汎用オペレーティングシステムの
プロテクションプロファイル

バージョン：4.0
2015-08-14
National Information Assurance Partnership

平成 28 年 3 月 30 日　翻訳 暫定第 0.1 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

改版履歴

バージョン	日付	コメント
4.0	2015-08-14	リリース―大幅な改版

目次

1. 序説

1.1 概要

本プロテクションプロファイル (PP) の適用範囲は、オペレーティングシステムのセキュリティ機能を [CC] の観点から記述し、そのような製品の機能及び保証要件を定義することである。オペレーティングシステムとは、コンピュータのハードウェア資源を管理しアプリケーションプログラムへ共通サービスを提供するソフトウェアである。その管理するハードウェアは、物理的なものであるかもしれないし、仮想的なものであるかもしれない。

1.2 用語

以下のセクションでは、本プロテクションプロファイルに用いられるコモンクライテリア用語と技術用語を説明する。

1.2.1 コモンクライテリア用語

コモンクライテリア (CC)	情報技術セキュリティ評価のためのコモンクライテリア。
共通評価方法 (CEM)	情報技術セキュリティ評価のための共通評価方法。
プロテクションプロファイル (PP)	あるカテゴリの製品に関する、セキュリティ要件の実装非依存のセット。
セキュリティターゲット (ST)	具体的な製品に関する、セキュリティ要件の実装依存のセット。
評価対象 (TOE)	評価の対象となる製品。ここでは、TOE 境界 のセクション及びそのサポート文書で記述されるオペレーティングシステム。
TOE セキュリティ機能 (TSF)	評価の対象となる製品のセキュリティ機能。
TOE 要約仕様 (TSS)	TOE がどのように ST の SFR を満たすかという記述。
セキュリティ機能要件 (SFR)	TOE によって実施されるセキュリティに関する要件。
セキュリティ保証要件 (SAR)	TOE のセキュリティを保証するための要件。

1.2.2 技術用語

アドレス空間配置ランダム化 (ASLR)	メモリマッピングを予測不可能なロケーションにロードする、悪用防止機能。ASLR によって、攻撃者がプロセスのアドレス空間へ導入したコードへ制御を渡すことがより困難となる。

管理者 (Administrator)	管理者は、エンタープライズによってオペレーティングシステムへ適用されるポリシーの設定を含めた、管理アクティビティに責任を負う。この管理者は、システムが構成ポリシーを受け取る管理サーバを介してリモートから操作を行ってもよい。管理者は、管理者以外の利用者には上書き不可能なシステムに、設定を適用できる。
アプリケーション (アプリ)	プラットフォーム上で動作し、そのプラットフォームの利用者または所有者を代行してタスクを実行するソフトウェア、ならびにその支援のための資料。
アプリケーションプログラミングインタフェース (API)	ライブラリなど、他のソフトウェアコンポーネントによって提供されるサービスをアプリケーションが利用できるようにするための、ルーチン、データ構造、オブジェクトクラス、及び変数の仕様。API は、プラットフォームに含まれるライブラリのセットとして提供されることが多い。
クレデンシャル (Credential)	暗号鍵またはパスワードなど、利用者の識別情報を立証するデータ。
クリティカルセキュリティパラメタ (CSP)	利用者またはシステムのいずれかによって定義される情報であって、暗号鍵及び、パスワードなどの認証データを含む暗号機能の処理を行う暗号モジュールの運用に用いられ、その開示または改変が暗号モジュールのセキュリティまたはそのモジュールによって保護される情報のセキュリティの危殆化をもたらす可能性のあるもの。
保存データ (DAR) の保護	たとえ物理的なアクセスを有する場合であっても、攻撃者による不揮発性ストレージからのデータの抽出を防止する対策。一般的なテクニックとして、データの暗号化及び抹消がある。
データ実行防止 (DEP)	モダンなコンピューターハードウェア上で動作するモダンなオペレーティングシステムの悪用防止機能であって、メモリのページ上に非実行アクセス権限を実施するもの。DEP は、メモリのページにデータと命令の両方が含まれないようにすることによって、攻撃者が実行可能コードを導入することをより困難とする。
開発者 (Developer)	OS ソフトウェアを作成するエンティティ。本文書の目的においては、ベンダと開発者は同一である。
ホストベースのファイアウォール	OS 上で動作するプロセスへの、及びそのようなプロセスからの、内向き及び外向きネットワークトラフィックをフィルタリングするために、OS 上で動作するソフトウェアベースのファイアウォール実装。
オペレーティングシステム (OS)	物理的及び論理的資源を管理しアプリケーションへサービスを提供するソフトウェア。TOE という用語と OS という用語は、本文書においては同義である。
個人を識別可能な情報 (Personally	エージェンシーによって維持管理される個人に関する任意の情報であって、教育、金融トランザクション、病歴、及び犯罪歴または職歴などを含むが、これらに限定されない。また名前、社会保険番号、生年月日

Identifiable Information) (PII)	及び出生地、母親の旧姓、バイオメトリック記録など、個人の識別情報を区別または追跡するために利用可能な情報であって、個人へ結びつけられた、または個人へ結びつけられ得る、その他の任意の個人的な情報を含む。[OMB]
機微なデータ (Sensitive Data)	機微なデータにはすべての利用者またはエンタープライズデータが含まれてもよく、また PII、電子メール、メッセージ、文書、カレンダー項目、及び連絡先など特定のアプリケーションデータであってもよい。機微なデータには最低限、クレデンシャル及び鍵が含まれなければならない。機微なデータは、ST 作成者によって OS の TSS で識別されなければならない。
利用者 (User)	利用者は、管理者によってオペレーティングシステムへ適用される構成ポリシーに従う。特定の構成下にある一部のシステムにおいては、通常の利用者が一時的に権限を管理者の権限に上昇させることができる。その際、そのような利用者は管理者とみなされるべきである。

1.3 適合評価対象

1.3.1 TOE 境界

TOE 境界は、OS カーネルとそのドライバ、共有ソフトウェアライブラリ、及び OS に含まれる一部のアプリケーションソフトウェアを包含する。TOE の内部とみなされるアプリケーションは、基本的なセキュリティサービスを提供するものであり、その多くは上昇した特権で実行される。より具体的なプロテクションプロファイルによってカバーされるアプリケーションは、たとえその機能の一部が OS の一部としての役割に関連して評価される必要があっても、OS 評価の一部としての評価を主張することはできない。

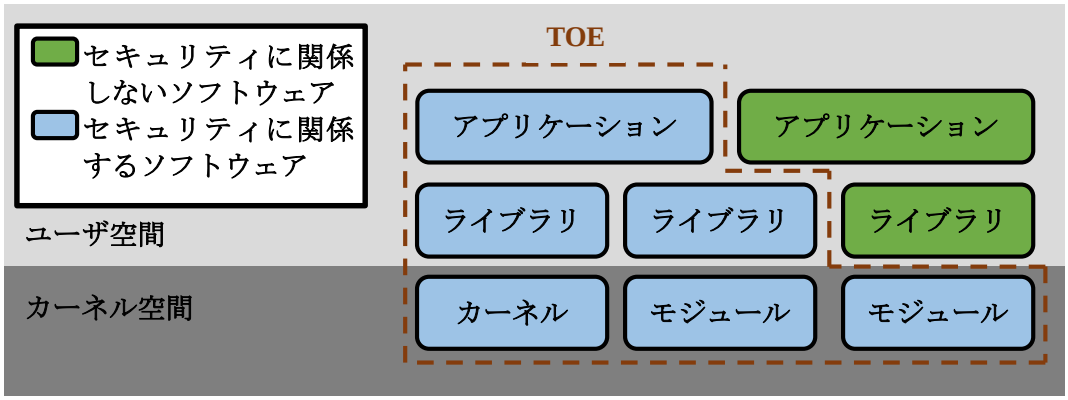

図 1：一般的な TOE

1.3.2 TOE プラットフォーム

TOE が動作する物理的または仮想的ハードウェアから構成される TOE プラットフォームは、評価の対象外である。同時に、TOE のセキュリティはプラットフォームに依存する。その他のハードウェアコンポーネントであって、それ自身のソフトウェアを独立に実行し、全体的なシステムのセキュリティに関連するものもまた、評価の対象外である。

1.4 使用事例

本プロテクションプロファイルの要件は、少なくとも以下の使用事例中のセキュリティ課題へ対処するようにデザインされている。オペレーティングシステムには多数の具体的な使用事例が存在するため、これらの使用事例は意図的に非常に範囲が広いものとなっている。また、これらの使用事例は互いにオーバーラップするかもしれない。オペレーティングシステムの機能が、その上にインストールされた特権を持つアプリケーションによって実質的に拡張されることさえあるかもしれない。しかし、これらは本 PP の適用範囲外である。

[使用事例 1] エンドユーザデバイス

OS は、デスクトップ、ラップトップ、コンバーチブル、及びタブレットなどの、エンドユーザデバイスへのプラットフォームを提供する。オプションとしてこれらのデバイスは、ディレクトリサーバまたは管理サーバへ束縛されているかもしれない。

本プロテクションプロファイルは保存データに対する脅威に対抗しないため、モバイルシナリオへオペレーティングシステムを展開するエンタープライズは、他のプロテクションプロファイルに詳説される保存データ保護がこれらのシステムに含まれることを保証すべきである。具体的には、*完全なドライブの暗号化―暗号化エンジン*、*完全なドライブの暗号化―許可取得*、及び*ソフトウェアファイル暗号化*のプロテクションプロファイルが含まれる。*モバイルデバイス基盤のためのプロテクションプロファイル*には保存データ保護の要件が含まれるため、多くのモバイルデバイスに適切である。

[使用事例 2] サーバシステム

OS は、物理的または仮想的いずれかのハードウェア上で、サーバサイドサービスのプラットフォームを提供する。ファイルサーバ、メールサーバ、及びウェブサーバなど、そのようなサービスのためのプラットフォームとして OS が機能する具体例は数多く存在する。

[使用事例 3] クラウドシステム

OS は、物理的または仮想的ハードウェア上で動作する、クラウドサービスのプラットフォームを提供する。典型的には OS はサービスとしてのインフラストラクチャ (IaaS)、サービスとしてのソフトウェア (SaaS)、及びサービスとしてのプラットフォーム (PaaS) として特定される提供物の一部である。

この使用事例には、*サーバ仮想化のプロテクションプロファイル*に対して評価されるべき仮想化技術の利用が伴うのが典型的である。

2. 適合主張

適合言明

本 PP へ適合するためには、 [CC] 第 1 部 (ASE_CCL) に定義される正確適合 (Strict Conformance) のサブセットである完全適合 (Exact Conformance) を ST は論証しなければならない。ST には、本 PP におけるコンポーネントであって

- 無条件のもの (常に要求される)
- 選択に基づくもの (無条件要件中で特定の*選択*が選択された際に要求される)

がすべて含まれなければならず、また

- オプションの、または
- オブジェクティブな

コンポーネントが含まれてもよい。

無条件の要件は文書の本体に存在する一方で、附属書には選択に基づく、オプションの、及びオブジェクティブな要件が含まれる。ST はこれらのコンポーネントのいずれをも繰り返してよいが、本 PP やそれに適合する PP 中に定義されないいかなる追加コンポーネント (例、CC パート 2 またはパート 3 から、もしくは本 PP に適合しない PP からのもの、または ST により拡張されたもの) も含んではならない。

本プロテクションプロファイルの一部のコンポーネントには、他のコンポーネントへの依存性が存在する。[CC] パート 1 に従い、附属書 Dには、それへの依存性が存在するコンポーネントが PP に明示的に含まれない場合の正当化が含まれている。

CC 適合主張

本 PP は、コモンクライテリアバージョン 3.1 改訂第 4 版のパート 2 (拡張) 及びパート 3 (拡張) に適合する。[CC]

PP 主張

本 PP は、いかなる他のプロテクションプロファイルへの適合も主張しない。

パッケージ主張

本 PP は、いかなるパッケージへの適合も主張しない。

3. セキュリティ課題定義

セキュリティ課題は、OS が対応することが期待される脅威、運用環境に関する前提条件、及び OS が適用することが期待される任意の組織のセキュリティ方針の観点から記述される。

3.1 脅威

T.NETWORK_ATTACK

攻撃者は、通信チャネル上やネットワーク基盤上の他のどこかに位置する。攻撃者は、危殆化の意図を持って、OS 上で動作したり OS の一部であったりするアプリケーション及びサービスとの通信へ関与するかもしれない。関与は、既存の許可された通信の改変を伴うかもしれない。

T.NETWORK_EAVESDROP

攻撃者は、通信チャネル上やネットワーク基盤上の他のどこかに位置する。攻撃者が、OS 上で動作したり OS の一部であったりするサービスと、アプリケーションとの間で交換されるデータを監視したり、そのデータへのアクセスを獲得したりするかもしれない。

T.LOCAL_ATTACK

攻撃者は、OS 上で動作するアプリケーションを危殆化するかもしれない。危殆化されたアプリケーションは、非特権システムコールやファイルシステムを介したメッセージ交換など、さまざまなチャネルを介して OS へ悪意を持ってフォーマットされた入力を提供するかもしれない。

T.LIMITED_PHYSICAL_ACCESS

攻撃者は、物理的なデバイスとの制限された時間内に、OS 上のデータへのアクセスを試行するかもしれない。

3.2 前提条件

A.PLATFORM

OS は、信頼性のあるコンピューティングプラットフォームに依存してその動作を行う。この基盤となるプラットフォームは本 PP の適用範囲外である。

A.PROPER_USER

OS の利用者は意図的に怠慢であったり敵対的であったりせず、また適用されるエンタープライズのセキュリティ方針を遵守してソフトウェアを使用する。同時に、悪意のあるソフトウェアは利用者*として*動作することができるかもしれないため、悪意のあるサブジェクトを制限する要件もまた、適用範囲内である。

A.PROPER_ADMIN

OS の管理者は不注意であったり意図的に怠慢であったり敵対的であったりせず、また適用されるエンタープライズのセキュリティ方針を遵守して OS を管理する。

4. セキュリティ対策方針

4.1 TOE のセキュリティ対策方針

O.ACCOUNTABILITY

適合 OS は、オペレーティングシステムの設定や動作の意図せぬ問題を管理者が発見し、その原因を究明できるような情報が存在することを保証する。事象情報を収集し、他のシステムへ即座に送信することもまた、システムの危殆化の際にインシデント対応を可能とする。

以下によって対応される：FAU_GEN.1

O.INTEGRITY

適合 OS は、そのアップデートパッケージの完全性を保証する。OS はめったにエラーなしで出荷されることはなく、パッチ及びアップデートを展開して完全性を付与する能力はエンタープライズネットワークのセキュリティにとって不可欠である。適合 OS は、システムを危殆化させるタスクの複雑性を高めることにより、攻撃者に対してコストを増加させる実行環境ベースの緩和を提供する。

以下によって対応される：FPT_SBOP_EXT.1, FPT_ASLR_EXT.1, FPT_TUD_EXT.1, FPT_TUD_EXT.2, FCS_COP.1.1(2), FCS_COP.1.1(3), FCS_COP.1.1(4), FPT_ACF_EXT.1, FPT_SRP_EXT.1, FIA_X509_EXT.2, FPT_TST_EXT.1, FTP_ITC_EXT.1, FPT_W^X_EXT.1.1, FIA_AFL.1, FIA_UAU.5

O.MANAGEMENT

利用者及びエンタープライズによる管理を容易にするため、適合 OS は一貫した、かつサポートされるインタフェースをそのセキュリティ関連設定及び維持管理のために提供する。これには、プラットフォームによってサポートされる展開メカニズム及びフォーマットの利用によるアプリケーション及びアプリケーションアップデートの展開、ならびに設定及びアプリケーション実行制御のためのメカニズムの提供が含まれる。

以下によって対応される：FMT_MOF_EXT.1, FTP_TRP.1

O.PROTECTED_STORAGE

ストレージ媒体の物理的コントロール喪失の際にクレデンシャルの機密性の損失の問題に対応するため、適合 OS はクレデンシャルに保存データ保護を提供する。また適合 OS は、利用者が自分のファイルを同一システムの他の利用者から秘密にしておくことを可能とする、アクセス制御を提供する。

以下によって対応される：FCS_STO_EXT.1, FCS_RBG_EXT.1, FCS_COP.1.1(1), FDP_ACF_EXT.1

O.PROTECTED_COMMS

パッシブ (盗聴) 及びアクティブ (パケットの改変) なネットワーク攻撃の脅威に対応するため、適合 OS は CSP 及び機微なデータに高信頼チャネルを作成するためのメカニズムを提供する。CSP と機微なデータはどちらも、プラットフォーム外部へ暴露されるべきではない。

以下によって対応される：FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_D

TLS_EXT.1, FCS_RBG_EXT.1, FCS_CKM.1, FCS_CKM.2, FCS_COP.1.1(1), FDP_IFC_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2, FTP_ITC_EXT.1

4.2 運用環境のセキュリティ対策方針

以下の運用環境のセキュリティ対策方針は、OS がそのセキュリティ機能を正しく提供することを補助する。これらは、環境に関する前提条件と対応する。

OE.PLATFORM

OS は、高信頼ハードウェア上にインストールされることに依存する。

OE.PROPER_USER

OS の利用者は意図的に怠慢であったり敵対的であったりせず、また適用されるエンタープライズのセキュリティ方針を遵守してソフトウェアを使用する。標準的な利用者アカウントは、最小特権モデルに従って配備される。より高いレベルのアクセスを必要とする利用者は、その利用に限定された別個のアカウントを持つべきである。

OE.PROPER_ADMIN

OS の管理者は不注意であったり意図的に怠慢であったり敵対的であったりせず、また適用されるエンタープライズのセキュリティ方針を遵守して OS を管理する。

4.3 セキュリティ対策方針の根拠

本セクションでは、前提条件、脅威、及び組織のセキュリティ方針がどのようにセキュリティ対策方針と対応付けられるのかを記述する。

脅威、前提条件、または OSP	セキュリティ対策方針	根拠
T.NETWORK_ATTACK	O.PROTECTED_COMMS, O.INTEGRITY, O.MANAGEMENT	脅威 T.NETWORK_ATTACK は、送信されるデータの完全性を O.PROTECTED_COMMS が提供するため、これによって対抗される。 脅威 T.NETWORK_ATTACK は、ネットワークからシステム上にインストールされるソフトウェアの完全性を O.INTEGRITY が提供するため、これによって対抗される。 脅威 T.NETWORK_ATTACK は、ネットワーク攻撃に対して防御するよう OS を設定する能力を O.MANAGEMENT が提供するため、これによって対抗される。
T.NETWORK_EAVESDROP	O.PROTECTED_COMMS,	脅威

	O.MANAGEMENT	T.NETWORK_EAVESDROP は、送信されるデータの機密性を O.PROTECTED_COMMS が提供するため、これによって対抗される。 脅威 T.NETWORK_EAVESDROP は、送信されたデータの機密性を保護するよう OS を設定する能力を O.MANAGEMENT が提供するため、これによって対抗される。
T.LOCAL_ATTACK	O.INTEGRITY	対策方針 O.INTEGRITY は、プラットフォーム上の他のソフトウェアによる攻撃に関して TOE を弱体化させるメカニズムの使用に対する保護を提供する。
T.LIMITED_PHYSICAL_ACCESS	O.PROTECTED_STORAGE	対策方針 O.PROTECTED_STORAGE は、TOE によって利用される物理的なストレージへアクセスしようとする許可されない試行に対する保護を提供する。
A.PLATFORM	OE.PLATFORM	運用環境の対策方針 OE.PLATFORM は、A.PLATFORM によって具体化される。
A.PROPER_USER	OE.PROPER_USER	運用環境の対策方針 OE.PROPER_USER は、A.PROPER_USER によって具体化される。
A.PROPER_ADMIN	OE.PROPER_ADMIN	運用環境の対策方針 OE.PROPER_ADMIN は、A.PROPER_ADMIN によって具体化される。

5. セキュリティ要件

本章では、OS によって満たされなければならないセキュリティ要件を記述する。これらの要件は、 [CC] パート 2 からの機能コンポーネントと、パート 3 からの保証コンポーネントによって構成される。以下の表記が用いられる：

