA_VAN.1 CEM ワークユニットの評価アクティビティへのマッピング

611　評価アクティビティとして要求される詳細レベルゆえに、保証アクティビティの「概説」は以下に提供されるが、指示の大部分は、附属書 A に含まれる。

5.6.1.1　評価アクティビティ (証拠資料):

612　表 2 にしたって CEM により規定されたアクティビティに追加して、評価者は以下のアクティビティを実行しなければならない(shall)。

613　*評価者は、ベンダによって提供された以下に概説された証拠資料を、それらが要求されたすべての情報を含むことを確認するために、検査しなければならない(shall)。本証拠資料は、以前に列挙された EA への回答として供給されるためにすでに要求された証拠資料への追加のものである。*

614　開発者は、TOE を構成するソフトウェアおよびハードウェアコンポーネント [7] のリストを識別する証拠資料を提供しなければならない(shall)。ハードウェアコンポーネントは、ST で主張されたすべてのシステムに適用され、かつ TOE に

[7] 本サブセクションでは、用語「コンポーネント」は、TOE を作り上げるパーツを参照する。ゆえに、分散型 TOE の 1 つの物理的部分に存在するような TOE の一部として参照される用語「分差型 TOE コンポーネント」とは区別される。それぞれの分散型 TOE コンポーネントは、ゆえに一般的に本サブセクションでさんしょうされるような多くのハードウェア及びソフトウェアコンポーネントを含む：例えば、それぞれの分散型 TOE コンポーネントは、一般的にプロセッサのようなハードウェアコンポーネント及びオペレーティングシステム及びライブラリのようなソフトウェアコンポーネントを含む。

よって利用されるプロセッサを少なくとも識別するべきである(should)。ソフトウェアコンポーネントは、暗号ライブラリのような、TOE によって利用されるあらゆるライブラリを含むこと。この追加の証拠資料は、単にコンポーネントの名称とバージョン番号のリストであり、かつ評価者によって彼らの分析の間に仮説を立てる際に利用される。

615 TOE が分散型 TOE である場合、開発者は以下を提供しなければならない(shall):

a) [NDcPP、3.4]にあるとおりコンポーネント間の要件の割り当てについて記述する証拠資料

b) [NDcPP、6.3.3]にあるとおりそれぞれのコンポーネントによって記録される監査対象事象のマッピング

c) 3.5.1.2 および 3.6.1.2 で識別されるような準備手続き中の追加の情報における AGD_PRE.1 の詳細化で識別されるとおり、準備手続きにおける追加の情報。

5.6.1.2 評価アクティビティ

616 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.3 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.2 に従って脆弱性分析を行わなければならない(shall)。分析の結果は、附属書 A.3 に従った報告書に文書化されなければならない(shall)。

6 必須の補足情報

617 本サポート文書ではさまざまな個所で、『必須の補足情報』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操作ガイダンス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 に識別されることになる。

618 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。

7 参考資料

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model
CCMB-2012-09-001, Version 3.1 Revision 4, September 2012

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components,
CCMB-2012-09-002, Version 3.1 Revision 4, September 2012

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components,
CCMB-2012-09-003, Version 3.1 Revision 4, September 2012

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology,
CCMB-2012-09-004, Version 3.1, Revision 4, September 2012

[FIPS 140-2] FIPS PUB 140-2, Security Requirements for cryptographic modules, May 25 2001 with change notices (12-03-2002)

[FIPS 186-4] FIPS PUB 186-4, Digital Signature Standard (DSS),
July 2013

[FWcPP] collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0, May 2017

[NDcPP] collaborative Protection Profile for Network Devices,
Version 2.0, 5 May 2017

[NIST SP800-56A] NIST Special Publication SP800-56A Revision 2: Recommendation for Pair-Wise Key EstablishmentSchemes Using Discrete Logarithm Cryptography,
May 2013

[NIST SP800-56B] NIST Special Publication SP800-56B Revision 1: Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography,
September 2014

[NIST SP800-90A] NIST Special Publication SP800-90A Deterministic Random Bit Generator Validation System (DRBGVS),
October 29 2015