- **詳細化**操作 (**太字テキスト**によって示される)：要件に詳細を付け加え、さらに要件を制限するために用いられる。
- **選択** (*イタリック体テキスト*によって示される)：要件のステートメントに [CC] によって提供される 1 つ以上の選択肢を選択するために用いられる。
- **割付**操作 (*イタリック体テキスト*によって示される)：は、例えばパスワード長のように、まだ規定されていないパラメタへ特定の値を割り付けるために用いられる。大括弧の中に示す値は割付を示す。
- **繰返し**操作：括弧内の数字で識別される (例、「(1)」)

5.1 セキュリティ機能要件

本セクションに含まれるセキュリティ機能要件は、情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1 改定第 4 版のパート 2 から導出されたものに、拡張機能コンポーネントを追加したものである。

5.1.1 暗号サポート (FCS)

FCS_CKM.1 暗号鍵の生成

FCS_CKM.1.1

OS は、以下に特定される暗号鍵生成アルゴリズムに従って非対称暗号鍵を生成しなければならない [**選択：**

2048 ビット以上の暗号鍵長を用い、以下を満たす ***RSA スキーム：[選択：FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3、ANSI X9.31-1998, Section 4.1]***、

「NIST 曲線」P-256、P-384 及び ***[選択：****P-521、その他の曲線なし]**を用い、以下を満たす* ***ECC スキーム：*** *FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4*

] 。

適用上の注釈：ST 作成者は、鍵確立及びエンティティ認証のために用いられるすべての鍵生成スキームを選択しなければならない。鍵生成が鍵確立のために用いられる場合、FCS_CKM.2.1のスキーム及び選択された暗号プロトコルが選択と一致しなければならない。鍵生成がエンティティ認証のために用いられる場合、公開鍵は X.509v3 証明書と関連付けられることが期待される。

OS が RSA 鍵確立スキームにおいて受信者としてのみふるまう場合、OS が RSA 鍵生成を実装する必要はない。

ANSI X9.31-1998 の選択肢は、本書の将来の版では選択から除かれることになる。現時点では、現行の FIPS PUB 186-4 標準への移行を業界が完了するまでにまだ多少時間がかかるため、この選択は FIPS PUB 186-4 のみに限定されてはいない。

保証アクティビティ

評価者は、OS のサポートする鍵長が TSS に識別されていることを保証する。ST に複数のスキームが規定されている場合、評価者はそれぞれの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 を検査すること。

評価者は、本 PP に定義されるすべての利用について、選択された鍵生成スキーム及び鍵長を用いるように OS を設定する方法について AGD ガイダンスが管理者に対して指示していることを検証すること。

保証アクティビティの注釈：以下のテストには、OS のエンドユーザには通常利用できない開発者環境と開発者ツールを提供することをベンダに要求するかもしれない。

FIPS PUB 186-4 RSA スキームの鍵生成

評価者は、鍵生成テストを用いて OS による RSA 鍵生成の実装を検証する。このテストは、公開鍵検証指数 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。鍵ペア生成では、素数 p 及び q を生成するための 5 とおりの方法 (または手法) を特定している。これには、以下のものが含まれる。

1. *ランダム素数：*
   - *証明可能素数*
   - *確率的素数*
2. *条件付き素数：*
   - *素数 p1、p2、q1、q2、p 及び q を、すべて証明可能素数としなければならない*
   - *素数 p1、p2、q1 及び q2 を証明可能素数とし、p 及び q を確率的素数としなければならない*
   - *素数 p1、p2、q1、q2、p 及び q を、すべて確率的素数としなければならない*

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。これには、1 つ以上の乱数シード値、RSA 鍵の公開鍵指数、及び望ましい鍵長が含まれる。サポートされている鍵長のそれぞれについて、評価者は 25 個の鍵ペアを TSF に生成させなければならない。評価者は、TSF により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 の実装の正確さを検証する。

可能な場合、ランダム確率的素数手法もまた、上述のように既知の良好

な実装に対して検証されるべきである。それ以外の場合、評価者はサポートされている鍵長 nlen のそれぞれについて TSF に 10 個の鍵ペアを生成させ、以下を検証する。

- $n = p \cdot q$,
- *p 及び q が、Miller-Rabin テストに従う確率的素数であること、*
- $GCD(p-1, e) = 1$、
- $GCD(q-1, e) = 1$、
- $2^{16} \leq e \leq 2^{256}$ *かつ e は奇整数、*
- $|p-q| > 2^{nlen/2-100}$、
- $p \geq 2^{nlen/2-1/2}$、
- $q \geq 2^{nlen/2-1/2}$、
- $2^{(nlen/2)} < d < LCM(p-1, q-1)$、
- $e \cdot d = 1 \bmod LCM(p-1, q-1)$。

ANSI X9.31-1998 RSA スキームのための鍵生成

TSF が ANSI X9.31-1998 スキームを実装する場合、評価者は鍵ペアが生成される方法が TSS に記述されていることをチェックして保証する。TSF の実装が ANSI X9.31-1998 に適合していることを示すため、評価者は TSS に以下の情報が含まれることを保証する。

- *TSS には、OS が適合する標準のすべてのセクションが列挙されていなければならない。*
- *TSS に列挙された該当するセクションのそれぞれについて、「しなければならない」でない言明 (即ち、「してはならない」、「すべきである」、及び「すべきでない」) のすべてにおいて、そのようなオプションを OS が実装している場合には、それが TSS に記述されなければならない。含まれる機能が標準においては「してはならない」または「すべきでない」とされている場合には、OS によって実装されたセキュリティ方針に対してこれが悪影響を与えない理由の根拠が TSS に提供されなければならない。*
- *附属書 B の該当するセクションのそれぞれにおいて、「しなければならない」または「すべきである」との言明に関連した機能が欠けている場合には、それが記述されなければならない。*

楕円曲線暗号 (ECC) のための鍵生成

FIPS 186-4 ECC 鍵生成テスト

サポートされている NIST 曲線、即ち 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) に生成させる。プライベート鍵は、承認された乱数ビット生成器 (RBG) を用いて生成されなければならない。正確であることを決定するため、評価者は、既知の良好な実装の公開鍵検証 (PKV) 機能

へ、*生成された鍵ペアを送出すること。*

FIPS 186-4 公開鍵検証 (PKV) テスト

サポートされている NIST 曲線、即ち 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、うち 5 個の公開鍵を不正な値となるよう改変し、残り 5 個を未改変の (即ち、正しい) 値のままにすること。評価者は、これに応じた 10 個の合格/不合格の値を取得すること。

FCS_CKM.2　暗号鍵確立

FCS_CKM.2.1

OS は、以下に特定される鍵確立手法に従って暗号鍵確立を行わなければならない：

RSA ベースの鍵確立スキームであって、以下を満たすもの：NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography”及び [**選択：**

> ***楕円曲線ベースの鍵確立スキーム****であって、以下を満たすもの：NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”、*
>
> *その他のスキームなし*

] 。

適用上の注釈：ST 作成者は、選択された暗号プロトコルに用いられるすべての鍵確立スキームを選択しなければならない。FCS_TLSC_EXT.1は、RSA ベースの鍵確立スキームを用いる暗号スイートを要求する。

RSA ベースの鍵確立スキームは、NIST SP 800-56B のセクション 9 に記述されている。しかし、セクション 9 は SP 800-56B の他のセクションの実装に依存する。OS が RSA 鍵確立スキームにおいて受信者としてふるまう場合、OS が RSA 鍵生成を実装する必要はない。

鍵確立スキームに用いられる楕円曲線は、FCS_CKM.1.1に特定される曲線と相関しなければならない。

保証アクティビティ

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

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

保証アクティビティの注意：以下のテストには、工場製品には通常含まれないツールを評価者へ提供するテストプラットフォームへのアクセスを、開発者が提供することが要求される。

鍵確立スキーム

評価者は、以下から該当するテストを用いて、OS によってサポートされる鍵確立スキームの実装を検証する。

SP800-56A 鍵確立スキーム

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 OS の実装を検証する。各鍵共有スキーム向けのこれらの検証テストは、勧告中の仕様に従った鍵共有スキームのコンポーネントが OS 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、離散対数暗号 (DLC) プリミティブ (共有秘密の値 Z) の計算と、鍵導出関数 (KDF) による導出鍵材料 (DKM) の計算が含まれる。鍵確認がサポートされる場合、評価者はまた以下に記述されるテスト手順を用いて、鍵確認のコンポーネントが正しく実装されていることも検証する。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

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

評価者は、DKM、対応する OS の公開鍵 (静的鍵または短期鍵またはその両方)、1 つまたは複数の MAC タグ、及びその他の情報フィールド (OI) や OS 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する。

OS 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する。

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する。

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

検証テスト

検証テストは、相手方の有効及び無効な鍵共有結果を、鍵確認と共

に、または鍵確認なしで、認識する OS の能力を検証する。このテストを実施するため評価者は、SP800-56A 鍵共有実装に含まれるサポートする暗号機能のリストを取得し、どのエラーを OS が認識可能であるべきかを決定する。評価者は、ドメインパラメタ値または NIST 認可曲線、評価者の公開鍵、OS の公開鍵／プライベート鍵ペア、MAC タグ、及びその他の情報や OS 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 30 個のテストベクタのセットを生成する。

評価者はテストベクタの一部にエラーを注入し、以下のフィールドが不正であるために生じる無効な鍵共有結果を OS が認識することをテストする：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 OS 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 OS の静的プライベート鍵へ個別にエラーを注入し、公開鍵検証機能または部分的な鍵検証機能 (ECC のみ)、またはその両方におけるエラーを OS が検出することをも保証する。少なくとも 2 個のテストベクタは未変更のままでなければならず、したがって有効な鍵共有結果をもたらすべきである (これらは合格すべきである)。

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

SP800-56B 鍵確立スキーム

評価者は、OS が RSA ベースの鍵確立スキームについて送信者、受信者、またはその両方としてふるまうか TSS に記述されていることを検証する。

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

このテストを行うために評価者は、OS 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する。サポートされている鍵確立スキームとそのオプション (サポートされている場合には鍵確認ありまたはなし、鍵確認がサポートされている場合にはサポートされている鍵確認 MAC 関数のそれぞれ、そして KTS-OAEP がサポートされている場合にはサポートされているマスク生成関数のそれぞれ) の組み合わせのそれぞれについて、試験者は 10 セットのテストベクタを生成しなければならない。各テストベクタには RSA プライベート鍵、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 Mac 鍵及び Mac タグ、そして出力された暗号文が含まれなければならない。テストベクタのそれぞれについて、評価者は同一の入力 (鍵確認が組み込まれている場合、通常の操作で用いられるランダムに生成された Mac 鍵の代わりに、テストベクタからの Mac 鍵が使われなければならない)を用いて OS 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。

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

このテストを行うために評価者は、OS 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する。サポートされている鍵確立スキームとそのオプション (サポートされている場合には鍵確認ありまたはなし、鍵確認がサポートされている場合にはサポートされている鍵確認 MAC 関数のそれぞれ、そして KTS-OAEP がサポートされている場合にはサポートされているマスク生成関数のそれぞれ) の組み合わせのそれぞれについて、試験者は 10 セットのテストベクタを生成しなければならない。各テストベクタには RSA プライベート鍵、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 Mac タグ、そして出力された暗号文が含まれなければならない。テストベクタのそれぞれについて、評価者は OS 上で鍵確立復号操作を行い、出力された平文鍵材料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する。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 Mac タグがテストベクタ中の Mac タグと同等であることを保証する。

評価者は、OS 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する。NIST Special Publication 800-56B に従い、出力された、またはロギングされたエラーメッセージの内容を通しても、またはタイミングの変更を通しても、OS は発生した具体的なエラーを開示してはならない。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別個に計画された暗号文の値を作成し、復号試行結果のそれぞれがエラーとなることを保証し、そして任意の出力された、またはロギングされたエラーメッセージが互いに同一であることを保証する。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別個に計画された暗号文の値を作成し、復号試行結果のそれぞれがエラーとなることを保証し、そして任意の出力された、またはロギングされたエラーメッセージが互いに同一であることを保証する。

FCS_CKM_EXT.3　暗号鍵の破棄

FCS_CKM_EXT.3.1

OS は、以下の規定された暗号鍵破棄手法に従って暗号鍵を破棄しなければならない [**選択：**

*揮発性メモリについては、 [**選択：***TSF の RBG を用いた疑似ランダムパタンからなる、ゼロからなる*] 単一直接上書きと、それに引き続く読み出し検証によって破棄が実行されなければならない。上書き*

されたデータの読み出し検証が失敗した場合、このプロセスが再び繰り返されなければならない。、

不揮発性 EEPROM については、(FCS_RBG_EXT.1に特定されるように) TSF の RBG を用いた疑似ランダムパタンからなる単一直接上書きと、それに引き続く読み出し検証によって破棄が実行されなければならない。上書きされたデータの読み出し検証が失敗した場合、このプロセスが再び繰り返されなければならない。、

*不揮発性フラッシュメモリについては、[**選択：**ゼロからなる単一直接上書き、ブロック消去] とそれに引き続く読み出し検証によって破棄が実行されなければならない。上書きされたデータの読み出し検証が失敗した場合、このプロセスが再び繰り返されなければならない。、*

EEPROM とフラッシュメモリ以外の不揮発性メモリについては、毎回書込み前に変更されるランダムパタンで 3 回以上上書きすることによって破棄が実行されなければならない。

] 。

適用上の注釈：上述のクリアは、各中間ストレージ領域に、その鍵が別の場所へ転送された際、適用される。

保証アクティビティ

評価者は、鍵材料の各種別が、その生成元及びストレージの場所を含めて TSS に列挙されていることをチェックして保証する。評価者は、鍵材料の各種別がいつクリアされるか、TSS に記述されていることを検証する。ソフトウェア鍵クリア状況のそれぞれについて、評価者は以下のテストを繰り返す。

- ***テスト 1：**評価者は、TOE 及び計測機能を備えた TOE ビルドに適切な専用の運用環境と開発ツール (デバッガ、シミュレータなど) の組み合わせを利用して、鍵 (その鍵に関する通常の暗号処理中に TOE によって内部的に作成される可能性のある鍵の中間コピーのすべてを含む) が正しくクリアされることをテストする。ソフトウェア中の暗号 TOE 実装は、デバッガの下でロード及び行使され、そのようなテストが行われなければならない。評価者は、TOE によって永続的に暗号化される鍵の中間コピーを含め、クリア対象となる鍵のそれぞれについて、以下のステップを実行する：*
    1. *計測機能を備えた TOE ビルドをデバッガへロードする。*
    2. *クリア対象となる TOE 内の鍵の値を記録する。*
    3. *#1 の鍵に関する通常の暗号処理を TOE に行わせる。*
    4. *TOE に鍵をクリアさせる。*
    5. *TOE に実行を停止させるが、終了はさせない。*

6. *TOE に、TOE の全メモリフットプリントをバイナリファイルへダンプさせる。*

7. *#4 で作成されたバイナリファイルの内容から、#1 の既知の鍵の値のインスタンスを検索する。*

このテストは、ステップ#7 で#1 の鍵のコピーが見つからなかった場合に成功し、それ以外の場合に失敗する。

評価者はこのテストを、暗号化された形態で永続するものを含めたすべての鍵に関して行い、中間コピーがクリアされることを保証する。

FCS_COP.1(1)　暗号操作―暗号化／復号

FCS_COP.1.1(1)

OS は、以下の特定された暗号アルゴリズム

- AES-XTS (NIST SP 800-38E に定義) モード；
- AES-CBC (NIST SP 800-38A に定義) モード；
- AES-CCMP (FIPS PUB 197、NIST SP 800-38C 及び IEEE 802.11-2012 に定義)

及び [**選択：**

AES 鍵ラッピング (KW) (NIST SP 800-38F に定義)、

パディング付 AES 鍵ラッピング (KWP) (NIST SP 800-38F に定義)、

AES-GCM (NIST SP 800-38D に定義)、

AES-CCM (NIST SP 800-38C に定義)、

AES-CCMP-256 (NIST SP800-38C 及び IEEE 802.11ac-2013 に定義)、

AES-GCMP-256 (NIST SP800-38D 及び IEEE 802.11ac-2013 に定義)、

その他のモードなし

] 及び暗号鍵サイズ 128 ビット及び 256 ビットに従ってデータの暗号化／復号サービスを行わなければならない。

適用上の注釈：最初の選択については、ST 作成者は AES が動作する 1 つまたは複数のモードを選択すべきである。第 2 の選択については、ST 作成者はこの機能によってサポートされる鍵長を選択すべきである。128 ビットの鍵長は、FCS_TLSC_EXT.1及び FCS_CKM.1への適合のため、これらが選択されている場合に要求される。

保証アクティビティ

評価者は、要求されるモード及び鍵長に OS を設定するために必要とされる指示が AGD 文書に含まれていることを検証する。評価者は、特定されるすべての指示を実行し、OS を適切な状態に設定する。評価者は、OS 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う：

AES-CBC 既知解テスト

既知解テスト (KAT) には、以下に記述される 4 つがある。すべての KAT において、平文、暗号文、及び IV の値は 128 ビットのブロックとしなければならない。各テストの結果は、直接評価者によって、または実装者へ入力を供給しその結果を受領することによって取得されてもよい。正確さを決定するため、評価者は、結果の値を、既知の良好な実装へ同一の入力を与えることによって得られた値と比較する。

- *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する。うち 5 個の平文の値は 128 ビットのすべてゼロの鍵で暗号化されなければならず、それ以外の 5 個は 256 ビットのすべてゼロの鍵で暗号化されなければならない。AES-CBC の復号機能をテストするため、評価者は 10 個の暗号文の値を入力として AES-CBC 復号を用いて、暗号化と同一のテストを行う。*
- *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する。うち 5 個の鍵は 128 ビットの鍵とし、それ以外の 5 個は 256 ビットの鍵としなければならない。AES-CBC の復号機能をテストするため、評価者はすべてゼロの暗号文の値を入力として AES-CBC 復号を用いて、暗号化と同一のテストを行う。*
- *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する。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、第 2 のセットは 256 個の 256 ビットの鍵からなるものとする。[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。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する。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、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する。[1,N] の範囲の i について、各セットの鍵 i の左端の i ビットは 1、右端の N-i ビットは 0 としなければならない。各ペアの暗号文の値は、それに対応する鍵で復号された際にすべてゼロの平文が得られるような値としなければならない。*
- *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) を取得する。[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 128-i ビットは 0 としなければならない。

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

AES-CBC 複数ブロックメッセージテスト

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り、暗号化機能をテストする。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択し、試験すべきモードを用いて、選択した鍵と IV によりメッセージを暗号化する。暗号文は、既知の良好な実装を用いて同一の鍵と IV により同一の平文メッセージを暗号化した結果と比較されなければならない。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り、各モードについて復号機能をテストする。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択し、試験すべきモードを用いて選択した鍵と IV によりメッセージを復号する。平文は、既知の良好な実装を用いて同一の鍵と IV により同一の暗号文メッセージを復号した結果と比較されなければならない。

AES-CBC モンテカルロテスト

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する。これらのうち 100 個は 128 ビットの鍵を用いるものとし、それ以外の 100 個は 256 ビットの鍵を用いなければならない。平文と IV の値は、128 ビットのブロックとしなければならない。3 つ組のそれぞれについて、以下のように 1000 回の反復処理が実行されなければならない。

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

1000 回目の反復処理において計算された暗号文 (即ち、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り 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。

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、復号機能をテストする。

AES-GCM モンテカルロテスト

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する。

- *128 ビット及び256 ビットの鍵*
- *2 とおりの平文の長さ。一つの平文の長さは、サポートされる場合、128 ビットのゼロ以外の整数倍としなければならない。他の平文の長さは、サポートされる場合、128 ビットの整数倍であってはならない。*
- *3 とおりのAAD 長。1 つのAAD 長は、サポートされる場合、ゼロとしなければならない。1 つの別のAAD 長は、サポートされる場合、128 ビットのゼロ以外の整数倍としなければならない。残りの1 つのAAD 長は、サポートされる場合、128 ビットの整数倍であってはならない。*
- *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。*

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 認証付き暗号化から得られた暗号文とタグを取得する。サポートされているタグ長はそれぞれ、10 個のセットにつき少なくとも 1 度はテストされなければならない。IV の値は、それが既知である限り、評価者によって供給されても、テストされている実装によって供給されてもよい。

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する。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。

各テストの結果は、直接評価者によって、また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、取得されてもよい。正しさを決定するため、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する。

AES-CCM テスト

評価者は、以下の入力パラメタ長とタグ長のそれぞれについて、AES-CCM の生成―暗号化及び復号―検証機能をテストする。

- *128 ビット及び256 ビットの鍵*
- *2 とおりのペイロード長。一方のペイロード長は、ゼロバイト以上のサポートされる最も短いペイロード長としなければならない。他方のペイロード長は、32 バイト (256 ビット) 以下のサポートされる最も長いペイロード長としなければならない。*
- *2 または3 とおりの関連データ長。1 つの関連データ長は、サ*

ポートされる場合、0 としなければならない。1 つの関連データ長は、ゼロバイト以上でサポートされる最も短い関連データ長としなければならない。1 つの関連データ長は、32 バイト (256 ビット) 以下でサポートされる最も長い関連データ長としなければならない。実装が 2 16 バイトの関連データ長をサポートする場合、216 バイトの関連データ長がテストされなければならない。

- *ノンス長。7 バイトから 13 バイトまで (上端及び下端を含む) のサポートされるすべてのノンス長がテストされなければならない。*
- *タグ長。4、6、8、10、12、14 及び 16 バイトのサポートされるすべてのタグ長がテストされなければならない。*

AES-CCM の生成―暗号化機能をテストするために、評価者は以下の 4 つのテストを行う。

- ***テスト 1 :** サポートされる鍵及び関連データ長さのそれぞれについて、またサポートされるペイロード、ノンス及びタグ長のいずれかについて、評価者は 1 つの鍵の値、1 つのノンスの値及び 10 ペアの関連データ及びペイロードの値を供給し、得られた暗号文を取得する。*
- ***テスト 2 :** サポートされる鍵及びペイロード長のそれぞれについて、またサポートされる関連付データ、ノンス及びタグ長のいずれかについて、評価者は 1 つの鍵の値、1 つのノンスの値及び 10 ペアの関連データ及びペイロードの値を供給し、得られた暗号文を取得する。*
- ***テスト 3 :** サポートされる鍵及びノンス長のそれぞれについて、またサポートされる関連データ、ペイロード及びタグ長のいずれかについて、評価者は 1 つの鍵の値及び 10 個の関連データ、ペイロード及びノンスの値の 3 つ組を供給し、得られた暗号文を取得する。*
- ***テスト 4 :** サポートされる鍵及びタグ長のそれぞれについて、またサポートされる関連データ、ペイロード及びノンス長のいずれかについて、評価者は 1 つの鍵の値、1 つのノンスの値及び 10 ペアの関連データ及びペイロードの値を供給し、得られた暗号文を取得する。*

上記のテストのそれぞれの正しさを決定するため、評価者は、暗号文を、既知の良好な実装による同一の入力の生成―暗号化の結果と比較する。

AES-CCM の復号―検証機能をテストするため、サポートされる関連データの長さ、ペイロード長、ノンス長及びタグ長のそれぞれについて、評価者は 1 つの鍵の値と 15 個のノンス、関連データ及び暗号文の 3 つ組を供給し、復号されたペイロードと共に不合格結果または合格結果のいずれかを取得しなければならない。評価者は、15 組のセットにつき、不合格となるはずの 10 個の組と合格となるはずの 5 個の組とを供

給する。

さらに、評価者は IEEE 802.11-02/362r6 文書“Proposed Test vectors for IEEE 802.11 TGi”(2002 年 9 月 10 日付) のセクション 2.1「AES-CCMP Encapsulation Example」及びセクション 2.2「Additional AES CCMP Test Vectors」のテストを用いて、AES-CCMP の IEEE 802.11-2007 実装をさらに検証する。

AES-GCM テスト

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する。

- *128 ビット及び 256 ビットの鍵*
- *2 とおりの平文の長さ。1 つの平文の長さは、サポートされる場合、128 ビットのゼロ以外の整数倍としなければならない 。残りの平文の長さは、サポートされる場合、128 ビットの整数倍であってはならない。*
- *3 とおりの AAD 長。1 つの AAD 長は、サポートされる場合、0 としなければならない。別の 1 つの AAD 長は、サポートされる場合、128 ビットのゼロ以外の整数倍としなければならない。残りの 1 つの AAD 長は、サポートされる場合、128 ビットの整数倍であってはならない。*
- *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。*

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 認証付き暗号化から得られた暗号文の値とタグを取得する。サポートされているタグ長はそれぞれ、10 個のセットにつき少なくとも 1 度はテストされなければならない。IV の値は、それが既知である限り、評価者によって供給されても、テストされている実装によって供給されてもよい。

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する。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。

各テストの結果は、直接評価者によって、また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、取得されてもよい。正しさを決定するため、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する。

XTS-AES テスト

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、XTS-AES の暗号化機能をテストする。

- *256 ビット (AES-128 について) 及び 512 ビット (AES-256 に*

ついて) の鍵

- *3 とおりのデータユニット (即ち、平文) の長さ。データユニット長の 1 つは、128 ビットのゼロ以外の整数倍としなければならない (サポートされる場合)。データユニット長の 1 つは、128 ビットの整数倍としなければならない (サポートされる場合)。データユニット長の 3 番目は、サポートされる最も長いデータユニット長か 216 ビットの、いずれか小さいほうとしなければならない。*

100 個の (鍵、平文及び128 ビットのランダムな tweak 値の) 3 つ組のセットを用いて、XTS-AES 暗号化から得られた暗号文を取得する。

評価者は、実装によってサポートされている場合、tweak 値の代わりにデータユニットシーケンス番号を供給してもよい。データユニットシーケンス番号は、0 から 255 の間の 10 進数であって、実装によって内部的に tweak 値へ変換されるものである。

評価者は、暗号化と同一のテストを用い、平文の値を暗号文の値と置き換え、XTS-AES 暗号化を XTS-AES 復号と置き換えて、XTS-AES 復号機能をテストする。

AES 鍵ラップ (AES-KW) 及びパディング付き鍵ラップ (AES-KWP) テスト

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-KW の認証付き暗号化機能をテストする。

- *128 ビット及び256 ビットの鍵暗号化鍵 (KEK)*
- *3 とおりの平文の長さ。平文の長さの 1 つは、セミブロック 2 個 (128 ビット) としなければならない。平文の長さの 1 つは、セミブロック 3 個 (192 ビット) としなければならない。データユニット長の 3 番目は、セミブロック 64 個 (4096 ビット) 以下でサポートされる最も長い平文の長さとしなければならない。*

100 個の鍵と平文のペアのセットを用いて、AES-KW 認証付き暗号化から得られた暗号文を取得する。正しさを決定するため、評価者は既知の良好な実装の AES-KW 認証付き暗号化機能を利用する。

評価者は、認証付き暗号化と同一のテストを用い、平文の値を暗号文の値と置き換え、AES-KW 認証付き暗号化を AES-KW 認証付き復号と置き換えて、AES-KW の認証付き復号機能をテストする。

評価者は、AES-KW の認証付き暗号化と同一のテストを用い、以下の変更を 3 とおりの平文の長さに行って、AES-KWP 認証付き暗号化機能をテストする。

- *平文の長さの 1 つは、1 オクテットとする。平文の長さの 1 つは、20 オクテット (160 ビット) としなければならない。*
- *平文の長さの 1 つは、512 オクテット (4096 ビット) 以下でサポートされる最も長い平文の長さとしなければならない。*

評価者は、AES-KWP 認証付き暗号化と同一のテストを用い、平文の値

を暗号文の値と置き換え、AES-KWP 認証付き暗号化を AES-KWP 認証付き復号と置き換えて、AES-KWP の認証付き復号機能をテストする。

FCS_COP.1(2)　暗号操作―ハッシュ

FCS_COP.1.1(2)

OS は、特定されたアルゴリズム SHA-1 及び [**選択：**

SHA-256、

SHA-384、

SHA-512、

その他のアルゴリズムなし

] 及びメッセージダイジェストサイズ 160 及び [選択：

256、

384、

512、

その他のメッセージダイジェストサイズなし

] ビットに従い、以下：FIPS Pub 180-4 を満たす暗号ハッシュサービスを行わなければならない。

適用上の注釈：NIST SP 800-131A に従い、SHA-1 によるディジタル署名の生成はもはや許可されず、また SHA-1 によるディジタル署名の検証は、これらの署名の受容にリスクが存在し得るため、強く非推奨とされる。

SHA-1 は現在、FCS_TLSC_EXT.1及び、選択に応じて、FCS_DTLS_EXT.1 に適合するため要求されている。ベンダには、SHA-2 ファミリをサポートする更新されたプロトコルの実装が強く推奨される。更新されたプロトコルがサポートされるまで、本 PP は SP 800-131A に適合した SHA-1 の実装を許可する。

本要件の意図は、ハッシュ関数を特定することである。ハッシュの選択は、メッセージダイジェスト長の選択をサポートしなければならない。ハッシュの選択は、用いられるアルゴリズムの全体的な強度と一貫しているべきである。

保証アクティビティ

評価者は、ハッシュ機能と他のアプリケーション暗号機能 (例、ディ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する。

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。即ち、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。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う。

以下のテストには、アプリケーション製品には通常見られないツールを評価者へ提供するテストアプリケーションへのアクセスを、開発者が提供することが要求される。

- ***テスト 1：****ショートメッセージテスト (ビット指向モード) — 評価者は m+1 個のメッセージからなる入力セットを生成する。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、疑似乱数的に生成されなければならない。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。*
- ***テスト 2：****ショートメッセージテスト (バイト指向モード) — 評価者は m/8+1 個のメッセージからなる入力セットを生成する。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、疑似乱数的に生成されなければならない。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。*
- ***テスト 3：****選択されたロングメッセージテスト (ビット指向モード) — 評価者は m 個のメッセージからなる入力セットを生成する。ここで m はハッシュアルゴリズムのブロック長である。i 番目のメッセージの長さは 512 + 99·i となる (ここで $1 \le i \le m$)。メッセージの本文は、疑似乱数的に生成されなければならない。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。*
- ***テスト 4：****選択されたロングメッセージテスト (バイト指向モード) — 評価者は m/8 個のメッセージからなる入力セットを生成する。ここで m はハッシュアルゴリズムのブロック長である。i 番目のメッセージの長さは 512 + 8·99·i となる (ここで $1 \le i \le m/8$)。メッセージの本文は、疑似乱数的に生成されなければならない。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。*
- ***テスト 5：****疑似乱数的に生成されたメッセージテスト — 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値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機能によって作り出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。

FCS_COP.1(3) 暗号操作―署名

FCS_COP.1.1(3)

OS は、以下の特定された暗号アルゴリズムに従って、暗号署名サービス(生成及び検証) を行わなければならない [**選択：**

*2048 ビット以上の暗号鍵長を用い、以下を満たす **RSA スキーム**：FIPS PUB 186-4, "Digital Signature Standard (DSS)"、セクション 4、*

*「NIST 曲線」P-256、P-384 及び [**選択：**P-521、その他の曲線なし] を用い、以下を満たす **ECDSA スキーム**： FIPS PUB 186-4, "Digital Signature Standard (DSS)" セクション 5*

] 。

適用上の注釈：ST 作成者は、ディジタル署名を行うために実装されたアルゴリズムを選択すべきである。2 つ以上のアルゴリズムが利用できる場合、本要件はその機能を特定するために繰り返されるべきである。選択されたアルゴリズムについて、ST 作成者は適切な割付／選択を行ってそのアルゴリズムに実装されるパラメタを特定すべきである。RSA 署名生成及び検証は現在、FCS_TLSC_EXT.1に適合するため要求されている。

保証アクティビティ

評価者は、ST 中の選択に基づいて以下のアクティビティを行う。

以下のテストには、アプリケーション製品には通常見られないツールを評価者へ提供するテストアプリケーションへのアクセスを、開発者が提供することが要求される。

ECDSA アルゴリズムテスト

- ***テスト 1：**ECDSA FIPS 186-4 署名生成テスト。サポートされている NIST 曲線 (即ち、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 を取得する。正しさを決定するため、評価者は既知の良好な実装の署名検証機能を利用する。*
- ***テスト 2：**ECDSA FIPS 186-4 署名検証テスト。サポートされている NIST 曲線 (即ち、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) を変更する。評価者は、5 つの応答で合格が示され、5 つの応答で不合格が示されることを検証する。

RSA 署名アルゴリズムテスト

- ***テスト 1：****署名生成テスト。評価者は、署名生成テストを用いて OS による RSA 署名生成の実装を検証する。このテストを行うために評価者は、TSF 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、信頼される参照実装から 10 個のメッセージを生成または取得しなければならない。評価者は、OS に自分のプライベート鍵と modulus の値を用いてこれらのメッセージへ署名させる。評価者は、既知の良好な実装及び関連付けられた公開鍵を用いて署名を検証することによって、TSF の署名の正しさを検証する。*
- ***テスト 2：****署名検証テスト。評価者は、署名検証テストを行って、相手方の有効及び無効な署名を認識する OS の能力を検証する。評価者は、公開鍵、e、メッセージ、IR フォーマット、または署名、またはこれらのうち 2 つ以上にエラーを注入することによって、署名検証テスト中に作成されたテストベクタへエラーを注入する。評価者は、それぞれの署名を検証する際に OS が失敗を検出することを検証する。*

FCS_COP.1(4)　暗号操作―鍵付きハッシュによるメッセージ認証

FCS_COP.1.1(4)

OS は、以下の特定された暗号アルゴリズム [**選択：**

SHA-1、

SHA-256、

SHA-384、

SHA-512、

その他のアルゴリズムなし

] 鍵長が [**割付：**HMAC に用いられる (ビット単位の) 鍵長]、そしてメッセージダイジェストのサイズが [**選択：***160*、*256*、*384*、*512*、*その他のサイズなし*] ビットの、以下： FIPS Pub 198-1 *The Keyed-Hash Message Authentication Code* 及び FIPS Pub 180-4 *Secure Hash Standard* を満たすものに従って、鍵付きハッシュによるメッセージ認証を行わなければならない。

適用上の注釈：本要件の意図は、OS によって用いられるさまざまな暗号プロトコル (例、高信頼チャネル) の鍵確立の目的に用いられる鍵付きハッシュによるメッセージ認証機能を特定することである。ハッシュの選択は、メッセージダイジェストサイズの選択をサポートしなければならない。ハッシュの選択は、FCS_COP.1(1) に用いられるアルゴリズムの全体的な強度と一貫しているべきである。SHA-256 を用いる HMAC (HMAC-

SHA-256) は本要件に選択可能な暗号スイートとして列挙されているが、FCS_TLSC_EXT.1によって適合 OS がそれを実装することは実質的に必須とされている。

SHA-1 は現在、FCS_TLSC_EXT.1及び、選択に応じて、FCS_DTLS_EXT.1 に適合するため要求されている。SHA-1 は現在 FCS_TLSC_EXT.1に適合するため要求されているが、すでに廃止されており、TLS 及び DTLS 以外の目的には使用されるべきでない。

保証アクティビティ

評価者は、ST 中の選択に基づいて以下のアクティビティを行う。

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する。各セットは、1 つの鍵とメッセージデータから構成されるものとする。評価者は、テストデータのこれらのセットについて OS に HMAC タグを生成させる。得られた MAC タグは、既知の良好な実装を用いて同一の鍵と IV によって生成された HMAC タグと比較されなければならない。

FCS_RBG_EXT.1　乱数ビット生成

FCS_RBG_EXT.1.1

OS は、以下に従ってすべての決定論的乱数ビット生成 (DRBG) サービスを行わなければならない [**選択、少なくとも 1 つ：**

*[**選択：**Hash_DRBG (任意)、HMAC_DRBG (任意)、CTR_DRBG (AES)] を用いる NIST Special Publication 800-90A、*

AES を用いる FIPS Pub 140-2 附属書 C：X9.31 附属書 2.4

] 。

適用上の注釈：ST 作成者は RBG サービスが適合する標準 (SP 800-90A または FIPS 140-2 附属書 C のいずれか) を選択すべきである。

SP 800-90A には、3 つの異なる乱数生成手法が含まれる。これらはそれぞれ、基盤となる暗号プリミティブ (ハッシュ関数／暗号) に依存している。ST 作成者は利用される関数を選択し (SP 800-90A が選択されている場合)、要件または TSS に用いられる具体的な基盤となる暗号プリミティブが含まれるようにする。特定されたハッシュ関数 (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) はいずれも Hash_DRBG または HMAC_DRBG に許可されるが、CTR_DRBG には AES ベースの実装のみが許可される。

FIPS Pub 140-2 の附属書 C については、現在のところ NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4, Section 3 に記述される手法のみが有効であることに注意されたい。この DRBG の利用は 2015 年以降、NIST SP 800-131A に従って禁止される。PP は、これを反映して更新されることになる。しかし、開発者はできるだけ早く、この DRBG からの移行を開始すべきである。

保証アクティビティ

評価者は、RBG が適合する標準に従って、以下のテストを行う。

FIPS 140-2 附属書C に適合する実装

本セクションに含まれるテストの参照情報は、The Random Number Generator Validation System (RNGVS) である。評価者は、以下の2 つのテストを実施する。「期待値」は、正しいことが知られているアルゴリズムの参照実装によって作成されることに注意されたい。正しさの証明は、各スキームに任される。

- ***テスト 1：****評価者は、可変シード値テストを行う。評価者は (Seed, DT) ペア (それぞれ 128 ビット) の 128 個のセットを TSF の RBG 機能に提供する。また評価者は、128 ペアの (Seed, DT) すべてについて一定である (AES アルゴリズムに適切な長さの) 鍵も提供する。DT の値は、各セットについて1 ずつ増やされる。シードの値は、セットの中で繰り返されてはならない。評価者は、TSF によって返される値が期待値と一致することを保証する。*
- ***テスト2：****評価者は、モンテカルロテストを行う。このテストについては、評価者がシード値及び DT の初期値 (それぞれ 128 ビット) を TSF の RBG 機能に提供する。また評価者は、テストを通して一定である (AES アルゴリズムに適切な長さの) 鍵も提供する。次に評価者は、繰返しのたびに DT の値を 1 ずつ増やしながら、そして ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms のセクション3 に基づく NIST-Recommended Random Number Generator に規定されるように次回の繰返しの際の新たなシード値を作成して、TSF の RBG を 10,000 回呼び出す。評価者は、得られた 10,000 番目の値が期待値と一致することを保証する。*

NIST Special Publication 800-90A に適合する実装

- ***テスト1：****評価者は、RNG 実装の 15 回の試行を行う。RNG が設定可能な場合、評価者は各設定について15 回の試行を行う。また評価者は、RNG 機能を設定するための適切な指示が操作ガイダンスに含まれていることも確認する。*

  RNG が有効な予測困難性を持つ場合、各回の試行は (1) DRBG をインスタンス化し、 (2) ランダムなビットの最初のブロックを生成し、 (3) ランダムなビットの 2 番目のブロックを生成し、(4) 非インスタンス化する、という手順になる。評価者は、ランダムなビットの 2 番目のブロックが期待された値であることを検証する。評価者は、各試行に8 つの入力値を生成する。最初はカウント (0～14) である。次の 3 つはインスタンス化操作のエントロピー入力とノンス、そして Personalization String である。次の2 つは、最初の生成呼び出しへの追加的入力とエントロピー入力である。最後の2 つは、2 番目の生成呼出しへの追加的入力とエントロピー入力である。これらの値は、ランダムに生成される。「ランダムなビットのひとつのブロックを生成」とは、返されるビット数が (NIST SP 800-90A に定義される) Output Block Length と等しい