[SHAVS] The Secure Hash Algorithm Validation System (SHAVS),
Updated: May 21, 2014

A. 脆弱性分析

A.1 脆弱性情報の情報源

619 CEM ワークユニット AVA_VAN.1-3 は、調査する欠陥のよりうまく定義されたセット及びこの特定の技術に基づき従うべき手順を提供するため、本サポート文書で補足されている。利用される用語は、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、次に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、CEM で利用される「潜在的な脆弱性」と同等である)。欠陥は、どのように考案されるかによって 4 つの「タイプ」に分類される：

1. 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) に適用可能な欠陥仮説のリストであって、セクション A.1.1 に記述されるような公開の情報源から導出されるもの—この固定のセットは、iTC によって合意されたものである。さらに、これは TOE やその識別されたコンポーネントに直接適用可能な (以下に示すような)公開の情報源のセットへのエントリによって、補足される (セクション A.1.1 のプロセスにより定義されるとおり) ; これは、評価者が、本 cPP が公開された後、発見された適用可能なエントリを彼らの評定に含めることを保証する。
2. セクション A.1.2 に記述されるとおり、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本書に列挙された欠陥仮説のリスト(例えば、その他の公開の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
3. 評価者が利用可能な情報から導出された欠陥仮説のリスト；これには、本サポート文書 (EA に関連する証拠資料、セクション 5.6.1.2 に記述された証拠資料、セクション 6 に記述された証拠資料)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が、セクション A.1.3 に記述されるとおりのその他の情報(公開及び／または評価者の経験に基づくもの)と同様に含まれる；及び
4. TC-定義のツール (例えば、nmap や fuzz テスタ)、及びセクション A.1.4 で規定されるそれらのアプリケーションの利用を通して生成される欠陥仮説のリスト。

A.1.1 タイプ 1 仮説—公開脆弱性ベース

620 iTC により選択された脆弱性情報の公開情報源のリストは、セクション A.4 で与えられる。

621 評価者は、セクション A.4 に列挙された情報源において、cPP の公開日付よりも新しいもの、及び上記の追加の証拠資料によって規定されるとおり TOE 及びそのコンポーネントに特有なものである潜在的な欠陥仮説のリストを決定するために検索を実行しなければならない(shall)。あらゆる重複 － 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のいずれかにおいて － は、それを記録した上で、評価チームにより検討から外すことができる。

622 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(shall)：

- 用語「ルータ (router)」及び「スイッチ (switch)」(または TOE のデバイス

タイプを記述しているより一般的な用語)

- 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)
- TOE 名称 (適宜、適切なモデル情報を含む)

623 TOE の具体的なコンポーネントのタイプ 1 欠陥仮説生成の一部として、評価者は、本仮説の基盤において欠陥仮説が作成できるかどうかを決定するため、コンポーネントの製造業者のウェブサイトについても検索しなければならない(shall) (例えば、評価中のコンポーネント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.1.2 タイプ 2 仮説—iTC 出典のもの

624 セクション A.5 には、脆弱性評定の実行における欠陥仮説として評価チームにより検討されなければならない(must)ような、iTC によってこの技術用に生成された欠陥仮説のリストが含まれる。

625 評価者が本 cPP の将来のバージョンでタイプ 2 欠陥とみなされるべきである(should)と評価者が確信するようなタイプ 3 またはタイプ 4 の欠陥を発見した場合、彼らは、iTC による検討のため、その欠陥の適切な提出手段を決定するために、認証機関と連携するべきである(should)。

A.1.3 タイプ 3 仮説—評価チームによって作成されたもの

626 製品によって提示された情報に基づき評価者により考案されたタイプ 3 欠陥 (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。

627 評価者が本 cPP の将来のバージョンでタイプ 2 欠陥とみなされるべきである(should)と評価者が確信するようなタイプ 3 欠陥を発見した場合、彼らは、iTC による検討のため、その欠陥の適切な提出手段を決定するために、認証機関と連携するべきである(should)。