ランダムなビットを生成することを意味する。

RNG が予測困難性を持たない場合、各回の試行は (1) DRBG をインスタンス化し、 (2) ランダムなビットの最初のブロックを生成し、 (3) シード値を再供給し、 (4) ランダムなビットの 2 番目のブロックを生成し、 (5) 非インスタンス化する、という手順になる。評価者は、ランダムなビットの 2 番目のブロックが期待された値であることを検証する。評価者は、各試行に 8 つの入力値を生成する。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、シード値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。

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。*

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

***追加の入力:** 追加の入力のビット長は、Personalization String の長さと同一のデフォルトと制限を持つ。*

FCS_RBG_EXT.1.2

OS によって利用される決定論的 RBG は、 [**選択：**

ソフトウェアベースのノイズ源、

プラットフォームベースのノイズ源

] であって、最小で [**選択：**

128 ビット、

256 ビット

] の、鍵とそれが生成するハッシュとの (NIST SP 800-57 による) セキュリティ強度の大きいほうと少なくとも等しいエントロピーを持つものか

らエントロピーを蓄積するエントロピー源によって、シード値が供給されなければならない。

適用上の注釈 : 本要件中の最初の選択について、DRBG への入力として追加的なノイズ源が用いられる場合、ST 作成者は『ソフトウェアベースのノイズ源』を選択する。

第 2 の選択については、ST 作成者は ST に含まれるアルゴリズムの中で最も大きなセキュリティ強度に対応するエントロピーの適切なビット数を選択する。セキュリティ強度は、NIST SP 800-57A の表 2 及び 3 に定義されている。例えば、実装に 2048 ビット RSA (セキュリティ強度 112 ビット)、AES 128 (セキュリティ強度 128 ビット)、そして HMAC-SHA-256 (セキュリティ強度 256 ビット) が含まれている場合、ST 作成者は 256 を選択することになる。

保証アクティビティ

附属書 E 及び エントロピー証拠資料と評定の附属書に対する明確化 に従って、証拠資料が作成されなければならない (そして評価者はアクティビティを行う)。

将来は、エントロピーの見積もりを検証するために (NIST SP 800-90B に沿った) 具体的な統計的テストが要求されることになる。

FCS_STO_EXT.1　機微なデータの格納

FCS_STO_EXT.1.1

OS は、不揮発性ストレージに保存される機微なデータを暗号化する機能を実装し、この機能を呼び出すためのインタフェースをアプリケーションに提供しなければならない。

適用上の注釈 : 機微なデータは、ST 作成者によって TSS で識別されなければならず、またこれには最低限、クレデンシャルと鍵が含まれる。この機能を呼び出すためのインタフェースは、さまざまな形態を取ることができる : API であってもよいし、単純にファイルとして保存されたクレデンシャルをアクセスするための明確に文書化された慣習であってもよい。

保証アクティビティ

評価者は TSS をチェックして、OS が格納機能を提供するすべての永続的な機微なデータが列挙されていることを保証する。これらの項目のそれぞれについて、評価者はそれが何の目的で利用できるか、及びどのように保存されるか TSS に列挙されていることを確認する。評価者は、そのデータを保護するために用いられる暗号操作が FCS_COP.1(1) に特定されているように行われることを確認する。

また評価者は開発者証拠資料を参照し、アプリケーションがセキュアにクレデンシャルを保存するためのインタフェースが存在することを検証する。

FCS_TLSC_EXT.1　TLS クライアントプロトコル

FCS_TLSC_EXT.1.1

OS は、TLS 1.2 (RFC 5246) を実装し、以下の暗号スイートをサポートしなければならない：

必須の暗号スイート：RFC 5246 で定義される
TLS_RSA_WITH_AES_128_CBC_SHA

オプションの暗号スイート： [**選択：**

RFC 5246 で定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA、

RFC 5246 で定義される
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256、

RFC 5246 で定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA、

RFC 5246 で定義される
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256、

RFC 4492 で定義される
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA、

RFC 5289 で定義される
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256、

RFC 5289 で定義される
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256、

RFC 4492 で定義される
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA、

RFC 5289 で定義される
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384、

RFC 5289 で定義される
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384、

RFC 4492 で定義される
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA、

RFC 5289 で定義される
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256、

RFC 5289 で定義される
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256、

RFC 4492 で定義される
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA、

RFC 5289 で定義される
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384、

RFC 5289 で定義される
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384、

RFC 5246 で定義される TLS_RSA_WITH_AES_128_CBC_SHA256、

RFC 5246 で定義される TLS_RSA_WITH_AES_256_CBC_SHA、

RFC 5246 で定義される TLS_RSA_WITH_AES_256_CBC_SHA256、

その他の暗号スイートなし

] 。

適用上の注釈：評価される構成においてテストされるべき暗号スイートは、本要件によって制限される。ST 作成者は、サポートされるオプションの暗号スイートを選択すべきである；必須スイート以外にサポートされる暗号スイートが存在しない場合には、「その他の暗号スイートなし」が選択されるべきである。テスト環境にあるサーバ上で評価される構成において管理的に使用可能な暗号スイートを制限する必要がある。上記の列挙された Suite B アルゴリズム (RFC 6460) は、実装が望まれるアルゴリズムである。
TLS_RSA_WITH_AES_128_CBC_SHA は、RFC 5246 への適合を保証するために要求される。

これらの要件は、新しい TLS バージョンが IETF により規格化されると見直しが行われる。

ECDHE を使用する任意の暗号スイートが選択される場合、FCS_TLSC_EXT.2.1が要求される。

保証アクティビティ

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すること。評価者は、規定された暗号スイートが本コンポーネントのために列挙されたものを含むことを保証するため、TSS をチェックすること。評価者は、TLS が TSS の記述に適合するように OS を構成するための指示を含むことを保証するため、操作ガイダンスについてもチェックすること。評価者は、以下のテストについても実行すること：

- ***テスト 1：****評価者は、本要件によって規定された暗号スイートのそれぞれを用いて TLS コネクションを確立すること。本コネクションは、より高いレベルのプロトコル確立の一部として、例、EAP セションの一部として、確立されてもよい。テストの意図を満たすには、暗号スイートのネゴシエーション成功を確認すれば十分である；利用される暗号スイート (例えば、暗号アルゴリズムが 128-bit AES であって 256-bit AES でないこと) を識別するために暗号化されたトラフィックの特徴を検査する必要はない。*
- ***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コネクションを確立する試行を行い、コネクションが確立されることを検証する。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、コネクション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。*

- ***テスト 3：****評価者は、TLS コネクションでサーバ選択の暗号スイートと一致しないサーバ証明書を送信すること (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、または ECDSA 暗号スイートのうちの 1 つを使用しているのに RSA 証明書を送信する等。) 評価者は、OS がサーバの証明書ハンドシェイクメッセージを受信後、コネクションを切断することを検証すること。*
- ***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、クライアントがコネクションを拒否することを検証すること。*
- ***テスト 5：****評価者は、トラフィックに対して以下の改変を実行すること：*
  - ***テスト 5.1：****ServerHello のサーバによって選択される TLS バージョンを非サポートの TLS バージョン (例、2 バイトの 03 04 によって表現される 1.3) に変更し、クライアントがコネクションを拒否することを検証する。*
  - ***テスト 5.2：****ServerHello ハンドシェイクメッセージのサーバのノンスの少なくとも 1 バイトを改変し、クライアントが ServerKeyExchange ハンドシェイクメッセージを拒否すること (DHE または ECDHE 暗号スイートを用いる場合) またはクライアントの 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。*
  - ***テスト 5.3：****ServerHello ハンドシェイクメッセージのサーバ選択の暗号スイートを ClientHello ハンドシェイクメッセージで提示されない暗号スイートに改変する。評価者は、クライアントが ServerHello を受信後にコネクションを拒否することを検証する。*
  - ***テスト 5.4：****サーバの KeyExchange ハンドシェイクメッセージの署名ブロックを改変し、クライアントが ServerKeyExchange メッセージ受信後にコネクションを拒否することを検証する。*
  - ***テスト 5.5：****サーバの Finished ハンドシェイクメッセージの 1 バイトを改変し、クライアントが受信時に 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。*
  - ***テスト 5.6：****サーバが Change Cipher Spec メッセージを発行後にサーバから意味不明なメッセージを送信し、クライアントがコネクションを拒否することを検証する。*

FCS_TLSC_EXT.1.2

OS は、提示された識別子が RFC 6125 に従った参照識別子と一致することを検証しなければならない。

適用上の注釈：識別子検証の規則は、RFC 6125 のセクション 6 で記述されている。参照識別子は、利用者によって(例、ウェブブラウザへ URL を入力、またはリンクをクリックして)、設定によって(例、メールサーバまたは認証サーバの名前を設定して)、またはアプリケーションによって(例、API のパラメタ) 確立される。単一の参照識別子の送信元ドメイン及びアプリケーションサービス種別 (例、HTTP、SIP、LDAP) に基づき、クライアントは、証明書のサブジェクト名フィールドのコモン名、及びサブジェクト別名フィールドの (大文字と小文字を区別しない) DNS 名、URI 名、及びサービス名のような、受容可能なすべての参照識別子を確立する。次にクライアントは、このリストのすべての受容可能な参照識別子を TLS サーバ証明書で提示された識別子と比較する。

望ましい検証手法は、DNS 名、URI 名、またはサービス名を用いたサブジェクト別名である。コモン名を用いる検証は、後方互換性の目的で要求される。さらに、サブジェクト名またはサブジェクト別名の IP アドレスの使用のサポートは、ベストプラクティスに反するため非推奨とされるが、実装されてもよい。最後に、クライアントはワイルドカードを用いた参照識別子の構築を避けるべきである。しかし、提示された識別子がワイルドカードを含む場合、クライアントは照合に関するベストプラクティスに従わなければならない; これらのベストプラクティスは、保証アクティビティに取り込まれている。

保証アクティビティ

評価者は、どのタイプの参照識別子がサポートされているか (例、コモン名、DNS 名、URI 名、サービス名、またはその他のアプリケーション特有のサブジェクト別名) 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、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クライアントの手法について TSS に記述されていることを保証すること。評価者は、この記述に、証明書ピンニングが OS によってサポートまたは利用されるかどうか、及びそのやり方が特定されていることを保証すること。

評価者は、TLS での証明書有効性確認の目的で使用される参照識別子を設定するための指示について AGD ガイダンスに含まれていることを検証すること。

評価者は、AGD ガイダンスに従って参照識別子を設定し、TLS コネクションの間、以下のテストを実行すること：

- ***テスト 1：****評価者は、参照識別子と一致するような識別子を、サブジェクト別名 (SAN) にもコモン名 (CN) にも含まないサーバ証明書を提示すること。評価者は、コネクションが失敗することを検証すること。*
- ***テスト 2：****評価者は、参照識別子と一致する CN を含み、SAN 拡張を含むが、参照識別子と一致する識別子を SAN に含まないサーバ証明書を提示すること。評価者は、コネクションが失敗することを検証しなければならない。評価者は、サポートされる SAN の各タイプについてこのテストを繰り返すこと。*
- ***テスト 3：****評価者は、参照識別子と一致する CN を含み、SAN*

拡張を含まないサーバ証明書を提示すること。評価者は、コネクションが成功することを検証すること。

- ***テスト 4：****評価者は、参照識別子と一致しない CN を含むが、SAN と一致する識別子を含むサーバ証明書を提示すること。評価者は、コネクションが成功することを検証すること。*
- ***テスト 5：****評価者は、サポートされる参照識別子の各タイプについて、以下のワイルドカードテストを実行すること：*
  - ***テスト 5.1：****評価者は、提示された識別子の左端のラベルにワイルドカードを含まないサーバ証明書を提示し (例、foo.*.example.com)、コネクションが失敗することを検証すること。*
  - ***テスト 5.2：****評価者は、左端のラベルにワイルドカードを含むがパブリックなサフィックスに先立たないワイルドカードを含む (例、 *.example.com) サーバ証明書を提示する。評価者は、左端に単一のラベルを持つ参照識別子 (例、foo.example.com) を設定し、コネクションが成功することを検証する。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、example.com) を設定し、コネクションが失敗することを検証する。評価者は、左端に 2 つのラベルを持つ参照識別子 (例、bar.foo.example.com) を設定し、コネクションが失敗することを検証する。*
  - ***テスト 5.3：****評価者は、公的ドメイン名 (public suffix)の直前の左端ラベルにワイルドカードを含む (例、*.com) サーバ証明書を提示すること。評価者は、左端に 1 つのラベルを持つ参照識別子 (例、foo.com) を設定し、コネクションが失敗することを検証すること。評価者は、2 つの左端ラベルを持つ参照識別子 (例、bar.foo.com) を設定し、コネクションが失敗することを検証すること。*
- ***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 名及びサービス識別子を設定すること。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、コネクションが成功することを検証すること。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、コネクションが失敗することを検証すること。*
- ***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一致しない証明書を提示し、コネクションが失敗することを検証すること。*

FCS_TLSC_EXT.1.3

OS は、ピア証明書が有効である場合にのみ高信頼チャネルを確立しなければならない。

適用上の注釈: 有効性は、識別子の検証、証明書パス、有効期限、及び RFC 5280 に従う失効状態によって決定される。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ない。

TLS コネクションに関しては、ピア証明書が無効である場合、このチャネルが確立されてはならない。

保証アクティビティ

評価者は、FIA_X509_EXT.1.1 の証明書有効性確認規則が遵守されることを検証するための機能として TLS を使用し、以下の追加のテストを実行しなければならない:

- ***テスト 1:** 評価者は、有効な証明パスのない証明書を使用するピアが認証を失敗することを実証すること。管理ガイダンスを用いて、評価者は、次にピアの証明書有効性確認に必要な 1 つまたは複数の信頼された CA 証明書をロードし、コネクションが成功することを実証すること。評価者は、次に CA 証明書のうちの 1 つを削除し、コネクションが失敗することを示さなければならない。*
- ***テスト 2:** 評価者は、失効された証明書を使用するピアが認証を失敗することを実証すること。*
- ***テスト 3:** 評価者は、有効期限を経過した証明書を使用するピアが認証を失敗することを実証すること。*
- ***テスト 4:** 評価者は、有効な識別子を持たない証明書を使用するピアが認証を失敗しなければならないことを実証すること。*

5.1.2 利用者データ保護 (FDP)

FDP_ACF_EXT.1 利用者データ保護のアクセス制御

FDP_ACF_EXT.1.1

OS は、特権のない利用者が他の利用者によって所有されるファイル及びディレクトリへアクセスすることを禁止できるようなアクセス制御を実装しなければならない。

適用上の注釈: アクセス制御による効果的な保護は、システム構成にも依存するかもしれない。本要件は、例えば、マルチユーザシステムにおける 1 人の利用者によって所有されるファイルやディレクトリを、そのシステムの別の利用者によるアクセスから保護できることを保証するよう設計されている。

保証アクティビティ

評価者は TSS に、OS によって強制されるアクセス制御方針が包括的に記述されていることを確認する。この記述には、特定のファイル及びディレクトリへのアクセスが特定の利用者のものと決定される規則が含まれなければならない。評価者は TSS を検査して、OS によって管理されるファイルと利用者との間に可能な任意のシナリオについてアクセス制御の決定が明確であるように、アクセス制御規則が詳細に記述されていることを保証する。

評価者は、2 人の新しい標準的な利用者の利用者アカウントをシステム上に作成し、以下のテストを実施すること：

- ***テスト 1：****評価者は、第 1 の利用者としてシステムへの認証を行い、その利用者のホームディレクトリ内にファイルを作成する。次に評価者はシステムからログオフし、第 2 の利用者としてログインする。次に評価者は、第 1 の利用者のホームディレクトリに作成されたファイルの読み出しを試行する。評価者は、読み出し試行が拒否されることを保証する。*
- ***テスト 2：****評価者は、第 1 の利用者としてシステムへの認証を行い、その利用者のホームディレクトリ内にファイルを作成する。次に評価者はシステムからログオフし、第 2 の利用者としてログインする。次に評価者は、第 1 の利用者のホームディレクトリに作成されたファイルの変更を試行する。評価者は、変更が拒否されることを保証する。*
- ***テスト 3：****評価者は、第 1 の利用者としてシステムへの認証を行い、その利用者のホームディレクトリ内にファイルを作成する。次に評価者はシステムからログオフし、第 2 の利用者としてログインする。次に評価者は、第 1 の利用者のホームディレクトリに作成されたファイルの削除を試行する。評価者は、削除が拒否されることを保証する。*
- ***テスト 4：****評価者は、第 1 の利用者としてシステムへの認証を行う。評価者は、第 2 の利用者のホームディレクトリにファイルの作成を試行する。評価者は、ファイルの作成が拒否されることを保証する。*
- ***テスト 5：****評価者は、第 1 の利用者としてシステムへの認証を行い、第 1 の利用者のホームディレクトリに作成されたファイルの変更を試行する。評価者は、ファイルの変更が受け入れられることを保証する。*
- ***テスト 6：****評価者は、第 1 の利用者としてシステムへの認証を行い、第 1 の利用者のディレクトリに作成されたファイルの削除を試行する評価者は、ファイルの削除が受け入れられることを保証する。*

FDP_IFC_EXT.1　情報フロー制御

FDP_IFC_EXT.1.1

OS は、VPN コネクションを確立するために要求される IP トラフィック

を例外として、 [**選択：**

VPN クライアントが IPsec を用いてすべての IP トラフィックを保護できるようなインタフェースを提供、

IPsec を用いてすべての IP トラフィックを保護できる VPN クライアントを提供、

] しなければならない。

適用上の注釈：典型的には、VPN コネクションを確立するために要求されるトラフィックは「制御プレーン」トラフィックと呼ばれ、IPsec VPN によって保護される IP トラフィックは「データプレーン」トラフィックと呼ばれる。すべての「データプレーン」トラフィックは VPN コネクションを介して流れなければならず、VPN はスプリットトンネリング (訳注：VPN を通るトラフィックと通らないトラフィックを送信先アドレスによって区別すること) を行ってはならない。

ネイティブな IPsec クライアントが全く検証されていない場合、またはサードパーティの VPN もまた要求された情報フロー制御を実装し得る場合、最初の選択肢が選択されなければならない。これらの場合、TOE は要求される情報フロー制御を行うために TOE のネットワークスタックを設定できる API をサードパーティの VPN クライアントに提供する。

ST 作成者は、TSF がネイティブな VPN クライアントを実装する (FTP_ITC_EXT.1 において IPsec が選択されている) 場合には 2 番目のオプションを選択しなければならない。ネイティブな VPN クライアントが検証される (FTP_ITC_EXT.1において IPsec が選択され、TSF が *IPsec 仮想プライベートネットワーク (VPN) クライアントの拡張パッケージ*に対して検証される) 場合、ST 作成者はこのパッケージから FDP_IFC_EXT も含めなければならない。また将来、本要件は現在の要件 (IPsec 高信頼チャネルが有効化される際、TSF からのすべてのトラフィックがそのチャネルを経由してルーティングされることを要求する) と、TSF による任意の通信を許可する IPsec 高信頼チャネルの確立を強制する選択肢を持つことを区別するかもしれない。

保証アクティビティ

評価者は、VPN クライアントが有効化されている際の IP トラフィックのルーティングが ST の TSS セクションに記述されていることを検証する。評価者はその記述に、どのトラフィックが VPN を通過せずどのトラフィックが通過するのか、そしてそれぞれについて VPN コネクションの確立に必要であると ST 作成者によって特定されたトラフィック (IKE トラフィックと、もしかすると HTTPS または DNS トラフィック) のみが VPN プロトコル (IPsec) によってカプセル化されないような設定が存在することが、示されていることを保証する。

5.1.3 セキュリティ管理 (FMT)