A.1.4 タイプ 4 仮説—ツールによって作成されたもの

628 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(shall)：

- Fuzz 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(should)。

  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(should)。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。

629 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利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(shall)。

630 評価者が本 cPP の将来のバージョンでタイプ 2 欠陥とみなされるべきである(should)と評価者が確信するようなタイプ 4 欠陥を発見した場合、彼らは、iTC による検討のため、その欠陥の適切な提出手段を決定するために、認証機関と連携するべきである(should)。

A.2 評価者脆弱性分析のプロセス

631 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、以下のようになる。

632 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、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、これらの議論のすべてに、CB は含まれるべきである(should)。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：

1. 仮説の策定に利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；
2. 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；
3. 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。

633 次に認証機関 (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)。

634 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。重要なのは、以下のセクション A.3 に概説されるとおり、結果が文書化されることである。

635 評価者が欠陥を見つける場合、評価者は、これらの欠陥を開発者へ報告することになる。報告されたすべての欠陥は、以下のとおり対処されなければならない(must)。

636 開発者がその欠陥が存在すること及びそれが基本的攻撃能力で悪用可能であることを確認した場合、開発者によって変更がなされ、もたらされる解決策は、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。

637 開発者、評価者、及び CB が、その欠陥が基本的攻撃能力を超えてのみ悪用可能であることに合意しその他の理由で解決が要求されない場合、一切の変更は行われず、欠陥は、CB 内部報告 (ETR) で残存脆弱性として記録される。

638 開発者、評価者が、その欠陥が基本的攻撃能力を超えてのみ悪用可能であることに合意したが、通常の利用事例または運用環境のような技術特有または cPP 特有の観点から解決することが重要であると見なされる場合、変更が開発者によって行われ、もたらされる解決が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。

639 ある欠陥の存在、その攻撃能力、または解決が重要と見なされるべきかについての疑義に関する評価者とベンダの間で意見の相違は、CB によって解決される。

640 評価者により実行されるあらゆるテストは、以下のセクション A.3 で概説されるとおりテスト報告書に文書化されなければならない(shall)。

641 セクション A.3 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.1 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、対処されなければならない(must)ことを示している。

642 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。決定の基準は、セクション A.3 で規定されるとおり、CB 内部の報告書 (訳注：ETR) に文書化されなければならない(shall)。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 の抵抗力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.3 報告

643 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(shall)； ひとつは公開向けの (すなわち、評価報告書(ETR)のサブセットであるような、機密情報を含まない評価報告書、)、もうひとつは監督している CB へ配付される完全な ETR である。

644 公開向けの報告書には、以下が含まれる：

- 公開情報源の検索のための手順がサポート文書のセクション A.1.1 の指示に従って行われたときに返った欠陥識別子；
- 評価者が本サポート文書のセクションの A.1.1 で規定されたタイプ 1 の欠陥仮説及び本サポート文書のセクション A.1.2 で規定されたタイプ 2 の欠陥仮説を検査したことを示すステートメント。

645 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.1.3、A.1.4 及び A.2 に従って開発したこと、及び CEM のガイダンスに従って CB により定義された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。これは、開発されたタイプ 3 及び 4 の欠陥仮説「の事実」についての単なるステートメントであること、及び欠陥の数、欠陥自体、または公開向けの報告に含まれるそれらの欠陥に関する分析についての具体的なものでは一切ないことに留意するべきである(should)。

646 その他の一切の情報は、公開向けの報告には提供されない。

647 内部の CB 報告書には、公開向け報告における情報に追加して以下を含む：

- 生成されたすべての欠陥仮説のリスト(参照、AVA_VAN.1-4)；
- 評価者侵入テスト作業、テストアプローチの概説、設定、深さと結果(参照、AVA_VAN.1-9)；
- 欠陥仮説を作成するために利用されたすべての証拠資料 (欠陥仮説を思い付くときに利用された証拠資料の識別において、評価チームは、読者が本サポート文書によって厳密に要求されるかどうかを決定できるように、その証拠資料を特徴付けなければならない(must)、また証拠資料の性質

(設計情報、開発者の技術ノート、等))；

- 評価者は、すべての悪用され得る脆弱性と残存脆弱性を、次のそれぞれを詳細に述べて報告しなければならない(shall)：
    - 出所 (例えば、脆弱性が予想されたとき実行していた CEM アクティビティ、評価者に既知である、公表されたものを読んで知った、など)；
    - 満たされていない SFR；
    - 記述；
    - 運用環境で悪用されるか否か(つまり、悪用される可能性があるか残存か)；
    - 識別された脆弱性を実行するために必要な時間量、専門知識のレベル、TOE に関する知識のレベル、機会のレベル、及び装置(参照、AVA_VAN.1-11)；
- 各欠陥仮説がどのように解決されたか (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持つ攻撃者によって悪用され得るかどうかに関する任意の分析が含まれる) (参照、AVA_VAN.1-10)；及び
- 調査において実際のテストが実行されたような場合に(セクション A.1.4 で iTC)によって規定されたツールを用いた欠陥仮説生成の一部として、または特定の欠陥の証明／反証において、のいずれか)、TOE のセットアップで従うステップ(及びあらゆる必須のテスト装置)；テストの実行；テスト後の手順；及び実際の結果(以下を含めて、テストの再現を許すような詳細レベルまで：
    - TOE はどの潜在的な脆弱性の調査のためにテストされるか、その脆弱性の識別；
    - 侵入テストを実行するために必要となるすべての必要なテスト装置を接続し、セットアップするための指示；
    - すべての侵入テスト前提初期条件を確立するための指示；
    - TSF を刺激するための指示；
    - TSF のふるまいを観察するための指示；
    - すべての期待される結果と、観測された結果と比較するために観察されたふるまいに実施する必要がある分析；
    - TOE のテストを終了し、終了後の必要な状態を確立するための指示(参照、AVA_VAN.1-6,AVA_VAN.1-8)。

A.4 公開脆弱性情報源

648 以下の公開脆弱性情報源は、具体的な TOE の評価中にキーワード検索を実行するために評価者への指示において参照するのと同様に、評価者によって調査されるべき欠陥の具体的なリストの考案で iTC が検討するための情報源である。

a) NIST National Vulnerabilities Database (以下の CVE 及び US-CERT データベースをアクセスするために利用可能) :
https://web.nvd.nist.gov/view/vuln/search

b) Common Vulnerabilities and Exposures:
http://cve.mitre.org/cve/
https://www.cvedetails.com/vulnerability-search.php

c) US-CERT:
http://www.kb.cert.org/vuls/html/search

d) Exploit / Vulnerability Search Engine:
www.exploitsearch.net

e) SecurITeam Exploit Search:
www.securiteam.com

f) Tenable Network Security
http://nessus.org/plufins/index.php?view=search

g) Tipping Point Zero Day Initiative
http://www.zerodayinitiative.com/advisories

h) Offensive Security Exploit Database:
https://www.exploit-db.com

i) Rapid7 Vulnerability Database:
https://www.rapid7.com/db/vulnerabilities

A.5 追加の欠陥仮説

649 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。

B. ネットワークデバイスの同等性の考察

B.1 序説

650 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さまざまなモデルについて製品の同等性について、ベンダの要求が許容されるかどうかを評価者が決定するための根拠を提供する。

2 評価の目的について、評価性は以下の 1 つに分けられる：

- モデルにおけるバリエーション：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。以下に列挙され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、それらのモデルは同等であると見なされるかもしれない。
- 環境における TOE 依存性におけるバリエーション(例、製品がテストされる OS／プラットフォーム)：TOE が機能を提供する方法(または機能そのもの)は、インストールされる環境に依存して変わるかもしれない。TOE 提供の機能または TOE が機能を提供するやり方において一切の違いがない場合、それらのモデルは同等であると見なされるかもしれない。

651 モデル間の同等性の決定は、さまざまなテスト結果をもたらす可能性がある。

652 いくつかの TOE が同等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(must)。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(must)。その他の同等な機能については、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。