FMT_MOF_EXT.1 セキュリティ機能のふるまいの管理

FMT_MOF_EXT.1.1

OS は、以下に示すように利用者によって制御され管理者によって上書きされる、以下の管理機能を行えなければならない：

- X：必須
- O：オプション

管理機能	**管理者**	**利用者**
最小パスワード長の設定	O	O
パスワード中の特殊文字の最小個数の設定	O	O
パスワード中の数字の最小個数の設定	O	O
パスワード中の大文字の最小個数の設定	O	O
パスワード中の小文字の最小個数の設定	O	O
画面ロックの有効化／無効化	O	O
画面ロック非アクティブタイムアウト時間の設定	O	O
リモートコネクション非アクティブタイムアウト時間の設定	O	O
認証されないログオンの有効化／無効化	X	X
[**選択：***試行間のタイムアウト時間*、*時間間隔内の試行の回数の制限*] による、不成功認証試行ロックアウトポリシーの設定	O	O
ホストベースのファイアウォールの設定	O	O
バインドするディレクトリサーバの名前／アドレスの設定	O	O
管理設定を受信するリモート管理サーバの名前／アドレスの設定	O	O
監査／ロギング記録を送信する監査／ロギングサーバの名前／アドレスの設定	O	O
ローカル監査ストレージの容量の設定	O	O
監査規則の設定	O	O
ネットワークタイムサーバの名前／アドレスの設定	O	O

自動ソフトウェアアップデートの有効化／無効化	O	O
WiFi インタフェースの設定	O	O
Bluetooth インタフェースの有効化／無効化	O	O
USB インタフェースの設定	O	O
[**割付 :** その他の外部インタフェースのリスト] の有効化／無効化	O	O
[**割付 :** TSF によって提供されるべきその他の管理機能のリスト]	O	O

適用上の注釈 :「管理者」及び「利用者」という用語は セクション 1.2.2に定義されている。本要件の意図は、OS によって提供される管理機能が ST に含まれることを保証することである。これによって、AGD_OPE.1.3Cに特定される利用者操作ガイダンスとして提供されるものを含めた適合チェックリストの開発者が、評価された項目それぞれについてエンタープライズ特有の値を提供することによって、この表を活用することが可能となる。

推測困難なパスワード複雑性要件及び一時アカウントの取り扱いなど、洗練されたアカウント管理方針はディレクトリサーバの機能である。OS は、ディレクトリサーバへのバインディングを行うことにより、そのようなアカウント管理を登録して情報システム全体にそのようなポリシーを達成させることができる。

利用者及び管理者の両方が特定の管理機能を制御可能な場合、管理者がポリシーを設定していなければ利用者はその機能の実行を許可されるかもしれない。ST 作成者は "-" ("X"の代わりに) を用いて、管理が提供されない場合を示すべきである。

保証アクティビティ

評価者は、ST に取り込まれたすべての管理機能が操作ガイダンスに記述され、その記述にはその管理機能と関連付けられた管理職務を行うために必要な情報が含まれていることを検証する。評価者は、オペレーティングシステムを設定し上記の選択された各オプションをテストすることによって、管理機能を提供するオペレーティングシステムの能力をテストする。評価者には、設定が管理できると ST 及びガイダンス文書に言明されているすべての方法において、これらの機能をテストすることが期待される。

5.1.4 TSF の保護 (FPT)

FPT_ACF_EXT.1 アクセス制御

FPT_ACF_EXT.1.1

OS は、特権のない利用者に以下の変更を禁止するアクセス制御を実装しなければならない：

- カーネル及びそのドライバ／モジュール
- セキュリティ監査ログ
- 共有ライブラリ
- システム実行可能形式
- システム設定ファイル
- [**割付：**その他のオブジェクト]

保証アクティビティ

評価者は、カーネルドライバ／モジュール、セキュリティ監査ログ、共有ライブラリ、システム実行可能形式、及びシステム設定ファイルの場所が TSS に特定されていることを確認する。すべてのファイルが個別に特定される必要はないが、そのようなファイルを保存し保護するためのシステムの約束が特定されなければならない。評価者は、特権のない利用者アカウントを作成する。このアカウントを用いて、評価者は以下のテストが否定的な結果となることを保証する (即ち、そのアクションによって、評価者がそのアクションを完了する許可が OS によって拒否される結果となる)：

- ***テスト 1：****評価者は、すべてのカーネルドライバ及びモジュールの変更を試行する。*
- ***テスト 2：****評価者は、ロギングサブシステムによって生成されたすべてのセキュリティ監査ログの変更を試行する。*
- ***テスト 3：****評価者は、システム全体で利用されるすべての共有ライブラリの変更を試行する。*
- ***テスト 4：****評価者は、すべてのシステム実行可能形式の変更を試行する。*
- ***テスト 5：****評価者は、すべてのシステム設定ファイルの変更を試行する。*
- ***テスト 6：****評価者は、選択された任意の追加的コンポーネントの変更を試行する。*

FPT_ACF_EXT.1.2

OS は、特権のない利用者が以下を読み出すことを禁止するアクセス制御を実装しなければならない：

- セキュリティ監査ログ
- システムワイドなクレデンシャルリポジトリ
- [**割付：**その他のオブジェクトのリスト]

保証アクティビティ

評価者は、特権のない利用者アカウントを作成する。このアカウントを用いて、評価者は以下のテストが否定的な結果となることを保証する(即ち、そのアクションによって、評価者がそのアクションを完了する許可がOSによって拒否される結果となる)：

- ***テスト1：****評価者は、監査サブシステムによって生成されたセキュリティ監査ログの読み出しを試行する。*
- ***テスト2：****評価者は、システムワイドなクレデンシャルリポジトリの読み出しを試行する。*
- ***テスト3：****評価者は、割付にて特定された任意のその他のオブジェクトの読み出しを試行する。*

FPT_ASLR_EXT.1　アドレス空間配置ランダム化

FPT_ASLR_EXT.1.1

OS は、 [**割付：**明示的な例外のリスト] を除いて、プロセスアドレス空間のメモリロケーションを常にランダム化しなければならない。

保証アクティビティ

評価者は、TSF に含まれる3 つの実行可能形式を選択する。これには、TSF に含まれる任意のウェブブラウザまたはメールクライアントが含まれなければならない。これらのアプリのそれぞれについて、評価者はまったく同じハードウェア上の 2 つの別個の OS のインスタンス上で同一の実行可能形式を起動し、すべてのメモリマッピングのロケーションを比較する。評価者は、どのメモリマッピングも同一のロケーションに配置されていないことを保証する。1 つの実行可能形式について2つのマッピングが同一となり他の 2 つの実行可能形式では同一でないというまれな事象が発生した場合、評価者はその実行可能形式についてテストを繰り返し、2 回目のテストでマッピングが異なることを検証する。

FPT_SBOP_EXT.1　スタックバッファオーバーフロー保護

FPT_SBOP_EXT.1.1

OS は、スタックベースのバッファオーバーフロー保護を有効化してコンパイルされなければならない。

適用上の注釈：カーネル、ライブラリ、及びOS ベンダからのアプリケーションソフトウェアを含むOS の大部分が、スタックベースのバッファオーバーフロー保護を有効化してコンパイルされることが期待される。

保証アクティビティ

評価者は、OS によって用いられるスタックベースのバッファオーバーフロー保護の記述が TSS に含まれることを決定する。実装の例としては、"-fstack-protector-all"、"-fstack-protector"、及び"/GS"フラグなどのコンパイラオプションによってアクティベートされるものが挙げられる。これらはまた、スタックガード (Stack Guard)、及びスタックカナリア (Stack Canaries) など、さまざまな名前でも呼ばれる。TSS には、この方法で保護されない任意のバイナリの根拠が含まれなければならない。

- ***テスト 1：****評価者は、カーネル、ライブラリ、及びアプリケーションのバイナリのインベントリを作成して、スタックベースのバッファオーバーフロー保護を実装しないものを決定する。このリストは、TSS に提供されるリストと合致すべきである。*

FPT_TST_EXT.1　ブート完全性

FPT_TST_EXT.1.1

OS は、OS カーネル及び [**選択：**

可換メディアに保存されたすべての実行可能コード、

*[**割付：**その他の実行可能コードのリスト]* 、

その他の実行可能コードなし

] に至るブートチェインの完全性を、その実行前に、以下を利用して [**選択：**

ハードウェアによって保護された非対称鍵を用いたディジタル署名、

ハードウェアによって保護されたハッシュ

] 検証しなければならない。

適用上の注釈：OS のブートチェインは、OS ローダ、カーネル、システムドライバまたはモジュール、及びシステムファイルを含むソフトウェアのシーケンスであって、最終的に OS のロードに帰結するものである。通常はファーストステージブートローダと呼ばれる OS の最初の部分は、プラットフォームによってロードされなければならない。その完全性を評定することは、重要ではあるが、プラットフォームの責任であり、したがって本 PP の適用範囲外である。このステージ以降にロードされるすべてのソフトウェアは、OS の制御範囲内にある可能性があるため、適用範囲内である。

検証は推移的 (transitive) な性質であってもよい。ハードウェア保護された公開鍵またはハッシュが可換ブートローダコードを検証するために用いられ、そのブートローダコードには可換 OS カーネルコードを検証するためにブートローダによって用いられる鍵またはハッシュが含まれ、その可換 OS カーネルコードには次のレイヤーの実行可能コードを検証するための鍵またはハッシュが含まれる、などとなっていてもよい。しかし、

ハードウェアがこれらの鍵を保存し保護する方法は適用範囲外である。

すべての実行可能コード (1 つまたは複数のブートローダ、カーネル、デバイスドライバ、プリロードされたアプリケーション、利用者によってロードされたアプリケーション、及びライブラリ) が検証される場合、「可換メディアに保存されたすべての実行可能コード」が選択されるべきである。

保証アクティビティ

評価者は、TSF のブート手続きの包括的な記述が、ブートチェイン全体の記述を含め、ST の TSS セクションに含まれていることを検証する。評価者は、OS がブートローダ及びカーネルを含めブートチェインでロードするソフトウェアの部分それぞれを暗号学的に検証することを保証する。プラットフォームによって直接実行されるためにロードされるソフトウェア (例、ファーストステージブートローダ) は適用範囲外である。実行前に検証される追加のカテゴリの実行可能コードについて、評価者は、TSS の記述がどのようにそのソフトウェアが暗号学的に検証されるかについて記述していることを検証すること。

評価者は、暗号検証を実行するメカニズムに与えられる保護の記述が TSS に含まれることを検証すること。

評価者は、以下のテストを実行すること：

- ***テスト 1：****評価者は、TSF ソフトウェアをロードさせるアクションを実行し、完全性メカニズムによっていずれの実行可能形式も完全性エラーが含まれるとフラグされることなく、OS が適切にブートすることを確認すること。*
- ***テスト 2：****評価者は、TSF によって保護されたブートチェインの一部である TSF 実行可能形式 (つまりファーストステージブートローダではない) を改変し、ブートを試行すること。評価者は、完全性違反が引き起こされ OS がブートしないことを保証すること (完全性違反がモジュールのロードに失敗した原因であり、そのモジュールの構造を無効とするような事実が原因ではないことを、十分に注意して決定しなければならない)。*
- ***テスト 3：****完全性検証が公開鍵を用いて実行されることを ST 作成者が指示している場合、評価者はアップデートメカニズムに FIA_X509_EXT.1 に従った証明書の有効性確認が含まれることを検証すること。評価者は、extendedKeyUsage フィールドにコード署名目的を持たない証明書で TSF 実行可能形式にディジタル署名し、完全性違反が引き起こされることを検証すること。評価者は、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、完全性検証が成功することを検証しなければならない。理想的には、2 つの証明書は extendedKeyUsage フィールドを除いて同一であるべきである。*

FPT_TUD_EXT.1　インストール及びアップデートの完全性

FPT_TUD_EXT.1.1

OS は、OS ソフトウェア自体のアップデートをチェックする能力を提供しなければならない。

適用上の注釈 : 本要件は、真正なアップデートの可用性をチェックする能力に関するものであり、真正なアップデートのインストールは FPT_TUD_EXT.1.2でカバーされる。

保証アクティビティ

評価者は、証拠資料に記述される手順を用いてアップデートをチェックして、OS が利用可能なアップデートのリストを提供することを検証すること。この機能のテストには、自動アップデートを規定するセキュアな構成ガイダンスに相反する設定をシステムにインストールし一時的にその状態に保つことが必要とされるかもしれない。(また評価者は、この問い合わせが FTP_ITC_EXT.1 に記述されるように、高信頼チャネル上で行われることも保証する。)

FPT_TUD_EXT.1.2

OS は、FCS_COP.1(3) で規定されるスキームを用いてインストールする前に、ディジタル署名を用いてそれ自身へのアップデートを暗号学的に検証しなければならない。

保証アクティビティ

以下のテストを行うために、評価者はアップデートのダウンロードを開始し、インストールされる前にアップデートを取り込む。ダウンロードは、ベンダのウェブサイト、エンタープライズによってホストされたアップデートのリポジトリ、または別のシステム (例、ネットワークピア) から行われてもよい。サポートされているアップデートの生成元すべてが、TSS に示され、評価されなければならない。

- ***テスト 1 :** 評価者は、アップデートにベンダに属するディジタル署名があることを、そのインストール前に保証する。評価者は、ディジタル署名がもはや有効ではなくなるようにダウンロードしたアップデートを改変する。次に評価者は、改変されたアップデートのインストールを試行する。評価者は、OS による改変されたアップデートのインストールが行われないことを保証する。*
- ***テスト 2 :** 評価者は、アップデートにベンダに属するディジタル署名があることを保証する。次に評価者は、そのアップデートのインストールを試行する (またはインストールが引き続き行われることを許可する)。評価者は、OS によるアップデートのインストールが成功することを保証する。*

FPT_TUD_EXT.2　アプリケーションソフトウェアのインストール及びアップデートの完全性

FPT_TUD_EXT.2.1

OS は、アプリケーションソフトウェアへのアップデートをチェックする能力を提供しなければならない。

適用上の注釈 : 本要件は、真正なアップデートをチェックする能力に関するものであり、そのようなアップデートの実際のインストールは FPT_TUD_EXT.2.2でカバーされる。

保証アクティビティ

評価者は、証拠資料に記述される手順を用いてアプリケーションソフトウェアへのアップデートをチェックして、OS が利用可能なアップデートのリストを提供することを検証する。この機能のテストには、自動アップデートを特定するセキュアな構成ガイダンスに相反する設定にシステムを一時的に保つことが必要とされるかもしれない。(また評価者は、この問い合わせが FTP_ITC_EXT.1 に記述されるように、高信頼チャネル上で行われることも保証する。)

FPT_TUD_EXT.2.2

OS は、インストールの前に、FCS_COP.1(3) で規定されるディジタル署名を用いて、アプリケーションへのアップデートの完全性を暗号学的に検証しなければならない。

保証アクティビティ

評価者は、アプリケーションへのアップデートを開始する。これはアプリケーションによって異なるかもしれないが、アプリケーションベンダのウェブサイト、商用アプリストア、または別のシステムによって行われてもよい。OS によってサポートされる生成元すべてが、TSS に示され、評価されなければならない。しかし、これには OS が高信頼インストール及びアップデート機能を提供しているメカニズムのみが含まれる。これには、利用者または管理者によって起動される任意のファイルのダウンロード及びインストールは含まれない。

- ***テスト 1 :*** *評価者はアップデートに、OS ベンダまたは OS によって管理されるその他の高信頼ルートへ連鎖するディジタル署名があることを保証する。評価者は、ディジタル署名がもはや有効ではなくなるようにダウンロードしたアップデートを改変する。次に評価者は、改変されたアップデートのインストールを試行する。評価者は、OS による改変されたアップデートのインストールが行われないことを保証する。*
- ***テスト 2 :*** *評価者はアップデートに、OS ベンダまたは OS によって管理されるその他の高信頼ルートに属するディジタル署名があることを保証する。次に評価者は、そのアップデート*

のインストールを試行する。評価者は、OS によるアップデートのインストールが成功することを保証する。

5.1.5 監査データの生成 (FAU)

FAU_GEN.1 監査データの生成

FAU_GEN.1.1

OS は、以下の監査対象事象の監査記録を生成できなければならない：

a. 監査機能の開始及び終了；

b. 監査レベルが規定されていないすべての監査対象事象；及び

c.

- 認証事象 (成功／失敗)；
- 特権／特別な権利の使用事象 (成功及び不成功のセキュリティ、監査、及び設定変更)；
- 特権または役割昇格事象 (成功／失敗)；
- [**選択：**

  ファイル及びオブジェクト事象 (成功及び不成功の、作成、アクセス、削除、変更、アクセス権限変更の試行)、

  利用者及びグループ管理事象 (成功及び不成功の、追加、削除、変更、無効化、

  監査及びログデータへのアクセス事象 (成功／失敗)、

  ソフトウェアの暗号学的検証 (成功／失敗)、

  プログラムの開始 (成功／例、ソフトウェア制限ポリシーによる失敗) 、

  システムのリブート、再開、及びシャットダウン事象 (成功／失敗)、

  カーネルモジュールのロード及びアンロード事象 (成功／失敗)、

  管理者またはルートレベルのアクセス事象 (成功／失敗)、

  コマンドライン入力 (成功／失敗)、

  *[**割付：**その他の特に定義された監査対象事象]* 。

  ]

保証アクティビティ

評価者は管理ガイドをチェックして、すべての監査対象事象が列挙されていることを保証しなければならない。管理者は、ST で選択されたすべての監査事象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。

評価者は、ST に列挙された事象に対する監査記録を TOE に生成させることによって、監査記録を正しく生成するための OS の能力をテストしなければならない。これには、規定された事象のすべてのインスタンスタイプが含まれるべきである。テスト結果を検証する際に、評価者はテストで生成された監査記録が管理ガイドで規定されたフォーマットと一致すること、及び各監査記録のフィールドが適切なエントリを有することを保証しなければならない。

FAU_GEN.1.2

OS は、監査記録のそれぞれに、少なくとも以下の情報を記録しなければならない：

a. 事象の日付及び時刻、事象種別、サブジェクトの識別情報 (該当する場合)、及び事象の結果 (成功または失敗)、及び

b. 監査事象種別のそれぞれについて、PP/ST に含まれる機能コンポーネントの監査対象事象の定義に基づいた、 [**割付：**その他の監査関連情報]

適用上の注釈：ここで*サブジェクト*という用語は、プロセスが代理として動作する利用者として理解される。機能コンポーネントの監査対象事象の定義が提供されない場合には、追加の監査関連情報は要求されない。

保証アクティビティ

評価者は管理ガイドをチェックして、監査記録のフォーマットが提供されていることを保証しなければならない。監査記録のフォーマット種別のそれぞれが、各フィールドの簡潔な記述と共に、カバーされなければならない。評価者は、そのフィールドに要求される情報が含まれることを保証しなければならない。

評価者は、ST に列挙された事象に対して TOE に監査記録を生成させることによって、正しく監査記録を生成する OS の能力をテストしなければならない。評価者はテスト中に生成された監査記録が管理ガイドに規定されたフォーマットと一致すること、及び各監査記録のフィールドが要求される情報を提供することを保証しなければならない。

5.1.6 識別と認証 (FIA)

FIA_AFL.1 認証失敗時の取り扱い

FIA_AFL.1.1

OS は、以下の際に [**選択：**

*[**割付：***正の整数値*]、

*管理者によって設定可能な [**割付：***受容可能な値の範囲*] *以内の正の整数値*

] 回の不成功に終わった以下の試行 [**選択：**

利用者名及びパスワードに基づく認証、

利用者名及び運用環境によって保護されたストレージに保存される非対称鍵を解除する PIN に基づく認証、

X.509 証明書に基づく認証

] が [**割付：**認証事象のリスト] と関連して発生したことを検出できなければならない。

保証アクティビティ

評価者は、管理者によって設定可能な失敗した試行に対する閾値を設定、または ST に特定された割付に留意する。評価者は次に (選択に従って) 正しくないパスワード、PIN、または証明書を用いた認証試行を、試行回数が閾値に達するまで繰り返す。認証試行及びロックアウトはまた、FAU_GEN.1 に特定されるようにロギングされなければならないことに注意されたい。

FIA_AFL.1.2

不成功の認証試行が定義した回数に達したとき、OS は [**選択：***アカウントのロックアウト、アカウントの無効化、必須クレデンシャルのリセット、[**割付：***アクションのリスト]*] をしなければならない。

適用上の注釈：取られるべきアクションは、ST の割付中に含まれると共に、管理者ガイダンス中に定義されなければならない。

保証アクティビティ

- ***テスト 1：****評価者は、既知の間違ったパスワードでシステムへの認証を繰り返し試行する。認証試行の失敗が定義された回数に達した際、評価者はテストに用いられていたアカウントに、上記に列挙された割付に詳述されたアクションが適用されていることを保証する。評価者は、そのアカウントにこれらのアクションが適用されたことを詳述する事象がセキュリティ事象ログにロギングされていることを保証する。*
- ***テスト 2：****評価者は、既知の間違った証明書でシステムへの認証を繰り返し試行する。認証試行の失敗が定義された回数に達した際、評価者はテストに用いられていたアカウントに、上記に列挙された割付に詳述されたアクションが適用されていることを保証する。評価者は、そのアカウントにこれらのアクションが適用されたことを詳述する事象がセキュリティ事象ログにロギングされていることを保証する。*
- ***テスト 3：****評価者は、間違ったパスワードと間違った証明書の両方を用いてシステムへの認証を繰り返し試行する。認証試行の失敗が定義された回数に達した際、評価者はテストに用*

いられていたアカウントに、上記に列挙された割付に詳述されたアクションが適用されていることを保証する。評価者は、そのアカウントにこれらのアクションが適用されたことを詳述する事象がセキュリティ事象ログにロギングされていることを保証する。

FIA_UAU.5　複数の認証メカニズム

FIA_UAU.5.1

OS は、利用者認証をサポートするため、以下の認証メカニズム [**選択：**

利用者名及びパスワードに基づく認証、

利用者名及び運用環境によって保護されたストレージに保存される非対称鍵を解除する PIN に基づく認証、

X.509 証明書に基づく認証

] を提供しなければならない。

保証アクティビティ

利用者名及びパスワードに基づく認証が選択された場合、評価者は既知の利用者名及びパスワードを OS に設定し、以下のテストを実施する：

- ***テスト 1：****評価者は、既知の利用者名とパスワードを用いて OS への認証を試行する。評価者は、認証試行が成功することを保証する。*
- ***テスト 2：****評価者は、評価者は、既知の利用者名と正しくないパスワードを用いて OS への認証を試行する。評価者は、認証試行が成功しないことを保証する。*

利用者名及び非対称鍵を解除する PIN が選択された場合、評価者はサポートされている保護されたストレージに関するガイダンスに関して TSS を検査し、次に OS がインタフェース可能な保護されたストレージ (TPM、ハードウェアトークン、または隔離された実行環境) から非対称鍵を解放させる PIN を確立するよう TOE または OE を設定する。次に評価者は、以下のテストを実施する。

- ***テスト 1：****評価者は、既知の利用者名と PIN を用いて OS への認証を試行する。評価者は、認証試行が成功することを保証する。*
- ***テスト 2：****評価者は、評価者は、既知の利用者名と正しくない PIN を用いて OS への認証を試行する。評価者は、認証試行が成功しないことを保証する。*

X.509 証明書に基づく認証が選択された場合、評価者は Client Authentication Enhanced Key Usage フィールドをセットして、利用者の X.509v3 証明書を生成する。評価者は OS に、X.509v3 証明書を用いる認

証を配備する。評価者は証明書が、FIA_X509_EXT.1.1に従ってOSによって有効性確認されることを保証し、次に以下のテストを実施する：

- ***テスト1：****評価者は、X.509v3 証明書を用いてOS への認証を試行する。評価者は、認証試行が成功することを保証する。*
- ***テスト2：****評価者は、公開鍵及び公開鍵から導出される任意の値を除いて第 1 の証明書と同一の第 2 の証明書を生成する。評価者は、この証明書を用いてOS への認証を試行する。評価者は、認証試行が成功しないことを保証する。*

FIA_X509_EXT.1　X.509 証明書有効性確認

FIA_X509_EXT.1.1

OS は、以下の規則に従って証明書の有効性確認を行う機能を実装しなければならない：

- RFC 5280 証明書有効性確認及び証明書パス検証。
- 証明書パスは、信頼済み CA 証明書で終わらなければならない。
- OS は、すべての CA 証明書について、basicConstraints 拡張の存在と CA フラグが TRUE にセットされていることを保証することによって、証明書パスを検証しなければならない。
- OS は、[**選択：***RFC 2560 に特定されるオンライン証明書状態プロトコル (OCSP)*、*RFC 5759 に特定される証明書失効リスト (CRL)*、*RFC 6066 に特定される OCSP TLS Status Request Extension (即ち、OCSP stapling)*] を用いて証明書の失効状態を検証しなければならない。
- OS は、以下の規則に従って extendedKeyUsage フィールドを検証しなければならない：
  - 高信頼アップデート及び実行可能コードの完全性検証に用いられる証明書は、extendedKeyUsage フィールドにコード署名目的 (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) を持たなければならない。
  - TLS に提示されるサーバ証明書は、extendedKeyUsage フィールドにサーバ認証目的 (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) を持たなければならない。
  - TLS に提示されるクライアント証明書は、extendedKeyUsage フィールドにクライアント認証目的 (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) を持たなければならない。
  - 電子メールの暗号化及び署名に提示される S/MIME 証明書は、extendedKeyUsage フィールドに電子メール保護目的 (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) を持たなければならない。
  - OCSP 応答に提示される OCSP 証明書は、extendedKeyUsage フィールドに OCSP 署名目的 (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) を持たなければならない。

- (条件付き) EST (訳注：Enrollment over Secure Transport)に提示されるサーバ証明書は、extendedKeyUsage フィールドに CMC Registration Authority (RA) 目的 (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) を持たなければならない。

適用上の注釈：FIA_X509_EXT.1.1 には、証明書有効性確認を行うための規則が列挙されている。ST 作成者は、失効状態が OCSP か CRL のどちらを用いて検証されるか選択しなければならない。FIA_X509_EXT.2は、証明書が HTTPS、TLS 及び DTLS に利用されることを要求している。この利用によって、extendedKeyUsage 規則が検証されることが要求される。

保証アクティビティ

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

記述されるテストは、FIA_X509_EXT.2.1 中の機能を含め、他の証明書サービス保証アクティビティと組み合わせて行われなければならない。extendedKeyUsage 規則のテストは、これらの規則を要求する用途と組み合わせて行われる。評価者は、少なくとも 4 つの証明書の連鎖を作成する：テストされるノード証明書、2 つの中間 CA、及び自己署名されたルート CA である。

- ***テスト 1：****評価者は、有効な証明書パスのない証明書の有効性を確認すると、その機能が失敗することを論証する。次に評価者は、信頼済み CA がその機能で用いられる証明書の有効性確認に必要とするような 1 つまたは複数の証明書をロードし、その機能が成功することを論証する。次に評価者は、これらの証明書の 1 つを削除して、その機能が失敗することを示さなければならない。*
- ***テスト 2：****評価者は、有効期限を過ぎた証明書の有効性確認を行うと、その機能が失敗することを論証する。*
- ***テスト 3：****評価者は、CRL、OCSP、または OCSP stapling のどれが選択されているかに応じて、OS が失効した証明書を適切に処理できることをテストする；複数の手法が選択されている場合には、それぞれの手法についてテストが行われなければならない。評価者はノード証明書の失効及び中間 CA 証明書の失効をテストする (即ち、中間 CA 証明書はルート CA によって失効させられるべきである)。評価者は、有効な証明書が用いられること、そして証明書有効性確認機能が成功することを保証する。次に評価者は、失効した証明書 (選択において選ばれた手法それぞれについて) を用いてテストを試行し、もはや証明書が有効ではない場合には証明書有効性確認機能が失敗することを保証する。*
- ***テスト 4：****OCSP が選択されている場合、評価者は OCSP サーバを設定するか中間者ツールを使用して OCSP 署名目的を持*

たない証明書を提示し、OCSP 応答の有効性確認が失敗することを検証する。CRL が選択されている場合、評価者は cRLsign 鍵使用ビットがセットされていない証明書を持つ CRL に CA が署名するよう設定し、CRL の有効性確認が失敗することを検証する。

- ***テスト 5 :** 評価者は、証明書の最初の 8 バイトの中の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論証する。(証明書の正しい解析は失敗すべきである。)*
- ***テスト 6 :** 評価者は、証明書の最後のバイトの中の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論証する。(証明書の署名は検証されるべきでない。)*
- ***テスト 7 :** 評価者は、証明書の公開鍵の中の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論証する。(証明書の署名は検証されるべきでない。)*

FIA_X509_EXT.1.2

OS は、basicConstraints 拡張が存在し CA フラグが TRUE にセットされている場合にのみ、証明書を CA 証明書として取り扱わなければならない。

適用上の注釈 : 本要件は、TSF によって用いられ処理される証明書に適用され、信頼済み CA 証明書として追加され得る証明書を制限する。

保証アクティビティ

記述されるテストは、FIA_X509_EXT.2.1 中の機能を含め、他の証明書サービス保証アクティビティと組み合わせて行われなければならない。評価者は、少なくとも 4 つの証明書の連鎖を作成する：テストされるノード証明書、2 つの中間 CA、及び自己署名されたルート CA である。

- ***テスト 1 :** 評価者は、OS の証明書を発行する CA の証明書に basicConstraints 拡張が含まれないような証明書パスを構築する。この証明書パスの検証は失敗する。*
- ***テスト 2 :** 評価者は、OS の証明書を発行する CA の証明書の basicConstraints 拡張中の CA フラグがセットされていないような証明書パスを構築する。この証明書パスの検証は失敗する。*
- ***テスト 3 :** 評価者は、OS の証明書を発行する CA の証明書の basicConstraints 拡張中の CA フラグが TRUE にセットされているような証明書パスを構築する。この証明書パスの検証は成功する。*

FIA_X509_EXT.2 X.509 証明書認証

FIA_X509_EXT.2.1

OS は、RFC 5280 に定義される X.509v3 証明書を用いて、TLS 及び **[選択 :** *DTLS*、*HTTPS*、 ***[割付 :** その他のプロトコル]* 、その他のプロトコル

なし] コネクションの認証をサポートしなければならない。

保証アクティビティ

評価者は、OS の TLS メカニズムを X.509v3 証明書と共に利用するアプリケーションを取得または開発する。次に開発者はそのアプリケーションを実行し、提供された証明書がコネクションの認証に用いられていることを保証する。

評価者は、列挙された任意のその他の選択について、このアクティビティを繰り返す。

5.1.7 高信頼パス／チャネル (FTP)

FTP_ITC_EXT.1 高信頼チャネル通信

FTP_ITC_EXT.1.1

OS は、 [**選択：**

FCS_TLSC_EXT.1 に適合する TLS、

FCS_DTLS_EXT.1 に適合する DTLS、

IPsec VPN クライアントの拡張パッケージ に適合する IPsec、

セキュアシェルの拡張パッケージ に適合する SSH

] を用いて、他の通信チャネルとは論理的に区別されていると共に、その端点の保証された識別とチャネルデータの暴露からの保護及びチャネルデータの改変の検出を提供する、それ自身と以下の機能をサポートする許可された IT エンティティ：[**選択：***監査サーバ*、*認証サーバ*、*管理サーバ*、*[**割付：***その他の機能*]] との間の高信頼通信チャネルを提供できなければならない。

適用上の注釈：ST 作成者が IPsec を選択した場合、TSF は *IPsec 仮想プライベートネットワーク (VPN) クライアントの拡張パッケージ*に対して検証されなければならない。ST 作成者が SSH を選択した場合、TSF は*セキュアシェルの拡張パッケージ*に対して検証されなければならない。ST 作成者は、FTP_ITC_EXT.1 に選択された高信頼チャネルプロトコルのセキュリティ機能要件を ST の本体中に含めなければならない。

保証アクティビティ

評価者は、2 番目の選択中に特定される他の高信頼 IT 製品との通信を行うよう OS を設定する。評価者は、2 番目の選択中に特定されるサーバのそれぞれと OS が通信を行っている間にネットワークトラフィックを監視する。評価者は、各セションについて、最初の選択中に特定されたプロトコルに適合して高信頼チャネルが確立されたことを保証する。

FTP_TRP.1　高信頼パス

FTP_TRP.1.1

OS は、それ自身とリモート利用者間に、他の通信パスと論理的に区別され、その端点の保証された識別と、改変及び暴露からの通信データの保護を提供する通信パスを提供しなければならない。

FTP_TRP.1.2

OS は、 [**選択：***TSF*、*ローカル利用者*、*リモート利用者*] が高信頼パスを介して通信を開始することを許可しなければならない。

FTP_TRP.1.3

OS は、すべてのリモート管理アクションに対して、高信頼パスの使用を要求しなければならない。

適用上の注釈：本要件は、許可されたリモート管理者が高信頼パスを介して OS とのすべての通信を開始すること、及びリモート管理者による OS とのすべての通信はこのパス上で行われることを保証する。この高信頼通信チャネルを通過するデータは、FTP_ITC_EXT.1に定義されるように暗号化される。

本要件の保証アクティビティは、要件 FTP_TRP.1.1及び FTP_TRP.1.2をもテストする。

保証アクティビティ

評価者は、リモート OS 管理の手法が、これらの通信が保護される方法と共に示されていることを決定するため、TSS を検査する。また評価者は、OS 管理をサポートするものとして TSS に列挙されたすべてのプロトコルが要件中に特定されたものと一貫しており、ST 中の要件に含まれていることを確認する。評価者は、サポートされている手法のそれぞれについて、リモート管理セションを確立するための指示が操作ガイダンスに含まれていることを確認する。また評価者は、以下のテストを行う：

- ***テスト 1：****評価者は、操作ガイダンスの記述どおりにコネクションを設定し通信が成功することを保証することによって、各リモート管理手法を用いた通信が評価中にテストされることを保証する。*
- ***テスト 2：****サポートされるリモート管理の各手法について、評価者は操作ガイダンスに従って、高信頼パスを伴わずにリモート管理セションを確立するためにリモート利用者が利用できるインタフェースが存在しないことを保証する。*
- ***テスト 3：****評価者は、リモート管理の各手法について、チャネルデータが平文で送信されないことを保証する。*
- ***テスト 4：****評価者は、リモート管理の各手法について、チャネルデータの改変が OS によって検出されることを保証する。*

5.2 セキュリティ保証要件

セクション 4のセキュリティ対策方針は、セクション 3.1で識別された脅威に対処するために作られた。セクション 5.1のセキュリティ機能要件 (SFR) は、セキュリティ対策方針の形式的な実体化である。PP は、評価者が評価で利用可能な証拠資料を評定し、独立テストを実行する範囲を設定するため、セキュリティ保証要件 (SAR) を識別する。

本セクションには、本 PP に適合する評価で要求される CC パート 3 からの一連の SAR が列挙される。実行されるべき個別の保証アクティビティは、本セクションと セクション 5 の両方で規定される。

本 PP へ適合するために書かれた ST に対する OS 評価の一般的モデルは、以下のとおりである：

ST が評価について承認された後、情報技術セキュリティ評価機関 (ITSEF) は、OS、支援環境 IT、及び OS の管理者／利用者ガイドを入手する。その ITSEF は、ASE 及び ALC の SAR に関して情報技術セキュリティ評価のための共通方法 (CEM) によって義務付けられたアクションを行うことが期待される。その ITSEF は、セクション 5に含まれる保証アクティビティについても実行する、これらのアクティビティは OS で具体化される特定の技術に適用されるようにその他の CEM 保証要件の解釈として意図されるものである。セクション 5で取り込まれた保証アクティビティは、OS が PP に適合することを論証するために開発者が何を提供する必要があるかについての明確化も提供する。

5.2.1 ASE クラス：セキュリティターゲット

[CEM] に定義される ASE アクティビティによる。

5.2.2 ADV クラス：開発

OS についての情報は、ST の TSS 部分と共に、エンドユーザに利用可能なガイダンス文書にも含まれる。OS 開発者は、TSS に含まれる製品の記述を機能仕様との関連において一致させなければならない。セクション 5.1に含まれる保証アクティビティは、TSS セクションの適切な内容を決定するため、ST 作成者に十分な情報を提供すべきである。

ADV_FSP.1　基本機能仕様 (ADV_FSP.1)

開発者アクションエレメント：

ADV_FSP.1.1D

開発者は、機能仕様を提供しなければならない。

ADV_FSP.1.2D

開発者は、機能仕様から SFR への追跡を提供しなければならない。

適用上の注釈：本セクションの序説で述べたように、機能仕様は AGD_OPE 及び AGD_PRE 文書に含まれる情報から構成される。開発者は、アプリケーション開発者及び評価者にアクセス可能なウェブサイトを参照してもよい。機能要件の保証アクティビティは、証拠資料及び TSS セクションに存在すべき証拠を参照している；これらは SFR と直接関連付けられているため、エレメント ADV_FSP.1.2D での追跡は暗黙的にはす

でになされており、追加の証拠資料は必要とされない。

内容・提示エレメント：

ADV_FSP.1.1C

機能仕様は、SFR 実施及び SFR 支援の各 TSFI の目的と使用方法を記述しなければならない。

ADV_FSP.1.2C

機能仕様は、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なければならない。

ADV_FSP.1.3C

機能仕様は、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、その分類の根拠を示さなければならない。

ADV_FSP.1.4C

追跡は、機能仕様での TSFI に対する SFR の追跡を実証するものでなければならない。

評価者アクションエレメント：

ADV_FSP.1.1E

評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_FSP.1.2E

評価者は、機能仕様が、SFR の正確かつ完全な具体化であることを決定しなければならない。

保証アクティビティ

情報が提供されていることを保証すること以外に、これらの SAR に関連付けられた具体的な保証アクティビティは存在しない。機能仕様書証拠資料は セクション 5.1 に記述された評価アクティビティと、AGD、ATE、及び AVA SAR に関して記述されたその他のアクティビティをサポートするために提供される。機能仕様書情報の内容についての要件は、実行されるその他の保証アクティビティの特質によって暗黙的に評定される；不十分なインタフェース情報しか存在しなかったために評価者があるアクティビティを実行できなかった場合、十分な機能仕様書が提供されなかったこととなる。

5.2.3 AGD クラス：ガイダンス文書

ガイダンス文書は、ST と共に提供される。ガイダンスには、運用環境がセキュリティ機能の役割を満たすことが可能であることをどのように IT 要員が検証するかの記述が含まれなければならない。証拠資料は、非形式的なスタイルかつ IT 要員によって読解可能であるべきである。ガイダンスは、ST 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なければならない。このガイダンスには、そのような環境において TSF をうまくインストールするための指示を含む；また、製品として、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を含む。特定のセキュ

リティ機能に関するガイダンスもまた提供される；このようなガイダンスについての要件は、各要件と共に規定される保証アクティビティに含まれる。

AGD_OPE.1　利用者操作ガイダンス (AGD_OPE.1)

開発者アクションエレメント：

AGD_OPE.1.1D

開発者は、利用者操作ガイダンスを提供しなければならない。

適用上の注釈：利用者操作ガイダンスは、単一の文書に含まれる必要はない。利用者、管理者及びアプリケーション開発者向けのガイダンスが、複数の文書またはウェブページに分散されていてもよい。ここで繰返し情報を提示するのではなく、開発者はこのコンポーネントに関する保証アクティビティをレビューして、評価者がチェックすることになるガイダンスの詳細を確認すべきである。これによって、受容可能なガイダンスの作成に必要な情報が提供されることになる。

内容・提示エレメント：

AGD_OPE.1.1C

利用者操作ガイダンスは、適切な警告を含め、セキュアな処理環境で管理するべき、利用者がアクセス可能な機能と権限について、利用者の役割ごとに記述しなければならない。

適用上の注釈：利用者及び管理者が、利用者役割の定義において考慮されることになる。

AGD_OPE.1.2C

利用者操作ガイダンスは、OS により提供された利用可能なインタフェースをセキュアな方法でどのように使用するかを利用者の役割ごとに記述しなければならない。

AGD_OPE.1.3C

利用者操作ガイダンスは、利用可能な機能とインタフェース、特に利用者の管理下にあるすべてのセキュリティパラメタを、必要に応じてセキュアな値を示し、利用者の役割ごとに記述しなければならない。