653 TOE が環境にかかわらず同じ動作をすることが決定される場合、テストは、すべての同等な構成に対して 1 つのインスタンスにおいて実行されればよい。しかし、TOE が環境特有の機能を提供すると決定される場合、テストは、機能における相違が存在するようなそれぞれの環境において実施されなければならない(must)。上記のシナリオと同様に、環境の相違により影響を受ける機能のみが再テストされなければならない(must)。

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

B.2 同等性を決定するための評価者ガイダンス

B.2.1 戦略

655 同等性分析を実行するとき、評価者は、それぞれの要素について独立に検討するべきである(should)。ある要素は、デバイスが利用するプロセッサから、ソフトウェアアプリケーションが依拠する下位のオペレーティングシステム及びハードウェアプラットフォームまで、さまざまなレベルの抽象化で、任意の数のものであるかもしれない。例としては、製品により採用される様々なチップセット、ネットワークインタフェースの種別 (異なるデバイスドライバ)、ストレ

ージ媒体(半導体ドライブ、回転ディスク。EEPROM) であるかもしれない。SFR を実施する TOE の能力に影響するかもしれないこれらの要素において、どのような違いがあるかについて検討することは重要である。個別の要素のそれぞれの分析は、2 つの結果の一つをもたらすだろう。

- 特定の要素について、すべてのサポートされるプラットフォームについての TOE のすべてのバリエーションが同等である。この場合、テストは、1 つのテスト環境における 1 つのモデルについて実行されてもよく、すべてのサポートされるモデルと環境をカバーする。
- 特定の要素について、それがその他すべての同等な TOE とまったく同一に動作することを保証するため、別々のテストを要求するための、製品のサブセットが識別される。分析は、テストされる必要があるモデル／テスト環境の具体的な組み合わせを識別することになる。

656 製品の完全な CC テストは、識別された要素のそれぞれについて実行されるご別分析それぞれの全体を包含することになる。

B.2.2 ネットワークデバイスのガイダンス

657 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同等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、同等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同等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

要因	同一／同一でない	評価者ガイダンス
		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同等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、それらのモデルは同等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同等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 機能の提供に利用されるライブラリの相違	同一	さまざまな TOE モデルで利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同等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利用される場合、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、モデルは同等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同等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同等であると考えなければならない。
	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同等であるとは考えられず、別々のテストを実行しなければならない。評価者は、

要因	同一／同一でない	評価者ガイダンス
		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同等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同等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、それらのモデルは同等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同等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 3：評価の同等性分析

B.3 テストプレゼンテーション／告知における真実

658 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(must)。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。

B.4 分散型 TOE の追加のコンポーネントの評価

659 分散型 TOE の場合に、セキュリティターゲットは、cPP の要件を集積的に満たすような、ST 作成者によって選択された数多くの別々のコンポーネントからなる、評価された構成を識別する。この評価される構成は、cPP をおそらく満たすことができるような(例、TOE が大企業での配備を意図するような場合、評価される校正は、期待される接続性と負荷をサポートするために複数のコンポー

ネントにおいて何らかの冗長性を含むに違いない)、最小限のコンポーネントのセットである必要はないが、ゆえにこれは、ST 及び評価において参照される主な構成であって、本セクションにおいて「評価された構成」と同様に「最小構成」としてここでは参照され、興味のある最小構成として取り扱われる。

660 上記最小構成に追加して、ST は、(作成者の裁量で、かつ本セクションに記述されるように検証の対象で) 度のコンポーネントが CC 認証の有効性に影響を与えることのなしに運用環境にインスタンスを追加できるかについても識別することができる。ST 記述は、コンポーネントの必須の及び／または禁止された構成を含めて、このようなコンポーネントがどのように追加されるかについての制約を含むかもしれない。