適用上の注釈：利用者操作ガイダンスのこの部分は、適合アクティビティにおける利用に適した、IT 要員 (または、必要な場合にはエンドユーザ) によって迅速に照合できるチェックリストの形態で提示されるべきである。可能であれば、このガイダンスはセキュリティ自動化 (訳注：SCAP (Security Content Automation Protocol)) をサポートするためセキュリティ設定チェックリスト記述形式 (XCCDF) で表現される。最低限、それは各設定項目のタイトル、セキュアな設定を達成するための指示、及び任意の関連する根拠を含む、構造化されたフォーマットで提示されるべきである。

AGD_OPE.1.4C

利用者操作ガイダンスは、TSF の制御下にあるエンティティのセキュリティ特性の変更を含む、利用者がアクセス可能で実行が必要な機能に関連するセキュリティ関連事象の各タイプについて、利用者の役割ごとに

明確に提示しなければならない。

AGD_OPE.1.5C

利用者操作ガイダンスは、OS の操作のすべての可能なモード(障害や操作誤りの後の操作を含む)、それらの結果、及びセキュアな運用を維持するために必要なことを識別しなければならない。

AGD_OPE.1.6C

利用者操作ガイダンスは、ST に記述された運用環境のセキュリティ対策方針を満たすために従うべきセキュリティ手段を、利用者の役割ごとに記述しなければならない。

AGD_OPE.1.7C

利用者操作ガイダンスは、明確で、合理的なものでなければならない。

評価者アクションエレメント：

AGD_OPE.1.1E

評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

保証アクティビティ

操作ガイダンスの内容のいくつかは、セクション 5.1 の保証アクティビティ及び [CEM] に従った OS の評価によって検証される。以下の追加情報についても要求される。暗号機能が OS によって提供される場合、操作ガイダンスには、OS の評価される構成と関連する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。その他の暗号エンジンの使用が OS の CC 評価中に評価もテストもされなかった、という警告が管理者に提供されなければならない。証拠資料には、ディジタル署名の検証によって OS へのアップデート検証の処理が記述されなければならない － これは OS または基盤となるプラットフォームによって行われてもよい。評価者は、この処理に以下の手順が含まれることを検証する：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 OS からアクセス可能とするための指示 (例、具体的なディレクトリへの配置) が含まれるべきである。アップデート処理を開始するための指示、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／ディジタル署名の生成が含まれる。OS には、本 PP の下での評価の適用範囲外のセキュリティ機能が含まれることもあるだろう。操作ガイダンスは、管理者に対して、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明確にしなければならない。

AGD_PRE.1　準備手続き (AGD_PRE.1)

開発者アクションエレメント：

AGD_PRE.1.1D

開発者は、準備手続きを含めて OS を提供しなければならない。

適用上の注釈：操作ガイダンスと同様に、開発者は保証アクティビティを

検査して準備手続きに関して必要とされる内容を決定すべきである。

内容・提示エレメント：

AGD_PRE.1.1C

準備手続きは、開発者の配付手続きに従って配付された OS のセキュアな受入れに必要なすべてのステップを記述しなければならない。

AGD_PRE.1.2C

準備手続きには、OS のセキュアな設置、及び ST に記述された運用環境のセキュリティ対策方針に従った運用環境のセキュアな準備に必要なすべてのステップを記述しなければならない。

評価者アクションエレメント：

AGD_PRE.1.1E

評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

AGD_PRE.1.2E

評価者は、OS が運用に向けてセキュアに準備できることを確認するために、準備手続きを適用しなければならない。

保証アクティビティ

上記の序説で示すとおり、－ 特に OS 機能要件を支援する運用環境を構成するとき － 証拠資料について多大な期待がある。評価者は、OS に提供されるガイダンスが、ST で OS について主張されるすべてのプラットフォームへ十分に対処することを保証するため、チェックしなければならない。

5.2.4 ALC クラス：ライフサイクルサポート

本 PP に適合する OS に提供される保証レベルでは、ライフサイクルサポートは OS ベンダの開発及び構成管理プロセスの検査ではなく、ライフサイクルのエンドユーザに可視の側面に限定される。これは、製品の全体的な信頼度の向上に開発者の実践が果たす重要な役割を低減しようとするものではない。むしろ、本保証レベルにおける評価に関して利用可能とされるべき情報を反映したものである。

ALC_CMC.1　TOE のラベル付け (ALC_CMC.1)

開発者アクションエレメント：

ALC_CMC.1.1D

開発者は、OS 及び OS の参照を提供しなければならない。

内容・提示エレメント：

ALC_CMC.1.1C

OS は、その一意の参照でラベル付けされなければならない。

適用上の注釈：一意な参照には、以下のものが含まれる：

- OS の名称

- OS のバージョン
- OS の記述
- 提供される場合は、ソフトウェア識別 (SWID) タグ

評価者アクションエレメント：

ALC_CMC.1.1E

評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

保証アクティビティ

評価者は、ST の要件を満たすバージョンを具体的に識別するような識別子 (製品名／バージョン番号等) を ST が含むことを保証するため、ST をチェックすること。さらに、評価者は、バージョン番号が ST のものと一貫していることを保証するため、AGD ガイダンス及びテスト用に受け取った OS サンプルをチェックすること。ベンダが OS を宣伝するウェブサイトを維持管理している場合、評価者は、ST の情報がその製品を区別するために十分であることを保証するため、そのウェブサイト上の情報を検査すること。

ALC_CMS.1　TOE の CM 範囲 (ALC_CMS.1)

開発者アクションエレメント：

ALC_CMS.1.1D

開発者は、OS の構成リストを提供しなければならない。

内容・提示エレメント：

ALC_CMS.1.1C

構成リストは、OS 自体、及び SAR が要求する評価証拠を含まなければならない。

ALC_CMS.1.2C

構成リストは、構成要素を一意に識別しなければならない。

評価者アクションエレメント：

ALC_CMS.1.1E

評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

保証アクティビティ

本 PP での「SAR によって要求される評価証拠」は、ST の情報、及び AGD 要件の下で管理者及び利用者に提供されるガイダンスとの組み合わせに限定される。OS が具体的に識別されること、及びその識別情報が ST 及び AGD ガイダンスで一貫していることを保証することにより (ALC_CMC.1 の評価アクティビティで行われるとおり)、評価者は、本コンポーネントによって要求される情報を暗黙的に確認する。ライフサイクルサポートでは、TSF 製造業者の開発及び構成管理プロセスの

詳細な検査ではなく、開発者のライフサイクルの側面と、開発者のデバイス向けアプリケーション提供者への指示を対象としている。これは、製品の全体的な信頼性の向上に開発者の実践が果たす重要な役割を軽減することを意味するものではなく;むしろ、評価で利用可能な情報の反映である。

評価者は、開発者が開発者のプラットフォーム向けアプリケーションの開発での用途に適した 1 つ以上の開発環境を (対象となるプラットフォームに関するアプリケーション開発者向けガイダンス証拠資料で) 識別したことを保証すること。これらの開発環境のそれぞれについて、開発者は 1 つ以上の環境でバッファオーバーフロー保護メカニズムが起動されることを保証するための環境設定方法 (例、コンパイラ及びリンカのフラグ) についての情報を提供しなければならない。評価者は、このような保護がデフォルトでオンであるか、具体的に有効化されなければならないのかについての表示についても、本証拠資料に含まれることを保証すること。評価者は、TSF が一意に識別され (その TSF ベンダからの他の製品との関連で)、ST の要件と関連して開発者から提供される証拠資料が、この一意の識別情報を用いて TSF と関連付けられることを保証すること。

ALC_TSU_EXT.1　タイムリーなセキュリティアップデート

開発者アクションエレメント：

ALC_TSU_EXT.1.1D

開発者は、OS のセキュリティアップデートがタイムリーに行われる方法についての TSS 記述を提供しなければならない。

ALC_TSU_EXT.1.2D

開発者は、アップデートがセキュリティ特性または製品の設定を変更するとき利用者へ通知する方法についての TSS 記述を提供しなければならない。

内容・提示エレメント：

ALC_TSU_EXT.1.1C

記述には、OS ソフトウェアのセキュリティアップデートを作成し使用するためのプロセスを含まなければならない。

ALC_TSU_EXT.1.2C

記述には、OS に関するセキュリティ問題を報告するため公知のメカニズムを含まなければならない。報告メカニズムには、報告の機微性を保護する手段 (例、悪用の概念実証の詳細を暗号化するために使用可能な公開鍵)と共に、ウェブサイト、電子メールアドレスを含むかもしれない。

評価者アクションエレメント：

ALC_TSU_EXT.1.1E

評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

保証アクティビティ

評価者は、セキュリティアップデートを作成し展開するため、開発者によって利用されるタイムリーなセキュリティアップデートプロセスの記述が TSS に含まれることを検証すること。評価者は、この記述がアプリケーション全体に対処していることを検証すること。また評価者は、OS 開発者のプロセスに加えて、任意のサードパーティのプロセスが記述において対処されていることも検証すること。さらに評価者は、セキュリティアップデートの展開のための各メカニズムが記述されていることも検証すること。

評価者は、アップデートプロセスのために記述された展開メカニズムのそれぞれについて、展開におけるサードパーティまたはキャリアの遅延を含め、脆弱性の公的な開示からこの脆弱性にパッチを当てる OS へのセキュリティアップデートが公的に利用可能となるまでの間の時間が TSS に列挙されることを検証すること。評価者は、この時間が日数または日数の範囲として表現されることを検証すること。

評価者は、OS に関連するセキュリティ問題を報告するため公知のメカニズム (電子メールアドレスまたはウェブサイトのいずれかを含む) がこの記述に含まれることを検証すること。評価者は、このメカニズムの記述に、電子メールを暗号化するための公開鍵またはウェブサイトへの高信頼チャネルのいずれかを使用して報告を保護するための手法が含まれることを検証しなければならない。

5.2.5 ATE クラス：テスト

テストは、システムの機能的側面と、設計または実装の弱点を利用する側面について規定される。前者は ATE_IND ファミリによって行われるが、後者は AVA_VAN ファミリによって行われる。本 PP で規定される保証レベルにおいては、テストは広告される機能及びインタフェースに基づき、設計情報の利用可能性に依存して行われる。評価プロセスの主要なアウトプットのひとつは、以下の要件で規定されるテスト報告書である。

ATE_IND.1 独立テスト―適合 (ATE_IND.1)

開発者アクションエレメント：

ATE_IND.1.1D

開発者は、テストのための OS を提供しなければならない。

内容・提示エレメント：

ATE_IND.1.1C

OS は、テストに適していなければならない。

評価者アクションエレメント：

ATE_IND.1.1E

評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ATE_IND.1.2E

評価者は、TSF が仕様どおりに動作することを確認するために、TSF のサブセットをテストしなければならない。

適用上の注釈 : 評価者は、プラットフォームの最新の完全にパッチされたバージョン上で OS をテストすること。

保証アクティビティ

評価者は、テスト中にアプリケーションのクラッシュがあればそれを含め、システムテストの側面を文書化したテスト計画書とテスト報告書を作成すること。評価者は、アプリケーションのクラッシュがあればその根本原因を決定し、その情報を報告書へ含めなければならない。テスト計画書は、 [CEM] と本 PP の保証アクティビティの本体に含まれるすべてのテストアクションを網羅すること。

保証アクティビティに列挙されたテストのそれぞれについて 1 つのテストケースを用意する必要はないが、ST の該当するテスト要件のそれぞれがカバーされていることを評価者はテスト計画書中に文書化しなければならない。テスト計画書にはテストされるプラットフォームが特定され、そしてテスト計画書には含まれていないが ST に含まれているプラットフォームについては、そのプラットフォームをテストしないことについての正当化をテスト計画書が提供する。この正当化には、テストされるプラットフォームとテストされないプラットフォームとの相違を取り上げ、行われるべきテストにその相違が影響しないという論拠を示さなければならない。単にその違いが影響しないと主張するだけでは十分ではなく、根拠が提供されなければならない。ST 中に主張されるすべてのプラットフォームがテストされる場合には、根拠は必要とされない。テスト計画書にはテストされるべき各プラットフォームの構成が記述され、また AGD 文書に含まれるもの以外に必要な設定があれば、それも記述される。評価者は、テストの一部として、または標準的なテスト前の条件として、AGD 文書に従って各プラットフォームの設置及び設定を行うことが期待されていることに、注意すべきである。これには、特別なテストドライバまたはツールが含まれるかもしれない。ドライバまたはツールそれぞれについて、そのドライバまたはツールが OS 及びそのプラットフォームによる機能の実行に悪影響を与えないという、(単なる主張ではなく) 論拠が提供されるべきである。

またこれには、用いられるべき暗号エンジンの設定が含まれる。このエンジンによって実装される暗号アルゴリズムは、本 PP によって規定され、評価される暗号プロトコル (IPsec, TLS) によって用いられるものである。テスト計画書には、高レベルのテスト目的と共に、これらの目的を達成するために行われるべきテスト手順も特定される。これらの手順には、期待される結果も含まれる。

テスト報告書 (テスト計画書へ単に注釈を加えたものであってもよい) には、テスト手順が実施された際に行われたアクティビティが詳述され、またテストの実際の結果が含まれる。これは累積的な記述でなければならない。したがって、あるテストの実行が失敗となり、修正がインストールされ、そして次にテストの再実行が成功したということがあれば、報告には単なる「成功」の結果だけではなく、「失敗」及び「成

功」の結果 (及びそれを支持する詳細) が示される。

5.2.6 AVA クラス：脆弱性評定

本プロテクションプロファイルの第一世代については、オープンソースの調査を行って、これらの種類の製品にどのような脆弱性が発見されているのかを見出すことが評価機関に期待される。多くの場合、これらの脆弱性には基本的な攻撃能力を超える攻撃能力が要求される。侵入テストツールが作成されて評価機関へあまねく配付されるまでは、評価者には OS のこれらの脆弱性のテストを行うことは期待されない。評価機関には、ベンダによって提供された証拠資料から得られるこれらの脆弱性の存在する可能性についてコメントすることが期待される。この情報は侵入テストツールの開発と、将来のプロテクションプロファイルの開発のために用いられることになる。

AVA_VAN.1　脆弱性調査 (AVA_VAN.1)

開発者アクションエレメント：

AVA_VAN.1.1D

開発者は、テストのための OS を提供しなければならない。

内容・提示エレメント：

AVA_VAN.1.1C

OS は、テストに適していなければならない。

評価者アクションエレメント：

AVA_VAN.1.1E

評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

AVA_VAN.1.2E

評価者は、OS の潜在的脆弱性を識別するために、公知の情報源の探索を実行しなければならない。

適用上の注釈：公知の情報源には、脆弱性に関する共通脆弱性識別子 (CVE) 辞書が含まれる。また公知の情報源には、ファイルのウィルスチェックをフリーで提供するサイトも含まれる。

AVA_VAN.1.3E

評価者は、基本的な攻撃能力を持つ攻撃者からの攻撃に OS が耐えられることを決定するために、識別された潜在的脆弱性に基づいて侵入テストを実施しなければならない。

保証アクティビティ

評価者は、本要件に関連する所見を文書化する報告書を作成すること。この報告書は、物理的には ATE_IND で言及される全体的なテスト報告書の一部、または別文書であるかもしれない。評価者は、アプリケーションが利用するネットワークプロトコルと解析する文書フォーマットに特に注目して、同様のアプリケーションに発見されている脆弱性を見出すため、公開情報の検索を行うこと。評価者は、参考とした情報源

と発見された脆弱性を報告書に文書化する。

発見された脆弱性のそれぞれについて、評価者はそれが該当しないことを示す根拠を提供するか、またはそのほうが適切であれば脆弱性を確認するためのテストを (ATE_IND に提供されるガイドラインを用いて) 策定するかのどちらかを行う。どちらが適切かは、その脆弱性を利用するために必要とされる攻撃ベクタの評定によって決定される。例えば、脆弱性の悪用に専門的なスキルと電子顕微鏡が必要とされる場合には、テストは適当ではなく、適切な正当化が策定されることになるであろう。

附属書 A. オプション要件

セクション 2で示したように、本 PP の本体にはベースライン要件 (OS によって行われなければならないもの) が含まれている。これに追加して、これ以外の 3 種類の要件が 附属書 A、附属書 B、及び 附属書 Cに特定されている。(本附属書の) 第 1 の種類は、ST に含まれ得る要件であるが、OS が本 PP への適合を主張するためには必要とされないものである。(附属書 Bの) 第 2 の種類は、PP の本体中の選択に基づく要件である。特定の選択がなされた場合には、その附属書中の追加的要件が含まれなければならない。(附属書 Cの) 第 3 の種類は、本 PP へ適合するためには要求されないが、本 PP の将来のバージョンのベースライン要件に含まれることになっているコンポーネントであり、ベンダによる採用が推奨される。ST 作成者には、附属書 A、附属書 B、及び 附属書 Cに含まれる要件と関連し得るが列挙されていない要件 (例、FMT タイプの要件) もまた、ST に含まれることを保証する責任があることに注意されたい。

FCS_TLSC_EXT.4　TLS クライアントプロトコル

FCS_TLSC_EXT.4.1

OS は、X.509v3 証明書を用いる相互認証をサポートしなければならない。

適用上の注釈：TLS での X.509v3 証明書の利用は、FIA_X509_EXT.2.1において対処される。本要件は、TLS 相互認証のためにクライアントが TLS サーバへ証明書を提示できなければならないことを追加する。

保証アクティビティ

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する。

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

また評価者は、以下のテストを行う：

相互認証を要求するようサーバを設定し、次にサーバの CertificateRequest ハンドシェイクメッセージの CA フィールドの 1 バイトを改変する。改変された CA フィールドは、クライアントの証明書の署名に用いられた CA であってはならない。評価者は、コネクションが成功しないことを検証する。

FTA_TAB.1　デフォルト TOE アクセスバナー

FTA_TAB.1.1

利用者セションを確立する前に、OS は OS の許可されない利用に関して注意を喚起する警告メッセージを表示しなければならない。

保証アクティビティ

評価者は、OS マニュアル中の指示に従って、「TEST TEST Warning

Message TEST TEST」という注意喚起警告メッセージを表示するようOSを設定する。次に評価者はログアウトし、ログインができるようになる前に注意喚起メッセージが表示されることを確認する。

附属書 B. 選択ベース要件

本 PP の序説で示したように、本 PP の本体にはベースライン要件 (OS またはその基盤となるプラットフォームによって行われなければならないもの) が含まれている。これ以外にも PP の本体の選択に基づく追加の要件が存在し、特定の選択がなされた場合には、以下の追加の要件が含まれることが必要となる。

FCS_DTLS_EXT.1　DTLS の実装

FCS_DTLS_EXT.1.1

OS は、 [**選択 :** *DTLS 1.0 (RFC 4347)*、*DTLS 1.2 (RFC 6347)*] に従って DTLS プロトコルを実装しなければならない。

本要件は、FTP_ITC_EXT.1.1 での選択による。

保証アクティビティ

● ***テスト 1 :*** *評価者は、DTLS サーバとのコネクションの確立を試行し、パケットアナライザでトラフィックを確認し、そしてコネクションが成功しトラフィックが DTLS と特定されることを検証する。* *その他のテストは、FCS_TLSC_EXT.1 に列挙された保証アクティビティと組み合わせて行われる。*

FCS_DTLS_EXT.1.2

OS は、DTLS 1.2 (RFC 6347) に従った変更が許可される場合を除き、DTLS の実装には TLS の要件(FCS_TLSC_EXT.1) を実装しなければならない。

本要件は、FTP_ITC_EXT.1.1 での選択による。

適用上の注釈 : DTLS と TLS との違いは、RFC 6347 に概説されている ; それ以外の点では、これらのプロトコルは同一である。特に、TSF に定義される適用可能なセキュリティ特性については、2 つのプロトコルに違いはない。ゆえに、TLS に列挙されたすべての適用上の注釈と保証アクティビティは、DTLS 実装に適用される。

保証アクティビティ

評価者は、FCS_TLSC_EXT.1 に列挙された保証アクティビティを実行すること。

FCS_TLSC_EXT.2　TLS クライアントプロトコル

FCS_TLSC_EXT.2.10

OS は、以下の NIST 曲線を伴う Supported Elliptic Curves Extension を Client Hello にて提示しなければならない : [**選択 :** *secp256r1*、*secp384r1*、*secp521r1*] 及びその他の曲線なし。

*本要件は、**FCS_TLSC_EXT.1.1** での選択による。*

適用上の注釈：本要件は、認証及び鍵共有に許可される楕円曲線を、FCS_COP.1(3) 及び FCS_CKM.1及び FCS_CKM.2からの NIST 曲線に限定する。本拡張は、楕円曲線暗号スイートをサポートするクライアントに対して要求される。

保証アクティビティ

評価者は、Supported Elliptic Curves Extension 及び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構成可能かについて TSS に記述されていることを検証すること。TSS が Supported Elliptic Curves Extension が本要件を満たすように構成されなければならないことを指示する場合、評価者は、AGD ガイダンスに Supported Elliptic Curves Extension の構成が含まれていることを検証する。 *評価者は、以下のテストについても実行すること：* *評価者は、非サポートの ECDHE 曲線 (例、P-192)を用いる TLS コネクションで ECDHE 鍵交換メッセージを実行するようサーバを構成すること、また、評価者は、サーバの鍵交換ハンドシェイクメッセージの受信後、OS がコネクションを切断することを検証しなければならない。*

附属書 C. オブジェクティブな要件

本附属書にも、脅威に対抗するセキュリティ機能を規定する要件が含まれる。これらの要件は、いまだに実用化された技術においては広く提供されていないセキュリティ機能を記述しているため、現時点では本 PP の本体では必須とされない。しかし、これらの要件は、OS が依然として本 PP に適合するように ST へ含まれてもよいし、またできるだけ早くそれらが含まれることが期待される。

FCS_TLSC_EXT.3　TLS クライアントプロトコル

FCS_TLSC_EXT.3.1

OS は、Client Hello 中の signature_algorithms 拡張に以下のハッシュアルゴリズムを含む supported_signature_algorithms 値を提示しなければならない : [**選択 :** *SHA256*、*SHA384*、*SHA512*] 及びその他のハッシュアルゴリズムなし。

適用上の注釈 : 本要件は、クライアントによるディジタル署名検証の目的でサポートされるハッシュアルゴリズムを制限すると共に、サーバによるディジタル署名生成の目的でサポートされるハッシュにサーバを制限する。signature_algorithm 拡張は、TLS 1.2 のみによってサポートされる。

保証アクティビティ

評価者は、signature_algorithm 拡張について、そして要求されるふるまいがデフォルトで実施されるのか設定され得るのかのどちらであるか、TSS に記述されていることを検証する。本要件を満たすために signature_algorithm 拡張が設定されなければならないと TSS に指示されている場合、評価者は signature_algorithm 拡張の設定が AGD ガイダンスに含まれることを検証する。

また評価者は、以下のテストを行う :

評価者は、signature_algorithms 中のクライアントの HashAlgorithm 列挙に従えばサポートされない証明書を TLS コネクション中に送信する (例、SHA-1 署名を持つ証明書を送信する) ようにサーバを設定する。評価者は、OS 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する。

FPT_SRP_EXT.1　ソフトウェア制限方針

FPT_SRP_EXT.1.1

OS は、管理者規定の以下のものと照合するようなプログラム実行のみに制限しなければならない[**選択 :**

ファイルのパス、

ファイルのディジタル署名、

バージョン、

ハッシュ、

*[**割付 :** その他の特徴]*

]

適用上の注釈 : 割付は、容量として低レベルの粒度を提供する実装を許可する。制限は、実行可能プログラムの直接実行に対してのみ課される。たとえ、このデータがその後任意の計算に帰結する場合であっても、データを入力として取るインタープリタを禁止するものではない。

保証アクティビティ

ST で規定された選択それぞれについて、評価者は以下のテストが否定的な結果となることを保証する (即ち、評価者がそのアクションを完了するための許可を OS が拒否するような結果をそのアクションが招く):

- ***テスト 1 :*** *評価者は、核となる OS ディレクトリからのコード実行のみを許可するよう OS を設定すること。次に評価者は、許可されたリストにあるディレクトリからコードの実行を試行する。評価者は、実行を試行したコードが実行されることを保証する。*
- ***テスト 2 :*** *評価者は、中核となる OS ディレクトリからのコードの実行のみを許可するよう OS を設定する。次に評価者は、許可されたリストにないディレクトリからコードの実行を試行する。評価者は、実行を試行したコードが実行されないことを保証する。*
- ***テスト 3 :*** *評価者は、OS ベンダによって署名されたコードの実行のみを許可するよう OS を設定する。次に評価者は、OS ベンダによって署名されたコードの実行を試行する。評価者は、実行を試行したコードが実行されることを保証する。*
- ***テスト 4 :*** *評価者は、OS ベンダによって署名されたコードの実行のみを許可するよう OS を設定する。次に評価者は、他のディジタルオーソリティによって署名されたコードの実行を試行する。評価者は、実行を試行したコードが実行されないことを保証する。*
- ***テスト 5 :*** *評価者は、バージョンに基づいて特定のアプリケーションの実行を許可するよう OS を設定する。次に評価者は、同一バージョンのアプリケーションの実行を試行する。評価者は、実行を試行したコードが実行されることを保証する。*
- ***テスト 6 :*** *評価者は、バージョンに基づいて特定のアプリケーションの実行を許可するよう OS を設定する。次に評価者は、古いバージョンのアプリケーションの実行を試行する。評価者は、実行を試行したコードが実行されないことを保証する。*
- ***テスト 7 :*** *評価者は、アプリケーション実行形式のハッシュに基づいて実行を許可するよう OS を設定する。次に評価者は、ハッシュが一致するアプリケーションの実行を試行する。評価者は、実行を試行したコードが実行されることを保証する。*
- ***テスト 8 :*** *評価者は、アプリケーション実行形式のハッシュに基づいて実行を許可するよう OS を設定する。評価者は、アプ*

リケーションのハッシュが変更されるようにアプリケーションを改変する。次に評価者は、ハッシュが一致するアプリケーションの実行を試行する。評価者は、実行を試行したコードが実行されないことを保証する。

FPT_W^X_EXT.1　書込み XOR 実行メモリページ

FPT_W^X_EXT.1.1

OS は、 [**割付**：例外のリスト] を除いて、書込み及び実行の両方のアクセス権限を持つあらゆるメモリ領域の割当てを防止しなければならない。

適用上の注釈：書込み及び実行の両方のアクセス権限と共にメモリ割当てを要求することは、DEP によって提供されるプラットフォーム保護を阻害する。OS が例外 (例、実行時コンパイル) を提供しない場合には、「例外なし」が割付に示されるべきである。本要件の完全な実現にはハードウェアのサポートが要求されるが、これは一般的に利用可能である。

保証アクティビティ

評価者は、ベンダによって提供される開発者証拠資料を検査して、割付に列挙された場合を除いて、書込み及び実行アクセス権限と共にメモリ割り当てが行われないことを検証する。

- ***テスト1：****評価者は、書込み可能であると同時に実行可能でもあるメモリの割当てを試行するテストプログラムを取得または構築する。評価者はそのプログラムを実行し、書込み可能であると同時に実行可能でもあるメモリの割当てが失敗することを確認する。*
- ***テスト2：****評価者は、実行可能であるメモリの割当てを行い、その後そのメモリに書込み／変更アクセス権限の追加を要求するテストプログラムを取得または構築する。評価者はそのプログラムを実行し、プロセスのライフタイムのどの時点でもメモリが書込み可能であると同時に実行可能とはならないことを確認する。*
- ***テスト3：****評価者は、書込み可能であるメモリの割当てを行い、その後そのメモリに実行アクセス権限の追加を要求するテストプログラムを取得または構築する。評価者はそのプログラムを実行し、プロセスのライフタイムのどの時点でもメモリが書込み可能であると同時に実行可能とはならないことを確認する。*

附属書 D. 本来的に満たされている要件

本附属書では、本プロテクションプロファイルに適合した評価に合格した製品によって満たされるとみなされるべき要件を列挙する。しかし、これらの要件は SFR として明示的に特徴付けられておらず、また ST に含まれるべきでない。それらが単独の SFR として含まれないのは、評価の時間、費用、及び複雑さが増大させるからである。このアプローチは、[CC] パート 1、**8.2 コンポーネント間の依存性**によって許可される。

この情報は、具体的なセキュリティ管理策を含めることを求めるようなシステムエンジニアリングアクティビティの利益となる。プロテクションプロファイル適合評価は、これらの管理策が存在し、評価されたという証拠を提供する。

要件	満たされる根拠
FIA_UAU.1 — 認証のタイミング	FIA_AFL.1は、未認証の利用者を代行して行われるアクションを含め、認証するために必要なすべてのアクションを OS が行うことを暗黙的に要求する；ゆえに、これらのアクションを別の割付及びテストとして含めることは重複となる。
FIA_UID.1 — 識別のタイミング	FIA_AFL.1は、未識別の利用者を代行して行われるアクションを含め、認証するために必要なすべてのアクションを OS が行うことを暗黙的に要求する；ゆえに、これらのアクションを別の割付及びテストとして含めることは重複となる。
FMT_SMR.1 — セキュリティ役割	FMT_MOF_EXT.1は、利用者及び特権のアカウントを暗黙的に定義するような役割ベースの管理機能を規定する；ゆえに、別の役割要件を含めることは重複となる。
FPT_STM.1 — 高信頼タイムスタンプ	FAU_GEN.1.2は、OS がタイムスタンプを監査記録に関連付けることを明示的に要求する；ゆえに、別のタイムスタンプ要件を含めることは重複となる。
FTA_SSL.1 — TSF 起動セションロック	FMT_MOF_EXT.1は、セションロック管理の要件を定義する；ゆえに、別のセションロック要件を含めることは重複となる。
FTA_SSL.2 — 利用者起動ロック	FMT_MOF_EXT.1は、利用者起動セションロックの要件を定義する；ゆえに、別のセションロック要件を含めることは重複となる。
FAU_STG.1 — 保護された監査証跡格納	FPT_ACF_EXT.1は、監査ログを保護する要件を定義する；ゆえに、別の監査証跡保護要件を含めることは重複となる。

FAU_GEN.2 — 利用者識別情報の関連付け	FAU_GEN.1.2は、OS が各事象と関連する任意の利用者アカウントを記録することを明示的に要求する；ゆえに、利用者アカウントを各事象に関連付けるような別の要件を含めることは重複となる。
FAU_SAR.1 — 監査レビュー	FPT_ACF_EXT.1.2は、監査ログ (及びその他のオブジェクト) が特権を持たない利用者による閲覧から保護されることを要求する；ゆえに、監査情報のみを保護するための別の要件を含めることは重複となる。

附属書 E. エントロピー証拠資料と評定

本附属書では､OS によって用いられるエントロピー源に要求される補助的情報を記述する。

エントロピー源の証拠資料は、それを読んだ後で評価者が完全にエントロピー源を理解し、それが十分なエントロピーを供給すると信頼できる理由を完全に理解できるように、十分に詳細であるべきである。この証拠資料には、設計記述、エントロピーの正当化、運用条件及びヘルステストという､複数の詳細なセクションが含まれるべきである。この証拠資料は､TSS の一部である必要はない。

E.1 設計記述

証拠資料には､すべてのエントロピー源のコンポーネントの相互作用を含め､各エントロピー源の全体的な設計が含まれなければならない。製品に含まれるサードパーティのエントロピー源についても、設計に関して共有可能なあらゆる情報が含まれるべきである。

証拠資料には、どのようにエントロピーが作り出されるのか、及びテストの目的で未処理(生の)データをエントロピー源の内部からどのように取り出せるかを含め、エントロピー源の動作を記述すること。証拠資料では、エントロピー源の設計の概略説明(ウォークスルー)が行われ、エントロピーがどこに由来し、次にどこへエントロピー出力が渡されるのか、生の出力に対するあらゆる後処理(ハッシュ､XOR 等)、もし保存される場合にはどこに保存されるのか､そして最後に、どのようにエントロピー源から出力されるのかを示すべきである。処理に課されるあらゆる条件(例、ブロッキング等)があれば、それについてもエントロピー源の設計で記述されるべきである。図や例を利用することが推奨される。

この設計には､エントロピー源のセキュリティ境界の内容の記述､及び境界外部の敵対者がエントロピー割合に影響を与えることができないことをセキュリティ境界がどのように保証するかについての記述も含まれなければならない。

サードパーティのアプリケーションが RBG へエントロピーを追加できる方法が実装されている場合､設計記述にはその記述が含まれなければならない。電源切断から電源投入までの間で保存される RBG 状態があれば、その記述が含まれなければならない。

E.2 エントロピーの正当化

エントロピー源の予測不可能性がどこに由来し、(この特定の OS による) RBG 出力を使う複数の用途に対して、十分なエントロピーをエントロピー源が供給できることをなぜ確信できるのかについての技術的な論拠が存在すべきである。この論拠には､期待される最小エントロピー割合(即ち、情報源データの 1 ビットまたは 1 バイト当たりの最小エントロピー(ビット単位))の記述と､十分なエントロピーが OS の攪拌シード生成処理へ投入されることを説明する記述を含むこと。この論考は、なぜエントロピー源がエントロピーを含むビット列を生成すると確信できる理由の正当化の一部となる。

期待される最小エントロピー量を正当化するために必要な情報量は、製品に含まれるエントロピー源の種別に依存する。

開発者が提供するエントロピー源について､最小エントロピー割合を正当化するため､大量の生の情報源ビットが収集され､統計学的なテストが実行され､統計学的なテストから最小

エントロピー割合が決定されることが期待される。現時点では、特定の統計学的なテストは要求されないが、各出力における最小エントロピーの量を決定するために何らかのテストが必要であることが想定される。

サードパーティが提供するエントロピー源について、OS ベンダは、エントロピー源の設計及び生のエントロピーデータへのアクセスが制限されるため、証拠資料にはこのサードパーティ情報源から取得される最小エントロピー割合の見積りが示されること。ベンダが最小エントロピー割合を「想定」することは受け入れ可能だが、この想定は提供される証拠資料に明確に記述されなければならない。特に最小エントロピーの見積りは特定されなければならず、その想定が ST に含まれなければならない。

エントロピー源の種別にかかわらず、正当化は、ST に示されるエントロピーで DRBG が初期化される方法が含まれること。例えば、最小エントロピー割合に DRBG へシード値を供給するために使用される情報源のデータ量が乗算されること、または情報源のデータ量に基づき期待されるエントロピー割合が明示的に示され、統計学的な量と比較されることを検証することによって行われる。DRBG へシード値を供給するために使用される情報源のデータ量が明確でなく、または計算された量が明示的にシード値と関連付けられていない場合、証拠資料は完結したとは考えられない。

エントロピーの正当化には、サードパーティのアプリケーションからの追加データも、再起動の間で保存される状態から追加されるデータも、一切含めてはならない。

E.3 動作条件

エントロピー割合は、エントロピー源それ自体が制御できない条件によって影響を受けることがある。例えば、電源電圧、周波数、温度、及び電源投入後の経過時間等は、エントロピー源の動作に影響し得る要因のほんの数例である。このように、証拠資料にはエントロピー源が乱数データを生成すると期待される動作条件の範囲も記述されることになる。これには、これらの条件の下でエントロピー源が動作し続けることを保証するために、システムの設計に取り入れられた対策が明確に記述されることになる。同様に、証拠資料にはエントロピー源が動作不良または矛盾した動作となることがわかっている条件も記述されなければならない。エントロピー源の故障または機能低下を検出するための方法が含まれなければならない。

E.4 ヘルステスト

さらに具体的には、すべてのエントロピー源のヘルステスト及びそれらの根拠が、文書化されること。これには、ヘルステストの記述、各ヘルステストが実行される頻度や条件(例、起動時、連続的、またはオンデマンド)、各ヘルステストでの期待される結果、及び各テストがエントロピー源において 1 つ以上の故障を検出するために適切であるという確信を示す根拠を含むこと。

附属書 F. 参考資料

識別子	タイトル
[CC]	情報技術セキュリティ評価のためのコモンクライテリア— ● パート 1 : 概説と一般モデル、CCMB-2012-09-001、バージョン 3.1 改訂第 4 版、2012 年 9 月。 ● パート 2 : セキュリティ機能コンポーネント、CCMB-2012-09-002、バージョン 3.1 改訂第 4 版、2012 年 9 月。 ● パート 3 : セキュリティ保証コンポーネント、CCMB-2012-09-003、バージョン 3.1 改訂第 4 版、2012 年 9 月。
[CEM]	情報技術セキュリティ評価のための共通方法—評価方法、CCMB-2012-09-004、バージョン 3.1、改訂第 4 版、2012 年 9 月。
[CESG]	CESG - End User Devices Security and Configuration Guidance
[CSA]	Computer Security Act of 1987, H.R. 145, June 11, 1987.
[OMB]	Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, OMB M-06-19, July 12, 2006.

附属書 G. 頭字語

頭字語	意味
AES	Advanced Encryption Standard
ANSI	American National Standards Institute (米国規格協会)
API	Application Programming Interface (アプリケーションプログラミングインタフェース)
ASLR	Address Space Layout Randomization (アドレス空間配置ランダム化)
CESG	Communications-Electronics Security Group (英国電子通信安全局)
CMC	Certificate Management over CMS
CMS	Cryptographic Message Syntax
CN	Common Names (コモン名)
CRL	Certificate Revocation List (証明書失効リスト)
CSA	Computer Security Act
DEP	Data Execution Prevention (データ実行防止)
DES	Data Encryption Standard
DHE	Diffie-Hellman Ephemeral
DNS	Domain Name System (ドメイン名システム)
DRBG	Deterministic Random Bit Generator (決定論的乱数ビット生成器)
DSS	Digital Signature Standard
DT	Date/Time Vector
DTLS	Datagram Transport Layer Security (データグラムトランスポート層セキュリティ)
EAP	Extensible Authentication Protocol (拡張認証プロトコル)
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm(楕円曲線ディジタル署名アルゴリズム)

EST	Enrollment over Secure Transport
FIPS	Federal Information Processing Standards (米国連邦情報処理規格)
DSS	Digital Signature Standard
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol (ハイパーテキスト転送プロトコル)
HTTPS	Hypertext Transfer Protocol Secure
DSS	Digital Signature Standard (米国ディジタル署名規格)
IETF	Internet Engineering Task Force
IP	Internet Protocol (インターネットプロトコル)
ISO	International Organization for Standardization (国際標準化機構)
IT	Information Technology (情報技術)
ITSEF	Information Technology Security Evaluation Facility (情報技術セキュリティ評価機関)
NFC	Near Field Communication
NIAP	National Information Assurance Partnership (米国国家情報保証パートナーシップ)
NIST	National Institute of Standards and Technology (米国国立標準技術研究所)
OCSP	Online Certificate Status Protocol (オンライン証明書状態プロトコル)
OID	Object Identifier (オブジェクト識別子)
OMB	Office of Management and Budget (米国行政管理予算局)
OS	Operating System (オペレーティングシステム)
PII	Personally Identifiable Information (個人識別可能情報)
PKI	Public Key Infrastructure
PP	Protection Profile (プロテクションプロファイル)
RBG	Random Bit Generator (乱数ビット生成器)
RFC	Request for Comment
RNG	Random Number Generator (乱数生成器)

RNGVS	Random Number Generator Validation System (乱数生成器検証システム)
SAN	Subject Alternative Name (サブジェクトの別名)
SAR	Security Assurance Requirement (セキュリティ保証要件)
SFR	Security Functional Requirement (セキュリティ機能要件)
SHA	Secure Hash Algorithm (セキュアハッシュアルゴリズム)
S/MIME	Secure/Multi-purpose Internet Mail Extensions
SIP	Session Initiation Protocol (セション確立プロトコル)
SWID	Software Identification (ソフトウェア識別情報)
TLS	Transport Layer Security (トランスポート層セキュリティ)
URI	Uniform Resource Identifier (統一資源識別子)
URL	Uniform Resource Locator (統一資源位置指定子)
USB	Universal Serial Bus (ユニバーサルシリアルバス)
XCCDF	eXtensible Configuration Checklist Description Format (セキュリティ設定チェックリスト記述形式)
XOR	Exclusive OR (排他的論理和)