661 TOE コンポーネントの余分なインスタンスは、評価された構成に含まれたオリジナルなコンポーネントとして、同じハードウェアとソフトウェアを持たなければならない(must)。

662 望ましくない構成は、TOE の運用展開(訳注：運用上の機器の配備・配置)にあるかもしれないことに留意されたい―別の管理ドメインから管理される TOE コンポーネント及び管理ドメインと対立する可能性のあるような TOE コンポーネントを許容するような場合。しかし、このような場合に含まれる「望ましくない」及びリスクの定義は、それぞれの運用環境に特有である、ゆえに評価の一部としては、取り扱われない。この種の正しく適切な構成は、運用環境のネットワーク計画と設計のエキスパートの問題として残る。

B.4.1 ST 評定のための評価者アクション

B.4.1.1. TSS

663 評価者は、ST で許容される TOE コンポーネント余分なインスタンスを識別するため、TSS を検査しなければならない(shall)、また評価された構成の中でそのコンポーネントが演じる役割と一貫していることを確認するため、その SFR を追加のコンポーネントがどのように維持するかについての記述を検査しなければならない(shall)。例えば : TOE 内通信(FPT_ITT)及び外部通信(FTP_ITC)のための余分なコンポーネントによって利用されるセキュアチャネルは、一貫していなければならない(must)、余分なコンポーネントにより生成された監査情報は、維持されなければならない(must)、また、余分なコンポーネントの管理は、最小構成におけるコンポーネントのオリジナルなインスタンスで利用されるものと一貫していなければならない(must)。

B.4.2 ガイダンス証拠資料の評定のための評価者アクション

B.4.2.1. ガイダンス証拠資料

664 評価者は、ST で許容されるものとして識別されるものとそれらが一貫していることを確認するため、ガイダンス証拠資料における TOE コンポーネントの余分なインスタンスの記述を検査しなければならない(shall)。これには、余分なコンポーネントを設定するためにガイダンス証拠資料を適用した結果が TOE を各コンポーネントでサポートする SFR についての主張が ST に記述されたとおりであるような状態に置くこと、ゆえに余分なコンポーネントが存在するときにすべての SFR は満たされ続けることの確認が含まれる。

665 評価者は、それらが最小構成におけるコンポーネントのために記述されたものと同じであることを確認するため、余分なコンポーネントについて記述されたセキュアな通信を検査しなければならない(shall) (許容された余分なコンポーネントと最小構成のコンポーネントの間の追加の接続は、もちろん許容される)。

B.4.3 TOE のテストのための評価者アクション

B.4.3.1. テスト

666 評価者は、ST (及びガイダンス証拠資料) で定義されたとおり、最小構成で TOE をテストすること。

667 ST 及びガイダンス証拠資料の余分なコンポーネントの利用の記述があるコンポーネントに割り当てられた SFR で何らかの相違を識別する場合、または SFR の適用範囲が含まれる場合(例、異なる選択がそのコンポーネントの異なるインスタンスに適用される場合)、評価者は、最小構成に含まれなかったようなこれらの追加の SFR の場合についてテストすること。

668 さらに、評価者は、分散型 TOE で許容されるとおり識別された余分なコンポーネントのそれぞれについて、以下の観点でテストすること：

- 通信 : 評価者は、余分なコンポーネントと共に導入された任意の追加の接続で最小構成において存在しないものが、ST で記述された要件と一貫していることを、テストにより確認するため、ガイダンス証拠資料に従うこと (例、利用されたプロトコルと暗号スイートン関して)。このような追加の接続の 1 つの例は、コンポーネントの 1 つのインスタンスが最小構成に存在しており重複するコンポーネントを追加する場合、1 つのインスタンスの間の余分の通信を導入することである。別の例は、追加のコンポーネントの利用が必要とされる場合、ローカルに格納されたクレデンシャルを利用する代わりに外部認証サーバへの接続を利用することである。
- 監査 : 評価者は、あるコンポーネントの異なるインスタンスからの監査記録が度のインスタンスが記録を生成したか明確となるように、区別可能であることを確認すること。
- 管理 : 余分なコンポーネントが分散型 TOE のその他コンポーネントを管理する場合、評価者は、余分なコンポーネント経由の管理が最小構成におけるそのコンポーネント用として管理者のための同じ役割と役割保持者を利用することを確認するため、ガイダンス証拠資料に従わなければならない(shall)。